Bitcoin & Gresham's Law - the economic inevitability of Collapse

Philipp Güring & Ian Grigg

October-December 2011

Abstract. The Bitcoin economy exhibits remarkable and predictable stability on the supply side based on the power costs of mining. However, that stability is challenged if cost-curve assumption is not solely expressed by the fair cost of power. As there is at least one major player, the botnets, that can operate at a power-cost-curve of zero, the result is a breach of Gresham's Law: stolen electricity will drive out honest mining. This has unfortunate effects for the stability of the Bitcoin economy, and the result is inevitable collapse.

We would like to share some thoughts about the economic models involved in the Bitcoin economy [SN], and the results that the model predicts.

The Bitcoin Mine

First, let us take a look at the process for manufacturing bitcoins, known as *mining*. To run a mining business, we need hardware (motherboard, graphics-card, ...) and power. Mining is a process of calculating/finding random inputs which, when hashed, fulfil certain requirements. When you have successfully mined a block, you earn 50 bitcoins as reward. The value of those 50 bitcoins depends on the market (e.g. https://www.mtgox.com/) of offers and requests, and therefore prices vary such as with national currencies or stocks on the stock market.

Bitcoin has a *difficulty* parameter which is calculated approximately every 14 days from the global mining speed of the previous 14 days. This is to keep the overall mining rate of the whole network approximately constant to 1 block every 10 minutes.

The difficulty tells us something about the current global mining capacity. If there are too many people mining at the same time, the difficulty factor goes up, and it is less likely/possible for a given miner to earn enough money in mined bitcoins to pay for the costs of production. At the margin, miners withdraw from mining, and the difficulty goes down. The miners do not have much direct influence on the market price of bitcoins, they can only sell the coins under-priced.

After a longer period of time, the investment costs of the hardware marginalizes, and power-consumption in Watts of the hardware dominates the costs-side of the mining equation. For Bitcoin mining to be profitable, the following formula applies:

Number of miners * average power costs per 10 minutes < 50 BTC * bitcoin price

Where Costs cross with Price - First Model

Let us look at an example of costs and income distribution. For now, we shall assume a fixed power cost of 0.1203 USD per kWh = 0,02005 USD per 10 Minutes Reference: [EIA1], and a production unit of 200 Watt equipment [BMH] which we will call a *miner*.

For a given average power price, and a given price of bitcoins, the maximum number of miners that are profitable can be calculated. If the price rises, more miners can be profitable, if it drops, profitability can be only achieved by less miners.

Maximum number of miners for averages of 200 Watts and 0.20 USD/kWh

BTC/USD	0,01 USD	1 USD	5 USD	10 USD	20 USD	32 USD
Maximum number of profitable miners	125 miners	12469 miners	62344 miners	124688 miners	249377 miners	399002 miners

Bitcoin trading started at a price of 0.01 USD, and therefore could potentially support up to 125 profitable miners at inception. The maximum trading price reached 32 USD, at which peak there was potential support for approximately 400,000 miners.

Due to the shared nature of the difficulty parameter, it is transparent for all operators what their average costs curves are at any moment in time. As prices are reflected in the open market, every operator can regularly calculate estimated income against costs, and whether mining is profitable or not.

Stability

When mining becomes unprofitable for an individual miner, he can either

- stop mining and hoping for better prices or less difficulty to continue mining again
- continue mining and hoping that the Bitcoins he mined will be more valuable in the future
- stop mining and sell the equipment, i.e., exit the business permanently

If a miner finds that mining is unprofitable, due to higher power prices, that miner can cease mining. In which case, the overall network capacity will go down again, and the difficulty will go down as well. When the difficulty goes down enough, lowest-cost idle miners will enter the business again, and continue mining, which will raise the difficulty again.

This system therefore exhibits stability. In the long run, the number of miners will likely diverge around some stability ruled by their profitability, which in turn is ruled on the supply side at least by long-run power costs stability. Complete crashes, or events where all miners cease mining at the same time are not expected, and this model shows self-correction around some form of stability.

Examining the Assumptions - Cost of Power

An important assumption above is that of fixed power costs. Since miners can be spread across the planet, and there are different power-costs in different regions, regionally diverse miners will have different mining costs. Power-costs within a region are usually relatively stable and only change slowly. The power costs we have found range from a minimum of 0.12 USD/kWh up to a maximum of 0.26 USD/kWh (in EUR, from 0.09 up to 0.2).

