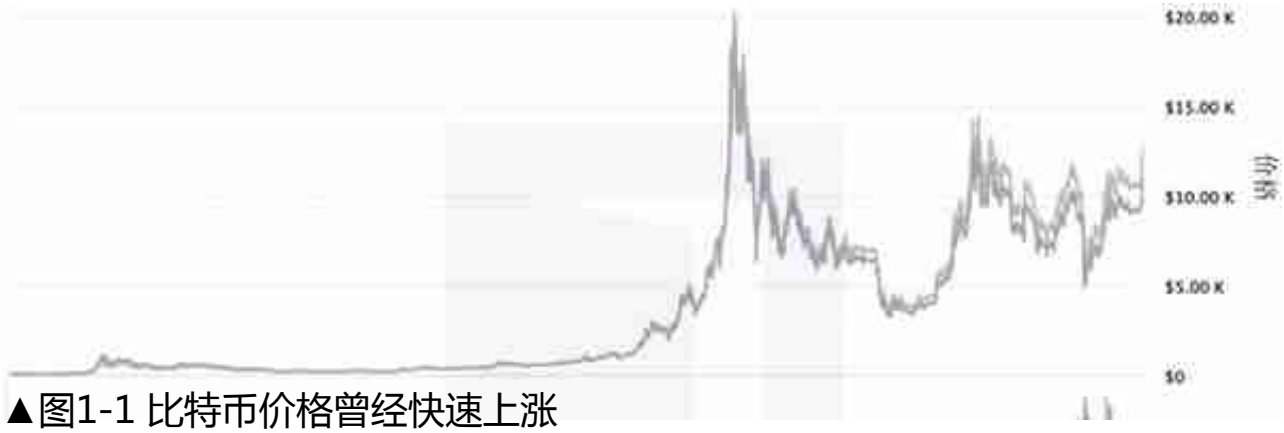
导读：近几年来“区块链”似乎横空出世，引起广泛的关注。区块链从何而来？它到底是一种什么样的技术？它是否意味着新一波的技术浪潮？它将如何改变这个世界？怀着这些问题，我们一同来探究区块链技术的前世今生。

作者：周兵 方云山

来源：华章科技



▲图1-1 比特币价格曾经快速上涨

隐藏在虚拟货币背后的是一种叫作“区块链”的神秘技术。它究竟是何物？又从何而来？

区块链从何而来？“区块链”源自英文BlockChain。普遍的观点是，区块链技术发源的标志性事件是2008年中本聪（Satoshi Nakamoto）提出了比特币系统设计。

在中本聪最初发布的《比特币白皮书》中，Block和Chain这两个词是单独出现的，而在后来的讨论中，人们逐渐将这两个词连接起来，以BlockChain来称呼这种技术。BlockChain（区块链）这种提法后来流传开来。

中本聪所提出的比特币系统是一个电子货币系统，在不需要第三方信用背书的情况下，可以实现完全点对点的电子货币转账。虽然许多人主要是将比特币作为一种虚拟的“币”，但从技术的角度来看，比特币系统中最重要的其实是分布式账本。

在中本聪的设计理念中，遍布全球的分布式节点共同维护这个不断延伸的链式账本，而所有关于“币”的权属的数据都完整地留存在分布式账本中，不会被篡改或删除。

区块链技术的范畴早已远远超过虚拟货币账本本身，而逐步发展成为能应用于多个行业和领域的综合化信息技术。

什么是区块链？从信息的组织形式来看，区块链是一个不断增长的数据链表，该数据链表的基本组成单位是一系列的“账本”（通常也称为“区块”），这些账本是通过密码学技术连接起来的。

从网络结构来看，区块链上所有的数据由一系列分布式、相互独立的“节点”共同维护。以上这些数据和网络结构方面的特殊规则保障了区块链上的数据无法被随意篡改，也不会失序、丢失。

区块链是若干学科的交叉综合，它涵盖了分布式计算机系统、密码学，乃至商业和经济等课题。
在区块链系统的设计中包含网络结构、数据结构、密码学算法和分布式系统的一致性算法（即区块链共识机制）等技术问题。

在本文后续部分中，我们将继续了解区块链技术的演进历程，以及区块链技术的意义。

02 区块链技术的演进

首先，区块链技术在发展过程中衍生出了多种类别。最常见的是根据节点间的组织形式和决策机制将区块链系统分为
公有链、私有链和联盟链三类，具体如表1-1所示。

▲图1-2 区块链技术的演进过程

第一阶段以中本聪在200
8年提出的比特币区块链为代表。
比特币区块链的实质是利用区块链技术实现一种分布式的记账机制，并以此为基础实现比特币虚拟货币的交易，其核心技术点包含UTXO交易模型、链式账本数据结构、加密技术，以及基于“工作量证明”的共识机制等。

比特币区块链是公有链，由全球的分布式节点共同维护。同时代的区块链应用还有Namecoin、Colored Coins，以及Metacoins等。

比特币区块链有一些局限性。例如，UTXO模型缺少对状态的支持，只适合简单、一次性的交易合约。这些限制使得它很难应对金融领域中各种较复杂的场景。还有一些专家认为比特币区块链中的“工作量证明”共识机制过于消耗计算量，平均10分钟出一个区块，效率很低。

区块链技术第二阶段的主要特点是引入了“智能合约”理念，成为可编程的区块链系统，进而支持简单的金融合约业务场
景。
和第一阶段的区块链技术相比，这个阶段的区块链技术通过图灵完备的编程语言，让开发者们能够创建合约，实现去中心化应用，以太坊和Fabric是这个阶段的主要代表。

