How to succeed in Bitcoin's command economy

By Tim Swanson

Summary:

- The network contains an inelastic monetary policy that does not integrate with our historical insights about self-interest and profit sharing contracts
- Due to its centralized governance and production method, there are conflicting stakeholders at the core of Bitcoin which determine its direction and evolution
- One size fits all policy leads to lobbying by special interest groups limiting some long-term business opportunities – legal specialization is used as a concluding example

As noted in my recent article, the Bitcoin network (as nearly all other cryptocurrency networks) operates very similar to a command economy. This is done through the arbitrary reward mechanism built into the protocol. And as noted later below, despite the challenges there are probably several ways to bring value to this space using blockchains.

Before we discuss that though, historically one way command economies were characterized in the 20th century is one in which a committee arbitrarily set wages irrespective of the amount, type or quality of labor involved. For example, in China, wages for doctors are still set at a flat rate by a planning commission, roughly 3,000 RMB per month (or 10,000 RMB per month in some cities) irrespective of the amount of patients you see (sometimes up to 100 a day) or quality of care you provide. Coupled with an explicit profit-sharing agreement with pharmaceutical companies through drug prescriptions, this has led to a number of perverse incentives for *underpaid* doctors to overprescribe medicines (which they receive commissions from) to compensate for their relatively meager salaries (I wrote a whole chapter about this issue). For comparison, according to a 2013 report from the Bureau of Labor Statistics, the mean annual wage for physicians was $187,200 in the US.

How does this tie in with Bitcoin mining?

Any organization with limited resources will eventually run out of its assets if it continues in this fashion (coincidentally the Bitcoin Foundation itself has a 40% burn rate). And this is also what happens with the Bitcoin network which only has 21 million bitcoins in its 'trust fund' (to reuse an apt analogy). To incentivize early adoption, Satoshi Nakamoto, the creator, used an asymptote distribution method which essentially front loaded the reward cycle to the point where approximately 62% of all bitcoins have already been distributed in less than 6 years. The remaining will be similarly rewarded over the next 100 years. As detailed below, the reward schedule has not matched security incentives (block rewards) with security requirements (economic activity).

One of the purportedly core strengths of bitcoin (the currency) is that it follows a strict, inelastic monetary expansion hardcoded since day one.

Or in other words, there is no merit-based mining, all wages for the labor (mining) were arbitrarily set for perpetuity on January 3, 2009 and henceforth divvied out irrespective of economic conditions.

While this may sound like a strength to those who view monetary policy through a binary lens, this artificially caused distortions to the incentive and motivational mechanisms and has sustainability ramifications now that the network actually contains some commercial transactions.

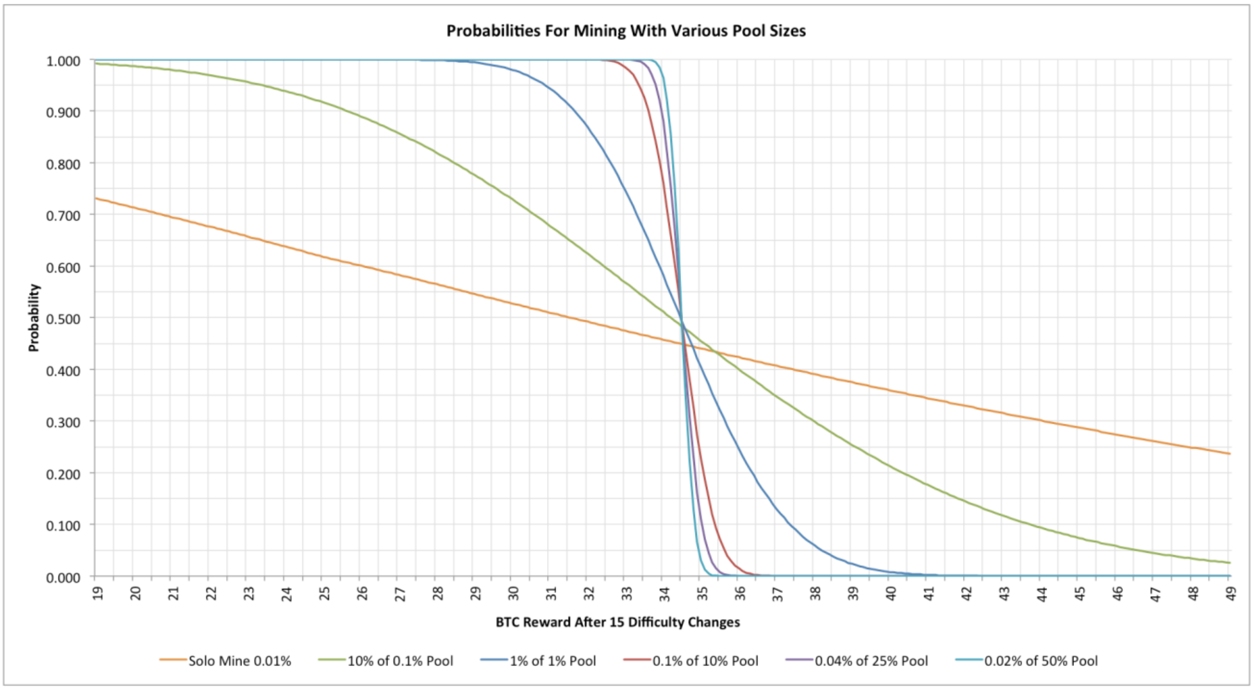
I contacted Blockr.io and they provided the following data (that was cross-checked with Blocktrail):