As above, miners with higher power costs will be unprofitable at a lower market price than those with lower power costs. Hence, we can expect that miners with higher power costs will be squeezed out over time, and following the modified assumption of regional power costs, mining will migrate to the area where costs are lowest.

Another assumption is whether the user is necessarily a rational actor, and is conscious of the cost of power. At the moment, the standard BitCoin client does not contain functionality to calculate, display and/or alert whether mining is profitable or not for the user, so some users might be uninformed when it becomes unprofitable for them, and keep mining.

Pursuing this further, Daniel Nagy has suggested in [DN1] that there will be a point in time, when the market will be flooded with a large amount of second-hand graphics cards. If the overall size of such depreciated hardware and misallocated power were large enough, it could lead to a *market shock* that dramatically resets the cost curves. However, assuming this is limited to a hobbyist market, and given the inherent flexibility that miners have (e..g, to adjust production or exit the business), this effect is more likely to be absorbed into the market more gradually.

Challenging the Power Cost Assumption - What about the botnets?

Building on the scenario of misallocated power costs by hobbyists or other users, what possibility is there for a simple power cost of zero? If a hobbyist is successful once, she might be encouraged to branch out to use the computers that are perhaps under control but are not directly owned. Farms of computers exist in families, in universities, corporates, governments, intelligence agencies .. and in botnets [Symantec].

Of those, most of them have approximate but non-zero power costs, and at the limit, the cost reduces to the opportunity cost - what is the best use that can be made of the power? By far the most interesting are the botnets, which earn their direct power cost of zero to the owner by dint of the fact that the power is stolen.

Hence, we can currently see 3 different classes of miners:

- For-profit miners who mine Bitcoins for selling them afterwards. For them to mine, it must be profitable. They pay for power.
- Non-profit miners who mine for other reasons: Just for fun, Education, Political or any other reasons. They do

not care that much about the power costs unless they would be prohibitively high. Because they "borrow" the power from people near them, and near people are limited, their scale is small.

- Botnet operators mine strictly for money. As the power-bill is paid by the victims within the botnets, it is effectively stolen. Their scale is huge.

All 3 classes of miners are sharing the profits of the mining. But they have very differently cost curves. The for-profit miners work according to the original model of market stability - as the price rises and lowers, they enter and exit the market. But the botnet operators do not have to pay for the power, they get it more or less for free. Their cost curve is zero. (We can ignore the hobbyist market from now on.)

Let us examine the potential size of the market where one group has an honest paid power curve, and another group has a dishonest free power curve. At a chosen (earlier) time of writing, the current Bitcoin price enabled a market for e.g. 37500 miners. Consider an operator in control of a botnet with 100,000 computers, known as *bots*. If he were to switch 20% = 20,000 computers into mining, then the market-size for profitable miners would be reduced to 17500 miners. In the event that he were to activate more than 37500 miners, it would make mining unprofitable for the for-profit miners, assuming the latter group have known and honest power costs.

A botnet of only 100,000 computers is capable of stealing a share of the cake, and indeed, for smaller cakes, of stealing the entire thing.

The market for Botnets

What then is the market for botnets? According to [Damballa], there were in 2011 five botnets with greater than 1 million computers, and 32 botnets which were between 100,000 and 1 million bots. If one or even several of the larger botnets start mining, they can likely take over the whole mining market.

Is there a cost to botnets? Some or many botnets are offered for rent, so it is at least hypothetically possible to rent 1 million bots for 24 hours. According to [DamballaBlog1] a botnet with 100,000 bots was available in 2009 for 200$ USD for 24 hours, and [Symantec] points at $400 for other perhaps similar purposes. This would imply a non-zero power curve. (At a then-bitcoin price of $20 [Symantec] estimates the earnings at $3000, and [Zooko] concurs with $5000 per day using conservative assumptions, so even at that cost there is money potentially to be made.)

