The Rise and Fall of Bitcoin

By Benjamin Wallace November 23, 2011 | 2:52 pm | Categories: Wired December 2011

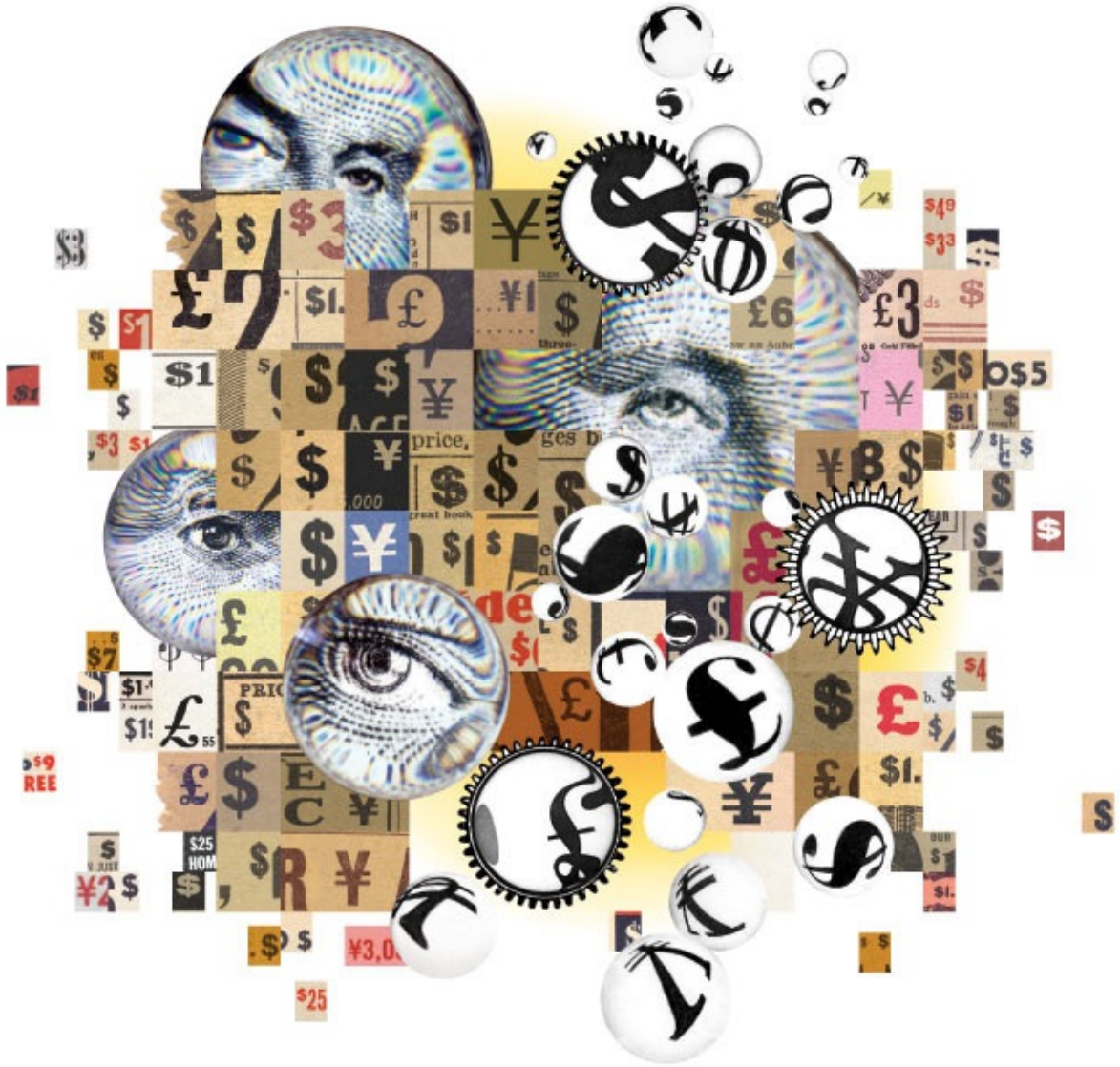


Illustration: Martin Venezky

In November 1, 2008, a man named Satoshi Nakamoto posted a research paper to an obscure cryptography listserv describing his design for a new digital currency that he called bitcoin. None of the list's veterans had heard of him, and what little information could be gleaned was murky and contradictory. In an online profile, he said he lived in Japan. His email address was from a free German service. Google searches for his name turned up no relevant information; it was clearly a pseudonym. But while Nakamoto himself may have been a puzzle, his creation cracked a problem that had stumped cryptographers for decades. The idea of digital money—

