第03课：以太坊...

你好，我是丹华。这一讲里我们为大家重点介绍以太坊的基础知识。

由于比特币设计追求安全性和可靠性，内置的脚本语言限制和操作码有限，因此在比特币中只能实现极为有限的功能扩展。人们渐渐意识到，可以扩展比特币的设计，实现一个功能更强大、更灵活、通用的去中心化计算平台。由天才少年程序员、俄裔加拿大人维塔利克 · 布特林（Vitalik Buterin）创建的以太坊，正是这样的平台。

关于维塔利克 · 布特林，业内都称他为 V 神。2013年末，他发表了以太坊白皮书，描述了以太坊的技术设计和基本原理。2014年，V 神开始和 Gavin Wood 合作。2014年4月，Gavin 发表了以太坊黄皮书，给出了以太坊虚拟机的技术说明。该黄皮书充满数学符号，极为晦涩难懂，笔者曾挑战数次，最终放弃。

2014年6月，以太坊开启了为期42天的 ICO，募集到3万个比特币，当时价值1843万美元。从此以太坊步入正轨。

以太坊 Ethereum，是一个通用的图灵完备的智能合约和去中心化应用（Decentralized Application，简称 Dapp）平台。所谓图灵完备，可以简单理解为：一切可计算的问题都能够计算。

智能合约概念最早由密码学家尼克 · 萨博（Nick Szabo）在1995年提出，是一种在区块链上运行的相对独立的程序，是纸质合同的代码化和自动化的产物，极具革命性。智能合约完全按照程序设定的条件运行，可以自动实现条件判断、资金划转，杜绝了扯皮推诿、中心化操控、欺诈和干涉的可能性。去中心化应用（Dapp）是指一个功能完备的独立应用，类似于手机 App，包括一个或多个智能合约，以及交互界面。

要实现这样的宏大目标，以太坊的结构设计要远比比特币更复杂和抽象。V 神意识到了这一点，所以开发了一些设计原则来管理这种复杂性。

以太坊的设计原则（摘自白皮书）

1. 简洁：协议应尽可能简单，即使要付出数据存储和时间的代价。这可以降低个体对协议的影响。团队会拒绝增加复杂性的改进，除非它有根本性的好处。
2. 通用：没有“特性”是以太坊设计哲学中的核心特征。以太坊提供了一个图灵完备的脚本语言，以帮助用户创建任何的智能合约或交易类型。
3. 模块化：组件应尽可能模块化和独立。应支持在协议中做小改动的同时，应用层却可以不加改动地继续正常运行。最大程度地模块化可以帮助整个加密货币生态系统。
4. 无歧视：协议不应主动限制或阻碍某一特定的项目或用途，协议中的所有监管机制都应被设计为直接监管，不应拒绝不受欢迎的应用。你可以运行一个无限循环的程序，只要你支付足够的交易费用。

以太坊的结构

整个以太坊系统，可以分解为：一个 P2P 网络，共识规则，交易，以太坊虚拟机 EVM，区块链，共识算法和客户端。软件层面的构成包括：账户，状态，瓦斯和费用，交易，区块，交易执行，挖矿和工作量证明。如图3.1所示为以太坊的基本架构。

