

区块链及其在航空发动机领域的潜在应用

Blockchain and Its Potential Application in Aero Engine Industry

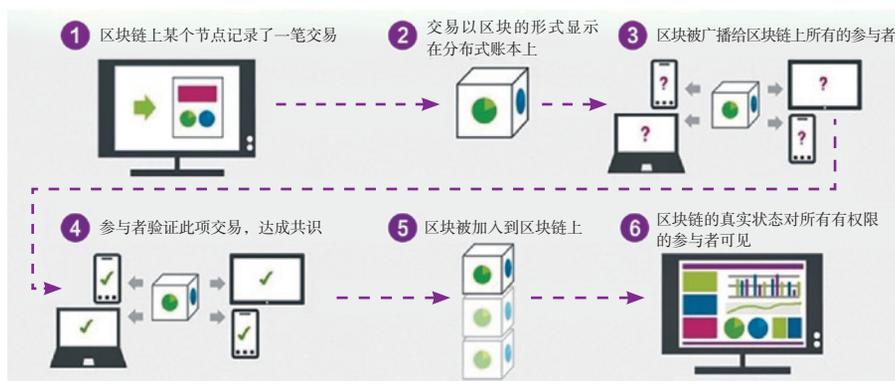
■ 尚勇 付玉/中国航发研究院

区块链是当下被谈论得最多也是最热门的话题之一。区块链的优势在于提升协同效率、优化业务流程、降低运营成本，有着较为广阔的应用前景。区块链技术在航空发动机的制造过程、供应链管理及应用售后服务中的应用值得期待。

斯图尔特·哈伯 (Stuart Haber) 与 W. 斯科特·斯托尼塔 (W.Scott Stornetta) 于 1997 年提出用时间戳确保数字文件安全的协议，成为公认的区块链技术的最早应用。从 2009 年起，随着比特币的大热，区块链作为比特币的底层技术，逐渐引起了人们的重视。

什么是区块链？

区块链的底层算法和具体实施方案很复杂，但其思想相对简单。也就是说，区块链是指通过去中心化和去信任化的方式来集体维护一个可靠数据库的技术方案。区块链中的区块，是指使用密码学方法产生的数据块，每个数据块中包含了一段时间内系统信息交流的全部数据及其有效性的确认信息；多个区块按照时间顺序叠加成链，形成永久的、不可篡改的记录。简单地说，当一笔交易产生时，会先被广播到区块链网络中的各节点，各节点将该笔交易的哈希 (Hash) 值收到自己的区块中进行工作量证明 (PoW) 的计算，并由最快算出结果的节点来验证交易；验证交易的节点将自己的区块广播给其他节点，其他节点会确认这个区块所包含的交易是否有效，验证成功后，该区块被区块



区块链运行流程 (来源: IFS 实验室)

链所接受，盖上时间戳后将无法再进行更改。区块链技术通过全民参与，共同维护的方法，保证了数据存储的一致性、安全性和实时性。

具有分布式去中心化特点

传统的数据库需要建立在一个中心服务器上，数据库的读写权限集中在一个公司或一个控制中心上。而在区块链中，任何有能力架设服务器的人都可以参与其中，成为这个分布式数据库存储系统中的一个节点；一旦加入，该节点享有同其他所有节点完全一样的权利与义务，分布式存储机制使网络中每个节点都拥有整个网络的数据。去中心化的处理方式会节约很多资源，使得整个交易自主化、简单化，并且排除了被中心化代理控制的风险，防止单点故障，降低了系统

性风险和监管成本。

解决了中介信用问题

通常情况下，两个互不认识和缺乏信任的人要达成合作是很难的，必须要依靠第三方。比如支付行为，任何一种转账必须要有银行或者支付宝这样的机构存在，但有了区块链技术后，网络上的交易行为对所有节点公开透明，并形成对所有人可见的不可更改的共享记录。原来由权威中心构建的信用机制被无数个平等个体组成的新的信用体系所代替。比特币是人类第一次实现在没有任何中介机构参与的情况下，完成双方可以互信的转账行为，并从运行之初起从未出现过大的漏洞。它打破了传统纸币的“暗黑”盒子，让每一笔交易的动向都清清楚楚有“链”可查，同时还可以保

