**CHAPTER THREE: Discovering Satoshi**  
  
Companies like Visa, Dun and Bradstreet, Underwriter's Laboratories, and so forth connect untrusting strangers into a common trust network. Our economy depends on them. Many developing countries lack these trust hubs and would benefit greatly from integrating with developed world hubs like these. While these organizations often have many flaws and weaknesses–credit card companies, for example, have growing problems with fraud, identity theft, and inaccurate reports, and Barings recently went belly up because their control systems had not properly adapted to digital securities trading–by and large these institutions will be with us for a long time.—[Nick Szabo](https://nakamotoinstitute.org/trusted-third-parties/)  
  
The greatest financial threat to people’s wealth and freedom is the trusted third party system that does not serve customers but rushes, instead, to comply with government regulations such as reporting requirements.  
  
Anonymity is a powerful tool for privacy, but individuals also need to eschew state channels that counter confidentiality. Modern data collection is voracious, and surveillance is accelerating. If you play the state’s game by following the financial paths it directs you down, then the state has written the rulebook, and it has the home advantage. It will not play fair. So do not play at all. To repeat Buckminister Fuller, “You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete.” Walking away from the state and simply living gives freedom the home advantage. Until recently, however, walking away meant a massive sacrifice of economic opportunities and quality of life because the state had a lock on what Nick Szabo calls “trust hubs.”  
  
**Satoshi and Buckminister Fuller**

The brilliance of Bitcoin: It is the new model of which Fuller spoke. Blockchain users are able to walk away from trusted third parties without deep sacrifice. The blockchain either performs the valid services of a trusted third party or it obviates the need for them. Decentralized exchanges—peer-to-peer exchanges— increasingly provide sophisticated services such as buying and selling crypto as speculation.  
  
Satoshi’s “White Paper” and the step-by-step “[Bitcoin Whitepaper: A Beginner’s Guide](https://www.bitcoin.com/guides/bitcoin-white-paper-beginner-guide)” spell out how the blockchain replaces trusted third parties. The paper defines “an electronic coin as a chain of digital signatures.” The coins travel over a distributed digital ledger, called the blockchain, by which they are recorded in a transparent, chronological, and immutable fashion. These are the basic steps in a coin’s journey:  
  
1. An individuals broadcasts a new transaction to all nodes or computers in the network.  
  
2. The nodes collect the new transaction into a block. A block is akin to a single page in the ledger of the blockchain, and it contains information on a specific transfer, as well as processing data.  
  
3. The controller of each node—called a “miner”—performs a proof of work for the block. Proof of work is a computer calculation that is difficult to produce in terms of processing power and time, but it is easy for others to verify.  
  
4. When a node has a proof of work, it broadcasts the completed block to all other nodes.  
  
5. Nodes accept the block only if the transaction is valid and the coin has not already been spent. Unique timestamps, which are included in every block, prevent double spending.  
  
6. The nodes express acceptance of the block by proceeding to work on the next one in the chain, using the hash of the previously accepted block to build a seamless continuity of information. A hash is a function that converts an input into an alphanumeric string of fixed size. Each block has a unique hash value.  
  
Trusted third parties originally arose because they provided valid functions to customers. The functions included verification of a transaction, ease and security of a transfer, preservation of privacy, prevention of double spending, mediation of disputes, and provision of a record. Today’s trusted third parties have perverted these valuable services to customers into assaults upon them. Bitcoin returns these services to individuals without attendant attacks.  
  
*Verification of a transaction.* A valid trusted third party authenticates a transaction. A bank may compare the signature on a check with one that’s kept on file, or it may verify that money is not counterfeit. These services have value. But a staggering amount of authentication performed by banks today is a *dis* value to customers. The exhaustive verification of a customer’s identity, for instance,  
  
violates his privacy to satiate the government’s appetite for data, which is often used to damage the customer.  
  
