BUSINESS DAY

Decoding the Enigma of Satoshi Nakamoto and the Birth of Bitcoin

By NATHANIEL POPPER MAY 15, 2015

Minh Uong/The New York Times

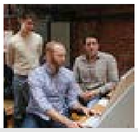
It is one of the great mysteries of the digital age.

The hunt for Satoshi Nakamoto, the elusive creator of Bitcoin, has captivated even those who think the virtual currency is some sort of online Ponzi scheme. A legend has emerged from a jumble of facts: Someone using the name Satoshi Nakamoto released the software for Bitcoin in early 2009 and communicated with the nascent currency's users via email — but never by phone or in person. Then, in 2011, just as the technology began to attract wider attention, the emails stopped. Suddenly, Satoshi was gone, but the stories grew larger.

Over the last year, as I worked on a book about the history of Bitcoin, it was hard to avoid being drawn in by the almost mystical riddle of Satoshi Nakamoto's identity. Just as I began my research, Newsweek made a splash with a cover article in March 2014 claiming that Satoshi was an unemployed engineer in his 60s who lived in suburban Los Angeles. Within a day of publication, however, most people knowledgeable about Bitcoin had concluded that the magazine had the wrong man.

RELATED COVERAGE

The Money Issue: Can Bitcoin Conquer Argentina? APRIL 29, 2015



Data Security Is Becoming the Sparkle in Bitcoin MARCH 1, 2015

While regulators debate the pros and cons of bitcoins, this volatile digital currency inspires the question: What makes money, money? By Channon Hodge, David Gillen, Kimberly Moy and Aaron Byrd on November 24, 2013.

Many in the Bitcoin community told me that, in deference to the Bitcoin creator's clear desire for privacy, they didn't want to see the wizard unmasked. But even among those who said this, few could resist debating the clues the founder left behind. As I had these conversations with the programmers and entrepreneurs who are most deeply involved in Bitcoin, I encountered a quiet but widely held belief that much of the most convincing evidence pointed to a reclusive American man of Hungarian descent named Nick Szabo.

Mr. Szabo is nearly as much of a mystery as Satoshi. But in the course of my reporting I kept turning up new hints that drew me further into the chase, and I even stumbled into a rare encounter with Mr. Szabo at a private gathering of top Bitcoin programmers and entrepreneurs.

At that event, Mr. Szabo denied that he was Satoshi, as he has consistently in electronic communications, including in an email on Wednesday. But he acknowledged that his history left little question that he was among a small group of people who, over decades, working sometimes cooperatively and sometimes in competition, laid the foundation for Bitcoin and created many parts that later went into the virtual currency. Mr. Szabo's most notable contribution was a Bitcoin predecessor known as bit gold that achieved many of the same goals using similar tools of advanced math and cryptography.

It may be impossible to prove Satoshi's identity until the person or people behind Bitcoin's curtain decide to come forward and prove ownership of Satoshi's old electronic accounts. At this point, the creator's identity is no longer important to Bitcoin's future. Since Satoshi stopped contributing to the project in 2011, most of the open-source code has been rewritten by a group of programmers whose identities are known.

But Mr. Szabo's story provides insight into often misunderstood elements of Bitcoin's creation. The software was not a bolt out of the blue, as is sometimes assumed, but was instead built on the ideas of multiple people over several decades.

This history is more than just a matter of curiosity. The software has come to be viewed in academic and financial circles as a significant computer science breakthrough that may reshape the way money looks and moves. Recently, banks like Goldman Sachs have taken the first steps toward embracing the technology.

Mr. Szabo himself has continued to be quietly involved in the work. In the beginning of 2014, Mr. Szabo joined Vaurum, a Bitcoin start-up based in Palo Alto, Calif., that was operating in stealth mode and that aimed to build a better Bitcoin exchange. After his arrival, Mr. Szabo helped reorient the company to take advantage of the Bitcoin software's capability for so-called smart contracts, which enable self-executing financial transactions, according to people briefed on the company's operations who spoke on condition of anonymity.

After Mr. Szabo led the company in a new direction, it was renamed Mirror, and it recently raised $12.5 million from several prominent venture capitalists, these people said. The company declined to comment for this article.

