**CHAPTER TWO: Technology Meets Anarchy and Both Profit**  
  
Bitcoin is the catalyst for peaceful anarchy and freedom. It was built as a reaction against corrupt governments and financial institutions. It was not solely created for the sake of improving financial technology. But some people adulterate this truth. In reality, Bitcoin was meant to function as a monetary weapon, as a cryptocurrency poised to undermine authority. Now it is whitewashed. It is seen as a polite and unassuming technology in order to appease politicians, banksters, and soccer moms. Its purpose is sometimes concealed in order to make the tech palatable to the unwashed masses and power elite. However, no one should forget or deny why the protocol was written.—[Sterlin Lujan](https://news.bitcoin.com/bitcoin-built-incite-peaceful-anarchy/)  
  
Crypto was created to make a political difference not to make a profit. If the core developers wanted to reap a fortune, then they would not have employed open source software and eschewed the patents that would have made them billionaires. Profiting from crypto and the blockchain are laudable by-products for some, and those who accumulated riches on the free market should be applauded. This is especially true because the manner in which they made money did not interfere with anyone else’s privacy and financial freedom. Equally, the blockchain was not forged to make banking more efficient but to render it obsolete. Anyone who believes Bitcoin was designed for financial gain is not paying attention to its history or to the idealism built into its algorithms. Bitcoin was conceived as a vehicle for creating political and social change by empowering individuals and impoverishing government. The developers were [revolutionaries](https://news.bitcoin.com/original-cypherpunks-recalls-bitcoins-inception/) . Bitcoin was their opening volley.  
  
Not a moment too soon. The Internet gave the government an incredible weapon against the privacy of individuals, which would have been radically reduced without cryptography—the art of secret communication.  
  
**The History of Bitcoin**  
  
The history of Bitcoin is sometimes traced back to the engineer and scientist  
  
[Timothy C. May](https://news.bitcoin.com/introduction-cypherpunk-tale/). May’s “[Crypto Anarchist Manifesto](http://www.notbeinggoverned.com/crypto-anarchist-manifesto/)” (1988) first appeared by being distributed to a few techno-anarchists at the Crypto ’88 conference. The six- paragraph manifesto calls for a computer technology based on cryptographic  
  
protocols that would “alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation…The technology for this revolution—and it surely will be both a social and economic revolution—has existed in theory for the past decade…But only recently have computer networks and personal computers attained sufficient speed to make the ideas practically realizable.”  
  
The manifesto concludes with a cry to arms. “Arise, you have nothing to lose but your barbed wire fences!”  
  
Even in 1988, May could draw upon a rich crypto history. In the mid-1970s, cryptography ceased to be the nearly exclusive domain of military and intelligence agencies, which operated largely in secrecy. By contrast, the academic research that later surged forward was openly shared. One event in particular broke government’s grip on the field. In 1975, computer guru [Whitfield Diffie](https://news.bitcoin.com/like-gold-bitcoins-cryptography-has-been-valued-for-millenia/) and electrical engineering professor Martin Hellman invented public-key encryption and published their results the next year in the essay “[New Directions in Cryptography](https://www-ee.stanford.edu/~hellman/publications/24.pdf).” (Arguably, the public key was a re-invention as the British had developed such encryption earlier, but they had been silenced on the subject by government.) In 1977, cryptographers Ron Rivest, Adi Shamir, and Leonard Adleman created the [RSA encryption algorithm](http://projects.csmonitor.com/cypherpunk), which was one of the first practical public-key systems.  
  
[Public-key encryption](https://news.bitcoin.com/tag/public-key-encryption/) hit the computer community like an explosion. Its brilliance is its simplicity. Every user has two keys—a public and a private one—both of which are unique. The public key scrambles the text of a message that can be unscrambled only by the private key. The public key can be thrown to the wind but the private one should be closely guarded. At the time, the result was close to impenetrable privacy.  
  
