Bitcoin.

The time had finally come for me to really understand it. I started by researching blockchain, and then started in on Bitcoin. It always seemed a bit fishy to me, something never sat right and so I avoided it. Until now.

Blockchain is an interesting technology, seeming to democratize file storage and reduce system vulnerability to hacks and other cyber attacks. And it's supposed to be very anonymous, at least in terms of Bitcoin. The first site I researched made blockchain sound like a fortress of privacy impenetrable to attack and manipulation. But what little I knew of Bitcoin always had me doubtful, knowing all I do about banking, finance, and monetary theory.

Like mining bitcoins. It can only be done with a computer devoted solely to doing the complex calculations to maintain the blockchain, and then the miner is rewarded. This automatically gives an advantage to people with the means to devote farms of computers to doing nothing but mining bitcoins, not terribly fair nor democratic. Money creation in bitcoin is not controlled by the needs of government, it is inflexible and therefore cannot expand and contract with the needs of the economy. Bitcoin miners become the new bankers, extracting a form of "interest" for doing the "mining". Which they don't do, their computers do, they just need money to buy such a computer.

As I researched further I found there are of course scams and imbalances. Massive farms can dominate the network and start dictating the flow of information. A few years ago a company got 51% of the network, and currently two Chinese companies control over 50%. When a nation notorious for control over commercial enterprise starts getting control over a global currency there is a BIG problem. There are other tricks too, to ensure your computer gets ahead in calculating the next few blocks.

It was also interesting to find bitcoin is quite political, beloved by Libertarians for its anonymity and supposed democratization of money. It has a darker side to that anonymity, criminals have been trading in bitcoins to keep their transactions secret.

But now it has been revealed that bitcoins can be traced back to an IP address! So when push comes to shove it's not as anonymous as everyone thinks and criminals are being busted. Not to mention the records of bitcoin in blockchain means every single bitcoin can be traced to its original miner.

Bitcoin mining is also an incredible waste of resources. The computers necessary to mine bitcoins are expensive and run hot, and companies are devoting massive amounts of hardware and energy into "mining" a digital currency. Seems a lot of that could be better spent doing something productive.

Add to this that it seems the blockchain is hitting limitations due to its increasing size, and that mining for new bitcoins takes more and more computational power as the chain gets longer, and soon bitcoin may have hit its maximum output.

In the end, as far as a monetary instrument, bitcoin fails on a number of levels. First and foremost, its supply cannot be adjusted for the needs of the economy, there is no way to use some of the stabilizers of monetary policy the government uses to ensure a stable currency and manageable inflation. Second, it is unfairly created by people with the resources to buy and power a computer designed solely for bitcoin mining, it has no other purpose. Lastly, it is vulnerable to attack and susceptible to manipulation. Hackers or powerful companies cannot easily hack or take control of our money supply or bank records currently, while bitcoin, especially being less regulated, is open for taking advantage.

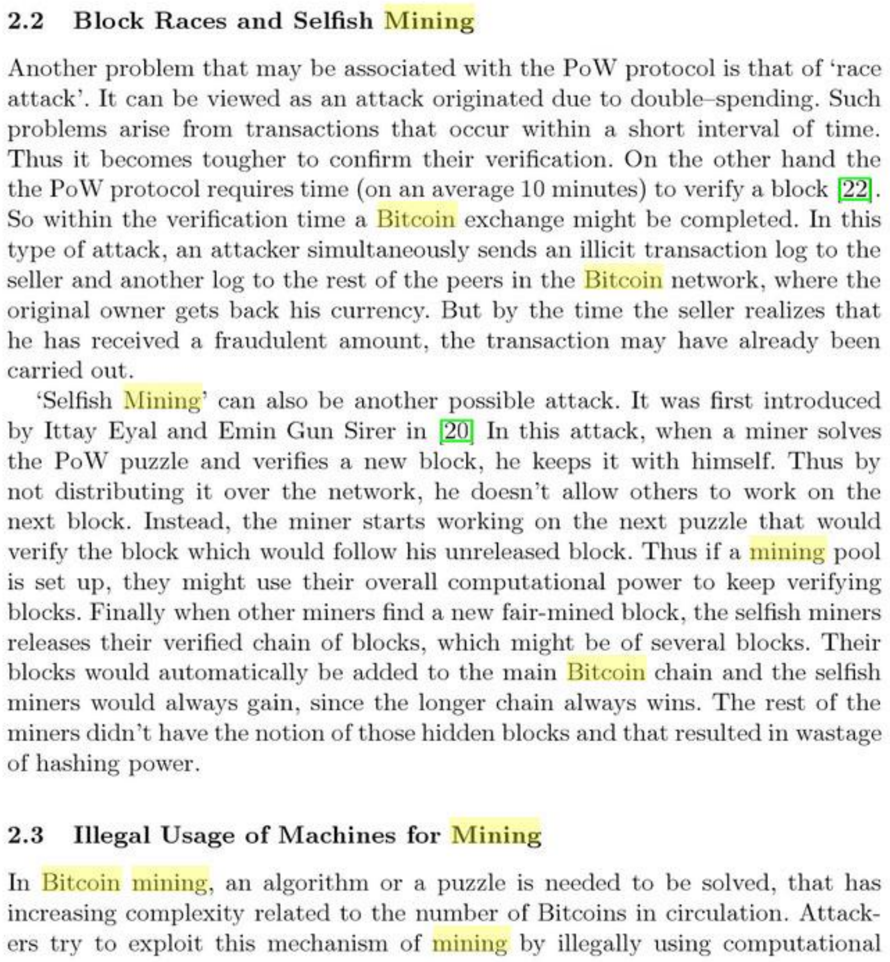
http://www.forbes.com/sites/jasonbloomberg/2016/01/18/something-rotten-in-the-state-of-bitcoin/#389dbca94650

