Mining Difficulty

Difficult is always computed at the time that a block is received: that is, you quickly compute the difficult that that block was paired against, and then verify that their hash is valid given that target.

Over time, mining power has generally increased at an exponential rate. However, there have been some instances (e.g., around July 2014) where the hash rate has dropped for a short period of time. The most likely explanation is that the price of Bitcoin changed or the price of electricity changed which made mining less lucrative and, in turn, led some minors to temporarily turn off their machines.

SHA-256

SHA-256 is the hash function used in Bitcoin. It was designed in the 90s and is considered to be cryptographically secure.

In more detail, SHA-256 returns a 256-bit digest by running a 256-bit state (divided into 4-byte chunks) through a series of bitwise tweaks and modular arithmetic over 80 iterations.

You might be tempted to do something cheaper and only compute the first few bytes (i.e., to check if they're all-zero, as is necessary to be a valid target), but this is impossible given that each iteration depends on the complete state of the previous. =

(One minor optimization would be to short-circuit on the 80th iteration if the first few bytes are non-zero. This would lead to roughly a 1% increase in margins. However, for whatever reason, you actually hash the header *twice*, so this optimization only applies in the secure computation and thus yields more like a 0.5% increase in margins.)

Mining Hardware

CPU Mining

On a high-end PC, you can reach a throughput of roughly 10-20 MHz, requiring nearly 139,461 years to find a block. Things like Bitcoin mining via malware wouldn't be very profitable.

GPU Mining

GPUs are easily available and easy to setup. They typically include parallel ALUs and bit-specific instructions. A single CPU can often run multiple GPUs, all of which can be *over-clocked*.

The key idea behind over-clocking is that *some* errors are okay if you increase the throughput at a disproportionate amount. For example, define the “good put” to be the throughput multiplied by the success rate. Over-clocking by 50% with 30% errors is clearly a worthwhile tradeoff.

The practicalities of GPU over-clocking led to some sketchy tactics. GPUs aren’t designed to be run at these high speeds and withstand the resulting heat, nor are they designed to be fed this much power. Miners would typically remove the cases, fry the cards, feed power directly to the chips, etc. In short, these GPUs have poor cooling and a large power draw, so miners came up with hacks to get around these.

FPGA Mining

Field-**P**rogrammable **G**ate **A**rrays (FPGAs) started to be used for Bitcoin mining around June 2011. Mining software was implemented in Verilog and resulted in better performance (for bitwise operations in particular), better cooling, and extensive customization and optimization.

Unlike with the GPUs, you didn’t need another board to drive the cards and the setup was much more sane. However, there was a high failure rate as the power draw was above their capacity.

On a good card, you had throughput of 100-1000 MHz, leading to roughly 25 years per block.

ASIC Mining

Today, Bitcoin mining is all about ASICs.

There have been a number of companies that have promised mining-specific ASICs, but almost all of them have been incredibly delayed on shipping–it’s a common thread among Bitcoin-related companies. (There’s some suspicion that miners had been using the hardware themselves before sending them out.)

(When Arvind went to Vegas, there was a booth of miners followed by a single class-action lawyer giving away his card.)

It’s expected that ASICs can provide less than a 10x performance improvement as we’re approaching known limits on feature sizes. They’re designed to be run constantly for their entire life.

Case Study: TerraMiner IV

The TerraMiner IV first shipped in January 2014, hashing at 2 TH/s and costing $6000. Still, it’s expected that it will take 14 months for a single TerraMiner IV to find a block.

Market Dynamics

Most boards are obsolete within 3-6 months, with half of their profits coming in the first six weeks. This means that the shipping delays (e.g., those experienced with ASICs) are crippling for customers. (Interestingly enough, many customers have actually come out ahead due to the rapid price increase of Bitcoin.)

Energy

Landauer's principle: Any non-reversible computation must consume a minimum amount of energy. SHA-256 is a non-reversible computation and thus we can ascribe some fundamental limit to the amount of energy that must be consumed for a block to be mined.

Bitcoin mining consumes energy through both electricity usage and cooling. We can reason about usage in two ways.

Top-down

Assume a miner is spending *everything* on electricity.

