Cryptocurrencies and Blockchains

Quinn DuPont
CHAPTER TWO

Origins and Futures of Cryptocurrencies

Bitcoin is the first cryptocurrency: a cryptographically secured, privately issued digital money. Or at least it wants to be money. Designed around 2008 and released in early 2009 by a shadowy and unknown inventor, “Satoshi Nakamoto,” Bitcoin was a response to the 2008 global economic crisis, the worst economic crisis in decades, perhaps centuries. A whole generation of people—derided as millennials—were economically devastated (see Hobbes 2017) and unsurprisingly many are now thoroughly enticed by Bitcoin. But Bitcoin was also designed to be more than just another digital money. Nakamoto wanted to remake the entire economic system anew, from the roots of cyberlibertarian politics and extreme Austrian economics (Golumbia 2016). While Bitcoin has dramatically changed since its early days—it is now largely used for investment (see Chapter 5)—these radical economic and political origins are still visible. Literally encoded in the original (or “genesis”) block, Nakamoto set his political aim: “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.”

The design and architecture of Bitcoin reflects these political and economic goals. Bitcoin is issued on a predetermined schedule that reaches a maximum and then stops. This monetary cap ostensibly prevents inflation, which is the worst sin of central banks that print money with abandon, according to Bitcoin’s economic logic. In reality, however, Bitcoin does not avoid inflation because inflation is not a simple monetary issue (instead, Bitcoin suffers deflation, even hyperdeflation). Bitcoin is also a peer-to-peer system that ostensibly does
away with central banks and government backing, another key dimension of the ideology inscribed in its design. Since Bitcoin is passed peer-to-peer without a central clearinghouse, it is supposed to be unstoppable and impervious to censorship. This, too, in reality, is not so simple. Because Bitcoin is a complex socio-technical ecosystem and not just a technical protocol, it is shaped by many externalities, including users bent on manipulating or attacking the market, systemic risks caused by cryptocurrency exchanges, and evolving legal status dictated by government regulators (see Gerard 2017).

This chapter details the origins of Bitcoin and offers a description of its future uses and present issues. Bitcoin emerged from the panic of the 2008 global economic crisis but traces its roots through the long history of alternative and private currencies, and in particular the ways these were taken up by a subculture of “cypherpunks.” The predecessors of Bitcoin that emerged out of the cypherpunk community combined recent advances in cryptography with quixotic political and economic goals. This chapter sets up the discussion that is completed in the next chapter, about how cryptocurrencies do and do not count as money, which marks a transition between the first and primary use of cryptocurrencies as money and the second and broader use of blockchain technologies for everything else. The broader arch over these three chapters is the transition from money to media.

Origins

Bitcoin was not the first private money, nor the first digital money, and not even the first to use cryptography. Money has a long history beyond the familiar stuff found in wallets (Maurer 2006). Money comes in many different forms and is used in many different ways (Maurer 2015). Some scholars distinguish between money, currency, and cash (see Agha 2017). These are, however, multidimensional categories: money is the broadest (and abstract) category of value,
currency is whatever kind of money is accepted and counts for “passing current” (Brunton 2018), and cash is the physical form of currency (or “pecuniary media” that are usually state-issued banknotes and coins). While these distinctions may at first seem clearcut, they are quickly blurred, especially in the digital realm.

The variety and accessibility of money today is vast. Money has been issued by people, companies, banks, states, collectives, and groups. Sometimes, money is not “issued” at all, appearing by spontaneous social consensus (but some scholars claim that in order to count as “money,” it must be issued by someone; see Ingham 2004, p. 12). Money has taken many shapes, sizes, and material forms, ranging from shells, stones, metal coins, paper notes, and digital data—to say nothing of the ways that abstract notions such as labor, credit, or purchasing power count as kinds of money. Nor is this variety of issuers and materials just a historical curiosity. Money is still widely issued outside of the familiar forms of state-issued currencies. Money, or perhaps “money-like” things, includes private scrips (IOUs, company money, and loyalty programs), video game currencies, monthly transit passes, and arguably the largest category of all, government bonds (Ferguson 2009).

There are also many “alternative” forms of money still passing hand to hand, as currencies in their own right. In fact, privately issued currencies are surprisingly common, usually filling some unmet need specific to their context. For example, Salt Spring Dollars can only be spent on the small island off the coast of western Canada, Euskos can only be spent in Northern Basque country, and North London LETSs (a “Local Exchange Trading Scheme”) allow community members to directly trade skills and services instead of exchanging the abstract and alienating value of state-issued currency. Sometimes ready-made things or abstractions take the place of money, such as the exchange of mobile phone airtime minutes in Egypt, Ghana, Uganda, and Kenya. In Kenya, this
grassroots practice grew until a major telecommunications company, Safaricom, adopted it and formally developed it into M-Pesa, now a successful alternative banking and monetary system across Africa (Dodd 2016; Harris, Goodman, & Traynor 2012).