其中，以太坊是继比特币之后一个很具影响力的公有链协议，它采用了合约账户的概念，能够通过执行智能合约实现两个账户之间价值和状态的转换。Fabric是由IBM主导开发的一个联盟链，支持用容器技术运行智能合约代码，对高级语言开发有良好的开放性。该阶段的区块链技术在共识算法方面也有很多创新。

第三个阶段是区块链在应用领域、效率，以及安全性方面的扩展，即目前的发展阶段。

可能的技术发展方向包含：

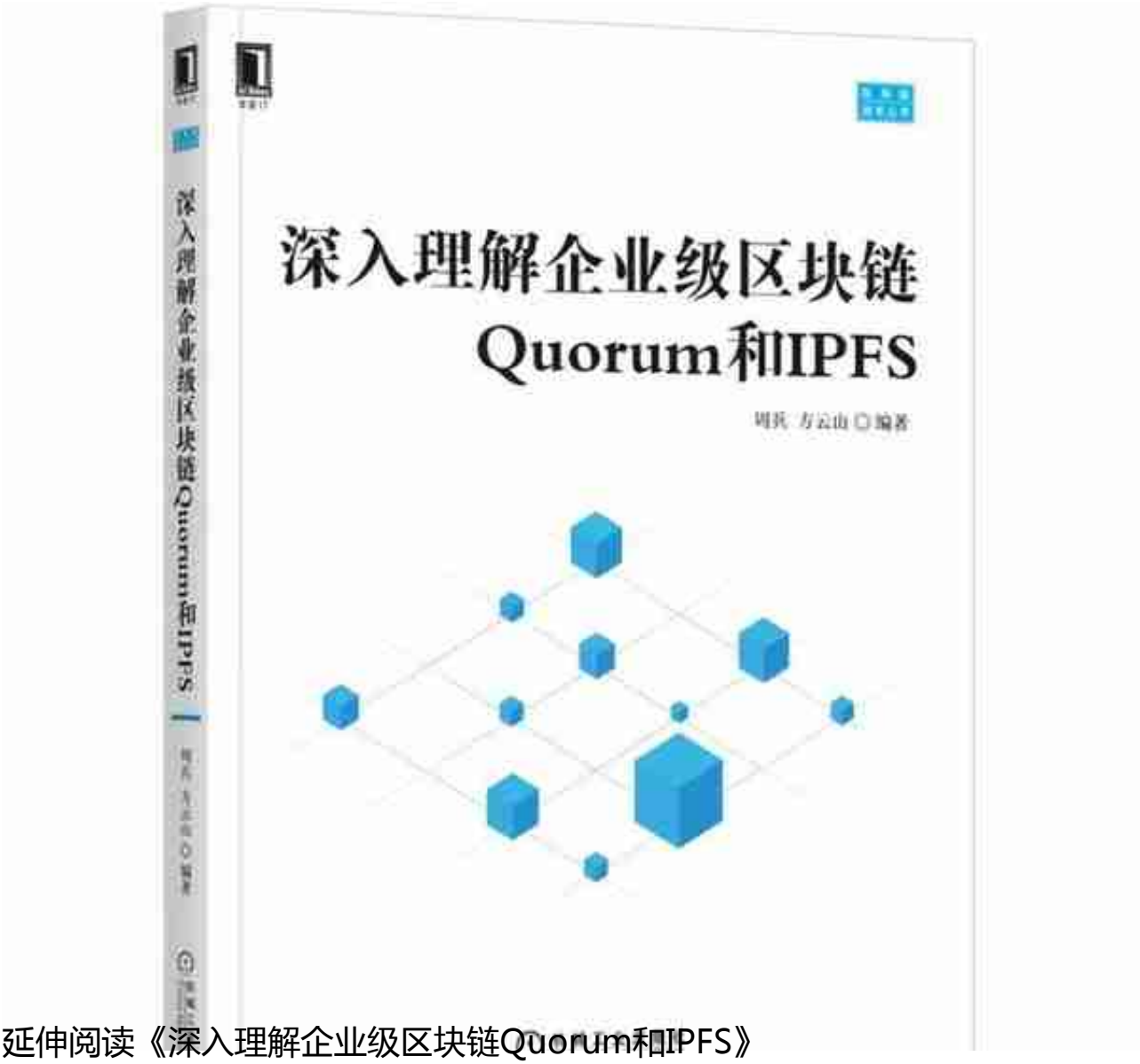
- 利用分片、跨链等技术提升区块链的记录效率，接近高并发场景下的需求；
- 利用新型的密码技术提升区块链系统的安全性，例如密钥管理技术、抗量子攻击密码等；
- 提升智能合约的开放性，增加适用的行业场景等。

据笔者观察，这个阶段目前尚处于探索阶段，还未有标志性的、被大规模运用的系统出现。

03 区块链能否“改变世界”

加拿大学者、数字经济领域的知名专家Don Tapscott曾将区块链称为一场“革命”，并认为区块链的底层技术可以改变货币、商业和世界。

事实真是如此吗？
区块链真能像工业化、互联网化一样改变世界，从而成为新一波技术浪潮吗？如图1-3所示，我们需要从多个维度来寻找这些问题的答案。



延伸阅读《深入理解企业级区块链Quorum和IPFS》

推荐语：
阐述企业以太坊Quorum和分布式存储系统IPFS的架构设计、系统配置以及编程实

践。