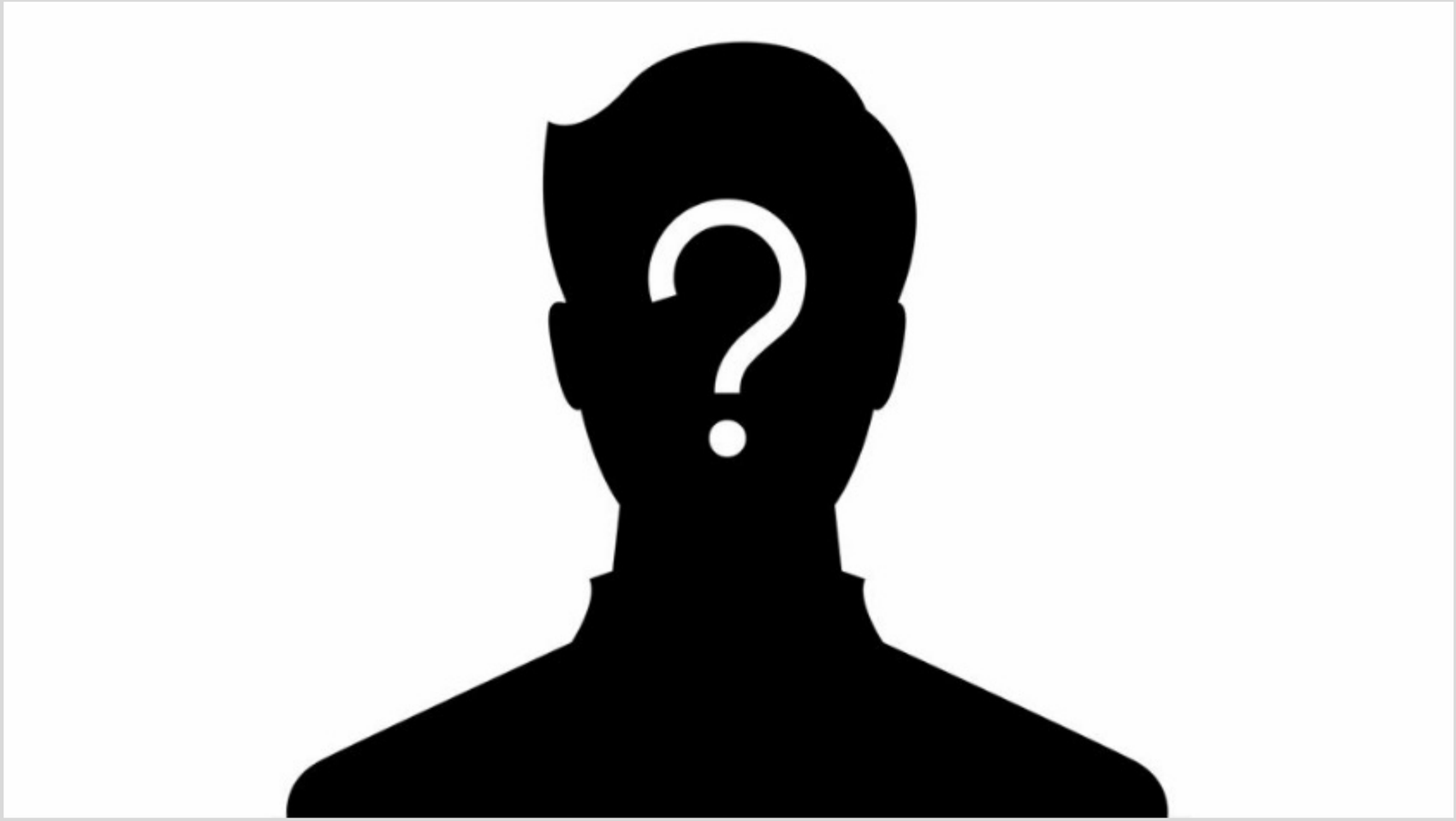


# WHO IS SATOSHI NAKAMOTO?

# MYSTERY MAN

While we may not know who he (or she) was, we know what he did. Satoshi Nakamoto was the inventor of the bitcoin protocol, publishing a paper via the Cryptography Mailing List in November 2008.

He then released the first version of the bitcoin software client in 2009, and participated with others on the project via mailing lists, until he finally began to fade from the community toward the end of 2010.

