由于虚拟货币价格高昂，越来越多的人参与到“挖矿”活动中，这使得“挖矿”对计算机的计算能力要求更高。到现在，挖矿用的硬件经历了很多升级和改造，从最初的CPU挖矿到GPU，再从FPGA到ASIC。同时，随着矿机数量和规模的增加，“矿”的危害也越来越明显。

矿机设备的发展历程

CPU“挖矿”(2008~2009)

2008年11月，比特币的开发者和创始人中本聪在P2P基金会网站上发表了比特币白皮书《比特币:一个点对点的电子现金系统》，提出了电子货币的新思路，为比特币的诞生奠定了基础。2009年1月3日，他开发出第一个实现比特币算法的软件程序并进行第一次“挖矿”，获得50个比特币，这标志着比特币金融体系正式诞生。之后市场上逐渐出现了用于挖矿比特币的加密货币矿机，“挖矿”进入了最初的发展期。2008-2009年，市场上的加密货币矿机主要是CPU矿机。

GPU和FPGA“挖矿”(2010~2012)

从2010年到2012年，比特币的关注度逐渐提高，挖矿人数不断增加，“挖矿”难度明显加大，计算能力的竞争越来越激烈，对电脑配置的要求也越来越高。由于CPU运算能力低，“挖矿”利润低，CPU矿机逐渐被市场淘汰，性能进一步提升的GPU矿机和FPGA矿机逐渐出现。

虽然CPU和GPU都可以做计算，但是擅长的方面不同。CPU较少，但有复杂的逻辑控制单元，更擅长复杂运算；GPU的核心数量多，架构相对简单，非常适合高通量、高密度的计算。然而，“挖掘”所需的计算能力往往是通过哈希、解密等算法来完成的。这类算法具有复杂度低但强度大的特点，所以GPU“挖掘”更快更高效。很多人转而用GPU“挖矿”，组装一个或多个高级显卡，构建自己的矿机。

此外，比特币价格的不断上涨，让矿工们“挖矿”的热情不断高涨。矿工希望拥有更强大的矿机，挖掘更多的比特币，获得更多的收入。因此，现场可编程门阵列(FPGA)这种先进的采矿设备应运而生。2011年年中，市场上出现了第一台FPGA比特币挖矿机，这是第一次出现针对“挖矿”的专业芯片设计。简单来说，FPGA“挖矿”就是把GPU的核心芯片单独拿出来，然后把多个核心芯片集成到同一个设备上“挖矿”。但是由于FPGA的开发难度太大，这种“挖矿”的方式并没有得到普及。

ASIC“采矿”(2012年至今)

随着矿工越来越多，比特币的价格不断上涨，“挖矿”的竞争也越来越如何购买比特币（如何购买比特币?新手如何购买比特币指南攻略）激烈，更专业的挖矿机器和设备开始出现。在此期间，以ASIC为代表的专业矿机正式进入人们的视野。ASIC是专用集成电路(Application Specific Integrated Circuit)的缩写，即专门为特定目的而设计的电子电路(芯片)。专门为“矿”设计时，生产ASIC矿机，相当于数字货币中专门为矿定制的集成电路设备，没有其他功能和作用。

ASIC因为只运行特定的算法，所以与通用集成电路相比，具有体积更小、功耗更低、可靠性更高、性能更高、安全性更高、成本更低的优势。就“挖矿”计算能力而言，ASIC“挖矿”比CPU、GPU高几万倍甚至几十倍。

从CPU到GPU，从FPGA到ASIC矿机。为了提高计算效率，比特币挖矿机经历了这几个发展阶段。到目前为止，包括比特币在内的基于SHA
256算法的加密货币，基本都是用ASIC“挖矿”的。

“挖矿”模式的升级转变

比特币刚刚兴起的时候，每个人都可以用CPU和GPU在个人电脑上“挖矿”，获得相应的收益。但随着矿工人数的逐年增加，在全网计算能力提升到一定程度后，个人电脑挖到比特币的概率变得很低，个人矿工在计算能力和能效上越来越不占优势。因此，市场上很快出现了集成大量计算资源的矿池。矿突破地理位置的限制，用“矿”的计算能力连接分散在世界各地的矿工，协同“矿”。相比单个算力低的矿工，矿池的成功率要高很多。当一个矿池成功挖出一个区块，矿池中的所有矿工都将获得比特币奖励，奖励金额与矿工对计算能力的贡献成正比。同时，矿池也在这个过程中收取费用。

此外，由于采矿设备昂贵，运维复杂，云采矿逐渐成为一些个体矿工的选择。云“挖矿”是指利用从第三方(云“挖矿”服务商)租用的计算能力生成加密货币的过程。通过向服务提供商购买一定量的“哈希能力”，每个矿工就相当于参与了一个“矿”(专门用于加密挖掘的远程数据中心)。作为交换，供应商将给予他们与矿工购买的计算能力份额成比例的奖励。由于采矿作业是通过云进行的，矿工们无需担心计算机设备维护、噪音、热量或能源成本。找到可靠的云“挖矿”服务商后，矿工只需要选择要签订的合同类型和所需期限，提供商就会设置好运营所需的一切。

“挖矿”的危害

首先，虚拟货币“挖矿”需要大量的电力支持，能源消耗和碳排放量惊人，这与新

发展理念背道而驰，也不利于实现国家二氧化碳排放峰值和碳中和。

中国的虚拟货币“矿”多分布在电力资源丰富、电费便宜的地区，如火电资源丰富的新疆、内蒙古，水电资源丰富的四川、云南等。然而，虚拟货币“挖矿”的高能耗引起了地方政府的高度警惕。今年以来，内蒙古自治区采取了多项政策措施，清退虚拟货币“挖矿”项目。截至4月底，已有35家“采矿”企业被关闭和退役。据初步统计，淘汰这35家“采矿”企业每年可节约52亿千瓦时的电力，相当于160多万吨标准煤。

其次，“挖矿”扰乱了正常的金融秩序乃至社会秩序，往往成为洗钱、非法转移资产等违法犯罪活动的工具；更多的犯罪团伙通过向公众出售虚拟货币“挖矿”设备，或者租赁计算能力进行“挖矿”，吸引投资者购买计算能力，从而骗取居民个人钱财，影响社会秩序稳定。

第三，“挖矿”消耗大量计算资源，使得系统、软件、应用服务运行缓慢。个人电脑或服务器一旦被“挖矿”程序控制，就会造成数据泄露或病毒感染，容易引发网络安全问题。哈工大、CERT实验室发布的挖矿木马简要技术分析揭示，挖矿木马会影响政企机构运行速度，占用计算机资源，对其他相关设备、校园网运行甚至科研都有一定影响。此外，“挖矿”木马通常会关闭防火墙、获取管理员权限、植入后门等。，并用于窃取核心业务数据和发起勒索等其他网络攻击。

整理:王雅静