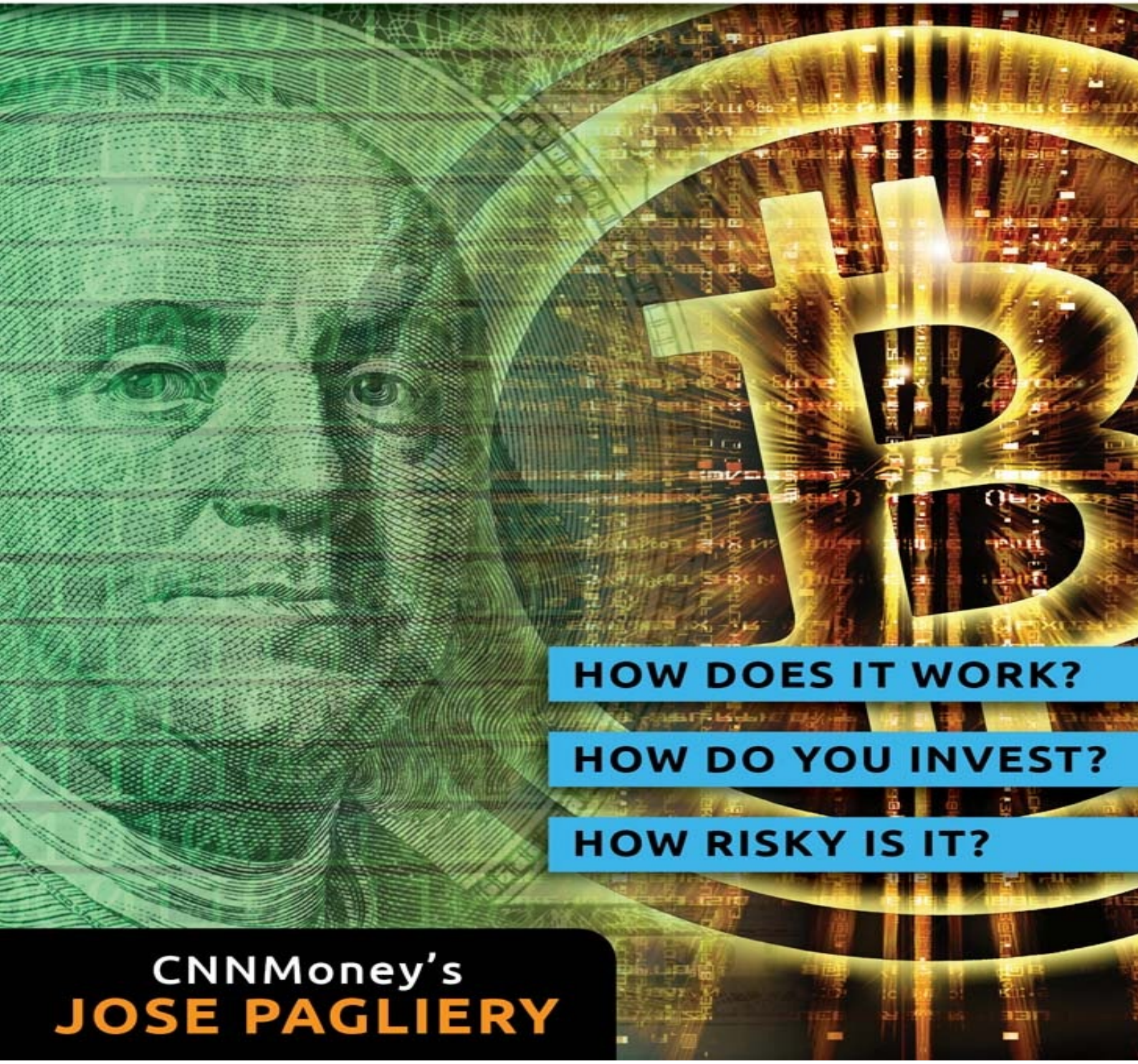
"Bitcoin is the beginning of something, not the end." —*TIME*

Bitcoin

AND THE FUTURE OF MONEY



HOW DOES IT WORK?

HOW DO YOU INVEST?

HOW RISKY IS IT?

CNNMoney's
JOSE PAGLIERY

Bitcoin

AND THE FUTURE OF MONEY

JOSE PAGLIERY

TRIUMPH
BOOKS

Triumph Books LLC
814 North Franklin Street
Chicago, Illinois 60610
(312) 337-0747
www.triumphbooks.com

Printed in U.S.A.
ISBN: 978-1-62937-036-1
Book design by Alex Lubertozzi
Photo of Sapan Shah courtesy of Christa Neu, Lehigh University.
Photo of Josh Arias courtesy of Studio Moirae Photography.

To my wife, Bridget, who inspires me, guides me, and always shows me there is a kinder, more noble way

We have progressively abandoned that freedom in economic affairs without which personal ar
political freedom has never existed in the past.

—Friedrich Hay

Contents

Acknowledgments

I AM grateful to those within the Bitcoin community who were willing to share their stories with m
Remain true to your ideals. They are rooted in a desire for a better, freer world.

To my editor at CNNMoney, David Goldman, thank you for encouraging quality journalism. T
CNNMoney's executive editor, Lex Haris, thank you for always pushing for clarity in my writing. An
thanks to CNN for approving this. I am indebted to those at Triumph for this opportunity. Thanks t
my friends who reviewed my writing and tested my logic.

I am grateful to my sister and mother for being models of strength. Mike, you pull me up when I fa
Sam Frade, you are my Doc Brown.

Baby Steps

IT WAS an otherwise quiet news day in February when word got out that the niche online trading s
Mt.Gox (mtgox.com) went offline. The difficulty for me then, as a technology and business reporter a
CNNMoney, was to explain to the average reader how a website that few had ever heard of sudden
wiped out the savings of people around the globe. The loss totaled nearly $400 million at the time. An
it was all in a currency no one understood, no less.

That was, for many people, the first time they'd heard of Bitcoin. The circumstances were less tha
ideal. But the occasion was an appropriate wake-up call.

The world was finally paying attention to the term *digital currency*. Put simply, it's electronic money-
nothing more than bits in a computer, be it your laptop, smartphone, or some far-off computer server i
a chilly, climate-controlled data center.

Make no mistake. It's real money. But it's unlike anything we've ever seen. Although it has simila
properties to the paper bills we all carry in our wallets, a digital currency like Bitcoin is not printed by
recognized authority like a government that determines how many are put into public circulation. Nor
it valued in a traditional sense like gold, whose limited supply is slowly extracted from the earth at gre
labor and expense.