Mr. Szabo's role at Vaurum has been kept a secret because of his desire for privacy, and he left in late 2014 after becoming nervous about public exposure, according to the people briefed on the company's operations. While he was still there, though, the array of arcane skills and knowledge at his command led several colleagues to conclude that Mr. Szabo was most likely involved in the creation of Bitcoin, even if he didn't do it all himself.

I met Mr. Szabo, a large bearded man, in March 2014 at a Bitcoin event at the Lake Tahoe vacation home of Dan Morehead, a former Goldman Sachs executive who now runs a Bitcoin-focused investment firm, Pantera Capital. Mr. Szabo worked for Vaurum at the time. Mr. Morehead and other hedge fund executives in attendance dressed in expensive loafers and slim-cut jeans; Mr. Szabo, his bald pate encircled by a ring of salt-and-pepper hair, wore beat-up black sneakers and an untucked striped shirt.

While he kept to himself, I managed to corner him in the kitchen during the cocktail hour. He was notably reserved and deflected questions about where he lived and had worked, but he bristled when I cited what was being said about him on the Internet — including that he was a law professor at George Washington University — and the notion that he had created Bitcoin.

"Well, I will say this, in the hope of setting the record straight," he said acidly. "I'm not Satoshi, and I'm not a college professor. In fact, I never was a college professor."

The conversation grew less heated when I asked about the origin of the many complicated pieces of code and cryptography that went into the Bitcoin software, and about the small number of people who would have had the expertise to put them together. Mr. Szabo mentioned bit gold, saying it harnessed many of the same obscure concepts, like secure property titles and digital time stamps, that made Bitcoin possible.

"There are a whole bunch of parallels," he told me. "I mean, the reason people tag me is because you can go through secure property titles and bit gold — there are so many parallels between that and Bitcoin that you can't find anywhere else."

When I asked if he believed that Satoshi had been familiar with his work, Mr. Szabo said he understood why there was so much speculation about his own role: “All I’m saying is, there are all these parallels, and it looks funny to me, and looks funny to a lot of other people.”

Dinner began, interrupting the conversation, and I never got another chance to talk to Mr. Szabo.

When I emailed him on Wednesday, he repeated his denial: “As I’ve stated many times before, all this speculation is flattering, but wrong — I am not Satoshi.”

Many concepts central to Bitcoin were developed in an online community known as the Cypherpunks, a loosely organized group of digital privacy activists. As part of their mission, they set out to create digital money that would be as anonymous as physical cash. Mr. Szabo was a member, and in 1993, he wrote a message to fellow Cypherpunks describing the diverse motivations of attendees at a group meeting that had just taken place. Some people, he wrote, “are libertarians who want government out of our lives, others are liberals fighting the N.S.A., others find it great fun to ding people in power with cool hacks.”

Mr. Szabo had a libertarian mind-set. He was drawn to those ideas partly, he told me, because of his father, who fought the communists in Hungary in the 1950s before coming to the United States, where Mr. Szabo was born 51 years ago. Reared in Washington State, Mr. Szabo studied computer science at the University of Washington.

Several experiments in digital cash circulated on the Cypherpunk lists in the 1990s. Adam Back, a British researcher, created one called hashcash that later became a central component of Bitcoin. Another, called b money, was designed by an intensely private computer engineer named Wei Dai.

When these experiments failed to take off, many Cypherpunks lost interest. But not Mr. Szabo. He worked for six months as a consultant for a company called DigiCash, he has written on his blog. In 1998, he sent the outline for his own version of digital money, which he called bit gold, to a small group that was still pursuing the project, including Mr. Dai and Hal Finney, a programmer based in Santa Barbara, Calif., who tried to create a working version of bit gold.

The concept behind bit gold was very similar to Bitcoin: It included a digital token that was scarce, like gold, and could be sent electronically without needing to pass through a central authority like a bank.

This history points to the important role that Mr. Szabo and several others played in developing the building blocks that went into Bitcoin. When Satoshi Nakamoto's paper describing Bitcoin appeared in the fall of 2008, it cited Mr. Back's hashcash. The first people Satoshi emailed privately were Mr. Back and Mr. Dai, both men have said. And Mr. Finney, who recently died, helped Satoshi improve the Bitcoin software in the fall of 2008, before it was publicly released, according to emails shared with me by Mr. Finney and his family.

