OC BITCOIN NETWORK:

WEEKLY CURRENT EVENTS

05 DECEMBER 2021

NEWPORT BEACH, CA

TABLE OF CONTENTS

Vijay Anand

CNBCTV18

03 December 2021

Bitcoin network surpasses PayPal in transaction volumes

The bitcoin network has reportedly surpassed transaction volumes of payments platform PayPal. At an average $489 billion, the bitcoin network transacted $187 billion more than PayPal per quarter this year, dailyhodl.com reported quoting data by blockchain intelligence company Blockdata. PayPal processed an average of around $302 billion per quarter.

However, bitcoin's current transaction volume per quarter is still only a fraction of the value processed by credit card companies Mastercard and Visa, Blockdata noted.

Mastercard processed an average of $1.8 trillion per quarter this year, 260 percent more than PayPal.

"It's impressive how bitcoin, as a 12-year-old decentralised network, is 27 percent of the way in terms of one metric (volume processed) compared to Mastercard, a company founded in 1966, especially when you take into account that this is a decentralised movement," Blockdata said in the report.

The blockdata report makes a case for the bitcoin network beating Mastercard based on three factors -- the rise in the number of transactions, the average amount of bitcoin sent per transaction and the surge in bitcoin price.

The bitcoin network would have to scale 260 percent to process an equivalent volume to the Mastercard network on a daily basis, and 540 percent for Visa. However, there has not been any indication that the amount of bitcoin set per transaction is rising, it said.

Alternatively, if the price of bitcoin were to rise by 260 percent, then the bitcoin network could reach Mastercard's volume, it noted. As the rise in the price of bitcoin has been unpredictable historically, it is hard to say if it will reach this point.

According to the report, at the current growth rate, bitcoin could reach Mastercard's volume anywhere between 2026 and 2060, taking into account that Mastercard would also be processing more transactions than today.

Source:

https://www.cnbctv18.com/cryptocurrency/bitcoin-network-surpasses-paypal-in-transaction-volumes-11693172.htm

Anthony Cuthbertson

Independent

02 December 2021

Facebook unbans bitcoin ads in huge boost for crypto industry

Meta, formerly called Facebook, has reversed its ban on cryptocurrency ads across its platforms.

The move will give bitcoin exchanges, wallets and other crypto companies access to more than 3 billion people around the world who use the firm's various platforms, which include Instagram, WhatsApp and Facebook itself.

The ban was originally introduced in January 2018 in an effort to prohibit "misleading or deceptive promotional practices" like initial coin offerings (ICOs), which spiked in popularity during the crypto market rally of 2017/18.

Since then, the cryptocurrency industry has evolved considerably, with milestones including the first crypto exchange to go public through Coinbase's Nasdaq listing, El Salvador becoming the first country in the world to recognise bitcoin as legal tender, and massive corporate investment in cryptocurrency through companies like MicroStrategy, SpaceX and Tesla.

"We're doing this because the cryptocurrency landscape has continued to mature and stabilise in recent years and has seen more government regulations that are setting clearer rules for their industry," Meta said in a statement.

"This change will help make our policy more equitable and transparent and allow for a greater number of advertisers, including small businesses, to use our tools and grow their business."

The policy update follows the social media giant's decision to pivot towards the metaverse, which will likely support some form of cryptocurrency payments and other blockchain-based technologies like non-fungible tokens (NFTs).

The news also comes just one day after Facebook executive David Marcus announced his departure from the tech giant, having failed in his attempt to launch the Libra and then Diem cryptocurrency.

The crypto project faced resistance from lawmakers and regulators in Europe and the US, however the company was able to release a digital wallet called Novi in October under Mr Marcus's guidance.

"While there's still so much to do right on the heels of launching Novi – and I remain as passionate as ever about the need for change in our payments and financial systems – my entrepreneurial DNA has been nudging me for too many mornings in a row to continue ignoring it," he wrote on Twitter when announcing his decision to quit.

"I find comfort and confidence in knowing that they will continue to execute our important mission well under [new Novi leader] Stephane Kasriel's leadership, and I can't wait to witness this from the outside. I know there's greatness ahead."

