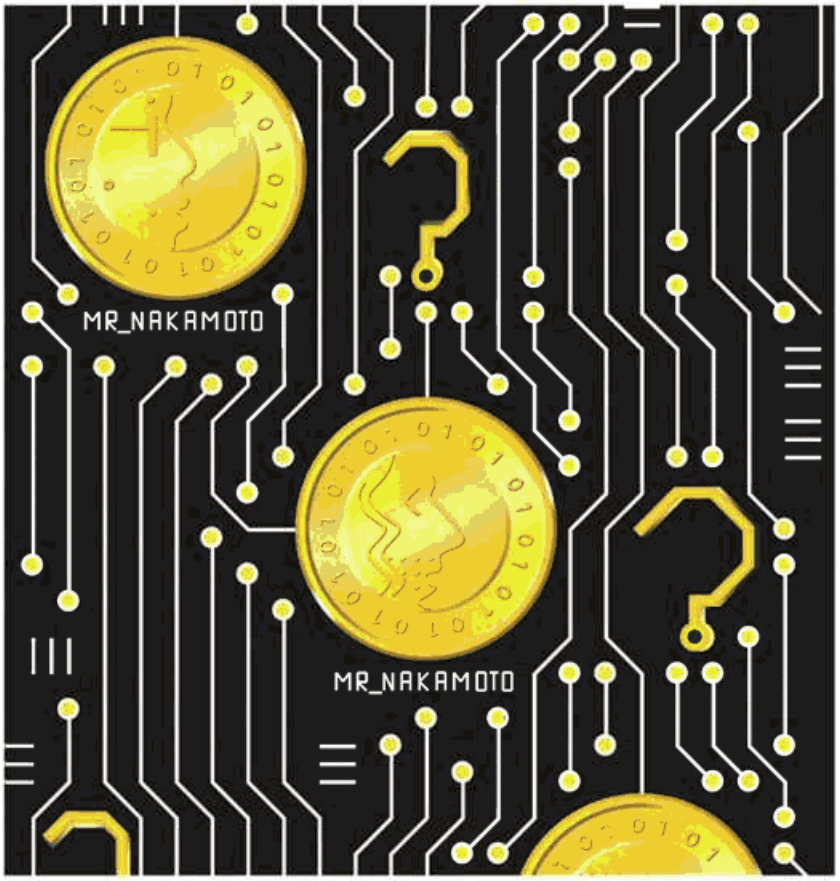
DEPT. OF TECHNOLOGY

THE CRYPTO-CURRENCY

Bitcoin and its mysterious inventor.

BY JOSHUA DAVIS



It's not clear if bitcoin is legal, but there is no company in control and no one to arrest.

There are lots of ways to make money: You can earn it, find it, counterfeit it, steal it. Or, if you're Satoshi Nakamoto, a preternaturally talented computer coder, you can invent it. That's what he did on the evening of January 3, 2009, when he pressed a button on his keyboard and created a new currency called bitcoin. It was all bit and no coin. There was no paper, copper, or silver—just thirty-one thousand lines of code and an announcement on the Internet.

Nakamoto, who claimed to be a thirty-six-year-old Japanese man, said he had spent more than a year writing the software, driven in part by anger over the recent financial crisis. He wanted to create a currency that was impervious to unpredictable monetary policies as well as to the predations of bankers and politicians. Nakamoto's invention was controlled entirely by software, which would release a total of twenty-one million bitcoins, almost all of them over the next twenty years. Every ten minutes or so, coins would be distributed through a process that resembled a lottery. Miners—people seeking the coins—would play the lottery again and again; the fastest computer would win the most money.

