

【本文原刊载于*Futureautics* (www.futureautics.com)，作者为区块链专家Deanna MacDonald、Karim Jabbar和Simon Ousager。经许可在此提供原文的精编版。以示读者。】

近年来区块链在各大媒体出尽风头，有论者认为它将是新经济模式的缔造者。在区块链技术的支撑下，现有交易将变得高效、透明、安全且可追溯，甚至实现了零阻力贸易。有数家公司表示正积极“试水”区块链的具体应用，以迎接其给行业带来的无论机遇抑或挑战。

从比特币到区块链

区块链基础设施仍处于起步阶段。2009年，金融危机余波未平，一位化名为Satoshi Nakamoto的人士匿名共享了一项协议，在无需可信第三方参与的情况下，用户通过该协议在P2P网络上交易数字货币，而这个货币，正是我们今天所熟知的比特币。在过去的几年内，该协议及其小型底层用户群自然发展成为一种技术框架，目前的市场总值接近200亿美元。

“区块链”一词最初由Nakamoto创造，用以描述新区块形成的过程（也称“挖矿”，英文为Bitcoin mining）。套用Nakamoto的说法，“区块链是多个交易的集合，加密嵌入了复杂数学算法，而生成特解的时间节点为10分钟”。此后，block chain演变为blockchain，涵盖了除比特币和其他加密货币系统之外的其他应用场景。

在财务领域，对区块链的研究集中于将其作为贸易结算方式以及其他特殊的银行用途。但与比特币不同，它需要进行身份验证以符合反洗钱/了解客户原则。

新兴企业和其他企业已经开始将他们现有版本的区块链定制成可用于其他用途的区块链。作为此项发展的一部分，比特币的交易脚本特性成为了利益所在。简而言之，这意味着每笔交易可以用任何类型的数字数据进行注释。这为使用区块链来储存任何分布式记录提供了可能性。

接下来，为了有目的地使用这些数据记录，基于“如果，那么”逻辑的自执行代码排列被嵌入到数据库中。这些都是所谓“智能合同”的基础，现今的大部分区块链解决方案都围绕于此。一部分新兴区块链要求使用者获得进入区块的授权（许可级别），另一部分则无需使用者被授权（非许可级别）。其中一些被打造成可以构建应用程序的平台，另外一些则是具有特别用途的操作软件。

区块链在航运业的应用

以下表格是正在开发或者已经被应用的解决方案——

公司	针对	问题所在	解决方案
Blockfreight	完整的航运区块链	兼容性非常有限的各种IT系统	完整的航运区块链，拥有内置的密码代币
Wave BL	提单	提单具有收据，运输合同和物权凭证的功能，目前这些功能并不总是能够实现	区块链应用允许共享提单信息和提单匿名流转
Maersk; IBM	文件传输	一件货物经过各种供应链环节出口，往往需要提供超过30种不同文件	基于共享区块链的存储模式：（i）使有关文件对相关方开放；（ii）追踪和记录货物保管状态的改变
Port of Rotterdam; ABN AMRO; Royal Flora Holland; TU Delft; and more	贸易金融	在货物产地和目的地银行复杂冗长的信用证程序	自主智能合同使得货款在交货证明具备的情况下自动支付
SKUchain	贸易金融	目前贸易金融体系下的流动资金问题	智能合同，也叫“括号”，基于区块链的支付，密钥签署
Everledger	出处和可追溯性	最终用户往往不知道产品真正原产地	追踪钻石产地的区块链应用
Provenance	出处和可追溯性	由于供应链的模糊不清，导致许多公司无法告知消费者产品的真实产地	公开的区块链追溯平台
SOLAS VGM/MTI	大批量集装箱信息认证（VGM）和共享	VGM数据必须提前提供给承运人，目前使用EDIFACT系统	在一个分类帐上记录集装箱上有数据（装货点和岸磅）的应用，同EDIFACT和API兼容

现在很难评估区块链在航运业的全部应用潜力。整个行业还有许多先行步骤要完成。行业参与者需要开始提出一些关键问题（例如链接中的问题）。在开始投入大笔资金前，他们还必须开始强化他们对于区块链及其潜在行业应用的知识。

并非所有公司都需要区块链，也并非一个公司所做的所有事情都需要放到区块链上。只有那些涉及与其他方交流，并且具有较高社会、经济、和环境价值，或者可能被篡改的交易才能从区块链上最为获益。

北英关于区块链的信息速递：

- 区块链是一个安全的去中心化的共享数据库。
- 该数据库旨在将交易的数据化账目落户到一个共享平台之上。
- 每次交易—无论是支付还是合同协议—都会被录入到一个“区块”中，而每个新生成的区块都将链接到上次生成的区块从而形成一个有时间顺序的“链”。
- 区块链整体保存在某个网络当中，不受制于某个中心化的控制。

- 信息共享提升了安全度。每一个录入生成的区块都必须经过其他人通过网络核准，而区块的密码学设计可以保障各方沟通的安全度。
- 每个区块都链接到上一个区块，如有人企图篡改或删除一笔交易，网络内的其他人都会得到通知并且该行为会被拒绝执行，因此无法对其做手脚。
- 系统的共享不等于区块链对任何人都准入。从系统的用途出发，可以将网络分级为“许可级别”（网络用户须经管理员许可才能登录）和“非许可级别”（其内容对互联网上所有人公开，用户可以都是匿名的）。
- 智能合同指的是数字化合同在代码与逻辑应用之下可以将传统纸面合同中“如A具备了则实施B”的功能自动实现，因而称之为“自动履行”的合同。