Bitcoins: Made in China

Tim Swanson

Revised: May 11, 2014

Abstract: The discussion over the actual costs of maintaining a decentralized seigniorage network is a new area of research. In practice it appears that the logistical cost of operating the Bitcoin network rises linearly with its total value. More efficient mining gear does not reduce energy use of the Bitcoin network. It only raises the network difficulty. The proof-of-work method used to mitigate rogue attacks, must expend real work, which means it must consume energy. Consequently, the price of bitcoin reflects its demand which in turn incentivizes hardness, which reflects how much work goes into the proof-of-work scheme, which directly converts into how much energy is being expended.

Moses Lake, Northern Europe, Canada and now China. What do these geographic regions have in common? Relatively cheap electrical costs and an environment that is increasingly conducive for acting as a natural exergetic heat reservoir. In the case of China, the issue is more complex because mining is incentivized by subsidized coal power plants – that is to say, the actual costs of operating a mining pool in China are externalized by taxpayers in China.

Why are pools moving to these regions in the first place?

Mining most proof-of-work-based (PoW) cryptocurrencies (such as bitcoin and litecoin) is an increasingly energy intensive operation; the fact that all seigniorage gets burned up from hashing is the essence of crypto scarcity.[1] Nobody has an incentive to produce additional units of the token. Some commentators seems to think that it is an inherently beneficial phenomenon, that the market cap is greater than the cost of minting the coin. But the fact that MV> MC (marginal value is greater than the marginal cost) is the reason policy makers typically argue that money needs to be a state sanctioned monopoly.[2] In contrast, private seigniorage incentivizes the production of money until MV=MC (note: this is not an endorsement of either but serves as a historical explanation).[3]

Because outputs (blocks) are fixed, the amount of inputs will vary according to profitability forecasts.[4] That is to say, economically rational miners will direct their depreciating capital goods towards the most profitable activity, comparing the expected mining award to the variable operating costs (electricity, mostly).[5]

As noted in a working paper last month, the price level of tokens such as bitcoin are determined by market participants based on supply and demand.[6] The value of a token serves as a signaling mechanism for miners to either partake in the effort to hash blocks or to redirect their effort towards other more profitable tokens relative to the difficulty rating.

In addition, there is one variable cost that all large scale mining operations must take into account: electrical costs. For the same reason that cloud computing providers such as Facebook, Microsoft and Google have scoured the globe for prime locations based on reliable always-on electricity, settling down in areas like Prineville, Oregon or Quincy, Washington (whose facilities are powered by the Wanapum Dam) 98% - 99% of the operating costs for large professionally run mining pools boils down to electricity and cooling costs.[7]

Andrew Poelstra recently published a paper regarding ASICs and decentralization. In one passage he notes that:[8]

> [D]edicated hardware brings us closer to the thermodynamic limit, and is therefore eventually a good thing for mining decentralization. Also, because ASIC's produce more hashes for the same amount of energy, they produce stronger proofs-of-work with proportionally less environmental impact.

This is false as it is conflating network difficulty with probability of successful attack. Only capital burned influences the latter.[9] The only thing that would cause less environmental impact without affecting security is an increase in the price of electricity which is discussed later. Even at the thermodynamic limit, network difficulty will still fluctuate with the price of electricity and the price of bitcoin. Thus, the difficulty can change but capital spent hashing remains the same (or vice versa). Furthermore, centralization is incentivized due to network propagation constraints, an issue that Jonathan Levin dubs "Hash War 2.0" – and as a consequence peering agreements now exist among the larger pools, to propagate the blocks faster by removing all of the unnecessary hops and overhead a decentralized network creates.[10][11]

China

If you have never lived or worked in China then you are likely unaware of the all-important concept of *guanxi* (social connections). While the PBOC has alluded to the fact that it does not want China to lead the globe in either Bitcoin volume or regulatory governance, *guanxi* – or lack thereof – is what likely doomed the exchanges.[12] Exchange operators did not have the right *guanxi* with the right government officials. Despite the seemingly financial success of several exchanges, they still could not overcome the political issues as it relates to personal connections; thus the effort needed to obtain the correct *guanxi* for survival was apparently beyond the financial incentives of operating an exchange.[13]

In contrast, miners in China have taken a different approach and have found the right people to partner with (at least for the moment). One such team is working within the current system and has access to a double digit megawatt power facility, which when coupled together with 3rd party chips, the production costs of which are less than $2.00 / gigahash.

There are at least three other funded teams in China with 3rd party chips (e.g., nangua, "fried cat") with access to similar energy sources. Some of these have little experience operating and optimizing their own internal networks (to efficiently propagate blocks in and out of their hashing stations). Others are more malevolent, using denial-of-service (DoS) attacks to reduce their competition. The longer you are offline, the less time you have to hash for a target value (nonces) preventing you from receiving block rewards which currently account for roughly 99.69% of the miner's income.[14] Yet it should be noted that since mining pool began to aggregate in late 2010 (with Slush) and early 2011, DoS attacks have occurred on a global level and is not merely a Chinese phenomenon.