- There are 84,580 blocks with "empty" blocks containing just coinbase transactions (a coinbase reward is the first transaction of a block, going to the miner who found the lucky number)
- 83,867 blocks were rewarded 50 bitcoins each prior to the first halving day in November 2012, the remaining 713 blocks received 25 bitcoins
- There are an additional 12,404 blocks with 2 transactions (the coinbase transaction + one other)
- 12,223 of these blocks came prior to the block reward halving in November 2012 which equates to 611,150 and another 181 blocks each received 25 bitcoins (amounting to 4,525 bitcoins)

Altogether this comes to roughly 4.8 million bitcoins (~37%) of the nearly 13 million total mined thus far that have been indiscriminately rewarded to labor participants, many of whom as I noted before, had very little downside risk of securing the network in the first couple of years (just turn on a laptop). In other words, unlike in other resource extraction-based industries (like gold mining as described by Hass McCook) there was no merit or performance-based decision making as hashers are rewarded for securing (mining) what are essentially transactionless blocks.

The mining pool Discus Fish (F2Pool) is a notable contemporary example in that they occasionally include only one transaction into a block (perhaps zero looks bad for PR reasons). While speculative, there is some economic rationale behind it, because in practice, the smaller a block is, the faster a miner can broadcast and propagate it leading to less orphans. Or in short, they are maximizing profits. Further research will likely uncover the timing incentives (i.e., is it really just milliseconds or does it aggregate into larger non-trivial units of time?).

As described above, the network rewards quantity of hashrate and not transaction processing (e.g., amount or type of transaction). As a consequence you have participants that understandably try to capitalize off the system by pooling as much hashrate as possible sometimes without including transactions: why should they expend extra effort for little reward?



What is the incentive for pooling? The above chart was recently published by Dave Hudson, a network engineer and statistician. In the past he has discussed the Poisson process within Bitcoin, how the fluctuating variance in payouts creates incentives for centralization. This chart shows the net results of running a Monte Carlo simulation 10 million times. The key finding is that there is an incentive for miners to all use large pools to smooth out their variance or in Hudson's words, "The larger pools are definitely more attractive to anyone seeking predictable returns." Thus, investors with expected return on investments would rather be safe than sorry as anything less than a large pool is effectively gambling on lower probabilities.

What does this have to do with including transactions? Again, while more research will be needed to solidify the motivations for doing so, faced with the variance shown above there may not be a financial incentive to necessarily include transactions (or many transactions) within a block (because the fee reward pales in comparison to the seigniorage subsidy).

This in turn results in potential free-rider issues – a conundrum that Gavin Andresen pointed out last year. It also leads to the question of: who are the actual decider(s) of this system?

One common rejoinder is that in the first few years there were no transactions or few transactions to include – that the first year alone was essentially no commercial transactions.

True, but a rational company, country or organization with a flexible ability to allocate scarce resources would simply, dynamically lower the amount of rewards. So instead of receiving 50 bitcoins perhaps the miner would receive 1 bitcoin. It is unclear what the number should or should not be because there is no market process involved; the rationing of resources is arbitrarily done irrespective of the underlying conditions – just as the rationing process in command economies is.

