OC BITCOIN NETWORK:

WEEKLY CURRENT EVENTS

13 FEBRUARY 2022

NEWPORT BEACH, CA

TABLE OF CONTENTS

PAGE 3 Venezuelans reportedly hit by new Bitcoin tax of up to 20%

PAGE 4 Quantum hackers could break bitcoin in minutes, but don't panic just yet: The best quantum computers in the world are not powerful enough to hack bitcoin

PAGE 8 Congress Introduces A Radical Crypto Bill To ‘Unleash Innovation’ As The Price Of Bitcoin And Ethereum Suddenly Soar

PAGE 10 Bitcoin Is Better Than Gold and National Currencies, According to Report

PAGE 12 Bitcoin donations are pouring into Ukraine as Russia masses troops on the border

Helen Partz
CoinTelegraph
07 February 2022

Venezuelans reportedly hit by new Bitcoin tax of up to 20%

Bitcoin adoption has been on the rise in Venezuela in recent years amid hyperinflation and the national currency crisis.

The Venezuelan government has approved a new tax bill aiming to collect up to 20% in taxes from cryptocurrency transactions, according to local reports.

Venezuela's National Assembly held a second discussion session on Thursday for a new draft bill targeting taxes on "large financial transactions" in cryptocurrencies like Bitcoin (BTC).

The Venezuelan government reportedly approved the draft bill last Thursday, requiring local firms and individuals to pay up to 20% for operations carried out in cryptocurrencies as well as foreign currencies such as the United States dollar.

Filed on Jan. 20, the draft law aims to collect 2%–20% from transactions in any currencies other than those issued by the Bolivarian Republic of Venezuela, or the Venezuelan bolivar and the country's oil-backed cryptocurrency, El Petro.

The initiative aims to incentivize the use of the national currency, which reportedly lost over 70% in value last year alone and shed nearly all its value over the past decade.

"It is necessary to guarantee treatment at least equal to, or more favorable, to payments and transactions made in the national currency or in cryptocurrencies or crypto assets issued by the Bolivarian Republic of Venezuela versus payments made in foreign currency," the bill reads.

As previously reported by Cointelegraph, Bitcoin adoption has been skyrocketing in Venezuela in recent years, with many thousands of local businesses starting to move into cryptocurrency to survive hyperinflation. In October 2021, a major international airport in Venezuela was preparing to start accepting cryptocurrencies like BTC as payment for tickets and other services.

Source: https://cointelegraph.com/news/venezuelans-reportedly-hit-by-new-bitcoin-tax-of-up-to-20

Monisha Ravisetti
CNET
08 February 2022

Quantum hackers could break bitcoin in minutes, but don't panic just yet: The best quantum computers in the world are not powerful enough to hack bitcoin

During the last decade, computational programming has evolved steadily and reached into the quantum domain, yielding mind-bending devices that promise unthinkable levels of power.

In 2020, for instance, Chinese scientists tapped a quantum computer to run a math problem that would've taken a typical supercomputer 2.5 billion years to solve. The quantum machine solved it in 200 seconds.

But the hype goes far beyond superhero calculations. Quantum computing holds the potential to transform how we interact with nature.

It could hyperfast-track drug discovery by rapidly sifting through molecular structures, a feat IBM has partnered with Cleveland Clinic to explore. It could boost internet security toward near-unhackability, earning attention from the US Department of Energy. Even manufacturing companies, such as automobile giant BMW, have entered the quantum game because it could perfect materials science and rewrite the framework for artificial intelligence.

We could be on the verge of a quantum revolution where scientists can develop medication at record speeds, predict weather with incredible certainty and uncover new angles on physics.

There's a catch, though.

Prototype quantum computers still work on relatively small scales. Qubits, the basic units in the quantum version of computer language, are the driving force behind a quantum PC's power. Most current quantum processors top out at a few dozen qubits, and the largest processor, built by IBM, presently stands at 127 qubits. These numbers aren't nearly enough for quantum breakthroughs.

But what would be? In an attempt to judge how far along the quantum timeline we currently are, Mark Webber, a quantum architect at English startup Universal Quantum, and his team calculated the amount of qubits one would theoretically need to hack the formidable security system employed by bitcoin, the decentralized digital currency that's been a volatile investment, captured the attention of Elon Musk and become the symbol of a looming revolution in finance.

