

# How to prove you are Satoshi Nakamoto - the father of Bitcoin?

It is not recognized that Satoshi Nakamoto will be recognized.

The world of bitcoin from its birth, is always curious about who invented this currency. Especially with the present value, this person is among the 50 richest people in the world.

But it is not allowed to claim to be Satoshi Nakamoto and it will be recognized. Many times the bitcoin community thought of finding this father but all missed when the 'candidate' could not prove he was the father of bitcoin. Thankfully for Satoshi Nakamoto himself and for those who have been waiting for this mysterious person, there are certain ways for this character to prove himself. According to bitcoin experts and cryptographers, there are many ways and each with different levels of certainty.

The creator of Bitcoin will get the **key to control the first bitcoins** on his or others' computers. These bitcoins have never been moved during their eight-year history, despite their current value of a billion dollars according to the Bitcoin exchange rate.

This treasure is kept on several bitcoin addresses, each containing 50 bitcoins, protected by a key sequence - a string of characters - which is theoretically only known to Nakamoto. Who owns this key segment can move them to another address. 'It's unmistakable,' said cryptographer Matthew Green, 'you'll see a lot of old money moving. That is the miracle that I want to witness.'



It's just that Satoshi Nakamoto hasn't (no?) Wanted to show up

But with Jerry Brito, the director of Coin Center - a virtual money research center - that's not enough. Brito says that Nakamoto must have the **Genesis Block key - the first block of bitcoin** , opening the bitcoin transaction book called Blockchain. Because of its own design, these Genesis Block bitcoin cannot be moved or usable - but the key can be used to sign messages. According to Brito, Satoshi really didn't just sign the message with that key, but also signed many messages from the first few bitcoins.

If you only own one or two first blocks that are not Genesis Block or the first few coins, then Brito is in doubt. 'Why just own a key? If it's Satoshi, you have to sign and move money from the first few blocks. '

There is also a **PGP key** that is said to be Nakamoto used on the PGP server operated by MIT. But Brito pointed out that Nakamoto's PGP was never actually used to sign anything, so it was difficult to prove. In addition, the key can be stolen when the computer is hacked or shared the key for others.

Gavin Andresen, one of the few people in the world who exchanged emails with Satoshi Nakamoto before he disappeared from the Internet in 2011 also gave a list to the father of bitcoin to prove himself. Including the message with Nakamoto PGP key and the first key from the bitcoin block, his private correspondence with Andresen.

See more:

1. Whoever the father of Bitcoin is, he is also in the top 50 richest people in the world
2. Why is the price of bitcoin so high?
3. Guide to digging Bitcoin for beginners

You finished reading the article "**How to prove you are Satoshi Nakamoto - the father of Bitcoin?**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.