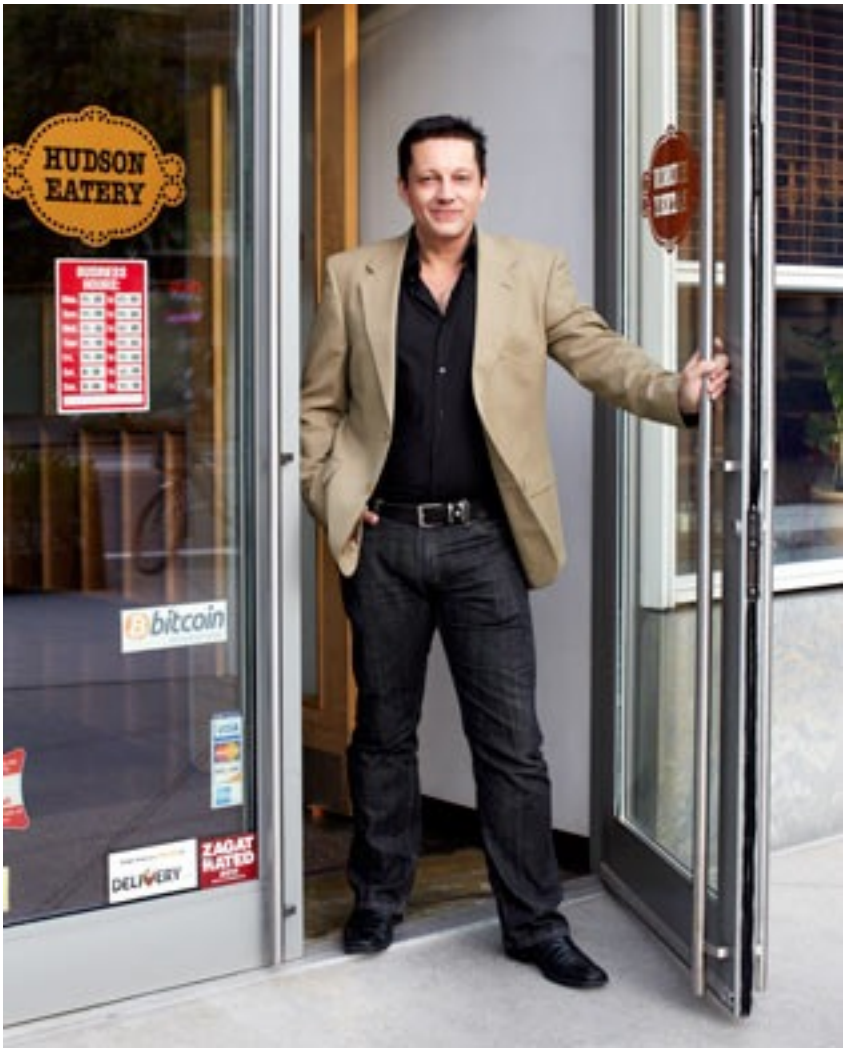
convenient and untraceable, liberated from the oversight of governments and banks—had been a hot topic since the birth of the Internet. Cypherpunks, the 1990s movement of libertarian cryptographers, dedicated themselves to the project. Yet every effort to create virtual cash had foundered. Ecash, an anonymous system launched in the early 1990s by cryptographer David Chaum, failed in part because it depended on the existing infrastructures of government and credit card companies. Other proposals followed—bit gold, RPOW, b-money—but none got off the ground.

One of the core challenges of designing a digital currency involves something called the double-spending problem. If a digital dollar is just information, free from the corporeal strictures of paper and metal, what's to prevent people from copying and pasting it as easily as a chunk of text, "spending" it as many times as they want? The conventional answer involved using a central clearinghouse to keep a real-time ledger of all transactions—ensuring that, if someone spends his last digital dollar, he can't then spend it again. The ledger prevents fraud, but it also requires a trusted third party to administer it.