三种不同形式的区块链对比分析

	共有链	联盟链	私有链
参与者	任何人自由进出	联盟成员	个体或公司内部
共识机制	PoW/PoS/DPoS	分布式一致性算法	分布式一致性算法
记账人	所有参与者	联盟成员协商确定	自定义
激励机制	需要	可选	不需要
中心化程度	去中心化	多中心化	多中心化
突出特点	信用的自建立	效率和成本优化	透明和可追溯
承载能力	3 ~ 200000 笔/s	1000 ~ 10000 笔/s	1000 ~ 100000 笔/s
典型场景	虚拟货币	支付、结算	审计、发行
代表项目	比特币、以太坊	R3、Hyperledger	

护参与者的隐私，这是区块链所带来的重大突破。

保证了数据不可篡改

区块链采取单向哈希算法，每个经过共识的新产生的区块都被盖上时间戳，并严格按照时间顺序推进，时间的不可逆性导致任何试图入侵篡改区块链内数据的行为都很容易被追溯，导致被其他节点所排斥，从而可以限制不法行为。

随着区块链技术在各个行业应用的探索，区块链的部署方式也出现了创新。除了向所有人开放的共有链（比如比特币）外，按照去中心化程度和开放权限的不同，还衍生出联盟链和私有链。联盟链采取多中心式，参与成员是预先根据一定特征所设定的。联盟链更容易进行控制权限设定，拥有更高的应用可扩展性；私有链没有去中心，但具有分布式特点，由中心控制者制定可以严格控制每个节点的访问权限。随着区块链技术的发展，每个节点的读写权限将会更加复杂，将会出现更多类型的区块链，以适应区块链技术在不同领域的应用。

区块链技术的一些应用

简化流程，降低交易成本及制度性成本，提升协同效率

区块链技术以极低的成本解决了信任与价值的可靠性传递难题，具有去中心化、开放性、自治性的特点，可以构建一个更加共享开放、更透明可信并可核查追溯的可靠系统。区块链技术依靠强大的密码学原理建立了一套可信的身份验证的工具和身份识别系统，方便链上的各个节点进行交互，各种认证手续、审核登记等都可以通过区块链技术自动完成，削减了中介化和制度性成本；共有链的开放性使所有参与者都能及时得到最新数据，能够促进不同开发人员、研究人员以及机构间的协作，相互取长补短，从而实现更高效、更安全的解决方案。利用区块链技术，将各环节加以整合，加速流通，有效缩短价值创造周期。

例如，2015年10月，VISA与数字交易管理公司DocuSign联合推出概念证明项目，使用区块链技术记录、保管租车数据，推动汽车租赁过程的数字化。该项目在区块链上为客户创建数字指纹，在链上进行登记，通过分布式账本记录交易，使租车协议、保险项目等内容实时更新，简化传统汽车租赁过程中的繁琐步骤；被研究者广泛采用的

Wolfram Mathematica 计算机代数系统也正在支持一个叫做Multichain的开源区块链平台的建设。在Multichain平台上，科学家可以上传数据到一个共享的开放工作区里，而这个工作区不被任何具体的用户控制，能够可靠地收集和保存与研究活动有关的数据。

组建和管理工业物联网，打造低成本可信环境，实现信息点对点的安全传输和存储

随着物联网技术的进一步应用，数以千亿计的物联网设备的管理和维护将会给生产商、运营商和用户带来巨大的成本压力。目前的物联网应用基本上都是采用中心化的体系结构，所有的数据流都汇总到单一的中心控制系统，中心化服务器需要付出的计算、存储和带宽成本也会达到无法负担的程度。在去中心化的物联网愿景中，区块链是发生互动的设备之间促进交易处理和协作的框架，网络上的每个设备都是可以作为一个独立、微型的商业主体运行，并通过设备间的彼此交流，构建一个权力分散且完全自治的系统。IBM研究团队开发了一个使用区块链技术的物联网分布式平台“去中心化P2P自动遥测”（Autonomous Decentralized Peer-to-Peer Telemetry, ADEPT）系统，该系统可以让物联网里的各种设备自动运转，并在需要的时候实现数据共享，互联互通。当设备运转出故障时可以自动发送信号，并可以自动更新软件，甚至设备本身可以通过ADEPT来与周边的设备“沟通”，从而提高能源的利用效率。在ADEPT系统中，当数十亿个设备自动交互信息时，区块链将发挥分布式账本的作用，通过在系统中植入协议还可以大大降低