https://books.google.ca/books?id=AqyvBQAAQBAJ&pg=PA187&lpg=PA187&dq=bitcoin+mining+unfair+competition&source=bl&ots=Xu0xuYGCIh&sig=t7HHryBPvYNFUPrsRcwAFY0Du1o&hl=en&sa=X&ved=0ahUKEwjhhsutoOjQAhVS-2MKHcGyCQwQ6AEIKTAB#v=onepage&q=bitcoin%20mining%20unfair%20competition&f=false

http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin

By Adam Smith

adam8mith@gmail.com



2.2 Block Races and Selfish Mining

Another problem that may be associated with the PoW protocol is that of 'race attack'. It can be viewed as an attack originated due to double–spending. Such problems arise from transactions that occur within a short interval of time. Thus it becomes tougher to confirm their verification. On the other hand the the PoW protocol requires time (on an average 10 minutes) to verify a block [22]. So within the verification time a Bitcoin exchange might be completed. In this type of attack, an attacker simultaneously sends an illicit transaction log to the seller and another log to the rest of the peers in the Bitcoin network, where the original owner gets back his currency. But by the time the seller realizes that he has received a fraudulent amount, the transaction may have already been carried out.

'Selfish Mining' can also be another possible attack. It was first introduced by Ittay Eyal and Emin Gun Sirer in [20] In this attack, when a miner solves the PoW puzzle and verifies a new block, he keeps it with himself. Thus by not distributing it over the network, he doesn't allow others to work on the next block. Instead, the miner starts working on the next puzzle that would verify the block which would follow his unreleased block. Thus if a mining pool is set up, they might use their overall computational power to keep verifying blocks. Finally when other miners find a new fair-mined block, the selfish miners releases their verified chain of blocks, which might be of several blocks. Their blocks would automatically be added to the main Bitcoin chain and the selfish miners would always gain, since the longer chain always wins. The rest of the miners didn't have the notion of those hidden blocks and that resulted in wastage of hashing power.

2.3 Illegal Usage of Machines for Mining

In Bitcoin mining, an algorithm or a puzzle is needed to be solved, that has increasing complexity related to the number of Bitcoins in circulation. Attackers try to exploit this mechanism of mining by illegally using computational

2.1 Rich Gets Richer, Poor Gets Poorer

Here we identify, how due to the existing protocol, there is an unfair competition among the miners. Bitcoin network purely relies on trustless consensus. Thus if a situation arises when a mining pool controls majority of the voting power, then it could cause havoc.

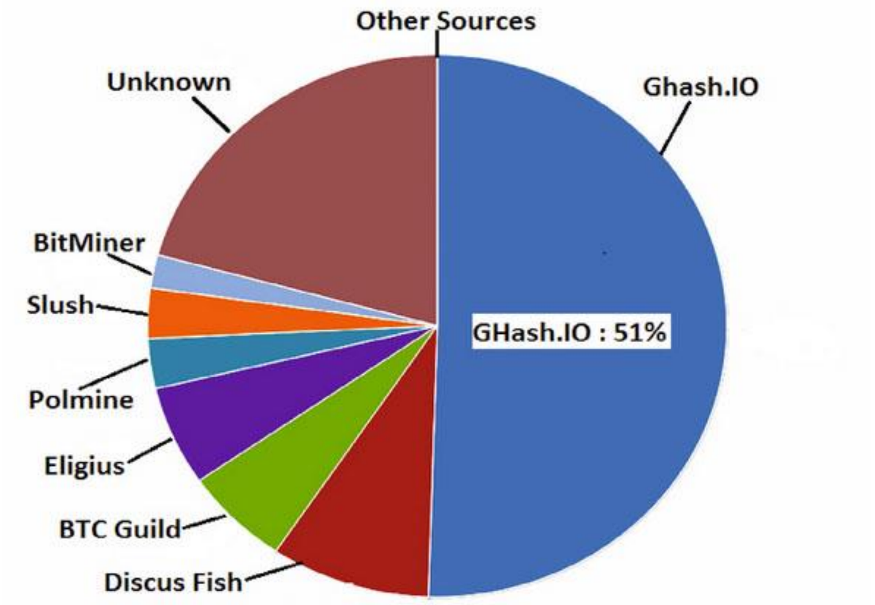


Fig. 1. GHash.io mining pool controlling about 51% of the total processing power (from [18])

A group of miners having 'rich' computational resource may set up a mining pool in such a way that it may control more than 50% of the network's computing power. In such a case that mining pool has the liberty to either modify the ordering or exclude the occurrence of transactions by launching a 51% attack [24]. With the combined mining power, the pool may indulge in double spending by simply reversing transactions that they send. Thus having the required computational power, the pool may be able to validate series of blocks in the block chain by just unscrambling the encrypted series of numbers attached to every Bitcoin transaction. It may also prevent other valid transactions from being confirmed or reject every block found by competing miners. They cannot directly affect the BTCs stored in the user wallets but they would have the power to make certain addresses unusable. And that allows them to impose any mining fee they like. The mining pool keeps on earning maximum profit and thus the use of the term 'Rich gets richer' sounds appropriate.

On 14^{th} June, 2014, a particular mining pool, namely GHash.io [12,18], was able to take control of 51% of Bitcoins processing power, thus extracting the maximum amount of profit for their work. Figure 1 shows the amount of Bitcoin processing power held by each major mining pool on 14^{th} June, 2014. The 'Unknown' group represents the individual users who are not associated with any mining pools, while others, for example, BitMinter, Eligius etc, are different mining pools associated with solving the PoW puzzle. Thus, it can be easily seen that the pools dominate the process of mining.