Source:

https://www.independent.co.uk/life-style/gadgets-and-tech/facebook-crypto-ban-meta-bitcoin-b1968321.html

Hououin Kyouma

NewsBTC

03 December 2021

Understanding Bitcoin UTXO: Mid-To-Long Term Holders Responsible For November Correction

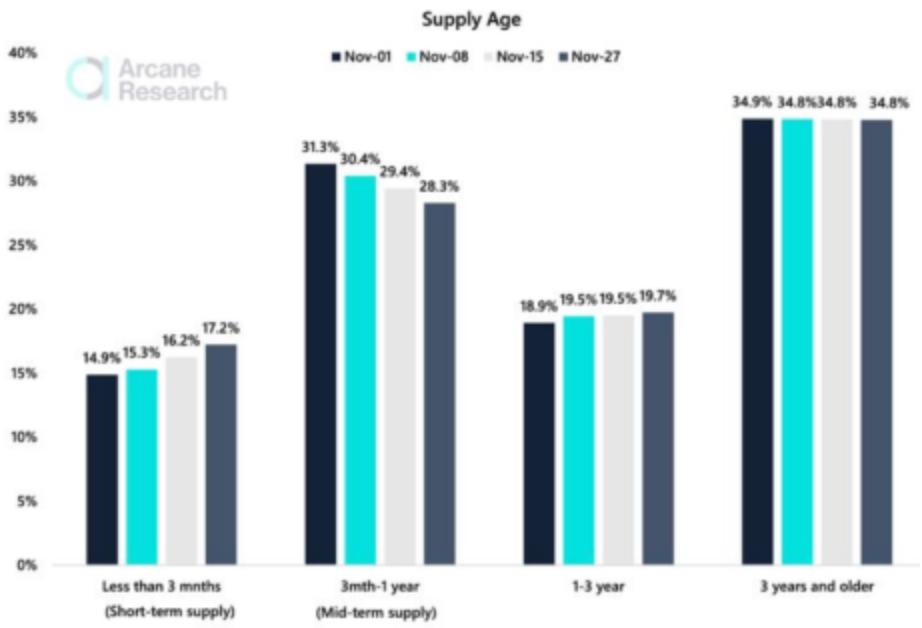
As per the latest weekly report from Arcane Research, mid-term holders seem to be behind the decline in BTC's price during the month of November.

The relevant on-chain indicator here is the "UTXO Age." UTXO stands for Unspent Transaction Output; you can think of it as a Bitcoin mechanic that keeps track of coins on the chain.

The UTXO age metric measures how long it has been since a coin on the BTC blockchain was last transacted. Based on the amount of time each coin hasn't been moved for, the corresponding holders can be categorized into short-term holder (STH), mid-term holder (MTH), and long-term holder (LTH).

Arcane Research takes UTXO age shorter than three months as belonging to STH, and longer than one year as LTH. Holders falling in the period in between are termed MTH.

Now, here is a chart that compares how the supply belonging to the different Bitcoin holders moved during the month of November:



As you can see in the above bar graph, the Bitcoin short-term supply saw significant growth during the period as it went from 14.9% at the start of the month, to 17.2% at the end.

This growth suggests that some holders in the longer age bands sold off their coins. From the chart, it's visible that the MTH supply had a sizeable drop during the month.

This means that most of the increase in the Bitcoin STH supply can be accounted for by the sell-off from mid-term holders.

Also, the one-to-three year supply saw some increase as well. This means that part of the MTH supply matured and entered into this longer age band.

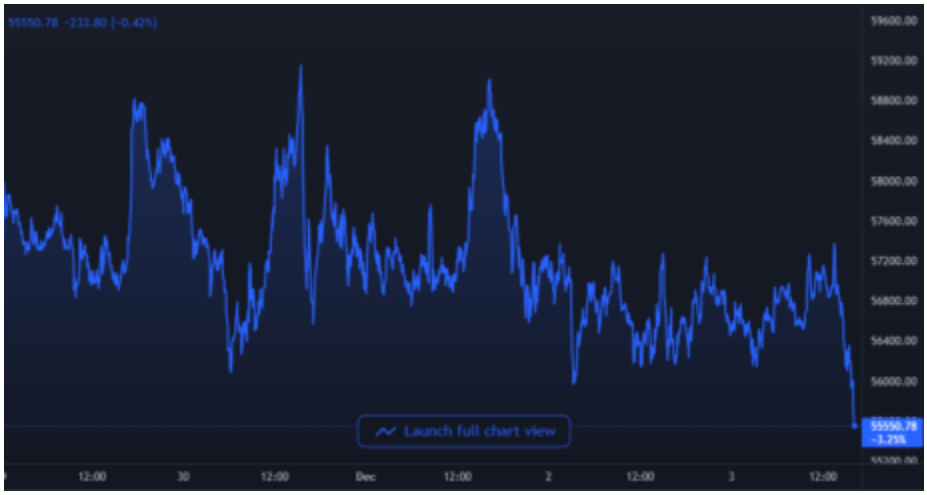
The 3-5 year supply also had a slight decrease in November, suggesting that some of these long-term holders reaped their profits, and thus added to the increase in STH supply.

So in conclusion, selling from mostly mid-term holders with some long-term holders may be behind the correction in November.

BTC Price

At the time of writing, Bitcoin's price floats around $55.5k, up 2% in the last seven days. Over the past month, the crypto has lost 11% in value.

The below chart shows the trend in the price of BTC over the last five days.