区块链技术在供应链管理中可能的应用范围（来源：IFS实验室）

ADEPT系统作为设备间的沟通桥梁时的成本。

提升供应链的管理效率，避免供应链纠纷，解决假冒伪劣问题

现代企业的供应链不断延长，出现零碎化、复杂化、地理分散化等特点，给供应链管理带来了很大的挑战。核心企业对于供应链的掌控能力有限，同时对假冒商品的追溯和防范也存在很大的难度。作为一种分布式账本技术，区块链能够确保透明度和安全性，也显示出了解决当前供应链所存在问题的潜力。由于数据在交易各方之间公开透明，从而在整个供应链条上形成一个完整且流畅的信息流，确保参与各方及时发现供应链系统运行过程中存在的问题，并有针对性地提出解决问题的方法，进而提升供应链管理的整体效率。区块链技术所具有的数据不可篡改性和时间戳的存在性证明的特质，能很好地应用于解决供应链体系内各参与主体之间的纠纷，实现轻松举证与追债。

区块链技术还可以用于产品防伪，数据不可篡改与交易可追溯两

大特性相结合，可根除供应链内产品流过程中的假冒伪劣问题。伦敦的区块链初创企业Provenance为企业提供供应链溯源服务，通过区块链上记录零售用链上的全流程信息，实现产品材料、原料和产品的起源和历史等信息的检索和追踪，提升供应链上信息的透明度和真实性。通过Provenance的区块链平台，整合产品制造、运输、交易环节过程中的全部信息，重建供应链条中的信用体系，促进体系的良性发展。

区块链在航空发动机领域应用的一些设想

虽然近期关于区块链技术的探讨如日中天，但是距离实际的应用尚需时日。同时，该技术在航空发动机领域的应用还处于探索阶段。

在航空发动机制造过程中实现智能化管理，降低运营成本

面对日益增长的人工成本和生产压力，越来越多的制造领域开始推进数字化转型。航空发动机生产巨头GE公司推出全球第一个工业数据收集与分析平台Predix，并将其打

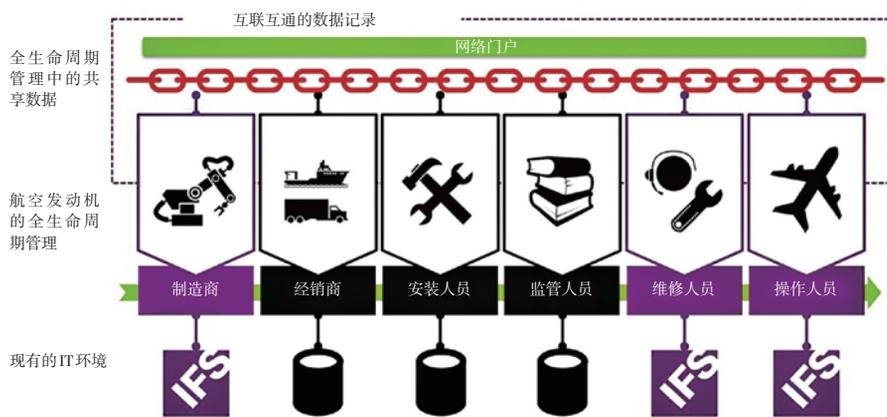
造成综合性工业物联网云平台；2017年年底，罗罗公司也宣布与印度塔塔咨询服务公司合作，搭建自己的物联网平台。

随着智能设备呈指数级增长，如何实现数据的高速可靠传输及存储成为制约物联网发展的一大因素。目前的工业物联网使用“云管端”网络管理架构，所有的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运维将占用高昂成本；不同信任域下的物联网节点由于安全性和系统可靠性的束缚，依然采用集中服务器的间接访问方式，无法实现有价值的直接互联互通。

而区块链技术的分布式架构使链上的每个生产设备都作为一个独立的主体运行，整个解决方案不需要引入大型数据中心进行数据同步和管理控制，降低物联网的运营成本；不同所有者的生产设备可以通过加密协议传输数据，连入其中的设备安全高效地点对点直接通信，并通过智能合约，使设备在给定的规则逻辑下进行自主协作：每个设备可以自主地根据区块链上的最新数据和自身工况决定自己下一步的动作；多个设备彼此协同，减少中间环节提高能源利用率等，实现生产过程智能化管理。