However, as [Zooko] recognises, the various rented uses of the botnet are not mutually exclusive. Further, while much of the rental business is based on trade that the botnet operator likely finds more efficient to contract out (phishing, spam, DoS, etc), the bitcoin business is something that is easily kept in-house. No other customer can likely better the efficiency than the operator, and doing it in-house saves on transaction costs, so the operator will keep this opportunity to self. Botnets may idle and mine, waiting for other customers. Indeed, if anything, this might cause the rental price for botnets to rise to above the value earned by mining, at least as far as the (GPU) resource is exclusive, and it would be interesting to test today's current low prices as being indicative of the idling costs of a botnet.

Hence, for our purposes we approximate the power cost curve for botnets at zero. This leads to several possibilities: botnets take a slice of the market, botnets dominate the whole mining market, or botnets do other non-mining interventions into the market. Given the nature of botnets, it seems reasonable to assume the botnet herders will simply attempt to maximise their take from the market. This suggests that they face an optimisation problem: how to ensure the greatest slice of the pie, while not destroying it.

Testing the model: Mining is owned by Botnets

Let us examine the various points along an axis from honest to stolen mining: 0% botnet mining to 100% saturation. Firstly, at 0% of botnet penetration, the market operates as described above, profitably and honestly. Everyone is happy.

But at 0%, there exists an opportunity for near-free money. Following this opportunity, one operator enters the market by turning his botnet to mining. Let us assume that the operator is a smart and careful crook, and therefore sets his mining limit at some non-damaging minimum value such as 1% of total mining opportunity. At this trivial level of penetration, the botnet operator makes money safely and happily, and the rest of the Bitcoin economy will likely not notice.

However we can also predict with confidence that the market for botnets is competitive. As there is free entry in mining, an effective cartel of botnets is unlikely. Hence, another operator can and will enter the market. If a penetration level of 1% is non-damaging, 2% is only slightly less so, and probably nearly as profitable for the both of them as for one alone.

And, this remains the case for the third botnet, the fourth and more, because entry into the mining business is free, and there is no effective limit on dishonesty. Indeed, botnets are increasingly based on standard off-the-shelf software, so what is available to one operator is likely visible and available to them all.

As each new botnet enters the market, supply increases, and the operators drop their prices. Each new botnet faces some shrinking amount of easy money, but it's still worth it -- to them. But to honest miners, they are quickly pushed below their minimal cost of honestly purchased power.

In the end, honest miners are squeezed out by the cheaper prices, one by one, and the market settles at a new stability. At the limits, the new price will settle at above the cost of botnet mining, and below the cost of honest mining. In effect, the market becomes addicted to the price of bitcoins mined using stolen resources. With little difficulty it is easy to see that the market for mining is owned, or will be owned, by the botnets.

Collapse

Using Mancur Olsen's rationale that a prince is a bandit that stops roving, the notion of the mining franchise being captured by the botnets might have been an acceptable compromise to the economy growing up around bitcoin mining, if it went no further [Olsen]. However, criminals are rarely satiated. Several things happen: (a) incentives for easy money naturally cause an increase in criminal participation at all levels, such as direct theft of bitcoins. This increase across the board encourages (b) honest users to pack up and leave. Both of these effects combine to create rising criminality, and (c) at some stage the Feds get involved. Finally, (d) the system collapses.

It might be claimed that honest users can simply continue to trade, as bitcoins are fungible and can be used as money, independent of their prior history. Such a claim is hopeful and naive, and not supported by history of such systems. A counterintuitive effect happens when criminality is inherent in a market: *the Feds* (a handy label for all policing authorities, world wide) will assume that all activity is criminal, even knowing it is some percentage in the midrange, and let any remaining honest users suffer the costs of proving otherwise [Feds]. Indeed, given this present hypothesis that the mining market is owned by the botnets, the Feds will simply claim that all or nearly all bitcoins are the proceeds of crime. It is an easy claim to make, and likely will impress a court when presented in a colourful fashion.

The court will then hand the Feds the order to go in with all guns blazing, to use a phrase. Their approach is to seize as much as possible, cause as much chaos as possible, gum up the economy and see who they can shake out [Zetter]. As the Feds will then hold the value, typically many honest players will be legally or financially wiped out, including to the extent of being unable to mount a legal challenge. Those that remain will face the onerous burden of proving their activity was honest.

Once this risk arises, there is substantial incentive for honest owners of assets to wisely exit.

