Jackson Mackeral

Bitcoin and Scalability

Today, a growing number of people believe that the current monetary system is riddled with inherent flaws. Satoshi Nakamoto succinctly summarized what he believed to be the most prevalent of these flaws:

> Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model.

The necessary trust in outside organizations is just one of the various flaws of today's different currencies. The majority of the population accepts these flaws as necessary, or is unaware to them. However, a number of critics of today's common currency propose a solution called Bitcoin, which Nakamoto first implemented in 2009.

Bitcoin is fundamentally distinct from the currencies used today in a myriad of ways. Bitcoin is decentralized. Unlike currencies like the United States dollar, and other similar government issued currencies, no singular person or organization is in sole control of the protocols regarding Bitcoin. The amount of Bitcoin introduced to the economy is limited to a finite total, and to a certain rate at which they will be introduced; Bitcoin exists in harsh contrast to other currencies which allow limitless amounts to be printed at any time. Bitcoin's value is held by the mathematics that support its function, unlike other currencies which are sanctioned by governments, which designate a value for them. These currencies with a designated value, also called fiat currencies, often have vastly inflationary natures. Bitcoin, as a general rule, is deflationary-it gains value over time (Nakamoto).

Bitcoin's technicalities allow it the advantages previously stated. Transactions take place between "addresses", which are approximately 30 character strings of numbers and letters unique to the user that owns the Bitcoin within the address. The transactions are fully recorded and publicly available. The transactions are recorded in an ever expanding "Blockchain", which groups transactions in chunks called blocks. A new Block is added to the chain about every ten minutes. Each Block references the one previous to it. The Blockchain's name reveals the chaining of Blocks as they are added.

The Blocks added to the chain must be confirmed; this job is done by "miners". These miners compute mathematical problems until one of them reaches a correct answer. The miner who arrives at a correct solution is rewarded with a large sum of Bitcoin, incentivising the process. The difficulty of these mathematical problems is scaled in relation with the amount of computing power the miners are using to confirm the blocks in order to be sure blocks are created every ten minutes. Bitcoin's security is reliant on the timing previously mentioned; the timing vastly decreases the possibility of attackers from "creating" their own blocks with false information (How Bitcoin).

Currently, the maximum Block size is capped. The cap on Block size results, since Blocks are always created about every ten minutes, in a cap on the transaction rate. The cap on the Block size was put in place to keep the Blockchain from ballooning to an unwieldy size before the network was ready to handle the complications involved.

Hesitant Bitcoin analysts often say that the majority of these protocols only give rise to concerns when and if Bitcoin becomes more widely used. They see these concerns as obstructions to the reality of Bitcoin becoming a legitimate currency as viewed by the public. These concerns are legitimate, and worthy of further discussion.

A major part of this discussion must consist of Bitcoin's scalability. The possibility must be considered that small problems that Bitcoin experiences today could become larger problems if it becomes a more mainstream currency. But Bitcoin, despite the concerns posed, is scalable.

For example, one concern often stated is the current maximum Block size. The result is, due to Blocks being created every ten minutes, to a current maximum transaction rate of about 7 transactions per second [tps]. The limit on Block size is removable. Removing it would require the majority of the network to accept the change, which would not be unreasonable, as similar changes have occurred before. The change would not require an entire new program for the nodes, just the changing of certain parameters within the client.

Despite the ease of the change, no immediate need to remove the limit exists, as the transaction rate currently peaks at around 1 tps (Bitcoin Number). Nonetheless, the concern posed is valid! The chances of Bitcoin becoming mainstream currency without surpassing 7 tps are highly unlikely. Visa currently peaks at around 47,000 tps (Trillo). Paypal averages around 100 tps (About). Various solutions to the issues that the maximum Block size could cause in the future have been proposed.

The simplest of the solutions is allowing the nodes to accept a higher Block size, as described above. Accepting the higher Block size is a fairly simple procedure, and could be implemented relatively quickly.

Until now, little has been mentioned of the maximum transaction rate being a problem. The media often misunderstands the inner workings of Bitcoin, leading to rumors of problems like the current maximum transaction rate. The rate is not a problem-yet. Currently, the maximum Block size is set as a way to allow the currency to mature before the Blockchain becomes significantly large. If a higher transaction rate were currently allowed, the possibility of a ballooned Blockchain would be immensely prevalent. Spam transactions would have a propensity to fill the majority of the Blockchain. The entirety of the transactions begin to add to a significant sum of memory required for the Blockchain. The possibility of the Blockchain becoming unmanageably large must be considered.

The ballooned Blockchain could pose a problem to the Bitcoin economy. The Blockchain is currently about 23 GB-a hefty download for most users (Bitcoin Blockchain). In the past, all users were required to download the Blockchain in order to operate. But thankfully, solutions have been developed in order for the casual Bitcoin user to avoid downloading the entire Blockchain. Various Bitcoin clients, which do not require a full download of the Blockchain, have been recently released, effectively solving the problem (Electrum). These clients are tailored for the common users of Bitcoin. The solution was originally described in Nakamoto's white paper, and has been implemented.