The blockchain verifies transactions without intruding upon users. The transfer is authenticated, not the participants. The transaction is verified by miners through a proof of work conducted on a block. A coin is authenticated when the proof of work is completed, and the block is accepted by the blockchain. Since the blockchain is an open public ledger, everyone can trace the history of a coin and be assured of a transaction’s accuracy without knowing the identity of those involved. The government is able to browse the blockchain, but the ledger is far more of a barrier than an aid to surveillance.  
  
*Ease of transfer.* As global commerce gallops forward and the Internet encourages instant gratification, the speed and ease of transfers become increasingly important—that is, to the customer. With a virtual monopoly on international transfers, however, banks set terms that advantage them and disadvantage customers. Banks impose direct and indirect costs. One direct cost is the fee attached to each transfer, which can be substantial. Three indirect costs: the currency conversion, if necessary; the personal information required; and the considerable time a transfer can take to clear. The clearing period is called the “float.” Float is money in the banking system that is counted twice in the process of transferring a payment—once when the it is deposited in the payer’s bank, and once when it is received by the payee’s bank. Since the payer’s bank receives interest on the floating money, it has incentive to make the process longer than necessary.  
  
By contrast, the blockchain does not recognize distance in the transfer of wealth or information. Two computers in the same household can be as close or far away from each other (in terms of transmission time) as two computers on different continents. Miners charge a fee for their service, but the fees are known and have no hidden gotchas. If the fee for transfer of one crypto is unsatisfactory, then there are many other cryptos to choose from. By contrast, bank fees tend to be standardized. Most transfers occur quickly—at least, compared to banks—and there is no float. The blockchain has no self-interest or hidden agenda.  
  
*Security of transfer.* Even honorable banks can be hacked, robbed, and compromised in transmissions. Although much is made of crypto exchanges losing or stealing wealth from their accounts—and this is an undeniable problem—banks are as vulnerable. There is one huge difference between the two regarding security, however. Every over-the-table financial institution delivers customer information to the government, which utilizes the data to tax, confiscate, fine, and arrest customers.  
  
The blockchain is decentralized and resists hacking attacks; it cannot be corrupted by bad intentions because it is inanimate. The widely publicized loss of coins through theft occurs when a person moves from the peer-to-peer transfers that he controls and deposits his coins into an exchange, especially a centralized  
  
one. The crypto community needs to reduce the risks in this category of crypto use. The work is underway.  
  
Meanwhile, no personal information is surrendered to government. The ledger is transparent to all, including the state, but it is relatively easy to mask an identity and to scramble transfers through services such as mixers or tumblers. The blockchain is currently the most secure method by which to transfer funds online. The main threat to security is if government attempts to control the entire Internet. If this is possible to do and if alternatives did not quickly arise, then all methods of online transmission are threatened, not merely crypto.  
  
*Preservation of privacy.* The type of privacy once notoriously offered by Swiss banks is long gone, even in Switzerland. Financial institutions are choke points at which a customer’s personal data are collected and shared with authorities. The only true privacy is the secrecy with which [banks inform on a customer](https://news.bitcoin.com/germanys-largest-bitcoin-exchange-hands-over-customer-data-voluntarily/), without the customer’s knowledge or consent.  
  
Maintaining privacy on a transparent blockchain seems to be a contradiction in terms. The “Bitcoin Whitepaper: A Beginner’s Guide” explains why it is not. “With the peer-to-peer network, privacy can still be achieved even though transactions are announced. This is accomplished by keeping public keys anonymous. The network may be able to see payment amounts being sent and received, but transactions are not linked to identities.”  
  
If a user decides to reveal public keys, then a common privacy strategy is pseudonymity. A peer-to-peer transfer does not require information beyond the crypto addresses of the sender and the recipient, which are privately generated by each participant’s wallet. Nevertheless, when a person joins the blockchain, he becomes vulnerable to network analysis that searches for patterns of transfers in order to piece together a user’s profile. That is why some users generate a different address for every transaction, which creates multiple pseudonyms. Satoshi explains, “When you generate a new bitcoin address, it only takes disk space on your own computer (like 500 bytes). It's like generating a new PGP private key, but less CPU intensive because it's ECC. The address space is effectively unlimited. It doesn't hurt anyone, so generate all you want. ”  
  
Other standard privacy practices: create multiple wallets to isolate a transaction or a type of transaction from being associated in a pattern; cloak an IP address by going through an anonymizing tool such as Tor; and go through a mixing service.  
  