Despite many well-established alternatives, the online world presents new challenges for money. Before Bitcoin, it was no secret that a better solution to online commerce and digital money was needed. Many companies tried to fill this gap (see Clark 2016), but credit card companies were the most successful. Credit card companies, however, left much to be desired. In addition to being rentier, for-profit companies selling parasitic credit-based solutions, actually using credit cards online was (and is) fraught with issues. Supporters of Bitcoin, the open-source, peer-to-peer, pseudonymous network controlled by no one with unblockable and immutable transactions, feel that it is just the thing the world needs.

The existing payments and digital money infrastructure has issues. First, payments companies block certain kinds of transactions. For example, in 2012, credit card companies blocked transfers to WikiLeaks, which then turned to Bitcoin as an alternative. These credit card companies were ostensibly acting on legal requirements: legitimate financial services are prohibited from working with criminals, terrorists, fraudsters, and money launderers, which includes WikiLeaks. But many saw the blockade against WikiLeaks as simply politically motivated financial censorship. Second, credit cards permit "chargebacks." That is, credit card transactions are never really "final" and can be reversed by the credit card company for any reason. Third, online credit card purchases are weakly authenticated—usually requiring only a credit card number and expiry date—so fraud online is rampant. Usually fraud is dealt with by credit card companies as a service to customers, but this cost is passed on in the form of fees. Fourth, while credit card companies filled the online payments gap, they failed to facilitate peer-to-peer transfers. Bank wires, Western
Union transfers, and other private money solutions like PayPal and later Alipay do permit peer-to-peer transfers, with some of the qualities of cash, but they also operate within the confines of laws and regulations and, like credit card companies, they are private businesses interested in profit maximization.

Early proto-cryptocurrencies solved some of these issues, but for a variety of reasons these failed to achieve widespread adoption. The most famous and successful was DigiCash, designed and launched by the cryptographer David Chaum in 1989. DigiCash was a private corporation, and it worked within the legitimate financial sector, but unlike the services offered by existing credit card and payments companies, DigiCash’s “e-Cash” was designed to be much more like cash in that it permitted untraceable online transactions. Anonymous transactions were made possible by Chaum’s own cryptographic innovation, a technique known as Blind Signatures (Chaum 1982). This anonymity was a key feature of DigiCash, which later inspired Bitcoin. However, because DigiCash was a private centrally organized company, when the company DigiCash went bankrupt in 1998, the e-Cash money system it sustained also shut down (Blanchette 2012).

In the years following DigiCash’s bankruptcy, systems using similar kinds of cryptographic technology were proposed and some were even developed. Leading up to the 1990s Internet bubble, dozens of companies followed DigiCash’s lead as they launched their products but found no users or interested business partners and were subsequently shuttered (Pitta 1999). The salad days of digital money have lessons for the current cryptocurrency market.

Direct antecedents to Bitcoin through the 1990s and 2000s included Adam Back’s Hashcash, Hal Finney’s Reusable Proofs, Nick Szabo’s Bitgold, and Wei Dai’s b-money, as well as numerous other commercially oriented “digital gold” systems like Liberty Dollar, Gold Money, and e-gold (Brunton 2018). Gold-like systems with “material” constraints and the perceived economic stability they entailed were popular (Dodd
Back's Hashcash system, for example, developed from an idea to use computational processing time (solving tough equations) as a kind of material constraint to limit sending email spam (Brunton 2013). By making it computationally expensive to send email spam, Hashcash implicitly made the virtual nothingness of solving tough equations a valuable commodity. (Back appears to have developed his system independently from an earlier one proposed by cryptographers Cynthia Dwork and Moni Naor; see Clark 2016.) In effect, the Hashcash system issued an unlimited but materially constrained supply of money. This system directly influenced the design of Bitcoin.

The materiality of traditional banknotes and coins is what makes cash work (see also Chapter 3), but this is not easily replicated by digital money. Cash solves two key issues: ownership and authenticity. With cash, the question of who owns it is usually pretty apparent; the owner is the person in physical possession of the cash (the same is true for bearer instruments). In cases where you “own” some cash not in your possession—perhaps the bank is holding on to it for you—your ownership claim is attenuated. As Bitcoin evangelists will tell you, cash in a bank isn’t really yours, and it takes just one bank run to discover this brutal fact. In the same way, cash is also an efficient medium of exchange. Once you spend your cash, physically handing it to the recipient, the cash transfers ownership. There are no chargebacks or payment reversals with cash. Once spent, cash is gone.

Authenticity is more difficult. Modern banknotes and coins guarantee authenticity by using sophisticated printing techniques and special materials, but this is an imperfect science. Users of cash can check authenticity by inspecting the material item, looking for telltale anti-counterfeiting markers. However, counterfeited money is not uncommon (especially for the notoriously low-tech US notes). Even with anti-counterfeiting measures, so-called “supernotes” can be printed on machines identical to the originals using
indistinguishable materials, but these notes are considered counterfeit. Supernotes are, in all but sovereign authority, identical forms of currency (see Chapter 3). This is a problem. Because the authenticity of cash is represented by its materiality, but ultimately lies in the authority of the issuing sovereign, it can never be proven to be authentic. One must trust in the general efficacy of anti-counterfeiting measures, the likelihood that cash will be accepted for payment, and that the sovereign will continue to authorize the currency.