- Each block worth $15,000.
- Approx. $25/s generated.
- Industrial electricity can be valued at $0.03/MJ or $0.10/kWh.

This gives us an **upper-bound** on electricity consumed of 900 MJ/s = 900 MW. However, this model doesn't provide any room for profit and takes neither hardware nor cooling into account.

Bottom-up

Look at how much hashing the network is doing and then assume everyone is running at peak performance.

- Best claimed efficiency: 1 GHz/W.
- Network hash rate: 150,000,000 GHz.
- (Excludes cooling and embodied energy.)

This gives us a **lower-bound** on electricity consumed of 150 MW. However, not everyone will be running at peak efficiency.

What is a MW?

The Three Gorges Dam produces roughly 10,000 MW, while a typically hydro plant produces roughly 1,000 MW and a major coal-fired plant produces roughly 2,000 MW. So, a power plant can power a few Bitcoins worth of mining.

You might argue that this is wasteful, but all payment systems require energy. Bitcoin is effectively using this energy to prevent double-spending. With cash (apart from actually minting the coins and moving them around), you have to devote significant resources to prevent counterfeiting and fraud.

Data Furnaces

In the limit, computing devices produce heat almost as well as electric heaters! Could we use mining rigs in homes as heaters?

This sounds crazy and there are certainly some challenges, e.g., who owns and maintains the rigs, gas heaters are still 10x more efficient, etc. But the key idea is not out of the question.

Open Questions

- Will Bitcoin drive out electricity subsidies?
- Will Bitcoin require guarding power outlets?
- Can we make a currency with no proof-of-work? Or can we come up with a useful proof-of-work (e.g., factoring large primes)?

Mining Pools

The economics of being a miner: you pay $6,000 for a rig, expect roughly 14 months to find a block, and expect to earn roughly $1,000/month.

However, there's a lot of uncertainty around mining. The expected revenue may be $1,000/month, but there's a lot of variance, e.g., there's a $>$ 40% chance that you don't find a single block over the course of a year.

To fight against this uncertainty, miners began to form **pools** in which pool participants all attempt to mine a block with the same coinbase recipient. Revenues would then be distributed to members based on how much work they performed. Under such a scheme, you can achieve roughly the same earning rate with a much better guarantee.

Mining Shares

How can you show that you've done a certain amount of work? The key idea is to prove work with "near-valid" blocks, known as "shares". For example, you could find hashes with a certain number of zeros at the beginning (but too few to be a valid block target).

Pools include a pool manager who tells everyone which block to work on–this puts a lot of trust in the pool manager. In the header of this block, the pool manager encodes that the block reward should go to the manager so that pool participants can't steal the block after they've found a valid hash target.

Payout

Once a valid hash is found, the pool manager collects all the shares and divvies out profits according to the number of shares submitted by each miner. There's typically no reward for being the miner who finds the valid hash–it's just about the number of shares.

Even under those rules, there are several different payout models:

- **Proportional payout**: Pool manager pays out based on the total BTC reward gained from mining, weighing that by the percentage of shares that a given participant submitted.
- **Pay-per-share**: Pool manager pays out regardless to the BTC reward gained from mining, paying out a fixed fee when a participant submits a share. The pool manager thus absorbs all the risk as the pool might get really unlikely by not finding a block, yet the manager is still required to pay participants.

Why might we want to give a slightly higher reward to the participant who finds the valid hash? The participant who finds the block actually has a lot of leverage: they can choose not to send in the hash, hurting everyone and worsening the pool's performance. If they're not being paid more for submitting it, then they might as well hold it back and continue to generate shares.

Pool Size

The key issue with pools: **you're motivated to join the biggest pool possible**, as larger pools have the least variance and are more likely to be honest (given that they've probably been around for longer, etc.). As a result, some pools are getting too big: for example, GHash.io attained over 51% of mining power in July. In practice, participants will jump ship if a pool gets too large, and in the GHash case the pool actually stopped accepting new participants.

Conclusion

Given their drawbacks, pools are a subject of some debate. We can summarize the pros and cons as follows.

Pros

- Make mining more predictable.
- Allow small miners to participate.
- More miners using updated validation software.

Cons

- Lead to centralization, as in the GHash case.
- Discourage miners from running full nodes, as participants typically run very light or thin clients.