Throwing a wrench into this issue is the Chinese internet itself because there are essentially just two state-owned providers, China Telecom and China Unicom and they are not exactly best friends and the

Great Firewall (金盾工程) itself could potentially affect network block propagation.[15]

Despite these issues, the major draw of China continues to be the electrical costs. This has been the case for several years as the average national rates in both India and China have hovered at approximately 8 cents / kWh which is significantly lower than others such as Denmark at 41 cents / kWh.[16] While Moses Lake in Washington State has made headlines for its 1.7 cents / kWh rates which have attracted numerous pools, in China, some commercial operators can get electricity for 3 cents / kWh.[17] And if you have the right connections (*guanxi*), you can get it essentially for free. Now, of course it is not free. Nothing is free. Someone bears this cost and that cost is borne by Chinese taxpayers and the environment because these energy generating facilities are almost all coal-powered power plants.[18] While pollution may seem to be a non-issue to most redditors and North American bitcoin holders, these subsidies act in much of the same way as botnets did two years ago, externalizing the true costs of the network, distorting the marketplace by incentivizing activity (mining) that would not exist in an actual open market. Or in other words, *ex*-China, mining operations would likely still be taking place in other regions and the collective network hashrate and therefore difficulty rating would be lower enabling other marginal miners to still compete. Outside participants cannot unilaterally blame the Chinese for this as other similar distortions existed in the past, largely from botnets operated by various malware authors (especially in Eastern Europe and the former Soviet Union) did and continue to externalize the costs of hashing.[19]

Furthermore you do not have to be Zhang Xin (a real-estate magnate in Beijing) to necessarily benefit from this type of private-public arrangement: other less connected mining operations in China still have access to relatively cheap systems, that once tweaked can operate at less than $2 / gigahash. For these sub-10% hasher pools, because virtually all ASIC chips are now being manufactured in Taiwan, costs come down to volume size and chip cost which are concluded via negotiations.

Cloud hashing

One particular enterprising Chinese individual has figured out how to do a shanzhai (山寨) form of cloud hashing. While specific commercial numbers are proprietary, the rate comes to less than $3 per ghash.

In terms of the global supply chain, 90% of ASIC chips are made in Taiwan (TSMC), others go through Singapore (Global Foundries), and the remaining parts (PCB, SMT, power, fans, integration) almost all goes through Shenzhen.[20] Or it will have to in the near future. One estimate explained to me by a mining operator in China is that allegedly more than 25% of all mining may be going on in China and likely more could come online due to these incentives.[21]

For comparison, CEX.io (which currently operates the largest mining pool, GHash.io) is around $3 per ghash and Cloudhashing (in Austin) is around $7-$8 per ghash. Even KnC, which is buildings its own 10 MW powerplant in Sweden will unlikely be able to compete long-term at these rates unless it continues its current business practice of using customer-purchased hardware first before shipping later.[22] In addition, even with Moses Lake competitive rates of 1.7 cents, operators in the US (and Sweden) have to deal with a variety of tax and environmental issues which at this time do not exist in China.

The same source estimates that all told there are at least 2 Western companies and another 5 Chinese companies developing and deploying mining pools in China. In addition, there are also cloned and counterfeit chips running in the wild which can impact the performance of pools (i.e., burn out boards due to fraud). Thus in his estimation, given sluggish prices in bitcoin and rapid growth rate of difficulty this could lead to an unsustainable situation in the medium-term. Or in his words, “irrational exuberance and excitement are being replaced by cold math and a few bankruptcies.” One such bankruptcy was Alydian.[23]

Furthermore, historically the most important factor to a miner's profitability is fast access to the latest chips. Actually, according to professional miners, the most important factor is access to a *working* system with the fastest chip. Because these chips draw so much power, it is hard to produce stable, working systems. For instance, Hashfast, purportedly has the best chip in the world, but have failed to ship working systems due in part to power issues.[24] A few days of hashing with the newest ASIC chips, when you were hashing at magnitudes faster than the competition, will more than cover the electricity costs for the lifetime of the chip.[25] However most hardware becomes obsolete in a matter of months and the turnover within this segment inevitably leads to incentives to create other profitable altcoins utilizing the same hardware. In the event of a block reward halving, this could lead to an exodus of miners looking to profitably hash for more profitable rewards. This is an issue that will likely need to be researched more within the next two years.

And while capital costs still arguably play the most important role in determining whether marginal participants should choose to join the mining effort in the first place, there is a major reason why large mining facilities have not set up in Denmark or Germany. In contrast, in 2009 Google purchased an old paper mill and set up a data center facility in Hamina, Finland due in large part to its energy infrastructure which was ideal for cooling purposes.[26] Similarly, Bitfury also purchased an old bank, also in Hamina, Finland to capitalize off the geographic cooling advantages.[27]

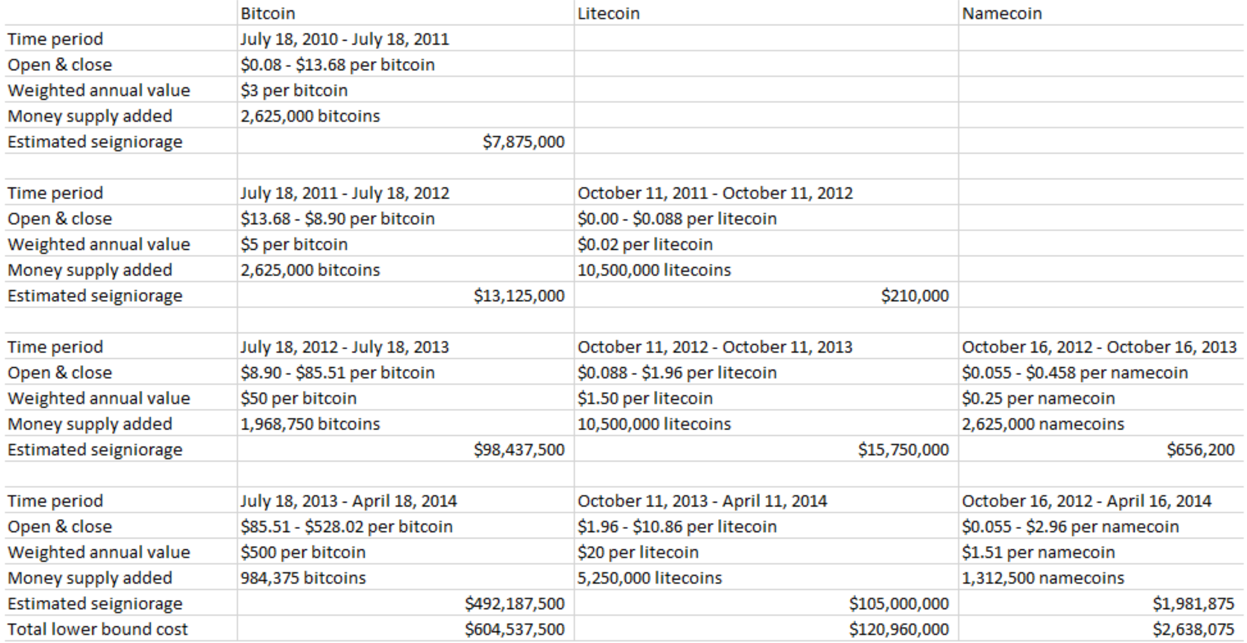
And barring changes in the incentivization framework, China will likely be “exporting” coins very soon.