In the digital world, ownership and authenticity are more complicated. Since digital files can be perfectly and endlessly copied and shared, special techniques are needed to make digital money behave like cash. Using cryptographic techniques developed in the late 1970s, it is easy to prove (and verify) the authenticity of digital money. Because these cryptographic techniques are considered robust, issues of authenticity are largely solved: users do not need to rely on trust for the authenticity of digital money, since, having been cryptographically generated, digital money is practically impossible to counterfeit. DigiCash and other proto-cryptocurrencies used these techniques for precisely this reason. In fact, in this regard, digital money is superior to cash since authenticity can be proven and independently verified. Bitcoin adopted these cryptographic techniques, but more significantly, Bitcoin also solved the issue of ownership that had plagued earlier versions of digital money.

Rather than trying to replicate the materiality of cash in a digital world, Bitcoin solved the ownership problem by adapting double-entry bookkeeping (in Chapter 4, I describe the specifics of the underlying transaction technology used in Bitcoin, which is called a "blockchain"). Far from a new invention, double-entry bookkeeping has been in use since the Renaissance (Poovey 1998). Traditionally, accountants kept track of incoming and outgoing finances by recording transactions on a ledger. With double-entry bookkeeping, the ledger has two columns, and every transaction has an entry in each,
which must add up correctly. For each transaction, assets are “cancelled” as they are moved from the asset column to the liability column. Having two entries ensures that any errors or fraud will be caught and can traced back to the origin. Digital versions of double-entry bookkeeping were of course in use before Bitcoin, being used for tracking company finances and, in effect, issuing digital money. A digital bank, for example, can manage its digital cash by tracking and cancelling funds as they are spent. If you send me a digital dollar, the dollar is deducted from your side of the ledger and added to mine. Once the transfer is completed, you cannot “spend” that same digital dollar again (even if you make a perfect copy) because it has been cancelled from your account. The ownership of digital cash, thus, must be carefully tracked and managed by the issuing bank, to prevent “double spending,” but the system works.

While double-entry bookkeeping is an elegant solution for keeping track of digital money, it also introduces a source of risk. First, to prevent users from double-spending money, transactions must be carefully tracked and cancelled. Second, those who control the ledger control the source of money. An unscrupulous digital bank could omit or censor certain kinds of transactions, or the ledger itself could be lost. Worst of all, if the bank that controls the ledger goes bankrupt, the entire system simply stops working and the digital money is rendered worthless. Accepting this risk requires a lot of trust from users, which is why traditional digital money companies have built their businesses on reputations of trustworthiness (“The Trust Machine,” 2015).

The fundamental issue facing traditional digital money companies, like PayPal or Alipay, is that they are organizationally and technically centralized. Removing this source of risk (and trust) would be an obvious innovation, but without a company keeping track of transactions on a ledger, how do you prevent someone from making perfect copies and spending the same digital dollar over and over? Bitcoin’s solution
(described in detail below and in Chapter 4) is to decentralize the ledger. By removing the central authority, participants in the money network are responsible for validating transactions and updating their own copy of the ledger. Then, using a clever "consensus protocol," the multitude of distributed ledgers are kept in sync to produce one version of the truth about who owns what (while ensuring that no fraudulent copies of the ledger are permitted). An additional benefit to decentralizing the ledger is that by removing the central controlling authority, all of the issues about censorship, fraud, and bankruptcy are removed. This distributed and decentralized ledger, when combined with a network of recording and validating nodes, became known as a blockchain.

These are the two key components to how Bitcoin works: cryptographic authentication of digital money and decentralized record keeping. While the latter was the real innovation, and as we will see in Chapter 4 it was the idea that really caught, it was the former that provided the social and cultural roots of Bitcoin. It is through its genealogy in cryptography that Bitcoin acquired the label of "cryptocurrency." Unlike, however, the underlying cryptographic algorithms, the idea for Bitcoin did not emerge from universities or government research labs. Cryptocurrencies and specifically Bitcoin came from an anarcho-capitalist movement known as "cypherpunk."

The cypherpunk movement was not a single group or ideology. It emerged from embryonic political strands in the early 1990s, with members who were interested in finding applications of cryptography to wrest control and power from governments and states (they were punks, after all). They also had wide-ranging and eclectic interests: cryogenics, transhumanism, technological singularity, Libertarian politics, and money (Brunton 2018). Part acid-trip culture, part California ideology, and part Wired magazine, cypherpunks soon became a political force that would change the course of technology regulation and spur innovation. The cypherpunks
were, for example, influential in releasing and proselytizing Phil Zimmerman's "Pretty Good Privacy" (PGP) email encryption software, protesting a "secure" telephone system that contained the government-mandated "Clipper Chip," and forcing the US government to transfer control and regulation of cryptographic software from the military to the Commerce Department. They also helped develop tactical organizations such as the Electronic Frontier Foundation (EFF), which emerged as a powerful ally to early Internet companies. With the help of the EFF and the cypherpunks, Internet companies such as Facebook and Google later became the dominant actors in the new media and communications industry.

