Jacob Arciniega-Bueno

25 September 2024

The BlockChain Revolution and The Bitcoin Problem

Blockchain technology is revolutionary, but bitcoin is borderline useless. The marvelous innovation of blockchain technology has made way for a new generation of tamper-proof data and soon we will likely find it implemented in all facets of our daily lives. Bitcoin however will not be adopted for widespread use unless it can solve issues related to its speed, cost, security, privacy, and energy problems.

Throughout all of human history we have been making locks to protect our valuables and finding ways to break into said locks to steal these valuables, moving into the digital age this is no different with cyber security specialists trying to protect valuable data and on the other side obtain it. Originally blockchain was made to be a new type of money where people owned their own portion and no third party had any control over it, a perfect lock. The problem was, how could they keep track of who owns what securely? They developed a “peer-to-peer network [that] timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work” (Nakamoto, 2008) . In this system users can create a virtual account to hold their digital tokens using a private key to send them and a public key to receive them in digital transactions. A network of users was then established to validate new transactions by checking pre-established consensus rules such as checking if the account associated with the given keys actually has the amount being sent, this process is known as mining. To pick which user gets to validate the

transaction, users have to solve arbitrary calculations, the fastest user to complete the calculation is chosen if no rules were broken, this system is known as proof-of-work. These transactions are then recorded to the blockchain ledger which is just a large public data set of valid transactions that can not be deleted or altered as per the consensus rules. In creating this network the bitcoin creators were able to have a secure data set that kept a record of what account holds what tokens. This is all bitcoin is and this is all bitcoin does, notably bitcoin has never had its ledger hacked or altered in any way. The concept of bitcoin being worth a price in fiat currency came with the first cryptocurrency exchange Mt. Gox in 2010, a website that would buy and sell bitcoin tokens from users for USD (Rasure, 2024). This application is just the start of the blockchain revolution because if we can create a tamper-proof data set, or ledger, for bitcoin we can theoretically make any data set unhackable for the first time in history the applications of which are endless!

The years following bitcoin's creation have seen thousands of new alternative blockchains being created. Personally, I like XRP which is a blockchain created by bitcoin founders to be thousands of times cheaper, faster, more secure, and more energy efficient than bitcoin. As more people buy new tokens their prices on various exchanges have fluctuated dramatically leading to a frenzy of people trying to buy new tokens to sell them for a profit. This is essentially gambling as the technology was never designed to go up in value or even have any value to begin with and most of these new blockchains were created with no purpose in mind other than profiting off others. While this mirrors stock market bubbles more than traditional gambling, the underlying difference is that at the core of this crypto frenzy is a useful technology that solves problems we couldn't solve without it, namely data security.

One of the main reasons I find bitcoin borderline useless is because of scalability flaws inherent to its design. Transaction speed is a huge factor, early on transactions were confirmed in about 10 minutes but as more users participated the computations needed to validate became harder to solve increasing transaction wait times. Bitcoin transactions currently average about 15-60 minutes and have been known to spike to 80+ hours based on user activity. (Blockchain.com). We are all used to using our money instantly and will not adopt a new form of money that will leave you waiting in the grocery line for hours. Another problem is the fees that users have to pay to validators for each transaction, as the user base grows the fees increase. Currently bitcoin transaction fees average about $5 but have spiked to $100+ based on user activity (Blockchain.com). This is inherently ridiculous, just imagine trying to buy something for $1 with bitcoin and having to pay $5 for the transaction.

One of the largest security flaws of bitcoin is something known as a 51% attack. Recall that validations follow a set of rules, well a key feature of validators is the ability to alter what consensus rules they follow, the set of rules with the most users is what is used for validation. This means if a majority of the validators want to change how transactions are validated they can do it by coordinating their rules to match and gain a 51% majority. This means the network is only secure “as long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network” (Nakamoto, 2008). If a single party were to control the majority of validator nodes they would be able to directly control all bitcoin tokens. This happened in 2014 when the bitcoin mining company Ghash.io exceeded 51% and promptly shut down its validators to save network confidence (Matonis, 2022). Currently there are serious concerns that China has

the power to enact a 51% attack on bitcoin since “China accounts for more than half of the world’s Bitcoin mining capacity” (Peng, 2020).

Another huge problem with bitcoin is the lack of privacy. “ Bitcoin may be pseudonymous—no one’s identity is recorded on the blockchain—but every single transaction is.” (Salvo, 2022) meaning each transaction records how much, who it's from or to, and when it happened. This is a serious concern as we don’t want advertisers and solicitors tracking our spending, likewise we don’t want to share all our transactions and account balance for everyone to see. What if it’s embarrassing or incriminating? Once an identity is associated with an account all privacy is gone. We as consumers will not accept this because we already enjoy financial privacy with banks, and bitcoin can not offer the same privacy.

Arguably the largest problem with bitcoin is its growing energy demands amidst a global energy crisis. Every user trying to validate a transaction is using energy to do it, so more validators on the network increases the amount of energy bitcoin uses to run. Currently the energy cost of running bitcoin “uses more energy than many countries” (Huang, 2021). As we grow more environmentally conscious we will inevitably see the immense power usage of bitcoin as a complete waste of vital resources.

Frankly bitcoin is the worst performing functional blockchain in existence, meanwhile blockchains such as XRP and XMR have since solved the speed, cost, security, privacy, and energy problems. While bitcoin is an amazing proof of concept and does work, it is not good enough for modern use, much like Ford Model T was a great proof of concept but would not work today. So while I am adamant that blockchain is the future, bitcoin clearly is not.

Works Cited

Blockchain.com. Charts - average confirmation time. | Charts. (n.d.-a). https://www.blockchain.com/explorer/charts/avg-confirmation-time

Blockchain.com. Charts - fees per transaction (USD). | Charts. (n.d.-b). https://www.blockchain.com/explorer/charts/fees-usd-per-transaction

Huang, J., O'neill, C., & Tabuchi, H. (2021, September 3). Bitcoin uses more electricity than many countries. how is that possible?. The New York Times. https://www.nytimes.com/interactive/2021/09/03/climate/bitcoin-carbon-footprint-electricity.html

Matonis, J. (2022, December 12). The Bitcoin Mining Arms Race: Ghash.io and the 51% issue. CoinDesk Latest Headlines RSS. https://www.coindesk.com/markets/2014/07/17/the-bitcoin-mining-arms-race-ghashio-and-the-51-issue/

Nakamoto, S. (2008, October 31). Bitcoin: A peer-to-peer electronic cash system. bitcoin.org. https://bitcoin.org/bitcoin.pdf

Peng, T. (2020, August 11). Why Chinese miners won't stage a 51% attack on Bitcoin. Cointelegraph. https://cointelegraph.com/news/why-chinese-miners-wont-stage-a-51-attack-on-bitcoin

Rasure, E. (2024, April 22). What was Mt. Gox? definition, history, collapse, and future. Investopedia. https://www.investopedia.com/terms/m/mt-gox.asp

Salvo, M. D. (2022, August 12). Bitcoin's privacy problem-and what cypherpunks are doing to solve it. Decrypt. https://decrypt.co/107376/bitcoin-privacy-problem-what-cypherpunks-are-doing