A million dollar token

Of all the feedback I received from my previous paper, the one that some Bitcoin adopters have a tough time reconciling is the seigniorage of the network. That is to say, *ceteris paribus*, the cost of creating a new bitcoin (capital depreciation, electricity, property lease), will eventually equal its market exchange value on average.[28]

Below is a chart I used to estimate the historical lowerbound seigniorage.[29]

Figure 1: Lowerbound seigniorage estimate



	Bitcoin	Litecoin	Namecoin
Time period	July 18, 2010 - July 18, 2011		
Open & close	$0.08 - $13.68 per bitcoin		
Weighted annual value	$3 per bitcoin		
Money supply added	2,625,000 bitcoins		
Estimated seigniorage	$7,875,000		
Time period	July 18, 2011 - July 18, 2012	October 11, 2011 - October 11, 2012	
Open & close	$13.68 - $8.90 per bitcoin	$0.00 - $0.088 per litecoin	
Weighted annual value	$5 per bitcoin	$0.02 per litecoin	
Money supply added	2,625,000 bitcoins	10,500,000 litecoins	
Estimated seigniorage	$13,125,000	$210,000	
Time period	July 18, 2012 - July 18, 2013	October 11, 2012 - October 11, 2013	October 16, 2012 - October 16, 2013
Open & close	$8.90 - $85.51 per bitcoin	$0.088 - $1.96 per litecoin	$0.055 - $0.458 per namecoin
Weighted annual value	$50 per bitcoin	$1.50 per litecoin	$0.25 per namecoin
Money supply added	1,968,750 bitcoins	10,500,000 litecoins	2,625,000 namecoins
Estimated seigniorage	$98,437,500	$15,750,000	$656,200
Time period	July 18, 2013 - April 18, 2014	October 11, 2013 - April 11, 2014	October 16, 2012 - April 16, 2014
Open & close	$85.51 - $528.02 per bitcoin	$1.96 - $10.86 per litecoin	$0.055 - $2.96 per namecoin
Weighted annual value	$500 per bitcoin	$20 per litecoin	$1.51 per namecoin
Money supply added	984,375 bitcoins	5,250,000 litecoins	1,312,500 namecoins
Estimated seigniorage	$492,187,500	$105,000,000	$1,981,875
Total lower bound cost	$604,537,500	$120,960,000	$2,638,075

Pardon the pun, but rather than rehashing the explanation used in the paper, I will focus on one particular hypothetical: a million dollar bitcoin.

While there are at least five exceptions, as noted above, if a token is worth $1 then no more than $1 worth of operating costs will be used to extract that rent by an economically rational miner (*homo economicus*).[30] Similarly, if a token is worth $1000, then mining pools will only operate their hashing systems at just below breakeven (otherwise they could simply turn off the machines and allow other mining pools to create seigniorage). In practice, many miners do not do this as many believe that any operating loss would eventually be recouped through token appreciation. Since this is the case, Bob effectively buys future network security on that price expectation creating temporary additional hashrate overhang – additional deadweight loss which is anything above 51% of "honest" network hashrate. However unless a survey is done of miners operating at losses, the additional extra operating costs are likely difficult to estimate (hence the lowerbound estimate).

One notable comment I did receive was the following, "that power consumption is already as high as it will ever need to be that is, a million dollar bitcoin will not cost more to process and transactions add nothing to the costs the cost of transactions will go down as volume increases."

This is false. If each token is worth a million dollars then why would not more people enter the market if you can produce one for $500? What would happen in reality is that if the token level increased to $10,000 then $100,000 and $1 million the same signaling mechanism tells miners when to operate and when to turn off their machines. If a token reached a price level of $1 million today, everyone on the planet would likely try to hash blocks with every available computing resource until that breakeven equilibrium was reached (e.g., once operating costs reached token rents). Whereupon, marginal mining participants would once again become purged from the market place as professionalized datacenters capable of profitably scaling are built, merged and acquired. Being purged does not affect the price of the token but it does lead to centralization; as token prices increase only those miners capable of *profitably* operating at the new level will be able to compete on seigniorage.

In other words, the logistical cost of running Bitcoin rises linearly with its total value.[31] More efficient mining gear (such as ASICs) does not reduce energy use of the Bitcoin network. It only raises the network difficulty. The proof-of-work method must expend real work, which means it must consume energy. Therefore, the price of bitcoin reflects its demand which incentivizes hardness, which reflects how much work goes into the proof-of-work scheme, which directly converts into how much energy is being expended. The end result is that at this level, at $1 million per token, a mining facility would need to expend a similar amount of energy (since ~98% of operating costs are related to electricity). There are very few locations on the globe capable of generating both that kind of electrical production.[32] For instance, in 2016 when block rewards halve (which creates another serious hurdle detailed in another paper last month),[33] if token values were $1 million then mining facilities would essentially need to expend $12.5 million in electricity every 10 minutes or $1.8 billion in electricity each day.[34]

Again, the reason why is because, token values signal to miners when to operate and when to shift their labor elsewhere.