For all of their eclectic interests, the cypherpunks considered money to be an essential ingredient in the realization of their punk goals and political aspirations. This meant in the first instance that cypherpunks were hostile to state-issued money. Cypherpunk theories of money were often bundled with Austrian economics, especially as these stem from the economist Friedrich Hayek. Famously, Hayek wanted money to be issued outside of national controls. But where Hayek thought private banks should be responsible for issuing money, the punk ethos ran deeper. Cypherpunks sought radical disintermediation, with no states or banks. This led them to experiment with money systems that ran like machines, or better yet, to think about money as a machine.

Bitcoin is a vision for digital cash, and like cash, it is supposed to be anonymous. But recall that in Bitcoin all transactions must be tracked and managed on distributed ledgers and that these ledgers must be open to inspection. Transactions are seen by all. Thankfully, in Bitcoin you are not represented by your real identity. Instead, your wallet address, where transactions go in and out, is a jumbled string of data that stand in for you. So long as you keep your real identity unlinked from your wallet address (as it turns out, this isn't so simple), you have an element of privacy. Therefore, the system is pseudonymous (not, as it is often mislabeled, anonymous).
But, like cash passing anonymously in the offline world, Bitcoin has also been taken up in earnest by criminals: from drug dealers to cyberwar actors and from tax dodgers to money launderers. More accurately, Bitcoin resembles Swiss or offshore numbered banking, and like these institutions, is often used illegally. These illegal use cases, however, are not the accidental outgrowth of an open system. Illegal use is an intentional and expected consequence. According to Bitcoin’s early developers and advocates, illegality is a symptom of a liberated money system. Money without borders or boundaries was a conscious design decision and key to the political agenda—to create a world without state or corporate oversight and sanction.

For reasons beyond the control of cypherpunks, the influence and power of state-issued money had already been eroding over the last several decades. This was not unusual, since, in the anthropological record, state-issued money is actually something of a recent invention. State-issued money played an important role in the development of modernity and the emergence of sovereign nations (see Chapter 3), which has led some scholars to argue that we are now living in a “golden era” of state-issued money. However, inspired in part by the advent of Bitcoin and cryptocurrencies, the sociologist of money Nigel Dodd questions this claim. Dodd asks if there has ever been a golden era of state-issued money (Dodd 2016, p. 212). He points out that state-issued money, along with sovereign power, has never been absolute. Today, state-issued money makes up a small percentage of the total money supply (less than 11 percent, according to Ferguson 2009). In recent years, most money, or at least the stuff that has replaced money, has been bound up in financial instruments like stocks and bonds or has been invented out of thin air through the financial wizardry that produced the Collateralized Debt Obligations responsible for causing the 2008 global economic crisis, to which Bitcoin was a response. In this way, the emergence of Bitcoin, seemingly out of thin air, is quite typical.
In sum, Bitcoin capitalized on a set of geopolitical trends, political alliances, and technological affordances to create a system of privately issued digital money, without state or bank backing, which operated pseudonymously and was impervious to censorship. It accomplished this with cryptographic algorithms and decentralized ledgers.

Developing cryptocurrencies and blockchains

While it is unknown who really invented Bitcoin, how the Bitcoin software was developed is less mysterious. A person going by the name “Satoshi Nakamoto” first publicly discussed Bitcoin on October 31, 2008 and released a whitepaper (early source code was available by request). A month earlier, Nakamoto had registered bitcoi.n.org domain and claimed that the software had been in development for “over the last year and a half” (according to an early forum post by Nakamoto). A discussion on the Cryptography Mailing List where Nakamoto made the announcement quickly ensued. Influential members of the cryptography community, such as Hal Finney (who later became an important contributor to Bitcoin), responded with questions about the system’s design and assumptions. Nakamoto actively responded to these questions and before long the source code was available on the open-source software repository SourceForge. Like other open-source software projects, a loose-knit community of developers began making contributions to the code. Some of the early and influential figures included Martii Malmi (“sirius_m”), Laszlo Hanyecz (“laszlo,” who later became famous for buying a pizza for 10,000 Bitcoins), Gavin Andresen (“gavinandresen”), Chris Moore (“dooglus”), Pieter Wuille (“sipa”), Jeff Garzik (“jgarzik”), Gregory Maxwell (“gmaxwell”), and many others. By late 2010, Nakamoto stopped personally contributing to the Bitcoin software and soon disappeared entirely, leaving the rest of the community to continue the project.
As to be expected, the software that is Bitcoin today looks very different from the first version that Nakamoto released and discussed in his famous whitepaper. In the early years of development, Nakamoto and others added features and cut superfluous ones (including a proposed decentralized marketplace, akin to eBay or Silk Road) and generally made the software more robust. Today, anyone can contribute to the Bitcoin “core” software, which is now stored on the open-source software repository GitHub. In addition to improving the software, contributions include submitting bug reports, writing documentation, and creating translations. No person or entity owns or controls Bitcoin software development, but a small group of developers have official “commit” access to the source code repository and therefore are ultimately responsible for the development of Bitcoin.

