区块链模组牵引物联网
迈入泛信任新世界

BoAT 区块链模组产品白皮书 V1.0

许刚

摩联科技 CTO

2019 年 12 月 25 日，区块链模组联盟在南京成立，九大模组厂商现场共同发布基于 BoAT Framework 的主流品牌区块链模组产品，这标志着物联网+区块链的融合创新走向纵深，产业界正携手从源头探索物联网数据价值。摩联科技 CTO 许刚详细介绍了区块链模组的协议架构，并匹配不同的物联网应用领域提出三大典型模组类型的区块链钱包软件框架 BoAT Framework 对应特点。

区块链模组如何帮助扫除区块链+物联网融合之路的重重藩篱？

根据 Gartner 对 500 多家美国公司的调研，有 75%的公司已经采用或计划在 2020 年底采用区块链，其中 86%计划实施物联网+区块链的应用。区块链作为一种基础设施，它与物联网的结合，能够为后者提供广泛的信任，从而为数据共享和数据价值的传递提供支撑。

尽管 Gartner 的调研令人振奋，但物联网与区块链从相识，到联姻，再到结出果实，仍然会面临许多挑战。这些挑战既包括在芯片、模组、设备、运营等物联网行业链条中找到令各方多赢的商业模式，也包括在技术上跨越通信、云、链、安全等多个领域的技术整合，还涉及 TTM（Time To Market）、BOM 成本、研发成本、运营成本等的平衡。这些挑战被妥善解决，才有可能产生可持续的物联网+区块链商业场景应用。

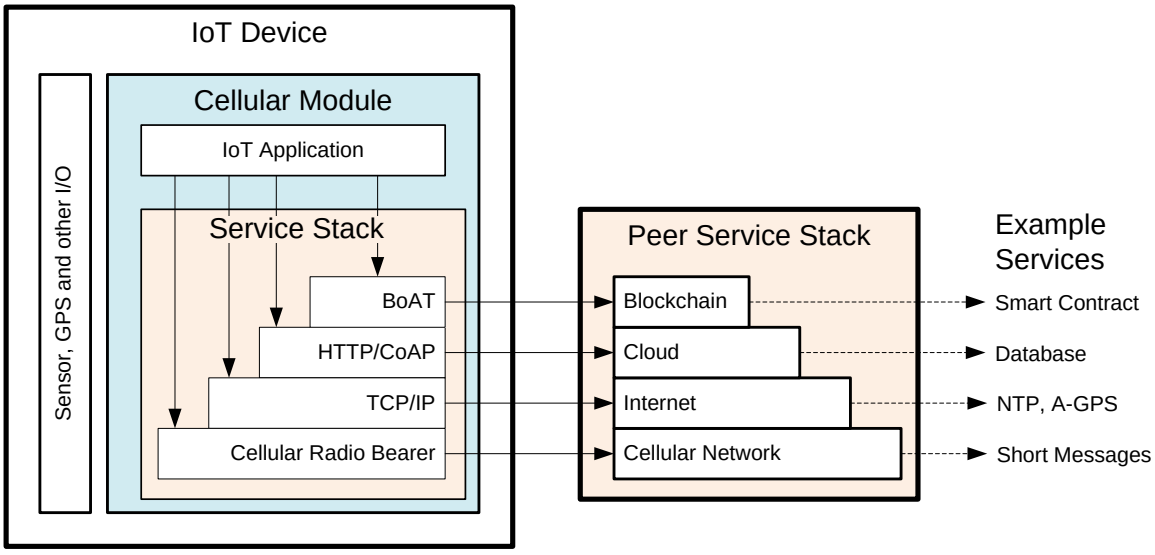
在物联网行业链条中，往往末端的商业场景运营商对区块链可能发挥的作用有敏锐的嗅觉，但其传统的物联网设备供应商，很可能不具备开发区块链功能的能力，无法提供满足其需求的设备。而另一方面，主流的区块链服务供应商，往往对碎片化的物联网行业了解也不深，试图将其区块链服务落地在碎片化的物联网设备中也会遇到很多困难。在这样的背景下，具备连接区块链能力的通信模组，即区块链模组应运而生。