You can't feel or touch bitcoins. And it's precisely that aspect of a digital currency that polarize
people. Bitcoin's most idealistic supporters celebrate it as something akin to a monetary messiah, a mean
of exchange that will let you buy anything, anytime without nasty roadblocks, like banks or la
enforcement. On the other end of the spectrum are the conservative cynics who think Bitcoin is bogu
nothing more than a moneymaking house of cards that's bound to fall as soon as the world wises up t
the fact that zeros and ones on a computer are quite worthless.

They're both wrong. Bitcoin won't upend the world's superpowers—not entirely, anyway. But it's
already leaving a lasting impact, because it represents a whole new way of thinking about mone
Therein lies Bitcoin's promise. It has the potential to transform something that's a pivotal element o
human history—shaking us to our very core.

To understand the significance of something like Bitcoin, it's worth doing a quick review of histor
While economists and anthropologists disagree about the origin of money,[1] this much is certain: It's a
old as human civilization. Money had already appeared by the time humans started jotting down th
earliest surviving accounts of their actions in ancient Mesopotamia around 3100 BCE. At the time,
wasn't a medium of exchange in the form of gold coins or paper bills, though. It was merely a ledger o
accounts, a running tally of who owes whom. But for all intents and purposes, the system of debt an
credit served as a way to trade.

Some thinkers are inclined to say that money predates even government.[2] That's the argument pu
forward by free-market proponents like Adam Smith, widely accepted as the father of capitalism, an
Austrian economist Carl Menger. Before the appearance of money, perhaps we bartered for goods. Bu
bartering—or the credit system of ancient Mesopotamia—is a terribly inefficient way to trade.

The turning point came around 2000 BCE, when money appeared in a fashion more similar to wh
we know today. People in Egypt and Mesopotamia used receipts that showed how much grain they ke

stored in temples. More than a thousand years later, metal coins gained ground in nearby areas. ~~eventually became too much of a hassle to lug around heavy sacks of misshapen bronze coins, so~~ peop everywhere opted instead for paper currency that represented value stored elsewhere, such as a bank. China, they first appeared with merchants during the Tang Dynasty around 900 CE.[3] At about the sam time in the medieval Islamic world, checks and promissory notes gained in popularity. Europe was th late bloomer, with paper currency making its first appearance in Sweden in 1661.

But that's just about where the story of monetary innovation ends. Surprising and disappointing, isn it? Since then, governments have strengthened their control over the money-printing process, an countries continue to struggle with the fact that paper notes have no intrinsic value. This makes the susceptible to inflation, as occurs when a government prints extra bills to pay off its debts. That devalue its currency relative to others and impoverishes its people.

Meanwhile, banking has evolved many times over. The concept of a bank as we know it began in Ital during the Renaissance as a simple provider of bills of exchange, financing trade. Over time, banking h morphed to include loans, quick transfers of wealth across great distances, as well as a means of investin and consulting on those very investments. Over the centuries, banking has squeezed itself into the wor of money, in the United States becoming the first and only entity to receive newly printed governme dollars. Banks have placed themselves squarely between the people who earn money and th governments that issue it. They have made themselves necessary middlemen.

Indeed, in the modern era, banks have become synonymous with money and necessary for prosperous life. Have you ever tried to conduct an expensive transaction without a bank? In most cas you'll get rejected or worse—a nasty glare from someone assuming you're up to no good. Or have yo ever tried to receive steady pay for work in cash? Professionals will most likely receive a paycheck th needs to be cashed out at a financial institution, and some employers even make direct bank deposi mandatory. But think about what that does to society at large. It puts banks at the top of the soci pyramid. Even though money is a necessary part of human interaction, something as ingrained in o consciousness as the rule of law, there exists an entity that retains firm control of it.

They are the gatekeepers. But that need not be the case.

Enter Bitcoin. For the first time in centuries, we're faced with a new kind of money. Because it runs o the Internet, this money can be sent across the globe in the blink of an eye with near anonymity. Anyon can receive it—and spend it—even if they live hundreds of miles away from their nearest ATM. An because it functions directly between one wallet holder and another, there are no banks that slow dow the transaction process. No fees. No restrictions.

It sounds too good to be true. Or maybe we just forgot how liberating money is supposed to be.

The Birth of Bitcoin

IT ALL started on an obscure online discussion forum dedicated to cryptography. The subject matter- the art of secure and secret communication—dictated that the regulars were mostly technical experts mathematics and engineering. The "low-noise moderated mailing list" on metzdowd.com served as a facto academic community, just the right place to introduce an experimental proposal that was equ parts economics and computer science.

It was Friday, October 31, 2008—Halloween, a day when millions don masks and hide their tru identity. That's when the mysterious Satoshi Nakamoto first appeared with a message titled, "Bitcoi P2P e-cash paper" posted at 2:10 PM (ET):

> I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.
> The paper is available at: http://www.bitcoin.org/bitcoin.pdf

The nine-page, academic-style document described the fundamental details for a new currency and th unique, theoretical network to deliver payments. It detailed the complex way transactions would wor the heightened privacy offered to account holders and how the software would keep people from doubl spending their digital coins.

The essay, "Bitcoin: A Peer-to-Peer Electronic Cash System" (see Appendix, p. 227), isn't a walk in th park to digest. But the introduction lays out a vision that's easy to grasp: Technological improvemen have outpaced the development of financial networks, and we've outgrown the need for banks in th process. The main gripe for Nakamoto* was that banks have become a third wheel. They used to spee up transactions, but now they slow them down. As middlemen, banks settle payment disputes betwe buyers and sellers. To do that, they must charge fees. With those costs, it's not profitable for a bank t process tiny transactions, so we're limited in the kind of purchases we can make. Making matters wors merchants fear customers might try to reverse a purchase, so they raise their rates too.

"What is needed is an electronic payment system based on cryptographic proof instead of tru allowing any two willing parties to transact directly with each other without the need for a trusted thi party," Nakamoto writes.

Nakamoto proposed a digital currency that would live on a network of computers, a well-meani community willing to lend their machines' processing power to keep it alive. Together they woul partake in a system that verifies transactions and "mines" for new bitcoins, producing electronic toke at a steady rate. Bitcoin with a capital "B" would be the name of the new system; bitcoin with lowercase "b" would mean the units of currency.

The key to the entire system was something called a block chain. This was an innovative approach th simultaneously verified transactions, kept a log of them, and created new money. Users would mine f bitcoins by solving puzzles in segments called blocks. Those blocks would house publicly viewab information about recent transactions. A solved block would produce a unique code, or hash, th formed the foundation for the next block.