Source:

https://www.newsbtc.com/news/bitcoin/bitcoin-utxo-mid-long-term-holders-november-correction/

Brian Colucci

Screen Rant

03 December 2021

It's Official: Lex Luthor Has His Own Version of Bitcoin

The Superman villain known as Lex Luthor has had some wild schemes and ideas over the years, and now his latest one sees him officially entering the cryptocurrency market! That's right, this conniving businessman now has his own version of Bitcoin, and this new "Lexcoin" is aiming for the moon.

Revealed in the very first issue of Justice League Incarnate, by Joshua Williamson, Dennis Culver, and Brandon Peterson, Lex finally deciding to jump into the crypto marketplace is a move that was undoubtedly a no-brainer for this evil mastermind. Needing to recruit a version of the Flash, Avery Ho, to the multiversal team called Justice League Incarnate, Earth-23's Superman and Flashpoint Batman watch her battle it out with the villain named Replicant as he explains why he's currently trying to destabilize the banks of China, bringing the idea of cryptocurrency into the conversation in the process.

Fighting one another in spectacular fashion as Flash rushes innocent bystanders out of the way, Replicant lets slip a detail about Lex's latest business venture set in the realm of digital currency. Saying that after he takes down the banks of China "the world will have to rely on cryptocurrency," Replicant tells Flash that another reason for his villainous actions is because by tampering with these banks, he'll be making himself — and any holder of Lex Luthor's Lexcoin asset — rich beyond all reason.

Confirming his motivation by referencing a popular crypto meme, Replicant says, “Lexcoin value will go to the moon!” succinctly revealing that not only does Lex Luthor have a stake in the crypto market, but he’s continued his patented trend of putting his name on everything he touches. Going on to say that he craves “exponential growth,” Replicant annoys Flash to a point that she gets fed up with his “get-rich-quick” antics and handily puts him down, leaving fans with a new wrinkle in Lex Luthor’s grand business strategy to think over as Flash is whisked away by the multiversal version of Superman and Batman.

Coming as no surprise to fans that Lex has jumped on the crypto bandwagon, Lex is constantly on the lookout for ways to increase his enormous wealth, social status, and his business — and villainous — mind, with these qualities becoming synonymous with the character to a point that fans might have been worried if Lex *didn’t* get into the digital currency game between the pages of DC Comics. But probably the most interesting thought coming from all of this is whether Lexcoin is a cheap memecoin like the infamous Dogecoin or Shiba Inu assets, or an industry giant a la the original Bitcoin or Ethereum.

Regardless of either, Lex now having his own cryptocurrency in the aptly named Lexcoin is another character moment that shows just how in tune Lex is to the ebb and flow of any industry that can make him money. Like Replicant, Lex Luthor is also probably banking on the idea of Lexcoin going "to the moon," so now fans are left to wonder who hired Replicant to destabilize all of China's banks in the first place!

Source:

https://screenrant.com/lex-luthor-bitcoin-lexcoin-cryptocurrency-justice-league-incarnate/

David Z. Morris

CoinDesk

29 November 2021

Who Sets the Rules of Bitcoin as Nation-States and Corps Roll In

"Little by little, and then all at once."

That's how people go bankrupt, of course. But it's also a fair description of bitcoin's ascendance from radical experiment to widely used technology. Recall, if you dare, that in March 2020 BTC was trading at about $5,000 per token and had been in the doldrums for years. Then COVID-19 lockdowns juiced boredom-driven day trading and increased interest in crypto, ultimately unleashing a string of transformational moments for Bitcoin. Those included the big BTC buy by Tesla, integration into Twitter, high-profile legislative debates in the U.S., a record-setting stadium name deal and national adoption in El Salvador.

The arrival of nation-states and tech corporations in Bitcoinland is a huge, positive milestone. Twitter and El Salvador are directly exposing new mass audiences to crypto usage instead of just speculation. Because bitcoin is more useful as more people use it (the "network effect"), these moves also increase the appeal of future integrations. Major corporate buys, meanwhile, open the door for more institutional investment and legitimize bitcoin's inflation-hedge thesis.

But those new players also bring new risks – arguably risks of a sort the world has never before seen. An array of centrally run, sometimes very powerful entities now have vested

interests in the design and growth of a system they all share. History suggests their interests will, sooner or later, diverge, and that some will try and change bitcoin to their liking.

They will find the system used to propose and execute changes to bitcoin is barely a "system" at all. Unlike a company or a national government, the Bitcoin blockchain doesn't have a formal leadership structure (with one debatable exception). Instead, as developer Gavin Andresen put it in 2015, Bitcoin's design and evolution "really comes down to, what code are people running, and how influential are the people who are running the code?" In other words, Bitcoin upgrades are largely a matter of persuasion.