*Prevention of double spending.* Double spending is when the same unit of money is spent in more than one transaction even though it can be spent legitimately only once. Satoshi describes how traditional payment systems prevent double spending, “A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double spent. The problem with this solution is that the fate of the entire money system depends on the company  
  
running the mint, with every transaction having to go through them, just like a bank.” The solution places the money supply in the hands of a trusted third party, or even a trusted fourth party, which makes it a *non* -solution.  
  
In theory, crypto is susceptible to double spending. Two transactions with the same coin could be transmitted in rapid succession so that the first is not publicly recorded before the second one is submitted. Satoshi’s solution is elegantly simple. Every transaction is not only public but also adopted by all network participants in one time line to assure that the order of the chain is the same for everyone. Each transaction is timestamped. If a second transaction with the same coin occurs, then the earliest timestamp is counted, and the later one discarded.  
  
*Mediation of Disputes.* Physical money has had an advantage over other forms of payment; the exchange is irreversible except with consent or through a lawsuit. Most online payment systems have a built-in procedure for reversing or contesting a transaction. This service increases the overall fees of the payment system, as well as placing a practical limit on the minimum size of a transaction. It also increases the payment system’s hands-on involvement in transactions.  
  
Blockchain transfers are irreversible. Funds can be returned only on a peer-to-peer basis if a recipient agrees to do so. This obviates a fee and enables micropayments. If the traditional guarantee of “money back” is desired, then some services provide escrow for an extra fee.  
  
*Provision of a record.* Financial institutions maintain records, but their content may or may not be provided to the customer. A bank’s interaction with a tax agency, for example, will almost certainly be withheld from an account holder. This means that many records are kept for the benefit of the bank and the government only, not for the customer.  
  
The blockchain itself is the record. It is an immutable, transparent ledger of every transfer that has occurred since the original Genesis block. No concealed interaction can harm a user.  
  
In summary, crypto provides both the services of an honest third party and additional advantages.  
  
**Is Satoshi a Libertarian and Anarchist?**  
  
Part of exploring the dynamic of trusted third parties and the importance of bypassing them is to ask, “Why was this task so important to Satoshi?” Was he a libertarian and anarchist or was he politically neutral and simply fed up with banks? An explicit statement from Satoshi on the issue would have been very useful in answering this question. As the situation stands, however, the best anyone can do is to examine surrounding evidence such as [his brief online statements](https://www.bitcoin.com/satoshi-quotes/) and the White Paper, then speculate from the structure of Bitcoin itself.  
  
On October 31, 2008, Satoshi published “[Bitcoin: A Peer-to-Peer Electronic Cash System](https://www.bitcoin.com/bitcoin.pdf)” (the “White Paper”) on the Cryptography Mailing List at metzdowd.com. It presents the technology behind Bitcoin and the design of its instrument of implementation—the blockchain. Satoshi’s brief explanation is a defining technological document of our century.  
  
It is all the more remarkable, therefore, that no one seems to know Satoshi’s identity, if “he” is really a team, or much of anything else about him. Clearly, he coded from a love of technology rather than a desire for fame because he shunned the spotlight; he also did not pursue academic status. Since the code is open source and unpatented, acquiring wealth was not a driving force either, even though the one million bitcoins in his account now constitute an incredible fortune. Unlike May and other predecessors, Satoshi exhibited no swagger or desire to shock; in one post, he apologetically and modestly says, “Sorry to be a wet blanket. Writing a description for this thing [Bitcoin] for general audiences is bloody hard.” In short, no one can definitively state Satoshi’s motives or his ultimate purpose. By process of elimination, political motivation becomes more probable. His acts and words provide other reasons to reach this conclusion.  
  