He was immediately peppered with highly technical questions and concerns from others on th mailing list. Could this system handle many simultaneous transactions? What would keep people fro

spending the same coin twice? After all, they're not physical. Such a blunder would topple the who system. And what about nefarious hacker types who hijack whole server farms and turn them in spam-spewing zombies? Surely a system that lives on a network of volunteers' computers wouldn't stan a chance against that kind of coordinated attack.

Nakamoto's responses were careful, controlled, and respectful. A novel approach to verifyin transactions would prevent someone from spending the same bitcoin twice, he explained. And th system, by relying on the combined computing power of lots of users, was designed to withstand an single attack of that kind.

The responses also revealed a great deal about him. He had a firm grasp of the most fundamental an often elusive characteristics of money. He was even more familiar with cryptography, having built th core functions of Bitcoin with the notion that new coins would be produced as computers sol increasingly difficult puzzles. But first and foremost, Nakamoto was a computer geek.

"I appreciate your questions," Nakamoto wrote. "I actually did this kind of backwards. I had to wri all the code before I could convince myself that I could solve every problem, then I wrote the paper."

But there was something else. Beneath the highly technical language was a youthful idealism, a gran vision of what this opaque, unproven project could become. Nakamoto imagined that bitcoins could on day become popular enough that they would give birth to a new industry, one dedicated solely maintaining much of the network and producing new bitcoins. By then, they'd be so desirable tha hackers in control of server farms would rather use those slaves to mine for electronic money than atta the network or distribute annoying spam. At some point, the network would be large enough to easi handle the same kind of bandwidth seen by payment networks like Visa, processing tens of millions transactions each day.

Above all, though, the system would be liberating. Although all transactions between digital walle would be recorded in a public ledger, nameless wallets would allow for enhanced privacy, a sort pseudo-anonymity. Without financial institutions taking a cut, it would be easier for people to mak small, casual payments to one another. With a predetermined, controlled growth in the supply electronic money built into the software, Bitcoin could avoid runaway inflation. It could become a go- currency for people living under a government eager to print money and depreciating its own currency.

Bitcoin's rebellious nature and thinly veiled intentions didn't get lost on one commenter, who tol Nakamoto point blank: "You will not find a solution to political problems in cryptography."

"Yes," Nakamoto replied. "But we can win a major battle in the arms race and gain a new territory freedom for several years."

It was typical cypherpunk talk, derived from a school of thought that holds privacy sacred an personal liberties above everything else. In fact, understanding cypherpunk culture (not to be confus with cyberpunk, which is more of an art form) is key to appreciating Bitcoin and its enigmatic founder.

The name says it all. To use a cypher (or spelled correctly, cipher) is to convert information—say, message to a friend—from its readable form into something incomprehensible, like a string of nonsen letters, numbers, and symbols. Using the right formula, you can take that indecipherable text and chan it back into something readable.

It's quite empowering, when you think about it. The ability to communicate privately opens the abilit to truly express your thoughts, to identify political or societal problems and criticize them without fear retribution. That's particularly true as the Digital Age brings about the Information Age, when ou means of communication via computers and phones have become practically seamless—as has th capability of governments and powerful corporations to spy on those conversations. We're all human and barring the possibility that those in power are truly benevolent and infallible, securing our dialogu

from prying eyes and ears is vital to maintaining any semblance of democracy—or any free and fa society.

But only rebels side against the powers that be. The punk part relates to their attitude. Ever sin cypherpunks appeared as highly intelligent, computer-savvy activists in the 1980s, they've arme themselves with cryptography as a means for social change. In many cases, it's worked and keep working. One early figure, John Gilmore, founded the Electronic Frontier Foundation, known as th world's top defender of civil liberties in the digital realm. Another is Philip Zimmermann, creator of th computer communication encryption method PGP, which stands for Pretty Good Privacy and is used b journalists and political dissidents around the globe to hide their communication from authoritaria governments. Another product of this school of thought is Tor, formerly known as The Onion Router, special kind of software developed via funding from the United States Navy Research Laboratory th lets you surf online anonymously and access otherwise unreachable corners of the Web. Also amon their ranks is Julian Assange, founder of the journalistic outfit WikiLeaks.

Most of these names and groups are familiar to those who pay attention to the tech world. But outsi of that, they're mostly unknown. People are quick to acquire the latest smartphones, download th newest apps, and join social media networks, but they don't pay much attention to the activists toilin away to protect their privacy on those platforms.

Cypherpunks are insurgents, agitators, digital guerillas. Satoshi Nakamoto and Bitcoin fit right in.

"It's very attractive to the libertarian viewpoint if we can explain it properly," Nakamoto wrote in post on November 14, 2008. "I'm better with code than with words though."

By that point, Nakamoto had been secretly working on his project for a year and a half, according his messages to the tiny online community of cryptographers. That's telling. It would mean that th individual had started developing the electronic currency in the earliest days of the 2007 financial crisis

Let's do a little time traveling. In the spring of 2007, New Century Financial Corporation, one of th top financial entities lending to folks with poor credit, collapsed under its own weight. It stoppe accepting loan applications and, weeks later in April, filed for Chapter 11 bankruptcy protection.[1] It w among the first signs that subprime mortgage lending was doomed.

Then, over the summer, two credit rating agencies placed severe warnings on more than 600 bond because they were backed by subprime mortgages. From its New York headquarters, global investmen bank Bear Stearns liquidated two hedge funds that had bet heavily on those types of loans. Members the United States' central bank, the Federal Reserve, issued a stark warning that problems in the financi markets threatened the nation's economic growth. And the problems were global. In September, th Bank of England got approval to bail out the country's fifth-largest mortgage lender, Northern Rock.

The public was waking up to a grotesque reality. The levees guarding an otherwise conservativ financial system had been broken for years, flooding us all with easy money that had been irresponsib borrowed, lent, and traded on. Everyone was about to pay dearly for it.

In the United States, two major forces were at play. From one angle, government policies meant t increase access to loans, and therefore home ownership rates, had backfired. The once restraine landscape was now a risky one. The federal government had inflated a housing bubble through i support of Fannie Mae and Freddie Mac, two enterprises meant to ease access to home loans. Those tw entities supported a secondary market for mortgages where they could be rounded up togethe packaged, and sold to investors. And by propping up Fannie Mae and Freddie Mac with governmen backed guarantees on loans, the federal authorities had vastly increased the supply of cash available make home loans. There was an unintended result, however. To compete with these two entities, Wa Street banks created riskier types of loans.

From another angle, deregulation during the final years of the Clinton administration paved the wa for banks to run amuck and drag us all down with them. The passage of the 1999 Gramm-Leach-Blile Act repealed strict rules put in place after the 1929 stock market crash that led to the decade-long Gre Depression. Gone were the provisions of the 1933 Glass-Steagall Act preventing everyday commerci banks, the ones holding all our precious home and business loans, from also becoming risky investme banks and insurance companies. In short time, we were all exposed to the whims of Wall Street banke who knowingly traded in what was essentially garbage yet peddled out to the rest of the world as AA rated investments, the highest grade available.

