Bitcoin's centralized endgame, and how to avoid it

Copyright © 2014 pabr@pabr.org
All rights reserved.

We review 19 common misconceptions about the Bitcoin crypto-currency system and show how the reality helps predict its endgame: centralized mining, then centralized governance.

We suggest that enforcing national mining quotas might be the lesser of many evils if centralization is to be avoided. More generally, we introduce the idea of *maximally-distrustful oligopolies* as a practical solution to distributed consensus.

READ THE HYPERTEXT VERSION HERE:
http://www.pabr.org/bcendgame/bcendgame.en.html

Revision History		
1.0	2014-09-03	Initial release.
1.1	2014-09-21	Added maximally-distrustful oligopolies.
1.2	2014-11-16	Added section on web of trust.
1.3	2016-06-17	Added note about scarcity as convention. Added post-scriptum. Added myth #19.

Table of Contents

1. Introduction

Currency control has been a powerful tool for governments at least since the Roman Empire. Hence, it is surprising that Bitcoin is still thriving after 5 years, whereas earlier candidate virtual currencies were promptly shut down. Is Bitcoin really more resilient than its predecessors ? Does it really have all the properties that its proponents advertise ? Or is it a giant decentralized Ponzi scheme and an environmental disaster, as opponents argue ?

Regardless of its future, Bitcoin is worth studying as possibly the first software system which successfully binds a wide variety of intellectually-challenging disciplines:

- Cryptography, the arcane art of securing data and communications
- Distributed systems theory, including the Byzantine generals' problem and the CAP theorem
- Economics and game theory (how to engineer sustainable economic systems)
- Politics (the making of consensus).

This article assumes familiarity with Bitcoin concepts such as the blockchain, mining and the 51% monopoly problem. Basic knowledge of economic theory is also expected.

2. Conventions

"Bitcoin", capitalized, denotes the whole system. "bitcoins", in lowercase, denotes units of account of the currency.

Following the customs of the Bitcoin community, we refer to Bitcoin accounts as "wallets", to emphasize that unlike bank accounts, they do not have to be controlled by a trusted third party.

Following definitions adopted by several banking institutions, we call Bitcoin a virtual currency even though nowadays traditional currencies are just as virtual (i.e. "dematerialized") as Bitcoin.

3. Common misconceptions about Bitcoin

Note: For a more balanced overview of Bitcoin misconceptions, see also [BITCOINIT_MYTHS].

3.1. Myth #1: Bitcoin was made possible by advanced cryptography

Actually, Bitcoin uses only two very old cryptographic concepts:

- Asymmetric cryptography: A public key identifies a compartment ("Bitcoin address") of a wallet, and the corresponding private key authorizes transfers from this compartment.
- One-way hash functions for bandwidth reduction, for protection of public keys, and as part of the mining scheme.

The actual primitives used are ECDSA (2005), SHA256 (2001) and RIPEMD-160 (1996).

Other digital cash systems involve more sophisticated concepts such as blind signatures and zero-knowledge proofs. Often, this is because they emphasize untraceability, whereas Bitcoin focuses on eliminating trusted third parties.

3.2. Myth #2: Bitcoin transactions are anonymous and untraceable

Bitcoin does provide anonymity in so far as anyone can create and use a wallet without providing identification.

However, anonymity is not the same as untraceability. Actually, the way Bitcoin works implies that all transactions are public. Real estate is possibly the only other asset class where that level of transparency is enforced.

The Bitcoin community uses a variety of techniques to work around this constraint:

- Users are strongly discouraged from publicly posting Bitcoin addresses, although this is a popular way to ask for donations.
- Some wallet applications refrain from reusing Bitcoin addresses or merging funds, even when this would be the natural way of doing things. But this is merely obfuscation. "Blockchain forensics" appears to be a rapidly growing industry.
- Using an online wallet provides some protection from public scrutiny, at the cost of having to trust a third party. But flows can still be traced with cooperation from the service provider.
- There are trusted third parties whose sole business is to "mix" (i.e. launder) bitcoins from large numbers of users. There are also plans to implement such mixing in a decentralized way.
- There are semi-legitimate businesses which are technically equivalent to laundering services. For example, in early 2013, gambling accounted for half of all Bitcoin transactions and 5% of volume [http://lsvp.com/2013/08/23/at-least-half-of-all-bitcoin-transactions-are-for-online-gambling/gambling].
- Bitcoins can also be transferred off-chain by simply handing over the private key of their address. For obvious reasons this requires that the recipient trust the sender, except maybe if the keys are generated and stored inside tamper resistant hardware.

With Bitcoin, as these examples suggest, there is a very thin line between trying to protect one's privacy and actively engaging in money laundering. At the very least, to avoid suspicion, users should refrain from using service providers who operate under foreign jurisdictions with weak financial regulations. Unfortunately the blockchain does not record at what moment money changes hands. So if a law-abiding customer pays a merchant and the merchant immediately forwards the funds to a laundering service, the customer might be in trouble.

