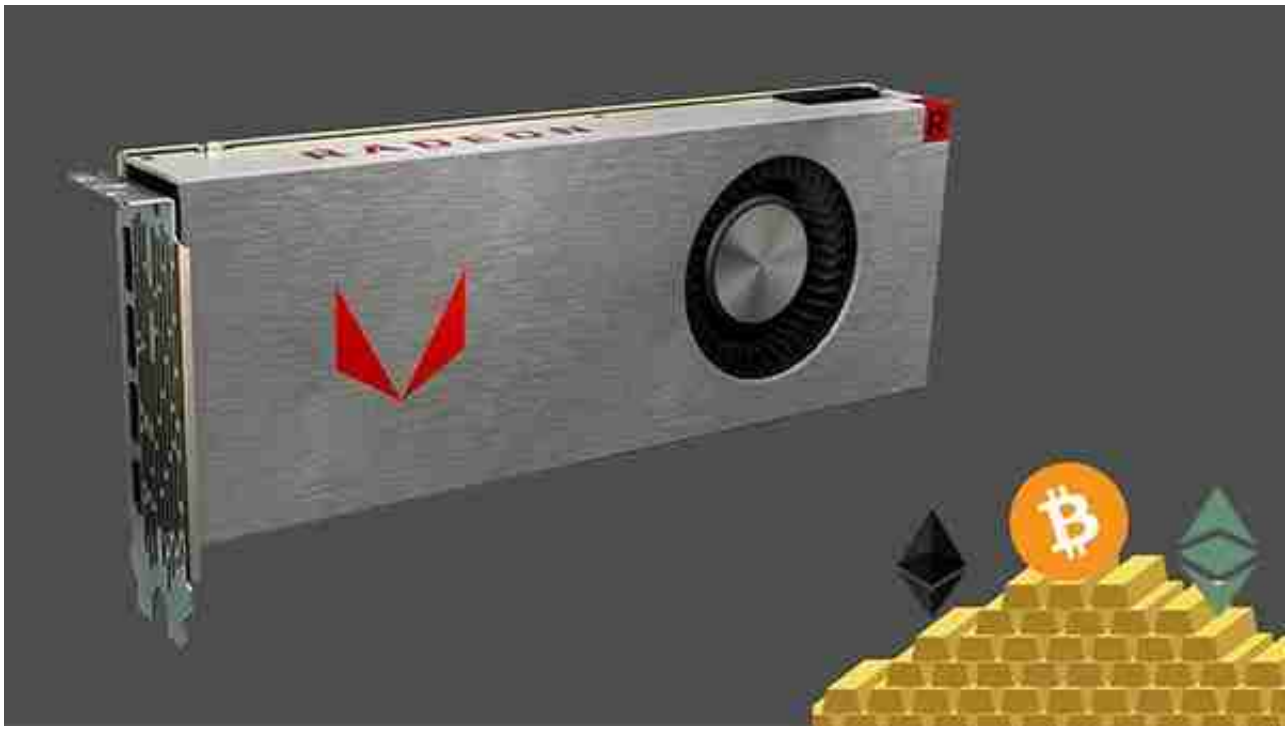
没说CPU不能挖啊，最开始都是用CPU挖。但是随着对挖矿算法的深入研究，大家发现原来挖矿都是在重复一样的工作，而CPU作为通用性计算单元，里面设计了很多诸如分支预测单元、寄存单元等等模块，这些对于提升算力是根本没有任何帮助的，而且CPU根本不擅长于进行并行运算，一次最多就执行十几个任务，这个和显卡拥有数以千计的流处理器差太远了，显卡高太多了，因此大家慢慢针对显卡开发出对应的挖矿算法进行挖矿。



以BTC为例，它最基本的算法原理就是，把已有的10分钟内的所有交易作为一个输入，加上一个随机数，当10分钟内所有交易记录加上你的这个随机数计算出一个SHA256的hash。里面几乎都是整数运算，这个根本就像是为显卡特别打造一样，显卡非常适合这种无脑性算法，流处理器数目越多约占优势。

就Hash计算而言，它几乎都是独立并发的整数计算，GPU简直就是为了这个而设计生产出来的。相比较CPU可怜的2-8线程和长度惊人的控制判断和调度分支，GPU可以轻易的进行数百个线程的整数计算并发（无需任何判断的无脑暴力破解乃是A卡的强项）。OpenCL可以利用GPU在片的大量unified shader都可以用来作为整数计算的资源。而A卡的shader（流处理器）资源又是N的数倍（同等级别的卡）

不过到了后来大家发现显卡还是太弱了，直接上ASIC大规模堆ALU单元就能极大程度提升算力，巴掌大的算力板的算力已经是显卡的好几十倍，所以现在比特币不用专门的ASIC矿机根本挖不动。

尽管后期的币种LTC所使用的 Scrypt
算法还引入了大量相互依赖的、随机的访存指令，当 Footprint 足够大时，还会在 GPU 的 L2 级别、甚至 TLB 级别出现大量的缓存失效，从而产生更多的 DRAM 访问，以弱化矿机（ASIC/FPGA）相较于 GPU 在整数运算性能上的优势，但是依然被人针对性研发出矿机，目前也只有专门矿机才能挖。

不过像第二代虚拟货币（比如说是ETH、ZEC这种）由于吸取了前辈们被爆算法的经验，在挖掘算法上做了更加特别优化，防止出现无脑的运算，对于显存要求特别高，因此可以有效抵抗矿机的入侵。

也因为ETH这种只能靠显卡挖矿，造成了2017年下半年开始的显卡涨价潮、缺货潮，很多矿主都卖了成千张显卡回去组建矿机挖掘这些虚拟货币，久而久之，大家都认为CPU不能挖矿，其实只是效率、效益太低了而已。