蜂窝通信模组是物联网设备中的核心部件。从协议栈的角度看，蜂窝模组向物联网应用提供了一套通信业务栈。业务栈的底层是基础蜂窝通信业务，通过 2G/3G/4G/5G 的无线承载（RB, Radio Bearer），提供诸如 PLMN（Public Land Mobile Network）选择、空闲态和/或连接态及其移动性、数据传输、短消息等蜂窝通信能力。在基础蜂窝通信能力之上，蜂窝模组一般集成了 TCP/IP 协议栈，使得应用可以通过 TCP 或 UDP 连接 Internet，获得相应业务服务。模组在 TCP/IP 协议之上通常还会集成

HTTP, CoAP, MQTT, TLS/DTLS 等更上层的偏应用的协议，应用通过这些协议，可以方便地与云（服务器）交换数据，实现设备管理、数据上传等业务。

从协议栈角度看，这些协议自底向上层叠，下层协议向上层协议提供服务，上层协议的数据是下层协议的载荷。然而有趣的是，尽管这些协议具有层次关系，但它们每一层却都是开放的。顶层的物联网应用，既可以向 HTTP 等上层协议提出 POST/GET 等业务请求，也可以向中层的 TCP/IP 层提出基于 TCP 或 UDP 的业务请求，甚至还可以直接向基础的蜂窝通信协议提出收发短信这样的业务请求。这种有层次却又开放的协议栈体系，构造了非常灵活多样的业务生态。

区块链模组并非全新的模组品类。如下图所示，区块链模组本质上就是在上述开放的协议栈层次体系上，又叠加了一层区块链客户端协议。应用可以向这层区块链客户端协议，请求区块链交易、智能合约调用等区块链业务。区块链客户端协议再进一步结合密钥生命周期管理、设备 Attestation 等，就构成了基于模组的区块链软件框架（BoAT Framework, Framework for Blockchain of AI Things），或者称为区块链设备钱包（Device BoAT Wallet）。



区块链模组支持下的物联网业务栈

一方面，物联网行业高度碎片化，无论场景还是设备，差异都很大，BoAT 通过适配用于多种物联网场景的不同蜂窝模组，使得各种场景下的物联网设备具备数据上链的能力。另一方面，区块链行业也呈现多样化，BoAT 通过适配多种适用于物联网领域的主流区块链，使得物联网数据上链能够有多样化的选择。

从物联网行业视角看，区块链模组为物联网应用搭乘区块链航船，提供了快捷的舷梯。而反过来，从区块链行业视角来看，区块链模组也为区块链业务落地物联网场景，提供了一站式的直达通道。从物联网行业视角看，物联网中的区块链应用场景，与以人为主要使用者的区块链应用场景，存在较大的差异。

	物联网的区块链应用场景	人为使用者的区块链应用场景
典型业务举例	物联网数据上链存证	转账 dAPP（游戏、投票等等）
行为确定性	设备行为是事先编程的，基本是确定性行为	人作为操作主体，行为通常有较高的不确定性
设备类型	设备类型广泛	集中于智能手机和个人计算机
处理器	处理器以 ARM 为主，RISC-V 正在茁壮成长。 处理能力不同设备差异很大。处理器从单核几十 MHz 到八核 2GHz 甚至带有 GPU 都有	主流智能手机均为 ARM，个人计算机均为 x86。不同设备处理器大致相似，处理能力相差有限。
操作系统	各种 RTOS、linux、安卓、Windows 等都有	智能手机集中在安卓和 iOS，个人计算机集中在 Windows 和 MacOS
设备资源	不同设备差异很大，存储器容量从几十 kB 到几十 GB 都有，	无论智能手机还是个人计算机，资源差异有限
功耗要求	有持续供电的；也有要求苛刻，使用不可充电的电池供电且要保持数月甚至数年可用的	功耗要求相对宽松，软件层面一般无需特别考虑
通信能力	不同设备差异较大，从偶发性传输少量数据的，到持续高速传输数据的都有	具有高速通信能力

区块链自中本聪提出比特币以来，在其长期的发展中，是以给人用为主的。总体而言，与物联网的市场碎片化、需求离散化、软硬件平台差异化相比，人用区块链的差异性相对较小。近年来，结合物联网，成为了区块链的一个应用分支，但物联网的碎片化、离散化、差异化，成为区块链行业面前的一条天堑。区块链行业亟需在这条天堑上摆渡的技术手段，连接起一个个碎片化的物联网应用孤岛，而区块链模组正是这样一艘将物联网世界的碎片化、离散化、差异化屏蔽起来，向区块链世界呈现一致界面的摆渡船。

