1. Blockchain: from ideology to implementation

1 BLOCKCHAIN THROUGH THE AGES

Blockchain is a relatively new technology,¹ whose origins are to be found in the so-called “cypherpunk” movement that grew out of an old van in California in the 1960s. Understanding the ideology behind blockchain is a requirement for anyone wanting to apply the law without hindering the technology. I invite you to embark on this journey with me.

1.1 Blockchain’s Premises… in a Van

“Don’t mourn, organize.”²

The setting: California, 1968. Stewart Brand and his wife, Lois Jennings, go on a road trip across America.³ They plan on going to educational fairs with a truck full of tools and equipment – such as for “drilling a well, or grinding flour.”⁴ They also carry a small library of books written by Robert Heinlein, the dean of twentieth century science fiction. They have a lot of unique items for sale, so Brand quickly initiates the creation of a catalog to help potential buyers find their way around the inventory. A few weeks after returning from their road trip, he opens a shop in Menlo Park, not far from San Francisco. The hippie youth are riding on the 1967 “Summer of Love” euphoria. Brand quickly becomes one of their gurus. He is about to initiate the “do it yourself” (DIY) culture.

Brand’s store is a significant success. More products are added and the catalog expands. In Fall 1968, the Portola Institute (an education nonprofit in Menlo Park) gives Brand the platform to spread his message. Together, they publish the first official issue of the Whole Earth Catalog. The magazine’s name comes from a campaign Brand ran in 1966, when he publicly asked NASA to publish the first image ever taken of the “Whole Earth.” The magazine’s aim is that “anyone on Earth can pick up a telephone and find out the complete information on anything.” In 1969, the fall issue of the catalog specifies:

We are as gods and might as well get good at it. So far, remotely done power and glory—as via government, big business, formal education, church—has succeeded to the point where gross defects obscure actual gains. In response to this dilemma and to these gains a realm of intimate, personal power is developing—power of the individual to conduct his own education, find his own inspiration, shape his own environment, and share his adventure with whoever is interested. Tools that aid this process are sought and promoted by the WHOLE EARTH CATALOG.

The Whole Earth Catalog rapidly gains popularity, with more than 1 million copies printed in just a few months. It promotes a new social order empowering the individual—letting him “conduct his own education, find his own inspiration, shape his own environment, and share his adventure with whoever is interested,” after acquiring the right tools. Publication ceases in 1972, but Brand’s influence continues to grow. Steve Jobs will call it “one of the bibles of [a] generation,” but Brand is already aiming toward cyberspace. He is about to create the “internet before the internet.”

In 1984, Brand publishes the first issue of the Whole Earth Software Catalog and Review. That is when he first writes about “[c]omputers and their

---

9 Id.
programs,” with the ambition of opposing centralized forms of production. He also creates The Whole Earth 'Lectronic Link (The WELL) in 1985, a mailing list still in operation to this day. In 1989, he further starts The Electronic Whole Earth Catalog, which is distributed on CD-ROM. Brand

12 Stewart Brand, Whole Earth Software Catalog (Quantum Press/Doubleday, 1984); for more on that, see Fred Turner, From Counterculture to Cybersculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism (University of Chicago Press, 2006).

hails computers as one of the tools of personal liberation. Years later, a technology writer for the *New York Times* describes him as “the first person to understand cyberspace.” Brand not only coins the term “personal computer”\(^\text{14}\) and the phrase “information wants to be free,”\(^\text{15}\) but also contributes to the emergence of the Web 2.0.\(^\text{16}\)

Brand’s influence is still visible to this day. TED’s curator confides that Brand has been his “intellectual hero”\(^\text{17}\) for numerous years. Kevin Kelly – the creator of *Wired* magazine, known for his support of early cyber-libertarian communities – has said the Whole Earth Catalog inspired the genesis of his magazine.\(^\text{18}\) And Jeff Bezos has donated $42 million to a project by the Long Now Foundation, of which Brand is the president.\(^\text{19}\)

Not surprisingly, Brand is regularly on the side of blockchain communities or quoted by them. In November 2018, he took part in a conference organized in Prague by the Ethereum Foundation.\(^\text{20}\) The DIY culture he has helped to flourish is that of the blockchain communities which are developing infrastructures outside of government circuits. Brand wants every individual to access emancipating tools. Blockchain communities want to emancipate themselves from current transactional methods; this explains why they draw inspiration from Brand. In that sense, his influence is very much visible, even if it is only indirect (i.e., does not directly concern blockchain architectural choices). He contributed to the decentralized philosophy of Web 2.0; while blockchain communities want to implement this into Web 3.0.