Bitcoin did away with the third party by publicly distributing the ledger, what Nakamoto called the "block chain." Users willing to devote CPU power to running a special piece of software would be called miners and would form a network to maintain the block chain collectively. In the process, they would also generate new currency. Transactions would be broadcast to the network, and computers running the software would compete to solve irreversible cryptographic puzzles that contain data from several transactions. The first miner to solve each puzzle would be awarded 50 new bitcoins, and the associated block of transactions would be added to the chain. The difficulty of each puzzle would increase as the number of miners increased, which would keep production to one block of transactions roughly every 10 minutes. In addition, the size of each block bounty would halve every 210,000 blocks—first from 50 bitcoins to 25, then from 25 to 12.5, and so on. Around the year 2140, the currency would reach its preordained limit of 21 million bitcoins.

When Nakamoto's paper came out in 2008, trust in the ability of governments and banks to manage the economy and the money supply was at its nadir. The US government was throwing dollars at Wall Street

and the Detroit car companies. The Federal Reserve was introducing “quantitative easing,” essentially printing money in order to stimulate the economy. The price of gold was rising. Bitcoin required no faith in the politicians or financiers who had wrecked the economy—just in Nakamoto’s elegant algorithms. Not only did bitcoin’s public ledger seem to protect against fraud, but the predetermined release of the digital currency kept the bitcoin money supply growing at a predictable rate, immune to printing-press-happy central bankers and Weimar Republic-style hyperinflation.



Bitcoin's chief proselytizer, Bruce Wagner, at one of the few New York City restaurants that accept the currency.
Photo: Michael Schmelling

Nakamoto himself mined the first 50 bitcoins—which came to be called the genesis block—on January 3, 2009. For a year or so, his creation remained

the province of a tiny group of early adopters. But slowly, word of bitcoin spread beyond the insular world of cryptography. It has won accolades from some of digital currency's greatest minds. Wei Dai, inventor of b-money, calls it "very significant"; Nick Szabo, who created bit gold, hails bitcoin as "a great contribution to the world"; and Hal Finney, the eminent cryptographer behind RPOW, says it's "potentially world-changing." The Electronic Frontier Foundation, an advocate for digital privacy, eventually started accepting donations in the alternative currency.

The small band of early bitcoiners all shared the communitarian spirit of an open source software project. Gavin Andresen, a coder in New England, bought 10,000 bitcoins for $50 and created a site called the Bitcoin Faucet, where he gave them away for the hell of it. Laszlo Hanyecz, a Florida programmer, conducted what bitcoiners think of as the first real-world bitcoin transaction, paying 10,000 bitcoins to get two pizzas delivered from Papa John's. (He sent the bitcoins to a volunteer in England, who then called in a credit card order transatlantically.) A farmer in Massachusetts named David Forster began accepting bitcoins as payment for alpaca socks.

When they weren't busy mining, the faithful tried to solve the mystery of the man they called simply Satoshi. On a bitcoin IRC channel, someone noted portentously that in Japanese *Satoshi* means "wise." Someone else wondered whether the name might be a sly portmanteau of four tech companies: SAmsung, TOSHIba, NAKAmichi, and MOTOrola. It seemed doubtful that Nakamoto was even Japanese. His English had the flawless, idiomatic ring of a native speaker.

Perhaps, it was suggested, Nakamoto wasn't one man but a mysterious group with an inscrutable purpose—a team at Google, maybe, or the National Security Agency. "I exchanged some emails with whoever Satoshi supposedly is," says Hanyecz, who was on bitcoin's core developer team for a time. "I always got the impression it almost wasn't a real person. I'd get replies maybe every two weeks, as if someone would check it once in a while. Bitcoin seems awfully well designed for one person to crank out."

Nakamoto revealed little about himself, limiting his online utterances to technical discussion of his source code. On December 5, 2010, after bitcoiners started to call for Wikileaks to accept bitcoin donations, the

normally terse and all-business Nakamoto weighed in with uncharacteristic vehemence. “No, don’t ‘bring it on,’” he wrote in a post to the bitcoin forum. “The project needs to grow gradually so the software can be strengthened along the way. I make this appeal to Wikileaks not to try to use bitcoin. Bitcoin is a small beta community in its infancy. You would not stand to get more than pocket change, and the heat you would bring would likely destroy us at this stage.”