Satoshi began writing Bitcoin code in 2007. When the “White Paper” appeared on the Cryptograpy mailing list in 2008, it was also made available on a website created by Satoshi—bitcoin.org. The mailing list consisted of experts in math, statistics, and cryptography, who immediately argued against the viability of Bitcoin. [It will not scale](http://satoshinakamoto.me/page/58/), they claimed; it requires too many resources to be practical, they argued. Moreover, “bad” nodes could control the network’s CPU power and generate a longer chain than “honest” nodes; bad actors could control the blockchain.  
  
Satoshi’s patient responses gradually convinced most of the list that Bitcoin might work. Meanwhile, developments in the rollout happened quickly. Highlights include:  
  
• January 3, 2009, the Genesis Block is mined.  
  
• January 9, 2009, version 0.1 of bitcoin software is released on Sourceforge. • January 12,2009, the first bitcoin transaction occurs.  
  
• October 5, 2009, an exchange rate of $1 US=1,309.03 BTC is established. • October 12, 2009, the #bitcoin-dev channel is registered for open source development communities.  
  
• December 16, 2009, version 0.2 is released.  
  
• March 6, 2010, dwdollar establishes a Bitcoin currency exchange.  
  
• May 22, 2010, first real-world transaction occurs when a pizza is purchased for 10,000 bitcoins.  
  
• July 7, 2010, version 0.3 is released.  
  
• October 16, 2010, the first escrow transaction occurs.  
  
In mid-2010, Satoshi [transferred](http://news.bitcoin.com/gavin-andresen-resumes-bitcoin-core) bitcoin.org to Gavin Andresen. Andresen  
  
[explains](http://www.huffingtonpost.ca/entry/gavin-andresen-bitcoin_n_3093316) :  
  
I started to submit code to Satoshi to improve the core system. Over time he trusted my judgment on the code I wrote. And eventually, he pulled a fast one on me because he asked me if it’d be OK if he put my email address on the bitcoin homepage, and I said yes, not realizing that when he put my email address there, he’d take his away. I was the person everyone would email when they wanted to know about bitcoin. Satoshi started stepping back as leader of [the] project and pushing me forward.  
  
In 2010, Satoshi went silent. Again, it is clear that he did not write for fame.  
  
The systematic and meticulous release of Bitcoin, as well as the elegant structure of the blockchain, reflects a man who thinks situations out in detail and understands their implications. Satoshi grasped the political impact of his revolutionary system, but he made scant comment on the matter.  
  
**Evidence of Satoshi’s Political Motives**  
  
Great debate revolves around Satoshi’s politics with many people projecting their own attitudes toward Bitcoin onto him. But all real-world indications point to Satoshi being a libertarian, an anarchist, or both. Evidence of Satoshi’s political beliefs dates back to the [Genesis block](https://news.bitcoin.com/bitcoins-quirky-genesis-block-turns-eight-years-old-today/)—the first link in the blockchain. It contains the message: “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.” The message is a headline from the front page of the UK newspaper the London *Times*. January 3, 2009 is the blockchain’s birthday—the unveiling of Satoshi’s gift to the world. Why did he choose to announce it with these specific words?  
  
Some people think the wording was a random pluck from the January 3 issue of the *Times,* and it was inserted for the sole purpose of proving the date. They claim the message could as easily have been “Ten Sex Workers Arrested in Sting.” This contention defies credibility. Satoshi was a methodical programmer who went directly to the heart of matters without frivolity, caprice, or asides. He released what he must have known was a masterpiece of coding, and it is not plausible that he slapped a random message into the Genesis block. The very fact that the first block is named “Genesis”—probably a reference to the first book of the Bible in which God creates the world—shows the significance Satoshi placed on the event.  
  