3.3. Myth #3: Bitcoin transactions are instantaneous

It is true that anyone can generate a Bitcoin transaction in just a few seconds, using a variety of wallet applications and online services.

But Bitcoin transactions are not validated instantaneously. Technically, they are never really finalized (except as a side-effect of checkpointing [https://en.bitcoin.it/wiki/Checkpoint_Lockin], in some implementations). The system merely ensures that the probability of having transactions invalidated decreases rapidly according to the following timeline:

Offline, within seconds . A sender signs a Bitcoin transaction, and the recipient verifies the cryptographic signature. This provides about the same security as an anonymous check.

Online, within seconds . The transaction is broadcast to the Bitcoin network. The recipient obtains an acknowledgement from one or more well connected Bitcoin nodes. At this point the recipient knows, with good probability, that the funds being transferred actually exist, that unsophisticated double-spending attacks will be rejected, and that the transaction is likely to be added to the blockchain within minutes. Note that the concept of "well connected nodes" implies that "some nodes are more equal than others". More about this later.

Online, within 10 minutes . The recipient obtains a first confirmation, i.e. a proof-of-work endorsement of the transaction. Note that this delay of several minutes makes Bitcoin unsuitable for many popular applications such as point-of-sale payments, vending machines, toll booths and ATMs. Workarounds involve off-chain transactions and trusted third parties.

Online, after 1 hour . The recipient has obtained six confirmations, which is historically considered sufficient for most uses. More about this threshold later.

Online, after 17 hours . The recipient has obtained 100 confirmations. This is the maturation delay that Bitcoin uses internally to validate newly mined bitcoins.

3.4. Myth #4: Bitcoin is money

Economists define money as having at least three functions:

- **Medium of exchange .** As of August 2014 Bitcoin does not work well offline. It does not have legal tender status anywhere. No government accepts it as payment for taxes. An increasing number of merchants accept it, but often only via third party intermediaries.
- **Unit of account .** Because of its volatility, Bitcoin is not currently a convenient unit of account. Merchants who accept it typically set their prices in traditional currency and compute amounts in bitcoins on-the-fly. Mainstream adoption would stabilize rates, but only to some extent, for lack of a central authority to provide liquidity, fend off speculators, and prosecute "pump and dump" and "short and distort" schemes. At the very least, in the short term, its market value will continue to reflect fluctuations in the electricity and semiconductor markets.
- **Store of value .** Because it lacks intrinsic value and its future is still uncertain, Bitcoin is obviously not a safe long-term investment.

In addition, money is implicitly expected to be fungible, i.e. two sets of coins, banknotes or bank deposits representing the same numerical amount should be interchangeable. But the extreme traceability of Bitcoin implies that a freshly mined coin might be worth more than one coming from a gambling website or a laundering service. There are proposals to allow bitcoins to be "redlisted", i.e. marked as suspicious [http://www.coindesk.com/bitcoin-tracking-proposal-divides-bitcoin-community/].

Note that traditional currencies are not perfectly fungible either. For example, in late March 2013, one euro deposited in Cyprus was certainly worth less than one euro stored anywhere else.

3.5. Myth #5: Bitcoin is a currency / Bitcoin is a commodity

Whether Bitcoin is a currency or a commodity is a matter of fiscal policy, with significant implications wherever a value added tax is applicable. If Bitcoin is declared a currency, then a merchant who accepts it is receiving a payment. If Bitcoin is only a commodity, then the merchant is engaging in bartering.

3.6. Myth #6: How can Bitcoin not be a currency when it has an official ISO code like USD and EUR?

It is true that, in an interesting development, ISO has allocated a three-letter code to Bitcoin. Note that the code is XBT, not BTC.

However, ISO 4217 is not restricted to currencies. It also defines codes for gold (XAU) and other commodities.

3.7. Myth #7: As a currency and a payment processing system, Bitcoin is efficient

The cost of running the Bitcoin network can be estimated based on the following data from mid August 2014:

- Total hash rate: 200 PH/s
- Mining reward rate: 25 bitcoins per 10 min

- All mining performed on state-of-the-art hardware costing 0.7 USD per GH/s and consuming 0.77 J/GH
- Hardware must be renewed every 6 months
- Cost of electricity: 0.15 USD/kWh.

Under these assumptions, the operating cost of Bitcoin is least 250 million USD per year, i.e. about 4% of the monetary base.

According to some estimates the daily transaction volume is about 59 million USD ([BLOCKCHAININFO_STATS]). This puts the overhead at 1.2%. Note: This figure could be heavily underestimated because the blockchain does not distinguish between book-keeping operations and actual commercial transactions.

Regardless of how this compares with the operating overhead of traditional currencies and payment systems, a centralized version of Bitcoin would obviously be more efficient.

