

Nine Pages That Changed Money

A Short History of Bitcoin, from the Cypherpunks to the Hundred-Thousand-Dollar Coin

Biscuit Research

October 2026

Abstract

On 31 October 2008, an unknown author calling themselves Satoshi Nakamoto sent a nine-page paper to a small mailing list of cryptography enthusiasts. Barely anyone paid attention. Seventeen years later, the system it described was worth more than two trillion dollars, was held by national governments, and traded on Wall Street. This paper tells that story for readers with no technical background. We meet the dreamers who tried to build digital cash before Bitcoin, follow the first years of the network, from a pizza bought for ten thousand coins to the disappearance of its creator, and trace its stormy path to the mainstream. Along the way we explain, with nothing more than school arithmetic, three of Bitcoin’s cleverest ideas: why there will never be more than 21 million coins, why mining is a lottery, and why rewriting the past is practically impossible.

Contents

1	Introduction: Why Was Digital Money So Hard?	2
2	Before Bitcoin: The Dream of Digital Cash	2
3	2008: A Crisis and a White Paper	3
4	How Bitcoin Works, in Plain Words	3
4.1	A shared notebook: the blockchain	3
4.2	Who writes the next page? Mining as a lottery	4
4.3	Why it is so hard to rewrite the past	4
5	The Early Days (2009–2010)	5
6	The Vanishing Creator	6
7	Growing Pains (2011–2014)	6
8	The 21 Million: Bitcoin’s Built-in Scarcity	7
9	Civil Wars and Upgrades (2015–2021)	8
10	Bitcoin Goes Mainstream (2021–2025)	8
11	Conclusion	9
	Further Reading	10

1 Introduction: Why Was Digital Money So Hard?

Money has taken many forms: shells, salt, gold coins, paper notes, and numbers in a bank's computer. When the Internet arrived, an obvious question followed: *could we have cash that lives on the Internet?* Not a bank account, which someone else controls, but something like a banknote: yours, that you can hand to anyone, without asking permission.

The difficulty is surprisingly simple. Anything digital can be *copied*. If I send you a photo, I still have the photo. If a digital coin were just a file, I could pay you with it and then pay someone else with the very same file. This is called the *double-spending problem*, and for decades it seemed to have only one solution: a trusted middleman, such as a bank or PayPal, who keeps the official record of who owns what.

The double-spending problem. Digital money must prevent the same coin from being spent twice. Before Bitcoin, the only known way to do this was to trust a central authority to keep the books. Bitcoin's breakthrough was to let *thousands of strangers* keep the same books together, with no one in charge.

This paper tells how that breakthrough happened, who made it possible, and what became of it.

2 Before Bitcoin: The Dream of Digital Cash

Bitcoin did not appear out of nowhere. It stands on the shoulders of two decades of attempts, most of which failed.

David Chaum and DigiCash (1980s–1990s). The American cryptographer David Chaum was the first to take digital cash seriously. In 1982 he invented “blind signatures,” a mathematical trick that allowed a bank to approve a digital coin without seeing who would spend it, much like signing an envelope without opening it. In 1989 he founded the company DigiCash in Amsterdam. Its technology was brilliant, but it still depended on banks, and too few of them signed up. DigiCash went bankrupt in 1998.

The Cypherpunks (1992). In 1992, Eric Hughes, Timothy May, and John Gilmore started a mailing list for people who believed that cryptography could protect personal freedom against both governments and corporations. They called themselves *cypherpunks*. Their motto, from Hughes's 1993 manifesto, was that cypherpunks write code: rather than asking for privacy, they would build it. Many of the names in the rest of this story passed through that list.

Hashcash (1997). The British cryptographer Adam Back wanted to fight e-mail spam. His idea, *Hashcash*, forced the sender of every e-mail to solve a small computational puzzle first. For a normal person sending a few e-mails, the cost was negligible; for a spammer sending millions, it became expensive. This idea of proving you have spent effort, now called *proof of work*, became the engine of Bitcoin.

b-money and Bit Gold (1998–2005). In 1998 the computer engineer Wei Dai described *b-money*, a system in which every participant keeps a copy of the accounts. Around the same time, the legal scholar and computer scientist Nick Szabo designed *Bit Gold*, in which proof-of-work puzzles would be “mined” like gold and chained one after another. Neither system was ever built, but together they contained most of the ingredients of Bitcoin.