A much different scenario is highly likely. Satoshi is sitting at his computer, preparing to release the first block to the world like a seed on the wind. He knows its power, and he wants people to know its purpose without having to crack open his shell of anonymity. He has just read the morning paper with its continuing reports of financial turpitude in which political and financial elites have acted solely for their own benefit at the expense of taxpayers. A headline provides the perfect snippet about the two agencies most responsible for the economic rape of taxpayers—government and the banking system. The eight words also capture the collusion between them. Satoshi carefully types, “Chancellor on brink of second bailout for banks,” and he embeds this message into the Genesis of a  
  
dynamic he believes can change the world. The intent is anti-Chancellor, anti- bank, and [anti-bailout](https://news.bitcoin.com/tag/bailout/). From the blockchain’s first blink, it declares that the power of money is returned to the people.  
  
**Evidence From the “White Paper”**  
  
Another point of debate on Satoshi’s political intentions revolves around the neutral tone of the “White Paper.” The paper even states that a system of trusted third party financial institutions “works well enough for most transactions.” Only practical objections to the existing system are outlined within it. In short, the “White Paper” does not read like a political manifesto.  
  
Nor should it. A white paper is technical. It is an authoritative explanation of an idea or an experiment and of its results or conclusions, which is presented for review to experts in the same field. Its purpose is to lay out a concept, to solve a problem, or to reveal a finding. Ideology has no place. Moreover, the list on which Satoshi posted the “White Paper” was composed of experts in math, statistics, and cryptography who wanted the bare technical facts, not the politics surrounding them. The members undoubtedly held a variety of political views, and they may well have stumbled over ones with which they disagreed. The List was not the time, it was not the place to state political motives or beliefs.  
  
One political reference is prominently positioned, however. Footnote [1] reads, “W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.” This is Satoshi’s nod of appreciation to the 1998 b-money proposal developed by famed cypherpunk Wei Dai, with whom Satoshi had [email exchange](https://www.gwern.net/docs/bitcoin/2008-nakamoto)s. Dai’s proposal is widely viewed as a precursor to the “White Paper,” with some people believing that Dai is Satoshi. On August 22, 2007, Satoshi [emailed](http://www.gwern.net/docs/bitcoin/2008-nakamoto) Dai to inform him, “I’m getting ready to release a paper that expands on your ideas into a complete working system.” The fact that Dai’s views are a springboard to the “White Paper” make them worth examining.  
  
Dai’s [b-money proposal](http://www.weidai.com/bmoney.txt) opens:  
  
I am fascinated by Tim May’s crypto-anarchy. Unlike the communities traditionally associated with the word ‘anarchy’, in a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It’s a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations.” The proposal concludes, “The protocol proposed in this article allows untraceable pseudonymous entities to cooperate with each other more efficiently, by providing them with a medium of exchange and a method of enforcing contracts. I hope this is a step toward making crypto-anarchy a practical as well as theoretical possibility.  
  
It is also reasonable to examine the features Satoshi chose to embed within Bitcoin as a reflection of his politics. The features include:  
  
• Radical [Decentralization](https://news.bitcoin.com/decentralization-death-salvation-bitcoin/). The first line of the abstract of the “White Paper” states, “A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.” No leaders, no bureaucracy, no position of power beyond what the individual wields over himself.  
  
• Privacy. Section 10 of the “White Paper” is entitled “Privacy.” While not perfect, the anonymity sought and offered by Bitcoin is far superior to that of other forms of online payment. Section 10 ends with a warning and, perhaps, an indication of an improvement Satoshi was planning to make to the blockchain. “As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.“  
  
• Pro-capitalism. The “White Paper” stresses Bitcoin’s advantages to commerce and merchants as a free-enterprise payment system. It states, “With the possibility of reversal [which Bitcoin does not accommodate], the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need.” It is difficult to imagine a socialist having this insight or caring about merchants at all.  
  
• Anti-banking. The entire purpose of Bitcoin is “online payments…without going through a financial institution.” O[n the PGP forum](http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source), Satoshi explained, “The root problem with conventional currency is all the trust that's required to make it work. 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. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts.”  
  