Users do not have to bear these costs because they are dwarfed by inflation (4% vs 13% - see Section 3.12, “ Myth #12: Bitcoin is deflationary ”). But this cannot last forever, and critics see similarities with Ponzi schemes.

Based on the same best-case hypotheses, it takes at least 190 USD to mine a new bitcoin (hardware: 35 USD, electricity: 154 USD). The actual cost, taking into account the installed based of older hardware, infrastructure and cooling, is probably very close to the exchange rate of 500 USD. Note that this is not surprising: Whereas central banks have a monopoly on issuing their currencies, anyone can mine bitcoins. In a market with no barriers to entry, prices cannot significantly and sustainably exceed production costs. A similar situation exists in the precious metals market, where the market price of gold (about 1300 USD/oz) is close to the average cost of extracting it from the ground (about 1200 USD/oz), despite the overhead of obtaining mining permits.

Is it economically rational for a currency to be worth no more than the cost of producing its tokens ? This is beyond the scope of this article.

3.8. Myth #8: Bitcoin is open and egalitarian

It is true that Bitcoin allows anyone with Internet access to make international transactions, which is a major societal innovation. Billions of people do not have a bank account, but many of them do have smartphones.

However, the mining process favours those with cheap electricity, cheap semiconductors, cheap real estate and a cold climate. Botnets used to be a concern because they got all of this for free; fortunately ASICs have made them irrelevant. At the time of writing, mining activity appears to be concentrating in China [http://bitcoinmagazine.com/12914/bitcoins-made-in-china/], possibly due to the proximity of semiconductor factories and subsidized electricity costs.

3.9. Myth #9: The recent rise in exchange rates must reflect massive demand for bitcoins

First we need to understand how the market value of bitcoins is determined.

The Bitcoin money supply is sometimes analyzed in terms of industrial production, as the phrase "mining" suggests. But this analogy does not hold. Indeed, the production of new bitcoins has been centrally scheduled since the beginning [https://en.bitcoin.it/wiki/Controlled_supply]. Regardless of how much capital is invested in mining activity, and whatever the miners do, the difficulty adjustment mechanism will prevent them from producing more than 25 bitcoins per 10 min (as of August 2014).

Actually, the Bitcoin money supply is more like an auction. Everything happens as if a central bank were putting 25 bitcoins up for sale every 10 min. Each miner estimates how much the others are willing to

spend and decides whether to match their bids or not. Since Bitcoin does not want to have a central bank, the money goes to the energy and semiconductor industry instead, but this does not affect price discovery.

Unfortunately, it is well known that auctioning scarce resources often results in overbidding. For example, auctions for the allocation of radio spectrum to telecom operators are sometimes organized in such a way that the highest bidder pays the second highest bid, rather than his own. This is done out of fear that otherwise candidates would overbid and go bankrupt. In the case of Bitcoin the only thing that can prevent overbidding is alternative supply from the secondary market, i.e. old bitcoins being offered for sale on exchanges. As of August 2014 the daily production of new bitcoins is about 2 million USD and the daily exchange trade volume is about 3 million USD. Is is unclear whether this ratio between primary market and secondary market can lead to fair price discovery.

All things considered, there are several candidate explanations for the rising market value of bitcoins:

- Actual demand from users and investors.
- A perception that due to upcoming regulation, freshly mined bitcoins are more valuable than ones which can be traced back to disreputable addresses. This would explain a disconnect between the primary market (mining) and the secondary market (exchanges), and over-investment in mining hardware. Also, from this perspective, "cloud mining" could be considered as a form of money laundering.
- Rapid technical innovation: Whenever market prices fall below average production costs, the only way to mine profitably is to invest in newer, more efficient hardware. But in the long term this increases production costs for everyone via the difficulty adjustment mechanism.
- Spontaneous over-investment by miners. Note that this is not economically rational unless miners are secretly expecting a payoff beyond the sale of mined bitcoins. In a traditional market this would be akin to eliminating competition by selling at a loss. More about this hypothesis later.

3.10. Myth #10: Bitcoin has no processing fees

Actually, the Bitcoin protocol does have provision for fees: Each transaction may include a "tip" which will be claimed by the miner who succeeds in adding it to the blockchain. The network expects a mandatory tip (a.k.a. fee) for unusual transactions which could be interpreted as flooding attacks. There are no fees for regular transactions, but offering a tip incentivizes miners to process the transaction more rapidly. According to some estimates, voluntary fees amount to about 0.3% of the transaction volume ([BLOCKCHAININFO_STATS]).

It is expected that as the Bitcoin monetary base approaches the ceiling of 21 million bitcoins, transaction fees will be the main incentive for miners to keep the network running. Until then, the cost of running the network is paid by inflation. According to some estimates, miners currently receive about 4% of the transaction volume in freshly-minted bitcoins ([BLOCKCHAININFO_STATS]).