Short answer? Several millions more than IBM's mere 127-qubit processor lighting the way.

Bitcoin's quantum weakness

Bitcoin's security system is considered ultra-secure against classical computers, which is why it offers a terrific way to gauge quantum computing power. It's very complex, but here's what you need to know for our purposes.

Every time a transaction is made, two important things happen.

A public key, available to everyone, and a secure private key, visible only to the spender, are generated. This key combo is then digitally "written" onto a ledger of monetary transactions within the system, aka a blockchain.

After that, the transaction sort of "locks," thereby preventing anyone from doing anything with the associated funds. But there's a blindside: "When someone makes a transaction in bitcoin, it's announced to the world, but it's not completely secure until it has been integrated into the blockchain," Webber said.

In other words, between the public declaration of a transaction and the integration, there's a vulnerability window. Within that window, the funds can, technically, be manipulated. I say technically because that'd require algorithms so utterly complex even the strongest supercomputers don't have enough computing power to perform them -- and you can forget about humans manually attempting to. Quantum computers may, eventually.

"If you did have a quantum computer and it could function quickly enough, you could theoretically apply it to transactions routinely to re-divert [them] to a different address, for example," Webber said.

Though the window's general ballpark ranges from 10 minutes to a day, Webber says its finiteness makes it a particularly good test for "We've got a desired runtime, how many qubits do we need?"

But before we go any further, let's discuss where all this qubit power originates. It's thanks to two dazzling quantum features you won't believe aren't science fiction: superposition and entanglement.

Quick trip to qubit-land

Suppose I spin a coin on a table and ask, "Is it heads or tails?" You'd probably say, "What?" because my question doesn't make much sense. Before the coin settles on a side, it essentially exists as both options simultaneously. Think of this dizzying coin as being in a "superposition."

If you interrupt its superposition to examine its fate -- that is, make the coin stop spinning -- you can't bring back the exact state of limbo. Once you break superposition, it's broken forever.

Now let's modify the case to include two coins spinning next to each other. This time, I have a condition: If coin A lands on heads, so will coin B. These coins are now interdependent, so to speak. Each coin's superposition is "entangled" in the other's.

Adjustments to coin A's superposition instantaneously affect coin B's. Even if only coin A stops spinning, for instance, you gain knowledge about coin B – thus breaking its superposition, too. This would ring true even if the coins are on opposite ends of the universe.

OK, you're probably thinking: These analogies sort of depend on the mind of the observer. You're right. But that's because we're talking about coins. With quantum particles like electrons and photons, these things really, physically happen.

Traveling back to the quantum computing-verse, superposition determines the state of a bit. Classical bits exist as either 0 or 1, but qubits, made of quantum particles, can be in

superposition -- 0 and 1 at the same time. Most importantly, they retrieve data while still in that state.

As you can imagine, qubits zip through calculations at unfathomable speeds, testing several iterations simultaneously and entangling with other qubits to transmit information instantaneously. That's the general gist.

For context, Google and IBM quantum computers evenly distribute qubits on a grid, using what's called superconducting quantum hardware. Adjacent qubits can entangle to communicate information. Webber's company zeroes in on trapped ion hardware, which allows qubits to move freely and collaborate anywhere on a grid. Either way, though, more qubits equals exponentially more computing power.

But how many of these qubits must sync up to take advantage of bitcoin's vulnerability window?

Challenge accepted: Hack bitcoin

Here's what we know so far: Bitcoin transactions have a window during which they're vulnerable to quantum computers -- but not classical computers and definitely not people. That's because quantum systems are filled with qubits, firing away and performing calculations at speeds the human brain can barely comprehend.

Using external research, Webber laid out how many qubits are needed to penetrate that window, uncovering some solid estimations. But recall the delicacy of qubits. If anything goes wrong in a quantum computer, superposition is interrupted and all the precious quantum data can be lost forever. And things go wrong.

To prevent that disaster, quantum programmers do something rather intuitive. They just use more qubits. It's called quantum error correction.

Saving for simplification, they throw an army of qubits at every computation to increase the chances of correct data. For example, if 9/10 qubits offered the same solution, it'd be safe to say that's correct.

"To have one pretty high-quality, logical qubit -- it's not perfect, but it's good -- it's something like 1,000 physical qubits for one," Webber said. Thus, he multiplied his initial estimation by 1,000 to get a final answer.

