“The Man Who Really Built Bitcoin: Who cares about Satoshi Nakamoto? Someone else has made Bitcoin what it is and has the most power over its destiny” by Tom Simonite, August 15, 2014


**WHY IT MATTERS**

The 13 million bitcoins in existence are worth more than $7 billion.

In March, a bewildered retired man faced journalists yelling questions about virtual currency outside his suburban home in Temple City, California. Dorian Nakamoto, 64, had been identified by Newsweek as the person who masterminded Bitcoin—a story that, like previous attempts to unmask its pseudonymous inventor, Satoshi Nakamoto, was soon discredited. Meanwhile, the person arguably most responsible for enabling the currency to swell in value to $7.7 billion, and with the most influence on its future, was hiding in plain sight on the other side of the country, in Amherst, Massachusetts.

That person is Gavin Andresen, a mild-mannered 48-year-old picked by the real Satoshi Nakamoto, whoever he or she is, as his successor in late 2010. Andresen became “core maintainer”—chief developer—of the open source code that defines the rules of Bitcoin and provides the software needed to make use of it. The combination of Nakamoto’s blessing and Andresen’s years of diligent, full-time work on the Bitcoin code has given him significant clout in Bitcoin circles and stature beyond. The CIA and Washington regulators have looked to him to explain the currency. And it was Andresen who conceived of the nonprofit Bitcoin Foundation—established in 2012—which is the closest thing to a central authority in the world of Bitcoin.

Some Bitcoin enthusiasts offer bombastic predictions that Americans will shake off the shackles of the Federal Reserve and poor nations will rise to prosperity with the low-cost transactions made possible by the stateless virtual currency. Other Bitcoin boosters have the air of salesmen chasing a mark, reeling off reasons you should buy into the currency that make you feel you’re not getting the whole story. In contrast, Andresen seems to be in search of quiet personal satisfaction, cheerfully calling himself a “geek interested in nuts and bolts things.” He can make a pretty good pitch for Bitcoin, but he quickly slides into technical nuances that would be a turnoff for most. “We say this is going to be the year of the multisignature wallet,” he says when summing up what 2014 holds for Bitcoin.

Still, Andresen has had and maintains more influence than anyone else on the code that determines how Bitcoin operates—and ultimately whether it can survive. Although there is no central bank for the currency, its design needs significant changes if it is to become widely used. How Andresen wields his power over Bitcoin will shape not only its fate but also the prospects for other virtual currencies.

**Lucky Bet**

Bitcoin’s origins may be shrouded in mystery, but plenty is known about Andresen and his past. Formerly known as Gavin Bell, he has been a software engineer ever since he graduated in computer science from Princeton in 1988 and took a job with the Silicon Valley computing company Silicon Graphics. He worked there for seven years, and then at a series of startups building products from 3-D drawing software to online games for blind and sighted people to play together. Then he encountered Bitcoin in 2010.

Bitcoins were essentially worthless at the time and extremely finicky to get ahold of and use. But Andresen saw technical elegance in Nakamoto’s design, and a currency outside the control of any government appealed to what he calls his “mostly libertarian” politics. Rather than being created by a central bank, bitcoins are “mined” by people running
software that races to solve a mathematical puzzle and win a prize of newly minted bitcoins. The mining process is
designed to gradually pay out less and less over time, until 21 million bitcoins exist, and it also serves to verify
transactions made in the currency (see “What Bitcoin Is and Why It Matters”).

Eager to see people start using Bitcoin, Andresen launched a website in 2010 called the Bitcoin Faucet that handed out
five free bitcoins to every visitor. (A bitcoin was worth only cents at the time but each one trades for $600 today;
Andresen reduced the size of the handout as bitcoins rose in value, then shut the site down in 2012.) He also began
sending code tweaks and improvements to Nakamoto. Bitcoin’s founder liked his work, and soon made his protégé’s e-
mail address the only one on the project’s homepage. Andresen formally stepped forward in a December 2010 post on
the Bitcoin forum. “With Satoshi’s blessing, and with great reluctance, I’m going to start doing more active project
management for Bitcoin,” he wrote. He has worked full-time on it ever since. The Bitcoin Foundation paid him $209,648
in 2013—a salary he received in bitcoins.

His smooth ascent has led to frequent accusations that Andresen is Nakamoto and shed the pseudonym once the
currency gained traction. He always flatly denies it. “I am not Satoshi Nakamoto; I have never met him; I have had many
e-mail conversations with him,” he said after giving a talk in April. “Nobody knows who he is, I think.” If that was a lie,
Andresen is a remarkable con man. Throughout hundreds of forum posts, e-mail messages, and lines of code, his style
has been distinct from that of Nakamoto.

Andresen dedicated himself to Bitcoin out of what he calls “enlightened self-interest,” but without the promise of
anything in return. “This was a project that I wanted to see succeed,” he says. His gamble has paid off, giving him a
lucrative new career and strengthening his family’s safety net. It’s not known how many bitcoins Andresen holds, but he
has said that the return on the bitcoins he accumulated in the currency’s early days has been big enough that he could
comfortably retire. He proudly reports that his wife, a geology professor, doesn’t refer to Bitcoin as “pretend Internet
money” anymore. His kids became convinced last Christmas that their dad had been onto something after he used
Bitcoin to pay for a white-water rafting trip in New Zealand.

**Upwardly Mobile**

The rise of Bitcoin during Andresen’s involvement with the project is emphasized by the location of our meeting, in the
lobby of the Beverly Hilton hotel in Beverly Hills, California. A suited Andresen is sipping oatmeal stout after speaking at
the Milken Global Conference, an event that attracts leading figures in the financial industry, who pay $8,500 for a
ticket. Some financiers seem fascinated—if perplexed—by Bitcoin, and Andresen is the perfect person to represent it to
them. He makes it sound like a logical, overdue upgrade to the archaic currency in your pocket.

