PART One

Introduction and Economics

CHAPTER 1
Foundations

There has been ample media coverage of Bitcoin, and many public figures have been compelled to state their opinion. As Bitcoin is a complex topic, covering cryptography, software engineering and economics, it is difficult to grasp its essence and implications with only a superficial look at it. Thus some commentators might not have a clear picture of how it works and the implications. It is the goal of this book to equip the reader with the knowledge to evaluate the merits of this technology.

Figure 1.1 summarizes some misconceptions around Bitcoin.

Bitcoin is a decentralized digital currency. This means there is no person or institution behind it, either backing it or controlling it. Neither is it backed by physical goods, such as precious metals. This might seem counter-intuitive at first glance: how could it exist if no one controls it? Who created it then? How did the creator lose control over it?

The answer to this seeming paradox is that Bitcoin is just a computer program. How exactly this computer program works is the subject of the second part of this book. The program has a creator (or creators) but his identity is unknown as he released the Bitcoin software using what is believed to be a pseudonym: Satoshi Nakamoto. Bitcoin is not controlled in a tight sense by anyone. The creator did not lose control of it because he

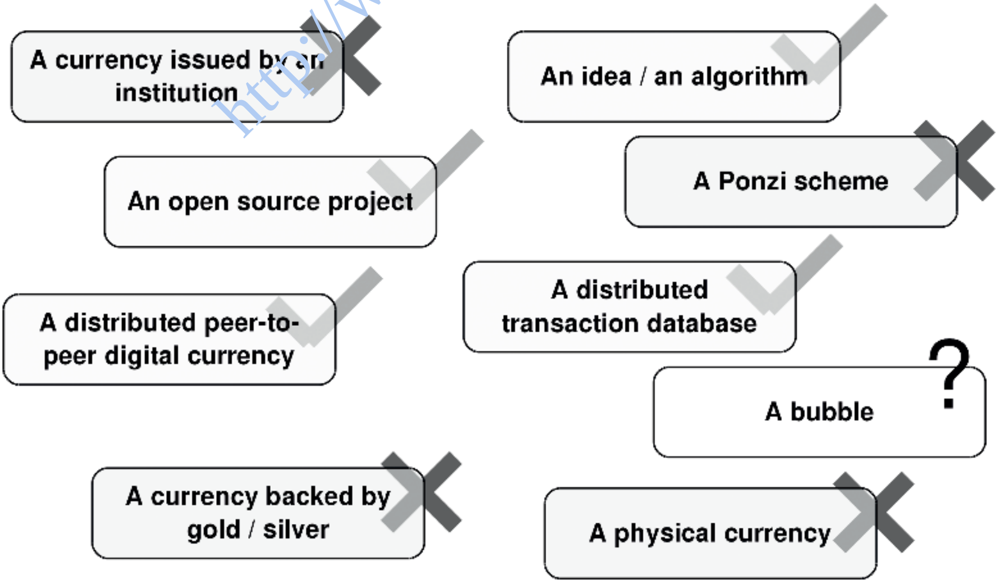
A currency issued by an institution
An idea / an algorithm
An open source project
A Ponzi scheme
A distributed peer-to-peer digital currency
A distributed transaction database
?
A bubble
A currency backed by gold / silver
A physical currency

FIGURE 1.1 What Bitcoin is (and isn't)

(she?, they?) never owned the code. The code is **open source** and thus it belongs to the public domain, as will be further explained in section 1.2.

One of the most innovative features of Bitcoin is that it is **decentralized**. There is no central server where Bitcoin is running. Bitcoin operates through a peer-to-peer network of connected computers. Bitcoin is the first digital currency built in a decentralized way, a technological breakthrough. The decentralized nature of Bitcoin will be further explored in section 1.1.

Bitcoin creates its own currency called bitcoin, with a small b. The creation of a currency is integral to how the system operates, as it serves two simultaneous purposes. First, it serves to represent value. Second, issuance of new bitcoins is used to reward operators in the network for securing the distributed ledger. These two functions cannot be unbundled without significantly changing the design.

The heart of the Bitcoin network is a database holding the transactions that have occurred in the past as well as the current holders of the funds. This database is sometimes called a ledger, because it holds the entries representing the owners of the funds. Bitcoin is not the first distributed database to be created. However, the requirements of a financial database are different from those of other applications, such as file sharing or messaging systems. In particular, financial databases must be resilient against users trying to double-spend their funds, which Bitcoin solves elegantly. This is explored in the following sections and in Chapter 2.

Some critics have argued that Bitcoin is a **Ponzi scheme**. **It is not.** In a Ponzi scheme there is a central operator who pays returns to current investors from new capital inflows. First of all, in Bitcoin there is no central operator who can profit from the relocation of funds. Second, there is no mechanism to deflect funds from new investments to pay returns. The only funds recognized in the Bitcoin protocol are bitcoins, the currency. Transfers of bitcoins are initiated by the users at their will: the protocol cannot deflect funds from one user to another. Third, a new investment in Bitcoin is always matched with a disinvestment. Investors who put money into bitcoins usually operate through an exchange where they buy the bitcoins from another investor who is selling her investment. There is simply no new investment flowing into bitcoins: the amount of sovereign currency that has flown into bitcoins exactly matches the amount that has flown out of bitcoins.