Diffie was inspired by the trusted third party problem. The book *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace* (1996) quotes him as saying, “You may have protected files, but if a subpoena was served to the system manager, it wouldn’t do you any good. The administrators would sell you out, because they’d have no interest in going to jail.” His solution was to remove the need for trust through a decentralized network in which each individual possesses the mathematical key to his own privacy—the right most threatened by digital society. Public-key encryption also removed the tension of sending secure information over insecure channels. It excluded “Eve”; this is the name cryptographers call an unwanted eavesdropper who could be the state or a common criminal. Importantly, public-key encryption was free to all because a successful revolution requires nothing so much as participation.  
  
Government was not amused. The [National Security Agency (NSA)](https://news.bitcoin.com/tag/nsa/) could no longer eavesdrop at will because its domestic monopoly on encryption was suddenly ripped away. The journalist Steven Levy commented in a *Wired* article, “In 1979, Inman [then head of the NSA] gave an address that came to be known as ‘ [the](https://www.wired.com/1993/02/crypto-rebels/)  
  
[sky is falling](https://www.wired.com/1993/02/crypto-rebels/)‘ speech, warning that ‘non-governmental cryptologic activity and publication...poses clear risks to the national security’.”  
  
A later statement by cryptographer John Gilmore captured the rebellious  
  
response.  
  
Show us. Show the public how your ability to violate the privacy of any citizen has prevented a major disaster. They’re abridging the freedom and privacy of all citizens to defend us against a bogeyman that they will not explain. The decision to literally trade away our privacy is one that must be made by the whole society, not made unilaterally by a military spy agency.  
  
What could be called “the first crypto war” erupted when the NSA tried to curtail circulation of Diffie’s and Hellman’s ideas. The agency informed publishers that the two rebels and anyone who published them could face jail time for violating laws restricting the export of military weapons. One of Hellman’s outlets, the Institute of Electrical and Electronics Engineers (IEEE), received a letter that read, in part, “I have noticed in the past months that various IEEE Groups have been publishing and exporting technical articles on *encryption and cryptology* —a technical field which is covered by Federal Regulations, viz: ITAR ( [International Traffic in Arms Regulations, 22 CFR 121-128](https://alumni.stanford.edu/get/page/magazine/article/?article_id=74801)).” Gag orders were issued. Legislation was proposed. The NSA attempted to control funding to crypto research and considered requiring people to escrow their private keys with a third party who would be vulnerable to a judge’s order or to the police. This would have returned the trusted third party problem that public-key encryption was intended to avoid. In reaction, Electronic Frontier Foundation co-founder John Perry Barlow declared, “You can have my encryption algorithm…when you pry my cold dead fingers from my private key.”  
  
The NSA failed. Powerful encryption became a public good that offered  
  
extraordinary privacy to individuals.  
  
**Arise Cypherpunks**  
  
In the late 1980s, cypherpunks emerged as something akin to a movement. The deliberately humorous label was coined by hacker Judith Milhon who blended “cipher” with “cyberpunk.” The cypherpunks wanted cryptography to defend against both surveillance and censorship by the state. They also sought to build a counter-economic society as an alternative to existing bank and financial systems. As defined by its exemplar and anarcho-capitalist Samuel E. Konkin III, counter- economics is the study and practice of all peaceful human action that is forbidden by the state.  
  
The cypherpunks’ vision was facilitated by the pioneering work of computer- scientist David Chaum, nicknamed the “Houdini of crypto.” Three of his papers were particularly influential.  
  
• “[Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms](https://www.freehaven.net/anonbib/cache/chaum-mix.pdf) ” (1981) lays the groundwork for research into and development of  
  
anonymous communications based on public-key cryptography.  
  
• “[Blind Signatures for Untraceable Payments](https://link.springer.com/chapter/10.1007/978-1-4757-0602-4_18)” (1983) states, “Automation of the way we pay for goods and services is already underway…The ultimate  
  
structure of the new electronic payments system may have a substantial impact on personal privacy, as well as on the nature and extent of criminal use of payments. Ideally a new payments system should address both of these seemingly conflicting sets of concerns.” The essay calls for digital cash.  
  
• “Security without Identification: Transaction Systems to Make Big Brother Obsolete” (1985) further describes anonymous digital cash and  
  
pseudonymous reputation systems.  
  