3.11. Myth #11: Bitcoins are inherently scarce, like gold

Proponents argue that Bitcoin is similar to physical gold because by design, mining can generate no more than 21 million coins. However:

- Since some users entrust the management of their wallets to third-party services who handle accounts off-chain, Bitcoin is subject to fractional reserve banking, just like paper gold. This practice may increase the money supply well beyond the monetary base.
- Not everything that is scarce is valuable. Gold's value does not result solely from its scarcity, but also from its uniqueness among metals. Bitcoins may be scarce, but there are already about 50 alternative virtual currencies [http://altcoins.com/] with similar properties. Assuming virtual currencies become popular and their value significantly exceeds the cost of issuing them, exchange rates between Bitcoin

and its competitors will be decided based on popularity and technical merit. For example, a virtual currency that guarantees both anonymity and untraceability would certainly become more popular than Bitcoin for some applications. Conversely, a virtual currency with legal tender status somewhere, or one with built-in legal compliance mechanisms, would have a better chance of becoming mainstream.

- The scarcity of bitcoins is not written in stone, nor in math. It is merely a consensual convention. If the Bitcoin community collectively decides that the monetary base should be increased for the greater good, then this can be implemented easily. This could happen if Bitcoin becomes popular and new users feel that the early adopters (now a minority) are enjoying an unfair advantage. In practice this would be decided by a supermajority of miners switching to a new version of the protocol. Miners would probably agree, as this would make their business model more sustainable. In the current system, the scheduled reduction of mining rewards threatens them directly.

3.12. Myth #12: Bitcoin is deflationary

Ignoring fractional reserve banking and competition from other virtual currencies, it is true that eventually the Bitcoin monetary base will increase slower than the economy, and then decrease as users inevitably lose private keys. However:

- This does not guarantee that the purchasing power of one bitcoin will increase. Ultimately the value of Bitcoin as a medium of payment, as a unit of account and as a store of value will be determined by its actual usefulness.

- As of August 2014, the Bitcoin monetary base is still growing at about 13% per year.

3.13. Myth #13: The Bitcoin network is resilient

In practice Bitcoin is only as resilient as the Internet. Like all distributed/replicated databases, it is vulnerable to network partitioning: If a government decides to isolate its population from the Internet, then the blockchain forks and double-spending attacks become trivial.

Bitcoin proponents argue that the blockchain could be kept coherent by various means, including by attaching memory cards to carrier pigeons if need be. However, we have seen that real-time communications are crucial to detecting double-spending attempts and confirming transactions within reasonable time.

Alternatively, the Bitcoin protocol will automatically restore consensus after a partitioning event: When full network connectivity is restored, only the longest fork of the blockchain will survive. Transactions performed in isolation must be resubmitted. They will make it to the blockchain, unless a double-spending attack has occurred in the meantime.

In the context of databases, the network partitioning problem is sometimes solved with out-of-band kill mechanisms: Whenever one node suspects that another node is faulty or unreachable, it actively kills it, e.g. by switching its power supply off. If the mechanism is fast enough, the probability of mutual destruction is low. This approach is appropriate when data consistency is more important than service availability. Bitcoin implicitly has a similar mechanism: The isolated portion of the network will suddenly have less hashing power and will therefore experience longer confirmation delays and lower transaction throughput.

Therefore, users who live under oppressive regimes, who are the ones who most need a trustworthy alternative currency, are the ones who would most suffer from a network-level attack against Bitcoin.

3.14. Myth #14: Bitcoin security stems from a community of mutually distrustful miners

This is the core tenet of Bitcoin as a decentralized currency without trusted third parties. Originally the Bitcoin network consisted of personal computers competing against each other during their idle time.

But miners quickly realized that they could increase their return on investment by forming pools. This is a major departure from the zero-trust model because members of a pool have to trust each other and their leader.

As of mid August 2014, the largest pool controls 29% of the hash rate, two pools control 51%, and the seven largest pools control 75% ([BLOCKCHAININFO_POOLS]). Note that these figures are based on voluntary disclosures. There is no easy way to detect secret collusions between pools.

Recall that most players in the Bitcoin industry consider a transaction finalized after six confirmations (i.e. 1 hour). This number used to guarantee less than 0.1% fraud under the historical assumption that no node would ever control more than 10% of the hash rate. But now that one organization is known to control almost 30% of the hash rate, the risk associated with six confirmations has risen from 0.1% to 18%. To bring the risk back to 0.1%, users should wait 25 confirmations, i.e. 4 hours (source: [BITCOIN], page 8).

3.15. Myth #15: Double-spending attacks will never happen because they would result in a net loss for the perpetrator

It is true that massive double-spending attacks require significant hashing power. Such attacks would undermine the credibility of Bitcoin and therefore reduce the value of the perpetrator's stolen bitcoins and hardware investments. However:

- Various organizations may decide that they would profit from the destruction of Bitcoin. It is a matter of cost versus benefit.
- Mining hardware would not lose value if it can be retargeted toward another virtual currency scheme which uses the same hash function.