RPOW (2004). Hal Finney, a veteran programmer and cypherpunk, built *Reusable Proofs of Work*, which let a piece of proof of work be passed from person to person like a token. It worked, but relied on a central server.

Did you know? The Bitcoin white paper cites both Adam Back’s Hashcash and Wei Dai’s b-money. Before publishing, Satoshi Nakamoto e-mailed both men. Bitcoin was less a sudden invention than the final piece of a puzzle that many people had been working on.

3 2008: A Crisis and a White Paper

The financial crisis. On 15 September 2008, the American investment bank Lehman Brothers collapsed. Within weeks, the global financial system was in panic. Governments spent hundreds of billions of public money rescuing banks that had taken reckless risks. For many people, this was proof that the system depended on institutions that did not deserve the trust placed in them.

The white paper. A few weeks earlier, on 18 August 2008, someone had quietly registered the domain name `bitcoin.org`. Then, on 31 October 2008, a message arrived on a cryptography mailing list from one “Satoshi Nakamoto.” It announced a new electronic cash system that was fully peer-to-peer, with no trusted third party, and linked to a nine-page paper:

Bitcoin: A Peer-to-Peer Electronic Cash System.

The paper is short, clear, and contains almost no new mathematics. Its genius was in how it combined existing ideas. The first reactions were sceptical: experienced cryptographers doubted it could ever handle enough transactions, or that anyone would bother to run it. Satoshi answered every objection patiently.

4 How Bitcoin Works, in Plain Words

Before continuing the story, let us understand what Satoshi actually proposed. We only need three ideas.

4.1 A shared notebook: the blockchain

Imagine a notebook in which every payment ever made is written down. Thousands of people around the world each keep an identical copy. Every ten minutes or so, a new *page*, called a *block*, is added containing the latest payments. Each page also carries a “fingerprint” of the page before it (Figure 1). If anyone tried to secretly change an old page, its fingerprint would change, the next page would no longer match, and everyone would notice. This chain of pages is the *blockchain*.

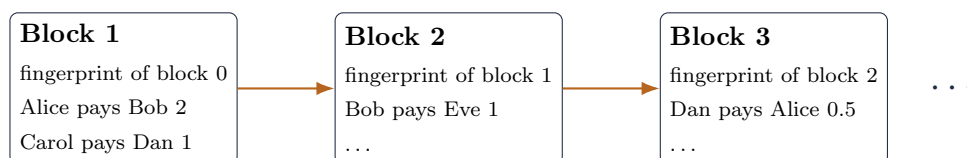


Figure 1: The blockchain: each page of the notebook is locked to the one before it by a digital fingerprint.

The “fingerprint” is produced by a *hash function*: a mathematical recipe that turns any text into a short code. The same text always gives the same code, but changing even one comma gives a completely different one, and there is no way to work backwards from the code to the text.

4.2 Who writes the next page? Mining as a lottery

If everyone keeps the notebook, who decides which page comes next? Bitcoin’s answer: the person who wins a lottery. Computers called *miners* race to find a fingerprint for the new page that is smaller than a certain target number. The only way to find one is to try again and again, changing a small counter each time. It is exactly like rolling dice until you get a very low score.

Example 4.1 (Rolling dice). Suppose you roll a normal six-sided die and you “win” if you roll a 1. The chance of winning on each roll is $p = \frac{1}{6}$. On average, how many rolls do you need? The answer is simply

$$\text{average number of tries} = \frac{1}{p} = \frac{1}{1/6} = 6.$$

Bitcoin mining works the same way, except that the “die” has an astronomically large number of faces. In 2025, miners around the world were making roughly a thousand *billion billion* (10^{21}) attempts every second.

The winner gets to add the next page and receives a reward of new bitcoins. This is how new coins enter circulation, and why the process is called *mining*, by analogy with digging for gold. Your chance of winning is simply your share of the total computing power: a miner with 1% of the world’s machines wins about 1% of the blocks.

Keeping time: the difficulty adjustment. If more miners join, pages would be found faster. To keep a steady rhythm of one block every ten minutes, Bitcoin automatically adjusts the difficulty every 2016 blocks (about two weeks):

$$\text{new difficulty} = \text{old difficulty} \times \frac{2 \text{ weeks}}{\text{time actually taken}}.$$

For instance, if the last 2016 blocks took only 12 days instead of 14, the difficulty is multiplied by $\frac{14}{12} \approx 1.17$, making the puzzle about 17% harder. This simple rule has kept Bitcoin’s clock running for more than seventeen years, through enormous changes in computing power.