So what if Twitter or Tesla or Germany decide that they want Bitcoin to be something else? With enough money, with courtrooms and jails, with an army division or two, could they force their vision on the most powerful stateless entity on the planet?

Why change Bitcoin?

We got a preview of such a conflict in the so-called "Blocksize War" of 2015-2017, recently chronicled in an excellent book by Jonathan Bier. In very broad strokes, the conflict was between entities, including companies like BitPay and Coinbase, that advocated for larger "blocks" of transactions to increase the network's speed. They were opposed by "small blockers," who warned that increasing the block size would make it more expensive and difficult to run a Bitcoin node, threatening the system's decentralization and, ultimately, its resilience.

As bitcoin becomes a more important component of the world's financial infrastructure, it's not hard to think of other motives for changing the way it works. Perhaps a surveillance-obsessed Western government will push for a change that threatens pseudonymity.

Miners might aim to increase their fees as block rewards decline. A coalition of authoritarian regimes might seek to add native geofencing. Or, if you want to get really crazy, imagine a populist uprising circa 2050 agitating to remove Bitcoin's 21 million coin-supply cap.

Some of these scenarios are more realistic than others. But their mere possibility is probably news to many bitcoin holders and users.

"It's safe to assume that 95% of people have no clue how [Bitcoin] upgrades work," says Jackson Wood, a financial adviser who works with crypto. "They're 100% taking it for granted that it just exists and will always be the way it is. But if consensus rules on Bitcoin, literally anything can change."

The tangled layers of Bitcoin governance

Various kinds of decision-making mechanisms hold sway over different aspects of bitcoin.

On a day-to-day basis, the combination of proof-of-work mining and blockchain database sequencing determines which transactions are valid and which aren't. There are at least two well-known forms of technical attack that could interfere with these "on-chain" rules, but they have limited potential. Though it's financially impractical at this point, an entity willing to spend many millions of dollars to rent bitcoin mining rigs could theoretically conduct a 51% attack on bitcoin, giving them the ability to manipulate a small subset of transactions.

The other purely technical attack would be a "hard fork," or software change, in which an alternate version of Bitcoin is released and promoted to miners. But previous Bitcoin forks show how difficult it is to gain adoption for a divergent Bitcoin: Dozens if not hundreds have faded

into obscurity. Even a relatively successful fork like Bitcoin Cash, which emerged from the Blocksize War with a large, built-in constituency, has fallen far behind Bitcoin.

"Governance" of a blockchain system, though, more often refers to how these consensus rules themselves can be changed. Very broadly, Bitcoin takes its fundamental development and administrative structure from the open-source model through which unaffiliated developers collaborate on software like Linux. Bitcoin's source code lives on Github just like that of many other open-source projects. Literally anyone can debate Bitcoin's future, and even propose specific changes – though actually getting traction for your proposal is a much bigger challenge.

The most direct approach for an entity hoping to reshape Bitcoin, then, would be "putting in pull requests on Github and suggesting code changes that go in that direction," says Pierre Rochard, a longtime Bitcoiner on the product team at Kraken.

But in practice, if the changes went against broader community sentiment, this would be basically impossible.

The Blocksize War is an important episode when considering the future of Bitcoin, because it illustrates both the motives and methods that we might see replayed on a still larger scale. In this case, the motives for big blockers were largely commercial. Businesses like BitPay needed more throughput to turn bitcoin into a coffee-cup currency. The other side of the debate, at least in Bier's telling, was made up of people prioritizing long-term stability and what we'd now call the "store of value" model, even if it meant bitcoin transactions stayed fairly slow.

"What they would run into is that Core has a tremendous amount of peer review," says Rochard. "Even small changes require two or three reviewers who have experience and

somewhat of a reputation to get merged [into the reference client]. And then big changes that would affect consensus rules, those receive just a tremendous amount of scrutiny – both from developers and from interested laypeople. And it's not based on votes, it's somewhat based on reputation."

In practice, this nebulous, reputation-based approach boils down to a web of protracted debates at conferences and online, across message boards like r/bitcoin, Telegram and Twitter. This swarm approach means changes are slow. "It took forever to get [recent Bitcoin upgrade] Taproot approved," observes Wood. "It was months and months and years of debate."

In an abstract sense, you can compare that interminable and open-access debate to the "proof of work" in Bitcoin's on-chain transaction rules. Just as a block of transactions can't be approved on-chain if a miner hasn't taken an economic risk in certifying it, a Bitcoin upgrade that arrives without a paper trail of months and months of rhetorical free-for-all would be instantly flagged as suspicious.

Rochard believes that this crowdsourced scrutiny will grow along with the rising stakes of Bitcoin design. "Even though we're at a different scale than 2017, I see Bitcoin's governance pattern as a bit of a fractal. Even as the scale increases, we'll see the same patterns play out."