3.16. Myth #16: Bitcoin security does not depend on trusted third parties

Ignoring the problem of monopoly mining pools, it is true that the Bitcoin system does not involve trusted third parties. Bitcoin is possibly the first virtual currency with that property.

However, this assumes that the protocol and the rules of mining are fixed forever. But Bitcoin is still evolving, and changing the rules sometimes requires consensus at a higher level than the blockchain. In practice decisions are taken informally by a community of entities with conflicting interests:

- **Miners .** They appear to have a long-term stake in Bitcoin because of their infrastructure investments, but note that the hardware typically becomes obsolete after 6 months. Still, miners would object to any protocol modification that renders their ASICs instantaneously useless.
- **Exchanges .** As customer-oriented businesses with marketing investments, they probably have a slightly longer-term stake in Bitcoin. Exchanges have to deal with traditional banks and with financial regulators. For example, exchanges based in the U.S. are undoubtedly money service businesses. If a choice had to be made between privacy and legal compliance, mainstream exchanges would certainly favour compliance. Most exchanges already require personal identification from their users. Some of them voluntarily refuse to process bitcoins coming from with disreputable services such as unlawful gambling.
- **Core developers .** There is a reference Bitcoin protocol implementation and a group of core developers whom users trust to fix all problems. On two occasion (August 2010 [https://en.bitcoin.it/wiki/Incidents#CVE-2010-5139] and March 2014 [https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki], software bugs caused the blockchain to fork, and the developers ultimately decided which branch was canonical. Note that this meant retroactively invalidating transactions recorded on the other branch.

- **Merchants (including workers paid in bitcoins) .** Ultimately they are the ones who will define the usefulness, and therefore the market value, of bitcoins. But most merchants do not have a long-term commitment to Bitcoin. They are willing to receive payments in traditional currencies via trusted third parties who handle the technical details of Bitcoin transactions, as long as the fees are lower than what credit card companies charge.

3.17. Myth #17: Miners, acting out of self interest, will collectively prevent a 51% monopoly from emerging.

Classical economic theory postulates that anyone with mining resources will choose rationally between these two options:

- Join the largest pool in existence, and take responsibility for pushing the system a little bit toward the 51% monopoly doomsday scenario.
- Join a smaller pool, and immediately accept a lower return on investment.

The optimal choice depends on the perceived cost of the 51% scenario. History suggests that markets do not fear it, otherwise exchange rates would have crashed in January 2014 when a well-known mining pool approached the threshold, and again in June 2014 when it probably exceeded it despite earlier assurances [https://bitcoinfoundation.org/2014/06/centralized-mining/].

See also: diffusion of responsibility and tragedy of the commons.

3.18. Myth #18: Bitcoin is already too big to fail

Based on the figures in Section 3.7, “ Myth #7: As a currency and a payment processing system, Bitcoin is efficient ”, anyone can double the current hash rate (and therefore control half the resulting total rate) at a cost of 140 million USD in hardware investments and 554,000 USD per day of operation. The cost of such an attack is even lower if the perpetrator is able to simultaneously kick a few large pools out of the network, e.g. with a denial of service attack, or by sabotaging their power supply, or simply with a legal injunction. Besides, large players could probably negotiate better prices on the hardware, obtain free electricity from idle nuclear plants, and find a use for the waste heat.

The perpetrator would then be able to claim 100% of the mined coins, i.e. 25 coins per 10 min as of mid August 2014. Assuming exchange rates remain stable despite the attack, break-even would be achieved in four months.

These amounts would be pocket change for a coalition of banks or governments intent on destroying the credibility of Bitcoin. Expensive bets are not unheard of in the financial sector.

3.19. Myth #19: "Blockchain technology" will outlive Bitcoin

Whenever Bitcoin experiences a downturn, proponents tend to emphasize so-called "blockchain technology" instead. It is true that worldwide, decentralized, trustworthy and inexpensive notarization services would be useful, especially in politically unstable regions. And as long as the Bitcoin blockchain exists, free-riding services can use it to permanently record all sorts of non-financial transactions.

Unfortunately, blockchains cannot be simultaneously trustworthy and inexpensive. The only reason people spend 250 million USD per year on Bitcoin mining (as of August 2014) is because they get their money back in the form of freshly-minted bitcoins. A blockchain dedicated to notarizing, say, real-estate transactions for free would not be able to reward its miners in the same way.

Besides, a notarization service is worthless without an enforcement mechanism. The Bitcoin blockchain is its own enforcement mechanism, because bitcoins do not exist outside of it. But how would a blockchain resolve disputes about real-estate transactions ? And who would ultimately decide which blockchain is legitimate for each type of transaction ?