Bingo, it'd take about 317 million qubits to hack bitcoin in one hour. If you're looking at a 10-minute window, "it would just be a larger number," he said. "Probably six times more." That would put the number of qubits into the billions. We're not even close to that point just yet.

"If you want to break it more slowly," Webber added, "it requires less qubits overall -- so something like 13 million to break it in one day."

Webber isn't the only one thinking about how quantum computing could bypass cryptocurrency security. The US National Institute of Standards and Technology, for instance, is on the hunt for quantum-proof cryptography algorithms to keep cryptocurrency secure, while the Ethereum Foundation is investigating notions of quantum resistance.

Though we've still got a ways to go before we arrive at a bitcoin quantum hack, Webber urges thinking about advances now: "Look at the transition of classical computing from vacuum

tubes of 10 bits, or however many they had early on, to the extremes that we have now. "Surely, quantum computing will go through a similar transition."

Source: https://www.cnet.com/news/quantum-hackers-could-break-bitcoin-in-minutes-but-dont-panic-just-yet/

Billy Bambrough
Forbes
05 February 2022

Congress Introduces A Radical Crypto Bill To 'Unleash Innovation' As The Price Of Bitcoin And Ethereum Suddenly Soar

Bitcoin and ethereum, the two largest cryptocurrencies have suddenly surged higher this week, with prices leaping following a much stronger than expected U.S. jobs report.

The bitcoin price, which has fallen sharply from a peak of almost $70,000 per bitcoin late last year, has bounced from a low of $32,000 in January, surging back above $40,000. The ethereum price has also jumped, rising 20% over the last week.

Now, a bipartisan group of U.S. House representatives has reintroduced a bill that would exempt people from paying taxes on bitcoin and crypto payments under $200, called "an important step forward" by one congressman.

"Virtual currency is reshaping our everyday lives, and the United States needs to recognize this and work to treat these currencies fairly in our tax code," congressman David Schweikert (R-Ariz.) said in a statement. "This legislation is an important step forward, and it lays the groundwork for growing the digital economy."

Designed to simplify tax burdens on daily crypto users who must now report even the smallest capital gains, the Virtual Currency Tax Fairness Act—an amendment to the Internal Revenue Service's tax code—was announced this week by crypto-friendly representatives Schweikert, Suzan DelBene (D-Wash.), Darren Soto (D-Fla.) and Tom Emmer (R-Minn.) and would retroactively apply to all qualifying transactions from December 31, 2021 if the legislation becomes law.

Emmer, Schweikert and Soto are co-chairs of the Congressional Blockchain Caucus, a congressional group that now counts 35 lawmakers as members.

"Not only will this create a level playing field for digital currencies, it will also help unleash innovation on applications like micropayments, which can consist of dozens of transactions per minute and thus are difficult to square with the current law," said Jerry Brito, executive director of cryptocurrency think tank Coin Center, who has lobbied for the bill.

Currently, bitcoin and crypto users must report changes in a cryptocurrency's value in dollars from when they purchased the crypto to when it was used in a transaction, including small retail purchases.

"While bitcoin and other cryptocurrencies are technologically innovative payment methods, today you have to keep track of and report every transaction you make using them, whether it's a $10,000 investment trade or whether you're buying a 99¢ song online or a latte at a café," added Brito. "This obviously creates friction and puts cryptocurrencies at a disadvantage relative to other digital payment methods."

Bitcoin and many other cryptocurrencies have developed a reputation as speculative investments over recent years as prices have rocketed higher, with few companies accepting bitcoin as a payment method.

The bitcoin price has surged 300% over the last two years with the ethereum price climbing at an even faster pace as demand for blockchain-based decentralized finance (DeFi) and collectible non-fungible tokens (NFTs) has exploded.

Technological developments such as the second layer bitcoin lightning network, allowing faster and cheaper bitcoin payments, and Tesla billionaire Elon Musk's backing of the meme-based bitcoin rival dogecoin have strengthened crypto's payment use-case. Last month, Tesla began allowing people to buy branded merchandise using dogecoin.

"As the use of virtual currencies for retail payments increases, it's important that Americans are able to easily understand their tax obligations," said Kristin Smith, executive director of the Blockchain Association. "By providing an exemption for small everyday purchases, the Virtual Currency Tax Fairness Act would ease this burden for consumers."