• Anti-government. Although government is not mentioned in the “White Paper,” Bitcoin is a direct attack on an allegedly vital state function— banking. The message in the Genesis block was a slap at the Chancellor as much as at the bank bailout.  
  
• Anti-inflation. Section 6 of the “White Paper,” entitled “Incentive,” claims that “once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.” The predetermined number is 21 million coins that are each divisible down to a tiny fraction of a whole coin.  
  
The preceding features come close to a statement of [economic anarchism](https://news.bitcoin.com/bitcoin-built-incite-peaceful-anarchy/). A *CoinJournal* article entitled “Op-Ed: Satoshi Nakamoto is Clearly an Anarchist” refers to a 2014 presentation by Daniel Krawisz of the Satoshi Nakamoto Institute. Krawisz states, “Someone who promotes bitcoin who is not an anarchist is a crypto-anarchist because bitcoin is [inherently anarchistic](https://news.bitcoin.com/bitcoin-stop-apologizing-for-victimless-crime/) .”  
  
**Evidence From Posts and Personal Association**  
  
Satoshi’s less formal posts on forums are further evidence of his politics. Again, the remarks are anti-banking and anti-government while openly acknowledging Bitcoin’s appeal to libertarians.  
  
• Anti-banking. Again, Satoshi writes, “Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with hardly a fraction in reserve .”  
  
• Anti-government: When a poster objects to Bitcoin, saying, “You will not find a solution to political problems in cryptography,” [Satoshi responds](https://satoshi.nakamotoinstitute.org/emails/cryptography/4/) ,“Yes, but we can win a major battle in the arms race and gain a new territory of freedom for several years. Governments are good at cutting off the heads of a centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be [holding their own](http://www.mail-archive.com/cryptography@metzdowd.com/msg09971.html) .”  
  
• Pro-libertarian. “[Bitcoin is] very attractive to the libertarian viewpoint if we can explain it properly. I’m [better with code than with words though](https://www.mail-archive.com/cryptography@metzdowd.com/msg10001.html) .” Moreover, Satoshi’s post on the bitcointalk forum, [Bitcoin does NOT violate Mises' Regression Theorem](https://bitcointalk.org/index.php?topic=583.msg11405#msg11405), indicates his familiarity with Mises, and the thread itself discusses Rothbard’s signature book *Man, Economy, and State* .  
  
Personal associations are another indicator of personal beliefs. Foremost among Satoshi’s associates was the late [Hal Finney](https://news.bitcoin.com/tag/hal-finney/). A developer for the PGP Corporation, Finney was the first recipient of a bitcoin transaction, which Satoshi sent to him on January 12, 2009. Finney obviously cooperated closely with Satoshi—some believe *he* was Satoshi—which makes Finney’s political views relevant. In the early 1990s, Finney contributed regularly to the cypherpunks’ listserv. Satoshi also posted a link to his “White Paper” on the P2P Foundation’s [cypherpunk website](https://wiki.p2pfoundation.net/Cypherpunk_Movement), where he was a list member. In a post, Finney [states](http://fennetic.net/irc/finney.org/~hal/why_rem1.html), “Naturally, in today’s society, with power allocated so disproportionately, such ideas [cryptography] are a threat to large organizations. Balancing power would mean a net loss of power for them. So no institution is going to pick up and champion Chaum’s ideas. It’s going to have to be a grass-roots activity, one in which individuals first learn of how much power they can have, and then demand it.”  
  
Martti Malmi provides another clue. Malmi was a student at the Helsinki University of Technology, who became a Bitcoin enthusiast. Nathaniel Popper’s book [*Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*](https://www.theverge.com/2015/6/10/8751933/the-shy-college-student-who-helped-build-bitcoin-into-a-global) describes Malmi’s journey. Posting on the anti-state.org forum, which explored free-market anarchism, Malmi writes of Bitcoin, ‘I’m really excited about the thought of something practical that could truly bring us closer to freedom in our lifetime’. :-)” In an email to Satoshi, Malmi included a link to this post.  
  