区块链模组能成为这样一艘摆渡船，其关键是区块链钱包软件框架 BoAT Framework 对不同的蜂窝模组类型进行针对性的适配。

蜂窝模组之所以能在物联网行业中发挥巨大作用，一个关键因素是，物联网产业链条高度碎片化，但在无线通信的需求上却非常聚焦。在解决无线通信能力基础上，为了更加匹配不同的物联网应用领域，蜂窝模组又细分为几个主要的类型。

模组类型	主要特点	应用场合举例
智能模组	SoC 芯片能力与低端手机芯片相当，具有多核 CPU 和 GPU，以安卓为操作系统，支持 4G 等高速率通信制式。适合带有屏幕，有复杂人机交互的物联网应用场景 典型 SoC 芯片如高通 SDM450，其中应用处理器为八核 Cortex A53，典型工作时钟 1.8GHz，典型存储器容量为几 GB RAM，十几 GB Flash 量级	带彩屏的自动贩售机 行业手持终端（如 POS 机）
标准模组	SoC 芯片一般具有处理能力较强的单核应用处理器，以 linux 或 RTOS 为操作系统，支持 4G 或 NB-IoT、eMTC 等通信制式。适合有持续供电，没有直接人机界面或只需要按钮/指示灯一类简单人机界面的物联网应用场景 典型 SoC 芯片如高通 9207，其中应用处理器为单核 Cortex A7，典型工作时钟 1.2GHz，典型存储器容量为数百 MB RAM，几 GB Flash 量级	车载 TBox 电力设备监控
瘦模组	SoC 芯片采用低功耗的弱应用处理器（或与通信协议共用处理器），以 RTOS 为操作系统，支持 NB-IoT 或 eMTC 等低速通信制式。适合对成本要求苛刻或者以电池供电，工作占空比很低，传输数据量很小，没有直接人机界面的物联网应用场景 典型 SoC 芯片如海思 Boudica 150，其中应用处理器为单核 Cortex M0，典型工作时钟约 50MHz，典型存储器容量为数十 kB RAM 和数百 kB Flash 量级	表计 智能锁

基于对物联网碎片化、离散化、差异化的理解，针对这些不同的模组类型，区块链钱包软件框架 BoAT Framework 具有不同的特点。

模组类型	区块链钱包软件框架主要特点
智能模组	应用处理器能力强，存储空间较宽松，区块链钱包软件框架可以采用 Java、JavaScript 等高级语言，具有良好的跨平台特性，易于和物联网应用集成。而区块链厂商为满足基于智能手机和基于浏览器的使用，通常都会提供 Java 和 JavaScript 版本的区块链客户端软件，这也使得在智能模组上更容易集成区块链客户端与密钥生命周期管理等其他配套功能，实现功能较为完备的区块链钱包软件框架。 SoC 芯片脱胎于手机芯片，一般继承了 TEE（可信执行环境）、Secure Boot、fuse 等安全特性，区块链协议报文组装、私钥生命周期管理和签名、加密运算等敏感操作可以在 TEE 中处理，具备达到金融级安全的条件。 注：尽管智能模组具有和低端手机相当的处理能力和存储能力，不过受限于流量资费以及 Flash 存储空间和擦写寿命，采用智能模组的物联网设备仍属于能力受限物联网设备，一般不下载存储完整账本或参与节点共识。
标准模组	受处理器能力和存储空间限制，区块链钱包软件框架通常以 C/C++语言编写，不同的模组平台根据芯片、编译环境、操作系统环境等的不同，需要进行移植。 此类 SoC 芯片有些具有 TEE 能力，有些不具备 TEE 能力，有些虽然具备 TEE，但 TA（可信应用）不具有二次开发能力。具备 TEE 且具有 TA 二次开发能力的芯片平台可以将敏感操作放在 TEE 内。不具备 TEE 能力，或者虽有 TEE 但不支持 TA 二次开发的芯片平台，需要根据安全要求和成本要求的不同，采用外挂加密芯片，或者采用软件混淆加固的方式保护敏感信息和敏感操作。 安全和成本是一对矛盾。过高的安全技术所导致的物联网设备成本上涨，有可能导致薄利的物联网相关厂商放弃使用区块链。而过低的安全技术所导致的安全风险可能带来的损失，也有可能导致物联网厂商放弃使用区块链。安全与成本的平衡点，通常应该使攻击者的攻击成本远大于攻击成功所获得的利益。这是一种经济学安全。
瘦模组	SoC 的 CPU 处理能力和存储空间限制很大，对耗电要求通常苛刻，区块链钱包软件框架一般以 C 编写，并针对具体应用场景进行定制移植，取消不必要的功能，尽可能减少资源占用。 如果 SoC 芯片自身不支持区块链签名和加密所需的密码学算法（例如区块链中常用的 ECDSA secp256k1 椭圆曲线签名算法），受处理能力和存储空间限制，以软件方式实现密码学算法可能不具有可行性，需外挂安全芯片，或借助定制 SIM 卡，实现密码学算法和密钥管理。 此类主流 SoC 芯片也普遍不具有 TEE 能力，但某些芯片厂商在尝试具备相关安全能力的下一代芯片，可能成为将来瘦模组的新选择。后者有可能在芯片开发时就支持相关密码学算法。