As part of the ethos of open-source software development, any person is free to “fork” the software. Software forking is a routine activity in open-source software development, but controversial forks emerge when developers with commit access refuse to integrate features or changes that some part of the community believe are important (think of software forking like a vote of non-confidence in politics). Since the source code is freely and openly available, anyone can create a duplicate version and set off development in a different direction, thereby splitting (or “forking”) from the original. The results of a forked software project are two (possibly incompatible) versions that over time have grown increasingly distinct (in theory, the forks can at some point recombine, but this is very rare).

The Bitcoin software has been forked several times, mostly in response to the refusal by the developers of the original version to implement suitable solutions for scaling network capacity (an issue that has plagued Bitcoin since 2015). The result is that there are now several versions of Bitcoin software (the original Bitcoin software was renamed “Bitcoin Core”). In cases where the various Bitcoin software forks are
compatible they co-exist on the same Bitcoin peer-to-peer network and therefore are part of the same monetary system. When the resulting forked software is no longer compatible with the original network protocol, as was the case with the emergence of Bitcoin Cash in 2017, the result is a fork in the distributed ledger as well. Since any transaction data stored on the forked distributed ledger are separate from the original, the new software, network, and transaction data comprise a distinct monetary system. In this way, there can be—and currently are—several competing and completely independent versions of “Bitcoin.”

Of the many cryptocurrency and blockchain software projects that have emerged since the invention of Bitcoin, most take their design cues from the original Nakamoto whitepaper, but they often follow different trajectories. And while most cryptocurrency and blockchain software remains open-source (for reasons of security more than anything else—it is important that source code can be inspected and evaluated by outsiders), only a few exceptional cases can be considered truly open-source software community projects like Bitcoin. Ethereum is the most notable example for comparison. It, like Bitcoin, was invented by a singular individual (Vitalik Buterin) but soon became a true community project with no formal leader. Unlike Bitcoin, however, the development of Ethereum is guided and funded by a nonprofit association, the Ethereum Foundation (the comparable Bitcoin Foundation was set up post facto and is mostly responsible for education, outreach, and lobbying efforts). Most other cryptocurrency and blockchain software projects are developed exclusively by the companies that launch them, and therefore more closely resemble traditional software products.

For any cryptocurrency and blockchain project, the kind of software development that is required is new and difficult and there are few existing best practices or successful models to follow. In particular, the programmers creating the core blockchain infrastructures for these projects are largely
without the ecosystem of tools and testing methodologies that are typical in other software environments, and the security requirements are stringent and uncompromising. Even leading computer security developers frequently make mistakes today. In Chapter 8, for example, I discuss the development of a blockchain platform (The DAO) that was hacked and lost the equivalent of US $78 million. What is unique about this case is that, unlike the slapdash programming of cryptocurrency exchanges (which are constantly hacked and tend not to even use blockchain technologies), the system was developed by a seasoned veteran with a background in high performance computing and security. The system was also vetted by numerous experts in the field, and despite all of this, a tiny unforeseen error in logic was exploited within days of its launch. What this story tells us is that the economic incentive to hack cryptocurrencies and blockchain technologies is a strong motivator, and robust, secure systems require vigilant software development practices.

An especially thorny issue facing blockchain systems that use an open network architecture (like Bitcoin and Ethereum) are the ways in which software is patched, upgraded, and deployed. In the distributed environment of open blockchain systems that use computing resources outside of an organization’s or individual’s control, the previously simple task of updating software becomes a balancing act of persuasion and technical development. As cases like The DAO platform or the Bitcoin scaling debates have made clear, software changes on open platforms must be guided by social consensus. Ultimately, the independent miners that validate transactions are wholly responsible for implementing changes and therefore are truly in charge of the network. Miners may be economically incentivized to update software but sometimes they will be reluctant to do so, and no amount of social pressure may change their decisions.
Future uses and issues

Bitcoin can be used as money, but also in many more ways. Bitcoin can be used for payments, salaries, financial services, remittances, charity, and so on. You can even "burn" Bitcoin to gin up scarcity (more boring than burning real cash—just ask the electro-avant-garde band The KLF who burned £1 million in 1994). Bitcoin can also be used in ways that state-issued money cannot. Because of the recordkeeping system powering Bitcoin—a blockchain—it can be used as a generic "token" system for side-currencies, for tracking material goods, and even for limited scripted programming. In Chapter 4 I discuss blockchain technologies that can be used for an even wider range of applications.