This pattern was observed in other innovative money markets, and is now playing out in the BitCoin market place [e-gold] [epassport] [USSS]. Once beyond some tipping point, we can predict the market will move quickly into routine criminality, and become contaminated with criminality at all levels, not just mining. At this point, honest users will be increasingly scarce, and the Feds will move in and slice out parts of the sector, triggering a collapse [Feds]. Not necessarily in that order.

Hence, from the result that mining is owned by the botnets, and from the general patterns of increasing criminality, the Bitcoin unit and the market facilitated by it inevitably move to collapse.

This stands in contrast to for example the credit card business which has a long run sustained fraud rate of around 0.1%; in this market, entry is not free, and policing increases with increasing fraud. This limit to the growth of the criminality scales up as more losses are covered by the credit card operators, which see reducing those losses as increased margins to themselves.

Breaking Gresham's Law - stolen electricity beats out honest mining

What went wrong? In economic terms, BitCoin breaches Gresham's Law, which states in simple terms that *bad money drives out good* [Gresham]. More deeply, Gresham's Law postulates two forms of money with distinct demand or supply curves (or, uses in society). Normally these would trade up and down in price as per their distinctions. Yet, in Gresham's model, we find the two distinct forms of money are mandated to be equal in price or at a fixed exchange rate. Then, the form that is otherwise cheapest to society will drive out the other, taking into consideration all the uses and costs to society.

Gresham's Law is more generally stated as the law of economy: we use the most efficient resource where we can. For money, the corollary is that the resource which supports the accounting function of money sits (e.g., cows, gold, paper, bits) should have no better use in society than use as money. For example, printed paper is so cheap that it typically makes no difference whether it is used for money or not.

Bitcoin breaches the law of economy in that its use of proof-of-work causes costs in power, which is otherwise better used or better desired. Then, botnet-mined bitcoins circulate alongside honestly-mined bitcoins at the same price, as mandated by the software design, and thus we find bad money circulating alongside good. BitCoin's breach of Gresham's law can be seen as "stolen electricity beats out honest mining." The above *proceeds of crime* argument adds some coincidental colour to the term 'bad money.'

What good the bitcoin unit then?

Participants in the economy exhibit a supreme amount of faith in Bitcoin, and perhaps with merit. The design for distributed coordination is a stroke of genius.

It is possible to envisage this technologically-derived faith transferring into a belief in the monetary properties of BitCoin, however irrational. Thus, we could see a steady series of new people bringing new value in via the mechanism of sales of bitcoins. This demand curve of believers stands against the prediction of collapse, hence, the best we can hope for is that the bitcoin price will exhibit very high volatility, reflecting the continual battle of new suckers *versus* new shakedowns.

A unit that is volatile in value is unsuitable for pricing goods & services, so the bitcoin unit cannot sensibly be seen as a money.

Could bitcoins then be seen as a financial instrument such as an investment? No. This is because there is no underlying contract. Typically, every investment instrument must somehow have a contract that describes its underlying value, so that owners always have the option of redeeming that underlying value in some sense. E.g., a bond returns a face value in some years, so can be held until then, and a share is a part ownership of assets that generate profits. An extreme alternative is an implied contract found in national monies, where the knowledge of being able to pay ones taxes with the unit is sufficiently stable as to make the money desirable.

Bitcoin offers no contract, written or implied, and therefore cannot be an investment. If it is not a money, and not an investment, the challenge then is to identify what it is good for, if not nothing? Its value may ultimately only be found in the potential for suckers and shakedowns, a purpose which dovetails nicely with the above mining prediction.

Repairing the Breach - whiteboarding some ideas to fix BitCoin

In this section, we consider some ideas to fix the flaws in BitCoin as a stable money. This is in the sense of *whiteboarding* where all possibilities might be considered, even if we know some are unlikely or impossible. The challenge is to find some way to escape from the inevitable trap created by the requirements for free-entry and proof-of-work.

Mafia-concentration. What if we could have a mining cartel? Instead of a competitive market with free entry, consider a single player dominating the market. This could be for example by a successful botnet operator getting the jump on others, and using his profits to buy out the competitors, or otherwise defeat them, mafia-style. As his size grows, his capability to force out competitors increases. This model still ends up in collapse, as above.