4. How email became centralized

Bitcoin aims to replace traditional currencies in a way that is reminiscent of how email replaced postal mail.

SMTP, the protocol which defines modern email, is decentralized and peer-to-peer: Anyone can set up MX records in the DNS so as to have email delivered directly to their workstation. That is how things worked in the late 1980s.

But administering an always-on Internet-facing server is a lot of work, so eventually the IT departments of universities and large companies found themselves managing email accounts on behalf of thousands of users. Then in the late 1990s the Internet went mainstream and ISPs started handling email for millions of customers. Fast forward to 2014: Gmail has 500 million users, Outlook.com (formerly Hotmail) has more than 400 million, and Yahoo Mail has a few hundred million too.

This shows that most users are willing to sacrifice privacy and control in exchange for access to a free, easy to use service.

5. How public-key cryptography became centralized

When it was (re)discovered in 1977, public-key cryptography was heralded as a revolution that would allow individuals to communicate securely without depending on secret keys issued by trusted third parties.

Almost 40 years later, the decentralized web of trust model pioneered by PGP has failed to capture the imagination of the general public, and every mainstream operating system trusts a few hundred certification authorities, some of which have been hacked, coerced or bribed into issuing fake certificates for prominent Internet domains such as google.com, yahoo.com and microsoft.com.

This shows, again, that most users are not interested in taking charge of security matters.

6. The Bitcoin endgame

6.1. Phase 1: Centralized mining

We have seen that from a business perspective, it does not make sense for miners to refrain from crossing the 51% threshold. All it would take for centralization to happen right now is a behind-the-scenes handshake between the leaders of a few large pools. Representatives of the Bitcoin mining industry "accounting for 30% of the world's hashing rate" are reportedly already holding private meetings [http://www.coindesk.com/private-china-meeting-bitcoin-mining-industry-leaders/].

The libertarian advocates of Bitcoin should rejoice that pure unregulated capitalism is giving birth to a natural monopoly in just a few years, exactly as economic theory predicted.

What happens after a pool publicly claims monopoly status ?

- Bitcoin will not die overnight. The newly established mining monopoly will not immediately abuse its power. It will run the Bitcoin ecosystem as a benevolent dictator, receiving 100% of newly mined bitcoins. Most users will not even notice.

- The mining monopoly will actually be able to provide better service, e.g. real-time transaction confirmations and guaranteed rejection of double-spending attacks.

On the other hand:

- Bitcoin will not be decentralized and trust-less anymore. This will be a major turn-off for the users (now a minority) who adopted it for ideological reasons.
- The mining monopoly will become a single point of failure. Even if its rational interest is to keep Bitcoin alive, it may be coerced into acting otherwise, or convinced to sell out for a good price.
- At this point the proof-of-work scheme will be useless. However, to fend off challengers, the mining monopoly will have to keep investing in hashing power, at great financial and environmental cost. Therefore the mining monopoly will suggest protocol modifications that will effectively designate it as the central authority.

In the long term, as mining becomes less profitable, the monopoly will try to profit from its position in other ways:

- Users will find that their transactions clear faster if they voluntarily pay a larger tip.
- The mining monopoly could also offer privileged access, peering agreements and other value-added services to large players in the Bitcoin ecosystem.
- Or the mining monopoly will simply change the rules, e.g. it could raise the ceiling of the monetary base beyond 21 million.

6.2. Phase 2: Centralized governance

Ultimately users will realize that Bitcoin is not what it used to be. This may happen quickly if the mining monopoly finds itself having to make decisions on polarizing issues such as:

- Privacy versus regulatory compliance
- How to blacklist stolen bitcoins
- Whether Bitcoin needs a mechanism to reissue stolen or lost bitcoins (after they have been black-listed)
- Whether to ban gambling and laundering services
- How far back in time any form of taint analysis should apply
- How to respond to legal injunctions, e.g. seizures of bitcoin assets.

At this point the user community will expect someone to step in and take control. The Bitcoin foundation [https://bitcoinfoundation.org] will immediately come to mind, but a coalition of exchanges might be better equipped to fight the mining monopoly. Several technical solutions will be considered:

- Periodic checkpointing of the blockchain. Unfortunately decentralized checkpointing is a form of distributed consensus, i.e. the very problem that the blockchain was supposed to solve. Therefore this approach would probably require some kind of centralization.
- Forbid miners from exceeding a fixed portion of the total hash rate (say, 10%). This would require putting a central authority in charge of micromanaging them, to prevent behind-the-scenes collusions.
- Make the consensus system more democratic, as in "one person, one vote" instead of "one gigahash/s, one vote". This would require registration, i.e. the end of anonymity.
- Switch to a hashing function that is less amenable to hardware optimization, i.e. restore the original "one computer, one vote" concept. This would still favour miners with cheap electricity, and bring back botnets.
- Abandon proof-of-work and switch to proof-of-stake [https://en.bitcoin.it/wiki/Proof_of_Stake], i.e. "one bitcoin, one vote". This might incentivize users to pool their stakes (i.e. their assets) into banks.
- Periodically designate new miners at random, as in sortition. But the chosen ones might be tempted to sell their privilege to the highest bidder.