This issue was discussed in a paper published in September 2013 by Michael Taylor who studied the evolution of chip designs used in bitcoin mining. He noted that:[35]

> However, unlike in the "race to ASIC" days, the cost/performance difference of future generations of hardware will not be great enough to quickly obsolete the last generation. Rather, it will be energy costs that are likely to dictate which ASIC will be the most profitable. This is especially true in the case where there is a supply glut of chips of a given generation, such as is likely to happen in the next year, as the NREs have been paid, and the three groups are simply paying wafer costs now. One can imagine Bitcoin users dumping their chips, and groups with access to cheap energy buying them for almost free and putting them back to use for mining. Of course, there are two factors that dictate energy costs -- the cost of energy, and the energy consumption of the part. The parties with the greatest advantage will be those that have cheaper access to large quantities of energy and already have their mining hardware paid off when returns on hashing were higher. Cheaper energy allows these parties to pay off their newly acquired hardware over longer cycles, and to continue to operate even when $ per Gh/s, as shown in Figure 3, drops precipitously low. Others may have an advantage because they have more energy efficient hardware designs.

One common conjecture is whether or not solar power or nuclear power could change this. Unfortunately, this is purely a matter of expending energy and not about what exactly is generating it. Even if you were to replace all the coal powered plants in China (or elsewhere for that matter) with renewable energy, mining facilities would still consume and expend electricity at roughly the same value as a token because MV=MC.[36]

Can distributed workloads create lower energy requirements?

No. Another interesting story in China is a Bitcoin start-up in Beijing that fleshed out a business proposal with a well-known telecommunication provider to integrate ASIC chips inside routers. At the time, the thought was this telecom company could sell the routers globally and users could receive a steady stream of income as routers are typically left on day and night. Ideally this would involve some kind of 70/30 split in which the start-up would receive 30% of the bitcoins generated and the customer would receive the other 70%. Yet the reality of developmental process illustrates how this is unprofitable. It takes between 3-9 months to design an ASIC from scratch and tape-out (3 months assumes double shifts). By the time an ASIC passes its verification process, tapes-out, goes through maskmaking, is shipped to the client, integrated into the router and shipped globally, the ASIC is no longer capable of profitably hashing. In other words, supply chain integration and logistical deployment will likely prevent the dream of everyone globally of having an ASIC processor on their smartphone *profitably* hashing away at block headers based on electrical consumption alone.

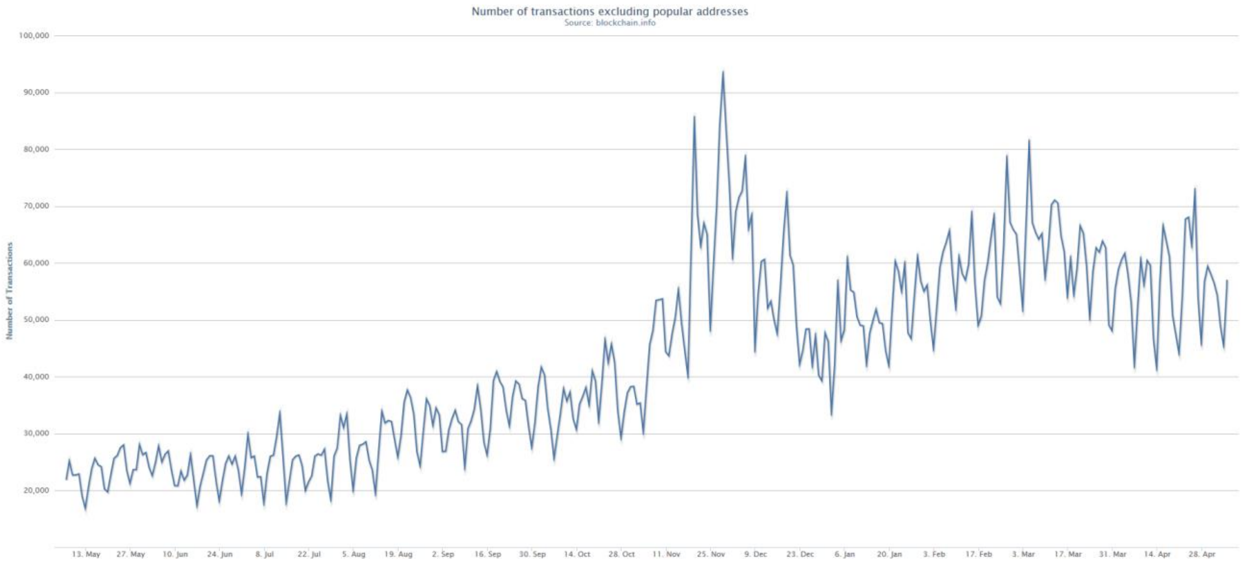
But what happens once the ultimate thermodynamic efficiencies of ASICs are reached, would that lead to any different geographical distribution?

No. Andrew Poelstra's paper on this subject attempts to broach this topic and comes to the conclusion that once the thermodynamics of a chip are reached, this would lead to decentralization. For the sake of argument, assume that someone like Nvidia, BFL or KnC creates a chip at the Planck length ($\ell_{P)}$.[37] However even at that level, a rational actor would not set up a large pool in San Francisco because of relatively high operating costs. Or in other words, even with the most efficient chip design, the sole competitive force would be electricity. If that is the case, then the chips would simply end up wherever the cheapest energy source is, potentially leading to centralization. While the issue as to the degree to which centralization is occurring is actively being discussed, this does not necessarily impede the networks current effectiveness, though it could lead to social engineering challenges.

And again, over the past 24 months mining equipment typically had a profitability window of roughly 3-5 months whereupon it would become obsolete by newer and better generations, but this "race" will soon be over. As a consequence a 10% improvement alone will likely not make investing into new mining hardware profitable. More precisely, a 10% improvement in mining hardware efficiency does not provide a competitive advantage over someone who has access to energy at half the cost.