Satoshi replies, “Your understanding of Bitcoin is spot on.”  
  
Again, Satoshi fully realized how revolutionary his system would be. When Wikileaks enabled bitcoin donations as a way to sidestep a financial blockade, Bitcoin was propelled to a new level of attention and popularity. An appalled Satoshi [posted](https://bitcointalk.org/index.php?topic=2216.msg29280#msg29280), “It would have been nice to get this attention in any other  
  
context. WikiLeaks has kicked the hornet’s nest, and the swarm is headed towards us.” He pleaded with Wikileaks not to spotlight Bitcoin because the project was young enough to be destroyed by government. Indeed, Satoshi’s decision to stay anonymous points to his understanding of the danger involved with Bitcoin. After all, earlier creators of digital money had been prominently prosecuted, and Satoshi must have watched closely as the prosecutions unfolded.  
  
The preceding argument is not definitive proof that Satoshi was either a libertarian or an anarchist, but it comes close to it. “Libertarian, anarchist, or both” becomes the most plausible answer *by far* to the question about his political beliefs.  
  
**Evidence From Satoshi’s Environment**  
  
The political-economic atmosphere from which Bitcoin emerged provide one more indication of Satoshi’s beliefs.  
  
Bitcoin’s coding began in 2007, and the timing is unlikely to be a coincidence. The  
  
[financial crisis](https://news.bitcoin.com/revolutionary-protocol-emergence-bitcoin/) of 2007-2008 has been called the worst one to occur since the Great Depression of the 1930s. It was caused largely by the trusted third parties Satoshi opposed the most: government and banking.  
  
What happened? In simplistic terms the subprime mortgage industry collapsed and sparked the crisis. A subprime mortgage is typically issued to a borrower with poor credit who poses a high risk of default. To compensate the lender for this risk, the borrower pays a high rate of interest. Subprimes became increasingly common in the period before 2007 for several reasons. One was the use of automated underwriting software that sped up the loan process but bypassed the standard review of data and documents. In short, lending institutions failed to authenticate a borrower’s eligibility. Housing prices soared on a flood of artificially loose credit. Peaking in 2006, prices started a downward spiral that lasted for years and caused massive foreclosures both in the U.S. and internationally.  
  
The high delinquency rate led to a devaluation of financial instruments, which threatened to collapse the trusted third party system—aka the financial system. The state would not and could not allow this to happen; the financial system was its right arm. On September 7, 2008, the U.S. federal government assumed the liabilities of the extremely shaky Freddie Mac and Fannie Mae. Other bailouts followed. On October 3, the [Emergency Economic Stabilization Act of 2008](https://en.wikipedia.org/wiki/Emergency_Economic_Stabilization_Act_of_2008)  
  
authorized spending up to $700 billion to purchase distressed assets and to fund financial institutions, including foreign ones. The cost of saving the hierarchy of trusted third parties was passed on to taxpayers, of course.  
  
Satoshi watched the bailouts unfold, as the Genesis block message attests. The looting of tax funds to enrich the elite, while average people lost their homes, must have looked like a trusted third party nightmare come true.  
  
Something else occurred in 2007. The U.S. federal government charged the heads of e-gold, Inc. with money laundering and the transmission of money without a license. E-gold’s owners were tried and convicted; the ruined company was forced to close its e-doors. Satoshi must have watched this situation closely as well. And he learned from it. Anonymity was safety.  
  
**Satoshi’s Legacy**  
  
Satoshi produced an elegant, original technology that rivals the Gutenberg printing press in its importance to human progress because it allows easy economic freedom on an individual level.  
  