A typical cypherpunk distrusted and disliked government, especially the federal variety; the NSA’s crusade against unclassified encryption only strengthened this response. Most cypherpunks also embraced the counterculture with its stress on free speech, sexual liberation, and the freedom to use drugs. In short, they were civil libertarians. One of the earliest portraits of the coding radicals was the Levy *Wired* article previously mentioned. Levy called them “techie-cum-civil libertarians.” They were idealists who “hope for a world where an individual’s informational footprints—everything from an opinion on abortion to the medical record of an actual abortion—can be traced only if the individual involved chooses to reveal them; a world where coherent messages shoot around the globe by network and microwave, but intruders and feds trying to pluck them out of the vapor find only gibberish; a world where the tools of prying are transformed into the instruments of privacy.” The stakes? “The outcome of this struggle may determine the amount of freedom our society will grant us in the 21st century.” The ideal is not to be granted freedom, of course, but to take it as a natural right.  
  
In 1991, Phil Zimmermann developed [Pretty Good Privacy](https://www.bitcoin.com/wp-content/uploads/2017/09/PGP-GUIDE-Public-PDF.pdf) (PGP), which became the world’s most popular email encryption software. He viewed PGP as a human rights tool and believed in it so deeply that he missed five mortgage payments and almost lost his house to design it. The original version was called “a web of trust.” Zimmermann describes this protocol in the manual for PGP version 2.0.  
  
As time goes on, you will accumulate keys from other people that you may want to designate as trusted introducers. Everyone else will each choose their own trusted introducers. And everyone will gradually accumulate and distribute with their key a collection of certifying signatures from other people, with the expectation that anyone receiving it will trust at least one or two of the signatures. This will cause the emergence of a decentralized fault-tolerant web of confidence for all public keys.  
  
PGP was initially distributed for free by being posted on computer bulletin boards. Zimmermann explained, “[l]ike thousands of dandelion seeds blowing in the wind” PGP spread around the globe. Government noticed, and Zimmermann was  
  
targeted in a three-year criminal investigation based on the possible violation of U.S. export restrictions on cryptographic software.  
  
Fast forward to 1992. [May, Milhon, Gilmore and Eric Hughes](https://www.activism.net/cypherpunk/manifesto.html) formed a small group of coding zealots who met every Saturday in a small office in San Francisco. A *Christian Science Monitor* article describes the group as “all united by that unique Bay Area blend: passionate about technology, steeped in counterculture, and unswervingly libertarian.”  
  
The group grew rapidly. An electronic posting forum called The List became its most active aspect, with the “people’s algorithms” drawing staunch support from the likes of Julian Assange and Zimmermann. The [*Christian Science Monitor* article](http://projects.csmonitor.com/cypherpunk)  
  
comments, “Radical libertarians dominated the list, along with ‘some anarcho- capitalists and even a few socialists’. Many had a technical background from working with computers; some were political scientists, classical scholars, or lawyers.” Eric Hughes contributed another manifesto to the movement. “ [A Cypherpunk’s Manifesto](https://nakamotoinstitute.org/static/docs/cypherpunk-manifesto.txt)” opens, “Privacy is necessary for an open society in the electronic age.” It continues, “for privacy to be widespread it must be part of a social contract. People must come and together deploy these systems for the common good. Privacy only extends so far as the cooperation of one’s fellows in society.”  
  
The group quickly encountered an objection that would come to dominate the government’s attack on private encryption; “bad actors,” it was argued, will use anonymity to commit crimes. During a 1992 interview, a skeptic confronted May. “Seems like the perfect thing for ransom notes, extortion threats, bribes, blackmail, insider trading and terrorism,” he [challenge](https://news.bitcoin.com/report-financing-terrorism-bitcoin-exaggerated/)d. May replied, “Well, what about selling information that isn’t viewed as legal, say about pot-growing, do-it- yourself abortion? What about the anonymity wanted for whistle blowers, confessionals, and dating personals?” What about the “good actors” who would be penalized by the removal of private encryption?  
  