Interest in Nakamoto's invention built steadily. More and more people dedicated their computers to the lottery, and forty-four exchanges popped up, allowing anyone with bitcoins to trade them for official currencies like dollars or euros. Creative computer engineers could mine for bitcoins; anyone could buy them. At first, a single bitcoin was valued at less than a penny. But merchants gradually began to accept bitcoins, and at the end of 2010 their value began to appreciate rapidly. By June of 2011, a bitcoin was worth more than twenty-nine dollars. Market gyrations followed, and by September the exchange rate had fallen to five dollars. Still, with more than seven million bitcoins in circulation, Nakamoto had created thirty-five million dollars of value.

And yet Nakamoto himself was a cipher. Before the début of bitcoin, there was no record of any coder with that name. He used an e-mail address and a Web site that were untraceable. In 2009 and 2010, he wrote hundreds of posts in flawless English, and though he invited other software developers to help him improve the code, and corresponded with them, he never revealed a personal detail. Then, in April, 2011, he sent a note to a developer saying that he had "moved on to other things." He has not been heard from since.

When Nakamoto disappeared, hundreds of people posted theories about his identity and whereabouts. Some wanted to know if he could be trusted. Might he have created the currency in order to hoard coins and cash out? "We can effectively think of 'Satoshi Nakamoto' as being on top of a Ponzi scheme," George Ou, a blogger and technology commentator, wrote.

It appeared, though, that Nakamoto was motivated by politics, not crime. He had introduced the currency just a few months after the collapse of the global banking sector, and published a five-hundred-word essay about traditional fiat, or government-backed, currencies. "The root problem with conventional currency is all the trust that's required to make it work," he wrote. "The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve."

Banks, however, do much more than lend money to overzealous homebuyers. They also, for example, monitor payments

GRAFILU

so that no one can spend the same dollar twice. Cash is immune to this problem: you can't give two people the same bill. But with digital currency there is the danger that someone can spend the same money any number of times.

Nakamoto solved this problem using innovative cryptography. The bitcoin software encrypts each transaction—the sender and the receiver are identified only by a string of numbers—but a public record of every coin's movement is published across the entire network. Buyers and sellers remain anonymous, but everyone can see that a coin has moved from A to B, and Nakamoto's code can prevent A from spending the coin a second time.

Nakamoto's software would allow people to send money directly to each other, without an intermediary, and no outside party could create more bitcoins. Central banks and governments played no role. If Nakamoto ran the world, he would have just fired Ben Bernanke, closed the European Central Bank, and shut down Western Union. "Everything is based on crypto proof instead of trust," Nakamoto wrote in his 2009 essay.

Bitcoin, however, was doomed if the code was unreliable. Earlier this year, Dan Kaminsky, a leading Internet-security researcher, investigated the currency and was sure he would find major weaknesses. Kaminsky is famous among hackers for discovering, in 2008, a fundamental flaw in the Internet which would have allowed a skilled coder to take over any Web site or even to shut down the Internet. Kaminsky alerted the Department of Homeland Security and executives at Microsoft and Cisco to the problem and worked with them to patch it. He is one of the most adept practitioners of "penetration testing," the art of compromising the security of computer systems at the behest of owners who want to know their vulnerabilities. Bitcoin, he felt, was an easy target.

"When I first looked at the code, I was sure I was going to be able to break it," Kaminsky said, noting that the programming style was dense and inscrutable. "The way the whole thing was formatted was insane. Only the most paranoid, painstaking coder in the world could avoid making mistakes."

Kaminsky lives in Seattle, but, while visiting family in San Francisco in July, he retreated to the basement of his mother's house to work on his bitcoin attacks. In a windowless room jammed with computers, Kaminsky paced around talking to himself, trying to build a mental picture of the bitcoin network. He quickly identified nine ways to compromise the system and scoured Nakamoto's code for an insertion point for his first attack. But when he found the right spot, there was a message waiting for him. "Attack Removed," it said. The same thing happened over and over, infuriating Kaminsky. "I came up with beautiful bugs," he said. "But every time I went after the code there was a line that addressed the problem."