另一方面，从区块链行业视角来看，区块链模组能成为一艘摆渡船，亦在于 BoAT Framework 对不同的区块链及其合约调用接口，进行针对性的适配，使得多样性的区块链呈现相对一致的界面给物联网应用。

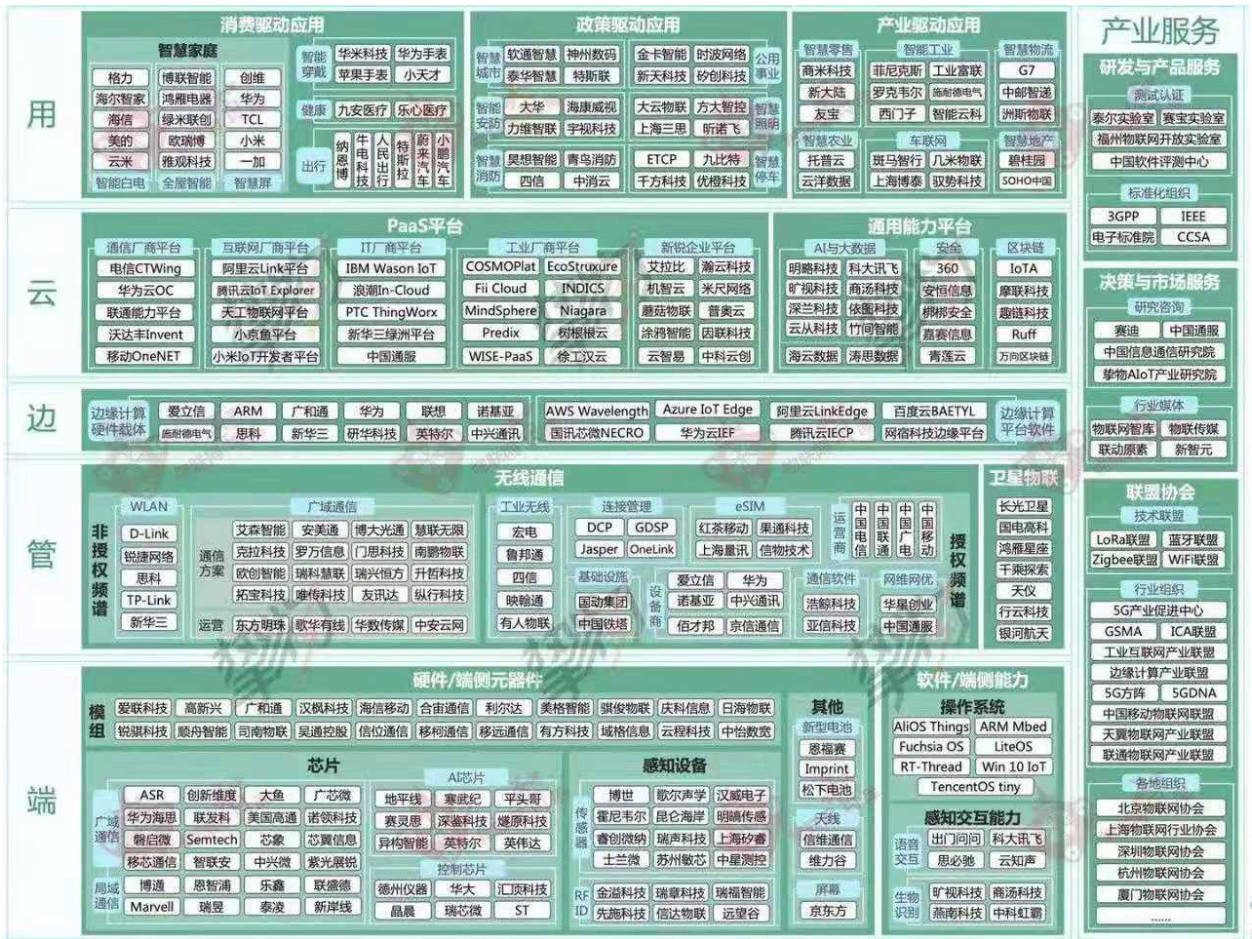
据不完全统计，目前各种区块链已经有上百种，它们有的以高 TPS 见长，有的主打隐私保护，有的注重扩展性。尽管只要是支持智能合约的链，都有用于物联网场景的可能，但现实中，由于物联网行业的碎片化，物联网+区块链应用中的区块链的选择，往往受到应用场景中的各种不同诉求的影响，呈现一定的差异化。区块链模组作为一种通用零部件，必须为物联网应用提供一定的区块链选择灵活性，这对物联网+区块链生态多样性至关重要。