Cypherpunks believed public-key encryption actually made society *less* dangerous, *less* criminal because it reduced or removed at least two major sources of violence. The first was the state; its criminal intrusion into the personal lives of individuals could be largely neutralized by effective privacy. If financial exchanges were invisible, for example, the theft of taxation or confiscation would be impossible. The second source of violence was the risk attached to victimless crimes such as drug use ,which were not viewed by the cypherpunks as crimes at all. Public-key encryption reduced or removed this risk. Ordering drugs online, for example, was safer than buying them in a back alley of a bad neighborhood at midnight.  
  
Without question, public-key encryption could shield activities that *did* violate rights, just as paying by cash could do so. This prospect was largely irrelevant, however, as encryption was a reality that would spread in spite of unpleasant side effects. Cypherpunks argued that technology or community could evolve solutions to real online crime.  
  
**The Crypto Wars Continue**  
  
One incident captured the core of the crypto wars between cypherpunks and the state. Gilmore determined to save and spread the information in documents being threatened by NSA censorship. He distributed a paper by a cryptographer whose work the NSA had been instrumental in suppressing. After Gilmore posted it on the Internet, the paper went viral. In 1992, Gilmore filed a Freedom of Information Act (FOIA) request to acquire the declassified parts of a four-volume work by William Friedman, who is sometimes called the father of American cryptography. The manuals were decades old. Gilmore also requested the declassification of Friedman’s other books.  
  
While NSA dragged out its response to the FOIA, Gilmore heard fascinating news from a cypherpunk friend. Friedman’s personal papers had been donated to a library after his death and they included the annotated manuscript of a classified book. The friend simply lifted the book off the library shelf and Xeroxed it for Gilmore. Another of Friedman’s classified books was found on microfilm at Boston University. Gilmore notified the judge in what had become a FOIA appeal that the so-called classified documents were publicly available in libraries. Before he did so, however, Gilmore made several copies of the material in question and hid them in obscure places, including an abandoned building.  
  
The NSA reacted with extreme prejudice. They raided libraries and reclassified documents that had been publicly available. The Justice Department called Gilmore’s lawyer to say that his client was close to violating the Espionage Act, which could bring a prison term of ten years. The violation: he showed people a public library book.  
  
In turn, Gilmore contacted technology reporters in the press. The NSA feared publicity, and the cypherpunks knew it. Articles critical of the NSA began to flow, including one in the *San Francisco Examiner*. Two days later, the [*New York Times* stated](http://www.nytimes.com/1992/11/28/us/in-retreat-us-spy-agency-shrugs-at-found-secret-data.html), “The National Security Agency, the nation’s secretive electronic spy agency, has abruptly retreated from a confrontation with an independent researcher over secret technical manuals he found in a public library several weeks ago….[I]t said that the manuals were no longer secret and that the researcher could keep them.” The *Aegean Park Press*, a California publisher, quickly printed the books.  
  
The early cypherpunks were prototypes who set the attitude, technology, and political context in which much of the next generation of crypto zealots operated. The goals were disobedience to unjust authority, counter-economics, personal freedom, and the disruption of a corrupt system through cryptography.  
  
**Cautionary Tales From Earlier Digital Cash**  
  
There are 3 eras of currency: commodity based, politically based, and now, math based.—Chris Dixon  
  
Versions of digital cash and online transfer systems existed decades before Bitcoin. DigiCash and e-gold are among the better-known, but neither one could shake the dogged trusted third party problem. Both lacked the essential vehicle of privacy and self-banking created by Satoshi: the blockchain. The early systems are useful as cautionary tales, however, and they spotlight the elegance of Bitcoin.  
  
*DigiCash: Its Lessons.*  
  
In 1983, the renowned cryptographer David Chaum introduced the idea of digital cash in a path-breaking research paper. In 1989, he founded an electronic money corporation named DigiCash, which, in turn, established the electronic payment system e-cash. (The actual currency was dubbed DigiCash.) E-cash has been called “technically perfect.” It built upon an earlier system designed by Chaum: Blind Signature. This is a digital signature in which the content of a message from one person is disguised so that it is not seen by a second person who authenticates the message.  
  