He was like a burglar who was certain that he could break into a bank by digging a tunnel, drilling through a wall, or climbing down a vent, and on each attempt he discovered a freshly poured cement barrier with a sign telling him to go home. "I've never seen anything like it," Kaminsky said, still in awe.

Kaminsky ticked off the skills Nakamoto would need to pull it off. "He's a world-class programmer, with a deep understanding of the C++ programming language," he said. "He understands economics, cryptography, and peer-to-peer networking."

"Either there's a team of people who worked on this," Kaminsky said, "or this guy is a genius."

Kaminsky wasn't alone in this assessment. Soon after creating the currency, Nakamoto posted a nine-page technical paper describing how bitcoin would function. That document included three references to the work of Stuart Haber, a researcher at H.P. Labs, in Princeton. Haber is a director of the International Association for Cryptologic Research and knew all about bitcoin. "Whoever did this had a deep understanding of cryptography," Haber said when I called. "They've read the academic papers, they have a keen intelligence, and they're combining the concepts in a genuinely new way."

Haber noted that the community of cryptographers is very small: about three hundred people a year attend the most important conference, the annual gathering in Santa Barbara. In all likelihood, Nakamoto belonged to this

insular world. If I wanted to find him, the Crypto 2011 conference would be the place to start.

"Here we go, team!" a cheerleader shouted before two burly guys heaved her into the air.

It was a foggy Monday morning in mid-August, and dozens of college cheerleaders had gathered on the athletic fields of the University of California at Santa Barbara for a three-day training camp. Their hollering could be heard on the steps of a nearby lecture hall, where a group of bleary-eyed cryptographers, dressed in shorts and rumpled T-shirts, muttered about symmetric-key ciphers over steaming cups of coffee.

This was Crypto 2011, and the list of attendees included representatives from the National Security Agency, the U.S. military, and an assortment of foreign governments. Cryptographers are little known outside this hermetic community, but our digital safety depends on them. They write the algorithms that conceal bank files, military plans, and your e-mail.

I approached Phillip Rogaway, the conference's program chair. He is a friendly, diminutive man who is a professor of cryptography at the University of California at Davis and who has also taught at Chiang Mai University, in Thailand. He bowed when he shook my hand, and I explained that I was trying to learn more about what it would take to create bitcoin. "The people who know how to do that are here," Rogaway said. "It's likely I either know the person or know their work." He offered to introduce me to some of the attendees.

Nakamoto had good reason to hide: people who experiment with currency tend to end up in trouble. In 1998, a Hawaiian resident named Bernard von NotHaus began fabricating silver and gold coins that he dubbed Liberty Dollars. Nine years later, the U.S. government charged NotHaus with "conspiracy against the United States." He was found guilty and is awaiting sentencing. "It is a violation of federal law for individuals…to create private coin or currency systems to compete with the official coinage and currency of the United States," the F.B.I. announced at the end of the trial.

Online currencies aren't exempt. In 2007, the federal government filed charges against e-Gold, a company that sold a digital currency redeemable for gold. The government argued that the project enabled money laundering and child pornography, since users did not have to provide thorough identification. The company's owners were found guilty of operating an unlicensed money-transmitting business and the C.E.O. was sentenced to months of house arrest. The company was effectively shut down.

Nakamoto seemed to be doing the same things as these other currency developers who ran afoul of authorities. He was competing with the dollar and he insured the anonymity of users, which made bitcoin attractive for criminals. This winter, a Web site was launched called Silk Road, which allowed users to buy and sell heroin, LSD, and marijuana as long as they paid in bitcoin.

Still, Lewis Solomon, a professor emeritus at George Washington University Law School, who has written about alternative currencies, argues that creating bitcoin might be legal. "Bitcoin is in a gray area, in part because we don't know whether it should be treated as a currency, a commodity like gold, or possibly even a security," he says.