\(^{18}\) *Id.*


1.2 The Cypherpunks are Not Coming to Get You

Satoshi Nakamoto first introduced blockchain in his article “Bitcoin: A Peer-to-Peer Electronic Cash System” published on October 31, 2008.21 It resulted from decades of research strongly dominated by a cyber-libertarian ideology, finding its roots in the Whole Earth Catalog.23 More specifically, blockchain can be traced back to the work of the cypherpunks: cyber-libertarians writing code.24

In the 1970s, for the first time, cryptographic methods became accessible to civilians.25 For example, Rivest, Shamir and Adleman showed how two persons could use public–private key encryption and digital signatures to ensure communication integrity.26 In 1982, David Chaum, an American com-
A Timeline of Cyberlibertarianism

Focus on the defining events

- **1970s**: Cryptography becomes available to civilians.
- **1982**: David Chaum introduces a first privacy-preserving protocol.
- **1983**: Publication of "Technologies of Freedom" by líthel de Sola Pool.
- **1985**: Publication of the GNU Manifesto (creating the Free Software Movement) & David Chaum introduces anonymous digital cash.
- **1988**: Timothy May publishes "The Crypto Anarchist Manifesto".
- **1990**: John Gilmore, John Perry Barlow and Mitch Kapor create the Electronic Frontier Foundation.
- **1991**: Linus Torvalds creates Linux & the Pretty Good Privacy encryption program is introduced.
- **1992**: Eric Hughes, Timothy May and John Gilmore found a group in the San Francisco Bay Area.
- **1993**: Eric Hughes published "A Cypherpunk’s Manifesto".
- **1994**: Esther Dyson, George Gilder, George Kayworth, and Alex Tofler publish a "Magna Carta for the Knowledge Age".
- **1995**: Richard Barbrook and Andy Cameron formulate "The Californian ideology".
- **1996**: John Perry Barlow published "A Declaration of the Independence of Cyberspace".
- **1997**: Peter Huber publishes "Law and Disorder in Cyberspace".
- **1998**: Wei Dai introduces the B-money BNick Szabo introduces the Bit gold.
- **2008**: Satoshi Nakamoto published "Bitcoin: A Peer-to-Peer Electronic Cash System".
- **2015**: Vitalik Buterin launches the Ethereum.

Figure 1.2 A timeline of cyberlibertarianism
puter scientist, published his thesis which he had written at the University of Berkeley. Entitled “Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups,”27 it introduced a new protocol that harnessed cryptographic tools to protect private information.28

A year after, in 1983, Ithiel de Sola Pool – then a professor at Massachusetts Institute of Technology (MIT) – published a book entitled Technologies of Freedom,29 in which he analyzed the impact of several technologies on free speech and freedom of the press. The objective was clearly stated: technology and freedom go hand in hand. Two years later, David Chaum published “Security without Identification: Transaction Systems to Make Big Brother Obsolete,” an article in which he introduced anonymous digital cash.30 Here again, freedom was mainly intended as freedom from the government. In the same vein, the GNU Manifesto was introduced the same year, starting the Free Software Movement. It argued that: “[T]here is no intrinsic right to intellectual property. The kinds of supposed intellectual property rights that the government recognizes were created by specific acts of legislation for specific purposes.”31 It was deeply libertarian.

A few years later, in 1988, Timothy May published “The Crypto Anarchist Manifesto” in which he called for further action.32 It read:

Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. ... The methods are based upon public-key encryption, zero-knowledge interactive proof systems, and various software protocols for interaction, authentication, and verification. ... But only recently have computer networks and personal computers attained sufficient speed to make the ideas practically realizable.

---

... The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be traded freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy. ... Arise, you have nothing to lose but your barbed wire fences!