Source: https://www.forbes.com/sites/billybambrough/2022/02/05/congress-introduces-a-radical-crypto-bill-to-unleash-innovation-as-the-price-of-bitcoin-and-ethereum-suddenly-soar/?sh=b7821271aca5

Daren Fonda
Barron's
02 February 2022

Bitcoin Is Better Than Gold and National Currencies, According to Report

The world is awash in cash and cryptocurrencies, but Bitcoin is special, with the potential for significant price gains, according to a new report from Fidelity.

Bitcoin is a scarce "monetary good," superior in many ways to other cryptos, gold, and even government-issued money like the dollar, the firm said. "We would expect Bitcoin to be a lot higher five to 10 years from now," Chris Kuiper, director of research at Fidelity Digital Assets and author of the report, told Barron's in an interview.

Fidelity's application for an ETF based on the spot price of Bitcoin was recently rejected by the Securities and Exchange Commission. But the firm has launched a Bitcoin ETF and mutual fund in Canada, and it is seeking SEC approval for two crypto/metaverse ETFs.

As Fidelity sees it, the bull case for Bitcoin is that it's a "store of value asset in an increasingly digital world." No other blockchain network or token can match Bitcoin's advantages as the most "secure, decentralized, sound digital money," Kuiper wrote. While other digital assets and networks have some advantages—-notably Ethereum, with its programmable features–trying to improve on the Bitcoin network means making a trade-off in speed, scalability, or security.

While other tokens and networks battle it out, Kuiper said, Bitcoin's advantage as a store of value reduces its comparative risk. And while other tokens may have more potential for price gains, Bitcoin should hold its value as more people adopt it worldwide.

Bitcoin, in his view, also has advantages over gold. Both are scarce, with limits on the amount that can be mined. Bitcoin is more easily transported and stored and is impervious to counterfeiting, due to the security of its underlying blockchain network, he argues. Bitcoin's supply-inflation rate of 1.8% is equal to gold's annualized increase in supply, he notes.

Macro conditions may also favor Bitcoin, due to rising levels of debt in the legacy financial system, negative real interest rates, and the potential for traditional currencies to lose purchasing power, Kuiper argues.

To be sure, none of these arguments are particularly novel. And Bitcoin has many drawbacks. Among them: Its price instability makes it unsuitable for one of the prime functions of money–a medium of exchange. Mining Bitcoin is also environmentally costly, resulting in carbon emissions similar to those of small countries. And governments that view Bitcoin as a threat to their monetary sovereignty and policies–notably China–are restricting its use.

Kuiper proposes several counterarguments to those points. He says investors should think of Bitcoin as a store of value first and foremost. Its volatility is a consequence of the fact that its supply is limited while demand fluctuates wildly. "As more people adopt it, you'd expect the volatility to die down and its use as a medium of exchange to pick up," he says.

Governments, he argues, are learning to live with Bitcoin, rather than ban it. Russia and India appear more open to taxing and regulating it, he points out, and the U.S. government may be headed down a similar path with tighter regulations and tax policies.

As for the environmental toll, he points out that the network accounts for less than 1% of the world's energy usage, equivalent to the power consumption of domestic washers and dryers in the U.S. "The question for Bitcoin is whether it's a valuable use of resources," he says, but one could pose the same question about other energy uses, like videogames or washing machines.

For now, the market doesn't seem particularly receptive to the bullish case for Bitcoin. The token is still down nearly 50% from the record highs it hit last November, trading at around $37,500 early Wednesday afternoon.

Source: https://www.barrons.com/articles/bitcoin-gold-dollar-crypto-51643829216

MacKenzie Sigalos
CNBC
08 February 2022

Bitcoin donations are pouring into Ukraine as Russia masses troops on the border

As more than 100,000 Russian troops mass on the border with Ukraine — and global powers work to stave off all-out war between the two countries — new data shows that Ukrainians are crowdfunding bitcoin to fight back.

Donations totaling hundreds of thousands of dollars have flooded into Ukrainian nongovernmental organizations and volunteer groups, according to a report from Elliptic, which sells blockchain analytics tools to banks and some of the world's largest cryptocurrency platforms, including Binance and Circle.

Activists have deployed the crypto for a variety of purposes, including equipping the Ukrainian army with military equipment, medical supplies and drones, as well as funding the development of a facial recognition app that identifies if someone is a Russian mercenary or spy.

"Cryptocurrency is increasingly being used to crowdfund war, with the tacit approval of governments," said Tom Robinson, Elliptic's chief scientist.