Does it matter if people use the network as an actual payment platform?

I have written on this topic several times, the latest post of which delved into this particular graph from Blockchain.info: the number of transactions excluding the 100 most popular addresses (such as gambling sites like Satoshi Dice).[38]



What this means is that over the past 6 months, there has been essentially no new on-chain transactional volume. Despite the tens of thousands of merchants that BitPay and others have on-ramped, most users (or rather holders) of bitcoin are unwilling to actually spend it. Almost all of the additional activity occurs on the edges, in “trust-me” silos which defeats the purpose of having a blockchain. This is not to say that trusted solutions do not provide utility (in fact, they empirically do as shown by their continued popularity) however users of those services are essentially trading IOUs of an SQL entry.

What do other more qualified people have to say about it? I reached out to Jonathan Levin, co-founder of Coinometrics and a post-graduate student at Oxford. His explanation is thus:[39]

- Looking at some of the mining pools there are plenty of transactions that are used just to pay miners and also to conceal identities.
- There are also transactions used by exchanges and other large corporations every day for internal settlement and security. Every transaction that gets done through BitPay and the like will inevitably trigger multiple transactions for privacy protections and security
- Private individuals also move coins between wallets to ensure privacy and security of funds

His conclusion is that, "A lot of this creates price insensitive demand for transactions as it is not strictly economic activity."

This is the Kevin Costner problem: if you build it, will they come? So far the answer has been a muted no. Perhaps this will change as security and usability improves and more merchants and users adopt the technology yet the energy limitation could become a factor.

Aside from edge case security issues, even though historically 0.7 tx are conducted on average per second, perhaps one issue preventing wider spread usage of the Bitcoin network as a payment platform is the artificial 7 tx per second limitation and subsequent confirmation delay.[40] While there are hypothetical workarounds to the transactional limit such as Sergio Lerner’s proposed DECOR protocol – which when paired with GHOST can potentially reach 2,000 transactions per second, it is doubtful that this alone will on-board real-time gross settlement (RTGS) users because any technological benefit that Bitcoin is privy to, will likely benefit the competition as well.[41] For comparison, last fall, Visa reached 47,000 tx per second at the Gaithersburg IBM testing facility.[42]

In the future, merchant processors like BitPay could on-ramp every merchant on the globe and someone else could potentially even solve some of the network delay issues in Jonathan Levin’s upcoming research through the deployment and use of neutrino detectors.[43][44] Yet this is not to say that that increased transaction volume will necessarily require more energy usage. Even though transaction are packed into a block which is then processed and paid for almost entirely by seigniorage rewards which itself changes due to the fluctuation of token prices, the relationship between mining and volume is so far, a side note.

No one has to use the actual network (very few in fact do) for value to be burnt through heat processes.[45] In fact, over the next 6 years, transaction fees could rise substantially (to offset the diminished block rewards) and as a consequence bitcoins may be solely used as a store of value, transmitted intermittently. Yet the token value and the network costs to secure that token can and will still scale linearly.

Thus the energy limits are real and will likely put an upper bound to its ultimate size as described below.

Energy limits

The issues above are *dissimilar* to the claims that the internet will not be able to scale, this includes anachronistically hackneyed claims that the internet cannot do voice, quality voice, video or anything larger than a few kilobytes per second. Those were largely caused by immature software stacks and hardware constraints. In contrast, for the Bitcoin network (and other cryptocurrencies using a PoW mechanism), the built-in thermodynamic hurdle still remains. In the event that the token appreciates (which disincentivizes spending due to volatility and also incentivizes continued speculation and stockpiling), the network will cost as much as it is worth.[46]

Following the block reward halving in 2016, a million dollar token would hypothetically incentivize $656.2 billion in expended energy (exergy) per annum, or roughly the current GDP of Switzerland.[47] There is no way around the exergetic requirements (a process Fred Trotter dubs “malignant computation”), it is built into proof-of-work mechanisms and because of a type of *regulatory capture* (i.e., miners will only hash and protect code that is profitable to them) the PoW mechanism will likely never be switched to something less capital intensive like proof-of-stake.[48] Or in other words, while there may be a hypothetical scenario where Bitcoin could evolve to some more energy efficient block verification model, this is unlikely possibility because the miners will never agree to it. Furthermore the price is a lowerbound estimate due to exceptions like charitable donations of hashrate. And more precisely, these funds went to utility, energy and hardware companies and *not* back into the Bitcoin ecosystem, to fund its development.

The end result is a joke a friend in China told me last year when I was helping build Litecoin machines: that taken to an extreme, bitcoin mining (or litecoin mining for that matter) would eventually gravitate to facilities located in the Arctic Ocean, which acts as a natural heat reservoir and dissipater.[49] Peered together with microwave towers these pools would provide the financial backbone – to a network funded primarily through gambling revenue, the networks on-chain “killer app.”[50]

Incidentally, the Hamina site used by Google purportedly features, “underground tunnels running to the Baltic sea, which Google utilized to cool the facility’s servers. The company included the tunnels in the new data center design, utilizing pumps to push cold sea water from the Gulf of Finland into the facility’s cooling system.”[51] Another report notes that Google, “uses the sea to replace the chiller in its cooling system, collecting cool water from an inlet pipe located about 7.5 meters beneath the service of the Baltic Sea. The water than travels into the facility through large tunnels carved out of granite, and is used in a water-to-water heat exchanger.”[52]

In a twist, perhaps the Arctic Ocean joke will not be too far off the mark.

Limitations

Cal Abel, a statistical modeler, suggested that future research look specifically at the *time value of money* by doing a conventional internal rate of return (IRR) analysis of a miner.[53] According to him, "this will give you an idea of the cost of delaying the mining rig and its future obsolescence." This could be done by quantifying the cost expended for utilities and real-estate and converting this dollar figure into energy by using what he dubs an energy price index (EPI). This could potentially give a researcher a measure of the computational efficiency (hash/joule of primary energy). Or in his words, "There is some quantum limit to the the energy of a hash, which converts it into energy. This will give you the thermodynamic efficiency of bitcoin and allow you to measure transactions in terms of their ability to do work."