Similarly, in its first several years of development, the general idea was that the economic activity on the network would result in a higher incentive to secure the network and that mining is simply the provision of security. This may still be the case long-term, however the data from the blockchain itself does not lend support to this particular interpretation.

To try and change this or set a minimum amount of transactions that need to be processed would introduce other unintended consequences that are part and parcel to price floors or minimum wages (i.e., recreational miners demanding "living wages"). Future analysis can be done on the possible changes that can not only be done but also explore ways to incentivize miners to adopt those changes (i.e., one view is that miners collectively have a long term interest in the networks health and rapidly depreciating capital supposedly makes them more adept to change).

An inelastic economy

One consequence is that this leads to what Hungarian economist János Kornai called a shortage economy. While Kornai was describing the effects of central planning on consumer goods, as I have previously noted, there is a shortage of bitcoins (credit) in the bitcoin economy. In other words, the Bitcoin economy is in a perpetual credit crunch. That growth cannot expand through lending facilities because its user base (bitcoin holders) are collectively funneled into only one option: non-interest bearing mandatory holding accounts – or what some advocates eagerly refer to as hoarding. Businesses need financing, loans or some kind of investment in order to get off the ground and scale yet because there is no real banking system within Bitcoin, the economy recreates that of a 100% full reserve system. This is a bug. (Note: for balance there are some non-ideological proposals surrounding full reserve banking solutions from John Kay and Martin Wolf)

And consequently most entrepreneurs within the ecosystem thereby need to rely on foreign currency and capital – flexible fiat-based credit – outside the Bitcoin ecosystem, to build the Bitcoin ecosystem.

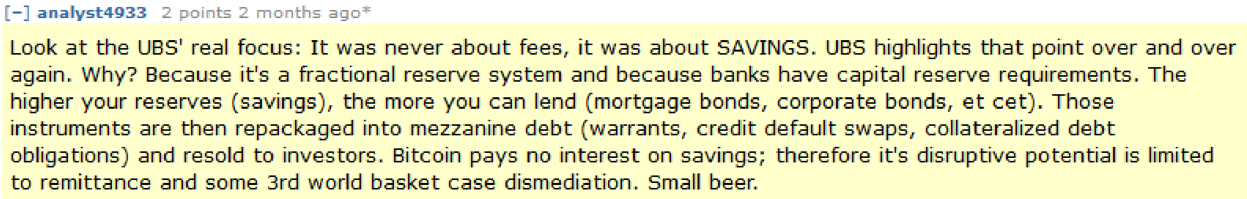
Incidentally this is not a historical anomaly: nearly all emerging countries go through similar hurdles to attract capital, opening up lines of credit denominated in foreign currencies and stockpiling foreign currency reserves in part to provide settlement of debt obligations with trading partners (see also Trilemma). Yet the inability to natively create credit or lending instruments dramatically handicaps the growth and expansion of the network.

For a more thorough explanation there are three thought provoking papers that critically examine these issues: The False Premises and Promises of Bitcoin by Brian Hanley, Hayek Money: The Cryptocurrency Price Stability Solution by Ferdinando Ametrano and Inv and Sav Wallets: The Role of Financial Intermediaries in a Digital Currency by Massimo Morini. Hanley notes that, "Bitcoins, since they cannot be used in reserve banking, can only be hoarded, spent, or lost, not saved in the usual sense it is thought of in the modern world."

Similarly, Morini states that:

> Denominating salaries or financial payments in bitcoins would be unthinkable today: from April 15, 2011, to March 29, 2014, the USD/BTC (dollar/bitcoin) rate of exchange moved from 1 to 500. This would mean a 500 times, or 50,000%, change in the dollar value of salary. Also loans are unthinkable when prices are strongly unstable.

This presents a challenge: in order for Bitcoin to replace the banking and financial institutions that some of its promoters claim it will do, then it will necessarily have to provide instruments they previously created, sold and managed. One adroit reddit user pointed this out several months ago regarding the possibility of banks such as UBS "absorbing the benefits" of Bitcoin:



[–] analyst4933 2 points 2 months ago*

Look at the UBS' real focus: It was never about fees, it was about SAVINGS. UBS highlights that point over and over again. Why? Because it's a fractional reserve system and because banks have capital reserve requirements. The higher your reserves (savings), the more you can lend (mortgage bonds, corporate bonds, et cet). Those instruments are then repackaged into mezzanine debt (warrants, credit default swaps, collateralized debt obligations) and resold to investors. Bitcoin pays no interest on savings; therefore it's disruptive potential is limited to remittance and some 3rd world basket case dismediation. Small beer.

