Why People Wonder if Bitcoin is Alien Technology

Tomer Strolight
11 min read
·
Jul 22, 2021

You can listen to my reading and discussion of this article on the Dumbest Guy in the Room Podcast here.

Where Did Bitcoin Come From?

We don't know.

It mysteriously appeared.
It was introduced by a mysterious figure.
Nobody knows their true identity.

Bitcoin is an invention.
Like all inventions, it does something that nothing before it did.
However, **Bitcoin is unlike any invention we have seen before.**
Many people who study Bitcoin closely eventually give their head a shake and say "**How did any person manage to come up with this?**". Often, for at least a moment, they are also struck by thought "**Was it even a person who came up with it?**". As a result, the Internet is filled with suppositions that Bitcoin was sent here by aliens or time travellers.

I will try here to point out those things about Bitcoin that lead to people wondering about its origin. To be very clear, **this is not an attempt to claim that Bitcoin came from outer space** or the distant future. It simply spotlights the aspects of Bitcoin which operate so differently from anything else we see on Earth that they make people wonder about the strange circumstances behind its creation. I do intend for this to be a fun way to learn about some of what makes Bitcoin so unique.

One-Of-a-Kind

Bitcoin appeared on Earth as an invention that satisfied a need all by itself: A need every person has; A need which was not being satisfied — The need for reliable money.

There was only one Bitcoin for the whole world (which was set to issue 21 million bitcoins). There wasn't one Bitcoin for you and one for me and one for Alice and one for Bob. **To this day, there remains only one Bitcoin,** but it is available to every human being on Earth. As we'll see later, **it will be available to all humans who ever live** on Earth, essentially forever.

Other inventions require being reproduced in mass quantities so that each person who wants the invention can have one of their own. You've got your computer, I've got mine. But when it comes to Bitcoin, we all share the one invention.

This itself is not *entirely* unique. Networks tend to have the property that they are 'shared' by all their users. You may be thinking, for example, about the Internet — Isn't there only one Internet?

Bitcoin is not like the Internet or other networks in many ways. **You don't have a copy of the whole Internet on your computer.** In fact, the Internet is a technology you use to access information that's specifically not in your possession, but is instead in someone else's. Because I want you to read this article, I posted it on a computer that will use "internet protocols" to send it to your computer. If I delete this article it goes away (unless someone made a copy). **What makes Bitcoin unique is that it is a network that self-replicates in its entirety** in a way unlike anything we've ever seen before on Earth.

Self-Replication of a Different Kind

Replication Unlike Other Man-Made Things

Bitcoin is **self**-replicating. When anyone starts up *Bitcoin Core* it will begin working on creating a perfect, flawless replica of the entire Bitcoin blockchain — all the data in the Bitcoin network — from the genesis block of data, to the most recent one.

No other human invention is self-replicating. Everything else is replicated, manufactured or produced by people creating a copy. No two copies of anything physical can be truly exactly alike due to some imperfections somewhere in the production process.

We can make perfect digital copies of songs or software, but even in these cases that is because they are static, unchanging content. **If you add a note to your copy of a song, it doesn't change on every copy of the song everywhere in the world.** However, Bitcoin is constantly adding data to its network, and **what gets added anywhere, gets added, perfectly, flawlessly, everywhere**. Nothing else on Earth does this — not in the way Bitcoin does.

Replication Unlike Life

There are other things here on Earth that exhibit the property of self-replication. Not human inventions, but living things. Living things self-replicate. Single cells divide into two cells — often identical to each other (but sometimes taking on different attributes).

Does Bitcoin simply mimic life then? No, **Bitcoin doesn't self-replicate the way life does**. Unlike every new living cell that comes into existence, which has a 'sister' cell (since we can't say after a cell division which is the mother and which is the daughter), **every new instance of Bitcoin that is spawned does not come from a single previous instance**.

The process a new Bitcoin instance utilizes to replicate itself is that **it looks across the entire world to *many* other instances** of Bitcoin and begins replicating the data from them that makes it Bitcoin — that data is known as the blockchain. **It does not have one parent cell** or instance. Rather it checks with many instances to ensure they are all alike to avoid any discrepancy between itself and any other copies.