In his signature, Timothy May linked “Crypto Anarchy” to the “collapse of governments.” His manifesto would be quoted several thousand times. Two years later, in April 1990, the Federal Bureau of Investigation questioned John Perry Barlow (lyricist of the Grateful Dead) about stealing and distributing the code of Macintosh ROMs. He recounted his experience on The WELL (the newsletter created by Brand) and obtained financial support from John Gilmore and Steve Wozniak (Apple’s co-creator). The idea of the Electronic Frontier Foundation was born. And in July of the same year, Gilmore, Barlow and Mitch Kapor created the Electronic Frontier Foundation. They aimed to provide legal and financial support to people that were subjected to unfounded legal threats regarding internet civil liberties.

Then came Linux in 1991 as one of the first major concrete outputs accessible to the public. Linus Torvalds released the operating system’s kernel under a GNU General Public License. Linux was perfectly in line with the 1985 GNU Manifesto. And Phil Zimmerman’s encryption program, Pretty Good Privacy, was also made freely available in 1991. Things started to become more concrete. The following year, Eric Hughes, May and Gilmore formed a group and agreed to meet every month at Gilmore’s company premises in the San Francisco Bay Area. Jude Milhon, an American hacker also known as St. Jude, attended one of the first meetings.33 She described the group as being “cypherpunks,” derived from “cipher” and “cyberpunk.” Hughes reused the term in 1993 in his “Cypherpunk’s Manifesto.”34 It read:

Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn’t want the whole world to know, but a secret matter is something one doesn’t want anybody to know. Privacy is the power to selectively reveal oneself to the world. ...

We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence. It is to their advantage to speak of us, and we should expect that they will speak. To try to prevent their speech is to fight against the realities of information. Information does not just want to be free, it longs to be free. Information expands to fill the available storage space. …

We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money. Cypherpunks write code. We know that someone has to write software to defend privacy, and since we can’t get privacy unless we all do, we’re going to write it. We publish our code so that our fellow Cypherpunks may practice and play with it. Our code is free for all to use, worldwide. We don’t much care if you don’t approve of the software we write. We know that software can’t be destroyed and that a widely dispersed system can’t be shut down.

Cypherpunks deplore regulations on cryptography, for encryption is fundamentally a private act. The act of encryption, in fact, removes information from the public realm. Even laws against cryptography reach only so far as a nation’s border and the arm of its violence. Cryptography will ineluctably spread over the whole globe, and with it the anonymous transactions systems that it makes possible.

Importantly, and perhaps more aggressively, Esther Dyson, George Gilder, George Keyworth and Alvin Toffler published “A Magna Carta for the Knowledge Age” in 1994. The authors quoted the “libertarian icon” Ayn Rand and pointed out that cyberspace:

spells the death of the central institutional paradigm of modern life, the bureaucratic organization. (Governments, including the American government, are the last great redoubt of bureaucratic power on the face of the planet, and for them the coming change will be profound and probably traumatic.)

From these writings came “The Californian Ideology,” introduced a year later by Richard Barbrook and Andy Cameron. It was arguably better embedded
in Silicon Valley’s free-market technology mindset. And in 1996, John Perry Barlow published “A Declaration of the Independence of Cyberspace.” He argued as follows:

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.

You have not engaged in our great and gathering conversation, nor did you create the wealth of our marketplaces. You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions.

You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don’t exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.

Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.

We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth. We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here. Our identities

Also, see Richard Barbrook and Andy Cameron, “The Californian Ideology”, in Crypto Anarchy, Cyberstates, and Pirate Utopias, ed. Peter Ludlow (The MIT Press, 2001): 363 (describing the “Californian ideology” as a “bizarre fusion of the culture bohemianism of San Francisco with the high-tech industries of Silicon Valley”).

have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge. Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose. …

We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before.

In the wake of the Declaration, Peter Huber, a Harvard and MIT graduate, published *Law and Disorder in Cyberspace* in 1997. The book – whose subtitle read: “Abolish the FCC and Let Common Law Rule the Telecosm” – was making a more technical point, namely defending the abolition of the Federal Communications Commission in favor of common law.