Bitcoin also has one key difference from Linux or Open Office that makes any non-consensus change difficult: Bitcoin does not have an automated upgrade system, or even an automated notification of an available upgrade. Miners instead have to manually install new versions of the client.

So even if someone successfully meddled with the Core Github, they would have to publicize the new version to get nodes to upgrade – at which point the non-consensus change would be exposed. It would then, most likely, be reversed, thanks to one of the last lines of defense against malicious Bitcoin code: a rollback.

"Even if the consensus is wrong, if all the core developers start acting crazy – there's nothing saying a group of people couldn't jump up and say, 'Let's go back to how it was before,'" says Wood. It wouldn't necessarily be an easy or smooth process, but in the face of an existential threat to Bitcoin, such a rollback would be an invaluable lifeline.

Just Core things

Not everything in Bitcoin is so decentralized, though. Only a handful of individuals scattered around the world have what's known as "commit access," or the ability to merge proposed changes into the Bitcoin Core reference implementation. This group of maintainers was created by Gavin Andresen, who was essentially handed the reins to Bitcoin when pseudonymous founder Satoshi Nakamoto stepped away in 2011. As described by Andresen in 2015, he picked two trusted collaborators and, with them, picked two more. Other maintainers have since left or been added, largely based on demonstrated commitment and contributions to the project.

This group has sometimes been regarded with suspicion because of its perceived power. But the job is far less glamorous or influential than it appears.

"In Bitcoin, maintainers are very much janitors," says Rochard, tasked, for instance, with removing spam from the repository. "They understand the backlash that would happen if they

were to make a decision, so they're very loath to do that. They only merge things when there's a rough consensus among frequent contributors, rather than themselves making a controversial call."

This was cemented as far back as 2014 with the handover of the lead maintenance role from Andresen to Wladimir Van Der Laan. Andresen has said that he was more willing to be something of a benevolent dictator in the early days of Bitcoin, but Van Der Laan explicitly renounced any actual decision-making power. Van Der Laan himself stepped back from responsibilities earlier this year, and signaled that he wanted even more decentralization of the maintenance role.

The upshot is that even if a powerful organization used bribery, blackmail, or other means to subvert one or more maintainers with commit access, they would make little headway in actually changing Bitcoin without the backing of broader consensus.

"There would be alarm bells," says Rochard. "How did this get merged in?" Rochard says there has been at least one instance of a maintainer accidentally merging code that hadn't been vetted. It was swiftly caught and undone.

Governance into the future

The strange, emergent, arguably chaotic status quo of Bitcoin's decentralized governance appears, for now, to make it highly resistant to hostile takeover. Amazingly, governments and other potential meddlers seem to have gotten the message.

"If you had some sort of Washington-corporate alliance that wanted to make Bitcoin a transparent chain, guess what? They would have fought Taproot," says Alex Gladstein at the

Human Rights Foundation, who advocates for Bitcoin as a tool against authoritarian governments. “But there was no organized resistance to Taproot. We’re just not seeing it, which is good.”

But not everyone is sure that the open-source scrum will be enough to keep things running smoothly forever.

“As much as we say this is decentralized, there are humans behind it,” says Merav Ozair, a blockchain-focused finance professor at Rutgers. “Someone has to write the software. It shouldn’t be at the hand of one developer, or a small group. We should have a long-term, bigger audit.”

To that end, the nonprofit International Association of Trusted Blockchain Applications (INATBA), where Ozair is an adviser, is developing a proposal for a European Union committee to monitor Bitcoin code and interface with governments. Such a committee would have no formal role in Bitcoin governance, but, over time, could build up legitimacy and community influence.

Ultimately, that sort of transparent bid for influence seems to be the only plausible way to “attack” Bitcoin: joining in the debate about its design, and building up a reputation for sound thinking. You might say that the best way to successfully infiltrate Bitcoin governance – maybe the only way – is to actually do the work of making the system better.

Source:

https://www.coindesk.com/business/2021/11/29/who-sets-the-rules-of-bitcoin-as-nation-states-and-corps-roll-in/

Nick Agar

Nasdaq

01 December 2021

Bitcoin May Be Big, But It's No 'Currency'

Bitcoin is currently the undisputed king of the crypto, so much so that its price action can work as a sort of a benchmark for the entirety of CoinMarketCap's listings. Whenever it goes up or down, altcoins normally follow, that’s hardly surprising by now. What is surprising, though, is that we are still calling it a currency, even though that’s clearly not what it is.

Currency is, fundamentally, a medium of exchange, a store of value, and a unit of account. It could work in many ways, from a gold coin that is valuable on its own, which is the old way to do it, to a banknote that is reliant on the trust in the government as well as the financial and monetary system behind it, which is what fiat is all about. One way or another, the main function of all of the above is to change hands as a fungible unit for value exchange that more or less retains its purchasing power over time, though in many cases fiat fails to do so.