4.3 Why it is so hard to rewrite the past

Suppose a cheater wants to erase a payment that is already six pages deep in the notebook. They must rewrite that page *and* every page after it, and then overtake the honest network, which keeps adding new pages all the while. In his paper, Satoshi computed how likely this is. The result is strikingly simple.

Proposition 4.2 (Satoshi’s catch-up estimate). *If a cheater controls a fraction q of the computing power and the honest miners control $p = 1 - q$, with $q < p$, the probability that the cheater ever catches up from z blocks behind is*

$$\left(\frac{q}{p}\right)^z.$$

Why? Think of it as a race in which the cheater is z steps behind. One can show that the chance of the cheater *ever* making up a single step of delay is exactly q/p . To make up z steps, this must happen z times in a row, and the probabilities of successive events multiply: $\frac{q}{p} \times \frac{q}{p} \times \dots$ (z times). Since q/p is less than 1, multiplying it by itself makes it shrink very fast.

Example 4.3 (The power of six confirmations). A cheater with 10% of the computing power has $q/p = 0.1/0.9 = 1/9$. Six blocks behind, the chance of success is

$$\left(\frac{1}{9}\right)^6 = \frac{1}{531\,441} \approx 0.0002\%.$$

Cheater's share of power, q	10%	20%	30%	45%
Chance to catch up from 6 blocks	0.0002%	0.02%	0.6%	30%

Table 1: The deeper a payment is buried, the safer it is. This is why exchanges traditionally wait for six “confirmations.” If a cheater ever controlled more than half the power ($q > p$), this protection would fail: the famous *51% attack*.

5 The Early Days (2009–2010)

3 January 2009: the Genesis Block. Satoshi mined the very first block, known as the *Genesis Block*. Hidden inside it is a line of text, the front-page headline of the British newspaper *The Times* that day:

Chancellor on brink of second bailout for banks.

It served as a timestamp, proving the block could not have been created earlier. It also reads as a statement of purpose: a new kind of money, born in the middle of a banking crisis.

“Running bitcoin.” On 9 January 2009, Satoshi released the first version of the software. The next day, Hal Finney, the creator of RPOW, downloaded it and posted a two-word message on Twitter: *Running bitcoin*. On 12 January, Satoshi sent him 10 bitcoins: the first Bitcoin transaction between two people.

The first price. For months, bitcoins had no price at all; they were a curiosity mined by a few dozen hobbyists on home computers. In October 2009 a website called New Liberty Standard published the first exchange rate, based on the cost of the electricity needed to mine a coin:

$$\$1 = 1309.03 \text{ BTC} \implies 1 \text{ BTC} = \frac{1}{1309.03} \text{ dollars} \approx \$0.00076.$$

In other words, one bitcoin was worth less than a tenth of a cent.

22 May 2010: Bitcoin Pizza Day. A programmer in Florida, Laszlo Hanyecz, offered 10,000 bitcoins on a forum to anyone who would deliver him two pizzas. Someone accepted, ordered two pizzas from a local restaurant, and had them delivered. It was the first known purchase of a physical good with bitcoin. The date is still celebrated every year as “Bitcoin Pizza Day.”

Example 5.1 (The most expensive pizzas in history). The value of those coins at a later price of \$100,000 per bitcoin:

$$10\,000 \text{ BTC} \times \$100\,000 = \$1\,000\,000\,000.$$

One billion dollars, or about half a billion dollars *per pizza*. Laszlo has said he has no regrets: someone had to show that bitcoin could actually be used to buy things.

The 184-billion-coin bug. On 15 August 2010, someone exploited a programming error to create more than 184 billion bitcoins in a single transaction, far beyond the 21 million that should ever exist. The community noticed within hours. Satoshi and other developers published a fix, miners switched to the corrected software, and the faulty block was abandoned in favour of a corrected chain. It remains the most serious bug in Bitcoin’s history, and a powerful demonstration that the network’s rules are enforced by its users.

6 The Vanishing Creator

Satoshi Nakamoto was active on forums and mailing lists for about two years, writing code, answering questions, and fixing bugs. Then, gradually, Satoshi withdrew. The last public forum post dates from December 2010. In April 2011, in a private e-mail to a developer, Satoshi wrote of having moved on to other things, and handed control of the project to others, notably the American developer Gavin Andresen. Satoshi has not been heard from since.