Then, as unexpectedly as he had appeared, Nakamoto vanished. At 6:22 pm GMT on December 12, seven days after his Wikileaks plea, Nakamoto posted his final message to the bitcoin forum, concerning some minutiae in the latest version of the software. His email responses became more erratic, then stopped altogether. Andresen, who had taken over the role of lead developer, was now apparently one of just a few people with whom he was still communicating. On April 26, Andresen told fellow coders: “Satoshi did suggest this morning that I (we) should try to de-emphasize the whole ‘mysterious founder’ thing when talking publicly about bitcoin.” Then Nakamoto stopped replying even to Andresen’s emails. Bitcoiners wondered plaintively why he had left them. But by then his creation had taken on a life of its own.

Bitcoin 101

How They’re Made

Bitcoin’s economy consists of a network of its users’ computers. At preset intervals, an algorithm releases new bitcoins into the network: 50 every 10 minutes, with the pace halving in increments until around 2140. The automated pace is meant to ensure regular growth of the monetary supply without interference by third parties, like a central bank, which can lead to hyperinflation.

How They're Mined

To prevent fraud, the bitcoin software maintains a pseudonymous public ledger of every transaction. Some bitcoiners' computers validate transactions by cracking cryptographic puzzles, and the first to solve each puzzle receives 50 new bitcoins. Bitcoins can be stored in a variety of places—from a "wallet" on a desktop computer to a centralized service in the cloud.

How They're Spent

Once users download the bitcoin app to their machine, spending the currency is as easy as sending an email. The range of merchants that accept it is small but growing; look for the telltale ₿symbol at the cash register. And entrepreneurial bitcoiners are working to make it much easier to use the currency, building everything from point-of-service machines to PayPal alternatives.

Illustrations: Martin Venezky

"Bitcoin enthusiasts are almost evangelists," Bruce Wagner says. "They see the beauty of the technology. It's a huge movement. It's almost like a religion. On the forum, you'll see the spirit. It's not just me, me, me. It's what's for the betterment of bitcoin."

It's a July morning. Wagner, whose boyish energy and Pantone-black hair belie his 50 years, is sitting in his office at OnlyOneTV, an Internet television startup in Manhattan. Over just a few months, he has become bitcoin's chief proselytizer. He hosts *The Bitcoin Show*, a program on OnlyOneTV in which he plugs the nascent currency and interviews notables from the bitcoin world. He also runs a bitcoin meetup group and is gearing up to host bitcoin's first "world conference" in August. "I got obsessed and didn't eat or sleep for five days," he says, recalling the moment he discovered bitcoin. "It was bitcoin, bitcoin, bitcoin, like I was on crystal meth!"

Wagner is not given to understatement. While bitcoin is "the most exciting technology since the Internet," he says, eBay is "a giant bloodsucking

corporation” and free speech “a popular myth.” He is similarly excitable when predicting the future of bitcoin. “I knew it wasn’t a stock and wouldn’t go up and down,” he explains. “This was something that was going to go up, up, up.”

For a while, he was right. Through 2009 and early 2010, bitcoins had no value at all, and for the first six months after they started trading in April 2010, the value of one bitcoin stayed below 14 cents. Then, as the currency gained viral traction in summer 2010, rising demand for a limited supply caused the price on online exchanges to start moving. By early November, it surged to 36 cents before settling down to around 29 cents. In February 2011, it rose again and was mentioned on Slashdot for achieving “dollar parity”; it hit $1.06 before settling in at roughly 87 cents.

In the spring, catalyzed in part by a much-linked *Forbes* story on the new “crypto currency,” the price exploded. From early April to the end of May, the going rate for a bitcoin rose from 86 cents to $8.89. Then, after Gawker published a story on June 1 about the currency’s popularity among online drug dealers, it more than tripled in a week, soaring to about $27. The market value of all bitcoins in circulation was approaching $130 million. A Tennessean dubbed KnightMB, who held 371,000 bitcoins, became worth more than $10 million, the richest man in the bitcoin realm. The value of those 10,000 bitcoins Hanyecz used to buy pizza had risen to $272,329. “I don’t feel bad about it,” he says. “The pizza was really good.”

Perhaps bitcoin’s creator wasn’t one man but a mysterious group—a team at Google, maybe, or the NSA.