When Andresen took over from Satoshi Nakamoto in 2010 he laid out the way the project would operate, drawing on his
experience managing teams building software products and what he knew of major open source projects such as Linux.
A group of five core developers emerged, with Andresen as the most senior. Only they had the power to change the
code behind Bitcoin and merge in proposals from other volunteers. That gave them unique power over the currency’s
basic operation and economic parameters. While the price of Bitcoin soared over the years, Andresen and the other
core developers toiled to improve the software that made it all possible. They fixed security bugs that had permitted
digital heists, made the software less prone to crashes, and spruced up the interface to make it easier to use.

That was no small task because what Nakamoto had left was not the kind of software you would hope to build a product
on, let alone an economy, says Mike Hearn, an ex-Google software engineer who has contributed code to the project.
“He released Bitcoin to prove his ideas would work,” Hearn says. “It wasn’t written to be a long-term sustainable
product.” Most of the work to fix that was done by Andresen and Wladimir van der Laan, the Amsterdam-based coder
who took over from Andresen as core maintainer in April, says Hearn (van der Laan, who also draws a salary from the Bitcoin Foundation, didn’t respond to an interview request). As bugs were fixed, messy code tidied up, and new features added, most of what Nakamoto wrote disappeared. Under one-third of Nakamoto’s code still remains. “He was a brilliant coder, but it was quirky,” says Andresen.

Peter Todd, a developer who has contributed to the Bitcoin project, says Andresen seems in more of a hurry than others involved with the project to tweak Nakamoto’s design, apparently motivated by a desire to get the currency in the hands of millions or billions of users. “I’m much more conservative in making changes than he is, and I think that’s true for other developers as well,” Todd says. As an example, he points to recent changes that Andresen masterminded to make fees on Bitcoin transactions rise and fall as the volume of transactions changes. Todd believes the design of those changes would have benefited from more time to research possible downsides.

The number of people working on the code remains small, even since Andresen helped establish the Bitcoin Foundation to support the software with donations from individuals and companies. But the software behind Bitcoin has never been more critical. As the currency has grown to be worth nearly $8 billion, its stakeholders have widened from the early libertarian enthusiasts to include investors on Wall Street and in Silicon Valley (see “Bitcoin Hits the Big Time”). U.S. lawmakers and regulators have spoken positively about Bitcoin and made efforts to regulate it (see “Regulators See Value in Bitcoin and Other Digital Currencies”).

**Security Fixes**

The risk of security flaws is a constant worry for Andresen. He laughs when he recounts how in 2010 someone tipped off Nakamoto about a bug that made it possible to spend anyone else’s bitcoins. “Satoshi just changed the code and told everybody, ‘Run this new code, I’m not going to tell you why,’” Andresen says. But although most bugs that turn up in the software today are minor, similar problems could still lurk. “It’s why I say Bitcoin is an experiment and you shouldn’t invest your life’s savings,” he says. Unfortunately, the best defense against security flaws—having people review other people’s code—is hard to deploy for Bitcoin. Unpaid volunteers prefer to write their own code rather than laboriously read other people’s. Andresen sees the recent Heartbleed bug that broke the security of hundreds of thousands of websites as a cautionary tale. It was caused by a single, unnoticed mistake by a volunteer contributor to a piece of open source software. Even design flaws that fall short of enabling easy thefts could seriously wound Bitcoin. The currency’s value is built almost entirely on speculation, so any indication that the system is less than bulletproof can cause a major price shock. “It would probably survive but it would be bad,” says Andresen.

Meanwhile, Andresen must also wrestle with a serious problem with Nakamoto’s design. The Bitcoin network is incapable of processing more than seven transactions a second, a tiny volume for a technology with global ambitions. (Only about one Bitcoin transaction is made per second today, but most people who own Bitcoin do so to speculate on its price, not to pay for goods or services). Visa processes almost 480 transactions a second worldwide and can handle up to 47,000 a second at peak times.
“I’m worried about it and there’s a big debate in the Bitcoin community about how are we going to do this,” says Andresen. His favored solution is to increase the size of the “blocks” of transactions that get confirmed by the network of bitcoin miners every 10 minutes. If that doesn’t happen, then getting a transaction processed promptly will require paying a significant transaction fee to promote it ahead of others, he says. Not everyone agrees with Andresen’s proposed fix. Some opponents argue it would make Bitcoin more centralized. Larger blocks would make mining the currency so computationally intensive that only major corporations could do it, they say, giving them a kind of centralized power over the currency’s use. Andresen underlines his own position using the Bitcoin version of scripture. “If you read Satoshi’s writings, it’s obvious he intended it as a day-to-day transaction network for everybody,” he says.

One way or another, whatever Andresen decides on will probably get done. He promises that he and the core developers always listen to other opinions before they make any change to Bitcoin’s code. “It really is a consensus-driven process,” he says. And he points out that because that code is open source, any dissenters can always use it to create a competing version with their preferred design. But other developers and users of Bitcoin have little incentive to threaten the status quo and Andresen’s role in it. The value of any currency ultimately rests on a collective belief. In the case of Bitcoin, that faith rests not just in Nakamoto’s code, but in the people who tend to it.

Andresen has an alternative explanation for why there won’t be big changes in the way Bitcoin works. After the transaction issue is resolved, the work of looking after its code will increasingly be a job for caretakers, not master builders, he says. Andresen anticipates spending less and less time worrying about keeping the currency working, and more in his Amherst home office pondering theories about the economics of virtual currencies and reading the growing academic literature on Bitcoin. “I’m very optimistic going forward,” he says. “I hope in 10 years that Bitcoin is really boring.”