Who is Satoshi? Nobody knows. The name is almost certainly a pseudonym. Satoshi wrote in fluent English, sometimes with British spellings, and posted at hours suggesting a life in the Americas, but none of this is proof. Over the years, many people have been suggested:

- **Hal Finney**, the first recipient of bitcoin. He always denied it, and e-mails show him corresponding *with* Satoshi. He died in 2014.
- **Nick Szabo**, the inventor of Bit Gold, whose ideas and writing style are close to Satoshi's. He has denied it.
- **Dorian Nakamoto**, a Californian engineer named by *Newsweek* in 2014, apparently because of his name. He firmly denied it.
- **Craig Wright**, an Australian computer scientist who claimed for years to be Satoshi. In 2024, the High Court of England and Wales ruled that he is not.

Did you know? Analysis of the earliest blocks suggests that Satoshi mined roughly one million bitcoins in 2009 and 2010. Those coins have *never moved*. If they ever did, it would be front-page news worldwide. The smallest unit of bitcoin, one hundred-millionth of a coin, is named a *satoshi* in the creator's honour:

$$1 \text{ BTC} = 100\,000\,000 \text{ satoshis} = 10^8 \text{ satoshis.}$$

7 Growing Pains (2011–2014)

Parity with the dollar. In February 2011, one bitcoin reached the price of one US dollar for the first time. Media attention followed, along with the first speculative frenzy: in June 2011 the price shot up to around \$30 before crashing back to a few dollars. This cycle of euphoria and collapse would repeat many times.

Silk Road. Also in February 2011, an anonymous online marketplace called Silk Road opened, accepting only bitcoin. It became notorious for drug sales, and for years many people associated bitcoin with crime. The FBI shut it down in October 2013 and seized its bitcoins. Investigators have since shown that bitcoin is far from anonymous: because every payment is written in the public notebook, payments can often be traced.

The rise and fall of Mt. Gox. Most early users bought their bitcoins on *exchanges*, websites that swap bitcoins for ordinary money. The largest was Mt. Gox, based in Tokyo, which at its peak in 2013 handled the majority of all bitcoin trading. In February 2014 it suddenly stopped withdrawals and declared bankruptcy: around 850,000 bitcoins belonging to its customers had disappeared, mostly through years of undetected theft. It was a painful lesson that is still repeated in the community today: *not your keys, not your coins*. If someone else holds your bitcoins for you, you are trusting them, exactly as with a bank.

The first \$1,000. In late 2013, the price passed \$1,000 for the first time, before falling by more than 80% over the following year. Many commentators declared bitcoin dead. It would not be the last time.

8 The 21 Million: Bitcoin's Built-in Scarcity

Unlike dollars or euros, which central banks can create as needed, the total number of bitcoins is fixed by the software. Here is how it works, and a short proof that the total is 21 million.

The halving. At the start, each new block rewarded its miner with 50 bitcoins. Every 210,000 blocks, this reward is cut in half: 50, then 25, then 12.5, and so on. Since a block arrives every ten minutes on average, the time between two halvings is about

$$210\,000 \times 10 \text{ min} = 2\,100\,000 \text{ min} \approx 4 \text{ years}.$$

Period	Reward per block	Coins created in the period	Total at the end
2009–2012	50	10,500,000	10,500,000
2012–2016	25	5,250,000	15,750,000
2016–2020	12.5	2,625,000	18,375,000
2020–2024	6.25	1,312,500	19,687,500
2024–2028	3.125	656,250	20,343,750

Table 2: Each four-year period creates exactly half as many coins as the one before. Halvings occurred in November 2012, July 2016, May 2020, and April 2024. The next is expected in 2028.

Proposition 8.1 (The 21 million limit). *The total number of bitcoins that will ever exist is (just under) 21 million.*

Proof. In the first period, $210\,000 \times 50 = 10\,500\,000$ coins are created. Each later period creates half as many as the one before, so the total is

$$10\,500\,000 \times \left(1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots\right).$$

The sum in brackets is equal to 2. To see why, imagine walking towards a wall 2 metres away: you first walk 1 metre, then half of the remaining distance ($\frac{1}{2}$), then half of what remains ($\frac{1}{4}$), and so on. You get ever closer to the wall but never pass it, so the total distance walked approaches exactly 2 metres. Therefore the total supply approaches

$$10\,500\,000 \times 2 = 21\,000\,000. \quad \square$$

In practice the true total is very slightly below 21 million (about 20,999,999.98), because bitcoin cannot be divided below one satoshi and the tiniest fractions are rounded away. The last satoshi should be mined around the year 2140. Figure 2 shows how quickly the supply approaches its limit: by 2024, more than 93% of all bitcoins already existed.