Bitcoin was drawing the kind of attention normally reserved for overhyped Silicon Valley IPOs and Apple product launches. On his Internet talk show, journo-entrepreneur Jason Calacanis called it “a fundamental shift” and “one of the most interesting things I’ve seen in 20 years in the technology business.” Prominent venture capitalist Fred Wilson heralded “societal upheaval” as the Next Big Thing on the Internet, and the four examples he gave were Wikileaks, PlayStation hacking, the Arab Spring, and bitcoin. Andresen, the coder, accepted an invitation from the CIA to come to Langley, Virginia, to speak about the currency. Rick Falkvinge, founder of the Swedish Pirate Party (whose central policy plank includes the abolition

of the patent system), announced that he was putting his life savings into bitcoins.

The future of bitcoin seemed to shimmer with possibility. Mark Suppes, an inventor building a fusion reactor in a Brooklyn loft from eBay-sourced parts, got an old ATM and began retrofitting it to dispense cash for bitcoins. On the so-called secret Internet (the invisible grid of sites reachable by computers using Tor anonymizing software), the black-and-gray-market site Silk Road anointed the bitcoin the coin of the realm; you could use bitcoins to buy everything from Purple Haze pot to Fentanyl lollipops to a kit for converting a rifle into a machine gun. A young bitcoiner, The Real Plato, brought *On the Road* into the new millennium by video-blogging a cross-country car trip during which he spent only bitcoins. Numismatic enthusiasts among the currency's faithful began dreaming of collectible bitcoins, wondering what price such rarities as the genesis block might fetch.

As the price rose and mining became more popular, the increased competition meant decreasing profits. An arms race commenced. Miners looking for horsepower supplemented their computers with more powerful graphics cards, until they became nearly impossible to find. Where the first miners had used their existing machines, the new wave, looking to mine bitcoins 24 hours a day, bought racks of cheap computers with high-speed GPUs cooled by noisy fans. The boom gave rise to mining-rig porn, as miners posted photos of their setups. As in any gold rush, people recounted tales of uncertain veracity. An Alaskan named Darrin reported that a bear had broken into his garage but thankfully ignored his rig. Another miner's electric bill ran so high, it was said, that police raided his house, suspecting that he was growing pot.

Amid the euphoria, there were troubling signs. Bitcoin had begun in the public-interested spirit of open source peer-to-peer software and libertarian political philosophy, with references to the Austrian school of economics. But real money was at stake now, and the dramatic price rise had attracted a different element, people who saw the bitcoin as a commodity in which to speculate. At the same time, media attention was bringing exactly the kind of heat that Nakamoto had feared. US senator Charles Schumer held a press conference, appealing to the DEA and Justice Department to shut down Silk Road, which he called "the most brazen attempt to peddle drugs

online that we have ever seen" and describing bitcoin as "an online form of money-laundering."

Meanwhile, a cult of Satoshi was developing. Someone started selling I AM SATOSHI NAKAMOTO T-shirts. Disciples lobbied to name the smallest fractional denomination of a bitcoin a "satoshi." There was Satoshi-themed fan fiction and manga art. And bitcoiners continued to ponder his mystery. Some speculated that he had died. A few postulated that he was actually Wikileaks founder Julian Assange. Many more were convinced that he was Gavin Andresen. Still others believed that he must be one of the older crypto-currency advocates—Finney or Szabo or Dai. Szabo himself suggested it could be Finney or Dai. Stefan Thomas, a Swiss coder and active community member, graphed the time stamps for each of Nakamoto's 500-plus bitcoin forum posts; the resulting chart showed a steep decline to almost no posts between the hours of 5 am and 11 am Greenwich Mean Time. Because this pattern held true even on Saturdays and Sundays, it suggested that the lull was occurring when Nakamoto was asleep, rather than at work. (The hours of 5 am to 11 am GMT are midnight to 6 am Eastern Standard Time.) Other clues suggested that Nakamoto was British: A newspaper headline he had encoded in the genesis block came from the UK-published *Times of London*, and both his forum posts and his comments in the bitcoin source code used such Brit spellings as *optimise* and *colour*.