The problem had several layers of complexity and points of failure. But many found the response b major governments even more appalling. Instead of letting irresponsible players pay the price for the own mistakes—banks, investors, and borrowers alike—governments moved in to bail them all out.

In the years since, the American people have had a difficult time accepting the narrative spun b politicians, central bankers, and their private banking brethren alike—that an economic disaster apocalyptic proportions could only be avoided with a collective effort using public funds. And it's easy t see why. As government shored back support of schools and community programs, the money flowe for the very banks that helped put us in this mess in the first place.

We often forget the numbers, because they all came too fast, attached to stories too complex for th average reader and at a time when people were more focused on saving their mortgages than reading th newspaper. Here's a shortlist of the dozen biggest bailouts in the United States, rounded to the neares billion, according to public interest news organization ProPublica.[2]

Entity	Total Disbursed
Fannie Mae	$116 billio
Freddie Mac	$71 billio
American International Group (AIG)	$68 billio
General Motors	$51 billio
Bank of America	$45 billio
Citigroup	$45 billio
JPMorgan Chase	$25 billio
Wells Fargo	$25 billio
GMAC (now Ally Financial)	$16 billio
Chrysler	$11 billio
Goldman Sachs	$10 billio
Morgan Stanley	$10 billio

Aside from two car manufacturers that naturally suffered from the fallout of the economic collaps every entity on the list is a financial institution.

It was in the midst of this turmoil that Bitcoin was born, just as the failures of the modern bankin system became apparent—as well as widespread disappointment in the politicians who enabled them an the regulators who failed to catch them. Our reliance on banks, middlemen that hoarded our cash an invested in risky assets, proved dangerous. And while the mass injection of money via bailouts and s called quantitative easing by the Federal Reserve have not resulted in the hyperinflation many feare there was a heightened state of distrust between the public and the bureaucrats controlling the nation

purse.

Meanwhile, in an unknown corner of the world, someone was developing a system that wouldn't ha any of these problems. Bitcoin, as Nakamoto explained in the first essay, would be a trustless syste without a need for trusted third parties: financial institutions. The entire thing would live in a netwo that is peer-to-peer; that is, it would rely solely on the users themselves. They create the currency, the transfer it, and they keep it safe.

Safeguards would be built into the software of this computer program. To prevent widespread frau stemming from people spending each electronic token twice, each transaction would carry a uniq signature that gets time-stamped on a public ledger. The system would simply reject anyone trying spend the same coin a second time. And while the list of transactions would remain public, peop would still maintain relative anonymity, because only their wallet IDs—a long string of numbers an letters—would appear for all to see.

The network would be powered and regulated by the computers people use to access the syste Computational power from people's machines would be used to create new coins by solving intrica puzzles, and their computers' processors would also be harnessed to verify transactions in the publ accounting book. In a nod to the lessons of capitalism, the system doesn't rely on the good nature people, but instead on their selfish desires. If you help solve a puzzle and mine a new batch of bitcoi you win a sort of lottery and keep your share of the proceeds. These puzzles would form the backbone the entire system, because they would regulate how quickly coins could be created. To keep productio steady and prevent inflation in their value, puzzles would increase in difficulty if computers starte solving them too quickly.

This is how Bitcoin would eliminate the need for central banks that control the money supply an subject the populace to inflation. Gone as well are banks, payment card networks, and financial wi services, like Western Union, that take a cut of every transaction.

However, banks and credit card payment companies play another role for which people rarely gi them credit. They form a buffer protecting most of us from fraud, siding squarely with consume against merchants anytime there's a disagreement about a transaction. It's called chargeback, and it's th bane of every small business owner in the United States. Say you pulled out your credit card to purcha a television that never got delivered to your door. Complain to Visa or MasterCard, and they w immediately revoke the payment. The $500 that was once on its way to the bank accounts belonging Big Al's TV Emporium is suddenly back in your possession. Lone entrepreneur Al Peabody is sudden down $500 and has one less television in stock. The delivery service swears it sent the package, and ongoing contract protects it from any liability.

Al still has to pay his hourly employees, so that money comes out of the cash flow he uses to resto the shelves. He hates the situation, but he's no match for the world's biggest financial giants. If he stop accepting credit cards, no one will buy from his shop. So instead, Al starts charging a few bucks extra every television to account for the occasional chargeback.

A payment system like Bitcoin, which cuts out trusted third-party banks, has no place f chargebacks. That's a big draw for merchants, who can rest assured they will receive payment no matte what. That says a lot about the system's philosophy: Personal responsibility is paramount. There's no wiggle room for the sorts of shenanigans that thrived during the housing bubble that led to the 200 financial collapse.

As Nakamoto wrote early on, "There's no reliance on recourse. It's all prevention."

Eventually, Nakamoto made good on his promise and delivered the actual Bitcoin software metzdowd.com's cryptography mailing list. Here's part of the message he posted on Thursday, January 8

2009, titled, “Bitcoin vo.1 released.”

Announcing the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It's completely decentralized with no server or central authority.

See bitcoin.org for screenshots.

Download link:

http://downloads.sourceforge.net/bitcoin/bitcoin-0.1.0.rar

Windows only for now. Open source C++ code is included.

- Unpack the files into a directory
- Run BITCOIN.EXE
- It automatically connects to other nodes

Evidence would later show Nakamoto had been running it for a few days. The software, Nakamo warned, was still “alpha and experimental.” As such, he offered no guarantees the system wouldn’t b restarted. But he had built the software so that it could be updated and patched as necessary.

The system was designed to produce 21 million bitcoins total—no more, no less. It was a number h picked at random. At the time in 2009, mining for new bitcoins was the easiest it would ever be. Th puzzles could be solved by the average PC in just a couple of hours. But as people joined the system, th puzzles would get more difficult and production would decrease over time. By its creator’s calculation the amount would be cut in half every four years, with 10.5 million tokens generated by 2013, anoth 5.25 million by 2018, then 2.625 million by 2023, and so on.

The electronic money could be sent in two ways. If your intended recipient was online, you could typ in their computer’s Internet Protocol (IP) address, the unique number assigned to each device connecte to the net. If they weren’t online at that moment, you could send tokens to their special Bitcoin address

It all still sounded like an elaborate game, though. What made them any different from the bra Chuck E. Cheese play tokens embossed with “In Pizza We Trust?” At least those had a 25¢ play valu you could reliably use at a skeeball machine.