As previously noted, there are at least three companies trying to work on solutions for lending: BTCJam, Bitreserve, Bitfinex and nearly a dozen that are working on building platforms that could eventually provide other services that are lacking in that reddit comment: SecondMarket (BIT), CampBX, TruCoin, Coinfloor, Atlas ATS, Kraken, Coinsetter, Vaurum, itBit, ICBIT, LedgerX. There is even a new web-based financial firm, Delta Finance that is purportedly offering interest-bearing bitcoin accounts; and OKCoin is relaunching a P2P trading and lending service. Obviously neither Rome nor the internet were built in a day, thus given time these instruments could potentially be built out.

For perspective about using Bitcoin to perform these functions I spoke with Preston Byrne, a London-based securitization attorney and co-founder of the Eris project, the first decentralized autonomous organization (DAO):

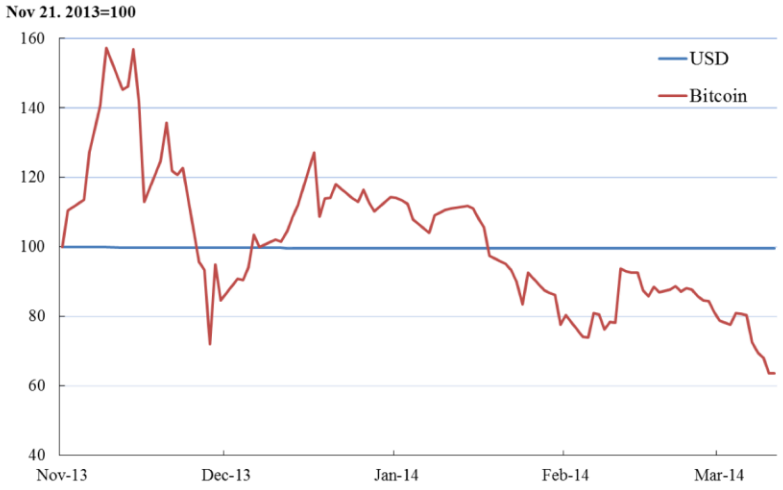
> "A bitcoin doesn't represent an obligation - there's an open question under English law as to whether a bitcoin or part thereof is even legally capable of constituting property. Because you can't enforce a Bitcoin against anyone, it'll never serve the function of a security. You could have a security denominated in Bitcoin, certainly. But given the high degree of volatility it isn't something I'd be overeager to put on my balance sheet. Most money takes the form of promises rather than specie; the world's more efficient that way."

This is a legal issue that varies depending on each jurisdiction; in the US, a few states like California have legally recognized bitcoins and on a national level agencies like the SEC has jurisdiction over their use as a security. There may be efficient solutions to this in the future (as I have also pointed out), but if history is any guide, the ecosystem is more reminiscent to pre-industrialized agrarian countries set on an inelastic commodity-based (gold) standard. Those with gold can absorb the purchasing power of the country – thereby increasing their own wealth – without actually creating new value or utility. This creates a feedback loop – similar to a prisoner's dilemma – since gold owners continue to have this incentive to simply hold; why risk spending or investing when you reap the benefits of those that do take risks?

For balance, perhaps, one could argue that the above statements do not fully do justice to the fact that the reward does vary based on the economic situation. It is, as some argue, just that it varies in dollar terms, not in bitcoin terms. Below is a chart representing this volatility from a presentation by David Andolfatto, Vice President at the Federal Reserve Bank of St. Louis:

Purchasing Power of Bitcoin and USD

Nov. 2013 – Mar. 2014



Source: Bureau of Labor Statistics, Haver Analytics and Bitcoincharts.com

According to Andolfatto, this illustrates that bitcoin would and does make a poor currency due to its rapid volatility relative to other money (e.g., USD, euros) which “maintain a stable purchasing power over a short period of time.” There are some adopters who disagree with this statement, however the current data reinforces Andolfatto’s position (i.e., a dearth of commercial activity on the blockchain) – perhaps this could change over time, but that is not knowable *a priori* as it is an empirical scenario.