Among the largest limitations to this approach however is creating a mean, a weighted average for an ASIC-based actor. Since the process of mining is itself decentralized, finding out the location of the miners – and thereby estimating local energy costs as well as the marginal utility of money (because exchange rates and purchasing power varies) – can be obfuscated in a number of ways. Furthermore, not everyone is using the same set of hardware. In all likelihood, the network is being oversecured by individuals who are providing inefficient hashrate (e.g., operating at a loss) at the network with the future expectation that these token (or more precisely, UTXOs) will appreciate in value.

For instance, based on calculations provided by Dave Babbitt, if all miners were using a new "Minerscube" system, based on its theoretical hashrate, the Hoover Dam Equivalent (HDE) for wattage consumption of these would be 0.002 HDE.[54] In contrast, if miners were all using the original first batch of Avalon, based on current network hashrate this amounts to 0.133 HDE being consumed. Another way of looking at the same phenomenon are estimates by John Ratfcliff who based his on the net profit from the sale of bitcoins.[55] According to his estimates, the lowerbound is 0.25 HDE and the upperbound is 0.5 HDE.

Thus attempting to quantify the EPI will in practice require producing a range of estimates based on confidence values.

Conclusions

In discussing this issue with Robert Sams of Kryptonomics, he noted that, "Economic logic dictates that eventually all mining will become concentrated in certain areas due to electricity arbitrage, which defeats the whole point of proof-of-work (PoW). One subsequent prediction is that the main casualty of this will be the belief that mining should be an anonymous and permissionless activity."[56]

In practice, increased anonymity has not been the case as mining pool operators are now accessible to 3rd parties for a variety of reasons.[57] If PoW is to be workable in the long-run, miners will likely need to authenticate themselves to the network in some way – an issue actively being discussed by Mike Hearn over the past six months – with some decentralized vetting process acting as a gatekeeper and potentially denying some of these miners the right to mine.[58]

The environmental dimension and China specifically should be taken with perspective: it is (currently) not a leverage point in the global picture as the automobile itself as a class is a much larger polluter by many orders of magnitude. They were used for illustrative purposes: perhaps other regions like Mongolia or Saudi Arabia will replace China and Moses Lake in the future.[59] Furthermore, the backlash towards China in general related to bitcoin price levels is arguably unwarranted – if the purpose of a peer-to-peer decentralized electronic cash system is to enable and empower the underbanked, then developing countries like China should be embraced irrespective of token valuations.

One common hurdle due to the computational arms race that has arisen is that, proof-of-work scaling ends up moving beyond the reach of the intended hobbyist – moving away from "recreational mining."

Consequently, an unintended consequence is that capital accumulation and therefore mining operations end up in jurisdictions that have superior infrastructure and/or lower energy costs. That is to say, while the underbanked and unbanked are supposedly one of the oft cited use-cases for a decentralized electronic cash system, in practice the only way for those residents to participate today is to purchase tokens through an exchange, because they do not have access to capital for mining equipment or competitive energy sources. And in many cases, there are no reliable exchanges (or even ATMs) to buy from. But that is a topic for another paper.

Internal to cryptocurrency, mining centralization could be viewed as a negative externality and this centralization is being driven by what Sams identifies as large differentials in $/kWh.[60] From this discussion above the key takeaway is the $/ kWh factor which is the core dimension to mining concentration. Over the past two years the discussion has largely been centered on ASICs *qua* ASICs, which are not really an issue so long as no one entity has a monopoly on the chip design. Instead, $/kWh is the real driver of concentration and future research can be conducted to propose methods for how to deal with it.

Sams proposed the following situation in which the network would apply a different difficulty to different miners, as a function of the price they pay per kWh.[61] According to him, in their view, that would be a levelling and decentralizing force. However, in practice it can only be had by sacrificing the anonymity and permissionless properties of PoW. Even then, it is not clear how to implement this technically, but it could be an area of research because the handwriting is on the wall for the current model. What is happening – geographic arbitrage – should make that clear to other outside parties.

In terms of Andrew Poelstra's intriguing "thermodynamic limit" to mining, it is valid regarding the physics of the computation. But the economics of mining has gone the opposite direction, a sort of antithesis of the Second Law of Thermodynamics, in the words of Sams "control of mining operations converge to minimal entropy, a monopoly at the limit, where one party with the cheapest source of electricity ultimately controls the network. Heat spreads out, wealth concentrates."[62]

While the amount of energy consumed mining bitcoin will always be at least equal to the value of bitcoin produced this is not to say Bitcoin will fail as an experiment or as a store of value. Energy consumption in the long run is not necessarily a condition for success. And even though a relatively large amount of energy will be consumed while bitcoin "bootstraps itself" – it could decline. Future block halving's may actually end up reducing energy consumption rates if token prices do not rise in tandem.[63]

This topic will likely continue to fill numerous works in the future and should be looked at again in the coming months and years.

Acknowledgements

I would like to thank Cal Abel, Dave Babbitt, DC, Joseph Chow, Dan Forster, Philipp Gühring, Karl Holmqvist, Petri Kajander, Jonathan Levin, Andrew Poelstra, John Ratcliff, Bryan Vu, JW and Weiwu Zhang for their feedback and constructive criticism. Special thanks to Robert Sams for his numerous contributions throughout including significant portions of the concluding remarks.