The "colored coins" proposal is a way to use Bitcoin for non-money applications. Early on, colored coins opened up exciting new vistas for Bitcoin, but since the widespread adoption of alternative cryptocurrencies and blockchain technologies, colored coin schemes have now become largely historical relics. Coins are "colored" by adding metadata to transactions that identify coins for an alternative use. The attached metadata (the coin's "color") distinguishes it from regular Bitcoins. Colored coins still remain Bitcoins, but users pretend that they stand in for something else, such as company stocks, voting slips, or coupons. Because Bitcoin can be denominated to 0.00000001 (known as a "Satoshi"), a portion of a Bitcoin, down to a single Satoshi, could represent a bond certificate worth thousands of dollars or just a cup of coffee. In practical terms, however, there are limits to the minimum cost of using a colored coin. Most Bitcoin software will not process "dust" transactions, variously defined as 546 Satoshi (about US $0.10 at the time of writing), and processing fees are often upward of US $20 (until the scaling debate gets settled). Therefore, colored coins only make economic sense for relatively valuable goods (the same is true, of course, for all Bitcoin transactions).
Although colored coin proposals are no longer being widely pursued, they were an important step towards more advanced cryptocurrencies and blockchains. Early software forks of the Bitcoin codebase grew the initial idea, suggesting that a powerful distributed ledger could be used to track, manage, and manipulate nearly anything. The Namecoin system (a distributed Internet Domain Name System) was the first fork of the Bitcoin software, adapting the Bitcoin system for naming websites. Others developed special purpose token systems that used “side chains” of the main Bitcoin network, and eventually alternative cryptocurrencies emerged using entirely new blockchains. With the launch of Ethereum in 2015—a generic blockchain system without a monetary design—the possible use cases expanded almost infinitely.

The difference between cryptocurrency and blockchain technology is not always clear, since most blockchain technologies retain at least some elements from cryptocurrencies, in particular the exchange of value. For example, the Ethereum blockchain system (described in Chapter 4) is the prototypical blockchain technology that is responsible for popularizing the concept and developing the terms we use today. Yet the Ethereum system makes extensive use of valuable tokens (known in the Ethereum system as “Ether”). These tokens—effectively a cryptocurrency—serve many purposes: they help secure the system from game theory attacks, they incentivize general use, they serve as a conduit of value between otherwise disparate systems, they help fund further development of the software, and so on. Other blockchain technologies make extensive use of valuable tokens for funding the organization that is developing the software, a practice known as an “Initial Coin Offering” (ICO) (see Chapter 6). Some of these blockchain technologies use their valuable tokens to economically incentivize or prohibit behaviors. In short, most blockchains utilize a cryptocurrency, and most cryptocurrencies are built on top of a blockchain.

Despite much promise, Bitcoin and cryptocurrencies have
many issues. The most significant issue is that Bitcoin is not being used as money. Instead, Bitcoin and cryptocurrencies have been taken up with vigor as a speculative investment class (see Chapter 5), but wild gambles on price fluctuations hardly live up to the world-changing rhetoric. Most cryptocurrencies also have volatile prices, illiquid markets, and appear to be largely controlled by illegal market manipulations. It is not clear what it would take for Bitcoin and many other cryptocurrencies to change tack at this point.

Replacing industry incumbents and getting real people to adopt digital money is not easy. In the 1990s, a digital money fever gripped the world, much like the “crypto” fever today, but nearly every company went bankrupt (with the notable exception of PayPal, but arguably PayPal succeeded because it did not change anything). Although Bitcoin has grown massively in size and value in recent years, it is arguably going in the opposite direction of its own goals. Today, the concentration of wealth in the Bitcoin market is at levels almost unprecedented for modern comparisons. A mere 1,000 people own 40 percent of the Bitcoin market (Kharif 2017). This concentration of wealth allows these people (“whales” in the vernacular) to manipulate the market to their advantage (or use bots; Gandal, Hamrick, Moore, & Oberman 2017). But for the most part, the majority of Bitcoin users simply retain their assets: 73 percent of Bitcoins are thought to be dormant (or lost) (Fry & Cheah 2016). Many cryptocurrency alternatives have similar market dynamics—for example, two-thirds of the cryptocurrency Ripple has been retained by the company (Weber 2016), making its owners billionaires, at least briefly, during an early 2018 spike in price.

Curiously, as soon as Bitcoin became valuable enough to be of possible use for actually buying things, it stopped being used to actually buy things. In part, this is due to the “switching costs” of using a money that so few others use (an early-user problem) (Luther 2016a; Weber 2014). While switching costs might have driven the early market’s reluctance to adopt
Origins and Futures of Cryptocurrencies

Bitcoin for payments, since then new market dynamics have taken over. In the early days of Bitcoin there still remained a glimmer of hope that it might be used like cash. Some start-ups developed Bitcoin Automated Teller Machines (ATMs) (Wolfson 2015) and a few high-profile retailers begun accepting it for online purchases. Even for these bleeding-edge companies, however, “accepting Bitcoin” really meant installing a pre-packaged widget on an ecommerce platform that would take care of the messy transactional plumbing and instantly exchange Bitcoin for local state-issued currency. Very few companies actually held Bitcoin. This surprised few economists, since Bitcoin’s extreme price volatility exposed retailers to external market shocks, conceivably wiping out a day’s profit without notice. On the other hand, the skyrocketing price of Bitcoin practically guaranteed that no rational economic actor would—or should—spend it. It isn’t a wise economic decision to buy a cup of coffee with Bitcoins today if you have reason to think that your money will be worth more tomorrow. Demurrage alternatives, such as “Freicoin,” reverse this impulse and automatically lose value when not spent, but they have yet to catch on. Either way, people still do not use cryptocurrencies to actually buy things, as a report by Morgan Stanley concluded, noting that by 2017 the use of Bitcoin for shopping was “virtually zero and shrinking” (Chaparro 2017). Plainly, Bitcoin is too volatile to be accepted by merchants, its value appreciates too quickly to be spent (hyperdeflation), and it is difficult to use.