However, certain situations require a complete download of the Blockchain. Full nodes, for example, are an integral part of the Bitcoin economy, and require a download of the entire Blockchain (Cawrey). Full nodes take the first step in the process of adding transactions to the Blockchain; they broadcast transactions to the network. As more Full nodes "hear" the transaction, they broadcast it as well, until the network agrees upon the transaction. With the Blockchain becoming larger and larger, beginning to run a full node is becoming more expensive and difficult; downloading the Blockchain takes quite a long time, and memory is expensive. Unlike miners, full nodes are not currently incentivized by default. These considerations could come together catastrophically-if full nodes begin going offline, the network will begin to become insecure!

Thankfully, this problem has been addressed before, and solutions have been proposed. In Nakamoto's original white paper on Bitcoin, he proposed a solution called Simplified Payment Verification, which would allow users to confirm transactions without running a full node. The solution allows more users the ability to secure the network.

Users who still see this problem as urgent have often described ways to incentivise nodes to prevent the possibility of nodes losing reason to secure the network; none of these ways are overly complicated. Integral contributors in securing the network would be compensated for their help.

J. D. Bruce's white paper, *The Mini-Blockchain Scheme*, describes not only the reasons the growing Blockchain is not an immediate or even catastrophic concern, but also proposes a solution (Bruce). He details a new possible system, using various different types of Blockchains, all with different purposes, with the effect of drastically reducing the memory required to store the information required to run a full node.

Most agree that implementing all of Bruce's ideas is unrealistic because of the sheer number of changes needed. Bruce's idea of pruning the Blockchain, however, is generally seen as more realistic. Although implementing this system would require a fairly massive overhaul of the way Bitcoin works, the majority of his points still stand true without the changes he suggested. For example, he stated that "Moore's Law is still going strong for the foreseeable future." Moore's law dictates the way computers advance, and the way capabilities grow with time. If this law is to persist, storage problems will be less impactful than if they were to happen today, as technology would also scale to handle them.

In addition, Deep Space Industries Inc. and Dunvegan Space Systems have partnered to begin an initiative to launch Bitcoin nodes into space as satellites (Cawrey). These "BitSats" would be solar powered, and would provide enhanced security for the network at no continual cost.

As seen with the previous solutions mentioned, The Bitcoin community seems to rise to the challenges presented to it. Anyone with the means to aid Bitcoin is not only allowed to, but is encouraged. Graphic designers, programmers, economists, videographers, animators, engineers, or writers, no matter the talent people have, they seem to have found ways to be at the forefront of promoting Bitcoin. In the end, this nature of the Bitcoin community could be what saves it from the Blockchain size issue.

However, Bitcoin's security measures have raised environmental concerns. Every Block added to the chain has to be "mined" before it is considered legitimate by the network, which involves a process called hashing. Hashing takes any input, and creates a random output in a repeatable fashion based on the input. Predicting an output from the input without actually hashing it is impossible. From the output, determining the input is impossible. A small change in the input creates a drastically different output.

Blocks are added to a random number called a nonce to make the input of hash. The nonce is changed until the hash has a certain number of leading zeroes. Then the Block is considered valid and is broadcast to the network. The miner who mined this Block would receive the Block reward (25 BTC) as compensation for securing the network, about $8000 today. The number of leading zeroes required scales in proportion to the amount of computing power of the network, found by the brevity of the previous Blocks that were mined. For this reason, Blocks are mined every ten minutes. Hashing is fairly resource intensive due to the massive number of hashes that must be performed before arriving at a satisfactory result.

Different numbers have been pushed around about the power consumption of the Bitcoin network. One speculator has even compared it to the power consumption of the entire country of Bangladesh. But recent estimates paint a story vastly different than a power consumption so enormous. Adam Rothstein estimated that Bitcoin expended about 7.31 gigawatt hours per year, about the same power consumption as 650 average American homes (Rothstein). The power consumed is reasonable for an entire currency, especially since Bitcoin avoids myriads of problems.

The concerns stated above are primarily technological scalability concerns. However, Bitcoin's psychological scalability must be considered as well.

Despite the various retailers beginning to accept Bitcoin (Frankel), most businesses do not accept Bitcoin. Bitcoin frequently receives a tainted reputation in the media, portrayed as an "internet funny-money" used primarily to buy drugs. No matter the truth, this is a hindrance to Bitcoin's growth. Bitcoin's technological stability is worth nothing if it is not accepted as a means of payment.