航空发动机供应链管理及售后服务，保证零部件生产维修记录可追溯

当飞机从一个运营商转手给另一个运营商时，很大一部分工作是创建、存储、管理、运输和验证飞机及其部件的记录，使之符合安全、飞机价值和适航标准。航空发动机的生产交付也是如此，而且文档验



区块链在航空发动机全生命周期管理中的应用 (来源: IFS 实验室)

证所用的时间可能会拖延产品的转手, 同时也会影响收益, 一些无法验证的记录需要返工。区块链技术的应用, 可以构建起可靠的信任协议, 在保证最终验证结果的前提下减少中间环节, 降低交易成本, 使供应商、集成商、航空公司及维修人员均从中获益。

区块链技术可以建立起完整而流畅的信息流, 存储发动机及其零件的所有生产及维修信息: 产品的产地, 哪家航空公司用了多少小时, 何时发生失效, 谁修理了它, 什么时候等。这些数据可以通过授权的人员手动输入, 也可通过ERP系统或维修管理系统导入; 信息一旦输入, 便发布给区块链的所有参与者, 可以有效避免由于潜在失效或网络攻击造成的数据丢失或篡改。零部件安装和修理的数据可以建立起一个完整的维修历史, 可以对部件从“生”至“死”进行跟踪, 给售后服务市场带来巨大的变化: 一个部件进入供应链, 就可以追踪其原产地, 以确保它不是仿制的产品; 一个部件发生了故障, 技术人员可以用历史记录和飞行小时数决定是对零件进行更换还是修理。目前, IFS,

Accenture, SITA 和微软等公司都在积极探索区块链技术在维修业的应用, 其中微软公司与VISEO咨询公司合作开发出基于区块链的数字维修日志, 法国汽车制造商雷诺公司已经宣布使用该平台并从中受益。

区块链技术应用的局限性 对共识机制的挑战

区块链技术中已经提出了多种共识机制, 最常见的是工作量 (PoW) 证明, 即通过计算哈希值来争取记录权。但随着数学、密码学和计算技术的发展, 这些共识机制对安全的保障性越来越脆弱。2017年, 美国谷歌公司安全研究团队宣布通过哈希碰撞, 在国际上首次利用非穷举方案成功破解安全哈希算法-1 (SHA-1), 终结了哈希算法的安全神话。此次破解对政府、银行及军事部门等机构内众多采用SHA-1加密机制的计算机系统造成重要影响。而量子计算机等新的计算技术的发展, 对区块链中的非对称加密算法也有一定的威胁。

数据真实性有待检验

在供应链管理中, 很多企业尝试用区块链技术做产品的溯源系统,

并且认为区块链上的数据都是真实可信的。在这种应用中, 区块链实际上是被当做一个底层的存储系统来使用, 它的时间戳和共识机制可以保证传到链上的数据不被篡改, 保证所有节点上数据的一致性, 但是无法保证一开始传到链上的数据是真实的。而在这种类型的应用中, 输入数据的真实性才是关键。一旦错误的信息被加入链中, 后续修改的过程会付出很大代价, 甚至会使整条记录失效。

数据的所有权有待探讨

每架A350上有超过6000个传感器, 每天产生的数据量多达2.5TB。预计到2020年, 这个数字还会再扩大3倍。再加上其零部件的生产流通等环节产生的数据, 即使是航空发动机这一单一部件, 也会产生惊人的数据量。而区块链技术如果应用到发动机的全生命周期管理中, 必然会要求大多数环节都能知悉整条链上的数据, 这就对区块链上数据的所有权, 特别是数据中所蕴藏的信息的所有权, 提出了疑问。

结束语

一种乐观的预测认为, 到2025年之前, 全球GDP总量的10%将利用区块链技术储存。现在, 区块链经济已处于爆发的前夜, 金融行业的探索领先一步, 而其他行业的应用正在快速展开。随着央行对区块链的重视加深、来自国外最新科技进展的溢出效应、海外以太坊作为区块链技术标准的逐渐确认、伴以区块链应用的更加成熟, 区块链有望成为“互联网+”后的下一个热捧对象, 其发展动态值得关注。

航空动力

(尚勇, 中国航发研究院, 工程师。)