Calculating the Hashrate of Ethereum

Method

From Ethereum yellow-paper follows that the proof-of-work algorithm used for the consensus algorithm is specified as follows:

$$(n, m) = PoW(H, H_n, d)$$

Here H is the header of the block without the nonce and mix-hash, H_n is the header with included 64-bit nonce and d is the DAG used. n is a 256-bit hash value resulting from the ethash algorithm and m is the 256-bit mix-hash. The mix-hash originates from the memory-hard loop in the ethash algorithm. This mix-hash is computed as a means of proof-of-work instead of finding a correct SHA256 hash value. The mix-hash is computing using memory-hard highly interdependent operations to achieve ASIC-resistance although numerous ASIC hardware has been developed last few years specifically for the ethash algorithm.

This must satisfy:

$$n \leq \frac{2^{256}}{H_d} \land m = H_m$$

The the above equation, the hash value n must be lower than a target value $\frac{2^{256}}{H_d}$ specified by the difficulty H_d at that time. The probability of finding a correct nonce is

$$p_{targetFound} = \frac{\frac{2^{256}}{H_d}}{2^{256}}$$

Each nonce value behaves like an independent trial such that the number of tries is geometrically distributed. Which means that the number of tries to find a block with given difficulty can be computed as

$$N = \frac{1}{p_{targetFound}}$$

The time to mine a block is kept relatively stable by adjusting the difficulty according to previously mined block's timestamp and difficulty.

`Note that computing the difficulty at a given time is not trivial as the difficulty is adjusted every Block instead of every 2016 blocks in Bitcoin`

The time to mine a block can be queried using various API's from mining pools and is kept track of by Ethereum as a timestamp t at the inception of a new block.

Since the time consumed to mine a block $E[i] = t_{B_i} - t_{b_{i-1}}$ is simply computed as the difference in timestamps between two existing block and it's difficulty can be easily queried, the hashrate R can be easily computed. The hashrate R denotes the amount of PoW (ethash) operations performed by the network per second.

$$R = \frac{N}{E[t]} = \frac{\frac{1}{(\frac{(\frac{2^{256}}{H_d})}{2^{256}})}}{E[t]} = \text{hashrate in hashes per second}$$

`Can also be deduced from the current increase in ETH`

```
SparkPool calculates hashrate using the shares count, and the time zoom is 20 minutes.
hashrate = validShares * 3.33 MH/s
```

Calculating the Energy usage

Lower bound

To calculate the lower bound of the energy usage of Ethereum, the most common (accepted) method, also used by Bevand, Stoll, etc is to assume the network hardware is made up of the most state-of-the-art efficient hardware currently available.

When the hashrate R (MH S^{-1}) of mining hardware is know together with its power usage P (W), the power efficiency PE can be calculated as $PE = \frac{P}{R}$ (J MH^{-1})

Ethereum was designed to counter ASIC hardware by using a dagger-hashimoto-like algorithm wich is memory-hard. Therefore the most efficient hardware remained GPU's for a long time. Recent developments of ASIC for the ethash algorithm changed this. The table below is made up from mostly ASIC machines as well as some popular/most-efficient GPU's.

Wednesday 4 dec:

Mining Hardware	**Hashrate (MH S^{-1}) (advertised)**	**Power Consumption (W)**	**Efficiency (J MH^{-1})**	**Release data**
Antminer E3	190	760	4	Jul 2018
Innosilicon A10(1)	432	740	1.713	Sep 2018
Innosilicon A10(2)	485	850	1.753	Sep 2018
Innosilicon A10(3)	500	750	1.500	Sep 2019
Canaan xxxxxxx	2200	1500	0.68	TBA
Radeon RX470	24	150	6.250	Aug 2016
AMD Vega 64	31	295	9.516	Aug 2017
Titan V	77	237	3.078	Jul 2018
Tesla V100 16GB HBM2	90	250	2.778	Jun 2017
GTX 1080 ti	50	250	5	Mar 2017

sources:
- https://www.asicminervalue.com/

- https://www.miningbenchmark.net/
- https://www.reddit.com/r/ethereum/comments/d9rh4r/canaans*new*asic*is*a*pipe*dream*not*an_ethereum/

From this table it becomes clear that ASIC developments have dramatically improved GPU mining efficiency.

Results

Using data from publicly available miningpool API's (Ethermine, Nanopool), the difficulty and blocktime (time to mine a block) are known. This way we can calculate the needed hashrate R needed **for one block**. The results are in line with commonly used sources like https://etherscan.io/chart/hashrate.

Of course, this is the hashing power needed to complete **one previously mined block**, assuming geometric distribution of probability of mining a block. So it might be better to take the average of blocks mined during one day (or other time period).

```
Still need to know how to aggregate data, one day? one year?
```

Knowing this hashing rate R together with the most efficient available hardware efficiency from the above table, the theoretical power usage at a given moment can be calculated.

Queried on *5 dec*, using a PE value of 1.713 (Innosilicon A10) the power usage is around 300 MW or $2471816.557939 \text{ MWh Year}^{-1}$ which is roughly $2,5 \text{ TWh Year}^{-1}$
Using the most efficient GPU (Titan V) this number is 530 MW and $4.4 \text{ TWh Year}^{-1}$

Upper Bound

- Use method of Bevand:
  - See what mining hardware is just/barely viable for mining Ethereum from an economic standpoint (profitability threshold). Then, use this mining hardwares efficiency for each iteration in mining efficiency.
  - Assume that the hardware is never upgraded to more efficient hardware.

- Economic analysis (Digiconomist):
  - Estimate what share of revenue of a miner is used for electricity. (need average electricity costs which may not be straight forward in Ethereum)
  - Digiconomist did not account for ASIC developments in Ethereum yet...

Best guess

Ideas

Using data from Krause & Tolylamat (2018) with given PE values.

Bevand's approach of hardware-mix (adoption time, economics)

Using the Api from large miningpools

Sparkpool, nanopool and ehtermine make up around 60% of total hashing power, source: https://www.poolwatch.io/coin/ethereum.
Miner data such as workers (hardware devices actually doing the mining) and corresponding hashrates can be an indicator of which class of hardware is used (GPU or ASIC) and maybe say something about the mining efficiency. At least it would give

a good idea about how much is being paid for electricity.
Average hashrates for workers in the above-mentioned mining pools are:
Sparkpool: 270 MH/s
Nanopool: 180 MH/s
Ethermine: 170 Mh/s
With the Api's I can figure out what the distribution of GPU vs ASIC is in these mining pools.

Currently working on:

- Uncles (phenomenon in Ethereum where blocks are not accepted on the blockchain because of network lag or a nonce is found by multiple parties at the same time)
    - Is this effort also captured in the energy usage?

- Upper bound
- Upper bound/best guess method, (Bevand?)
- Looking into ProgPow