Deciders

Another core attribute of command economies is that they typically do end up having some decider (a “strongman”) who invariably decides the course of action. In the case of Bitcoin, the deciders are mining pools who *understandably* will only secure code that is profitable to them – after all, it is their depreciating capital goods (mining equipment) that provides the entire utility for the network, why can’t they decide what to do with it? As a consequence they each decide which transactions to include (or what to leave in the mempool), what blocks to propagate (or potentially refuse) and what fees (if any) to set. And these issues are likely to become more prominent as the mining becomes more professionalized.

Simultaneously, another group of stakeholders are the core developers, who have proposed a myriad of clever, innovative features, but there is no immediate incentive for miners to currently adopt these changes. We saw this with the deliberation over the size (40 bytes versus 80 bytes) for OP_RETURN in March as well as the debate over the double-spend as a service startup (BitUndo) the following month. As a consequence, the challenge Mark DeWeaver noted several weeks ago related to special interest groups and emerging countries bears repeating:

> “The thing about developing economies is that they usually seem to be held hostage by special interest groups that insist that development must proceed along a path that doesn’t threaten their interests. So they tend to end up with what the political scientist Fred Riggs called

> "prismatic development"— a Potemkin version of the development seen in advanced countries. If it's like a developing country, it could be stuck where it is now pretty much forever."

Navigating these issues may just be a matter of growing pains, perhaps as the industry matures there will be less friction in these areas.

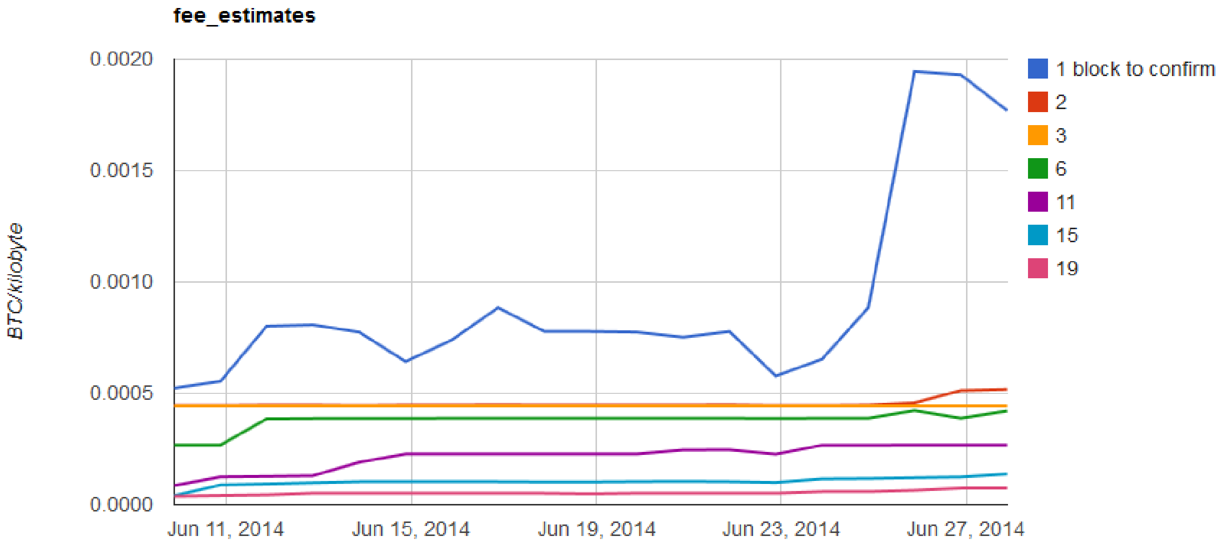
$40 transactions

Perhaps the most contentious area that I have received feedback is regarding my assertion that the full costs of transacting on the network is being grossly understated. It is not free, it is around $40 at the time of this writing (paid through via token dilution).