The process is often described by an analogy. A voter wants his ballot to remain secret. To be counted, however, it must be signed by an election official who verifies the voter’s eligibility. The solution: the voter writes his credentials on the outside of an envelope, wraps the marked ballot in carbon paper, and places it inside the envelope. The official verifies the credentials and signs the envelope, thereby transferring his signature to the ballot inside; he verifies the ballot without knowing its contents. The voter puts the now-authorized ballot into a new unmarked envelope that is slipped into a box of ballots waiting to be counted. The tabulator verifies the authenticating signature and the vote is recorded. The vote counter has no idea of who cast any particular ballot, however. Neither the content of the vote nor the ballot itself can be linked back to an individual voter. This is the essence of a blind signature.  
  
In simple terms, the Chaumian e-cash uses blind signatures as follows. At a bank that handles e-cash, you have an account with $20 to which a password gives access. To withdraw e-cash in sums of $1 each, you use software to generate 20 unique, random numbers of sufficient length that it is highly unlikely anyone else will also produce them. The problem: you need the bank to verify that each number represents $1 in value, but you don’t want the bank to know which $1 is which because then the currency could be tracked. If nothing else, the bank could match outgoing and incoming data, allowing it to know where you shop, what you buy, your lifestyle, and other information that you wish to remain private.  
  
You maintain privacy by “blinding” each request with special encryption. The bank then receives a scrambled request upon which it signs off with a private key for $1; this affirms both value and authenticity. The bank’s stamp converts the number into the equivalent of a $1 coin that can be used only by you. It is anonymous; the bank knows how many $1 units it stamped for you, but it cannot  
  
distinguish between those 20 units or recognize them from any other $1 unit it has ever authenticated.  
  
To spend the cash, you unblind the number. This results in a valid signed message that can be verified by the bank’s public key. The $1 units are stored on your computer, waiting to be sent to anyone who accepts e-cash. To do so, you send the person a decrypted, signed number, and they take it to the bank. The signature is verified; the serial number is recorded; the amount is redeemed. Recording the number allows the bank to reject any attempt at double-spending. But the bank cannot connect the transaction to your account, and the $1 recipient has no idea who you are unless you choose to reveal your identity.  
  
The process is as anonymous as cash. It stands in stark contrast to online credit- card use, which involves telling a company and a recipient who you are, where you are, and what you are purchasing. DigiCash is also safe from malicious people who are trying to steal identities. It has an extra advantage. Because it is highly divisible, it accommodates micro-payments—payments under $10, for which transaction costs make credit cards impractical. E-cash was perfect for transferring e-nickels and e-quarters over the Internet.  
  
DigiCash Inc. made quite an impact on the financial community. The first bank to adopt it was the Mark Twain Bank in St. Louis, Missouri, but others soon followed. By 1998, e-cash was available through Deutsche Bank in Germany, Credit Suisse in Switzerland, and several other powerful outlets. But, in 1998, DigiCash Inc. filed for Chapter 11 bankruptcy and subsequently sold its assets, including patents.  
  
What happened? Explanations vary and all may contain some truth.  
  
In a 1999 interview, Chaum claimed DigiCash was an idea before its time because e-commerce had not been firmly established. [*Forbes*](https://www.forbes.com/forbes/1999/1101/6411390a.html) had another explanation: “A brave new currency for a brave new world, with only one problem: No one wanted it–not banks, not merchants and, most important, not consumers. Electronic commerce is flourishing, but it turns out Visa and MasterCard–not digital cash–are the currency of choice.” Most governments were among those who did not like the untraceable money because it could be used to avoid taxes and commit other “crimes,” usually against the state.  
  
A fascinating [anonymous piece in *Next!*](https://cryptome.org/jya/digicrash.htm) magazine advanced an entirely different theory. Cryptographers, it explains, are generally paranoid. And Chaum is a GREAT cryptographer. The internal workings of DigiCash depicted in the article sound like a psychiatric ward, not a tech company. Chaum also seemed to be an abysmal businessman. One example:  
  
ING Investment Management was interested. This deal was about twenty million guilders [$10 million USD at the time]. The plans were all laid out. ING Barings together with Goldman Sachs would also bring DigiCash to the stock market within two years. ‘The day we were all set to sign, David didn’t want to’, tells Stofberg [the man responsible for DigiCash’s financial affairs].  
  