Endnotes

[1] In the economic sense, a more accurate term is "traded," in the thermodynamic sense, nothing is destroyed. The exergy is more like "converted" from the thermodynamic viewpoint and the security is more like "traded" from the economic viewpoint.
[2] My thanks to Robert Sams of Cryptonomics for pointing this out.
[3] This issue dovetails into more complex discussions involving legal tender laws. Enacting monetary and fiscal policies by fiat has its own series of drawbacks (i.e., interest rates can arbitrarily be set by committee, but these can create time-preference distortions).
[4] For more about the economic inputs and outputs of mining on the Bitcoin network see, Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms by David Evans
[5] Amortized costs, by definition, are fixed and are therefore irrelevant to the decision to turn the machine on or off (those costs are only considered when deciding to invest in a new machine or not). Before setting up, professional miners will look at calculations for recouping their operating costs and upfront investments (such as hardware, physical plant and real estate).
[6] More specifically, bitcoin price is a function of supply, current demand in the economy, and future demand discounted to present value. See Learning from Bitcoin's past to improve its future by Tim Swanson
[7] Facebook Has Spent $210 Million on Oregon Data Center from *Data Center Knowledge* and Large Crack Found in Dam Supporting Quincy Data Center Cluster from *Data Center Knowledge*
[8] ASICs and Decentralization FAQ by Andrew Poelstra
[9] Or in other words, network difficulty is an arbitrary metric in and of itself. The probability of success refers to an attacker amassing more than 50% of the hashrate (e.g., 51% attack). You could burn enormous amounts of electricity with CPUs yet fail to generate any meaningful hashrate to attack the network. An ASIC may be able to generate more hashrate than a single CPU but quantity is not the same as quality. One way to measure the quality of the security for a decentralized network is whether or not there are an increasing or decreasing amount of nodes. In this case, centralization of the hashrate has taken place leading to a qualitatively less secure network (due to less decentralization).
[10] [ANN] High-speed Bitcoin Relay Network by Matt Corallo and The Future of Bitcoin: Corporate Mines and Network Peering? from *Data Center Knowledge*
[11] Personal correspondence, April 8, 2014. See also, Bitcoin Hurdles: the Public Goods Costs of Securing a Decentralized Seigniorage Network which Incentivizes Alternatives and Centralization and Bitcoin Block Propagation Speeds by Ittay Eyal and Emin Sirer
[12] Fairweather fans in bitcoinland disowning China
[13] Chinese Banks don't know how to act appropriately, because Bitcoin is too tiny by Weiwu Zhang
[14] As of May 6, 2014, according to Blockchain.info, miners received 0.31% of their revenue from transactions, the remaining balance came in the form of block rewards (seigniorage).
[15] Its official name is the Golden Shield Project
[16] See Determining Electrical Cost of Bitcoin Mining by Ruben Alexander and The Average Price of Electricity, Country by Country from The Energy Collective
[17] Ignoring cooling requirements and management overhead another infrastructure issue is that this build-out needs approximately a $100,000 transformer for every 1 megawatt. See also Bitcoin Miner Taps Dad's Power Plant in Virtual-Money Hunt: Tech from *Bloomberg* and The Other Bitcoin Power Struggle from *Businessweek*
[18] More than two-thirds of China's energy needs are met through coal-powered power plants. The World Coal Association estimates that 79% of China's electrical generation capacity comes from coal.
[19] The ZeroAccess Botnet – Mining and Fraud for Massive Financial Gain by James Wyke and Botcoin: Monetizing Stolen Cycles by Huang *et. al.* Another paper from the same team discusses the differences between "light" and "dark" mining pools, Poster: Botcoin – Bitcoin-Mining by Botnets
[20] SMT stands for surface-mount technology.
[21] F2Pool, also known as Discus Fish, operates one of the largest known pools in China and the world
[22] KNC attracted unwanted attention in 2014 when following the release of pictures of its mining facility, it was discovered that customer investors ("investormers") learned how KNC was operating at their expense: KNC received funds from customers, built the systems and then used the machines first for an undisclosed amount of

time, generating bitcoins and increasing the difficulty rate at the expense of the customer. This would be akin to the primary dealer in open-market operations which receive US Treasury funds first before everyone else. See Bitcoin Miners Building 10 Megawatt Data Center in Sweden from *Data Center Knowledge*

[23] A Non-Outsourceable Puzzle to Prevent Hosted Mining by Andrew Miller and CoinLab's Alydian files for bankruptcy and reveals debt of over $3.6m from *CoinDesk*

[24] Embattled CEO of Bitcoin miner firm: "We are as poor as church mice" from *ArsTechnica*

[25] Those gains in magnitude are no longer occurring. Jeff Garzick was one of the first users to receive the first batch of Avalon ASICs in January 2013. He recouped the cost of the order in less than a month. Once upon a time in China, a package shipped by Jeff Garzik, The First Bitcoin ASICs are Hashing Away! from *The Bitcoin Trader,* AVALON ASIC has delivered first RIG (68GH/s Confirmed) 2nd out proof from Bitcoin Talk and Engineering the Bitcoin Gold Rush: An Interview with Yifu Guo, Creator of the First Purpose-Built Miner from *Motherboard*

[26] Google | Data Centers Finland, see also DCD industry census 2013: Data center power from Datacenter Dyanmics

[27] See BFSB Finland and Bitcoin sysselsätter i Kimito

[28] Arguably the most important tool for miners and mining operators is a mining profitability calculator which helps (accurately) estimate operating costs and revenue generation. One popular version is the Bitcoinx calculator.

[29] These are lowerbound estimates based on a weighted token over the corresponding time frame. The actual number is likely higher.

[30] These exceptions are 1) botnets, 2) hobbyists, 3) education & research, 4) political actors, 5) "honest" miners who are speculating that the price will increase whereupon their costs are paid for. Four of these are discussed in Learning from Bitcoin's past to improve its future

[31] My thanks to David Merfield for concisely describing this phenomenon.

[32] This creates centralization issues which in turn leads to social engineering issues (such as regulations, taxes, and vulnerabilities to organized criminals).