“The real trick will be to get people to actually value the BitCoins [sic] so that they become currency Dustin Trammel, a security researcher in Austin, Texas, said on the forum.

Nakamoto understood the concerns, but he didn’t have a solid answer. After all, the value of bitcoi wouldn’t be backed by anything tangible, like gold or the credit of a government. “It could get started i a narrow niche like reward points, donation tokens, currency for a game or micropayments for adu sites,” Nakamoto wrote. “It might make sense just to get some in case it catches on. If enough peop think the same way, that becomes a self fulfilling prophecy.”

But at the time, there wasn’t reason to get hung up on the debate about the actual value of a bitcoi The important thing was to introduce something progressive. “I would be surprised if 10 years from no we’re not using electronic currency in some way.”

With that, Nakamoto left the discussion forum. It was time to shop around his idea.

On February 11, 2009, someone under the name Satoshi Nakamoto became a member P2Pfoundation.net, an online community dedicated to peer-to-peer projects. He, she, or they nev bothered to upload an image to his profile, but the person claimed to be a 36-year-old Japanese male. H hid his IP address and registered under satoshin@gmx.com, the same email used at the cryptograph forum.

That same day, he posted a link to the newly created Bitcoin software program. One account tallied at 31,000 lines of code. He had already mined the first batch of bitcoins, and hidden the followi message within the “genesis block” of data:

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

It was a reference to a news story that had just graced the Saturday cover of the *Times* of London—and reminder of the very problems Bitcoin was meant to address.

This time around, the description was light on the highly technical talk about cryptography. Instead was more tailored to the everyday folks who had recently grown bitter at the world's bank bailouts. this description of the Bitcoin system, Nakamoto showed he had an axe to grind with fiat currency ar fractional reserve banking.

It's worth taking a short detour to clear up the term *fiat* and provide a clear picture of how mode banking actually works. That will help explain Nakamoto's mission. Most people are under two majo misconceptions about money and banking as they exist today. One is that paper money represents valu stored elsewhere, such as gold in bank vaults. It doesn't. Money today is fiat money. These paper bill derive their value from the fact that a government mandates them. The word itself comes from the Lati term *fiat,* which roughly translates into the phrase "it shall be." This kind of money is desired, not s much because people want it, but because they're legally required to use it. And it's partly driven by fea If your government forces you to pay taxes with it, you desire that currency because you don't want t end up in prison.[3]

Governments retain more power over their finances with this kind of money, because they ca increase the supply of money at their leisure. Overwhelmed with debt to foreign nations? Just print mo money to pay it off. The negative side effect is that each dollar is then worth less. But there's also a majo benefit: If there's outside pressure threatening to wildly change the value of your country's dollar, you government is in a better position to counter the damage.

The other way to run things is with a gold standard, something the world loosely relied on fo centuries until the 1970s. In that system, paper actually represents gold stored somewhere. It contras with fiat money in that gold-backed currencies don't let governments print bills at will without sufferin immediate consequences. However, that system also subjects people to violent changes in prices nations trade with one another and their physical stock of gold fluctuates.

The other misconception relates to the way banks work. Many people are under the impression that bank takes the money you deposit there and uses it to make loans. Instead, banks make loans wi money they don't actually have. That might sound confusing, but put bluntly, there's actually a legall permissible charade that goes on. It's called the fractional reserve banking system. In the United State the largest banks are allowed to lend out 10 times the amount of money they actually keep in the vaults. When a bank approves a loan, the money merely blinks into existence on the borrower's ban account.[4] Doing so, banks essentially create money out of thin air.

The fractional reserve system makes it easier to access loans, because banks don't have to charge a much money to be profitable. It also turns banks that would normally be tiny, stingy Scrooges int massive powerhouses more inclined to give you money. The approach works until everyone asks for a their money back at once. Then it collapses.

Nakamoto told those at the P2P Foundation's website that Bitcoin could avoid the pitfalls o fractional reserve banking and fiat. First, there'd be no banks. And second, Bitcoin wouldn't be subjec to the whims of central bankers, because new money is produced by software that sticks to a strict reliable schedule. Nakamoto was tipping his hat to the approach to money supply voiced by Nobel Prize winning American economist Milton Friedman, who suggested replacing the Federal Reserve with computer.[5]

"The root problem with conventional currency is all the trust that's required to make it work

Nakamoto wrote. "The central bank must be trusted not to debase the currency, but the history of fi currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massiv overhead costs make micropayments impossible."

That same week, Nakamoto posted a similar message on SourceForge.net, a website where comput developers could upload free, open-source software for others to download. Archived numbers the show the growth was slow and steady. In the early days, Bitcoin didn't exactly go viral. In the first yea or so, the program was downloaded by fewer than 60 people a month.[6] But word got out to key playe in the tech space.

Computer programmers and tech-savvy finance experts willing to help advance the project reached o to Nakamoto. Among the first was Hal Finney, a cypherpunk who was among the first to work on th PGP encryption method. He helped Nakamoto spot a few bugs in the software and on January received 10 bitcoins (BTC) as a test, thus becoming the first ever recipient of a Bitcoin transaction Others joined in the months that followed.

Mike Hearn, an engineer at Google living in Zurich, Switzerland, extended a willing hand Nakamoto in April of that year. A short time later, Jon Matonis, managing director at the electron payment consulting company Lydia Group, did the same. In mid-2010, a self-described "code monkey living in Amherst, Massachusetts, named Gavin Andresen offered to volunteer his C++ skills to fix an problems in the payment software. Nakamoto communicated with all of them, turning what was once secretive venture into a collaborative endeavor involving dozens of technicians around the world.

All the while, the Bitcoin founder remained elusive and fiercely protective of his identity, dodging an questions about who he was, where he lived, or what gave him the skills to take on such a extraordinary undertaking. He never talked by phone. All correspondence was done via email or o pubic Bitcoin forums.

"I'm very curious to hear more about you," read Andresen's first message to Nakamoto. "How old ar you? Is Satoshi your real name? Do you have a day job? What projects have you been involved wi before?"

Nakamoto evaded them all. But he did accept the offer. "Great to have you!" he wrote back.

Over the next year, Andresen and others worked day and night to refine the software's code. Whi the Bitcoin network and its inner workings were nothing short of genius, the execution had shortcomings. Parts of the code were sloppy by Andresen's standards, according to interviews he gave i later years.[8] Even tiny mistakes could have huge consequences.

The first and—as of this writing—only major security flaw ever found in Bitcoin was discovered August 2010.[9] Someone had managed to fool the Bitcoin software into producing more than 184 billio BTC in a transaction.[10] Nakamoto, computer developer Jeff Garzik, and others raced to address th problem, purging the transaction from the system's history and patching the hole.

