

Forum:[Hack Forums](#)

Thread: [What is preventing smart mathematicians from breaking bitcoin](#)

SIM-5602597 - February 8, 2025, 3:58 pm

Back in the old days if you broke a cryptographic algorithm you would probably work at a three letter agency and be rewarded a generous amount of money. Now with bitcoin this is a multi billion dollar problem. How do you think that affects crypto? What would be your reaction to hearing a multi billion dollar institute hiring many smart cryptographers to break bitcoin (although I doubt they will disclose that)? Personally I think bitcoin has no real future as there is now a lot of incentive to break it

SIM-5602597 - February 8, 2025, 5:20 pm

(Feb 8, 2025 05:31 PM)Lowkey Wrote: [\[CITE\]](#) It's the qubits bro!

<https://hackforums.net/showthread.php?tid=6287148>

We simply do not have enough qubits and neither do the spooky 3 letters!!!

Quantum computers might affect bitcoin but there is already quantum resistant algorithm that can be adopted and even then quantum computers are still a long way to go. I am talking from the side of mathematicians specifically going after bitcoin. I think one of bitcoin's main algorithms will be broken long before we have quantum computers

Heck, you will probably be in the top 10 richest people in the world at 100+ billion

DramaKing - February 8, 2025, 6:25 pm

(Feb 8, 2025 06:20 PM)MissAmFitamine Wrote: [\[CITE\]](#) Quantum computers might affect bitcoin but there is already quantum resistant algorithm that can be adopted and even then quantum computers are still a long way to go. I am talking from the side of mathematicians specifically going after bitcoin. I think one of bitcoin's main algorithms will be broken long before we have quantum computers

Heck, you will probably be in the top 10 richest people in the world at 100+ billion

AES and ECDSA are not codes that could be broken like the WWII Japanese code or even the Enigma cipher. Every wallet has its own keys. Effectively breaking the cryptography would be something like reversing public key algorithm.

If that happened you will be sitting on a pile of meaningless data.

SIM-5602597 - February 9, 2025, 6:43 am

(Feb 8, 2025 07:25 PM)DramaKing Wrote: [\[CITE\]](#) AES and ECDSA are not codes that could be broken like the WWII Japanese code or even the Enigma cipher. Every wallet has its own keys. Effectively breaking the cryptography would be something like reversing public key algorithm.

If that happened you will be sitting on a pile of meaningless data.

Reversing the public key would certainly break bitcoin but that is not the only way. Even an algorithm which can reverse SHA will also break bitcoin. These algorithms do not have to be completely broken. Any algorithm that can solve these faster than bruteforcing would be considered breaking them and would totally plummet the market when the news break out (enough for someone to make a lot of money). I think it is only a matter of time before retail investors realise they should be pouring money towards breaking these algorithms and we have a real test for bitcoin and

other cryptocurrencies

DramaKing - February 9, 2025, 7:51 am

(Feb 9, 2025 07:43 AM)MissAmFitamine Wrote: [\[CITE\]](#) Reversing the public key would certainly break bitcoin but that is not the only way. Even an algorithm which can reverse SHA will also break bitcoin. These algorithms does not have to be completely broken. Any algorithm that can solve these faster than bruteforcing would be considered breaking them and would totally plummet the market when then news break out (enough for someone to make a lot of money). I think it is only a matter of time before retail investors realise they should be pouring money towards breaking these algorithm and we have a real test for bitcoin and other cryptocurrencies

You mean like predicting what hash will be used to award the next block.

SIM-5602597 - February 9, 2025, 7:58 am

(Feb 9, 2025 08:51 AM)DramaKing Wrote: [\[CITE\]](#) You mean like predicting what hash will be used to award the next block.

Yes this will also kill btc there is still ~1m btc left to be mined and enough to make a lot of money for someone to go after

SIM-5602597 - February 13, 2025, 10:55 am

Any thoughts about this would love to hear some input?

Omniscient - February 13, 2025, 11:12 am

The moment Bitcoin is broken, it will be fixed within 24 hours, probably faster. It's like a power outage where everyone would just sit back and wait for the power to come back on. Bitcoin is a blockchain ledger, if it broke, people would know fast, fork to the last good block, and resume. It would happen very quickly, my guess is within 2 blocks everyone that mattered would know and within hours a fix in Bitcoin Core.

