第02课：比特币...

你好，我是丹华。今天我们来讲一讲关于比特币的基础知识。

比特币是在2008年由署名为中本聪（Satoshi Nakamoto）的匿名人士发明的，是一个完全去中心化的电子现金系统，它完全不依赖中央机构（如央行）。

比特币开发团队——Bitcoin Core

中本聪于2011年4月退出公众视线，将代码和网络维护的责任转交给一个志愿开发者小组身上，即所谓的比特币核心（Bitcoin Core，https://bitcoincore.org）团队。目前社区认为，Bitcoin Core 团队是比特币的官方开发者团队，负责比特币的权威和参考版本，其他版本一般与之兼容。可在 Github 找到 Bitcoin core 的最新源代码。

Bitcoin 是一个开源项目，源代码可以根据开放（MIT）许可证提供，可免费下载并用于任何目的。任何人(包括你)都可以参与比特币的代码开发。到2018年，比特币的源代码有551个contributor，大约十几位全职开发人员，几十名兼职开发者。

如图2.1所示，为比特币核心的基本架构，可以据此对比特币软件有初步认识。

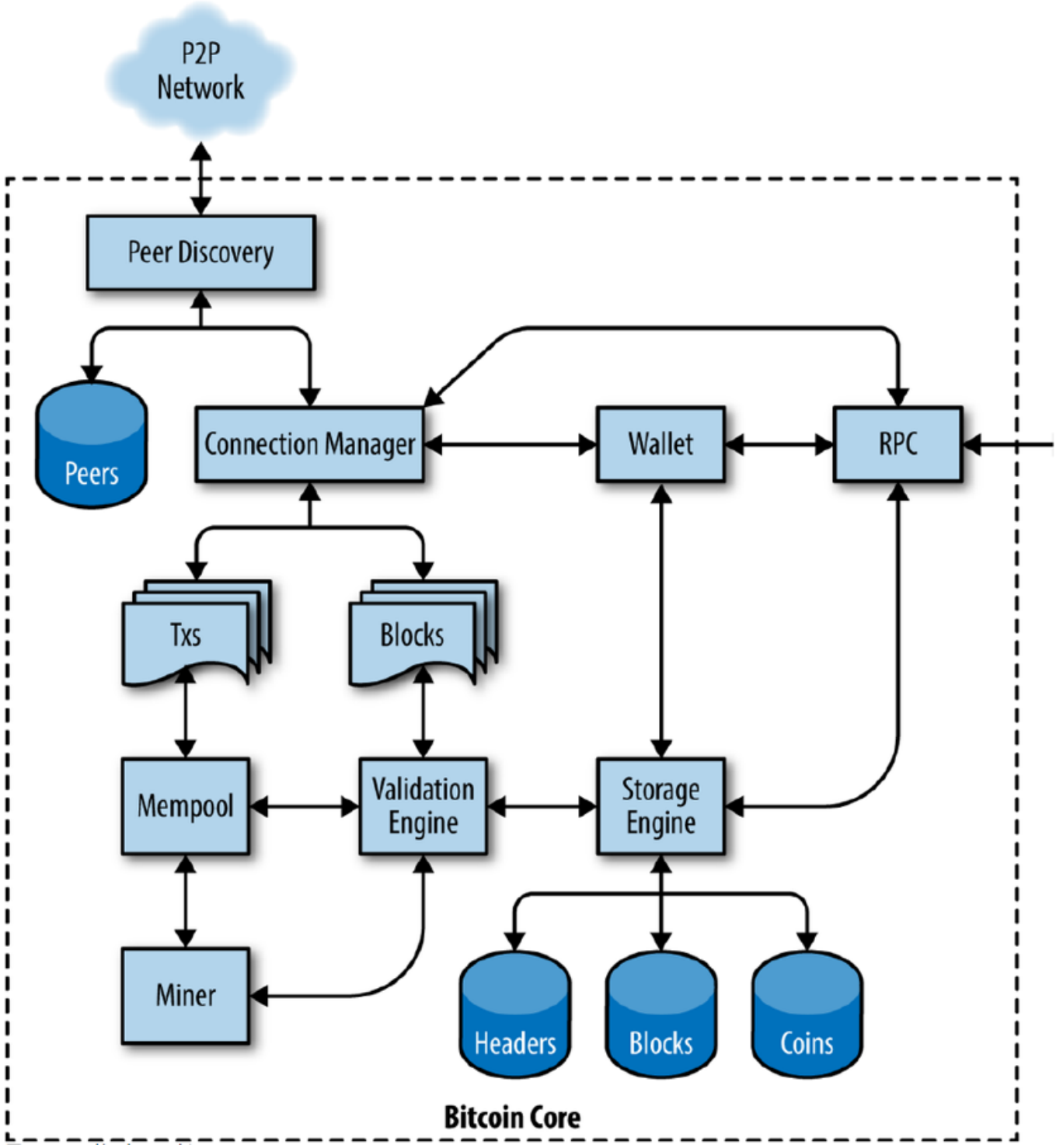

图2.1 比特币核心的基本架构

比特币：既是货币又是网络

比特币有三重含义：既代表比特币网络，也指网络节点使用的比特币软件，也可以指网络中交易的数字货币单位。用作数字货币或记账单位时，通常简写为 BTC 或 XBT。

比特币网络是一个由若干节点组成的用以广播交易信息和数据区块的 P2P 网络，这个网络包括矿工、比特币软件、钱包、用户、交易所等。

挖矿与工作量证明

矿工利用专门用于挖掘比特币的软硬件系统即矿机，来验证交易，并将交易打包成区块，完成工作量证明机制（proof-of-work），通过公平竞争，最终以获得区块奖励和交易手续费（也称矿工费）作为回报。比特币挖矿是一个极富竞争性的行业。自从比特币存在开始，每年比特币算力都成指数增长。