[33] See Bitcoin Hurldes. A block reward halving creates a dilemma for miners. In a nutshell they are being asked to continue providing the same amount of labor for half the wages. As a consequence, many will leave and focus on other more profitable jobs (such as altcoins). This was illustrated best with what has happened to Dogecoin this past year.

[34] If it looked like something like that (a large jump in prices) were happening, the Bitcoin network would be dramatically "oversecured" and miners would likely switch to an altcoin with a much lower inflation rate.

[35] NRE stands for non-recurring engineering. See Bitcoin and The Age of Bespoke Silicon by Michael Taylor

[36] There is no such thing as "free" electricity only cheaper or more abundant. Solar panels (which are also depreciating capital goods) still require upfront costs which are amortized over their lifetime (usually 10-20 years). And the (unseen) knock-on effects of pollution and emissions from the creation of those solar panels needs to be quantified – the supply chain to create these tools which tap into renewable energy needs to be accounted for in such a calculation.

[37] See Dennard scaling, Koomey's Law and Ultimate physical limits to computation by Seth Lloyd

[38] Will Bitcoin ever be used for its intended purpose on a widespread basis?

[39] Personal correspondence, May 5, 2014. See Coinometrics

[40] I have discussed some of these educations in a presentation given on April 27, 2014 (video) (slides)

[41] Even faster block-chains with DECOR protocol and DECOR+ by Sergio Lerner

[42] Stress Test Prepares VisaNet for the Most Wonderful Time of the Year from Visa

[43] A fun thought experiment involving neutrino detector comes from Peter Todd, see The end of bitcoin is nigh! (Again)

[44] See Creating a decentralised payment network: A study of Bitcoin by Jonathan Levin (forthcoming)

[45] Transactional volume is an unnecessary illustration in this examination. It was used solely to illustrate how the cost of maintaining the network is relatively high despite relatively little transactional action. The bulk of the security is simply for the store of value function. The transactional volume could fall, yet the demand for tokens could rise. If the token value rose, the cost for securing those tokens rises proportionally with it irrespective of transactional volume. Nothing is "left over" from the burning process. Or in other words, the value of a token is function of current or eventual economic demand. Yet, the network hashrate burns the other side of that -- the value of the token equals the cost (of some kind of burn) on the other side to secure it.

[46] This is not a complaint about capital savings. One argument could be made that savings creates reserve demand for a currency. Yet in practice, virtually no one spends the token treating it much like a commodity or collectible like a stamp. Thus the term "cryptocurrency" is debatable and in practice it is more akin to a commodity, see Bitcoin: a Money-like Informational Commodity by Jan Bergstra and Peter Weijland

[47] This figure is generated by the following: 656250 bitcoins mined each year following the block halving multiplied by $1 million per token. As of 2012, the nominal GDP of Switzerland $631 billion.

[48] See Regulatory capture and Malignant computation. There are several proof-of-stake systems under development, yet thus far they have all failed key vulnerability tests leading to some kind of centralization verification process. See also What Are Bitcoin Nodes and Why Do We Need Them? by Daniel Cawrey

[49] Disclosure: I do not own any litecoins nor do I maintain or operate any mining machine of any kind today.

[50] According to one statistical analysis, from between its April 2012 announcement through August 28, 2013, Satoshi Dice-related transactions accounted for 52.3% of all bitcoin transactions. See Re: Satoshi Dice -- Statistical Analysis from Bitcoin Talk and A Fistful of Bitcoins: Characterizing Payments Among Men with No Names by Meiklejohn *et al*.

[51] Google to Increase Finance in Finland Data Center from *WiredRE*

[52] Sea-Cooled Data Center Heats Homes in Helsinki from *Data Center Knowledge* and Helsinki data centre to heat homes from *The Guardian*

[53] Personal correspondence, May 9, 2014. See also, Quantifying the Value of Bitcoin by Cal Abel

[54] Personal correspondence, May 9, 2014. For Babbitt's calculations see his spreadsheet on Bitcoin Mining

[55] Personal correspondence, May 9, 2014. This is based on a baseline electricity cost of 10 cents per kilowatt hour (kWh) which works out to 16,200,000 kilowatts per day. The Hoover Dam produces 49,920,000 kilowatts per day, so roughly 1/4 the output of the Hoover Dam. In practice, according to him it is likely double this amount as many people are mining at a loss or stealing electricity (or ignoring the electrical component entirely).

[56] Personal correspondence, May 7, 2014.

[57] Implementing sidechains and merged mining for example. See Episode #99 from *Let's Talk Bitcoin*

[58] Mike Hearn has proposed using Tor as an authentication mechanism for the network. Miners currently do not know if they are connected to the "right" Bitcoin network. Their connection could be spoofed by a Sybil attack and thus Hearn's proposal could mitigate some of those risks. See Mike Hearn on Coming Bitcoin Protocol Updates from *Money & Tech* and 4 New Bitcoin Features Revealed by Core Developer Mike Hearn from *Cryptocoins News*

[59] Depending on the time of year and quantity, rates in Saudi Arabia can run from $0.03 to as low as $0.01 (wholesale commercial) – however the hot summers make the location less ideal for mining due to the increasingly important cooling requirements. One Chinese reviewer mentioned that in 2012 a team in China conducted a cost/benefit analysis of building a mining pool in Mongolia and came to the conclusion that within 5 years it could likely become a prime location due to its cooler climate and relatively cheap access to energy resources.

[60] Thanks to Robert Sams for this keen insight; spending KhW, a scarce resource, makes a Sybil attack (among others) costly.

[61] Personal correspondence, May 7, 2014.

[62] Ibid

[63] When block rewards halve, this could create network performance issues. If half the labor force leaves, then the network may have less security that can only be incentivized through transaction fees. Nicolas Houy has modeled how the fee requirements would necessarily need to increase for the network to maintain the same level that existed prior to the halving, The Bitcoin mining game