Why it matters. Bitcoin's supply schedule was fixed in 2009 and is known to everyone in advance. No government, company, or developer can print more. This is why supporters often call bitcoin "digital gold": its value comes in part from being scarce and unchangeable.

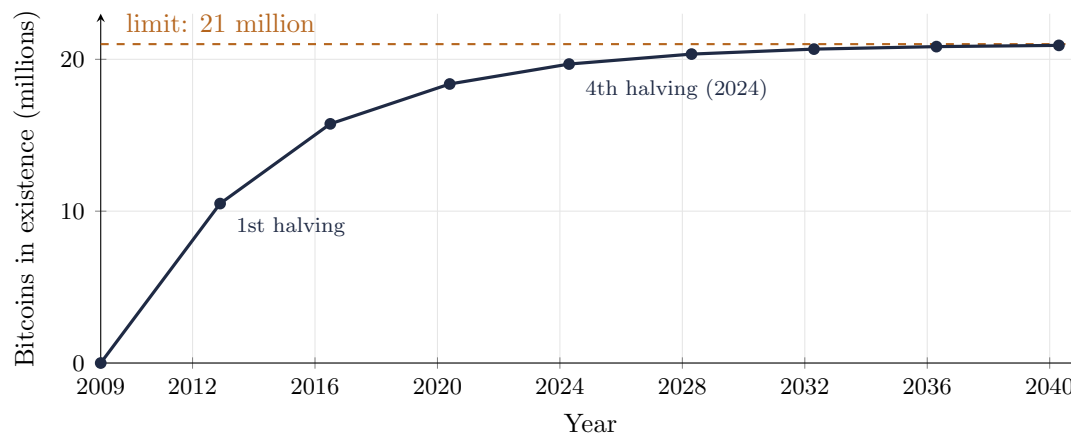


Figure 2: The supply of bitcoin over time. Each segment is half as steep as the one before: the curve flattens towards 21 million but never crosses it.

9 Civil Wars and Upgrades (2015–2021)

The block size war. Since 2010, each block had been limited to 1 megabyte, which allowed only a few transactions per second. As bitcoin grew, fees rose and payments slowed. One camp wanted to simply make blocks bigger. The other feared that bigger blocks would make it too expensive for ordinary people to run their own copy of the notebook, concentrating power in the hands of a few large companies. The debate, which ran from about 2015 to 2017, became bitter.

The split of 2017. The conflict ended with a *fork*. In August 2017, the network adopted an upgrade called *SegWit* (“Segregated Witness”), which fit more transactions into each block without raising the official limit. The big-block camp, unhappy with this compromise, created a separate currency on 1 August 2017: *Bitcoin Cash*. Both chains share the same history up to that date, but have been separate ever since. The market largely kept the original Bitcoin. The episode showed that no single person, not even the largest companies or miners, could impose changes on Bitcoin against the will of its users.

The Lightning Network. Instead of putting every coffee purchase in the main notebook, the *Lightning Network*, launched in 2018, lets people open a payment “channel,” exchange many quick payments between themselves, and settle only the final balance on the blockchain. It is a little like running a tab at a bar and paying once at the end of the night.

Taproot (2021). In November 2021, Bitcoin activated its largest upgrade in years, called *Taproot*. It introduced a more efficient type of digital signature (the *Schnorr signature*, named after the German cryptographer Claus-Peter Schnorr), making complex transactions cheaper and more private.

The bubbles. Meanwhile, the price kept its wild rhythm: close to \$20,000 in December 2017, then a fall of more than 80%, then a new record near \$69,000 in November 2021, followed by another crash in 2022, worsened by the collapse of several large crypto companies.

10 Bitcoin Goes Mainstream (2021–2025)

A country adopts bitcoin. In September 2021, El Salvador became the first country to make bitcoin legal tender alongside the US dollar. The experiment drew worldwide attention,

but adoption by ordinary citizens remained limited. In early 2025, as part of a loan agreement with the International Monetary Fund, the country amended its law so that businesses are no longer obliged to accept bitcoin.