This is the start of where the notion of Bitcoin as a currency already begins to fall apart. If you’re looking to spend your coins, you’d have to look up what businesses accept them in the first place, and you’d find that those are quite limited. El Salvador’s Bitcoin Beach may be living and breathing crypto, but not without some help from a philanthropist—in other words, it’s only sustained by a centralized gatekeeper. In the grander scheme of things, the country’s experiment with Bitcoin as legal tender stems from specific economic factors—namely, the inflow of

remittances from abroad accounting for more than one-fifth of its GDP—which makes it, at least for now, a one-off.

In fact, why would you even want to spend your bitcoin if you also owned fiat or a stablecoin? The $5 worth of Bitcoin you spent on a coffee today may be worth $10 next week, and assuming the price was denominated in USD, you just lost out on another cup of coffee. The same applies to anything else you may be buying with bitcoin, from a pizza to a car. In other words, Bitcoin's most appealing feature—its supply cap—may very well also be the biggest hurdle for using it as a currency. The limit drives the demand, the demand amps up the price, and if you expect the price to rise, why use it for transactions?

However, due to the volatility associated with Bitcoin, its purchasing power can swing far and wide in short periods of time. Meaning it already fails at properly fulfilling the requirements to be considered a strong store of value as well as provide the means to seen as a solid unit of account.

HODL to the moon

The reason why most people get involved with Bitcoin is not the same as why they carry fiat in their wallet. Only 24 and 12 percent of crypto investors said they planned on using their coins for, respectively, online and in-person purchases in a recent Bakkt survey. The most frequent aspiration among those purchasing crypto is not to "transact directly with each other without the need for a trusted third party," using Satoshi Nakomoto's words, but rather to make gains on investment or trading. Money is spent or invested, but with Bitcoin, "HODLing," or holding on for your dear life, is the way, as the coin may shoot up to the moon and higher.

"To the moon," a rallying cry of the cryptoverse, is a clear indication of this mindset. For many, Bitcoin's value is not in its (relative) anonymity or blockchain's transparency and security, but simply in its volatility. Such investors treat Bitcoin as a speculative asset holding the promise of plenty. In investment terms, it's a good idea to diversify your portfolio with instruments that can act as a reasonable hedge against not just inflation, but also the woes of centralized markets, which are increasingly volatile as evidenced by the 2008 financial crash, among other events. However, looking at past history, Bitcoin has also failed this test as significant downward pressure on markets correlated with a depreciation of the coin.

For all that's worth, though, the point is Bitcoin never really functioned as an actual currency. Consider this: While Bitcoin's price action graph has been on an unsteady upward trajectory since early 2017, shooting up in 2021, its monthly transaction total stayed more or less the same over time, with no corresponding explosive growth—which would have hit the wall of Bitcoin's low transaction processing capacity anyways. The point is, most of the transactions were made by people buying Bitcoin in hopes to sell it at a higher price down the road, and thus playing into its appreciation.

A bottlenecked system

Well, Bitcoin may fall short of being a currency, but so what, you might ask? It is still the banner that the cryptoverse is best known under in the greater world, it is the success story that kicked off the crypto gold rush and the industry's ongoing maturing, and it still is the point of reference for virtues of decentralization. The problem is, not all of that is true.

Bitcoin was conceived as "a purely peer-to-peer version of electronic cash," secure, anonymized, and free from the influence of any centralized entities. It was a challenge for the

fiat-dominated global economic system as such. And yet, while never actually turning into a currency, the Bitcoin ecosystem appears to have also walked back on another key value enshrined in the original vision. It has a variety of bottlenecks, from its infrastructure to the market dynamics, which, in all fairness, are not necessarily a product of the coin's own flaws.

At Bitcoin's inception, certain people who had the capacity could become a miner, and the system was attempting to be inherently emancipatory simply through what was hoped would be a lower entry barrier. These days, though, mining difficulty has increased, which is a feature hard-coded into Bitcoin's design (and one that played a key role in turning it into a speculative asset, while we're at it). Mining takes significantly more computational power and energy, and is thus only accessible to large companies or hedge funds. This forced smaller miners out of the business, while others scale up their operations, turning the system more oligopolized. As a result, in early 2021, five companies controlled almost 50 percent of Bitcoin's mining power, a potentially dangerous development.

Another bottleneck is in the distribution of wealth within the market. Only 1,000 accounts controlled some 40 percent of all Bitcoin in circulation as of early 2021. This does draw a parallel with the wealth distribution patterns, where the top one percent has over sixteen times more than the bottom fifty. Granted, money loves company, and the richer you are, the easier it is to get rich, that's just how our economy works. And yet, even looking past the inequality aspect, this disposition paves the way to market manipulation, effectively leaving hundreds of small-time investors at the mercy of whales lurking deep down below.