With the rise of speculative investment and the fall of digital money, the result is that most cryptocurrency users today do not truly own cryptocurrencies. Instead, investors trade cryptocurrencies on private exchanges, which use internal accounting systems. Only the most dedicated investors move their investments from private exchanges to cryptocurrency blockchains (which substitutes one kind of risk for another). With so much wealth stored on these centralized services, many of the larger exchanges have become a source of
systemic market risk, not unlike the “too big to fail” banks of the 2008 global economic crisis. The Bitfinex cryptocurrency exchange has been the worst example of this trend in recent years, responsible for over 10 percent of global trading volume in 2017. This market concentration is not as bad as the early days, when Mt. Gox was responsible for upwards of 70 percent of trading volume, but it still causes market instabilities and makes a ripe target for hackers. Like Mt. Gox previously, Bitfinex operates without regulatory oversight and exhibits signs of financial mismanagement. Bitfinex is owned by iFinex Inc., which is registered in the tax haven British Virgin Islands and appears to be operated from China, but little else is known about this shadowy organization (Popper 2017a). Bitfinex has also been hacked in the past, but unlike the Mt. Gox hack that bankrupted the company (and caused a massive crash in the Bitcoin market), Bitfinex inexplicably weathered the storm by issuing internal “IOU” tokens. Later, after much sleuthing by critics, Bitfinex also admitted that it created the cryptocurrency Tether, which was hacked in 2017.

While there are signs of professionalization on the horizon, the early years of cryptocurrencies have been marred by chaotic governance. From software developers engaging in petty fights to inexperienced coders left to develop mission-critical software, many outsiders have wondered if there are any adults involved. The issue is not that the software is open source—there are many highly professional and well-run open-source software projects (a great deal of the Internet is run on open-source software). Rather, call it growing pains or blame it on the propensity for software that literally mints money to attract scoundrels, these early days have been pretty calamitous. Still today, many cryptocurrency startups push the bounds of legal and ethical behavior in the vein of Silicon Valley “disruption," only to discover that finance is one of the most strongly regulated environments in modern society (and for good reason: money matters).

Regulators are to blame too. As part of a widespread
tendency for governments to adopt neoliberal positions on regulation, cryptocurrencies have been largely left unregulated. Even the Canadian government, widely praised for having a sound and well-regulated banking and finance industry, early on adopted a "light touch" to regulation of this sector (Gerstein & Hervieux-Payette 2015). In practical terms, light-touch regulation meant no regulation. In recent years governments have been reasserting control and authority, but one wonders if the lack of early government guidance contributed to the current state of affairs. In the US, for example, oscillating regulation has left a piecemeal and patchwork set of inconsistent and even sometimes contradictory rules. When the US Securities and Exchange Commission (SEC) cracked down on the industry in 2018, investigating some 80 companies and individuals, it was a clear warning to the market that financial compliance was required. Yet many cryptocurrency and blockchain startups decried the SEC's punitive actions, and instead requested clear regulation capable of creating a safe and level playing field. Ultimately, bad actors continue to thrive while legitimate companies are left to navigate uncertain regulation or in some cases have simply avoided entering the market.

The communities of miners have contributed their fair share of issues too. Bitcoin miners, in particular, are becoming enormously wealthy—to the detriment of the Bitcoin ecosystem. As I discussed above, the interests of miners are strategically misaligned with users, since they are capable of providing minimum service at maximum profit despite being critical infrastructure for the network. This is because the market for miners permits private seigniorage. Once popular with kings in early modernity, seigniorage is the government's right to sell its money at a value higher than the cost of production. Today, seigniorage is usually (somewhat) offset by treasury bonds, which the government pays interest on. When the government does not fully pay for its seigniorage the result is a tax on its citizens. In a rational market, the
cost of producing Bitcoins through mining (see Chapter 4) should be at equilibrium with their value (with, presumably, a small profit incentive or the existence of altruist actors). This is not the case. For example, in 2017, with the rise in price of Bitcoin and availability of cheap electricity (especially in China), Bitcoin mining was so profitable that even if the price of Bitcoin dropped by half, miners could still earn seigniorage profits. Consequently, all non-mining Bitcoin users are in effect paying a tax equivalent to the difference between the cost of production and the market price.