所谓工作量证明机制，就是重复计算区块头的哈希值，不断随机尝试一个参数，直到产生与难度哈希值匹配的过程。哈希函数的结果无法提前得知，也不存在得到特定哈希值的破解算法。所以，得到特定哈希值的唯一方法是依靠无数次不断的尝试，每次随机修改输入，直到出现适当的哈希值。因此这一机制催生了专用挖矿芯片和矿机的持续进化。矿机算力也构成对网络的一种保护。

可以将比特币挖矿类比为一个巨大的多人数独游戏。想象一个有几千行几千列的数独游戏。我们可以调整这个游戏的规模大小（更多或更少的行列），以保证全网计算机每次解开一个数独游戏需要大约10分钟。数独游戏与比特币挖矿 “谜题”都有一个非常好的性质：找到答案只能依靠诚实的计算，非常花时间；一旦找到，所有节点都可以很快验证答案是否正确。

手续费与区块奖励、减半发行机制

矿工挖矿，完成工作量证明的猜谜游戏是为了过去打包新区块的权力，这将为矿工带来两类收入：一是新区块中所有的交易手续费；二是区块奖励，即新币发行。

交易手续费是在发送比特币到另一地址时需要用户设定的支付给矿工的比特币数量，一般根据比特币网络中的市场力量动态确定。一笔交易的交易费越高，越可能被矿工优先处理。

挖矿所得的区块奖励就是新比特币的发行过程。新币发行被设计为产量递减模式，即 “四年减半”。系统设定，奖励给矿工的比特币数量大约每四年（或准确说是每210,000个块）减少一半。也就是说，2009年1月开始，区块奖励为50个比特币，然后到2012年11月减半为25个比特币。2016年7月再次减半为12.5个比特币，以此类推，直到2140年所有的比特币（21,000,000）全部发行完毕。2140年之后，不再有新的比特币产生，世界上流通的比特币上限恒定在2100万个。

比特币这种总量有限并且发行速度递减的机制，透明的、公平的、事前确定，保证了系统内生代币的长期价值，能够有效激励矿工、投资者及其他人及早进入积极行动，从而推动生态系统像滚雪球一样发展壮大。

比特币地址

比特币在不同的地址之间转移和交易。比特币地址（例如：1LVL7K3SNwZr7hUhBXrDYzx83mzL5h5eLt）由一串字符和数字组成，由公钥经过单向的加密哈希算法得到，相当于收款账户，类似于 email 地址。不同的数字货币有自己的地址体系，互相之间不能共用。

比特币交易

处理交易是比特币网络的核心功能。一笔交易是指把比特币从一个地址转移到另一个地址。更精确地，一笔“交易”指一个经过签名运算的、表达价值转移的数据结构。任何一笔交易的都附有交易费，意在通过对每一笔交易收取小额费用来防止对系统的滥用。

区块与区块链

每一笔“交易”都经过比特币网络广播和传输，由矿工节点收集并封包至区块中，永久保存在区块链某处。要确认一笔交易，一个交易必须包含在一个区块中，并被添加到区块链中。

一个区块（Block）就是若干交易数据的集合，它会被标记上时间戳和之前一个区块的独特标记，网络每10分钟生成一个区块。区块头经过哈希运算后会生成一份工作量证明，从而验证区块中的交易。所有的区块按时间顺序串联起来，形成区块链（Blockchain）。

比特币软件设定，平均每10分钟生成一个区块，称为出块速度。这就是比特币的心跳，是比特币的发行速率和交易达成的基准参数。为保证这一参数恒定，应对矿工算力的进入退出冲击，比特币网络设定了对挖矿难度进行动态调整的机制，即每2016个区块（约2周时间）调整一次，以实现平均10分钟产生一个新区块。

注意，并不是每个数字货币的出块速度都是10分钟。其他的数字货币都有自己的出块速度，如莱特币和 ZCash 是2.5分钟，以太坊是14秒左右。

你可以将区块链想象成地质上的沉积岩层构造。表层岩土会随着季节、洪水而变化，但是越往深处，地质层就越稳定。到了几十上百米甚至更深的地方，是保存了数百万年的岩层。在区块链里，区块在区块链中的位置越深，被改变的可能性就越小。

交易所

交易所是指提供数字货币与法币兑换服务的场所，是生态系统的重要参与者。大多数用户买卖比特币，都是通过交易所的币币交易（非法币）来完成的。目前全球有上万家交易所公司，也有一些场外交易的兑换平台。

小结

比特币代表了数十年的密码学和分布式系统的巅峰之作，这是一个独特而强大的组合，包括以下四个关键创新：

- 一个去中心化的点对点网络（比特币协议）
- 一个公共的交易账簿（区块链）
- 一个去中心化的数学的和确定性的货币发行（挖矿机制）
- 一个去中心化的交易验证系统（交易脚本）

这四点紧密协作，形成了整个比特币的软件系统。

以上是比特币景区的主要知识，接下来我们将进入另一个设计目标和原理完全不同的 5A 级景区——以太坊 Ethereum。