Finally, a year later, in 1998, Wei Dai and Nick Szabo both introduced models of cryptographic coins – B-money and Bit gold, respectively – which were very similar to what Bitcoin would become. These two digital currencies thus brought two decades of ideological and cryptographic research to fruition, building on top of the research mentioned in this section. The blockchain ecosystem has continued to flourish since then, but the core ideology remains the same – at least for now. This ideological tradition has technical implications that I will explain in Chapter 2. In turn, these technological underpinnings have important ramifications for economic policy and regulation.

---

2 TODAY’S COMMUNITY: ANOTHER VAN STORY

The blockchain community is growing exponentially. Despite this, the majority of its members remain true to the main ideology of Brand’s era. A specific episode of crisis management reminds us of this vividly.

2.1 One Big Community?

Another setting: 17 September 2018, seaside (the location remains a secret).

“Awemany” wakes up in his van (yes, a van, again!). He is part of the Bitcoin Unlimited team, a full-node implementation for the Bitcoin and Bitcoin Cash networks. That morning, he wants to work on implementing the “Checkdatasig/-Verify opcodes” that his team intends to activate on the Bitcoin Cash network in November. Around noon, he stumbles upon a problem in the way code counts signature operations in Bitcoin ABC, a full-node implementation of the Bitcoin Cash protocol. Awemany performs additional tests and writes a note to himself: “BitcoinABC does not check for duplicate inputs when processing a block, only when inserting a transaction into the mempool.” He adds: “This is dangerous as blocks can be generated with duplicate transactions and then sent through, e.g., compact block missing transactions and avoid hitting the mempool, creating money out of thin air.” The stakes are high. Awemany may have put his finger on “the most catastrophic bug in recent years, and certainly one of the most catastrophic bugs in Bitcoin ever.”

The Bitcoin blockchain could validate a block with double spending, which would put its entire integrity at risk.

A few minutes have passed. Awemany’s tests are now complete. The problem seems to come from Bitcoin Core, the developers in charge of proposing changes to the Bitcoin “constitutional” code. Instead of taking advantage of the bug, or revealing it publicly in a forum to jeopardize Bitcoin, Awemany alerts five Bitcoin Core developers. He does so despite the fact that he works mainly on Bitcoin Cash, a fork of the original Bitcoin (more on this later). Both communities are constantly taunting each other on social networks (Reddit, Twitter…). They are in competition, yes; but Awemany wants fair competition. “Let’s continue competing. Let’s civilly inform each other of bugs. Maybe

---

43 Double spending occurs when a Bitcoin user spends the same token twice. It puts the blockchain integrity, and usefulness, at risk.
the best chain win,” he will say later on. Oh… and he also owns a few Bitcoins, which may help. By 2:57 p.m., Pieter Wuille, Greg Maxwell and Wladimir Van Der Laan of Bitcoin Core, deadalnix of Bitcoin ABC and sickpig of Bitcoin Unlimited are made aware of the problem. Awemany has included his Bitcoin address in his email to them, hoping for “a little performance bonus.” Eighteen minutes later, Greg Maxwell shares the report sent by Awemany to Cory Fields, Suhas Daftuar, Alex Morcos and Matt Corallo, four Bitcoin Core developers. At 5:47 p.m., Matt Corallo “officially” identifies two issues: a denial of service (DoS), as identified by Awemany; and a “critical inflation vulnerability.” He has identified a way to duplicate one Bitcoin infinitely on top of the double-spending issue, going beyond an initial cap of 21 million mined Bitcoins.

Luckily, both problems have “the same root cause and fix.” A little more than an hour later, a patch is created. It now needs to be deployed on the Bitcoin blockchain; but, as we will see later, the Bitcoin Core team doesn’t have the power to unilaterally impose such a change (unlike how Apple can impose a minor update on its iPhone). For that reason, Matt tries to get in touch with Slushpool’s chief executive officer to ask him to apply the patch without further delay. Slushpool is “the world’s first Bitcoin mining pool,” and has over 180,000 active workers on the Bitcoin blockchain, giving it significant sway over the network’s development. Matt finally reaches him at 8:30 p.m. The update is implemented at 8:48 p.m.