That fix is likely going to be introduced long before Bitcoin is even broken. If Quantum even gets close to breaking Bitcoin you'd see the fix.

Anyone really wanting to break Bitcoin would likely go after Satoshi wallet which is \$106 Billion in BTC stashed away.

SIM-5602597 - February 13, 2025, 1:44 pm

(Feb 13, 2025 12:12 PM)Omniscient Wrote: [\[CITE\]](#) The moment Bitcoin is broken, it will be fixed within 24 hours, probably faster. It's like a power outage where everyone would just sit back and wait for the power to come back on. Bitcoin is a blockchain ledger, if it broke, people would know fast, fork to the last good block, and resume. It would happen very quickly, my guess is within 2 blocks everyone that mattered would know and within hours a fix in Bitcoin Core.

That fix is likely going to be introduced long before Bitcoin is even broken. If Quantum even gets close to breaking Bitcoin you'd see the fix.

Anyone really wanting to break Bitcoin would likely go after Satoshi wallet which is \$106 Billion in BTC stashed away.

If bitcoin broke it will not recover. If SHA was broken what is preventing someone from recreating the entire blockchain and gaining a lot of bitcoin in the process. It would depend on trusting a third party having the correct blockchain which defeats the whole purpose of bitcoin. If ECDSA broke then one can empty all wallets. Even after a fix how can one prove that the coins belong to him if anyone can get the private key from the public key? That is without even mentioning if that were to happen the price will not recover due to trust lost by investors. Of course a lot of money would be made in the process shorting bitcoin

Omniscient - February 13, 2025, 1:51 pm

(Feb 13, 2025 02:44 PM)SIM-5602597 Wrote: [\[CITE\]](#) If bitcoin broke it will not recover. If SHA was broken what is preventing someone from recreating the entire blockchain and gaining a lot of bitcoin in the process. It would depend on trusting a third party having the correct blockchain which defeats the whole purpose of bitcoin. If ECDSA broke then one can empty all wallets. Even after a fix how can one prove that the coins belong to him if anyone can get the private key from the public key? That is without even mentioning if that were to happen the price will not recover due to trust lost by investors. Of course a lot of money would be made in the process shorting bitcoin

It's not going to happen. You may as well start a thread about if aliens invade Earth Bitcoin will be useless. It's about the same chance of happening.

Braco22 - February 13, 2025, 1:53 pm

Even if SOMEHOW (and according to how technology is progressing, it MAY be possible) this can happen, the miners can always FORK a quantum resistant update and things will be back to normal.

SIM-5602597 - February 13, 2025, 1:57 pm

(Feb 13, 2025 02:51 PM)Omniscient Wrote: [\[CITE\]](#) It's not going to happen. You may as well start a thread about if aliens invade Earth Bitcoin will be useless. It's about the same chance of happening.

Unfortunately, I do not share the same view. Attempting to break bitcoin requires sophisticated knowledge in math and statistics limiting the number of people who can attempt such a problem. If this seems ridiculous to you do you think if someone were to spend 1 billion purely to break an algorithm used by bitcoin it would hold up? I personally don't and I haven't heard of anyone attempting that (yet)

(Feb 13, 2025 02:53 PM)Braco22 Wrote: [\[CITE\]](#) Even if SOMEHOW (and according to how technology is progressing, it MAY be possible) this can happen, the miners can always FORK a quantum resistant update and things will be back to normal.

Forking a quantum resistant update would require you to re compute the blockchain from the begging essentially killing bitcoin

Omniscient - February 13, 2025, 2:31 pm

(Feb 13, 2025 02:57 PM)SIM-5602597 Wrote: [\[CITE\]](#) Unfortunately, I do not share the same view. Attempting to break bitcoin requires sophisticated knowledge in math and statistics limiting the number of people who can attempt such a problem. If this seems ridiculous to you do you think if someone were to spend 1 billion purely to break an algorithm used by bitcoin it would hold up? I personally don't and I haven't heard of anyone attempting that (yet)

Forking a quantum resistant update would require you to re compute the blockchain from the begging essentially killing bitcoin

You're a clown.

Did you come up with all this nonsense after taking drugs?

First you say it takes someone with "really smart math", then you say it's about money and a billion dollars could break the algo, so which fucking is it? Human genius or a fucking computer?

And Bitcoin in electricity alone costs nearly \$9 billion annually to mine and continue the blockchain.

