

---

## Satoshi Nakamoto and the NSA

It is no secret that the identity of Satoshi Nakamoto, the mind behind Bitcoin's blockchain and the first promoter of crypto money life in the world, has been a mystery to his followers. However, it is not hard to believe that Bitcoin is actually the product of the creation of the U. S. National Security Agency. Satoshi Nakamoto means "Central Intelligence" in Japanese, which cannot be a coincidence. The image of Nakamoto-san is said to have been sold for the purpose of representing an ideal and maintaining the anonymity of the people involved in the project. But it's hard to believe that a group of programmers (or just one individual, to make it harder) has been so devoid of ego that they didn't want to brag about the fame they would get for the brilliance of their concept and the innovation that came with their ideas. In addition, no one has ever met Satoshi Nakamoto in person, and there is no conclusive evidence that can lead to his identification.

This means that, in the case of an individual, that person would certainly have intelligence training, since staying under the shadows for such a long time would be quite difficult for an average programmer. Other evidence includes the fact that Bitcoin uses a common encryption program to create secure passwords, which is believed to have a backdoor to NSA; numerous Reddit threads linking Bitcoin or Satoshi Nakamoto to NSA have been removed; and that Bitcoin is not decentralized, as it is being controlled by a small group led by Gavin Bell, one of the developers at the top. Claims that the NSA created Bitcoin have actually been released for years. As you know, the NSA invests millions of dollars in encrypting your information and may be one of the clues to assume that they are one of the main agencies that may be behind the creation of this virtual currency. In itself, it does not represent anything negative, since it is part of a temporary support for the world economy and trying to bring out new financial products, trying not to notice a drastic fall that would call into question the incompetence of our leaders and the management of the economy they are currently leading.

The NSA was one of the first organizations to describe a Bitcoin-like system. About twelve years before Satoshi Nakamoto published his legendary white paper on Metzdown. com's Cryptography mailing list, a group of NSA information security researchers published an article titled How to Make a Mint: Anonymous Electronic Money Cryptography in two prominent locations, being an MIT mailing list and the second is much more prominent, The American Law Review. The paper describes a system very similar to Bitcoin in that secure financial transactions are made possible through the use of a decentralized network to which researchers informally refer as the Bank. They list four things as indispensable in their proposed network: privacy, user identification (protection against impersonation), message integrity (protection against manipulation/substitution of transaction information - that is, protection against double

---

### Need help with the assignment?

Our professionals are ready to assist with any writing!

**GET HELP**

---

expenditure) and non-rejection (protection against subsequent denial of a transaction - a chain of blocks!). People have wondered why it uses the SHA-256 hash function, which was designed by the NSA and published by the National Institute for Standards and Technology (NIST).

The fact that the NSA is linked to the SHA-256 leads some to assume that it has created a backdoor to the hash function that no one has ever identified, allowing it to spy on Bitcoin users. Assuming that the NSA did something to the SHA-256 that no outside investigator has detected, what it gets is the ability, with credible and detectable action, to falsify transactions. The really scary thing is that someone finds a way to find collisions on the SHA-256 really fast without forcing or using a lot of hardware and then take control of the network. It is clear that SHA-256, the algorithm Satoshi used to secure Bitcoin, was not available because it was produced in 2001. However, SHA-1 would have been available, having been published in 1993. If Satoshi was, in fact, an individual who was part of the NSA, why not just claim ownership of the identity? Most importantly, if Satoshi Nakamoto-san is a real person, not a group that wants to remain secret, why not come forward and claim his nearly billions of dollars worth in Bitcoin? The identity of Bitcoin's creator causes constant controversy and, while several people have been attributed with his name, it always turns out to be a deception, although in this case, it is usually very ambitious and carefully planned. Behind the whole tangle of "convincing evidence" that has just arisen there are interests that seem very obvious: making Bitcoin regain the popularity that it has lost in recent years and, above all, making one of the factions involved with its economic model the dominant one. Further to the point about Bitcoin's success, it is impossible to deny that its design is very solid, robust, manageable, which proves this is not just any student's job. Of course, logically, the NSA employs individuals and ultimately is the work of mathematicians, programmers, and cryptographers, but if we deduce that the most likely group is able, willing and motivated to embark on such a project, suspect. Universities, on the other hand, did not produce such white papers from 1996 onwards.

The NSA has the capability, motive and operational capability - they have the cryptographic equipment, the world's fastest supercomputers, and they see the need. Whether instructed by friends at the Fed, in cooperation with their owners, or as part of a DARPA project, it is not clear and will never be known. In fact, the NSA employs some of the best mathematicians and cryptographers in the world. Few people know their work because it's a secret, and this is not the kind of work you leave behind to create your own cryptography company. Why does the NSA want to do this? A simple reason: Control.

As we explained in the penny division, the main U. S. media dominates the world is through economic policy, albeit backed by bombs. And the primary support of the US dollar is primarily military. The connection between the military system and the US dollar is inextricably intertwined. There are thousands of great examples, only one of them is how Iraq changed to the Euro just before the invasion of the Army. In October 2000, Iraq insisted on dumping the US

---

## Need help with the assignment?

Our professionals are ready to assist with any writing!

**GET HELP**

---

dollar for the more multilateral euro. The changeover was announced almost exactly the same day that the euro reached its lowest point, buying only \$0.82, and the G7 finance ministers were forced to bail out the currency. By Friday, the euro had reached \$1.08, 30 percent more than then. Almost all of Iraq's oil exports under the United Nations oil-for-food programme were paid in euros since 2001. Some €26 billion (£17.4 billion) has been paid for 3.3 billion barrels of oil in a blocked account in New York. The Iraqi account, held at BNP Paribas, has also been earning a higher interest rate in euros than it would have in dollars. The point here is that there are a lot of different types of control. The NSA monitors and collects literally all electronic communications; internet, phone calls, everything. They even listen to voice calls encrypted with high-powered microphones, devices such as cell phones equipped with recording devices. It is very difficult to communicate on planet Earth in private, without being heard by the NSA. Therefore, it is logical that they also want full control of the financial system, including records of all electronic transactions, which Bitcoin provides. Could there be an "additional" layer of security in the undetectable Blockchain that would allow the NSA to view more transaction information, such as network location data? It wouldn't be so extravagant, considering his previous work, as the Xerox copiers that kept a record of all the copies made. Of course, security experts will point out the fact that this layer is still invisible, but if it exists, it would be hidden.

---

## Need help with the assignment?

Our professionals are ready to assist with any writing!

[GET HELP](#)