As time went on, additional developers were brought in to address other issues with the code. Little l little, Nakamoto transitioned from the face of the project—albeit a masked one—into the backgroun By April 2011, he had successfully handed off the keys to Andresen, who in turn led a handful of oth trusted technicians.

In a note to a developer, Nakamoto said he had "moved on to other things" and vanished.[11]

The next month, the Bitcoin software was downloaded 174,184 times from SourceForge.net. Anoth 329,229 did it in the month that followed. The world was catching on.

In those first two and a half years, Bitcoin went from being a completely unknown cryptography proje to a niche online currency. Credit for that transformation belongs to exchanges—online tradi platforms where outsiders unable to successfully mine their own bitcoins could buy them for cash. Th first to open was BitcoinMarket.com in February 2010.[12] That was followed in July by Mt.Go (mtgox.com), a rebranded site that started out as "Magic: The Gathering Online Exchange," a hub wher fans of the nerdy trading card game could buy and sell their wares.

It was amateur hour. Users frequently complained about scammers, compromised accounts, misse trades, and halted trading. But at least they could get in on the action. Mt.Gox rose to prominence, an in the latter half of 2010, the total value of all bitcoins being traded there reached an estimated $ million.

Meanwhile, Bitcoin's popularity reached analysts at the Financial Action Task Force, a intergovernmental group that keeps a watchful eye on money laundering and terrorist financi activities. In October 2010, the organization noted the proliferation of digital currencies and warne about their ability to fuel illicit activities.[13] The report's writers were spot on. Within a few weeks, th website Silk Road was launched, creating a massive marketplace—running exclusively on Bitcoin—th functioned as an eBay for drugs.

The buzz around Bitcoin drove a surge in price that reached a notable point in February 2011, when reached parity with the U.S. dollar. That caught the attention of *Time* magazine, which featured a article explaining how the currency was breaking new ground.[14] Major finance companies Vis MasterCard, and PayPal had just shut off the flow of money to WikiLeaks, preventing the public at larg from donating to the organization as retribution for its release of damning U.S. State Departme diplomatic cables. But here was Bitcoin, this tiny, unheard-of currency that could circumvent the world financial powerhouses and allow everyone to exercise their First Amendment rights—with their wallets.

But entering the Bitcoin world and keeping your electronic money safe was no less difficult tha trying to survive a lawless town in a Spaghetti Western. Bad guys were everywhere. It was hard to tell th businesses from the bandits, especially when it became routine for them to shut their doors, claim massive hack, and leave their customers empty-handed. MyBitcoin was among the first popul transaction processors, because its service was user-friendly. Naturally, it attracted those newest to th Bitcoin system. But they made for easy prey as well. In the summer of 2011, MyBitcoin announced had been hacked, robbed of its 154,406 bitcoins and decided to shut down.[15] Their bitcoins were wort more than $2 million at the time, no small sum. Some customers said they reported the incident to th FBI, but little came of it. What should they have expected? The head of the site was a mysterious onlin persona known only as "Tom Williams." They had entrusted their bitcoins to a stranger—even thoug the system was specifically designed to eliminate third parties.

Slowly but surely, the world of Bitcoin drew in folks from all corners of the world. The first wave o privacy hawks and cryptography-obsessed mathematicians gave way to a crowd of comput programmers and Libertarians. Criminals and gold bugs soon followed. When the speculative investo and venture capitalists jumped in, major media outlets took notice.

Reporters began to ask who created this strange new technology. For journalists in the cross sectio between technology and business, finding Satoshi Nakamoto became equivalent to the mad archeologic hunt for the Holy Grail. My favorite attempt came from Joshua Davis, who wrote a sweeping piece f the *New Yorker* in October 2011 that vastly narrowed down what kind of person would fit th description. Nakamoto used flawless English and occasionally used British spelling, with words li

"colour" or "modernised." He spotted Nakamoto's reference to the *Times* of London. He spoke to Da Kaminsky, an accomplished and world-renowned computer security researcher, who sketched th portrait: "Either he's a team of people who worked on this…or this guy is a genius." [16] The investigatio took him to Crypto 2011, the absolute place to be for a cryptologist like Nakamoto, as well as those the U.S. National Security Agency. There, Davis tracked down Michael Clear, one of the few from th United Kingdom in attendance, one who had graduated as a top computer science student at Trini College in Dublin, worked on Allied Irish Banks' currency-trading software, and was an expert on pee to-peer technology. Bingo. Clear rose through the ranks to become Suspect No. 1. Except, that is, for th caveat that the young man denied being Bitcoin's father—albeit with dodgy answers and a mischievou tone.

Alas, it wouldn't end there. The same feat was attempted by journalist Adam Penenberg at *Fa Company,* who used circumstantial evidence to point at three men who had filed a patent using an exa phrase from Nakamoto's white paper. [17] Information technology pioneer Ted Nelson, after reading mystifying profile of Japanese mathematician Shinichi Mochizuki, identified him as the guy.[18] Vi reporter Alec Liu looped Bitcoin programmer Andresen, the federal government, and a few others in the mix.[19] Several toyed with the idea that Satoshi Nakamoto could be the joint project of electroni manufacturers **SA**msung, **TOSHI**ba, **NAKA**michi, and **MOTO**rola.

But none of them were as explosive as the *Newsweek* cover story in March 2014.[20] The current affai magazine had been absent from store shelves, and this was its big return to print. The cover was sexy hell: a faceless man being unmasked. "The mystery man behind the crypto-currency," it promised. An boy, did it deliver a story. Senior staff writer Leah McGrath Goodman's hypothesis was poetic in it simplicity: Satoshi Nakamoto is actually Dorian Prentice Satoshi Nakamoto, a retired 64-year-ol Japanese-American model train collector in California who had, at one point, worked on secret projec for the U.S. military. On that fateful Thursday, March 6, reporters from all over Los Angeles descend on this poor man's home, demanding to know if he truly was Bitcoin's father. He offered a singl Associated Press reporter an exclusive interview—to deny everything—and endured being chased acro town by a mad convoy of cars and television trucks.

What got lost in all this frenzy? A small yet compelling detail. Bitcoin was, by design, an open-sour project meant to be constantly updated, patched, and maintained by dedicated computer programmer By the time journalists were shoving cameras into the face of this bewildered old man, more than 5 percent of the Bitcoin code had already been rewritten. Some put that figure closer to 70 percent.

Consider what that would have meant to a painting: Sure, some individual or group had stretched th canvas, sketched the piece, and laid down the oils with a paintbrush. But more than half of it had bee completely reworked, with new layers coating the old ones, giving the work new life and brilliance.