The parallel deserves expansion. Although his printing press was not the first, Johannes Gutenberg pioneered creative innovations that had an impact similar to Satoshi’s creation. He replaced short-lived water-based inks with a durable oil- based one, for example. Most importantly, he used a strong alloy to create close to 300 separate type bits that could be quickly assembled into uniform templates and disassembled. Prior printers used fragile wooden bits or carved the letters of each page into a wooden block that was inked. The innovations transformed the printing press from a tool of elite classes—the court, the clergy—to a tool of the people. Gutenberg opened a world of information and ideas to average people who no longer had to rely on authorities for their version of the truth. The printing press decentralized knowledge into the hands of the common man, and knowledge is power. This made the printing press not merely a technical marvel but also an agent of social change and revolution.  
  
Those in power would have prevented the shift, if they could have, by plugging the flood of opinions and ideas. An illiterate, uninformed public is easier to control. A literate, informed public encourages the rise of populism and reformers who threaten the status quo. Preserving a status quo favorable to power is the main reason state censorship existed then and now, with control of the press being an essential factor. Unfortunately for the powerful, literacy increased and more people were able to judge for themselves which religious and political beliefs resonated within them as real.  
  
An example of social upheaval: without Gutenberg’s printing press, the Protestant Reformation would probably not have occurred, or it would have been very limited in scope. Martin Luther launched the Reformation in 1517 by nailing his Ninety- Five Theses to the door of a German church. The document was rapidly translated from Latin into German, then copied and reprinted; in today’s jargon, it went viral. As a man, Luther could reach only those people within the range of his voice and pen. As a mass-produced author, Luther spread ideas across Europe within months. Within three years, hundreds of thousands of copies of his Theses had been cranked off hundreds of printing presses. The Catholic Church responded by excommunicating Luther, prompting him to flee and hide. Ideas do not respond to threats of hellfire, however, nor do they flee.  
  
The Gutenberg printing press sparked movements and revolutions. But the printing press itself was not ideological, because any idea could be assembled in templates and printed en masse: Catholicism or Protestantism, individualism or socialism, Karl Marx or Ayn Rand. The machine itself was neutral. The printing press had strong ideological implications, to be sure, because it did empower the individual and the masses. In other words, it was a populist force. But authorities also used the new technology to their own statist ends. As magnificent as the printing press was, it was a tool for good or ill, depending on the purpose of the individual user.  
  
The same could be said of crypto. Its empowerment of the individual is a profoundly political act. But that empowerment makes everyone freer to choose whatever ideology they wish. Crypto itself has no settled ideological slant. That’s why individualists, anarchists, socialists and statists alike can use the blockchain as a way to pursue their own goals, whatever those goals may be. [Amir Taaki](https://news.bitcoin.com/tag/amir-taaki/), a developer of the [Darkmarket/Openbazaar and Dark Wallet](https://news.bitcoin.com/bitcoin-revolution-startup-government-syrian-kurds/), is an aggressive left- anarchist who spent time in Rojava [Syrian Kurdistan], helping to found a People’s Republic through the introduction of Bitcoin. Rojava was “under embargo, so there’s no way to move money in or out,” he explains. “So we have to actually create our own bitcoin economies. Now we have a technological tool for people to freely organise outside [the] state system. Because it is a currency not controlled by central banks.”  
  
Bitcoin can achieve a galloping diversity of goals. This is a great strength. The Gutenberg printing press provided information and perspectives that allowed people to choose religion and politics *for themselves*. Crypto gives people a control of their own economic future that allows them to choose their own lifestyles and commitments. Part of what makes the Satoshi Revolution sparkle is that it is profoundly political in empowering the individual, but it does not mandate an ideological position. That is, it does not tell empowered individuals what they must choose or how they may use their own power. Most people see little difference between the political and the ideological. Often there is not. But sometimes politics and ideology are distinct.  
  
Bitcoin is political in the same sense as the Gutenberg printing press. It decentralizes control down to the individual level—crypto is pure empowerment— but it does not dictate what individuals do with their self-control. This would be a contradiction in terms. Yet this is what the state does when it tries to control crypto; it tries to embed a contradiction in terms within society. The state takes an inherently decentralized and individualistic dynamic and attempts to centralize it into becoming an arm of government. The good news: the state attempts seem doomed to fail. The bad news: the state is going to keep on trying.