As I recently explained in several emails, there are actual infrastructure costs that some adopters hand-wave away as if it is run by magic. Collectively most of the mining labor force will not achieve an accounting profit (let alone an economic profit); relying solely on the appreciation of the token to pay for their costs. Conjoined with an automatically adjusting difficulty rating, proof-of-work via Hashcash or scrypt (which are not the only types) ensures that the marginal value of a token in the long run equals to the marginal cost of securing the network (MV=MC); and as Tadge Dryja notes in the video below the marginal product of labor (MP_L) is zero (a phenomenon that David Evans addressed at length in April). Thus, as I point out in my last piece, it is enormously costly in terms of security relative to other payment and value transfer mechanisms.

Obviously the ratios will shift back and forth throughout time, but decentralization axiomatically insures it cannot be cheaper or faster payments system than a centralized real-time gross settlement (RTGS) platform. Perhaps Peter Todd's tree-chain solution, Adam Miller's Permacoin (video), Proof-of-Activity from Bentov *et. al.*, or even the clever Proof-of-Idle (video) from Tadge Dyrja will be implemented in code, but again, why would existing mining pools or farms protect code that is unprofitable relative to their sunk costs (most have not even upgraded past 0.8.5. or 0.8.6 software still, what upgrade would fall within their time horizons)? The changes so far are not enough to get farms and pools to change yet a hard fork risks a serious network partition.

Another way to look at it is this, if block rewards were entirely removed today, how much of the labor force could continue providing their services in a profitable manner? The answer is probably none as 99.80% of revenue at the time of this writing comes from the seigniorage subsidy. Hashrate would drop to an equilibrium relative to the transaction fees (or as Kerem Kaskaloglu calls them, "donations"). Since the number one marketing slogan for the network is "transactions are free" you could very well end up with a network that could be insecure from relatively cheap outside attacks because few are willing to pay fees high enough to incentivize that same level of security.



The chart above was recently published by Gavin Andresen and illustrates bitcoin fees paid versus blocks-to-confirm over the past two weeks. Or in other words, the higher the fee a user is willing to pay, the faster their transaction is included in a block (and thereby confirmed). At a lower fee of around 0.0001 bitcoin (1.6 cents at current prices), 19 confirmations is roughly 3 hours of waiting time.

For comparison, the average network and processing expense per Visa transaction ($414 million / 77.6 billion transactions) is $0.0053. Similarly, the direct transaction costs for remittance firms like Western Union are relatively low. Instead, the fee assessed on top of the transactions (for Visa the 2.5% + $0.20 or for Western Union, global average of 9%) goes towards paying for insurance, legal compliance, brick-and-mortar physical locations, fraud protection and human network on the ground (these same costs will likely be levied onto Bitcoin ATM remitters as well; it is not zero percent).

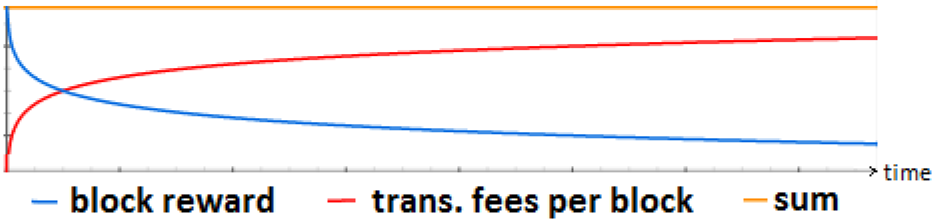
Again, this is not an entirely apples-to-apples comparison because both of these networks just transmit information and are not money creation (seigniorage) networks as well (which Bitcoin is).

For instance, because there are, on average, 3,600 bitcoins created each day and a lowerbound cost of securing these is currently around $600 (MV=MC), the actual operating costs of the Bitcoin network are around $2 million a day or $730 million a year (see Estimated costs). When taken into account the relatively low volume of commercial activity on the same network relative to Visa or Western Union, the per transaction and security costs of Bitcoin are very high (as noted in my previous article). For future cryptoledger designers, these variables may be tunable with agent-based modeling (ABM) such as that proposed by Dave Babbitt (forthcoming) yet due to the *cui bono* mention above, it is unlikely that this can be changed for Bitcoin itself. Leading Jonathan Levin, co-founder of Coinometrics, to wonder "who will break the social contract first?"

Again, in practice, a centralized system will be more efficient – copying a transaction once and then twice for security while applying SSL encryption only once is much more efficient than copying all transactions tens of thousands of times over and expending large quantities of energy to maintain the hashrate for security. For instance, while it arguably would not be as secure, a user could spin up a virtual machine and database on any number of cloud platforms to recreate the same transportation functions as Bitcoin for a fraction of the cost.

