# 新技术丨区块链

意见领袖丨范文仲（北京金融控股集团董事长）

第二章 新技术

人类的航海历史始于以人力、风帆为动力的传统时代。近代蒸汽机和燃油发动机的出现大大提升了航海的效率，全球贸易蓬勃兴起。应用现代核能技术，航空母舰和大型潜艇在大洋中实现了长期自由航行。可以说，动力的提升推动了人类航海时代的不断跃进。对金融业而言，科技创新同样是发展的重要动力。例如，纸张和印刷术的发明促进了中国古代飞钱、交子的创新，而电话、电报的出现导致全球金融交易方式和效率发生深刻变革。

新一轮金融科技的创新主要体现在大数据、物联网、云计算、人工智能、区块链、隐私计算等新兴科技的崛起。在这些新的技术出现之前，人类收集、处理数据的能力十分有限，只有高价值的数据才会被采集和利用。随着移动设备、传感器、物联网的出现，数据记录和分析工具不断创新，大量低价值的数据得以采集汇聚。数据量如此之大，需要巨大的计算能力，无法用单台的计算机进行处理，必须采用分布式架构对海量数据进行挖掘和存储。实时的大型数据分析需要向数十台、数百台甚至更多的电脑分配工作，云计算应运而生。正是因为计算硬件和分布式处理方式发展，巨量的数据和更复杂的算法才得以实现，机器智能开始向人工智能转变，各种社会应用功能不断拓展。

在产生了海量数据之后，如何安全、可信地记录和存储数据就越发重

要。区块链技术创新增强了数据的真实性和可靠性。数据成为社会核心经济资源后，价值大大提升，但同时也产生了原始数据保护和防范个人隐私侵犯等需求。通过明文加密和基于密码学基础，以及硬件环境保护的隐私加密技术应运而生，实现“数据可用不可见”，成为数据使用和交易过程中的保险箱。

总体来看，如果说大数据是基础资源，物联网则是采集途径，云计算是炼化基础设施，人工智能是应用工艺，区块链是新型记录储存方式，隐私计算则是数据资源的保险箱。

新金融书系
NEW FINANCE BOOKS

Digital Economy and Financial Innovation

# 数字经济与金融创新

范文仲◎编著

中国金融出版社

## 二、区块链与隐私计算

### （一）区块链

#### 1． 区块链的创新与挑战

近年来，随着比特币价格的暴涨，区块链迅速成为全球热门话题。比特币和区块链概念是 2008 年 11 月 1 日中本聪在其文章《比特币：一种点对点的电子现金系统》(Bitcoin：APeer-to-PeerElectronicCashSystem)中系统提出的。

互联网贸易的资金电子支付，传统上需借助第三方中介机构来处理。中本聪认为借助第三方中介机构处理信息，是点与点信息传输模式，具有缺乏信任的内生弱点，不能完全规避欺诈行为；第三方中介机构的存在，增加了交易成本， 限制了实际可行的最小交易规模；可以通过加密数字签名确认交易对手，交易信息分散存储来保证交易记录的真实稳健性。基于以上问题，中本聪阐述了基于 P2P 网络技术、加密技术、时间戳技术、区块链技术等的电子现金系统的构架理念，这标志着比特币的诞生。

在比特币形成过程中，区块是一个一个的存储单元，记录了一定时间内各个区块节点全部的交流信息。各个区块之间通过随机散列（也称哈希算法）实现链接，后一个区块包含前一个区块的哈希值，随着信息交流的扩大，一个区块与一个区块相继接续，形成的结果就叫区块链。2009 年 1 月 3 日第一个序号为 0 的创世区块诞生。2009 年 1 月 9 日出现序号为 1