Nakamoto worked with people on the open-source team, but took care never to reveal anything personal about himself, and the last anyone heard from him was in the spring of 2011, when he said that he had "moved on to other things".

But he was Japanese, right?

Best not to judge a book by its cover. Or in fact, maybe we should.

"Satoshi" means "clear thinking, quick witted; wise". "Naka" can mean "medium, inside, or relationship". "Moto" can mean "origin", or "foundation".

Those things would all apply to the person who founded a movement by designing a clever algorithm. The problem, of course, is that each word has multiple possible meanings.

We can't know for sure whether he was Japanese or not. In fact, it's rather presumptuous to assume that he was actually a 'he'.

We're just using that as a figure of speech, but allowing for the fact that this could have been a pseudonym, 'he' could have been a 'she', or even a 'they'.

# DOES ANYONE KNOW WHO NAKAMOTO WAS?

No,  but the detective techniques that people use when guessing are sometimes even more intriguing than the answer. The New Yorker's Joshua Davis believed that Satoshi Nakamoto was Michael Clear, a graduate cryptography student at Dublin's Trinity College.

He arrived at this conclusion by analyzing 80,000 words of Nakamoto's online writings, and searching for linguistic clues. He also suspected Finnish economic sociologist and former games developer Vili Lehdonvirta.

Both have denied being bitcoin's inventor. Michael Clear publicly denied being Satoshi at the 2013 Web Summit.

Anonymous group of peopleAdam Penenberg at FastCompany disputed that claim, arguing instead that Nakamoto may actually have been three people: Neal King, Vladimir Oksman, and Charles Bry. He figured this out by typing unique phrases from Nakamoto's bitcoin paper into Google, to see if they were used anywhere else.

One of them, "computationally impractical to reverse," turned up in a patent application made by these three for updating and distributing encryption keys. The bitcoin.org domain name originally used by Satoshi to publish the paper had been registered three days after the patent application was filed.

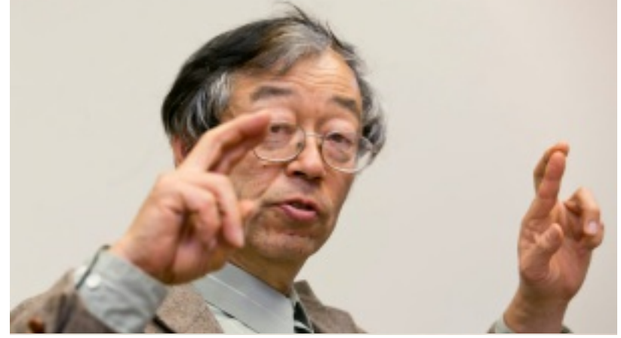
It was registered in Finland, and one of the patent authors had traveled there six months before the domain was registered. All of them deny it. Michael Clear also publicly denied being Satoshi at the 2013 Web Summit.

In any case, when bitcoin.org was registered on August 18th 2008, the registrant actually used a Japanese anonymous registration service, and hosted it using a Japanese ISP. The registration for the site was only transferred to Finland on May 18th 2011, which weakens the Finland theory somewhat.

Others think that it was Martii Malmi, a developer living in Finland who has been involved with bitcoin since the beginning, and developed its user interface.

A finger has also been pointed at Jed McCaleb, a lover of Japanese culture and resident of Japan, who created troubled bitcoin exchange Mt. Gox and co-founded decentralized payment systems Ripple and later Stellar.

MorCryp



Another theory suggests that computer scientists Donal O'Mahony and Michael Peirce are Satoshi, based on a paper that they authored concerning digital payments, along with Hitesh Tewari, based on a book that they published together. O'Mahony and Tewari also studied at Trinity College, where Michael Clear was a student.

Israeli scholars Dorit Ron and Adi Shamir of the Weizmann Institute retracted allegations made in a paper suggesting a link between Satoshi and Silk Road, the black market web site that was taken down by the FBI in October 2013. They had suggested a link between an address allegedly owned by Satoshi, and the site. Security researcher Dustin D. Trammell owned the address, and disputed claims that he was Satoshi.

In May 2013, Internet pioneer Ted Nelson threw another hat into the ring: Japanese mathematician Professor Shinichi Mochizuki, although he admits that the evidence is circumstantial at best.