The bitter truth is that Bitcoin has ultimately turned into a tool for wealth hoarding, and it's done so in a self-perpetuating way: The more people join the speculative trading, the less

likely Bitcoin is to ever be used as an actual currency. It is just another instrument for the rich to get richer, while the poor, as always, are left with the sharp end of the stick. As such, it weaves into and helps to sustain a system that has resulted in this regrettable situation and works to exacerbate it.

The biggest takeaway from Bitcoin's story is that enthusiast communities building up an innovative tech project can indeed challenge the grasp of the powers that be on the global economic system—the very one that's perpetuating inequality. Things don't have to always stay the same, that's the big lesson. But Bitcoin has largely caved in to the structural forces driving socio-economic injustice in the world.

Bitcoin has other serious flaws due to the fact that it is not a productive asset. As we've already noted, Bitcoin is volatile, has minimal utility, and has no intrinsic or underlying value, plus it is expensive and slow to transact with, offers no service and no social consciousness. Finally, the past decade has also shown us that Bitcoin is subject to price manipulation and collusion by individuals with concentrated large holdings (whales). It is latecomers (generally, average people) that suffer when markets fall and bubbles burst, these same people who cannot afford to lose. This does not sound like the solution our society, our economy or our planet needs.

Granted, Bitcoin was a breakthrough back in the day, and the innovation and vision behind it deserve respect. Particularly the advent of blockchain, which is unquestionably one of the most important innovations of our lifetime. But for all of its glory, it's time for the crypto community to acknowledge the obvious: The word "currency" doesn't stick well to Bitcoin, and it's not nearly as decentralized as it's supposed to be. It kick-started the crypto party, but for the

cryptoverse to grow and bring about the promise of decentralization, we need to get real about what it's become and welcome a world in which digital currencies offer much more utility.

Source: https://www.nasdaq.com/articles/bitcoin-may-be-big-but-its-no-currency

David P. Goldman

Asia Times

02 December 2021

Quantum hackers can bring down Bitcoin: expert

NEW YORK – $3 trillion of cryptocurrency assets are, or soon will be, vulnerable to hacking by quantum computers, one of China's top cryptographers told an Asia Times webinar on November 30.

You won't know if it's happening until it's too late, Professor Jintao Ding of Tsinghua University, a US citizen, explained. And the best thing about hacking Bitcoin, he explained, is that it isn't against the law.

Crypto analysts have worried about the quantum invasion for some time. Motley Fool's Zhiyuan Sun wrote in September, "The rise of quantum computing may soon give governments a means to crack down on Bitcoin and other types of cryptocurrencies… Governments could potentially decrypt digital currencies or launch hash attacks to take over their network for a regulatory shutdown with these machines."

"Most governments like Bitcoin as much as we like walking with rocks in our shoes," Sun added. No government dislikes Bitcoin as much as China, which banned onshore trading of cryptocurrencies in 2019 and forbade Chinese from trading on offshore crypto exchanges last September.

"Our modern information system relies completely on public key cryptography, including Bitcoin," Ding told the "Data Wars" webinar, co-sponsored by the American Affairs journal and Asia Times. "If we have a quantum computer, our Zoom would be finished, and everything actually—the whole information system, because our fundamental security solution relies on it."

Public key cryptography based on the RSA standard has been in use since the late 1970s. Each user has a public key for purposes of identification, and a private key – a password – for decryption.

The public key is based on two very large prime numbers, which are secret; only the recipient knows the prime numbers, which are required to decrypt the message. Factoring extremely large numbers into primes, decrypting the private key requires factoring extremely large numbers into primes, something that takes supercomputers a very long time to do.

As computers get faster, cryptography uses bigger numbers. But quantum computers will be able to factor extremely large numbers into primes very quickly. Maybe they already can—but if that's the case, no one is saying so yet.

Today's encryption methods "can be broken by quantum computers. We must work together to have a smooth transition from the current situation and find a solution. We have to do it. And the transition process will be very difficult," Ding added.

Mathematicians have known that quantum computers would be able to break the RSA code quickly since 1994, when Peter Shor published an algorithm for factoring extremely large numbers into primes.

Development of such a quantum computer is inevitable, Ding argues. There are rumors in the tech world that machines capable of using Shor's algorithm to break RSA already exist.

When will that happen? It might have happened already, but if it has, no-one will let on, Ding explained.

"Watch the movie 'Imitation Game' about [Alan] Turing," the great British mathematician who led the team that broke the German Enigma code during World War II. British signals intelligence (GCHQ) didn't reveal until the 1970s that it could read German coded messages in close to real time during World War II. "If I can read every message, why wouldn't I keep quiet about it? I would be in a very good position. I think this is what I would do," he said.

