第08课：区块链...

大家好，我是丹华。今天我们介绍区块链技术的第四个支柱：智能合约。

8.1 什么是智能合约

智能合约（Smart contract）是一种以计算机语言编写、由计算机自动验证和执行的代码化的合同，是纸质合同的数字化形式。

智能合约概念于 1994 年由计算机科学家、法学家及密码学家尼克 · 萨博（Nick Szabo）首次提出。他对智能合约的定义是“一个智能合约是一套以数字形式定义的承诺（promises），包括合约参与方可以在上面执行这些承诺的协议。”

智能合约概念面世后，自然面临如何落地的问题：

第一，谁来执行合约？显然，签署合约的双方不应成为执行人。

这带来一系列问题：如何激励他为你执行合约而不是免费？他如何保持公正和中立？他缺位、消失或者拒不执行怎么办？

第二，如何通过计算机程序支付现金和资产？

当时技术条件尚未成熟，无法解决上述问题，因此智能合约迟迟无法变为现实。

8.2 区块链是智能合约落地的土壤

数字货币和区块链诞生以后，上述问题得以顺利解决：

1. 执行智能合约的机制：去中心化网络+共识机制+受激励的矿工
2. 价值转移功能：内生可编程的数字货币
3. 去中心化的永不停机的计算网络，保持中立、公平、永远工作

区块链不仅内嵌数字货币系统，而且可编程可扩展，具有去中心化、不可篡改、过程透明、可追踪等优点，天然适合于智能合约。从此，智能合约才从理论构想变为落地的现实，从而插上了飞速发展的翅膀。区块链给智能合约提供了最佳的技术土壤，而智能合约功能也大大扩展了区块链的应用前景。目前一般认为，智能合约是基于区块链技术的自动执行的数字合约形式。

智能合约的出现，是社会经济运行进一步智能化、数字化的必然结果。人们用纸质合同做交易，已经有上千年的历史。合同，代表了不信任或者弱信任的双方做交易的标准形式。人们之所以信任合同、尊重合同，因为背后的机制是法律、法庭、名声、文化和道德感。智能合约以一种高度标准化、简洁、强大的方式，一举去掉了（至少削弱了）这些围绕纸质合同的繁琐机制，促进了社会进步。

8.3 智能合约与去中心化应用

去中心化应用（Decentralized Application，简称Dapp）是一种基于区块链的互联网应用，它运行在一个去中心化的点对点网络上 (P2P 网络)，代码开源，网络中不存在能够完全控制 Dapp 的节点。去中心化应用一般应包括至少一个智能合约和一个网页用户界面，有时还需要一个去中心化的存储协议和去中心化的通信协议。去中心化应用的背后没有中心化的实体负责和运营，这与 “中心化应用”完全相反，比如微信、淘宝。可以认为智能合约等同于去中心化应用。

8.4 智能合约的优点

与纸质合同相比，智能合约至少具有以下优点：

1. 合约制定的高时效性：合约制定中，不必依赖第三方或代理机构的参与，只需合约各方将共同约定的条款转化为自动化、数字化的计算机代码，繁文缛节大大减少；
2. 合约条款的明确性：代码化的智能合同含义明确，支持事前的测试，杜绝了纸质合同中的概念不清、理解分歧；
3. 合约签署的明确性：智能合约需要参与各方以私钥签名及发送交易才能启动，杜绝了签约过程中的假公章、恶意更改等；
4. 条款事先约定且自动强制执行：智能合约可对触发条件进行智能判断，根本上杜绝了人为错误、违约、拖延和“店大欺客”；
5. 合约执行的成本低、准确性高和效率高：智能合约一旦部署成功，利益各方均无法干预，由矿工节点按照约定条款监督、执行，一旦发生违约可由程序强制执行。与传统合约对应的律师法庭体系相比，智能合约大大降低了成本，提高了合约的执行准确性和高效性；
6. 更公正透明的商业环境：现实生活中存在大量的合同不公或欺诈，因为金额较小或诉讼成本太高或者不懂法律条文，受害一方往往只能忍气吞声。在智能合约世界里，一切清楚透明可查，且可以事先进行无限次的演练，这会塑造一个更公正透明的商业环境；
7. 跨国跨文化性：传统合同往往都与当地的商业文化、习俗、具体法规等有关，智能合约依赖于全球化的通用语言——编程语言，轻松越过了自然语言带来的障碍和瓶颈，可以在全球范围内推广使用。智能合约的盛行可能会带来数字世界的商业与信用文化逐渐走向统一。

8.5 智能合约前景——替代纸质合同

想想传统纸质合同吧：公章，骑缝章，签名，一式三份，抠字眼抠条款，纸质档案保存与查询的不便，面对强势缔约方的不公待遇和霸王条款，各种萝卜章、虚假合同、偷换条款，执行中的沟通与扯皮，律师——大多数人请不起，法律诉讼——大多数人想不敢想，合同诉讼管辖地问题，漫长的立案庭审上诉执行过程等等。

智能合约就是要试图颠覆笨重低效的纸质合同。智能合约能够大幅度地降低交易成本，降低人工，增强了各方对合同本身的信任和尊重，让经济交易回归交易本身，增加交易各方的福利。从此，陌生人之间可以无需信任地放心交易，这将革命性地提升交易的范围和深度，给经济和社会生活带来巨大的改变。

早期的区块链解决了货币和支付的去中心化问题，插上智能合约翅膀的区块链可以创建、确认、转移不同的数字资产，并将人类经济生活中的复杂交易形式-合同也实现了代码化、区块链化和自动化。实际上，简单分析可知，几乎所有类型的合同交易都可以改造成区块链上的智

能合约，包括：买卖合同，水电煤热类公用事业合同，借款合同，租赁与融资租赁合同，赠与合同，劳动合同等。

智能合约已经在以太坊、Hyperledger Fabric 等项目中得到广泛应用。最近智能合约这一概念被扩展为更宏大的智能经济、可编程经济等。围绕智能合约和去中心化应用平台的公有区块链竞争也日益激烈。

8.6 智能合约存在的问题

目前智能合约还不成熟，存在着一些理论、技术安全、推广应用、法律等方面的问题。

理论上的问题在于，现在还无法从技术上事先判断：一个智能合约是否会陷入无限循环而无法停止。简单的解决办法是为智能合约设定一个费用上限或时间上限，每一步执行需要支付费用，避免无限循环。这是以太坊采取的办法。

另一个问题在于安全性，目前的智能合约常会因安全漏洞导致资产被盗。

应用层面的障碍在于，智能合约由代码构成，有一定门槛，普通用户无法编写自己的智能合约。解决办法有两类，一是开发图形化、可视化的编程界面，一是开发大量的标准化的智能合约模板，用户做小修小补即可。

附录：

1. 尼克 · 萨博最早对智能合约的定义
2. 智能合约应用案例研究： Smart Contracts: 12 Use Cases for Business & Beyond
3. 一篇论文：*Smart Contracts – How will Blockchain Technology Affect Contractual Practices*https://www.researchgate.net/publication/312211462*Smart*Contracts-How*will*Blockchain*Technology*Affect*Contractual*Practices