例如，由万向区块链和矩阵元共同开发的 PlatONE，其特色是隐私计算，在不揭示明文数据的前提下，向其他人共享数据所含有的特定信息，适合对数据隐私特别敏感却又要进行数据共享的应用场景。而 Hyperledger Fabric 则具有很高的 TPS（相应的去中心化程度较低），适合数据上链频繁，但组织间信任度较高，无需完全依赖去中心化信任的场合。

尽管不同的链的协议接口有很多区别，但 BoAT Framework 将其封装为形式尽可能一致的一组对物联网应用的接口，使得基于区块链模组的物联网应用能够更从容地选择较适用的区块链。

物联网+区块链生态：以“利益相关人”为中心

根据最新发布的《中国物联网产业全景图谱报告2020》，物联网+区块链融合生态正在成为“网络型基础设施”的重要组成部分，对整个国民经济具有乘数效应和撬动效应。既然是基础设施，那么必然与过去单纯的公司制利益分配方式不同。围绕利益相关人构建的面向商业模式和技术创新的生态，其核心包括用户、投资者（政府&私人）、企业、开发者和研究机构。



❶ 用户使用区块链应用 dAPP、产品或者服务来实现数据资产的交易等服务；这些应用包括投票、治理、数据存储、ID 鉴权甚至包括商业流程中伴随履约相关的支付和其他金融操作。

❷ 投资者是指投入资本参与区块链生态建设的政府、单位或者个人。除了追求收益，更多的投资人是基于使命感和肯定区块链价值，希望区块链更好解决社会和经济类问题。

❸ 融合生态中的企业分为两部分，一类来自物联网行业的软件、硬件和系统运营商，他们在商业活动中使用区块链，作为行业领导者，积极为广大客户和最终用户带来 5G、IoT、人工智能等新技术。另一类则区块链技术方案公司，他们帮助实现构建区块链节点，积极参与区块链网络的共识机制。他们帮助传统物联网终端提供端到端的区块链解决方案。

❹ 社区开发者是另一支在融合生态中不可忽视的重要力量，作为开放生态，需要鼓励更多的应用开发者、产品和服务提供方使用区块链协议和平台实现分布式的应用创新并提供有力的技术支持。目前区块链主流协议都有开源社区。

❺ 研究机构和联盟协会也是我们生态不可或缺的组成部分，“教育胜过恐惧”新技术带来变革的机会，但在实现其潜力的道路上仍然有非常多的障碍，我们需要来自专业公正的第三方研究机构，带来中立冷静的观点以帮助教育公众。

区块链+物联网接下来将在哪些场景下重点发力?