Many of these issues highlight the difficulty of using cryptocurrencies and blockchains. Even after ten years of development the software ecosystem has failed to provide simple and robust tools. As I mentioned above, early on Bitcoin ATMs were supposed to bring Bitcoin to the masses, but with their comical complexity and long processing wait times (upwards of 10 minutes when the network was running well), they did not catch on. Most of the Bitcoin ATMs I have seen personally were constantly managed by nearby attendants. Users also need to possess a deep understanding of computer security to safely use cryptocurrencies, and even small errors can have disastrous and irreversible consequences. There are many stories of users accidently sending Bitcoin to the wrong address or making other simple mistakes, such as mixing up the payment and fee fields during a transaction, which led one poor person in 2016 to pay a US $130,000 fee for a US $5 transfer. Of course, such transactions cannot be reversed or changed, since there are no bank errors or mulligans in Bitcoin. Even if simple errors are avoided, due to the high value of Bitcoin, user pseudonymity, and irreversible transactions, Bitcoin wallets are frequent targets for hackers. Bitcoin hacking is so widespread that many spyware tools now look specifically for locally stored Bitcoin wallets. Because of rampant hacking, recommended best practice is to only store Bitcoin on computers that are completely offline (and, ideally, have never been online). Users
with large caches must go to paranoiac levels to secure their Bitcoin. For example, Cameron and Tyler Winklevoss store their Bitcoin billions on paper printouts in safe deposit boxes around the US, with each printout containing only part of the needed private key (Popper 2017b). This is not entirely dissimilar to how US nuclear launch codes are stored. As critic David Gerard (2017) points out, Bitcoin users need to be their own bank, which includes being their own chief security officer—a task few are equipped for.

The uncompromising design of Bitcoin means it is just as bad to lose Bitcoin to hackers as it is to forget the private key. In recent years a small cottage industry has emerged to help the forgetful recover their lost Bitcoins. The famous story of a man who in 2013 pitched an old hard drive containing his Bitcoin wallet had a 2017 update: with soaring Bitcoin prices he considered *excavating the landfill* with hopes of recovering his millions (Sulleyman 2017). Others who have simply forgotten the private key wrack their brains with hopes of unlocking their fortunes—even turning to hypnosis (Frauenfelder 2017). In most cases, however, it is hard to feel too sorry for these people. Many earned Bitcoins in the early days when they were effectively worthless, often by mining on a home computer. That they forgot about their Bitcoins until years later when they had increased 100 or 1,000 times in value and then were unable to access their newfound wealth is personally unfortunate but hardly a moral travesty. This also means that when Bitcoins are lost they are lost *forever*. Therefore, of the total twenty-one million Bitcoins that will be issued (a strict monetary cap programmed into the Bitcoin protocol), an estimated four million have already been permanently lost (Roberts & Rapp 2017; see also Swanson 2014).

Finally, the privacy protections of cryptocurrencies and blockchains are simultaneously too strong, too weak, and inflexible. Despite the de-anonymizing research being conducted on Bitcoin transactions, in practical terms a careful user can effectively conduct anonymous transactions that
even state intelligence agencies are unable to disentangle. For example, when the US Federal Bureau of Investigation (FBI) sought the owner and operator of the infamous Silk Road dark web marketplace ("Dread Pirate Roberts") they could plainly see Bitcoin going in and out of the marketplace, but the trail of transactions left few clues. It was only in discovering an early forum post announcing the Silk Road website that led the FBI to Ross Ulbricht, who was then convicted. Access to Ulbricht's stored Bitcoin helped make the case against him, but most of the evidence that tied Ulbricht to Dread Pirate Roberts came from the laptop seized during his arrest. On the other hand, the privacy protections of Bitcoin and most cryptocurrencies are not robust or flexible enough for many legal uses, such as for use with health information or national identity schemes. In real-world use cases, considerable privacy flexibility is needed and simple privacy maximizing approaches are inappropriate. For example, in the US, the Health Insurance Portability and Accountability Act (HIPAA) permits "break the glass" procedures to allow access to health records in emergency situations but requires robust privacy otherwise. In the EU, however, the "right to be forgotten" offers privacy protections that most cryptocurrencies are unable to comply with given their all-or-nothing design for records immutability (and with the passing of the EU General Data Protection Regulation, or GDPR, many blockchain companies face stiff penalties if they cannot accommodate nuanced privacy protections; see Chapter 6). Flexible blockchain technologies designed with privacy regulation in mind may be able to accommodate these kinds of issues, but these have yet to reach widespread adoption.

Summary

This chapter introduced cryptocurrencies, focusing on Bitcoin, the first cryptocurrency. I traced the origins of Bitcoin through alternative currency projects and the cypherpunk
community from which it originated. I described the context of Bitcoin as a currency system built on a distributed ledger. This description set up the next two chapters, where I complete the picture by detailing the intersection between the monetary aspirations of Bitcoin and the innovative distributed ledger that the system relies on (Chapter 3), an essential part of a network of computers that validate and secure the entire system (Chapter 4). I concluded this chapter by describing the recent turn away from monetary uses of cryptocurrencies, while recognizing that the distinction between cryptocurrencies and blockchains is fluid. Bitcoin and other cryptocurrencies have not yet been successfully adopted as money because of remaining usability issues, an uncertain regulatory climate, and the technical challenge of developing a robust and secure decentralized platform.