Much of the problems arise from false information of Bitcoin in the media. Bitcoin's reputation likely arises from the users who, in a variety of ways, use Bitcoin unwisely. One of the most prevalent of these ways that Bitcoin users are unwise is the lack of security precautions taken by them. If the majority of Bitcoin users were to research the measures they need to take in order to be secure, a large amount of the fraud around Bitcoin would decrease.

For example, using exchanges to store Bitcoin in a permanent manner is widely known to be insecure (Is). Yet Mt. Gox, a former Bitcoin exchange, suffered a security compromise which lost its users about half billion dollars worth of Bitcoin (McMillan). This one example shows the lack of security education leading to disaster. These problems would be solved with the education of new Bitcoin users. Abundant resources are available for educating oneself, and these resources continue to improve and expand (How to). Using Bitcoin is completely secure-if used correctly. As more and more resources for beginners enter the community, the probability that users will transact securely will be greatly augmented.

Another social aspect of Bitcoin is the media itself. Much of the media portrays Bitcoin in a skewed manner, and sections of the media even portray Bitcoin completely erroneously. The skewed portrayal will likely be aided with time, as media tends to reflect public opinion. Bitcoin is fairly new; the average population knows little to nothing about the inner workings of Bitcoin.

As both public opinion and likelihood of security increase, business acceptance will likely increase as well. This acceptance will spark the public to learn more about Bitcoin, as they will have more reason to use it . In an earlier article reflecting on what will influence Bitcoin's future, I stated that "I have also found that the Bitcoin community is very willing to help others understand whatever may confuse them." I have asked questions on fairly obscure Bitcoin concepts, received multiple quick responses. The community definitely wants to see the public understand Bitcoin.

All of these social aspects of Bitcoin seem to primarily require time. This pattern runs parallel to other technological advances in the past, like the personal computer (Timeline). Like these, Bitcoin will likely be accepted eventually by the general public.

While various aspects of Bitcoin have slight flaws, time has enabled increasing numbers of these flaws to be solved as the currency has developed. Projects are now in development to improve the currency. Since Bitcoin is a scalable currency, it has the ability to handle the various stresses of becoming a more mainstream currency. Therefore, Bitcoin is here to stay.

References

"About PayPal." *PayPal.* Paypal, n.d. Web. 06 Nov. 2014.

"Bitcoin Blockchain Size." *Blockchain.info.* Blockchain, n.d. Web. 06 Nov. 2014. <https://blockchain.info/charts/blocks-size>.

"Bitcoin Number Of Transactions Per Day." *Blockchain.info.* Blockchain, n.d. Web. 06 Nov. 2014. <https://blockchain.info/charts/n-transactions>.

Bruce, J. D. "The Mini-Blockchain Scheme." *Cryptonite.info* (n.d.): n. pag. July 2014. Web. 6 Nov. 2014.

Cawrey, Daniel. "Jeff Garzik Announces Plan to Launch Bitcoin Satellites into Space." *CoinDesk.* N.p., 23 Apr. 2014. Web. 06 Nov. 2014.

Cawrey, Daniel. "What Are Bitcoin Nodes and Why Do We Need Them?" *CoinDesk.* N.p., 9 May 2014. Web. 06 Nov. 2014.

"Electrum." *Electrum.* Electrum, n.d. Web. 6 Nov. 2014. <https://electrum.org/>.

Frankel, Matthew. "Bitcoin and Retailers: Who Accepts the Virtual Currency?" *Fool.com.* N.p., 15 Oct. 2014. Web. 06 Nov. 2014.

"How Bitcoin Mining Works." *CoinDesk.* N.p., 6 Mar. 2014. Web. 6 Nov. 2014.

"How to Set up a Secure Offline Savings Wallet." *Bitcoin.* N.p., 11 July 2014. Web. 06 Nov. 2014. <https://en.bitcoin.it/wiki/How_to_set_up_a_secure_offline_savings_wallet>.

"Is Bitcoin Secure?" *Beginners Guide to Bitcoin CEXIO.* CEX.IO, n.d. Web. 06 Nov. 2014.

Mackeral, Jackson. "Future of Bitcoin - Top 10 Considerations." *Bitcoin Price Live.* N.p., 25 Aug. 2014. Web. 06 Nov. 2014.

McMillan, Robert. "The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster." *Wired.com*. N.p., 3 Mar. 2014. Web. 6 Nov. 2014.

Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System* (n.d.): n. pag. Web. 25 Oct. 2014.

Rothstein, Adam. "How Much Electricity Does Bitcoin Use?" *Medium*. N.p., 13 Mar. 2014. Web. 06 Nov. 2014.

"Timeline of Computer History." *Computer History Museum*. N.p., 2006. Web. 04 Nov. 2014. <http://www.computerhistory.org/timeline/>.

Trillo, Manny. "Stress Test Prepares VisaNet for the Most Wonderful Time of the Year." *Visas Blog Visa Viewpoints RSS*. Visa, 10 Oct. 2013. Web. 06 Nov. 2014.