See also: Prohibited changes [https://en.bitcoin.it/wiki/Prohibited_changes], Hardfork Wishlist [https://en.bitcoin.it/wiki/Hardfork_Wishlist].

Most of these approaches would inevitably split the Bitcoin community. And the very necessity of such fundamental changes would severely undermine the credibility of Bitcoin and virtual currencies in general. Therefore, the most likely outcome is that nothing will change. Control over Bitcoin will be shared between the mining monopoly and the central governance body, each having the power to destroy the system if the other abuses its position. Note that three core developers already have the ability to broadcast emergency messages to all users [https://en.bitcoin.it/wiki/Alerts].

The governance body will define policies, reasonable fees and terms of use. The mining monopoly will run the infrastructure. Governments will easily coerce both into abiding by financial regulations.

Hopefully all parties will eventually agree on abandoning the wasteful and now useless proof-of-work scheme.

At this point the Bitcoin network will look very much like the VISA/MasterCard ecosystem, except more open and more flexible. Note that with proper security measures (chip and pin) and anti-trust regulation, an international credit card payment system can already operate with an overhead as low as 0.3% [http://www.europarl.europa.eu/news/en/news-room/content/20140219IPR36454/html/MEPs-back-cap-on-card-payment-fees]. This sets a benchmark for Bitcoin and all other virtual currencies.

6.3. Aftermath

Will centralization kill Bitcoin ? Probably not. The Internet does need a form of programmable money. For many applications, users are willing to give up on the ability to dispute charges, in exchange for flexibility and savings.

Will centralization weaken Bitcoin and allow another virtual currency to replace it ? Not necessarily. As regulation draws Bitcoin out of the underground economy, alternative currencies will fill the void in that market. But for mainstream use, although Bitcoin is far from perfect, it has proven that it is good enough and it enjoys first-mover advantage in an industry with a powerful network effect. Micropayments and offline transactions will be handled via trusted third parties, whose power will remain limited as long as the core of Bitcoin remains autonomous (at least in theory).

7. How to avoid centralization

7.1. Mining quotas

Can centralization be avoided ? Not without sacrificing at least one of the defining properties of Bitcoin.

In this section we argue that enforcing mining quotas is possibly the least damaging course of action.

For example, quotas could be allocated to nations based on GDP or on some measure of political influence (details are left as an exercise for the reader).

Mining quotas are not as incompatible with the spirit of Bitcoin as they appear. After all, Bitcoin already has a built-in production quota: no more than 25 bitcoins per 10 min (as of August 2014). The purpose of quotas would not be to control who is allowed to run the ASICs, but to decentralize control over which transactions are allowed to make it to the blockchain. It does not even matter if all nations decide to outsource the hashing work to China or to Iceland, as long as they prepare the blocks themselves and independently from each other.

Why allocate quotas to nations rather than, say, to individuals or corporations ? The rationale is that nations are natural competitors, and mutual distrust is exactly what is needed to prevent centralization. A variety of political trends and societal values would be reflected in the ways nations organize their share of the mining work and make use of their bitcoins. If all nations were to unite under a world government with unified financial regulations, saving Bitcoin would be the least of its advocates' worries.

The DNS is also decentralized into national top-level domains (plus a few transnational ones) each with its own policy. This promotes freedom of choice for users.

7.1.1. Benefits of mining quotas

- Quotas would solve the 51% monopoly problem, which is arguably the main threat to Bitcoin and the gateway to complete centralization.
- Quotas are a well-understood solution for markets which suffer from the tragedy of the commons.
- Quotas could slow down the arms race between miners and therefore reduce the environmental impact of mining.
- By design, mining is a portion of the Bitcoin ecosystem that is bound to become irrelevant anyway. 62% of the target monetary base has already been mined.

7.1.2. Benefits of national mining quotas

- National quotas would protect Bitcoin from overbearing regulation, because governments would have to reach consensus before drastic policies can be enforced at the blockchain level.
- Overseeing mining fits well with the historical tradition that governments strive to control the issuance of money, but not so much its day to day use.
- Getting governments involved would help legitimize Bitcoin as a mainstream currency.