Gray areas, however, are dangerous, which may be why Nakamoto constructed bitcoin in secret. It may also explain why he built the code with the same peer-to-peer technology that facilitates the exchange of pirated movies and music: users connect with each other instead of with a central server. There is no company in control, no office to raid, and nobody to arrest.

Today, bitcoins can be used online to purchase beef jerky and socks made from alpaca wool. Some computer retailers accept them, and you can use them to buy falafel from a restaurant in Hell's Kitchen. In late August, I learned that bitcoins could also get me a room at a Howard Johnson hotel in Fullerton, California, ten minutes from Disneyland. I booked a reservation for my four-year-old daughter and me and received an e-mail from the hotel requesting a payment of 10.305 bitcoins.

By this time, it would have been pointless for me to play the bitcoin lottery, which is set up so that the difficulty of winning increases the more people play it. When bitcoin launched, my laptop would have had a reasonable chance of winning from time to time. Now, however, the computing power dedicated to playing the bitcoin lottery exceeds that of the world's most powerful supercomputer. So I set up an account

with Mt. Gox, the leading bitcoin exchange, and transferred a hundred and twenty dollars. A few days later, I bought 10.305 bitcoins with the press of a button and just as easily sent them to the Howard Johnson.

It was a simple transaction that masked a complex calculus. In 1971, Richard Nixon announced that U.S. dollars could no longer be redeemed for gold. Ever since, the value of the dollar has been based on our faith in it. We trust that dollars will be valuable tomorrow, so we accept payment in dollars today. Bitcoin is similar: you have to trust that the system won't get hacked, and that Nakamoto won't suddenly emerge to somehow plunder it all. Once you believe in it, the actual cost of a bitcoin—five dollars or thirty?—depends on factors such as how many merchants are using it, how many might use it in the future, and whether or not governments ban it.

My daughter and I arrived at the Howard Johnson on a hot Friday afternoon and were met in the lobby by Jefferson Kim, the hotel's cherubic twenty-eight-year-old general manager. "You're the first person who's ever paid in bitcoin," he said, shaking my hand enthusiastically.

Kim explained that he had started mining bitcoins two months earlier. He liked that the currency was governed by a set of logical rules, rather than the mysterious machinations of the Federal Reserve. A dollar today, he pointed out, buys you what a nickel bought a century ago, largely because so much money has been printed. And, he asked, why trust a currency backed by a government that is fourteen trillion dollars in debt?

Kim had also figured that bitcoin mining would be a way to make up the twelve hundred dollars he'd spent on a high-performance gaming computer. So far, he'd made only four hundred dollars, but it was fun to be a pioneer. He wanted bitcoin to succeed, and in order for that to happen businesses needed to start accepting it.

The truth is that most people don't spend the bitcoins they buy; they hoard them, hoping that they will appreciate. Businesses are afraid to accept them, because they're new and weird—and because the value can fluctuate wildly. (Kim immediately exchanged the bitcoins I sent him for dollars to avoid just that risk.) Still, the currency is young and has several attributes that appeal to merchants. Robert Schwarz, the owner of a computer-repair business in Klamath Falls, Oregon, began selling computers for bitcoin to sidestep steep credit-card fees, which he estimates cost him three per cent on every transaction. "One bank called me saying they had the lowest fees," Schwarz said. "I said, 'No, you don't. Bitcoin does.' " Because bitcoin transfers can't be reversed, merchants also don't have to deal with credit-card charge-backs from dissatisfied customers. Like cash, it's gone once you part with it.

At the Howard Johnson, Kim led us to the check-in counter. The lobby featured imitation-crystal chandeliers, ornately framed oil paintings of Venice, and, inexplicably, a pair of faux elephant tusks painted gold. Kim explained that he hadn't told his mother, who owned the place, that her hotel was accepting bitcoins: "It would be too hard to explain what a bitcoin is." He said he had activated the tracking program on his mother's Droid, and she was currently about six miles away. Today, at least, there was no danger of her finding out about her hotel's financial innovation. The receptionist handed me a room card, and Kim shook my hand. "So just enjoy your stay," he said.

