第01课：概念与...

你好，我是丹华，欢迎来到《区块链全景课》。今天我们先从一个伟大故事的开端讲起。

2008年11月1日，正值金融危机最严重的时候，一个自称中本聪（Satoshi Nakamoto）的匿名人士在一个密码学讨论组上公开了一篇题为 *Bitcoin：A Peer-to-Peer Electronic Cash System* 的论文。

【英文版和中文版戳这里】：

- https://bitcoin.org/bitcoin.pdf
- http://satoshinakamoto.me/zh-cn/bitcoin.pdf

这篇论文中提出了一种全新的电子货币——比特币，宣告比特币的诞生。中本聪结合了诸如 b-money 和 HashCash 等先前的发明，创建了一个完全去中心化的电子现金系统，它不依赖中央机构进行货币发行或结算和验证交易。关键的创新是使用分布式计算系统（称为“工作量证明”算法）每10分钟进行一次全球性的“投票”，从而允许分布式网络达成关于交易状态的共识。

2009年1月3日，中本聪在位于芬兰赫尔辛基一个小型服务器上挖出了第一批比特币50个，这就是比特币的创世区块。从此，打开了数字货币创新的潘多拉盒子。

与政府法定货币不同，比特币不依靠特定货币机构发行，它依据特定算法，通过大量的计算产生，该计算能力来源于一个由众多节点构成的点对点（P2P）网络。该网络各节点共同维护一个去中心化的数据库（称为区块链），来确认并记录所有的交易行为，并使用密码学方法来确保货币流通各个环节的安全性。

这一设计可以确保安全性：比特币只能被真正的拥有者转移或支付，任何人无法通过大量制造比特币、或者伪造篡改交易记录来操纵、破坏整个比特币系统。

比特币是人类历史上第一次实现了去中心化的电子货币发行和交易，全网共同维护一份共享的账本。比特币的出现使得电子货币由传统的“中心化账本+中介”的模式向“公共账本+共识”的模式转变。

比特币的发行机制由比特币软件设定，其总数量为2100万个，任何人无权更改，因此具有极强的稀缺性。目前全世界发行流通的比特币共有1700万个（2018年6月），每一个比特币都是由矿工节点挖矿产生。

比特币软件设定，每10分钟全网产生一个区块，有幸挖到该区块的矿工将获得一定数额的比特币做为奖励，这就是所有流通比特币的发行源头。每隔210000个区块（即4年），奖励就会减半。也就是说，从第1个区块到第210000个区块，每个区块的奖励都是50个比特币，从第2100001区块到第420000区块，每个区块的奖励是25个比特币。以此类推，直到2140年左右，最后一枚比特币被挖出，从此再无新增的比特币。

比特币诞生后，人们被其设计上的简洁优美和未来的无穷可能性震惊，一批先知先觉的人开始关注这个领域。

著名的硅谷风险投资家马克·安德森（Marc Andreessen），对于比特币激发的巨大认知转变有着生动的描述：

> 我有很多的程序员朋友。他们总是说"比特人都疯了。" 然后，几乎每次，他们会坐下来，看论文读代码，这会持续几周，然后他们就一百八十度大转弯。他们会说："哦，额滴神啊，就是他！这是一个巨大的突破。这就是我们一直在等待的东西。他解决了一切的问题。不管他是谁，他都应该获得诺贝尔奖，他是一个天才（指中本聪）。就是它！分布式信任网络，这是互联网最最需要却从来没有出现过的。"

另外一个比特币的忠实粉丝、*Mastering Bitcoin* 的作者 Andreas · M · Antonopoulos 说：

> 对"不是货币，而是去中心化信任网络"的领悟，让我开启了为期四个月的比特币沉醉之旅。我如饥似渴地寻找任何关于比特币的点滴信息，变得越来越着迷，每天都花上12个小时以上紧盯屏幕，竭尽所能地不断阅读、写作、学习和编程。从这段着魔的状态中走出来的时候，我的体重由于饮食不规律轻了20 多磅……

基于比特币模型，人们发明了无数类似的系统。一开始是简单的模仿和复制，甚至仅仅是修改一下比特币源码的参数，这些数字货币被称为山寨币（Alt Coin）。众多山寨币中，最成功的要数莱特币（Litecoin）了，莱特币部分地得益于这一深入人心的口号：比特是金，莱特是银。

早期的炒作过后，比特币在技术创新上的启示和价值被越来越多人认可和传播，越来越多天才加入这个领域，开始全面挖掘、升级比特币模型，创新程度大幅提升，诞生了诸如比特股（Bitshares）、以太坊（Ethereum）等较成功的系统。

2015年前后，人们开始将"区块链"技术从比特币中剥离出来，认为"比特币没有价值，区块链才是未来"。当时的背景下看，这一区分是有实际意义的。因为一直以来，比特币的"货币属性"都极具争议性（到今天依然如此）。这一区分将比特币中的核心技术——区块链——和投机炒作区分开来，有利于鼓励更多人群了解区块链技术，从而引发了全世界范围内的区块链浪潮，包括政府、产业界和媒体等。

至此，这一领域就被非正式地划分为两个圈子：币圈和链圈。尽管没有公认的划分标准，但一般认为，币圈的人主要关心"币价"，属于投资者和投机者，链圈的人主要关心作为技术的"区块链"，对币价涨跌持冷漠和鄙视态度，相关的项目和技术创新也都与"币"和"通证 Token"无关。

从币圈来看，近十年的发展可谓日新月异。矿机与挖矿、交易所、钱包、媒体、投资基金、衍生产品（如 ETF 和比特币期货）等日益丰富和活跃。近日有消息称，矿机巨头比特大陆已经成为台积电的第二大客户。挖矿芯片的飞速发展与比特币社区，已经构成了完美的产业协同进化。币圈的社区管理、内容创新也层出不穷。

从链圈来看，技术发展也非常迅速。以联盟链为代表的无币区块链，如超级账本 HyperLedger，也已经开发了多个面向企业的技术平台，开始得到各路巨头们的广泛应用。各个行业都有一些创业项目在试图将业务流程实现区块链化改造。

到今天为止，比特币已经成功运行近10年，社区成熟稳健，市值超过千亿美元。全球数字货币已经有上千种，未来还会更多。价值互联网、智能合约、去中心化应用、数字身份、开放社区经济、通证经济这些概念，激励无数人幻想未来的数字世界。

无论你赞同有币还是无币，区块链和数字货币已经掀起了一场席卷每个角落的创新浪潮，火爆已经成为事实，而且必将继续前进。至此，区块链和数字货币正式出现在历史舞台上。

在即将开始的这场旅行中，有两个不可错过的必玩景点：比特币和以太坊。请大家跟上我。

附录

读者可参考 Coindesk 的 State of Blockchain 季度和年度报告：
https://www.coindesk.com/research/state-blockchain-2018/