本文中，我们参考 ITU-T FG DLTD2.1 Distributed ledger technology use cases 的分类方法，将案例以水平领域进行划分，物联网+区块链的应用主要涉及 5 大领域：

❶ 物联网身份认证管理

区块链技术可以通过加密技术和隐私计算来保护数字身份，个人和商业团体可以利用公私秘钥上链的方法，对存储和鉴权过程进行更有效的控制。通过去中心化、开源的区块链技术，配合身份管理工具，我们可以构建一个不可篡改的数字水印，为所有的实时交易进行签名和验签。

❷ 物联网设备安全防护

出于成本压力，物联网终端缺乏有效的安全保护机制，极易被挟持并对特定网络服务进行 DDoS 攻击，恶意软件可以通过控制穿戴设备、物流跟踪、无线抄表、共享单车、车载 Tbox、智慧路灯、智慧烟感等大量行业终端，使得城市、交通、供应链金融甚至儿童暴露在危险之下。通过安全管理机制，比如对资产和信息分类、威胁评估、风险评估来识别威胁，资产分类，系统漏洞分析，从而增加系统韧性、加密性、审计和透明度，实现全面阻止 DDoS 攻击，加强对可信 IoT 设备安全管理。

❸ 物联网数据管理能力

IDC 最新的预测表明，2025 年，随着 5G 的到来，全球数据总量中

过为所有的物联网设备设置一个唯一 XID，机器与机器进行沟通，通过区块链技术即可进行机器支付。基于去中心化的共识机制，提供智能合约技术，将智能设备变成可以自我维护和调节的独立个体。50% 来自于物联网设备，这部分的总量在 400 亿台规模，大概会是全球人口的 5 倍。通过引入区块链的公私钥加密签名技术，不仅可以有效改善了传统数据存储模式的中心化、易被攻击篡改的缺陷，更能从物联网数据产生的源头直接实时上链，将物联网智能终端全生命周期内所有活动信息原原本本实时签名，并存储到参与各方的区块链上，实现数据源头的隐私保护。

❹ 物联网网络基础设施运维管理

遍布全球的物联网海量设备构建的公共基础设施未来面临三大运维挑战：（1）日常维护、巡检等工作，耗费大量人力和时间；（2）运维数据也可能面临造假不信任等问题；（3）中心化的云和大型服务器群相关基础设施和维护成本高，短时数据处理能力有上限，过多数据上传将冲击网络。基于物联网+区块链+边缘计算等技术，可以减轻或解决这些问题。通过设备现场大量的温度、湿度传感器或者摄像头，实时获取各类运维数据和环境数据，从而实现数据自动采集和可信链上存证。

❺ 基于隐私保护的可信机器支付能力

物联网中海量智能硬件最大的问题就是数据无法可信安全的共享。通过为所有的物联网设备设置一个唯一 XID，机器与机器进行沟通，通过区块链技术即可进行机器支付。基于去中心化的共识机制，提供智能合约技术，将智能设备变成可以自我维护和调节的独立个体。

就像杰弗里·韦斯特在《规模》中提到的："你不可能靠一块木板跨越旧金山湾，为了在其上搭建桥梁，我们需要走上一条长长的进化征途，跨越多个创新层次，最终发现铁矿，发明吊桥。"随着区块链模组联盟的成立，主流模组厂商将基于 BoAT Framework 发布各自品牌的区块链模组产品，积极探索基于创新的物联网进化之路。BoAT 将成为区块链世界与碎片化、离散化、差异化的物联网世界之间的摆渡船，牵引物联网行业迈入基于区块链的泛信任新世界。

联盟核心成员代表金句

应凌鹏 广和通 CEO

作为最早推出区块链模组的行业先行者，广和通最早提出 MaaS（Module as a Service，“模块即服务”）战略。广和通成立 20 年以来，始终焕发着蓬勃的生命力，这主要得益于我们强大的研发实力和对新技术的持续投入。MaaS 战略是希望用模组改变商业模式，帮助我们的客户做数字化转型的战略地图。如何从大数据和万物互联中获利，MaaS 将是不可或缺的一环。早在 2019 年 4 月联通 5G 大会上，我们就关注到陈晓天总和肖风总针对“区块链+5G”的讲话，这也给了我们极大的信心投身到物联网+区块链的创新中来。非常荣幸加入到创新中心并共同发起区块链模组联盟，在联通物联网和万向区块链合力打造的大平台上，将 MaaS 与 BoAT SDK 结合起来，一起为数据治理做一份贡献。