Nakamoto's extensive online postings have some distinctive characteristics. First of all, there is the flawless English. Over the course of two years, he dashed off about eighty thousand words—the approximate length of a novel—and made only a few typos. He covered topics ranging from the theories of the Austrian economist Ludwig von Mises to the history of commodity markets. Perhaps most interestingly, when he created the first fifty bitcoins, now known as the "genesis block," he permanently embedded a brief line of text into the data: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."

This is a reference to a *Times* of London article that indicated that the British government had failed to stimulate the economy. Nakamoto appeared to be saying that it was time to try something new. The text, hidden amid a jumble of code, was a sort of digital battle cry. It also indicated that Nakamoto read a British newspaper. He used British spelling ("favour," "colour," "grey," "modernised") and at one point described something as being "bloody hard." An apartment was a "flat," math was "maths," and his comments tended to appear after normal business hours ended in the United Kingdom. In an initial post announcing bitcoin, he employed American-style spelling. But after that a British style appeared to flow naturally.

I had this in mind when I started to attend the lectures at the Crypto 2011 conference, including ones with titles such as "Leftover Hash Lemma, Revisited" and "Time-Lock Puzzles in the Random Oracle Model." In the back of a darkened auditorium, I stared at the attendee list. A Frenchman onstage was talking about testing the security of encryption systems. The most effective method, he said, is to attack the system and see if it fails. I ran my finger past dozens of names and addresses, circling residents of the United Kingdom and Ireland. There were nine.

I soon discovered that six were from the University of Bristol, and they were all together at one of the conference's cocktail parties. They were happy to chat but entirely dismissive of bitcoin, and none had worked with peer-to-peer technology. "It's not at all interesting to us," one of them said. The two other cryptographers from Britain had no history with large software projects. Then I started looking into a man named Michael Clear.

Clear was a young graduate student in cryptography at Trinity College in Dublin. Many of the other research students at Trinity posted profile pictures and phone numbers, but Clear's page just had an e-mail address. A Web search turned up three interesting details. In 2008, Clear was named the top computer-science undergraduate at Trinity. The next year, he was hired by Allied Irish Banks to improve its currency-trading software, and he co-authored an academic paper on peer-to-peer technology. The paper employed British spelling. Clear was well versed in economics, cryptography, and peer-to-peer networks.

I e-mailed him, and we agreed to meet the next morning on the steps outside the lecture hall. Shortly after the appointed time, a long-haired, square-jawed young man in a beige sweater walked up to me, looking like an early-Zeppelin Robert Plant. With a pronounced brogue, he introduced himself. "I like to keep a low profile," he said. "I'm curious to know how you found me."

I told him I had read about his work for Allied Irish, as well as his paper on peer-to-peer technology, and was interested because I was researching bitcoin. I said that his work gave him a unique insight into the subject. He was wearing rectangular Armani glasses and squinted so much I couldn't see his eyes.

"My area of focus right now is fully homomorphic encryption," he said. "I haven't been following bitcoin lately."

He responded calmly to my questions. He was twenty-three years old and studied theoretical cryptography by himself in Dublin—there weren't any other cryptographers at Trinity. But he had been programming computers since he was ten and he could code in a variety of languages, including C++, the language of bitcoin. Given that he was working in the banking industry during tumultuous times, I asked how he felt about the ongoing economic crisis. "It could have been averted," he said flatly.

He didn't want to say whether or not the new currency could prevent future banking crises. "It needs to prove itself," he said. "But it's an intriguing idea."

I told him I had been looking for Nakamoto and thought that he might be here at the Crypto 2011 conference. He said nothing. Finally, I asked, "Are you Satoshi?"

He laughed, but didn't respond. There was an awkward silence.