Bitcoin's group of core developers made it clear to me how much of Nakamoto's initial programmin had been reworked. It wasn't minor. In Garzik's words: "Satoshi was a brilliant designer, but not the bes software engineer. Satoshi's code lacked standard software engineering practices such as a test suite, an was quite disorganized. We have refactored or rewritten a great deal of source code."

Bitcoin's lead developer, Wladimir van der Laan, told me Nakamoto's "original C++ code was hard to read and understand, and had quite a few (usually minor) bugs." It took hundreds if not thousands o volunteer hours from smart, dedicated computer geeks in love with Bitcoin to make up for tho mistakes. They made it easier to use. And they continue to improve it with every passing day.

"It indeed doesn't matter who Satoshi is," van der Laan wrote to me. "If he/she/they would ever com back, they will have no special status in the project. By now there may be people that are mo

experienced and know more about Bitcoin and the underlying theory than Satoshi himself did. I don claim that I do, though :)"

The project had, in no small sense, outgrown its founder. It belonged to the world now.

* There are many competing theories about the true identity of Satoshi Nakamoto. Aside from the usual "Is he Japanese or not?" there also healthy debate about whether it's a man or a woman. It could be a single person or a group. For brevity and consistency, I'll abide Nakamoto's own description and simply refer to the mysterious founder as "he." But I acknowledge it could very well be a trio of intellige women at a secretive government agency.

Bitcoin Explained

SO HOW does it actually work? It helps to understand Bitcoin in two very different ways. One is to ski the surface and see how it mimics the real-life, physical money you already know. Thinking about it lik an electronic coin helps explain how it's earned, used, and traded. But it's not exactly accurate. To trul comprehend Bitcoin, you have to accept what it really is: a network that runs on a computer progra The whole system is nothing more than ones and zeros stored in computers around the worl Everything relies on the software operating at the very core of it all: the block chain.

It's worth issuing a disclaimer: Bitcoin is electronic money, it's not money stored electronically. There's a major difference. Google Wallet, for instance, is a service provided by Google that stores your cred cards, debit cards, and loyalty cards. It's a digital wallet that holds on to your traditional money. Bu Bitcoin is a totally different approach. It reimagines what money actually is.

You'll need to get up to speed on a few terms that no sensible person uses in everyday life. They com from the world of cryptography, a dizzying environment of locks and keys, puzzles and solutions, secr messages and passcodes that reveal them. Be patient. You won't need to remember everything. You ca get along fine using bitcoins without memorizing all of it. But it's worth going over at least once. In fac you'll likely come back to this chapter a few times, and the workings of the system will dawn on you ov time. For me personally, it came in waves.

Let's start by getting a view of the whole picture. The Bitcoin network consists of computers that kee up the entire system and, for doing so, get rewarded in bitcoins. Users have digital wallets and trac bitcoins between one another. The system produces a fixed number of bitcoins every hour, and tha number slowly dwindles over the years to max out at 21 million bitcoins. It's an arbitrary supply o money. There's no rhyme nor reason as to why the system tops out at that number. In any case, nearl 13 million were created by the spring of 2014. The last bitcoin is projected to be mined in the year 214 if the system survives that long.

This section will go over all of the steps and players in the Bitcoin ecosystem: miners who dig for ne bitcoins, exchanges where you can buy them, special wallets that let you store them and trade ther Everything is interconnected, so some things might not make sense at first. The true definition of bitcoin doesn't even appear until later in the chapter. Don't get ahead of yourself. Just keep reading, an everything will tie together. You can find a more formal and rigorous explanation at the end of th book, which includes the pivotal white paper published by Nakamoto.

What Is a Bitcoin?

On a superficial level, you can think of bitcoin as a token. The previous page's image depicts the mos

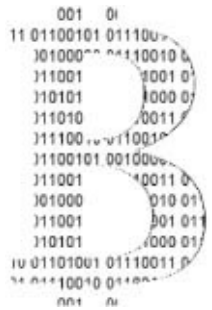
widely accepted symbol, created as a mix between a capital letter *B* and the *$* sign. That symbol didn exist in the Unicode standard used by computers when it was created, so an abbreviation is used instea BTC. A single bitcoin is denoted as 1 BTC. It's digital, so it can be broken down into tiny numeric values—all the way down to eight decimal places. That means the smallest fraction of a bitcoin 0.00000001, or one-hundred-millionth of a bitcoin (also known as a "satoshi").

Just as dollars are divided into pennies, nickels, dimes, and quarters, bitcoins are divided as well. Eac portion has a different name:

1 BTC	**a bitcoin**
0.01 BTC	**a bitcent**
0.001 BTC	**an mbit (pronounced em-bit)**
0.000 001 BTC	**a ubit (pronounced yu-bit)**
0.000 000 01 BTC	**a satoshi (named after Bitcoin's creator)**

Just like a physical token, bitcoins can be in someone's possession. That owner can move ther around, switching them to different personal wallets or handing them to someone else. Spending bitcoin means you put it in someone else's possession.

Now let's apply this thinking to the digital realm. A bitcoin can be understood as part of a large software system. Think of it as a computer file that is assigned to a certain owner's digital addre (similar to an email address). It can only be moved with special permission. It also keeps a record every place, or address, where it has ever been. That means it carries the history of every transaction in existence.



But even that definition doesn't go far enough. At a more fundamental level, bitcoins appear as section of data in a massive database. It's like a tally. There are entries on a public ledger. Any bitcoi that you "own" is really on that ledger. When you swap ownership, you hand over rights to that bitcoi Your address merely points to that bitcoin, which remains on the block chain.

What Is the Block Chain?