刘明辉 移远通信副总经理

区块链模组是物联网的重要入口，今天我们在产品研发和客户服务过程中，越来越多地需要考虑数据的安全和隐私问题。非常荣幸加入物联网+区块链创新中心，从 6 月份和摩联科技一起发布全球首批 5G 区块链模组到成为区块链模组联盟的共同发起人，与联通物联网、万向区块链、摩联科技等多家物联网和区块链头部科技企业合作，共同帮助各类 4G/5G 物联网设备更好地实现可信身份认证与数据隐私保护。未来，移远通信将加快推进区块链技术的创新发展，为物联网设备提供更加安全、稳定、快速的连接，催生多样化的应用场景，赋能传统行业数字化转型，这正是我们做物联网的初心。

杜国彬 美格智能 CEO

区块链模组作为本地设备上链的重要一环，在广泛的 IoT 链接中将起到上链保证作用，尤其是在金融资产，资产残值率保障，农业活体资产等领域。美格智能区块链模组致力于为客户提供安全、简易和可靠的上链技术保证，依靠在蜂窝网络超过十年的基带技术的积累经验，确保客户产品简易、安全的上链，实现产品的价值管理。

肖悦赏 有方科技 CTO

区块链与 IoT 行业应用的结合将首先在金融、保险、资产管理相关的场景下开始，确保资产状态和数据可信共享（交易），降低对物联网设备的重复投入。目前，区块链在终端模组上的挑战有两点：（1）如何在 NB/CAT-M 等瘦终端实

现“轻”集成？（2）如何保证传感器等原始数据的可信性？有方科技将与摩联科技一起在数据源头深入研究，针对具体应用，基于 Bo

AT SDK 优化现有的安全解决方案，即在蜂窝模块和数据采集单元，也需要考虑安全可信的数据交互。

姚楠 高新兴物联模块产品线总经理

作为一家全球知名的高科技企业，高新兴凭借卓越的研发能力和技术判断力，坚持以持续的技术创新不断为客户创造价值。作为 IMT-2020 C-V2X 工作组、5G 自动驾驶联盟、中国智能交通产业联盟的成员，高新兴与联盟伙伴和战略合作伙伴长期保持深入合作，致力于提供可信的物联网链接技术和产品。本次，高新兴物联更是作为区块链模组联盟的共同发起人，与联通物联网、万向区块链、摩联科技等一起，面向 5G 演进，在多类型模组中植入 BoAT SDK 实现区块链技术的部署。

李亚春 利尔达蜂窝物联网总经理

一直以来产业生态应用依托物联网技术不断地迭代升级以实现“设备即服务”，利尔达作为物联网模组和应用解决方案提供商，之前帮客户很多时候解决的是设备联网，终端传感器数据上云的诉求，重点解决了传感器数据采集的完整性，数据传输的可靠稳定性，然而区块链融合物联网应用就是要解决数据的可信问题，所以利尔达希望和区块链产业合作伙伴一起深度合作在客户原来产品架构上我们提供一套客户可以快速集成，低成本集成的设备上链的完整解决方案，以让更多的物联网传感设备实现上链，然而因为很多物联网传感设备 MCU 处理能力有限，功耗指标敏感，所以我们在设备或者模组侧集成开发上链的方案的时候需要做一些新的架构和处理优化，甚至匹配不同行业，我们要做细分行业上链的定制化解决方案以实现产品上链后其他产品关键指标不受影响。

潘峰 移柯通信副总经理

移柯通信从成立之初就明确制订一个专注于蜂窝移动物联网行业的长期计划并在过去的 10 年间深耕行业，积累了丰富的行业经验和客户资源。模组行业单纯的硬件行业毛利率不断下降，这几乎是灰犀牛式的危机。最好的应对策略是积极主动的改变自己，通过广泛的跨界合作来寻求新的发展机遇。这次很荣幸作为区块链模组联盟的共同发起人，这也是公司的关键战略举措。目前，移柯通信与摩联科技已经推出了基于摩联科技 BoAT SDK 的区块链智能模组 LYNQ®智能模组 SMART 系列产品阵列。未来我们将和联盟合作伙伴一起为各行各业提供更加安全、稳定、可靠的链接能力，迎接新数字经济的到来。