"If you'd like, I'd be happy to review the design for you," he offered instead. "I could let you know what I think."

"Sure," I said hesitantly. "Do you need me to send you a link to the code?"

"I think I can find it," he said.

Soon after I met Clear, I travelled to Glasgow, Kentucky, to see what bitcoin mining looked like. As I drove into the town of fourteen thousand, I passed shuttered factories and a central square lined with empty storefronts. On Howdy 106.5, a local radio station, a man tried to sell his bed, his television, and his basset hound—all for a hundred and ten dollars.

I had come to visit Kevin Groce, a forty-two-year-old bitcoin miner. His uncles had a garbage-hauling business and had let him set up his operation at their facility. The dirt parking lot was jammed with garbage trucks, which reeked in the summer sun.

"I like to call it the new moonshining," Groce said, in a smooth Kentucky drawl, as he led me into a darkened room. One wall was lined with four-foot-tall homemade computers with blinking green and red lights. The processors inside were working so hard that their temperature had risen to a hundred and seventy degrees, and heat radiated into the room. Each system was a jumble of wires and hacked-together parts, with a fan from Walmart duct-taped to the top. Groce had built them three months earlier, for four thousand dollars. Ever since, they had generated a steady flow of bitcoins, which Groce exchanged for dollars, averaging about a thousand per month so far. He figured his investment was going to pay off.

Groce was wiry, with wisps of gray in his hair, and he split his time between working on his dad's farm, repairing laptops at a local computer store, and mining bitcoin. Groce's father didn't understand Kevin's enthusiasm for the new currency and expected him to take over the farm. "If it's not attached to a cow, my dad doesn't think much of it," Groce said.

Groce was engaged to be married, and planned to use some of his bitcoin earnings to pay for a wedding in Las Vegas later in the year. He had tried to explain to his fiancée how they could afford it, but she doubted the financial prudence of filling a room with bitcoin-mining rigs. "She gets to cussing every time we talk about it," Groce confided. Still, he was proud of the powerful computing center he had constructed. The machines ran non-stop, and he could control them remotely from his iPhone. The arrangement allowed him to cut tobacco with his father and monitor his bitcoin operation at the same time.

Nakamoto knew that competition for bitcoins would eventually lead people to build these kinds of powerful computing clusters. Rather than let that effort go to waste, he designed software that uses the

processing power of the lottery players to confirm and verify transactions. As people like Groce try to win bitcoins, their computers are harnessed to analyze transactions and insure that no one spends money twice. In other words, Groce's backwoods operation functioned as a kind of bank.

Groce, however, didn't look like a guy Wells Fargo would hire. He liked to stay up late at the garbage-hauling center and thrash through Black Sabbath tunes on his guitar. He gave all his computers pet names, like Topper and the Dazzler, and, between guitar solos, tended to them as if they were prize animals. "I grew up milking cows," Groce said. "Now I'm just milking these things."

A week after the Crypto 2011 conference, I received an e-mail from Clear. He said that he would send me his thoughts on bitcoin in a day. He added, "I also think I can identify Satoshi."

The next morning, Clear sent a lengthy e-mail. "It is apparent that the person(s) behind the Satoshi name accumulated a not insignificant knowledge of applied cryptography," he wrote, adding that the design was "elegant" and required "considerable effort and dedication, and programming proficiency." But Clear also described some of bitcoin's weaknesses. He pointed out that users were expected to download their own encryption software to secure their virtual wallets. Clear felt that the bitcoin software should automatically provide such security. He also worried about the system's ability to grow and the fact that early adopters received an outsized share of bitcoins.

"As far as the identity of the author, it would be unfair to publish an identity when the person or persons has/have taken major steps to remain anonymous," he wrote. "But you may wish to talk to a certain individual who matches the profile of the author on many levels."

He then gave me a name.

For a few seconds, all I could hear on the other end of the line was laughter.