Government. Another possibility is for a legal player to use appropriated power. For example, it is known that national intelligence agencies have vast computing farms, and it is plausible for them to intervene in the market for BitCoin. Typically this would be via the interests of US Treasury's Secret Service unit which has the mandate to protect the US currency [USSS], and has a track record of intervention in digital currencies. In this case, an intervention might involve dumping supply, then stripping it, and the ensuing volatility driving out the honest players who might be looking for characteristics of stability in a monetary unit.

Cloud. A further hypothetical possibility is that of major corporations devoting their clouds to the task. Google, Microsoft, Apple, Amazon can probably muster the capital to shift the BitCoin market. Assuming they could find it in their hearts to do so, they can attempt to beat back the botnets, but then they are caught by the power trap: their electricity bill is honestly paid for. Rather than compete honestly, they would probably prefer to either secure the platforms, or appeal to the Feds for the botnets to be pushed out of the market.

Even if the corporates could win back the business with their cloud farms or similar, and gain some continued profitability, they would also quickly find themselves in open competition against each other. Traditional cartel theory would then lead to some legal or technical device to exclude small competitors and cooperate on prices between the half dozen majors [Dowd]. But then, once the industry is stabilised, there would be an opportunity to shift their users across to a lower-cost platform such as is found in more centralised payments systems rather than the BitCoin p2p exotica (c.f., ePointSystem or Ricardo) as these have zero power costs.

Anti-botnet. An alternate strategy for the Operating System shippers is to clean up their security, and put the botnets out of business. This would assume an incentive that to date has not been sufficient, e.g., Microsoft is trying to shut down the botnets but has to date only succeeded to a small extent. In the event that they could capture the Bitcoin market themselves, they still face the incentive to shift their users across to some lower cost form of money.

Proof-of-Work. The fundamental assumption that proof-of-work is a good mechanism for producing a shared solution to a problem breaks down if power is free (stolen) for some and costly for others. Inevitably, the lowest-cost power miners win, and in this case the differentiation is even worse, as between criminals and non-criminals, the criminals always win, and this inevitably leads to collapse. One can eliminate the dichotomy by taking away the proof-of-work calculation, but as this is a treasured part of the design, it is no longer Bitcoin.

Free entry. Legally, free entry could be banned, and specifically, only honest miners permitted to participate. A private law organisation could ensure that there is incentive to be honest [CAcert]. Yet, again, this 'fix' make a mockery of Bitcoin's original spirit. Further, once only honest issuers exist, there is less need for the coordination method of proof-of-work.

Segmentation. One perhaps feasible counter-measure would be to add competing currencies (e.g. SolidCoin [SC1]) which require the same kind of mining. E.g., if the additional currency has the same market value, the total currency market and mining market is doubled, and we could potentially grow the economy with multiple Bitcoin-like currencies. But this does not change the fundamental or economic rules of the Bitcoin economy, it just segments it. And as the current threat environment has shown, attackers more easily migrate to new segmentations than users. Any successful currency still faces the prize of success: collapse, and contagion will clean up the rest.

Pricing Controls. Another perhaps feasible counter-measure would be set a minimum price for bitcoins that is above the computing capacity of the botnets: If 1 BTC is guaranteed not to be less than 1000 USD, the problem would be gone. But this is implausible in the design as there is no ability to tie it to the value of something else. In order to tie it to something else such as USD, an escrow contract such as envisaged in Ricardian Contracts [Ricardo] is needed, or a reliable demand function such as US Treasury's income in taxes.

Conclusion

The security of Bitcoin relies on a single party or cartel of parties not being able to dominate the capacity for mining. Therefore Bitcoin relies on a large and diversified network of miners. Yet, the proof-of-work mechanism, the existence of free entry and no limits to honesty ensure that botnets will cause a breach of Gresham's Law: stolen electricity will drive out honest miners. Once botnets take over, criminality increases, honest users decamp and collapse follows.

Hence, the requirement of diversification is broken by Bitcoin's very mechanism to make diversification work fairly: proof-of-work. Attempts to repair the design generally result in the replacement of Bitcoin with some other architectural base.