Similarly, Bitcoin has the same fraud and theft issues as Visa – as many as 30% of all mined bitcoins have been lost, stolen, seized or destroyed (see Information security is hard). For Visa, these vulnerabilities are on the edges and not in the data centers (e.g., 40 million Target accounts being compromised). However, Bitcoin has no way to resolve fraud unless you increase costs through multisig services or customer service. If Bob wanted to build a system that is exactly the same as Bitcoin, he could just tell Visa to fire everyone in the fraud department, to not offer charge backs (even if the good or service is not delivered by the merchant) and to just charge people the cost of transaction plus a profit margin. He would end up with a Bitcoin-like system but with faster confirmation times as well as room for higher potential transactional volumes.

In the end, Bitcoin adopters have to pay real costs for decentralization because being your own bank can be hard and infrastructure is not free. And according to a working paper from Andrew Miller and Joseph LaViola, these costs may be "unavoidable" in order to protect against vulnerabilities such as Sybil attacks.



The chart above is from a new paper published by Kerem Kaskaloglu that illustrates the "ideal scenario" – the switch from block rewards (seigniorage subsidy) to transaction fees (donations).

Obviously the subsidy will not disappear anytime soon, but trying to incentivize people to pay fees for faster inclusion (priority) into blocks when those fees are greater than the equivalent for competing services such as other less capital intensive cryptoledgers or "rails" like Ripple, mobile payment solutions from Alipay (through Weibo), Google, Apple, or RTGS from Visa – is an uphill task.

According to the current narrative, the cost per transaction will eventually go down as the network adds more transactions per block. However the increase in transactions (e.g., the demand for the usage of the network) will also increase the price of bitcoin (due to the demand for tokens) and because the marginal value equals the marginal cost, the argument that more transaction will lower the cost per transaction is not as clear cut. This is not to say that they linearly increase, it is not that simple. Historically both the denominator and the nominator increase. Perhaps upcoming floating fees ('smartified fees') will be one potential solution to this challenge.

There is a distinct possibility that such fees could price-out a portion of the underbanked in developing countries, some of whose daily wages are less than the cost of a transaction. Perhaps it will be surmountable, however for every hardware or software boost Bitcoin receives there is a potential that other competitors such as Visa (fact sheet) could benefit from that as well.

Legal specialization

What then is a protocol like Bitcoin especially good at? Or as some people have asked, why am I still involved in this space? The world has seen virtual currencies (Beenz and Flooz), cryptographic currencies (DigiCash) and numerous commodity-standards (gold, silver, copper). Even if the "currency" aspect of bitcoin finds niches, according to preliminary research from Neil Gandal and Hanna Halaburda, it is unlikely that network effects alone will create a winner-takes-all scenario relative to other cryptocurrencies. Instead, the core innovation is the blockchain, which may be competitive at managing distributed trustlessness (a topic also broached by a recent OECD working paper). This space has also spurred the development of creative tools including a bevy of HDM wallets as well as authentication services (like up-and-coming Lastwall).

For perspective I spoke with several attorneys including James Duchenne, co-founder of Satoshi Legal and founder of SEiiAN Rewards. According to him,

> "For me, using bitcoin is a matter of choice. You can choose to trust in the laws crafted by people and their empowered third parties, or the laws of consensus algorithms. So, bitcoin is not a completely trustless system, as some would advocate, but rather it allows the possibility to shift trust from the status quo to an algorithm, the security provided by miners, the reliability of nodes and the confidence of the underlying system's economic viability.
>
> I also view bitcoin as being like the "Benjamin Button" of technology. It started its life as a currency and is currently backtracking to fulfill its promise as a distributed consensus network. Thus, it was born an adult, fought like one and is now growing towards its adolescence and *raison de vivre*. Perhaps, if it were the other way around, descriptions of it having no intrinsic value wouldn't be heard.
>
> In terms of use, I tend to view bitcoin as an "algorithmic-enforced" private contract assigning value amongst its users (in so far as price discovery exists and it doesn't contravene the laws of a relevant jurisdiction). Unfortunately, it currently sucks at that function due to its volatility. However, the point is that it is able to be the product, the registered agent, the legal system and the enforcer. Thus, implementations like coloring coins to represent an element (i.e. share, assets etc.) are kind of silly, since transacting in those "rights" must be replicated with paper work to comply with existing law.
>
> Lastly, some of the big hurdles in using bitcoin's consensus network are education, trust and liability, especially if it's to be used by the legal profession. Would an attorney, an accountant or a registrar use the blockchain as counterparty for the verification and authentication of a document or for other recording keeping purposes? They can, but it's unlikely it'll happen anytime soon. Who bears the risk if something goes wrong with bitcoin? Is it malpractice? Alternatively, someone can offer this service, keep copies of the records and bear that risk. Then why use the blockchain for this purpose? I can, however, entertain the thought of the consensus network being used in self-enforced private contracts for ownership and dissemination of digital intellectual property. While this is the promise of the consensus network, we have yet to see successful real world sustainable applications and examples."