"I would love to say that I'm Satoshi, because bitcoin is very clever," Vili Lehdonvirta said, finally. "But it's not me."

Lehdonvirta is a thirty-one-year-old Finnish researcher at the Helsinki Institute for Information Technology. Clear had discovered that Lehdonvirta used to be a video-game programmer and now studies virtual currencies. Clear suggested that he was a solid fit for Nakamoto.

Lehdonvirta, however, pointed out that he has no background in cryptography and limited C++ programming skills. "You need to be a crypto expert to build something as sophisticated as bitcoin," Lehdonvirta said. "There aren't many of those people, and I'm definitely not one of them."

Still, Lehdonvirta had researched bitcoin and worried about it. "The only people who need cash in large denominations right now are criminals," he said, pointing out that cash is hard to move around and store. Bitcoin removes those obstacles while preserving the anonymity of cash. Lehdonvirta is on the advisory board of Electronic Frontier Finland, an organization that advocates for online privacy, among other things. Nonetheless, he believes that bitcoin takes privacy too far. "Only anarchists want absolute, unbreakable financial privacy," he said. "We need to have a back door so that law enforcement can intercede."

But Lehdonvirta admitted that it's hard to stop new technology, particularly when it has a compelling story. And part of what attracts people to bitcoin, he said, is the mystery of Nakamoto's true identity. "Having a mythical background is an excellent marketing trick," Lehdonvirta said.

A few days later, I spoke with Clear again. "Did you find Satoshi?" he asked cheerfully.

I told him that Lehdonvirta had made a convincing denial, and that every other lead I'd been working on had gone nowhere. I then took one more opportunity to question him and to explain all the reasons that I suspected his involvement. Clear responded that his work for Allied Irish Banks was brief and of "no importance." He admitted that he was a good programmer, understood cryptography, and appreciated the bitcoin design. But, he said, economics had never been a particular interest of his. "I'm not Satoshi," Clear said. "But even if I was I wouldn't tell you."

The point, Clear continued, is that Nakamoto's identity shouldn't matter. The system was built so that we don't have to trust an individual, a company, or a government. Anybody can review the code, and the network isn't controlled by any one entity. That's what inspires confidence in the system. Bitcoin, in other words, survives because of what you can see and what you can't. Users are hidden, but transactions are exposed. The code is visible to all, but its origins are mysterious. The currency is both real and elusive—just like its founder.

"You can't kill it," Clear said, with a touch of bravado. "Bitcoin would survive a nuclear attack."

Over the summer, bitcoin actually experienced a sort of nuclear attack. Hackers targeted the burgeoning currency, and though they couldn't break Nakamoto's code, they were able to disrupt the exchanges and destroy Web sites that helped users store bitcoins. The number of transactions decreased and the exchange rate plummeted. Commentators predicted the end of bitcoin. In September, however, volume began to increase again, and the price stabilized, at least temporarily.

Meanwhile, in Kentucky, Kevin Groce added two new systems to his bitcoin-mining operation at the garbage depot and planned to build a dozen more. Ricky Wells, his uncle and a co-owner of the garbage business, had offered to invest thirty thousand dollars, even though he didn't understand how bitcoin worked. "I'm just a risk-taking son of a bitch and I know this thing's making money," Wells said. "Plus, these things are so damn hot they'll heat the whole building this winter."

To Groce, bitcoin was an inevitable evolution in money. People use printed money less and less as it is, he said. Consumers need something like bitcoin to take its place. "It's like eight-tracks going to cassettes to CDs and now MP3s," he said.

Even though his friends and most of his relatives questioned his enthusiasm, Groce didn't hide his confidence. He liked to wear a T-shirt he designed that had the words "Bitcoin Millionaire" emblazoned in gold on the chest. He admitted that people made fun of him for it. "My fiancée keeps saying she'd rather I was just a regular old millionaire," he said. "But maybe I will be someday, if these rigs keep working for me." ♦