7.1.3. Drawbacks of mining quotas

- Small-scale anonymous independent mining would become impossible. But it is already unprofitable anyway. In other words, mining quotas would safeguard fair and open access to the transaction system, at the cost of turning mining into a closed supervised oligopoly.
- Ideally, mining quotas should be enforced in a decentralized, trust-less manner. This requires consensual modifications to all Bitcoin software. In practice exchanges would be the easiest to convince, and everyone else would probably follow.
- Maybe the devil lies in the details and there is no practical way to enforce mining quotas in a decentralized manner.
- Miners would have to disclose their controlling interests and generally be much more transparent than they are today. But we believe that regulation and transparency are coming anyway.
- We have hypothesized (Section 3.9, “ Myth #9: The recent rise in exchange rates must reflect massive demand for bitcoins ”) that over-investment in mining might be one of the reasons for the current bubble (2013-2014) rather than merely its consequence, due to the unusual design of the Bitcoin money supply. As quotas would reduce the incentive to over-invest, exchange rates are likely to fall. It is unclear whether Bitcoin is already mature enough to reach a stable market value disconnected from mining costs.
- Mining quotas do not address the centralization of governance, which could be triggered not only by the emergence of a mining monopoly, but also by a variety of other crisis scenarios.

7.2. A generalization: maximally-distrustful oligopolies

The idea of national quotas fits well with the whole "mining" and "bitcoins-as-gold" analogy. But we are aware that the Bitcoin community might reject it for ideological reasons. In this section we propose a more general line of reasoning.

Let us start from the beginning. Bitcoin aims to provide a payment system without trusted third parties. This can be achieved by maintaining a public, decentralized ledger of all transactions. From the Byzantine generals' problem, it is known that distributed consensus on the content of this ledger can be achieved if and only if the proportion of dishonest participants is bounded.

Unfortunately, since Bitcoin also aims to provide anonymity, there are no participants to speak of in the first place. Therefore, Bitcoin must resort to an external, decentralized and reasonably fair metric in order to allocate decision rights. That is what proof-of-work is for. Hence the notion that "Bitcoin users vote with their computing power".

We have already mentioned alternatives such as proof-of-stake and pseudo-random selection of who gets to build the next block. But all these systems are biased toward centralization because votes can be bought. Whenever miners join a pool, they are effectively selling their right to debate which transactions make it to the ledger.

Centralization is not inherently bad (actually, it can yield economies of scale). Concentration of power only becomes dangerous when thresholds are crossed, e.g. resulting in the tyranny of the majority. A permanent oligopoly of three equally sized mining pools would make Bitcoin safe and efficient. Unfortunately it is well known that oligopolies tend to turn into cartels through secrets agreements.

Since *a posteriori* antitrust regulation would be impractical in an open, decentralized system with anonymity, we propose instead to deliberately engineer the oligopoly so as to minimize the risk of collusions. Hence the concept of maximally-distrustful oligopolies. In hindsight, adopting national mining quotas boils down to recognizing that centuries of wars and economic competition have shaped the world into an oligopoly of naturally distrustful entities: nations.

8. Acknowledgements

Thanks to Stéphane Gourichon for reviewing an earlier version of this document.

9. Post-scriptum

This article was originally written in mid-2014. Here is the situation two years later:

- Mining is still centralized, but pools do not approach the 50% threshold anymore. Hashrate distribution is quite stable, with a leading pool near 30% and the second and third pools totalling another 30%. Needless to say, this is too perfect to be the result of a natural market equilibrium.

- The consensual governance of Bitcoin has been shattered by debates about minor technical issues:

  - The (re-)implementation of Replace By Fee (RBF) [https://en.bitcoin.it/wiki/Transaction_replacement], a feature which highlights that Bitcoin transactions cannot be instantaneous.

  - The block size limit controversy [https://en.bitcoin.it/wiki/Block_size_limit_controversy], which includes an interesting dilemma for the credibility of Bitcoin: On the one hand, if the *status quo* is maintained, then Bitcoin will not scale and will not be able to compete with mainstream payment systems. On the other hand, if the block size limit is increased, then users will realize that the rules can be changed at any time (including possibly those about the monetary base ceiling and the permission-less nature of Bitcoin).

  As a result, several entities are fighting for control of Bitcoin.

- Various financial institutions are embracing "blockchain technology" and discussing plans about private blockchains. But without decentralized mining, a blockchain boils down to a notarization service operated by a trusted third party. At best, private blockchains will allow competing institutions to keep each other in check, as envisioned in Section 7.2, “ A generalization: maximally-distrustful oligopolies ”.

Bibliography

[BITCOIN] *Bitcoin: A Peer-to-Peer Electronic Cash System* . Satoshi Nakamoto. https://bitcoin.org/bitcoin.pdf.

[BLOCKCHAININFO_STATS] *Bitcoin Statistics* . http://blockchain.info/stats.

[BLOCKCHAININFO_CHARTS] *Bitcoin Charts* . http://blockchain.info/charts.

[BLOCKCHAININFO_POOLS] *Bitcoin Hashrate Distribution* . http://blockchain.info/pools.

[BITCOINIT_MYTHS] *Myths - Bitcoin* . https://en.bitcoin.it/wiki/Myths.