Working Paper presented at the

Peer-to-Peer Financial Systems 2016 Workshop

2016

The Fair Cost of Bitcoin Proof-of-Work

Tomaso Aste

UCL

P2P Financial Systems

Powered by

Exponential Science

The fair cost of Bitcoin proof of work

Tomaso Aste
UCL Centre for Blockchain Technologies, Department of Computer Science, University College London, Gower Street, London, WC1E 6BT, UK

Abstract
In this short note I provide a very simple estimation of the fair cost for the proof of work in Bitcoin mining. I conclude that the current cost, although large, is of a justified order of magnitude for an anonymous systems operating between untrustful parties

Blockchain

Bitcoin, a digital cash currency launched in 2009 by an anonymous inventor with alias Satoshi Nakamoto [1], has demonstrated that untrustful peers can exchange value over the Internet without any third party intermediary or trusted authority. Bitcoin has reached over 10 billion dollars capitalization and the system is processing tens of thousands of transactions a day without having being so far challenged by any serious attack. Blockchain is the main technology underneath Bitcoin; it is a distributed ledger available to anyone participating to the Bitcoin network. In the network Bitcoin transactions are publically announced and valid transactions are chronologically registered on the ledger. The validity of a transaction is verified by the network participants themselves and valid transactions are put into blocks which are cryptographically sealed and attached to the previous block every 10min on average. The blocks form a chronological sequence: a chain of blocks, a blockchain.

Consensus mechanism

At the basis of the bitcoin blockchain is the verification and cryptographic sealing mechanism that joins blocks together, in Bitcoin this mechanism is a majority vote. In Bitcoin a large portion of the nodes engage in the verification process which consists in generating from the list of transactions and the information on the previous block an hash number smaller than a given difficulty level. Hashing is a function that maps between an input of any length into a number of a given length (256-bits for Bitcoin). The map is deterministic but small changes in the input cause arbitrary changes in the output, so that that reconstructing the input is unfeasible and the output number is uniquely related to the given input.
In order to have a qualified majority, the cryptographic sealing process is made computationally very intensive requiring to produce by chance an hash number smaller than a given value. The idea is to avoid false duplications of voters by forcing voters to demonstrate computational capacity, using Satoshi words: “one CPU one vote” [1]. The first node which solves this challenge (called proof of work) gets a rewards in Bitcoin, and this is the mechanism through which new Bitcoins are generated (mining).

The cost of the proof of work

Bitcoin proof of work is very costly. Currently miners across the world are generating several billions of billion (10^{18}) hashes every second [2]. Hashing is a relatively efficient operation, however it can be estimated that, with current hardware, the computation of a billion of hashes consumes, with state-of-the-art technology, between 0.1 to 1 Joule of energy see Table.1. This implies that currently about a billion Watts are consumed globally every second (1GW/sec) to produce a valid proof of work for Bitcoin. Electricity prices changes across the world and prices depend on many factors, however we can estimate that this amount of energy could accounts for around $50,000 per hour.

Hardware	Hash rate	Energy Consumption
Central processing unit CPU	0.1 GH/s	2000 J/GH
Graphics processing unit GPU	0.5 GH/s	500 J/GH
Field-programmable gate array FPGA	10 GH/s	50 J/GH
Application-specific integrated circuit ASIC	10,000 GH/s	0.5 J/GH

Table 1 Estimated hash rates and associated energy consumption for various kinds of hardware for Bitcoin mining. CPUs and GPUs are no longer used. Data are inferred form various sources, mainly specifications from hardware producers.

Considering that the system is currently processing less than 10,000 transactions per hours, this results in a cost in excess of $5 per transaction. The cost is not paid by the users but by the miners that get rewarded with the accreditation of newly emitted Bitcoins rewarding the first miner that gets a small enough hash. Presently this remuneration to the fastest miner is 25 Bitcoins corresponding to around $15,000 at current change. According to the previous estimate the miners community consumes every ten minutes an average of about $50,000/6 = $8,333 in electricity to produce a block and gets about $15,000 in remuneration that makes the operation quite profitable even considering the hardware and infrastructure cost. Interestingly the remuneration will be shortly halved to 12.5 Bitcoins leaving very small margins for profit accordingly with the above estimations.
The overall mining electricity bill for a year of Bitcoin mining sum up to over $400 millions which is a large amount and, somehow, a big waste. On the other hand, proof of work is the mechanism that keeps the blockchain pure making an entire community competing to verify validity of transactions and making attacks costly. The question I address in this note is whether this cost is justified.