的区块，并与序号为 0 的创世区块相连接形成了链，标志着区块链的诞生。虽然世界对比特币的态度起起落落，但作为比特币底层技术之一的区块链技术日益受到重视。

传统交易中，A 借款给 B，需要经过第三方中心机构，A 和 B 的存款放入中心机构处，A 和 B 都要和中心机构进行对账。在区块链交易中，A 借款给 B，不需要经过中心机构，A、B 各自在区块链不同区块记账核账，共同形成新的公共总账本，A、B 分别拥有新的公共总账本副本。区块链通过上述去中心化方式，形成了一种新的交易支付流程，降低了交易成本。

2． 区块链的特点与类型

区块链上的交易账本分布存储在不同的交易者处，分布式系统必然面临如何保证一致性的难题。历史上重要的案例则是“拜占庭将军”问题，该问题由莱斯利·兰伯特（LeslieLamport）等人在 1982 年提出，属于点对点通信中的基本问题。

拜占庭是古代东罗马帝国的首都，为了防御，在每块封地都驻扎一支由单个将军带领的军队，将军之间只能靠信差传递消息。在战争时，所有将军必须达成共识，决定是否共同开战。但是， 在军队内可能有叛徒，这些人将影响将军们达成共识。“拜占庭将军”问题是指在已知有将军是叛徒的情况下，剩余的将军如何达成一致决策的问题。1982 年，莱利斯·兰伯特等在论文“TheByzantineGeneralsProblem”中证明当将军总数大于 3f，背叛者数为 f 或者更少时，忠诚的将军可以达成命令上的一致。

同理，要在去中心化的通信领域中，实现点对点通信且确保信息可信，就必须解决“拜占庭将军”问题，即构造出一个点对点的不需要第三方权威认证的有效信息传递系统，通过全系统共享的方式，获得信息传输的一致性和稳定性。简单地说，就是让每个人都知道信息 X，而且每个人还都知道“每个人都知道信息 X”，从而实现信息透明化、不可篡改。

中本聪通过工作量证明机制等方式解决了“拜占庭将军”问题。要去掉中心机构，就需要实现交易者 A、B、C、D 都有共识，也就是每一个人都确认交易有效。通过工作量证明方式，链上记录交易本身，每个人都保留一份总账本的副本， 最终留下的总账本就是唯一真实有效的。

区块链分布式账本技术与传统分布式存储系统存在两大明显区别：传统分布式存储系统执行受某一中心节点或权威机构控制的数据管理机制，而区块链分布式账本是基于一定的共识规则，采用多方决策、共同维护的方式进行数据的存储、复制等操作。传统分布式存储系统将系统内的数据分解成若干片段，然后在分布式系统中进行存储，而分布式账本中任何一方的节点都各自拥有独立的、完整的一份数据存储，各节点之间彼此互不干涉、权限等同，通过相互之间的周期性或事件驱动的共识达成数据存储的最终一致性。

按记账主体、信任机制、激励机制、中心化程度的不同，目前区块链可以分为公有链、联盟链、私有链三种表现形式。三种表现形式各有侧重点、应用场景和实现功能，以及基于此构成的不同经济生态模式。

公共区块链（PublicBlockchains），又称公有链，是指任何人都可读取、可发送交易进行有效性确认，任何人都能参与其共识过程的区块链。参与者通过密码学技术共同维护公有链数据的安全、透明、不易篡改，是完全意义上的分布式。公有链的典型应用包括比特币、以太坊、EOS 等。目前，公有链已历经公有链 1.0、公有链 2.0、公有链 3.0 的发展，呈现出承载能力不断提升等发展特点。

共同体区块链（ConsortiumBlockchains），又称联盟链，是指参与区块链的节点是事先选择好的，节点间通常有良好的网络连接等合作关系，区块链上的数据可以是公开的也可以是内部的，是部分意义上的分布式。联盟链的典型应用包括超级账本、区块链联盟 R3CEV 等。

私有区块链（PrivateBlockchains），又称私有链，是指参与区块链的节点只有有限的范围，比如特定机构的自身用户等，对于数据访问及使用有着严格的权限管理。相关应用包括数据库管理、数据库审计等，如 ErisIndustrier。

3． 区块链的金融应用场景