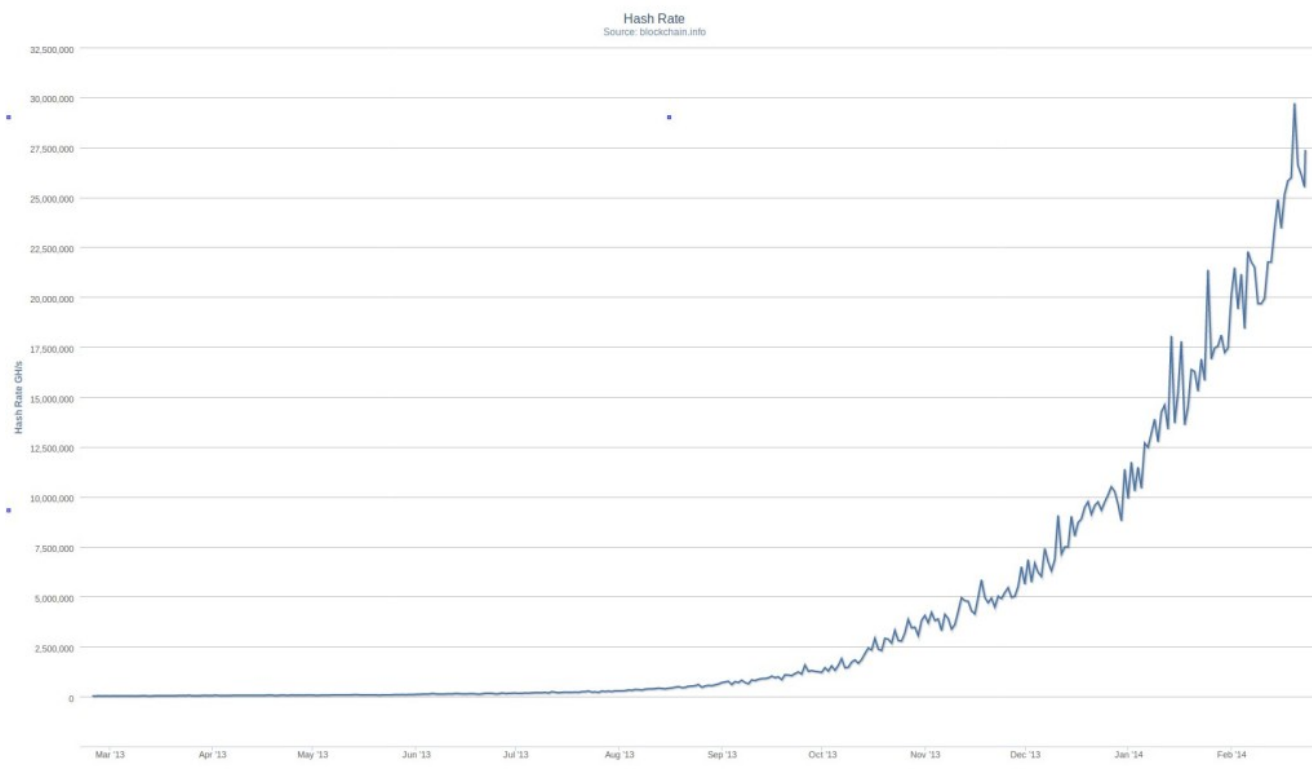


ASICS - Are They Evil?

As the arms race in bitcoin mining continues unabated, the flurry of misinformation and bad logic surrounding the issue is as intense as ever. Since litecoin originally launched and attempted to boast itself as having an “ASIC resistant” mining algorithm, people have been creating and touting various marginal alt-coins as the ultimate bitcoin successor because of supposed resistance to ASICs and mining centralization. This is flat out wrong. Any successful proof-of-work based crypto-coin that develops high enough value will experience the same kinds of mining dynamics we’re seeing with bitcoin. It’s all about the money.

The Arms Race

Now that each bitcoin is worth hundreds of dollars, the 25BTC block-reward distributed by the protocol to bitcoin “miners” every 10 minutes is very enticing. More and more serious, and well-funded, mining operations are appearing. You only need to glance briefly at a [bitcoin-mining hashrate chart](#) to understand that something explosive is going on here:



What are ASICs?

ASIC stands for Application Specific Integrated Circuit; ie, a specialized computer chip. Back in late 2012 when it became clear to some that bitcoin was likely to keep gaining in value, engineering teams started to work on developing ASIC chips for bitcoin mining. These chips could mine at 10-100x greater power-efficiency than the standard GPU (graphics-card) mining hardware at the time.

So what's the controversy?

ASICs are expensive. A single [top-of-the-line ASIC rig](#) (the chip + supporting hardware) can cost \$5,000-\$10,000. That makes cutting-edge bitcoin-mining hardware out of reach for many people. No longer can someone spend a few hundred dollars on a fast GPU card, stick it in any old computer, and profitably mine bitcoins.

That has some people in the bitcoin community forecasting doom at the hands of big-money, centralized, corporate bitcoin mining operators. The fear is that, eventually, there will just be a few huge bitcoin miners that are susceptible to less-than-honest practices or government interference.

How is this a problem with ASICs?

It isn't. People are just associating "big money" and centralized power structures with ASICs because ASICs cost "big money". The problem is not ASICs; it's the fact that when a coin achieves enough value, it suddenly becomes rational to throw significant money into mining it. This has already started happening to litecoin, with multi-thousand-dollar GPU rigs fairly common, and [scrypt-ASICs around the corner](#) (something that litecoin's proponents originally said would never happen).

It's simply the case that people are going to invest money into mining gear if there's profit to be made. Whether the specific mining algorithm lends itself to ASICs, GPU farms, CPU farms, lots of memory, or something else, those with the ability to throw lots of money and compute power at the problem are going to get a greater share of the mining market. Eventually, this centralizes to those with the most power-efficient hardware, no matter what the algorithm.

So make no mistake: proof-of-work mining will be done at data-center scale in any mature and valuable coin.