Wall Street arrives. In January 2024, after a decade of refusals, the US Securities and Exchange Commission approved the first *spot bitcoin ETFs*: investment funds, traded on the stock market, that hold real bitcoins. For the first time, a pension fund or a retiree could buy exposure to bitcoin as easily as buying a share. Billions of dollars flowed in within months.

Six figures. In December 2024 the price passed \$100,000 for the first time. In March 2025 the President of the United States signed an executive order creating a *Strategic Bitcoin Reserve*, made up of bitcoins previously seized by the government in criminal cases. In early October 2025, the price set a new record above \$125,000. From less than a tenth of a cent in 2009, that is an increase by a factor of more than a hundred million.

The energy debate. Bitcoin’s success has a cost that critics often point out: mining consumes a great deal of electricity, comparable to the annual consumption of a medium-sized country. Supporters reply that this energy is precisely what secures the network (it is the “cost of cheating” from our catch-up calculation), that miners increasingly seek out cheap surplus and renewable power, and that the traditional banking system also consumes energy. The debate continues.

11 Conclusion

In seventeen years, Bitcoin has gone from a nine-page paper read by a few dozen enthusiasts to an asset held by governments, banks, and millions of individuals. Its creator vanished, its price crashed more than once by 80%, it was declared dead hundreds of times, and its community nearly tore itself apart. And yet the network has never stopped: a new block has been added, roughly every ten minutes, since January 2009.

Whatever one thinks of it as an investment, Bitcoin answered a question that computer scientists had struggled with for decades: *how can strangers who do not trust each other agree on a single shared history, without anyone in charge?* That answer is perhaps its most lasting legacy.

A Small Glossary

Block A page of the shared notebook, containing a batch of recent payments.

Blockchain The full chain of blocks, each locked to the previous one by a fingerprint.

Hash A digital fingerprint of a piece of data. Change the data, and the fingerprint changes completely.

Mining Competing, with computing power, to add the next block and earn the reward.

Halving The automatic halving of the mining reward, every 210,000 blocks (about four years).

Fork A split, when part of the network adopts different rules from the rest.

Satoshi The smallest unit of bitcoin, 10^{-8} BTC; also the pseudonym of its creator.

Wallet Software that holds your secret keys, which give you the power to spend your bitcoins.

Date	Event
1982–1989	David Chaum invents blind signatures and founds DigiCash
1992	The Cypherpunks mailing list is founded
1997	Adam Back proposes Hashcash (proof of work)
1998	Wei Dai describes b-money; Nick Szabo designs Bit Gold
31 Oct 2008	Satoshi Nakamoto publishes the Bitcoin white paper
3 Jan 2009	The Genesis Block is mined
12 Jan 2009	First transaction: Satoshi sends 10 BTC to Hal Finney
22 May 2010	Bitcoin Pizza Day: 10,000 BTC for two pizzas
Apr 2011	Satoshi’s last known message
Nov 2012	First halving: reward falls from 50 to 25 BTC
Feb 2014	Collapse of the Mt. Gox exchange
Aug 2017	SegWit activated; Bitcoin Cash splits off
Sep 2021	El Salvador makes bitcoin legal tender
Nov 2021	Taproot upgrade activated
Jan 2024	First spot bitcoin ETFs approved in the United States
Apr 2024	Fourth halving: reward falls to 3.125 BTC
Dec 2024	Price passes \$100,000
Oct 2025	New record above \$125,000

Table 3: Key dates in the history of Bitcoin.

Further Reading

- [1] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. Available at bitcoin.org/bitcoin.pdf.
- [2] D. Chaum. Blind signatures for untraceable payments. *Advances in Cryptology: Proceedings of Crypto 82*, 1983.
- [3] E. Hughes. *A Cypherpunk’s Manifesto*. 1993.
- [4] A. Back. Hashcash: A denial of service counter-measure. 2002.
- [5] W. Dai. b-money. 1998.
- [6] N. Popper. *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*. Harper, 2015.
- [7] S. Ammous. *The Bitcoin Standard*. Wiley, 2018. (A strongly pro-bitcoin view.)
- [8] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. *Bitcoin and Cryptocurrency Technologies*. Princeton University Press, 2016.