ESSAY

The Eureka Moment That Made Bitcoin Possible

A key insight for the technology came to a physicist almost three decades ago at a Friendly's restaurant in New Jersey

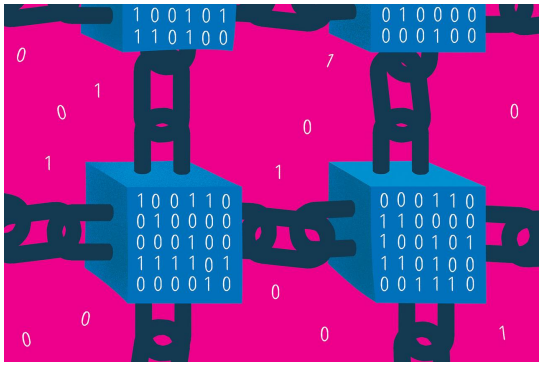

ILLUSTRATION: CHRISTOPHER SILAS NEAL

By Amy Whitaker
May 25, 2018 1:07 p.m. ET

Bitcoin and other digital currencies have been on a wild and much-publicized ride: Over the last year, the value of a single bitcoin has soared tenfold from $2,000 to $20,000 and then dropped by half again. A mystery surrounding the creator of the cryptocurrency, who has never been convincingly identified, has burnished its allure, and innovators and speculators now circle the globe attending high-priced industry conferences, many hoping to make their fortune.

But bitcoin didn't just materialize from thin air. The encryption technology that makes it possible —known as blockchain—was developed almost three decades ago, by scientists whose role in the story has not received much attention. Their aim was more idealistic than revolutionizing the world of money: They wanted to find a way to secure the past and safeguard our knowledge of it.

In 1990, the physicist Scott Stornetta had a eureka moment while getting ice cream with his family at a Friendly's restaurant in Morristown, N.J. He and his cryptographer colleague, Stuart Haber, had been thinking about the proliferation of digital files that accompanied the rise of personal computing and the ease with which files could be altered. They wondered how we might know for certain what was true about the past. What would prevent tampering with the historical record—and would it be possible to protect such information for future generations?

The sticking point was the need to trust a central authority. But at Friendly's, an answer came to Dr. Stornetta: He realized that instead of a central record-keeper, the system could have many dispersed but interconnected copies of a shared ledger. The truth could never be typed over if there were too many linked ledgers to alter.

'Their ledger, the first of its kind, is now the oldest blockchain in the world.'

Drs. Haber and Stornetta were working at the time at Bellcore, a research center descended from the legendary Bell Labs. The pair set out to build a cryptographically secure archive—a way to verify records without revealing their contents.

In 1991 they explained their find in a paper titled "How to Time-Stamp a Digital Document" in the Journal of Cryptography. The technology is called a blockchain because the distributed electronic ledger stores items of data in time-stamped digital groups called blocks. Each block includes an alphanumeric code called a "hash" summing up its data. The hash of each completed block also appears in the next one in the chain, which means that to alter one block you would have to alter all the ones connected to it. These cryptographic dominos function together to protect against tampering or fraud.

Drs. Stornetta and Haber went on to publish more papers on the subject and were eventually named as co-inventors on Bellcore's patent for the new technology. In 1994, they spun off a separate company called Surety, which offered to time-stamp any piece of information—a

chemistry lab result, a contract—into a block of transactions. As an additional security measure, Surety started publishing an alphanumeric code summarizing weekly blockchain additions in analog form in the classified section of the Sunday New York Times, under "Notices and Lost & Found." Their ledger, the first of its kind, is now the oldest blockchain in the world.

'Dr. Stornetta calls the connection to bitcoin "pretty cool." '

Dr. Stornetta stayed on at Surety for three years before moving on to teach high school math and to consult; Dr. Haber stayed for five years before he, too, moved on to other projects. Surety continues to represent clients, which have included pharmaceutical companies and intellectual property organizations. Privately held, the company quietly continues to publish the weekly hash.

The patent lapsed for non-payment of maintenance fees in 2004, four years before bitcoin emerged. Drs. Haber and Stornetta, who retained only small stakes in Surety, are philosophical about missing out on the potential financial windfall. As Dr. Haber says of their discovery, "It was an interesting little paper that turned into a company—which I didn't expect—and then I went back to being a research scientist." Dr. Stornetta calls the connection to bitcoin "pretty cool" and says that he would have contributed any royalties to nonprofit blockchain development.

But there is no mistaking their crucial contribution. When the founding document of bitcoin was published in 2008 under the name " Satoshi Nakamoto "—a pseudonym for one or more scientists —it had just eight citations of previous works. Three of them were papers co-authored by Drs. Haber and Stornetta.

MORE ESSAYS

- Science Prizes Add Intrigue to the Race for the Nobel June 1, 2018
- A Consumer Class Wields New Power in North Korea June 1, 2018
- Why We Find Self-Driving Cars So Scary May 31, 2018

My colleague David Yermack of NYU's Stern School of Business has recently drawn attention to the pivotal role played by the unassuming pair. Preparing to teach his own class on blockchain last spring, Dr. Yermack noticed Bellcore's Morristown address in the seminal 1991 paper. Dr. Yermack happened to live in Morristown, so he reached out to Dr. Stornetta and met him at what Dr. Stornetta still calls the "Blockchain Friendly's." The physicist is now a regular speaker on the subject at NYU.

The Nakamoto paper revolutionized the foundational work of Drs. Stornetta and Haber by adding the concept of "mining" cryptocurrencies. It created financial incentives for participation in retaining and verifying parts of the blockchain ledger. But it's worth recalling that what may become the currency of the future owes its origin to an effort to protect what we know of the past.

—Ms. Whitaker is an assistant professor at NYU's Steinhardt School of Culture, Education and Human Development and the author of "Art Thinking."