‘He was so paranoid, that he always thought something was wrong. There were 8 people from ING, including the CEO, and David simply refused to sign‘!  
  
A more interesting approach than psychologizing is to look at some of weaknesses of the e-cash and DigiCash systems, which contributed to its failure and to contrast them with the success of bitcoin and the blockchain.  
  
• Chaum believed in patent and copyright, both of which he applied to his designs. This severely restricted access and co-operative development by a global community of brilliant minds. Putting a price-tag on the product hindered broad public acceptance. By contrast, Bitcoin is patent-free and open-source, which gives unrestricted access and allows development to sprint forward.  
  
• E-cash did not get around the trusted third party problem because it needed an authorizing blind signature from a financial institution. Moreover, its growing alliance with prominent central banks indicated a growing presence of trusted third parties. Peer-to-peer bitcoin eliminates trusted third parties altogether because acceptance by the blockchain *is* the authorization, and each participant is a self-banker.  
  
• E-cash required a centralized issuer such as a bank. Bitcoin is  
  
decentralized down to the individual level.  
  
• E-cash preserved the existing banking system. Bitcoin renders the current system irrelevant.  
  
• E-cash was vulnerable to the personality flaws of one man. The Bitcoin community is haunted by internal conflicts, but no one personality can destroy it because no one owns the system. Besides which, it is always possible to create an alternate crypto to compete with one that is subpar in some manner.  
  
• E-cash was not designed for financial freedom. The essay “ Untraceable Electronic Cash,” co-authored by Chaum, stated, “Generating an electronic cash should be difficult for anyone, unless it is done in cooperation with the bank.” The anarchists and idealists who sculpted Bitcoin wanted to empower the individual against banks and the state and needed no one’s permission to do so.  
  
No wonder corporations showed immediate interest in e-cash. They have only recently shown interest in Bitcoin, which they now hope to patent, dominate, and tame for their own purposes.  
  
*E-gold: Its Lessons.*  
  
E-gold was a digital gold currency system that was operated between 1996 and 2009 by Gold & Silver Reserve, Inc. In 2000, G&SR restructured and a new company, e-gold Ltd., assumed the administration of e-metal issuance and transfers. The digital currency was linked to gold, with the typical unit of account being grams or troy ounces. Like early U.S. gold certificates, e-gold represented units of gold for which it could be redeemed on demand from stored metal.  
  
Customers with accounts on the e-gold website could also make instant transfers of precious metals to other accounts.  
  
It was one of the first payment systems to allow complex global exchanges outside the traditional banking system. A critic of fiat currency and conventional banking, co-founder and libertarian Douglas Jackson had a mission; he wanted to forge a private alternative to the financial mire caused by governments. In the book *A History of Digital Currency in the United States: New Technology in an Unregulated Market* (2016), the publisher of *Digital Gold* magazine P. Carl Mullan quoted Jackson as saying that such a “task required large-scale computational capacity, data storage and secure global means of communication.” The costs were prohibitive, except for national governments. That is, until the Internet.  
  
With the Internet, e-gold pioneered several breakthroughs. In 1999, for example, the company introduced wireless mobile payments using a web-enabled cellphone. This was seven years before PayPal offered a similar service. A less laudable innovation came in 2000 when the company required customers who wished to add value to their accounts to have a trusted and independent third party who could exchange e-gold for fiat and vice versa. Within a year, several dozen businesses and individuals filled that niche; a new industry was born.  
  
According to e-gold Ltd., the number of accounts grew from 1 million in 2003 to 5 million in 2008. E-gold users had a variety of motives. Some were gold bugs who devoutly believed e-gold was superior to fiat. Others were economic anarchists who thought government had no proper role to play in money. Still others wanted to evade taxes or the risks of other victimless crimes.  
  
Many more flooded into the emerging High Yield Investment Programs, some of which used e-gold as a payment platform. These programs offered unrealistically high returns that could be maintained only by redirecting the wealth of new investors; the Ponzi schemes led to an e-gold rush on an international level. Fraud artists took advantage of e-gold features such as the fact that all transactions were final and never charged back. The scammers opened e-gold accounts and urged prospective investors to do the same. Then they milked investors and buyers for all they could.  
  