In 2019, I serialized a spy thriller in Asia Times under the title, The Quantum Supremacy, premised on just such a scenario.

What does that mean for Bitcoin? I asked Ding during the webinar.

He replied: "That's a very good question. In my opinion, once you have a quantum computer, blockchain and Bitcoin are finished. Let me expand a bit. You don't own Bitcoin. The owner is your private key. When they give you the money, they give it to an address. The address is a short form of your public key. They use that to verify the address. Only you have the private key; everyone knows the public key to verify that it is from you."

"When they give you the money, they give it to an address," Ding said. " The address is a short form of your public key. We use that to verify when you give me the coins. But if I don't know the private part key, if I only know the address. I cannot take anything."

“But if I have a quantum computer,” Ding continued, “what I would do first is to get all the coins, because there’s no liability there. I wouldn’t attack banks—then there’s a big lawsuit, or you go to jail. But with a quantum computer, I just take the Bitcoin. It’s legal in my opinion. I didn’t do anything; I just see your public key and use your private key and assign the money to my own account.”

That’s the downside of anonymity. Your name and government ID number aren’t linked to a Bitcoin account (as they are to an ordinary bank account). Your proof of ownership is simply the fact that you have the private key (your password). If someone else hacks that, you have no legal recourse.

Bitcoins have another vulnerability, Ding said. “When I do a transaction, there’s 10 minutes delay because we have to confirm the transaction. In this period, if your transaction is delayed, if people have a quantum computer, then they can do a new transaction to replace your transaction, and then they can send it all the funds to themselves. Then you’re finished. They can just take all your Bitcoin right away.”

The professor doesn’t think that the cryptocurrency world’s efforts to enhance security will do much good. “Bitcoin did an update called Taproot,” he said. “This is actually very bad because in this case, because they are very much prone to attack from content within it.” Taproot creates an interface between Bitcoin and ordinary cash transactions, in order to reduce transaction costs.

If quantum computers capable of hacking your crypto account exist, they are in the hands of governments or large corporations with the resources to build them. If and when such

quantum computers are functional, their owners won't draw attention by stealing from individual bitcoin accounts.

If a state actor hacks cryptocurrency transactions, it almost certainly would use that capability to monitor ownership of these assets for intelligence purposes. Knowing who is trying to hide money, or transfer money away from the scrutiny of regulators, would give the intelligence service of any country enormous political leverage.

But if the whole $3 trillion crypto market were to disintegrate, no one would be more pleased than China, which wants to promote its own digital yuan at the expense of anonymously traded Bitcoins.

Source: https://asiatimes.com/2021/12/quantum-hackers-can-bring-down-bitcoin-expert/

Robert D. Knight

Be In Crypto

02 December 2021

‘The United States Is Already Mining’ Bitcoin Says Industry Insider

In a Dec 1 interview on Anthony Pompliano’s Best Business Show, Gibbs and Pompliano were discussing the nation-states which are mining BTC. While El Salvador is openly mining the cryptocurrency, most countries remain more tight-lipped about their bitcoin mining activities. Pompliano went on to name Venezuala as another nation that was mining digital gold before asking Gibbs what it would take for the US to start mining.

At that point, Gibbs confidently declared that “The United States is already mining…” before correcting himself and belatedly adding the word, “maybe.”

Maybe mining bitcoin

The crypto mining expert went on to add, “They might have 10-20 watts running somewhere in the midwest to test it out. Maybe. It’s hypothetically speaking,” he said with a knowing smile, “but it’s a matter of national security.”

If Gibbs intended to pour cold water on his previous statement that the U.S. government was already mining, what he said next did nothing to aid his cause.

“It is the future financial instrument that many, many things are going to be built on top of. Nations would have to be absolutely out of their mind to not be getting some exposure to the underlying infrastructure which supports it. So the US I think is on the front foot. We’ve

had a lot of conversations with the government in DC [and] state governments to help educate them, but they are very forward-thinking when it comes to supporting this."

Shifting the topic of conversation Gibbs went on to add that bitcoin mining will be a great method for developing nations to level up. The c-level executive went on to explain that the moves being made in El Salvador will prove themselves wise over the course of the next 20-30 years.

A risky game

Sensing that Gibbs was ready to spill the beans, Pompliano invited Gibbs to join him in a game of 'story poker' before sharing details of a U.S. government law enforcement agency that was involved in bitcoin mining.

According to Pompliano the agency in question discovered that it was difficult to get budgetary approval to buy bitcoin, but that by adding additional computers to their budget, they could mine their own BTC for use in undercover operations. Pompliano claimed that a former agent had told him that this secret mining had been going on since as early as 2013.

Pompliano then invited Gibbs to share another story with his viewers. It was at this point that Gibbs declared, "This is how you get in trouble."

Source: https://beincrypto.com/united-states-already-mining-bitcoin-industry-insider/