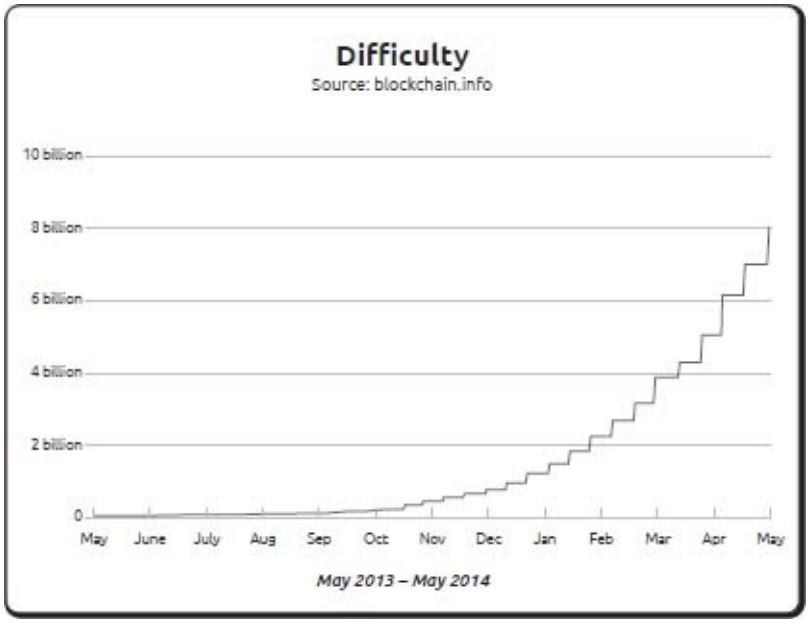
At the heart of the Bitcoin system is the function that makes it tick. It's the true innovative contributio of this entire idea. Bitcoin's block chain is a record of all the transactions that have ever taken plac which are recorded in a chain of blocks.[1] Each block houses the latest group of transactions. And whe you take the entire thing into account, it's a public ledger that details the history of every bitcoin. If bitcoin ever changed ownership, that movement shows up on the block chain. It doesn't list people names, though. It only shows digital wallets. Here's one example I randomly pulled from the popul website Blockchain.info, which lets you examine transactions:

As you can see, there's a certain degree of anonymity. Neither wallet shows anyone's true identity. Bu it's not right to call the entire system anonymous. If a wallet is tied to a specific person's name, the entir record of that person's wallet is easily available for anyone to see on the block chain. In that sense, it's th most transparent financial record the world has ever seen.

The block chain is maintained by participating computers, formally called "nodes," which verify th transactions in chunks called "blocks" and relay them across the network. This also involves solving a extremely complicated mathematical puzzle (for reasons I'll explain later). Anyone who downloads t Bitcoin software can become a node that helps sustain the system. It takes a lot of computing power an electricity, but there's a reason they volunteer. They're essentially "miners" who get rewarded in bitcoins

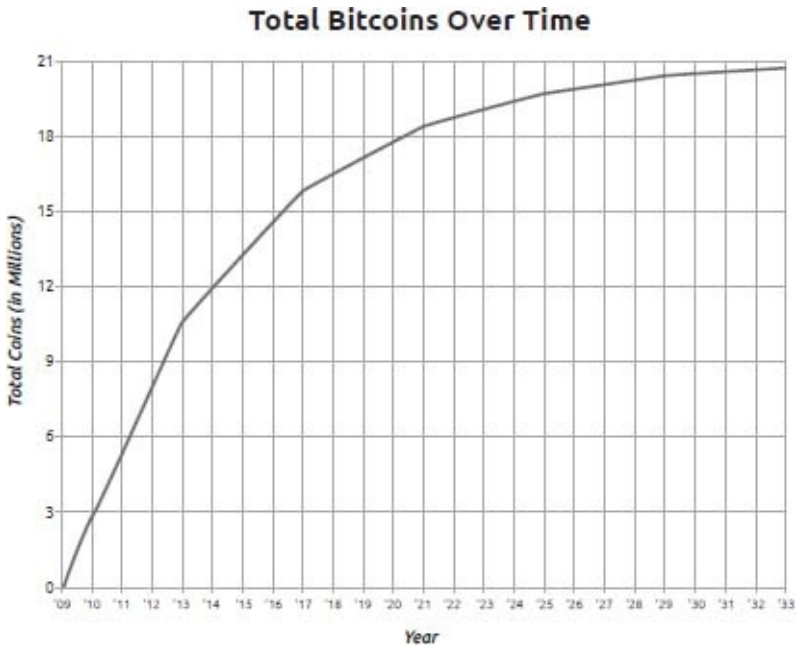
How Are Bitcoins Created?

They technically come out of thin air. The software produces them and hands ownership to the luck miner who first solved the puzzle. This is how the supply of bitcoins increases over time. Naturally, th lottery system attracts additional miners with more computing power. It's something of an arms race o powerful computing equipment, and miners even join forces to form stronger "mining pools" that sp the winnings. Sound like a farce? Consider how serious people have gotten about this. The computin power dedicated to mining for bitcoins is equal to more than 1,400 times the combined computin power of the world's top 500 supercomputers.[2] And it's only getting bigger. But Nakamoto saw th coming. To prevent them from figuring out the puzzles too often and having the money supply rise to quickly, there's a speed limit built into the software. Every two weeks (or 2,016 blocks), the difficulty o the mathematical problem increases to ensure that one block gets added to the block chain every minutes or so. That's also the time it takes for a transaction to get approved. Here's what the increasing difficulty looks like over the course of a year:



As of 2013, a miner who solves a block gets rewarded with 25 bitcoins, but that too gets smaller ov time. Every four years (or 210,000 blocks), the reward gets cut in half. In 2017 the prize gets cut down

12.5 bitcoins. Here's what Bitcoin production will look like over time:



As shown above, an estimated 98 percent of them should be produced by 2030, and the total number available bitcoins will increase very slowly after that.

How Are Bitcoins Stored and Moved?

Bitcoins are kept in digital wallets that function like a bank account. You can move funds in and ou Anyone who knows the address can deposit funds into it, but only a person with the right permissio can make withdrawals. And you can keep it locked out of reach, or accessible to others. It all depends o a special system of public and private keys.

A wallet is an encrypted computer file, and it communicates with other wallets using something call public key cryptography.[3] In the computer world, it's the tried and true method for securely transmittin information. It's quite complicated. But it's easily understood with an analogy.

Imagine you want to send a sensitive letter to a friend by physical mail. Licking an envelope shut ju won't do. Any postal worker can just open it and see what's inside. But they can't open a lock. So you ask your friend to buy a padlock, open it, and send it your way. He keeps the key. Once you receive h lock, you put your letter inside a box and close it shut with your friend's lock. Send it to him. Now h can open it with his private key, which never left his possession. This is called an asymmetric key systen and its major strength is that you never need to send keys to one another. You just share a lock—whic can't be used to open boxes anyway.

Here's how that applies to Bitcoin. Anyone can create a digital wallet. The identifying code is lon enough that, in real terms, they'll never run out. Every digital wallet is assigned a public key (the loc and a private key (the key). Your public key doubles as your address. You can share your public key t receive incoming bitcoins. That's like announcing your bank account number. That address look something like this: *1HcZyBdd53zbtoAUvUGSw1YaqTCLEA4o79*. It lets anyone deposit money in your account. But you never share your private key, because that authorizes transactions out of you wallet. It's like handing someone your secret password. That can empty your wallet in a flash.

Conversely, if you want to send bitcoins out of your wallet, you'll need your friend's public key. Bu you'll still need your private key to authorize that outbound transaction. Think back to our postal ma analogy. When you send bitcoins to another person's digital wallet, you're essentially saying this