The fair cost of the proof of work

How much Bicoin proof of work should cost? In my perspective, at equilibrium, the cost of proof of work should be such to make a double spending attack too expensive to be profitably carried over. Within this principle it is relatively straightforward to estimate the fair cost of the proof of work under an -ideal- equilibrium assumption.
Let us consider an attacker that owns some Bitcoin amount and wants to artificially multiply it by spending the same Bitcoin with several different users. This is a double spend attack. A greedy attacker will try to double spend the largest amount of Bitcoin possible, but this is limited to the amount normally exchanged within a block which currently is around $1 million. A transaction involving a substantially larger sum than the usual total value of transactions in a block will capture unwanted attention from the network. This limits the double spending amount to about $1 million. Of course, the duplication can be repeated several times both in parallel or serially but, as we shall see shortly, this does not affect the outcomes of the present computation. So the attacker has a potential gain of some fraction of $1 million. To be successful the attacker must make sure that both the duplicated transactions are validated and this requires to generate a fork with two blocks being attached to the previous block. If the attacker has enough computing power she can generate two valid hashes to seals the two blocks giving the false impression that both transactions have been verified. However, for a final settlement of the transaction it is presently considered that one should wait six new blocks to be

attached to the chain to make the transaction statistically unlikely to be reverted. The attacker should therefore use her computing power to generate six valid hashes before the double spent transaction might be considered settled. Note that only one of the two forks (the shortest) must be artificially validated by the attacker, the other will be considered valid by the system and can be let to propagate by the other miners; or the attacker can propagated it as well but she will also get compensated by the mining reward. Of course, it is quite unrealistic to assume that nobody notices the propagating fork for such a long time, but let's keep this as a working hypothesis. The artificial propagation of the fork has a cost that is the cost of the proof of work times six. The attacker will make profits if this cost is inferior to the gain. In summary we have a very simple breakeven point:

$$\begin{matrix} equilibrium\ fair\ cost\ of \\ proof\ of\ work\ per\ block \end{matrix} = \frac{duplicated\ fraction\ of\ the\ value\ of\ a\ block}{number\ of\ blocks\ required\ for\ settlement}$$

with the current values, and to make calculations clean, we can assume that the attacker duplicates 60% of the typical value of a block, double spending therefore $600,000. Requiring 6 blocks for settlement this yields to the following estimate for what should be the fair cost of the proof of work per block at equilibrium:

$$equilibrium\ fair\ cost\ of\ proof\ of\ work\ per\ block \approx \$100{,}000\ .$$

Clearly this computation over-estimates this cost because to be unnoticed that attack should be preformed on a smaller fraction of the block value and it is highly unlikely that a long forking can propagate for over one hour with all blocks validated by the same miner without anyone noticing that something unusual is happening. It is therefore reasonable to consider that 10% of the above cost is a sufficient deterrent to attackers. This is indeed the order of magnitude of the present electricity cost for the proof of work in Bitcoin.

We can therefore conclude that the current cost for Bitcoin proof of work is large, wasteful, but necessary. Reductions in such costs can be operated by increasing the number of blocks required for settlement or by automatically detecting and blocking forking at early stages. On the other hand, attacker can also reduce costs by stealing electricity or hacking mining farms.

Can a less expensive mechanism of qualified majority be implemented?
Blockchains can be constructed through several other mechanisms that do not require computationally intensive proof of work. Indeed the proof of work is a mechanism introduced to produce qualified voters in a system of anonymous untrustful parties. Any mechanism that can verify identity of the 'voters' or that can in any other way avoid uncontrolled duplications of the voters can reduce or eliminate completely the cost and even the need of a proof of work. However, these other mechanisms must relax also some other properties such as anonymity, openness or equalitarian distributed verification.

[1] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf
[2] See https://blockchain.info/stats