Even the purest technology has to live in an impure world. Both the code and the idea of bitcoin may have been impregnable, but bitcoins themselves—unique strings of numbers that constitute units of the currency—are discrete pieces of information that have to be stored somewhere. By default, bitcoin kept users' currency in a digital "wallet" on their desktop, and when bitcoins were worth very little, easy to mine, and possessed only by techies, that was sufficient. But once they started to become valuable, a PC felt inadequate. Some users protected their bitcoins by creating multiple backups, encrypting and storing them on thumb drives, on forensically scrubbed virgin computers without Internet connections, in the cloud, and on printouts stored in safe-deposit boxes. But even some sophisticated early adopters had trouble keeping their bitcoins safe. Stefan Thomas had three copies of his wallet yet inadvertently managed to erase two of them and lose his password for the third. In a stroke, he lost about 7,000 bitcoins, at the time worth about $140,000. "I spent a week trying to recover it," he says. "It was pretty painful." Most people who have cash to protect

put it in a bank, an institution about which the more zealous bitcoiners were deeply leery. Instead, for this new currency, a primitive and unregulated financial-services industry began to develop. Fly-by-night online “wallet services” promised to safeguard clients’ digital assets. Exchanges allowed anyone to trade bitcoins for dollars or other currencies. Bitcoin itself might have been decentralized, but users were now blindly entrusting increasing amounts of currency to third parties that even the most radical libertarian would be hard-pressed to claim were more secure than federally insured institutions. Most were Internet storefronts, run by who knows who from who knows where.

Sure enough, as the price headed upward, disturbing events began to bedevil the bitcoiners. In mid-June, someone calling himself Allinvain reported that 25,000 bitcoins worth more than $500,000 had been stolen from his computer. (To this day, nobody knows whether this claim is true.) About a week later, a hacker pulled off an ingenious attack on a Tokyo-based exchange site called Mt. Gox, which handled 90 percent of all bitcoin exchange transactions. Mt. Gox restricted account withdrawals to $1,000 worth of bitcoins per day (at the time of the attack, roughly 35 bitcoins). After he broke into Mt. Gox’s system, the hacker simulated a massive sell-off, driving the exchange rate to zero and letting him withdraw potentially tens of thousands of other people’s bitcoins.

As it happened, market forces conspired to thwart the scheme. The price plummeted, but as speculators flocked to take advantage of the fire sale, they quickly drove it back up, limiting the thief’s haul to only around 2,000 bitcoins. The exchange ceased operations for a week and rolled back the postcrash transactions, but the damage had been done; the bitcoin never got back above $17. Within a month, Mt. Gox had lost 10 percent of its market share to a Chile-based upstart named TradeHill. Most significantly, the incident had shaken the confidence of the community and inspired loads of bad press.

In the public’s imagination, overnight the bitcoin went from being the currency of tomorrow to a dystopian joke. The Electronic Frontier Foundation quietly stopped accepting bitcoin donations. Two Irish scholars specializing in network analysis demonstrated that bitcoin wasn’t nearly as anonymous as many had assumed: They were able to identify the handles of a number of people who had donated bitcoins to Wikileaks. (The

organization announced in June 2011 that it was accepting such donations.) Nontechnical newcomers to the currency, expecting it to be easy to use, were disappointed to find that an extraordinary amount of effort was required to obtain, hold, and spend bitcoins. For a time, one of the easier ways to buy them was to first use Paypal to buy Linden dollars, the virtual currency in Second Life, then trade them within that make-believe universe for bitcoins. As the tone of media coverage shifted from gee-whiz to skeptical, attention that had once been thrilling became a source of resentment.

Illustration: Martin Venezky

More disasters followed. Poland-based Bitomat, the third-largest exchange, revealed that it had—oops—accidentally overwritten its entire wallet. Security researchers detected a proliferation of viruses aimed at bitcoin users: Some were designed to steal wallets full of existing bitcoins; others

commandeered processing power to mine fresh coins. By summer, the oldest wallet service, MyBitcoin, stopped responding to emails. It had always been fishy—registered in the West Indies and run by someone named Tom Williams, who never posted in the forums. But after a month of unbroken silence, Wagner, the New York City bitcoin evangelist, finally stated what many had already been thinking: Whoever was running MyBitcoin had apparently gone AWOL with everyone's money. Wagner himself revealed that he had been keeping all 25,000 or so of his bitcoins on MyBitcoin and had recommended to friends and relatives that they use it, too. He also aided a vigilante effort that publicly named several suspects. MyBitcoin's supposed owner resurfaced, claiming his site had been hacked. Then Wagner became the target of a countercampaign that publicized a successful lawsuit against him for mortgage fraud, costing him much of his reputation within the community. "People have the mistaken impression that virtual currency means you can trust a random person over the Internet," says Jeff Garzik, a member of bitcoin's core developer group.