Take your head out of your ass.

I'll give you an AI response which basically aligns with what everyone else is saying to your dumb ass. I plugged in your first post, told AI to respond.

AI Quote: Your point is interesting, but I'd argue that Bitcoin's security model is fundamentally different from traditional cryptographic systems used in government intelligence. Here's why:

1. Breaking Bitcoin is Not the Same as Breaking a Traditional Cipher:

- Classical cryptographic algorithms (e.g., DES, RSA, AES) could be broken with mathematical advances or brute-force attacks if sufficient computing power was available.
- Bitcoin's security relies on SHA-256 (for proof-of-work mining) and ECDSA (Elliptic Curve Digital Signature Algorithm) for securing private keys. These are battle-tested cryptographic primitives.

2. Incentives Make Breaking Bitcoin Unlikely:

- Even if a three-letter agency or a multi-billion-dollar institution tried to break Bitcoin, they'd likely gain more by using Bitcoin rather than destroying it.
- The financial system, corporations, and even governments are already integrating Bitcoin in various ways—why crash a system you could profit from?

3. Quantum Computing Threats Are Overstated (For Now):

- The most realistic way Bitcoin could be "broken" is through quantum computing breaking ECDSA.
- However, quantum-resistant cryptographic solutions (like Lamport signatures, lattice-based cryptography) are actively researched and can be integrated into Bitcoin if needed.

4. Even If Bitcoin Were Attacked, What Happens?

- Let's say some powerful entity found a vulnerability in SHA-256 or ECDSA.
- Would they announce it? Probably not.
- Would Bitcoin developers respond? Yes, Bitcoin can be hard-forked to implement quantum-resistant algorithms.

5. The Game Theory of Attacking Bitcoin:

- If a state or corporate entity tried to undermine Bitcoin, they'd effectively be devaluing their own asset holdings, harming institutional investors and reducing trust in cryptographic systems they also rely on.
- Instead, governments would likely regulate or control Bitcoin, not outright break it.

My Reaction to a Major Institution Trying to Break Bitcoin?

- Expected, but not a death sentence. Bitcoin is a multi-trillion-dollar asset class, so yes, high-level cryptographers are likely researching weaknesses.
- However, Bitcoin's decentralization, adaptability, and global interest make it more resilient than a single cryptographic system being broken overnight.

So while your skepticism is valid, Bitcoin's long-term survival isn't solely dependent on its current cryptographic algorithms—it's also about adaptability, network effects, and incentives. ?

Put the fucking drugs away.

SIM-5602597 - February 13, 2025, 2:58 pm

(Feb 13, 2025 03:31 PM)Omniscient Wrote: [CITE](#) First you say it takes someone with "really smart math", then you say it's about money and a billion dollars could break the algo, so which fucking is

it? Human genius or a fucking computer?

Human genius. While one smart mathematician might get lucky and break one of these algorithms to get a better chance you can get hundreds to increase your odds. This doesn't come cheap hence the money requirement. The rest of your post does not have any good reason as to why this won't happen and the only thing I made if that you did not like that possibility and as such have let your emotions get in the way while my posts have been kept purely rational.

AI Quote:

1. Breaking Bitcoin is Not the Same as Breaking a Traditional Cipher:

- Classical cryptographic algorithms (e.g., DES, RSA, AES) could be broken with mathematical advances or brute-force attacks if sufficient computing power was available.
- Bitcoin's security relies on SHA-256 (for proof-of-work mining) and ECDSA (Elliptic Curve Digital Signature Algorithm) for securing private keys. These are battle-tested cryptographic primitives.

While these algorithms have been here for a long time. Bitcoin introduces incentive to break them never seen before

AI Quote:

2. Incentives Make Breaking Bitcoin Unlikely:

- Even if a three-letter agency or a multi-billion-dollar institution tried to break Bitcoin, they'd likely gain more by using Bitcoin rather than destroying it.
- The financial system, corporations, and even governments are already integrating Bitcoin in various ways—why crash a system you could profit from?

A multi billion dollar institution would make way more if they knew how to break bitcoin than using it.

I can respond to each AI point made (and it is not really hard to argue against it) but I doubt you have read them yourself

Omniscient - February 13, 2025, 3:01 pm

Accept the fact you're a moron. This thread closed because my brain can't handle this level of stupid.