It is, though, Mr. Szabo's activity in 2008, as Bitcoin emerged into the world, that has generated much of the suspicion about his role in the project. That spring, before anyone had ever heard of Satoshi Nakamoto or Bitcoin, Mr. Szabo revived his bit gold idea on his personal blog, and in an online conversation about creating a live version of the virtual currency, he asked his readers: "Anybody want to help me code one up?"

After Bitcoin appeared, Mr. Szabo reposted the item on his blog in a way that changed the date at the top and made it appear as though it was written after Bitcoin's release, archived versions of the website show.

Mr. Szabo's writing about bit gold from that time contains many striking parallels with Satoshi's description of Bitcoin, including similar phrasings and even common writing mannerisms. In 2014, researchers at Aston University, in England, compared the writing of several people who have been suspected to be Satoshi and found that none matched up nearly as well as Mr. Szabo's. The similarity was "uncanny," said Jack Grieve, the lecturer who led the effort.

When I went back and read Mr. Szabo's online writings, it was obvious that in the year before Satoshi appeared on the scene and released Bitcoin, Mr. Szabo was again thinking seriously about digital money.

He wrote frequently, over several months, about the concepts involved in digital money, including those smart contracts, a concept so specialized that Mr. Szabo is often given credit for inventing the term. Smart contracts later showed up as an essential piece of the Bitcoin software.

Mr. Szabo's blog explained why he was examining these issues with such passion: The global financial crisis then underway suggested to him that the monetary system was broken and in need of replacement.

"For those who love our once and future freedoms, now is the time to strike," Mr. Szabo wrote in an item on his blog in late 2007 endorsing the libertarian Ron Paul's bid for the presidency, in part because of Mr. Paul's views on the financial system.

For many Bitcoin watchers, just as notable as what Mr. Szabo wrote in that period was his silence once Bitcoin appeared in October 2008. After all, the virtual currency was an experiment in everything he had been writing about for years. Unlike Mr. Dai, Mr. Finney and Mr. Back, Mr. Szabo has not released any correspondence from Satoshi from this period or acknowledged communicating with him.

Mr. Szabo first made brief mention of Bitcoin on his blog in mid-2009, and in 2011, when the currency was still struggling to gain traction, he wrote about it again at greater length, noting the similarity between bit gold and Bitcoin. He acknowledged that few people would have had the expertise and the instinct to create either of them:

"Myself, Wei Dai and Hal Finney were the only people I know of who liked the idea (or in Dai's case his related idea) enough to pursue it to any significant extent until Nakamoto (assuming Nakamoto is not really Finney or Dai)."

That item, in May 2011, was one of the last posts Mr. Szabo made before he went on a lengthy hiatus to work, he said later, on a new concept he called temporal programming.

May 2011 was also the last time Satoshi communicated privately with other Bitcoin contributors. In an email that month to Martti Malmi, one of the earliest participants, Satoshi wrote, "I've moved on to other things and probably won't be around in the future."

Whoever it is, the real Satoshi Nakamoto has many good reasons for wanting to stay anonymous. Perhaps the most obvious is potential danger. Sergio Demian Lerner, an Argentine researcher, has concluded that Satoshi Nakamoto most likely collected nearly a million Bitcoins during the system's first year. Given that each Bitcoin is now worth about $240, the stash could be worth more than $200 million. That could make Satoshi a target.

With his modest clothes and unassuming manner, Mr. Szabo could be the kind of person who could have a fortune and not spend any of it — or even throw away the keys to the bank. People who know him say he drives a car from the 1990s.

That modest outward appearance hasn't diminished the deference toward him among Bitcoin cognoscenti. Potential employees were drawn to Vaurum when they heard that Mr. Szabo worked there, people who interviewed at the company said. They wanted to work alongside the person they suspected could be Satoshi Nakamoto — or who at least participated in Bitcoin's invention.

Some material in this article appears in "Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money," to be published this month by Harper, a division of HarperCollins.

A version of this article appears in print on May 17, 2015, on page BU8 of the New York edition with the headline: Decoding the Enigma of Bitcoin's Birth . Order Reprints | Today's Paper | Subscribe

NEWS

World

U.S.

Politics