And nobody had been as trusted as Nakamoto himself, who remained mysteriously silent as the world he created threatened to implode. Some bitcoiners began to suspect that he was working for the CIA or Federal Reserve. Others worried that bitcoin had been a Ponzi scheme, with Nakamoto its Bernie Madoff—mining bitcoins when they were worthless, then waiting for their value to rise. The most dedicated bitcoin loyalists maintained their faith, not just in Nakamoto, but in the system he had built. And yet, unmistakably, beneath the paranoia and infighting lurked something more vulnerable, an almost theodical disappointment. What bitcoiners really seemed to be asking was, why had Nakamoto created this world only to abandon it?

If Nakamoto has forsaken his adherents, though, they are not prepared to let his creation die. Even as the currency's value has continued to drop, they are still investing in the fragile economy. Wagner has advocated for it to be used by people involved in the Occupy Wall Street movement. While the gold-rush phase of mining has ended, with some miners dumping their souped-up mining rigs—"People are getting sick of the high electric bills, the heat, and the loud fans," Garzik says—the more serious members of the community have turned to infrastructure. Mt. Gox is developing point-of-sale hardware. Other entrepreneurs are working on PayPal-like online merchant services. Two guys in Colorado have launched BitcoinDeals, an etailer offering "over 1,000,000 items." The underworld's use of the bitcoin

has matured, too: Silk Road is now just one of many Tor-enabled back alleys, including sites like Black Market Reloaded, where self-proclaimed hit men peddle contract killings and assassinations.

“You could say it’s following Gartner’s Hype Cycle,” London-based core developer Amir Taaki says, referring to a theoretical technology-adoption-and-maturation curve that begins with a “technology trigger,” ascends to a “peak of inflated expectations,” collapses into a “trough of disillusionment,” and then climbs a “slope of enlightenment” until reaching a “plateau of productivity.” By this theory, bitcoin is clambering out of the trough, as people learn to value the infallible code and discard the human drama and wild fluctuations that surround it.

But that distinction is ultimately irrelevant. The underlying vulnerabilities that led to bitcoin’s troubles—its dependence on unregulated, centralized exchanges and online wallets—persist. Indeed, the bulk of mining is now concentrated in a handful of huge mining pools, which theoretically could hijack the entire network if they worked in concert.

Beyond the most hardcore users, skepticism has only increased. Nobel Prize-winning economist Paul Krugman wrote that the currency’s tendency to fluctuate has encouraged hoarding. Stefan Brands, a former ecash consultant and digital currency pioneer, calls bitcoin “clever” and is loath to bash it but believes it’s fundamentally structured like “a pyramid scheme” that rewards early adopters. “I think the big problems are ultimately the trust issues,” he says. “There’s nothing there to back it up. I know the counterargument, that that’s true of fiat money, too, but that’s completely wrong. There’s a whole trust fabric that’s been established through legal mechanisms.”

It would be interesting to know what Nakamoto thinks of all this, but he’s not talking. He didn’t respond to emails, and the people who might know who he is say they don’t. Andresen flatly denies he is Nakamoto. “I don’t know his real name,” he says. “I’m hoping one day he decides not to be anonymous anymore, but I expect not.” Szabo also denies that he is Nakamoto, and so does Dai. Finney, who has blogged eloquently about being diagnosed with amyotrophic lateral sclerosis, sent his denial in an email: “Under my current circumstances, facing limited life expectancy, I would have little to lose by shedding anonymity. But it was not I.” Both *The*

New Yorker and *Fast Company* have launched investigations but ended up with little more than speculation.

The signal in the noise, the figure that emerges from the carpet of clues, suggests an academic with somewhat outdated programming training. (Nakamoto's style of notation "was popular in the late '80s and early '90s," Taaki notes. "Maybe he's around 50, plus or minus 10 years.") Some conjecturers are confident in their precision. "He has at best a master's," says a digital-currency expert. "It seems quite obvious it's one of the developers. Maybe Gavin, just looking at his background."

"I suspect Satoshi is a small team at a financial institution," whitehat hacker Dan Kaminsky says. "I just get that feeling. He's a quant who may have worked with some of his friends."

But Garzik, the developer, says that the most dedicated bitcoiners have stopped trying to hunt down Nakamoto. "We really don't care," he says. It's not the individuals behind the code who matter, but the code itself. And while people have stolen and cheated and abandoned the bitcoiners, the code has remained true.

Benjamin Wallace (benwallace@me.com) *wrote about scareware in issue 19.10.*