What else can this distributed network be used for? What are some of these possibilities that Duchenne is referring to? For instance, in some places like Greece (which does not have a computerized central land title registry system), titles are held in different localities and law firms which makes the dispute over who owns a certain house complicated. For buyers and sellers this can result in expensive due diligence and fact-finding processes.

Yet, all things being equal, this notary niche is probably a bit easier, cheaper and less lawsuit prone for solutions with high infrastructure costs like Bitcoin because legalese is more semantical than the "currency" questions where uncertainty lies in many jurisdictions. For instance, in the Greek case above, a blockchain could store the metadata, the hash or even the entire land title itself.

Entrepreneurs could build companies around Proof-of-existence and Bistamped-like services such as these or perhaps, countries, communities and NGOs could use assurance contracts to fund the network through what Mike Hearn is trying to do with Lighthouse. Or maybe similar volunteer initiatives like NodeShares and "Adopt-a-node" can be done on the mining side as well (e.g., an intentional non-profit mining farm).

Attorney Pamela Morgan, founder of Empowered Law, thinks that:

> "Beyond currency, there are many uses for bitcoin technology. For example, we could create global jury pools for private dispute resolution. Participants could either provide value to the network through services, such as serving as a jury member or by paying for the service. Users of the service would have access to a more diverse, and possibly skilled, pool for dispute resolution which should result in improved outcomes. Jurors could be chosen randomly and elect to serve or not, thereby helping to prevent coercion or jury tampering. While a similar service could exist outside of the blockchain, the transparency provided by a public voting ledger would likely be the simplest and most easily implemented method."

However, according to Preston Byrne, perhaps this could still run into other hurdles:

> "Bitcoin is tremendously expensive to operate, capable of transmitting only very basic data, and even then only does so unidirectionally. It's basically ARPANET with the ability to fork - which it should do, and soon, if it is to have any chance of long-term survival.
>
> You can do virtually anything you want with a blockchain - much as you can do anything you want with software. The issue is that you have to structure it properly so that the blockchain creates the real-world impact you want in direct conjunction with the digital asset you want to transfer.
>
> Problem is, just 'colouring' a coin as one asset or another achieves practically nothing unless you can also present data which matches the token or contract and demonstrates evidence of ownership. Most of the proposals for virtual assets or title registration do not address this issue adequately, if they do so at all."

Skeptics could always be wrong, maybe this is all a replay of the Xerox Memo of the Month. Perhaps the currency or commodity aspect of bitcoin will grow beyond the niches of remittances (in corridors such as Southeast Asia), day trading and black markets. Or maybe, the current Cambrian explosion in altcoins repeats what Akinobu Kuroda elucidated of 18th century Bengal, where Dacca residents had 52 kinds of coins of different weights and measurements in circulation, each with a specific "circuit" (layered market) and use-case that fluctuated cyclically during the year. Time will tell on this front.

In the meantime, some startups to look at in this distributed asset digitization platform space include Blockstream, PeerNova and Cryptowerks.

Acknowledgements: I would like to thank the following individuals for their feedback on this article including Dave Babbitt, Preston Byrne, Hudson Cashdan, James Duchenne, Brian Hanley, Jop Hartog, Petri Kajander, Jonathan Levin, Pamela Morgan, Ratko Rudic, Chris Turlica and Jack Wang.

Disclosure: I hold no equity in any of the companies, nor was I compensated by them for their inclusion. Nor is this an endorsement of their services.