Living cells can (and do) introduce discrepancies in their replication from previous generations because they have no mechanism to check with other cells about what their 'correct' construction should be. Such discrepancies are called 'mutations'. However, **every Bitcoin instance checks in with numerous, random other existing instances. This ensures it contains no deviation, no mutation, from any other instance**. A Bitcoin instance never stops doing this. All the instances of Bitcoin in the world do this — every single one. Constantly. **They are *all* constantly checking in with the others to make sure they're each perfectly identical to one other.**

Doesn't this seem 'alien'? It's not like anything we've ever built and it's not like the living things we see on Earth either.

Leaderless, But Identical, Honoring Only Work as Their Leader

There is no instance of Bitcoin that is the *leader*. None has any rank different than any other. They are all exactlly the same. **Any instance can propose a new state of the blockchain to the others.** If its proposal is valid, all the instances it is connected to will accept its proposal and send the new, valid state to all the others they are connected to. All those others will also accept that proposed change. This will repeat until every instance in the world is in perfect synchronization again. Can you think of anything else on Earth that does this?

How does a proposal to change state achieve *validity*? There is only one way. That proposal must demonstrate, through a mathematical proof, that it performed enough computational work to surpass the threshold of work that is required to produce a new valid state. All instances agree on the identical threshold required, because it is calculated mathematically from the previous state that they all share identically. (The new proposal must actually even further demonstrate it achieved a higher threshold of work than any other competing proposal. If two instances have proposed two different valid proposals the one whose proposal eventually produces another valid proposal demonstrating more work will be deemed by all instances to be the valid one — even the one that issued the competing proposal.) **As a result, all instances will remain in perfect synchronization. Without any one of them having any special privelege or authority**.

Work is the only thing the network values, respects and obeys. Work alone. Not authority. Not title. Not rank. Not wealth. These first three things do not exist in Bitcoin. The fourth, wealth, does not matter. Bitcoin honors work and work alone — only work that can be proven to have been done. We've already seen that Bitcoin's self-replication is unlike anything else we've seen on Earth, and here we see this self-replication does not rely on any violence, tolerates no deception, and surrenders to nothing. It accomodates only hard work. Can you think of anything else on Earth in which this is the standard? I can't. It is benevolent and fair to an unprecedented degree.

Self-Adjusting, But Improvable

Every human invention eventually wears out, breaks, or at the very least needs ongoing maintenance to prevent it from falling apart. Every living thing eventually dies. Not Bitcoin.

Bitcoin doesn't come with a warranty to replace it if it breaks, because it has no maker. Fortunately, it will never need repairing. That's pretty different than anything else we've seen humans invent.

Bitcoin can just run forever. It's designed to operate at a steady pace either with lots of work put into it or with very little. It *self-adjusts*.

Bitcoin Adjusts Itself and Refuses Any Other Adjustments

To be clear — **the only adjustments that can be made to Bitcoin are the adjustments it *makes by itself to itself***. Nobody else can adjust it.

If you try to change Bitcoin's adjustment algorithm your instance of Bitcoin will halt or die.

If you try to make the work requirement harder your instance will soon fail to accept as valid a block that contains enough work as agreed to by all the other instances except yours. It will then fail to receive any other blocks ever again because all future blocks will depend on the one you rejected. If you try to make the work requirement easier you risk being attacked and forked off by anyone who tricks you into accepting an easier block than the rest of the network required. **Bitcoin will not tolerate anyone adjusting it**.

This isn't like someone selling you a device and saying "You're not *allowed* to modify it." Bitcoin's code is *open source*. You are welcome to modify it. It will just not be Bitcoin if you do. And you don't need a mechanic to maintain it.

There is a small exception to this — we do update Bitcoin Core from time to time with improvements that are related to usability or speed of performance. This is the human interface side of Bitcoin though and not the Bitcoin part of it. You don't need to install these updates though. They affect nothing fundamental.