In February 2014, Newsweek's Leah McGrath Goodman claimed to have tracked down the real Satoshi Nakamoto. Dorian S Nakamoto has since denied he knows anything about bitcoin, eventually hiring a lawyer and releasing an official statement to that effect.

## DORIAN SATOSHI NAKAMOTO

No, Satoshi Nakamoto is not a 64-year-old Japanese man living in California, probably...
Hal Finney, Michael Weber, Wei Dai and several other developers were among those who are periodically named in media reports and online discussions as potential Satoshis. A group of forensic linguistics experts from Aston University believe the real creator of bitcoin is Nick Szabo, based upon analysis of the Bitcoin White Paper.

Dominic Frisby, a comedian and a writer, also suggests that BitGold creator Szabo was the most likely candidate to be Satoshi in his book, "Bitcoin: The Future of Money". His detailed analysis involved the linguistics of Satoshi's writing, judging the level of technical skill in C++ and even Satoshi's likely birthday. In Nathaniel Popper's book, 'Digitial Gold', released in May 2015, Popper reveals that in a rare encounter at an event Szabo again denied that he was Satoshi.

Then in early December 2015, reports by Wired and Gizmodo tentatively claimed to have identified Nakamoto as Australian entrepreneur Craig S Wright. WIRED cited "an anonymous source close to Wright" who provided a cache of emails, transcripts and other documents that point to Wright's role in the creation of bitcoin. Gizmodo cited a cache of documents sourced from someone claiming to have hacked Wright's business email account, as well as efforts to interview individuals close to him. The idea that the Wright-Satoshi connection is nothing but a hoax has been floated by observers, though the compelling nature of the evidence published will no doubt fuel speculation for some time to come.

## SO WHAT DO WE KNOW ABOUT HIM?

One thing we know, based on interviews with people that were involved with him at an early stage in the development of bitcoin, is that he thought the system out very thoroughly.

His coding wasn't conventional, according to core developer Jeff Garzik, in that he didn't apply the same rigorous testing that you would expect from a classic software engineer.

## HOW RICH IS HE?

An analysis by Sergio Lerner, an authority on bitcoin and cryptography, suggests that Satoshi mined many of the early blocks in the bitcoin network, and that he had built up a fortune of around 1 million unspent bitcoins. That hoard would be worth $1bn at November 2013's exchange rate of $1,000.

## WHAT IS HE DOING NOW?

No one knows what Satoshi is up to, but one of the last emails he sent to a software developer, dated April 23 2011, said "I've moved on to other things. It's in good hands with Gavin and everyone."

## DID HE WORK FOR THE GOVERNMENT?

There are rumors, of course. People have interpreted his name as meaning "central intelligence", but people will see whatever they want to see. Such is the nature of conspiracy theories.

The obvious question would be why one of the three-letter agencies would be interested in creating a cryptocurrency that would subsequently be used as an anonymous trading mechanism, causing senators and the FBI alike to wring their hands about potential terrorism and other criminal endeavors. No doubt conspiracy theorists will have their views on that, too.

Perhaps it doesn't matter. Core developer Jeff Garzik puts it succinctly. "Satoshi published an open-source system for the purpose that you didn't have to know who he was, and trust who he was, or care about his knowledge," he points out. Open-source code makes it impossible to hide secrets. "The source code spoke for itself."

Moreover, it was smart to use a pseudonym, he argues, because it forced people to focus on the technology itself rather than on the personality behind it. At the end of the day, bitcoin is now far bigger than Satoshi Nakamoto.

# DID HE WORK FOR THE GOVERNMENT?

There are rumors, of course. People have interpreted his name as meaning "central intelligence", but people will see whatever they want to see. Such is the nature of conspiracy theories.

The obvious question would be why one of the three-letter agencies would be interested in creating a cryptocurrency that would subsequently be used as an anonymous trading mechanism, causing senators and the FBI alike to wring their hands about potential terrorism and other criminal endeavors. No doubt conspiracy theorists will have their views on that, too.

Perhaps it doesn't matter. Core developer Jeff Garzik puts it succinctly. "Satoshi published an open-source system for the purpose that you didn't have to know who he was, and trust who he was, or care about his knowledge," he points out. Open-source code makes it impossible to hide secrets. "The source code spoke for itself."

Moreover, it was smart to use a pseudonym, he argues, because it forced people to focus on the technology itself rather than on the personality behind it. At the end of the day, bitcoin is now far bigger than Satoshi Nakamoto.

MorCryp