Although Russia says it has no plan to mount an offensive, the U.S., U.K. and others have preemptively sent military hardware to Ukraine to help brace for a possible invasion.

Borderless and censorship-proof

For years, volunteer groups have augmented the work of Ukraine's military by offering additional resources and manpower. When Ukraine's pro-Russian president Viktor Yanukovych was ousted in 2014, for example, legions of organized volunteers stepped up to support protesters.

Typically, these organizations receive funds from private donors via bank wires or payment apps, but cryptocurrencies such as bitcoin have become more popular since they allow them to bypass financial institutions that might block payments to Ukraine.

"Cryptocurrency is particularly suited to international fundraising because it doesn't respect national boundaries and it's censorship-resistant — there is no central authority that can block transactions, for example in response to sanctions," said Elliptic's Robinson.

"The advantage of raising funds in crypto is that it's a lot harder to confiscate them," said Boaz Sobrado, a London-based fintech data analyst, who has advised charities in authoritarian countries, including former East bloc nations, on raising funds.

Volunteer groups and NGOs have collectively raised just over $570,000 in cryptocurrency, according to Elliptic's report. Much of that crypto cash was received in the last year.

Elliptic's software is sometimes used to investigate criminal activity on bitcoin's digital ledger and monitor transactions to fight money laundering. For this report, Elliptic identified multiple cryptocurrency wallets used by volunteer organizations across Ukraine, in order to trace where and how crypto funds are being put to use.

One such group, Come Back Alive, which began accepting cryptocurrency in 2018, provides the military with equipment, training services and medical supplies. The group says they saw bitcoin donations surge to $200,000 in the second half of 2021.

Another group, the Ukrainian Cyber Alliance, says it raises money exclusively in cryptocurrency. Over the past year, the group has received close to $100,000 in bitcoin, litecoin, ether and a mix of stablecoins. Since 2016, Alliance activists have engaged in cyberattacks against Russian targets, says Elliptic.

"Their operations have included attacks on propaganda sites, the Russian Ministry of Defense, and various individuals linked to Russia's activities in Ukraine. Intelligence collected during these operations is reportedly shared with Ukrainian law enforcement and intelligence agencies," according to the report.

Kyiv-based NGO Myrotvotrets Center has taken donations in crypto since 2016 and is currently working on a facial recognition app that would be able to identify "militants, Russian mercenaries, and war criminals" based on a photograph.

The organization — which says donations to its cause have come from more than 40 countries — already publishes information about people considered to be "enemies of Ukraine."

Thus far, the Myrotvotrets Center says it's raised at least $267,000 through more than 100 bitcoin donations.

Ukrainian activists aren't the only ones leaning into crypto.

Pro-Russian separatists have been raising funds in bitcoin since the early days of the Russo-Ukrainian conflict. Sobrado tells CNBC that some Russian officials mentioned they weren't shutting off opposition bank accounts for "fear they'd push them into crypto fundraising, which is a lot harder to monitor."

Sobrado went on to say that there is a long history of crypto fundraising for controversial causes, from WikiLeaks to Russian opposition politician Alexei Navalny, who has also been raising funds in bitcoin.

Ukraine's embrace of crypto

For months, Ukraine has taken steps to embrace cryptocurrencies at a national level.

Ukrainian President Volodymyr Zelenskyy signed a law in 2021 that paved the way for the country's central bank to issue its own digital currency.

The president and parliament are also going back and forth on a law that would legalize and regulate cryptocurrency. If the measure passes, it would go a long way toward elevating crypto out of the legal gray area where it currently sits, though it wouldn't go as far as El Salvador, which adopted bitcoin as legal tender in September.

On an official state visit to the U.S. in August 2021, Zelenskyy spoke of Ukraine's budding "legal innovative market for virtual assets" as a selling point for investment, and Minister of Digital Transformation Mykhailo Fedorov said the country was modernizing its payment market so that its national bank would be able to issue digital currency.

This year, the country plans to open the cryptocurrency market to businesses and investors, according to the Kyiv Post. Top state officials have also been touting their crypto street cred to investors and venture capital funds in Silicon Valley.

A war with Russia, however, could render all those plans moot.

Source: https://www.cnbc.com/2022/02/08/bitcoin-pouring-into-ukraine-as-russia-masses-troops-on-the-border.html