New Rules Can Be Added, None Can Ever Be Taken Away

Also, quite rarely, we even modify Bitcoin to allow for new types of transactions — what we call soft forks. We don't have to do this. Bitcoin doesn't need these to survive. Bitcoin will continue to work without these modifications. We do it because we think there are new technologies that can make Bitcoin better. Bitcoin only lets us do this under certain conditions:

When this happens, **these modifications can not violate any of the previous rules.** If they tried to, they would be rejected just as in the hypothetical attempt to adjust Bitcoin's work requirement above.

Theses soft forks are the introduction of new, additional rules. They are not a changing of the previous rules to violate any of them. Rather, they allow for new things to be done by introducing new rules. What other invention on Earth does this? **What other invention on Earth adds features by making its rules stricter?**

For example, when governments pass new restrictions it means we can do less things. When Bitcoin does it, it means we have the option to do more. This feature of Bitcoin is so counterintuitive, so different from anything we've seen before that it again looks unearthly.

Everlasting

What about running out of space or running out of capacity. Bitcoin won't run out of either. It's database, the blockchain, has infinite size potential. It already has built in the capacity to create trillions of addresses for everyone who will ever live without needing any upgrade. As far as how much work it can handle, it has the capacity to absorb more than all the energy stored in the sun itself.

Did I really just seriously say that Bitcoin already has built into it the capacity to absorb the entire energy of the sun, and more?

Yes.
Am I exaggerating?
No.

Bitcoin has a variable called “cumulative proof of work” which adds up all the work that went into creating the blockchain from Bitcoin’s genesis block until the present. This is how each instance of Bitcoin determines which proposals have the most work and are therefore the correct one. The variable Bitcoin uses for this is 256 bits long, which is big enough to store all that energy and more.

What human engineer would build this much ‘slack’ into their design? Certainly not the human programmers who wrote those mainframe apps in the 70s, 80s and 90s that didn’t think ahead a couple of decades and required that the whole world make huge preparations and adjustments for the Y2K (year 2000) bug.

Whoever created Bitcoin didn’t just plan ahead a few decades. They planned ahead billions of years. They planned ahead for longer than mankind has been around; for longer than life on earth has been around; for longer even than the earth has been around. **What human being designs something to last for that duration?**

I wish people engineered things to be self-replicating, self adjusting, self-governing, and ever-lasting. But nobody has engineered anything to do even one of these, and then along comes Bitcoin and does them all — Mysteriously appearing out of nowhere, and spreading everywhere in a short period of time. This is why some people wonder if it is of human origin.

Becoming Exponentially Scarcer Over 130 Years

What about the four year cycles after which Bitcoin cuts its issuance of new bitcoins by half? **No other human invention increasingly restricts the supply of the thing people find valuable about it**. Bitcoin does.

Humans usually design each invention to be ‘scaled up’ in supply as rapidly as possible. Not Bitcoin. It was designed to ‘scale down’ its new supply. Not gradually and smoothly, but suddenly — although very predictably. Not in a linear fashion, which humans can easily understand, but in an exponential fashion, which humans do not easily understand.

Nothing else on Earth, no human invention and no life form, exhibits any of these traits. So again, even in this, Bitcoin is like nothing else on Earth.

Why 130 Years of Issuance?

I myself wonder why does this halving event take place every four years? Why not every single year or why not every ten years? Is one year too short to incentivize humans to accumulate bitcoin? Is ten years too long to expect them to wait? I don’t know.

However, one thing that this four year cycle leads to is that the total issuance period of Bitcoin's 21 million coins takes about 130 years from start to finish. This is just safely outside the range of the longest human life ever documented of 122 years. Maybe that has something to do with it. Maybe it doesn't. I don't know.

What this does mean is that when the issuance period is completed, probably every living person will not have ever lived a day in their life in which Bitcoin did not exist on Earth. Bitcoin is taking its time to complete its issuance until every human on Earth has never known a world without it — and that includes the mysterious person who created it, if, in fact, he was human.

/FIN

Want to see where this leads? Read this story of what we'll do over billions of years thanks to Bitcoin: