Title: The Genesis Book

Subtitle: The Story of the People and Projects That Inspired Bitcoin

Author: Aaron van Wirdum

Copyright: Bitcoin Magazine Books Nashville, TN

© 2024 by Aaron van Wirdum; Creative Commons License 2.0

I don’t believe that we shall ever have a good money again before we take the thing out of the hands of government. Since we can’t take them violently out of the hands of government, all we can do is, by some sly, roundabout way, introduce something they can’t stop. - Friedrich Hayek (1984)

# Contents

### Introduction

### PART I: FOUNDATIONS

### Chanter 1: Spontaneous Order Chapter 2: Free and Open Source Software Chapter 3: Neutral Money Chapter 3: Neutral] Money Chapter 5: Denationalization of Money Chapter 6: Cash (an Trustless Time-stamps) Chapter 7: The Extropians

## PART II: CYPHERPUNKS

### Chapter 8: The Cypherpunk Movement Chapter 9: Cypherpunk Currency Chapter 10: Hashcash Chapter 11: Bit Gold Chapter 12: B-money (and BitTorrent) Chapter 13: RPOW

## PART III: BITCOIN

### Chapter 14: Twenty-First Century Fiat Chapter 15: The White Paper Chapter 16: The Release

### Acknowledgments About the Author Endnotes

### Introduction

* Digital Gold
* Legal Issues
* Satoshi Nakamoto

### PART I: FOUNDATIONS

### Chanter 1: Spontaneous Order

* Austrian Economics
* Economic Calculation
* Prices
* Interest Rates
* The Federal Reserve
* The Austrian Business Cycle
* Rivalry

### Chapter 2: Free and Open Source Software

* Hacker Culture
* Anarchism
* Trouble in Paradise
* Free Software
* GNU
* The Cathedral and the Bazaar
* Common Understanding

### Chapter 3: Neutral Money

* Barter to Money
* Gold
* The Stabilizers
* Rejecting Stable Money
* Gold Exchange Standard
  + The stabilizers also believed that international trade could still happen relatively smoothly under a gold exchange standard, if central banks would adhere to what Keynes had called the **rules of the game**.
* Monetary Nationalism
  + Series of lectures titled **Monetary Nationalism and International Stability**
  + **As a consequence, all products from United States become cheaper from the** perspective of England, while products from England become more expensive from the perspective the United States.
    - In either form, disturbed spontaneous order across borders, Hayek concluded.
* Neutral Money
  + Hayek rejected stabilization policies, and he rejected monetary nationalism.
    - Instead, he advocated for a homogenous, borderless type of money with a fixed supply.
* Currency Wars
  + When international demand shifts to the country that devalued its currency, it also means that demand shifts away from other countries.
    - Their economies tend to suffer as a result.
  + Series of currency devaluations, combined with a deep economic depression, was taking its toll-especially in the countries that had in lost the war
    - Destroyed savings, widespread unemployment, and a of prospects in large parts of Europe represented a source of uncertainty, despair and, ultimately, anger,
    - Fertile feeding ground for a new and particularly violent, nationalist, racist, and authoritarian collectivist ideology.

### Chapter 4: Cryptography

* WHITFIELD DIFFIE ALWAYS had a thing for codes.
  + He substitution cipher-a basic starting point in the mathematical branch of cryptography he’d been intrigued by this secret-keeping method.
  + Studied standard works like Helen Forché Gaines’s 1939 Cryptoanalysis, which detailed various schemes to convert messages into unreadable ciphertext, detailed various schemes to convert messages decipher them.
  + With the very basic Caesar cipher (supposedly used by Julias Caesar), messages can for example be turned into ciphertext by substituting every letter with a different letter.
    - The encryption key “+1,” say, replaces each letter by next letter in the alphabet-”a” becomes “b,” “b” becomes “c,” and so on.
  + Key isn’t very strong,
    - Patterns in an encrypted text can help specialized codebreakers figure which substitute letters likely correspond with which original letters.
    - The basic idea remained mostly unchanged. Like in the Caesar cipher, were the secret keys were always symmetric:
      * the decryption key was the same as 1 the encryption key, just used in reverse.
      * Communicate securely; people needed to share a key.
  + Diffie learned during his early studies, cryptographers believed there no other way; exchanging keys in person was how it had to be done.
* MIT
  + Diffie studied mathematics at MIT, when the first computers arrived
    - In 1965, Diffie accepted a job at Mitre, a defense contractor that ad, a few years prior, spun out of MIT’s Lincoln Laboratory.
    - Learned how much progress had been made in the field of crypto since he studied it as a kid, his intrigue was once again sparked.
    - Also learned that the real cutting edge of cryptography probably remained hidden behind closed doors.
      * The National Security (NSA)-the American intelligence agency which at the time operated in secret; it officially did not exist-had for years been scooping up many of the country's best cryptographers.
        + Idea that the NSA could be withholding important knowledge from the public did not sit well with Diffie at all.
* Stanford
  + Hacker culture first started spreading beyond MIT’s university campus, it found an early home away from home in the San Francisco Bay at Stanford University. And so would Diffie.
    - MIT graduate left litre to work for Stanford’s AI Lab instead.
    - Challenges was inspired by John McCarthy. The cofounder of MIT’s AI lab and original designer of the LISP programming language gone on to found Stanford’s AI Lab,
      * Interest in prospects of digital commerce,
      * Automated office, where software is used to digitally create, collect, store, and relay work-related documents.
        + Problem of authentication.
    - Another challenge was introduced by the Defense Department’s Advanced Research Projects Agency (ARPA),
      * Network of computers: ARPAnet.
      * Larry Roberts, was looking for ways to keep messages over the network private.
      * If communication would in the future increasingly happen electronically-and a start had now been made-sharing encryption keys **in person would likely become infeasible**, rendering private conversations impossible.
        + Unless people had access to tools that let them secure their communication anyone’s activity could potentially be monitored at any time. A chilling outlook.
  + Diffie’s renewed interest in cryptography slowly became an obsession.
    - Spurred on by reading The Codebreakers, a 1967 book by David Kahn
      * Comprehensively chronicled the entire history of cryptography and was partly based on intel from two NSA defectors who had fled to the vet Union;
* Touring America
  + Was hoping το eventually develop a logically formal theory, a mathematical system to serve as a foundation for cryptography.
    - Simplest cryptographic phenomenon he could find was the one-way function: an equation where the solution is easy to calculate in one direction, but much harder to calculate in reverse.
      * Basic type of one-way function-apolynomial should be familiar anyone who studied algebra in high schools a
        + x^2 - 5x + 8.

The input x in this example is 16, it’s relatively easy calculate that the equation would produce the output 184. However, when given only the output of 184, the equation can’t be used in reverse as easily to calculate that the original input (x) was 16.

* Public Key Cryptography |
  + It was on a regular afternoon, while housesitting for his former employer John McCarthy, that it finally hit Diffie.
  + The solution was to use two keys.
  + Cryptographers had traditionally considered it obvious that encryption keys needed to be secret since they also served as decryption keys.
    - Ignoring this “self-evident truth,” Diffie came up with the idea of key pairs.
    - A private key that should indeed remain secret, and a public key that could be freely shared.
  + Both the signature and the data itself would be impossible to forge.
  + Cryptography promised to offer both digital authentication as well as secure communication!
  + Diffie and Hellman’s first coauthored paper. “Multiuser Cryptographic Techniques,” was published in the spring of 1976, to be presented
    - “At present we have neither a proof that public key systems exist,” Diffie and Hellman admitted in their paper, “nor a demonstration system,’
* Ralph Merkle
  + Had written a paper of his own, his letter explained. However: “The people with whom I try and discuss it either fail completely to understand what’s going on, or regard any attempt at solution as impossible,”
    - About seven or eight years younger than Diffie and Hellman, Although about seven or eight Years younger
    - Merkle believed that in a world where more and more communication would go digital, a better solution was desperately needed.
  + Came up with a scheme that could, at least to an extent, do the trick.
    - First, Alice would create a great many cryptographic nuzzles, perhaps millions.
      * The solution to each puzzle would consist o a unique number in an equally unique secret key.
      * She’d know which numbers are matched with which secret keys. But each individual puzzle could also be solved by anyone else, with a little bit of computing power.
      * Alice would then send all the puzzles to Bob. Bob would in turn randomly would then send all the puzzles to Bob.
        + Bob would in turn randomly pick one puzzle, and solve it with a bit of computing power to find the unique number and the corresponding secret key.

He would then send the number (but not the corresponding secret key) back to Alice.

Alice would immediately know which secret key Bob found along with it. This secret key would be the encryption key they’d share.

Used to encrypt and decrypt messages between them.

* + - Eavesdropper would actually have to randomly start solving all the puzzles (brute force) to try and find that one unique number that Bob sent back, which would then also reveal the secret key Alice Bob settled on.
      * Computationally expensive process,
        + Power and take a long time.
        + Therefore have an asymmetric advantage against the eavesdropper.
    - Require that Alice and Bob share quite a bit of data in the form of puzzles. And the security of this solution would scale linearly with the total number of puzzles.
      * To make the scheme ten times harder to crack, they would have to share ten times as many puzzles
  + Well-funded attacker with a supercomputer could in decrypt messages within a matter of days.
    - Nonetheless, Merkle had conceived a solution that allowed two people to communicate fairly privately without the need to meet in person beforehand.
    - If not perfect, he believed that this key-exchange technique was certainly novel, and potentially useful.
      * Received little praise at Berkeley, while his paper was rejected by Communications ACM, the prestigious journal of the Association for Computing machinery (ACM).
      * Sending secret keys over an insecure network was considered unacceptable by reviewers. Besides, they had pointed out, no prior literature had established key-exchange as an important problem in the first place.
  + Merkle was quick to recognize that the duo was trying to solve a similar problem.
    - Diffie and Hellman admired the ingenuity of the proposal.
      * Key pairs, Merkle’s approach cleverly allowed Alice and to settle on a shared key in
    - Puzzle scheme did invite them to look at the problem from angle.
    - Hellman decided to take Merkle on as a summer intern,
  + The Breakthrough
    - It was Hellman who finally made the pieces click.
    - Without the need to share an encryption key in person beforehand. Similar to Merkle’s puzzle scheme, the idea behind the Diffie-Hellman key exchange (as this solution would come to be known) is that Alice and Bob can settle on a shared secret:
      * Essentially. A symmetric encryption key that they know.
    - Private keys would essentially just be very big random numbers-sa
      * Produce the shared secret, then, both Alice and Bob would each multiply their own private key with the other person’s public key. This should give both of them the same result: the shared secret.
* RSA
  + Ron Rivest, an assistant professor at university, Adi Shamir, a visiting professor, and Leonard Adleman, a computer scientist at the same institute, set out to design a one-way function specifically for public key cryptography:
    - Multiplying of prime numbers-to create a one-way function an embedded trapdoor.
  + The first multiplication would encrypt the data, while the second would decrypt it.
  + With RSA, Diffie’s vision for public key cryptography had truly arrived.
* David Chaum
  + “Cyberspace doesn’t have all the physical constraints,” Chaum later explained to a reporter from technology magazine Wired. “There are no walls. . . . it’s a different, scary, weird place, and with identification it’s a panopticon nightmare. Right? Everything you do could be known to any panopticon nightmare. Right? Everything you could be known to anyone else, could be recorded forever. Its antithetical to the basic principle underlying the mechanisms of democracy.”
  + Result in the first-vr Crypto conference in 1981,
  + On top of that, Chaum founded the International Association for Cryptologic Research, a nonprofit organization task with furthering research in cryptography
  + Greatest contributions to the field of cryptography weren’t events he organized or the organization he founded, but the tools he designed.
* Remailers
  + Public key cryptography allowed two people who’d never met before to exchange messages that only they could read. This offered privacy of communication
    - Significant privacy leak remained: traffic analysis could reveal who converses with whom, and when.
    - Metadata could reveal more about someone than they might feel comfortable with.
    - Paper “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms,”

### Chapter 5: Denationalization of Money

* ECONOMIC DEPRESSION AND currency devaluations had paved the way fascism and, ultimately, to the Second World War.
  + Friedrich Hayek sadly observed that many of his peers in academia the time failed to recognize the harm that monetary policy had done.
    - Many intellectuals of the day attributed the rise of fascism to the failure of free markets.
      * Economists, political scientists, and other academics in the West considered alternative ways to organize society, socialist ideas were gaining popularity
      * The Road to Serfdom, took a mor political approach
      * Written and published during the war years, its core thesis was that collectivist ideologies-including both fascism and socialism-tend to totalitarianism.
        + Most successful book of Hayek’s career
    - Good time for Hayek to shift more of his time and energy away from economics into the political realm. After two decades debate and rivalry, it was becoming evident that not his, but Keynes’s ideas on monetary policy were winning hearts and minds within universities, policy institutes, and government institutions.
* Bretton Woods system, as it was eventually called, started being rolled out shortly after the Axis powers were defeated in 1945-though in the West.
* The Age of Keynes
  + Hayek always contended that Keynes’s biggest oversight arguably wasn’t in economics, but in politics: elected representatives generally couldn’t be expected to apply the level of discipline that a countercyclical approach required.
* The Nixon Shock
  + President announced in a televised speech th “suspension” o th convertibility from dollars to gold,
  + In the interest of monetary stability, and in the best interest of the United “83 With no prior warning, Nixon via Executive Order single-handedly planted a bomb under the Bretton Woods system: co
    - Countries that held dollars as part of their reserves could no longer convert the paper notes precious metal.
    - Won reelection, And her 1973, the official, CPINixon got his way. He wound by 1973, the official, double-digit figures in the years that followed.85
* Inflation
* Cantillon Effect
  + Described in the eighteenth century by the Irish-French economist Richard Cantillon,
  + New money is first brought into circulation by spending it into the economy. And when the new money is first spent, is spent into an economy that still uses the “old” prices, which do not reflect the additional money created.
  + The businesses that sell these goods or services enjoy extra profits. The businesses that receive these payments, in turn, get to spend it into an economy where some prices been adjusted, bur not all; still a benefit
  + High inflation could so seriously disturb prices and, herefore, the allocation of resources, that it would eventually create strong public pressure for the imposition of price controls.
    - Disastrous outcome, in Hayek’s view:
      * “Open inflation is bad enough, but inflation repressed by controls is even worse: it is the real end of the market economy.
* Removing the Government
* Keynesians- which by that time meant almost all mainstream economists had not shared Hayek’s concern about inflation and, especially, stagflation
  + Phillips curve had shown, inflation and unemployment were inversely correlated; higher inflation would mean lower unemployment.
* Denationalizing Money
  + Quite radical form of free banking-bank
    - banks would compete to have customers use their money.
    - Could, indeed, include a currency with a fixed supply: or what Hayek had earlier in his career described as neutral money.
* Unbacked Money
  + Maintained that gold was still the best form of money: and that new currencies should at | very least be backed by the precious metal.
  + Hayek envisioned money as spontaneous order.
* Realizing Free Banking
  + Hayek’s work on money would soon after his death inspire a California-based group of hackers anɑ cryptographers.
    - But these hackers and cryptographers weren’t going to try to convince politicians, economists, and bankers to change the law. They were going to build a future without them. ..

### Chapter 6: Cash (an Trustless Time-stamps)

* Chaum who recognized that it could not yet offer privacy for a very particular type of communication: communication of value.
* A society with or without anonymous transactions would ultimately mean the difference between democracy and dictatorship, Chaum believed.
  + What was needed, he therefore concluded, was a type of digital money that offered users a similar level of privacy as physical cash.
    - The world needed electronic cash.
* The Double-Spend Problem
  + Currency consists purely of digital information—ones and zeros—it is trivial to copy.
  + “The most straightforward solution, then, is to use an account system
    - Exemplifies the privacy issue that Chaum was concerned about: the bank would know exactly who’s paying whom, how much, and when.
    - Total control over everyone’s balances, and could potentially block or vert payments, and even confiscate or delete funds.
* Blind Signatures
  + The RSA cryptographic signature algorithm. To
    - A cryptographic signature is essentially a piece of data (like sage) encrypted with a private key, which can be decrypted with a public key.
      * Blind signature, then, adds one layer of encryption to the mix.
      * The blinding key, and encrypt a message using
        + Bob would then give the encrypted message to Alice, for her to cryptographically sign with her private key.
        + When she signs the encrypted message, she doesn’t know what the original message actually she’s blind signing.
  + Mathematically linked to Alice’s public key, as any signature would be.
  + Bob could also use the blinding key first, in order to remove the layer of encryption created with it.
    - This should essentially result in a new, valid signature from Alice, this time corresponding to the original message.
    - Removed the envelope and showed Alice the letter with a carbon copy of her signature, she’d know that the letter had indeed been in the envelope she signed.
* Anonymous Payments
  + Follow-ups fleshed out exactly how to implement an electronic cash scheme, with the best detailed example of this being his 1985 paper with descriptive title “Security Without Identification: Transaction Systems Make Big Brother Obsolete.” 108
  + “The large-scale automated transaction systems of the near future can be designed to protect the privacy and maintain the security of both individuals and organizations,”
* DigiCash
  + Chaum rallied a group of students from the nearby Technical University Eindhoven, promising them a trip to the International Collegiate Programming Contest (ICPC) in Washington DC on his expense (and a vacation to Disney World in Florida to boot)
    - If they helped turn his blind signature scheme into a proof of concept.
    - Succeeded within ten days and their proof of concept earned Chaum contract.
    - Found Digian Amsterdam-based startup that would specialize in digital money;
    - “As payments on the network mature, you’re going to be paying for all kinds of small things, more payments than one makes today,” Chaum kinds of small things, more payments than one makes today, Chaum to have to pay for it.”110
* CyberBucks
  + DigiCash quickly began attracting international attention.
  + Ultimate goal to sell their eCash technology to banks, it also required bank-grade security.
    - A “made-up” currency, not backed by anything-play money, if you will. But the company did promise to never issue more than million units into circulation.
    - The company server prevented double-spends.
    - Fun and interesting experiment, DigiCash’s top priority was in the end to prepare their main electronic cash product for prime time. -
* eCash
  + Real-mony trials began in 1994
  + Institutions could acquire a license from Chaum’s startup to use
  + What was perhaps even more notable than the collaborations Chaum established, were the business deals that he failed to finalize
    - Bill Gates wanted to integrate eCash into the Windows 95 operating system, the story goes, and offered DigiCash some 100 million dollars to make it happen.
      * offered DigiCash some 100 mm dollars for each version of Windows 95 sold, which was too rich for the dollars for each version of Window 17 A
  + Employee later suggested that the same distrustful personality trait that made him a great cryptographer, got in the way when Chaum wore his business hat.
    - His “paranoid” nature would have made him unable to build up business relationships, causing him to back out of business deals at the last moment.
    - Maintains there simply wasn’t a large market for digital cash-a reading that some of the more commercially focused DigiCash employees have attested to as well.
* Bankruptcy
  + eCash simply wasn’t catching on with the greater public.
  + Chaum recalled in 1999. And: “As the Web grew, the average level of sophistication of users dropped. It hard to explain the importance of privacy to them.”117
  + Reliance on a trusted party in the form of DigiCash had turned out to be the project’s fatal flaw.
* Scott Stornetta
  + Bellcore was in the middle of what Storetta later described as a “golden age of research.” New hires weren’t even assigned specific tasks; the thirty-year-old physicist was instead instructed to find out what was important himself, and then go and on that.
    - Before his move to the East Coast, Stornetta spent the last few years at Stanford working from the Xerox PARC research center in Palo Alto.
      * Xerox division had facilitated groundbreaking innovations like the personal computer, Ethernet, and laser printing-b
        + Ugly new problem at the highly digitalized research center: forgery.
  + Humans have essentially tried to forge documents since the invention of writing. But digital
    - Foresaw a crisis of credibility
    - Wanted to design a time-stamping system for digital records:
      * Much harder when people can prove that the original document existed at an earlier point in time.
* Hash Chains
  + Digital data can be hashed, same data will result in the exact same hash every b
    - But if the original data is altered even a tiny bit, the resulting hash would change unrecognizably.
    - Special time-stamping service. A server.
* Distributing Trust
  + Hash chains did present a new problem: they didn’t scale particularly well, especially when considering the modest computational resources available to an average computer user in the early 1990s.
    - Need to store increasingly more data in order participate, more of them would likely opt out and instead just trust record held by the time-stamping service and other users,
      * Reintroduce trust into these systems: to really be secure, time-stamping scheme explicitly depended on broad participation.
    - Mathematician Dave Bayer who helped resolve this conundrum, Merkle Trees.
* Merkle Trees
  + Ralp} Merkle designed new one-way function, introduced a faster encryption protocol, proposed his own signature algorithm
  + 1979 invented the Merkle Tree. ®
    - Certificates for a public key directory:
    - Offer a compact and secure check on the contents of all sorts of data sets by combining hashes in a clever mathematical structure.
    - Pieces of data are hashed individually, so each piece of data has its own unique hash Next, all these hashes are paired in groups of two.
      * Paired again, and these pairs are again hashed together.
      * One hash left, called the Merkle Root
      * Facilitate checks to see whether the hash of a specific piece of dat is included in the tree. Importantly: this can be done without needing to any of the other dara that was hashed,
        + Merkle proofs consisting of the relevant “branches” of the tree: this essentially serves as a compact set of “directions” to find the path from the Merkle Root to the hash of the specific piece of data.
  + Unequivocally show whether data was altered,but in a much more compact format,
* A Chain of Roots

### Chapter 7: The Extropians

* FM-2030
  + Belgian-born, Iranian-American author and teacher born as Fereidoun M. Esfandiary but who went by the name FM-2030 Had throughout the 70s and 80s been popularizing a radically futurist vision for mankind.
  + Believed that any risks associated with technological innovation would offset by the rewards of progress: solar and atomic power would bring energy abundance, humans would colonize Mars, robot workers would increase leisure time, and people could earn a living from the comfort of their own homes thanks to the advent of teleworking.
    - Predicted that humans would eventually transform most radically, and turn themselves into synthetic post-biological organisms:
* Transhumanism
  + Ultimately formalized them into a new and distinct philosophical framework
    - General idea and term “transhumanism” had already been used by evolutionary biologist Julian Huxley in the 1950s, but it was More who really established it as an updated version of the humanist philosophy. 1;
      * Rejecting faith, worship, and supernatural concepts like an afterlife. But where humanists derive value and meaning from human nature and the existing human potential, transhumanists would anticipate and advocate transcending humanity’s natural limitations,
      * Neuroscience and neuropharmacology life extension, nanotechnology: artificial ultra-intelligence, and space habitation, combined with a rational philosand value system.
* Extropianism
  + A more prosperous tomorrow was best realized if society could self-organize as a spontaneous order today.
  + “The Extropian Principles: A Transhumanist Declaration.” -Max More
    - Boundless expansion, self-transformation, dynamic optimism, intelligent technology and an explicit nod to Hayak—spontaneous order.
    - Formed the acronym BEST. D.O. I. T. 50.
* The Subculture
* The High-Tech Hayekians
* AMIX
* Cryonics
* Digital Cash
* More Denationalizing Moncey

## PART II: CYPHERPUNKS

### Chapter 8: The Cypherpunk Movement

* TIM MAY COULD see glimpses of the future. He had a knack for recognizing the potential of new technologies, and could predict how they would impact society before almost anyone else could.
  + Primitive DARPA account as early as 1973 at the UC Santa Barbara college campus where he studied physics,
    - Intel, where he’d work in the Memory Products Division.
    - Solved the alpha particle problem: May discovered that Intel’s integrated circuits had been unreliable due to slightly radioactive packaging
  + Cypherpunk stories were typically in high-tech dystopias. The books generally conveyed a grim version of the future, but one where the internet (or some evolved version of it) offered a refuge for their freedom-minded protagonists.
    - Venom Vinge’s True Names,
    - Colorful and three-anncusivua
    - Ayn Rand’s Atlas Shrugged.
  + Extropians. Did share a commitment to freedom and technological advancement.
  + The “high-tech Hayekian” who’d unsuccessfully tried to establish a private space transportation industry with his startup Starstruck.
* BlackNet
  + Secret information.
    - People would be willing to pay good money for corporate secrets, classified government documents, military intel, credit data, medical records, banned religious material, or illegal pornography: May suggested, 142 And, importantly, some of those with access to this kind of information would | almost certainly be willing to sell it for the right price if they could do so anonymously.
  + The mere existence of a BlackNet could | fundamentally shake up the economic incentives that make large corporations viable in the first place.
    - Radical transparency could usher in a more dispersed and vibrant economy, characterized by a much more diverse range of smaller businesses.
* Eric Hughes
  + Concluded that DigiCash wasn't the place for him after all. He left the startup after only six weeks in amsterdam.
    - Stay with an old friend who’d moved there a few years prior: Tim Ma
      * Anonymous information markets with him.
    - After a few days of discussing potentially” game-changing use cases for public key encryption, remailers, and digital cash, their conversations kept leading back to the same nagging question.
      * Why were there still no software tools that implemented these protocols?
      * Of the breakthrough crypto innovations proposed since the 1970s were actually being put to practice by real people, because there were no computer programs available that implemented these protocols.
* The Meeting
  + Hughes and May had come agree that it was time to start closing this gap between academia and the real world, and they concluded that they were going to have to take the initiative to make this happen themselves.
    - Assembly of some of the brightest and most competent cryptographers and hackers from the Bay area, and got to work.
    - John Gilmore, an early Microsystems employee and cofounder of the digital rights group Electronic Frontier Foundation (EFF)
    - Had already been talking about bringing cryptography to the masses for some time within local hacker
    - Gathering a monthly event.
    - Hacker Jude Milhon, jokingly exclaimed: “You guys are just a bunch of cypherpunks!» 143
* The Cypherpunks
  + Early meetings outlined future goals,and formulated their strategies to realize these goals.
    - First and foremost, the Cypherpunks set out to prevent a dystopian future, future where digital communication can be monitored, analyzed and, } ultimately, abused.
    - Loss of privacy could empower despots and tyrants, at rave loss of individual liberty;
    - George Orwell’s Nineteen Eighty-Four was required reading for all
  + Weren’t just going to promote or even demand privacy. They would not limit themselves to lobbying elected officials, or otherwise work through the political and legal process, as some existing interest groups (like the EFF) were already doing.
    - To their strategy Cypherpunks were going to claim privacy themselves, 144
  + A Cypherpunk’s Manifesto,
    - Must come together and create systems which allow anonymous transactions to take place. People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. Technologies of the past did not allow for strong privacy, but electronic technologies do.
    - They were going to build these electronic technologies, distribute it as free software, and per the hacker ethic, they weren’t going to ask anyone permission to do sc
    - “Cypherpunks write code,” Hughes declared. “We know that someone to write software to defend privacy, and we’re Going to write it.” 145
* Mailing List
  + Monthly Cypherpunk meetings had an open character. Besides the core group of regular participants, curious newcomers would show up to a taste of what was going on.
    - To help coordinate this, Hughes set up an email list, hosted on Gilmore’s computer, where he announced upcoming events.
    - Mailing list quickly outpaced that of the actual Cypherpunk events.
  + Wired in May 1993 dedicated its cover story to the Cypherpunks
    - «Rebels with a Cause (Your Privacy)’ the cover read
    - Anyone with an interest in computers had now heard about the group of privacy activists, and its global reach, hundreds of people from all around the United States the rest of the world were flooding in to subscribe to their email list.
  + Cypherpunks were not an organization in the traditional sense.
    - Intentionally informal, unstructured, and open collective.
    - Anyone could become a Cypherpunk, but all Cypherpunks ultimately engaged as individuals. They were not tasked with responsibilities or subject to rules—nor could anyone hold others responsible for their own actions.
      * Still, action was encouraged.
      * It was up to them to take the initiative and see if others wanted to help.
    - Movement did not just work towards a different type of future. For May: it already represented that future. He
      * Open, permissionless, and nonhierarchical mode under which the Cypherpunks and their email list operated as a model for an upcoming crypto-anarchist society.
* Crypto-Anarchy
  + The Extropians would sometimes speculate about carving out areas of freedom to subvert, hide, or escape from state control over their lives.
    - Cities on big floating islands in the sea—seasteading-was the way to go. Others believed it might be possible to purchase a small island on which to found a libertarian society.
    - May didn’t really feel like moving. He had a better idea.
      * Connected the dots to see the disruptive potential of anonymous information markets, he’d begun envisioning a future that
        + He’d realized, could be made a reality.
  + “Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods ference in economic transactions.
  + Without forced redistribution of wealth, this future economy would self-organize around voluntary interaction free markets; spontaneous order would emerge through the internet.
* Code
  + Work towards a common goal regardless of their political affiliation: the goal of developing and distributing privacy tools.
  + The group had barely gotten started when Hughes developed an early version of the first-ever remailer, based on David Chaum’s mix network version
    - Hal Finney just started contributing to Phil Zimmermann’s PGP implementation
    - Wasn’t long before Finney rolled PGP into Hughes’s remailer code.
    - Just a few weeks after the first meeting, Cypherpunks had developed a fully functional remailer. And they would operate it, too. Finney and several other Cypherpunks took it on themselves to run the remailer programs, and distributed software and starter guides so others could join them.
* The Crypto Wars
  + Bill Clinton took office as the 42nd President of the United States in January 1993, his new administration was quick to share its concerns about potentially nefarious use of personal computers and the internet.
    - Law enforcement was going to require new tools in
    - Government was going to try to limit the use of cryptography
      * Protocols that used keys larger than 40 bits were classified as munitions within the definition of the Arms Export Control Act.
      * Sending or bringing a strong cryptosystem abroad required a license-the same type of license you’d need for international transport of firearms, ammunition, or explosives.
  + Clipper chip used pubkey cryptography to encrypt data, but the NSA had added a special decryption key to the protocol.
    - The plan was to have telecommunication companies like AT&T adopt the chipset, which would let users encrypt their phone calls. The telecom companies would hold on to a decryption key, however, which could be handed to the government on request. Such key escrow was needed for national security reasons, the Clinton administration insisted:
      * Authorities had to be able to listen in to the phone calls of potential and suspected terrorists.
    - Faced opposition from privacy advocates and civil liber interest groups across the country, including the (both Democrat and Republican)
  + “Our immediate goal must be to make sure the ‘genie is out of the bottle,’ that enough crypto tools and knowledge are widely disseminated so that such a government ban is futile.”156
* Successes
  + Cypherpunks were motivated and driven, but facing the full force of US government, few would have expected them to come out of the Wars as victors.
  + Even do what it was supposed to. Notable wins could be attributed to Matt Blaze, a Bell security researcher and regular on the Cypherpunks mailing list. In
    - Exposed a flaw in the chip’s design that would let users disable the special decryption key.
    - Suffering some reputational damage from the fierce opposition it faced, it now turned out that the Clipper Chip didn’t even do what it was supposed to.
  + Brad Huntting, had in 1994 came up came up with a clever idea to challenge export restrictions on such crypto protocols: to publish code in a physical format to demonstrate that bans on software distributions are in conflict with fundamental rights.
    - We need only show that encryption software = speech,”
    - Zimmermann published PGP: Source Code and Internals: he had printed the complete PGP source code in a book.
    - By freely and legally distributing in hardcover the exact same information that had made him subject to criminal investigation, Zimmermann highlighted the absurdity of crypto exports regulations.
      * US government dropped Zimmermann’s case in 1996.
  + American tech sector, and the by then already irreversibly widespread distribution of crypto protocols outside of the United States moved the Clinton administration to scrap commercial encryption from the Munitions List entirely

### Chapter 9: Cypherpunk Currency

* CYPHERPUNKS HAD SET out to defend privacy in the digital age, and they understood that the privacy offered by physical cash was at risk.
  + Posited electronic cash as something akin to the Cypherpunk’s holy grail.
* Chaum’s Compromise
* Privacy Hardliners
  + As long as any private payment solution existed anywhere in the world, the kidnappers would probably demand that the money is simply sent to them through that system instead . .. and some private payment and some private payment solution would likely always exist somewhere.
* Patents
* Alternatives
* The Experiments
  + Suggested that maybe this dollar redeemability t actually necessary. Perhaps, he mused, digital cash wouldn’t need be backed at all.
  + PrOduct Cypher concluded: “Your digicash should be scarce.”174
* Backing Digital Cash
* Adam Back
  + Shared a shortlist of six desirable properties for electronic cash 182.
    - 1. Anonymous (privacy preserving, payee and payer anonymous) +
    - 2. Distributed (to make it hard to shut down)
    - 3. Have some built in scarcity
    - 4. Require no trust of any one individual
    - 5. Preferably offline (difficult to do with pure software)
    - 6. Reusable
  + Properties were difficult enough to realize even in the most general computer science context, while integrating them into a digital currency scheme would almost certainly be significantly harder.
    - Didn’t just talk about regardless, in true He wrote code

### Chapter 10: Hashcash

* University of Exeter, in the southwest of England.
  + Distributed computing, where several computers connect through a network to collaborate on the same problem, typically by dividing the problem into smaller parts (“parallel computing”).
  + Long-standing challenges in distributed computing like the Byzantine Generals Problem,
    - Malicious (or even just unintentionally unreliable) nodes could join and frustrate the efforts of honest participants to reach a consensus.
* The Cypherpunk
* Taking Action
* Spam
* The First Electronic Postage
* Hashcash
  + Described as “hashcash”: a “partial hash collision based postage scheme.
  + A postage solution for email.
  + To generate hashcash, a user had to generate a hash out of an e-mail’s metadata (the sender’s address, the recipient’s address, the time, etc.) a random number-a nonce.
* Digital Scarcity
  + Hashcash’s key innovation was that it tied purely digital data (numbers, essentially) to real resources in physical reality.
    - Producing proof of work required computing cycles, and computing cycles themselves use up electricity, which in turn costs energy to produce.
  + Fundamental scarcity of energy in physical reality into the digital realm.
  + The main problem was that hashcash wasn’t reusable. Each currency unit was custom made to fit with a specific email, so it couldn’t be re-spent elsewhere, and was of no further benefit to recipients.
    - One of his first suggestions was, for example, a Chaumian system where bank would issue electronic cash upon receipt of hashcash: use
    - Would create proof of work and get unbacked digital cash in return.
    - Would be anonymous, reusable, and somewhat scarce- though this would admittedly be rather weak in practice as people could always create more proof of work if they wanted to.
      * With computer processors getting more powerful each year, producing valid proof of work would become cheaper and cheaper over time.
    - The entity that issues the digital currency and prevents double-spending, would itself need to be trusted to not erroneously enrich itself.
      * Perhaps you could have multiple banks and let reputation sort them out, if you could arrange the protocols so that it would be apparent if a bank was minting more cash than it had received hash collisions for. [.. 2]
      * “It would be nice to have something which required no trust and which had no possibility [sic] of cheating rather than relying on reputation to sort them out.

### Chapter 11: Bit Gold

* NICK SZABO’S FATHER was on o 200,000 Hungarians to have fled their | Country after Soviet troops crushed the anti-communist revolt of 1956.
  + He’d decided to leave everything behind, and eventually found a new home all the way across the Atlantic, in the land of the free.
    - Happened almost a decade before he was born, his father’s experience would shape Nick. As the son of a refugee, growing up from the oppressive Soviet stronghold over Eastern Europe, the second-generation American boy was instilled early on with a deep distrust of anything that even resembles communism or government overreach. 198
  + Found a great source of inspiration in the works of Fried - | Hayek. The Road to Serfdom seemed to have quite accurately described how the Soviet Union morphed into a totalitarian state,
    - And Szabo would later name Hayek’s 1988 book The fatal conceit as one of the most important books he ever read. 199
  + Finding an interest in computers which, perhaps fittingly, was a relatively new technology that was rapidly developing in the US and che rest of the Western world, while the communist lagged far behind.
* The Crypto-Anarchist
* Smart Contracts
  + It was not immediately clear how two people could trade this data without counterparty risk.
    - One party in the trade would always have to send their data or otherwise finalize their part of the deal first, at which point their counterparty could disappear and default on its obligation.
      * - In cyberspace, there were no courts or police to enforce contract law.
  + Proposed smart contracts-digital contracts Szabo proposed that would autonomously enforce their own terms, as embedded in computer code 201
  + O believed: “Protocols based on mathematics, called cryptographic proare the basic building blocks that implement the improved tradeoffs between observability; verifiability, privity; and enforceability in smart contracts,” he wrote, 202
    - Me risks remained if there were too many unreliable participants—he believed that robust enough protocols had been designed for most scenarios.
      * Economic incentives, protect the performance of the contract from both by the principals and attack from third parties, “203
* Trusted Third Parties
  + Szabo found that protocol developers had a tendency to assume away a particular type of risk-the risk inherent to relying on a trusted third party (TTP).
    - Typical example is a certificate authority that provides a registry of real-world identities coupled with their public keys.
    - Szabo later explained that TTPs were often not included in the cost of a design, and why he believed this to be a mistake. Trusted third parties security holes, the Cypherpunk argued, even if they are themselves truly honest: they could become hot targets for malicious hackers, or perhaps even for nation-states and their regulatory bodies during times of political instability or oppression.
    - “The best ‘TTP’ of all is one that does not exist, but the necessity for which has been eliminated by the protocol design, or which has been automated and distributed amongst the parties to a protocol,”
* Free Banking
  + Cypherpunks were for the most part interested in electronic cash because of the privacy features it could offer.
  + Especially interested in Hayek’s ideas around free banking, as also outlined bY Max More in the digital cash edition of Extropy
    - Szabo had studied the work of George Selgin-whose book The Theory of Free Banking had been reviewed in that same magazine-and that of Selgin’s colleague Lawrence H. White,
  + Mid-1990s, he therefore decided to create a new, more topic-dedicated mailing list: the Libtech list.
    - Free bankers like Selgin and White as well as interested Extropians and Cypherpunks had targeted discussions about banking, monetary economics, and-most importantly-digital currency designs. 206
  + Central banks were TTPs.
  + They’d have to design a trust-minimized form of electronic money from the ground up
    - In the same for cyberspace had to be reinvented from scratch, so too would a digital currency have to be created by starting from first principles.
* The Origins of Money
  + To create money, Szabo had to understand it first.
  + Aware of Carl Menger’s and Ludwig von Mises’s accounts on the origin of money, and to a large extent shared their assessment that money stemmed from barter.
    - Szabo went looking for actual historical records, and even archeological remnants.
      * Deep into human prehistory, and to preindustrial civilizations like that of Native Americans. Moneys he found, was even older than text: early forms of currency were already used by hunter-gatherer tribes.
      * Ultimately led him to hypothesize that money is quite literally as old as mankind itself. As first speculated by evolutionary biologist Richard Dawkins in his seminal work The Selfish Gene, 208
        + Ability to use money could well be embedded in human DNA, and might have benefited the survival of the species.
  + His later essay “Shelling Out: The Origins of Money,” 209 Szabo would nis later essay
    - Altruistic behavior could benefit everyone as long as all tribe members knew each other, and could roughly keep track of each othcontributions; all tribe members had a public reputation. Becau
    - Human brains can only maintain a limited number of social relationships (popularly known as “Dunbar’s number, which is 150
      * To avoid being taken advantage of, it would even become rational for each individual to stop sharing and become a freeloader themselves-even though everyone would be better off if everyone shared. In other words,
        + Something of a grand prisoners dilemma?’ would emerge.
        + Type of question an evolutionary biologist would ask. Why did people evolve to enjoy wearing ornaments?
  + Instead of remembering who shared their resources jewelry served as proto-money, and facilitated what evolutionary psychologists call reciprocal altruism.
* Proto-Money
  + Necklaces are probably the best example in this regard: they are almost impossible to lose if worn around the neck.
  + Second, the collectibles represented unforgeable scarcity.
    - Costly to create or hard to ind: a mammoth tooth was scarce
* Bit Gold
* The Registry
* Controlling Inflation