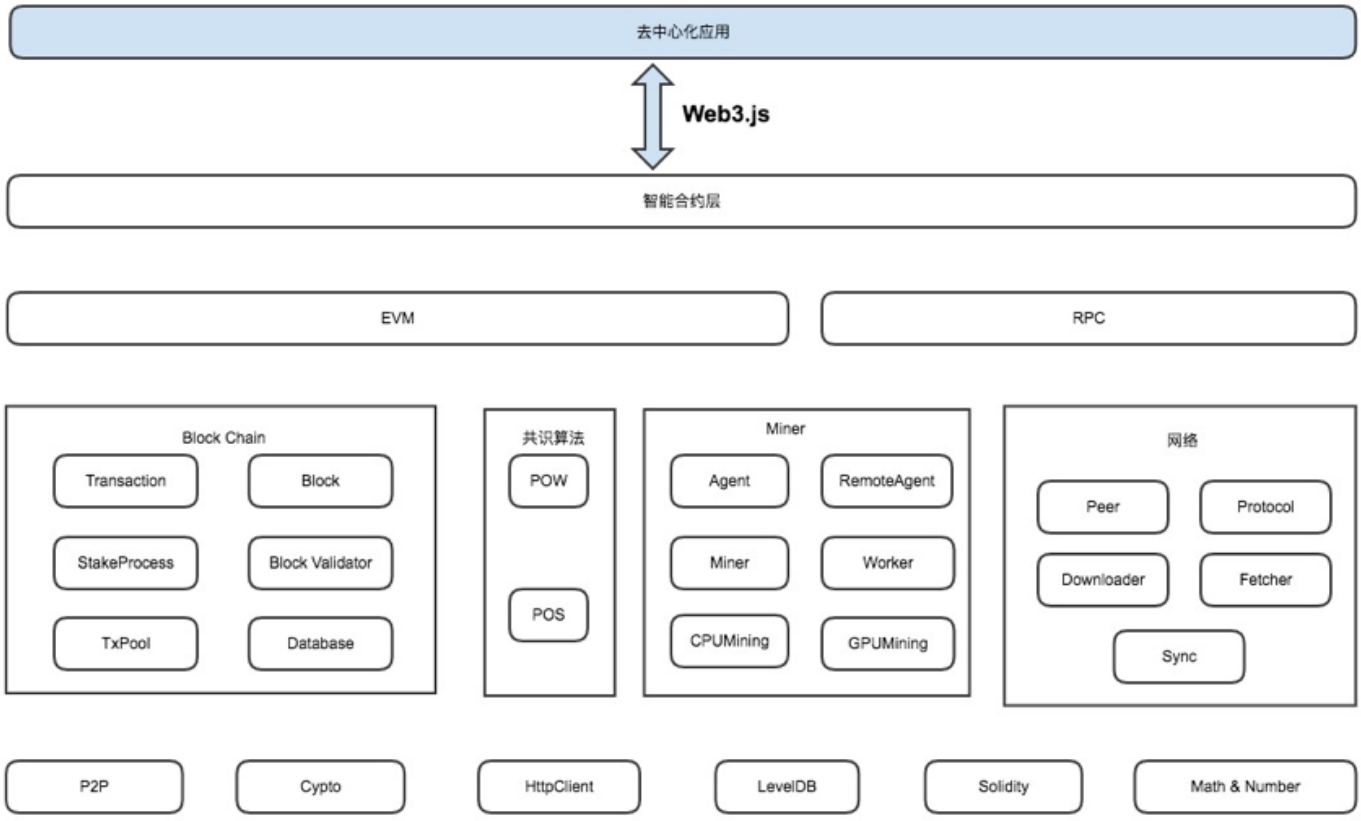

图3.1 以太坊的基本架构

以太坊虚拟机（EVM）是以太坊智能合约的执行环境。网络中的每个节点都运行 EVM，节点使用 EVM 执行所有的一般转账交易和智能合约交易，并获得区块奖励和交易费用。以太坊虚拟机是图灵完备的：这意味着 EVM 代码可以实现任何计算，包括无限循环。为防止智能合约陷入无限循环无法退出，以太坊引入了 Gas 费用机制，每一步计算都需要支付一定的费用，由于没有用户能支付无限的 Gas，这样就不会存在无限循环问题了。

Gas 是计算资源的计量单位，用来衡量在一个具体计算中需要的费用单位。对每个交易或智能合约，发送者都需要设置 Gas Limit 和 Gas Price。

Gas Limit 代表用户愿意花费在 Gas 上的钱的最大值。Gas Price 是为每个 Gas 支付费用的单价，即：你愿意在每个 Gas 上花费 Ether 的数量，以“gwei”进行衡量。如果交易使用的 Gas 少于或等于 Gas 上限，智能合约会被继续执行。如果 Gas 总数超过 Gas 上限，则撤销所有修改，除了依然合法且矿工能够收到费用的交易。

收取费用可以给矿工合理的经济激励，同时也是出于安全的考虑，防止节点向网络发送大量的零费用或极低费用的垃圾交易以堵塞网络。

以太坊的内生代币叫做以太币（Ether，简称 ETH）。以太币没有总量上限，目前采取了一个通胀率递减的发行模式，与比特币的递减发行机制不同。部署和执行智能合约需要用到以太币。因此，有人将以太币称为“燃料货币”，业界流行“比特币是黄金，以太币是石油”的说法。用户账户（所谓 EOA）和智能合约都可以拥有自己的地址，并持有以太币。

在以太坊中，可以用3种编程语言编写智能合约，包括 Solidity、LLL 和 Serpent，其中 Solidity 最受欢迎。

目前以太坊采用与比特币类似的 POW 工作量证明机制。矿工通过处理交易和执行智能合约来赚取以太币、生成区块。以太坊使用区块链数据结构和工作量证明共识协议，未来可能会升级到 POW+POS 的混合型共识协议。以太坊的出块时间更短（约14秒），因此带来了一些安全和技术问题，比如无效块（叔块）。

Whisper 是以太坊架构中的一个去中心化通信协议，Swarm 则是一个区中心化的文件系统。

以太坊的开发过程

以太坊的开发过程经历了4个阶段：前沿 Frontier，家园 Homestead，大都会 Metropolis 和宁静 Serenity。

- 从创始区块开始是 Frontier，只有命令行界面，持续时间为2015年7月30日至2016年3月。
- 区块高度1,150,000时，即2016年3月，进入以太坊第二阶段 Homestead，添加了图形界面。
- 在高度为1,192,000时，发生了著名的 DAO 被盗分叉事件，直接导致了以太坊经典（Ethereum Classic，简称ETC）的诞生，与回滚交易的 Ethereum 成为竞争的数字货币系统。DAO 事件细节戳这里：http://www.8btc.com/eth-thedao
- 在高度为2,675,000时，系统进入 Spurious Dragon 硬分叉，旨在解决拒绝服务攻击和重放攻击。
- 当前时点（2018年6月），以太坊处于 Metropolis 阶段，由两个硬分叉 Byzantium 和 Constantinople 带来。Byzantium 于2017年10月生效。预期 Constantinople 将于2018年年中生效，会引入 POW/POS 共识算法。
- 下一个里程碑版本是 Serenity，需要硬分叉，目前还没有明确的发布时间表。Serenity 将把共识协议改为 Casper（POS 的一个修订版本），并将整合状态通道和分片技术。

目前，市场上流通的以太币约1亿枚，单价为560美元，总市值约560亿美元，为第二大市值的公有区块链项目，仅次于比特币。

目前出现了一些新的公有区块链项目，旨在提供一个更强大的去中心化应用和智能合约的通用平台，与以太坊展开直接竞争，如 EOS。

理解比特币和以太坊之后，第4节我们会转向数字货币生态圈的更多玩家，如挖矿业、交易所和媒体等。

了解更多：

以太坊官网 https://www.ethereum.org/
区块链浏览器 https://etherscan.io/