The Bitcoin economy is highly vulnerable to attack. If an agent were to decide to attack Bitcoin, he has several strategies available. One could operate a mining botnet and slowly lower the Bitcoin market price by regularly selling small amounts of bitcoins with a declining price. As the honest miners are squeezed out, further manipulations of the Bitcoin system are possible. A second strategy is to pump & dump to generate volatility. Both strategies result in the honest mass market decamping for other fields. Once the market takes on the taint of criminality, the Feds are encouraged to shut it down by targeting the exchange makers; fear of criminality and the appearance of the Feds work together to cause the collapse.

Acknowledgements

Our thanks to Daniel A. Nagy, Peter Gutmann, Zooko Wilcox-O'Hearn and many others for taking the time to provide valuable insights into these issues.

References

SN: S Nakamoto, "A Peer-to-Peer electronic Cash System." 2009. Bitcoin.org.

EIA1: U.S. Energy Information Administration, Electric Power Monthly, 2011, http://www.eia.gov/cneaf/electricity/epm/epm_sum.html

BMH: , , 2011, https://en.bitcoin.it/wiki/Mining_hardware_comparison

DN1: Daniel A. Nagy, , 2011, http://unenumerated.blogspot.com/2011/05/bitcoin-what-took-ye-so-long.html#4030634241199385500

Symantec: blog post by Peter Coogan of Symantec Corporation, "Bitcoin Botnet Mining," 17th June 2011. http://www.symantec.com/connect/blogs/bitcoin-botnet-mining

Damballa: Damballa Inc., Threat Report - First Half 2011, 2011, http://landing.damballa.com/20110908-1H2011ThreatReport.html

Zooko: bog post by Zooko Wilcox-O'Hearn, "Are botnets a significant part of global Bitcoin mining?" 12 Nov 2011 https://plus.google.com/108313527900507320366/posts/3Z4trcerKLa

DamballaBlog1: Gunter Ollmann, Want to rent an 80-120k DDoS Botnet?, 2009

SC1: SolidCoin, http://solidcoin.info/

Feds: 'The Feds' in this case is likely the US Secret Service, which has a mission of protecting the US currency and payment systems. See photo in Wired article, below.

Zetter: Kim Zetter, "Bullion and Bandits: The Improbable Rise and Fall of E-Gold", Wired Magazine 2009 http://www.wired.com/threatlevel/2009/06/e-gold/ .

e-gold: See commentary on FC, for example: http://financialcryptography.com/mt/archives/001169.html

epassport: Ian Grigg, "Why did VISA pull the plug and leave the "little people" high and dry?", Financial Cryptography 05 Feb 2012, http://financialcryptography.com/mt/archives/001277.html

Olsen: Olson, M. (1993). Democracy, dictatorship,and development. American Political Science Review87: 567-576.

USSS: The Sunday Telegraph (Australia), "NSW Police will join forces with the US Secret Service to smash a blackmarket trade of guns, drugs and child pornography on the internet." http://www.dailytelegraph.com.au/news/sydney-nsw/deal-to-fight-blackmarket-online-crimes/story-fn7y9brv-1226193359778 Quote: 'Central to the underground market is the use of virtual currencies, which have the capacity to eliminate traditional money trails and provide users with anonymity. This includes Bitcoins, a legitimate currency created in 2009 which has become "the currency of choice" among criminals because of its capacity to mask transactions and money transfers. "A number of our investigations involve payment using some form of virtual currency - Bitcoins appear to be the currency of choice," Mr Dyson said. "It's favoured so much that it has its own market price." '

Gresham: Gresham's Law is reasonably described on wikipedia: http://en.wikipedia.org/wiki/Gresham%27s_law and many other Internet resources. Note that for present purposes it is not necessary to deviate from the popular understanding of the law.

Dowd: For a description of the cartel operation of payment systems without regulation, see Kevin Dowd, "The Evolution of a Free Banking System," in Laissez Faire Banking, Routledge Foundations of the Market Economy 1996. http://iang.org/free_banking/dowd_lfb_intro.html

CAcert: For example, CAcert is a worldwide network of nearly 5000 agents collected in what is sometimes called a *web of trust*. Each agent, called an Assurer, can make a *CAcert Assurer Reliable Statement* (or CARS) which others in the network can rely upon. If found to be unreliable, victims can take their case to CAcert's Arbitrator, who has wide latitude to rectify harms.

Ricardo: Ian Grigg, "The Ricardian Contract," WEC 2004. http://iang.org/papers/ricardian_contract.html