### Chapter 12: B-money (and BitTorrent)

* SHORTLY AFTER BIT GOLD had shown how proof of work might be converted into transferable electronic cash, a somewhat similar digital currency proposal was submitted to the Cypherpunks mailing list. Its
  + Author, Wei Dai, was well known within the Cypherpunk community though only by name.
  + Had as a student developed an interest for cryptography because believed that it could help protect humanity against future entities like Blight, artificial superintelligence that served as the main antagonist in Vernor Vinge’s novel A Fire Upon the Deep. 221
  + 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 community where the threat of violence is impotent Ullaus 17016 linked to their true names or physical locations.
    - A step toward making crypto-anarchy a practical as well as theoretical possibility.”224
* B-money
  + Trust-minimization was essential. Trusted third parties are security holes.
  + Instead of a central entity, all users of the system would maintain individual copies central
    - Suggested a way to keep the servers honest.
    - Bit Gold had not quite provided a solution to settle disputes between servers, b-money hadn’t done so either.
* B-money’s Monetary Policy
  + I ike Bit Gold, b-money would be a purely digital currency. There’d be no bank or company backing the digital units with dollars or gold, ultimately no guarantee that anyone would accept the currency for payment.
    - Like Szabo, Dai did not think this would be a problem.
    - “Think about it this way,” he argued on the Cypherpunks mailing list. “In the case of commodity money, its value comes partly from the industrial/ aesthetic value of the commodity and partly from the usefulness of the commodity money as a medium of exchange.
      * The usefulness of the and b-money, all of its value comes from its usefulness as a medium of exchange.
      * Dai wanted to embed his currency with a targeted monetary policy. Whereas the purchasing power of Bit Gold would have to be decided on the marker, with valid proof-of-work hashes freely trading for whatever buyers and sellers were willing to settle on,
      * Proposal offered a raw outline of what an electronic cash system could look like, but several problems remained to be solved before could function as an actual digital currency
        + Dai himself, however, decided that he wasn’t going to be the one
* Disillusionment
* Zero-Knowledge Systems
* Mojo Nation
* Mojo
* BitTorrent
  + Wilcox, for example, decided fork (copy) the Mojo Nation code to release a version of the protocol called Mnet, while another Autonomous Zone Industries employee and cypherpunk, the twenty-eight-year-old software developer Bram Cohen, released his own Mojo Nation-inspired file sharing solution.
  + From a legal perspective. For the Gest time this Made the users them From a legal perspective, for the first time this made u (SMTP), or even the internet itself (IP), BitTorrent was essentially just internet protocol, and Cohen was in no way liable for how people used it
    - Internet protocol, and Cohen was in no way AUMA ་ used illegally over BitTorrent on a large scale.
  + Whereas Wei Dai, Eric Hughes, and other Cypherpunks thought that electronic cash and other crypto tools could only succeed if public awareness about the importance of online privacy increased, BitTorrent would Years later demonstrate that it could work both ways: a powerful enough technology could, itself, help change the prevailing culture. V

### Chapter 13: RPOW

* BY THE EARLY 2000s, the Cypherpunk movement had lost most of its momentum,
  + Sion hub degraded, with many new sus
  + Mode ration policy, this was starkly rejected by the likes of iTirm May; who in response unsubscribed 242
    - (May returned when the policy was tweaked to redirect rather than censor flames and other low-quality
  + September 11, 2001, a sharp increase in digital surveillance made people more hesitant to facilitate discussions about radical privacy tools,
    - The only remaining Cypherpunks server was hosted from the web address al-qaeda.net,evea TL m May decided it was time to leave.
* Didn’t mean the Cypherpunk ethos was lost or forgotten completely;
  + Tools like pGI3 as well as new technologies such as Tor (The Onion
* Dystopian future that Chaum and many of the Cypherpunks had | warned about, a future where all financial transactions can be monitored, recorded, and potentially censored, was quickly becoming reality.
  + Not everyone was ready to give up hope. ..
* Hal Finney
* Cypherpunk Realism
* Electronic Cash
* Reusable Proofs of Work
* Trusted Computing
* Fate of RPOW
* E-gold

## PART III: BITCOIN

### Chapter 14: Twenty-First Century Fiat

* For Most oF his life, Friedrich Hayek found that his ideas had been marginalized. Bottom-up spontaneous order had to take a backseat to John Maynard Keynes’s top-down state intervention in the economy.
  + Central banks had abandoned gold to make interest rates manipulation even easier.
  + Trust in the dollar was indling now that it was no longer backed by precious metal, and it started to look like the United States could lose its dominant position in international financial system.
    - Nixon would find a solution against the backdrop of a worldwide oil crisis.
    - 1973, oil-producing Arab nations, united in the multi-governmental Organization of the Petroleum Exporting Countries (OPEC)
      * Oil embargo on countries that supported Israel during the October War between the Jewish state and Egypt. Amo
        + Embargoed nations were the US, the UK, and many other Western nations. It
        + It caused a surge in the price of oil, with far-reaching negative effects on the entire world economy.
  + The unofficial arrangement would come to be known as the petrodollar system. (Soon after this arrangement was established, on December 30, 1974, private gold ownership was once again legalized in the United States.)

### Chapter 15: The White Paper Chapter 16: The Release

### Acknowledgments About the Author Endnotes