By this time, e-gold offered a wide range of services from online casinos and auctions to metals trading and donations to non-profits. The company was rife with possibilities for scammers. Unfortunately, defrauded customers often made no distinction between the ethical e-gold itself and the con artists who ripped them off with faux investments or non-existent goods. Some disillusioned users complained to government authorities.  
  
In 2007, the U.S. Federal Government accused e-gold of money laundering and violating 18 U.S. Code § 1960, which prohibits businesses from transmitting money without a license. Several exchanges attached to e-gold were closed down. The publicity and disrupted exchanges caused a steep drop in the number of e- gold customers; the difficulty of exchanging e-gold for fiat caused potential  
  
recipients of e-gold to shy away. Many customers were trapped with accounts they could not liquidate.  
  
E-gold vigorously fought the charges, to no avail. In April 2008, the judge in  
  
[*United States of America v. E-gold, Ltd*.](http://caselaw.findlaw.com/us-dc-circuit/1465631.html) ruled against the company and in doing so dramatically increased the Treasury Department’s range of authority. The law now defined a “money transmitter” as a business that transferred any stored value from one person to another, even if the transfer involved cash. This was a blank check on future prosecutions.  
  
The company’s three directors pleaded guilty and entered into an agreement by which e-gold would comply with the legal requirements for a money-transmitting business, including being licensed. Jackson received 300 hours of community service, 3 years of supervision, and a $200 fine. He could have received 20 years and a $500,000 fine. The two other directors received the same sentence, with heavier fines.  
  
Then came a bitter irony. The guilty pleas precluded the directors from acquiring a license anywhere in the U.S. This put all of e-gold in lock-down because returning money to customers would involve transmitting money without a license, which violated the plea agreement. In 2010, the government finally allowed e-gold to return the monetized value of their accounts to customers.  
  
The Treasury’s expanded and vague definition of “money transmitter” has clear implications for bitcoin. The success of e-gold and the court case against it changed the way government handled online-payment systems. Now it had the legal precedent to act against crypto.  
  
The parallels between bitcoin and e-gold are clear. E-gold was highly divisible into micropayments as tiny as one ten-thousandth of a gram. It maintained an open ledger in which daily transactions were published live and in transparent form. Like bitcoin, e-gold was not a complementary currency. A complementary currency is one that does not compete with a national currency; an example would be private money issued as a promotion by a business to customers, which could be used to purchase merchandise in the store. E-gold was intended as a replacement for fiat and for the banking system, with the added advantage of being a hedge against inflation.  
  
The differences between bitcoin and e-gold are as important as the parallels. • E-gold embodied the trusted third party problem, as the customers  
  
stranded by legal proceedings found out. It is difficult to blame e-gold for the circumstances, of course, but dishonesty or inefficiency are not the only risks of trusting others with your money. Bitcoin eliminates this problem.  
  
• Arguably, e-gold introduced a trusted-fourth-party problem when it insisted customers use exchanges to convert into and out of fiat.  
  
• E-gold and the exchanges were points of centralization and easy targets for regulation or prohibition. They were also choke points at which to gather  
  
customer information. When e-gold restructured in 2000, OmniPay formed as the company’s exchange system. OmniPay used three methods to verify the identities of customers: universal postal verification; payment by bank wire only; and, safeguards to detect incoming third-party payments. In e- gold’s plea agreement years later, the government almost certainly gained access to that information. Peer-to-peer bitcoin is pseudonymous.  
  
• E-gold’s insistence on “membership for use” restricted the spread of its services. Bitcoin is open to all.  
  
The riskiness of a trusted third party exchange like OmniPay is a warning bell for crypto users. A centralized exchange is usually the first target of government regulation because it is visible, vulnerable, and constitutes a cache of valuable data on otherwise elusive users. Exchange owners are likely to comply with government demands because non-compliance means being closed down, imprisoned, or both. In short, centralization encourages even honest third parties to obey laws and regulations that harm customers.