2.2 Crisis Management … and Collusion?

Let’s explore how this crisis was handled. Just after 9:00 p.m., an alert was sent to Bitcoin ABC that a patch would be posted publicly around 10:00 p.m. For the first time, all the blockchain participants were informed of the issue; but rather than revealing the two vulnerabilities, the choice was made to mention only the most minor part: the DoS bug. When the message was finally sent

---

44 Awemany, “600 Microseconds,” Medium, September 22, 2018, https://perma.cc/T478-2LCB (“[U]nfortunately [I] still own a (for my poor soul significant) amount of BTC and for that reason and others do not like having bugs in Core either.”)
at 9:47 p.m., the critical inflation vulnerability was omitted. Bitcoin Core explained:

In order to encourage rapid upgrades, the decision was made to immediately patch and disclose the less serious Denial of Service vulnerability, concurrently with reaching out to miners, businesses, and other affected systems while delaying publication of the full issue to give times for systems to upgrade.48

The next day, on September 18, 2018, one participant posted banners on Bitcointalk and Reddit, “urging people to upgrade.” The day after, the Bitcoin Core mailing list distributed “an additional message urging people to upgrade.” Bitcoin Optech did the same, prompting users to “[u]pgrade to Bitcoin Core 0.16.3 to fix denial-of-service vulnerability.”49 It was not until September 20, 2018 that David Jaenson, a Qtum developer, discovered that the patch addressed not one but two problems – the DoS vulnerability and the critical inflation vulnerability. At that point,50 the Bitcoin Core team could no longer deny the truth: it was primordial that a majority of Bitcoin miners update their software to prevent the exploitation of the vulnerability. At the same time, they were also trying to determine whether some had already exploited this glitch. After all, it had been there for 18 months.51

Fortunately, the answer seemed to be negative. Nevertheless, the community was very keen to ensure that all miners had implemented the patch. Someone posted a new message on Reddit: “New info escalates importance: upgrading to 0.16.3 is REQUIRED.”52 It said: “You should not run any version of Bitcoin Core other than 0.16.3. Older versions should not exist on the network. If you know anyone who is running an older version, tell them to upgrade it ASAP.” The danger was indeed that, should two versions of the software run concomitantly, the blockchain would split. Putting them back together would have caused all the transactions validated under the old software to be lost.53 Once

52 Thymos, “New info escalates importance: upgrading to 0.16.3 is REQUIRED,” Reddit, www.reddit.com/r/Bitcoin/comments/9hko06/new_info_escalates_importance_upgrading_to_0163/.
again, network integrity was at risk; and once again, things luckily turned out fine.

A few days later, Bitcoin subreddit moderator Theymos minimized the event: “Even if the bug had been exploited to its full extent, the theoretical damage to stored funds would have been rolled back.” Bitcoin Core’s Pieter Wuille made the same point. Still, the worst had been avoided thanks to Awemany. The community hoped that he “and other Bitcoin developers, despite disagreements and some squabbles, will continue this practice.” Nothing could be less certain. Oversights that resulted from an overflow of confidence – probably a “young, cocky Core developer, a new ‘master of the universe’ wreaking havoc by sheer arrogance and hubris” – may have compromised the entire Bitcoin blockchain.

Ultimately, this story reveals a key weakness of decentralized systems where tasks are not always clearly defined. However, some would say that the same weakness is also a strength, pushing each member of the community to verify others’ work. It results from the original Stewart Brand ideology: empowering individuals, without asking institutions or governments for help. The blockchain community, for now, has handled this responsibility well. It responded quickly to challenges and activated the right defense mechanisms. This is no small feat; after all, “moments of crisis uncover where actual power lies in a system.”

3 CHAPTER SUMMARY AND BEYOND

In this first chapter, I have shown that blockchain’s ideological roots emerged in Stewart Brand’s van, in California during the 1960s. By making individual empowerment the center of his modern philosophy and providing the correct tools to achieve it, Brand started a powerful movement throughout the United States. It helped the DIY culture emerge to empower all individuals.

Later on, the cypherpunks made cryptography the newest means of empowerment, intending to free the people from the coercive state. Combining a strong ideological ambition with technical advances, the cypherpunks built the technological foundations of blockchain.

One finds these libertarian roots in blockchain, as the Bitcoin incident I describe above illustrates. Owing to the dangers that such an approach entails

by relying (too) heavily on good faith, part of the community may eventually move away from individual empowerment. Several blockchains will soon transfer power to (more) centralized organs and entities, despite its DNA, which I discuss in the coming chapter.