However, bitcoin, the currency, can be a bubble. Whether the value of bitcoin crashes, holds, or increases depends on whether bitcoins will be used in the future for different applications. There are several interesting applications for Bitcoin, of which the most straightforward (but not the only) are to serve as a medium of exchange and a store of value. It is too early to tell whether any of these applications will become important in the future. The merits of bitcoins as medium of exchange and store of value are explored in Chapter 3.

Finally, Bitcoin is not just a currency but a whole infrastructure that can be used to transfer value digitally: see section 1.4 and Chapter 12.

1.1 DECENTRALIZED

Most currencies in use today are fiat currencies, where the currency is issued by the government and its supply managed by a central bank.

FIAT MONEY

Most currencies today (Euro, US Dollar) are fiat money. Fiat money does not have intrinsic value, as it is not backed by anything. It is called fiat money because there is a government decree ("fiat") declaring the currency to be legal tender. The acceptance of fiat money depends on expectations and social convention. If confidence in a currency is lost, usually because of irresponsible monetary policy, fiat money can stop being accepted.

Experience has shown that leaving monetary policy in the hands of governments is usually not a good idea, as governments could have an incentive to increase the monetary supply to solve pressing short-term financial problems. This behavior can lead to high inflation and a loss of confidence in the currency.

The conventional solution is to entrust monetary policy to a semi-independent central bank. The central bank is tasked with managing the monetary policy, usually with the goals of economic growth, price stability, and, in some cases, stability of the financial system.

Bitcoin is based on a peer-to-peer network of computers running the software. These computers are called nodes. Participants in the network might be running nodes for different reasons: for profit as in the case of miners (Chapter 9), to manage full-node wallets (Chapter 8), to collect and study information about the network (Chapter 13), or simply as a social good.

Bitcoin's decentralized nature contrasts to the structure of fiat currencies. Central banks make monetary decisions after evaluating evidence gathered from the evolution of the economy. In a decentralized system such as Bitcoin, discretionary decisions are not possible. The original creators of the system have to take most of the decisions upfront at the design phase. These decisions have to be carefully balanced, and take into account the incentives of the different users, otherwise the decentralized system is doomed to fail. In Bitcoin the monetary policy follows a simple rule: the final monetary base is fixed at around 21 million bitcoins and new bitcoins are minted at a planned schedule and paid to users who help secure the network. This serves the double purpose of providing the bitcoins with value due to their scarcity and creating incentives for users to connect to the network and help secure it by providing their computational power.

Control in a centralized system is usually concentrated in an institution or a small group of key people. Thus changes in a centralized system are relatively straightforward to decide and implement. Control in a peer-to-peer network is more subtle: changes in a peer-to-peer network have to be agreed by a majority of the peers at least. But even then, if a strong minority does not agree to a change, implementing the change can be technically challenging as the network runs the risk of a split.

One advantage of the decentralization of power is that changes that are contrary to the interests of most users would be rejected. In contrast, in centralized systems sometimes the outcomes are adverse to most of the participants, as in a currency debasement by excessive printing which usually leads to high inflation.

Another feature of decentralized systems is their resilience. Decentralized systems are robust against attacks either by insiders or by external forces. This feature might have been critical for the existence of Bitcoin. Earlier centralized attempts to create digital currencies (section 2.1) were forced down by governments. However, to force down a decentralized system, all individual users must be forced down, which is a much harder task. Bitcoin's peer-to-peer nature makes it censorship-resistant, claim its supporters.

The technology to securely (cryptographically) transfer value digitally had been available many years before the creation of Bitcoin (Chapter 10). However, it had always required the creation of a centralized trusted party. Bitcoin not only does not require a central trusted party to operate, but it is also designed to resist the attacks of malicious participants in the peer-to-peer network. As long as these malicious participants do not control a majority of the network these attacks will not succeed (section 7.5).

The main technological breakthrough accomplished by Bitcoin is solving the double-spending problem in a distributed financial database. A double-spend attempt occurs when a user tries to spend some funds twice. All financial systems must reject these attempts. This is relatively straightforward in a centralized system, as transactions are recorded in a central database and future spending attempts are checked against this database first. In a decentralized system, many copies of the database are shared among the peers, and keeping a consistent state of the database is a difficult computational problem[1]. In the context of Bitcoin the problem is how the network can agree on the state of the distributed database when messages between the nodes can be corrupted and there might be attackers trying to subvert the distributed database. Bitcoin gracefully solves this problem (section 2.3 and Chapter 7).

1.2 OPEN SOURCE

Bitcoin is open source software. **Open source** software makes the source code available for anyone to use, modify, and redistribute free of charge. Some well-known open source software products include the Linux and Android operating systems or the Firefox web browser. A large portion of the internet infrastructure runs on less known (but no less important) open source software. The goal of open source is to make software development similar to academic peer-reviewed research. By publishing the source code for anyone to see and check, open source aims to increase the quality of the software.

The difference between open source software and proprietary software lies in their licenses. A proprietary software license grants the right to use a copy of the program to the end user. However, ownership of the software remains with the software publisher. In contrast, an open source license grants the user the right to use, copy, modify, and redistribute the software. The copyright of the software remains with the creator, but the creator of an open source software transfers the rights to the user as long as the obligations of the license are met.

Another difference between proprietary and open source programs is that proprietary programs are usually distributed as compiled binaries. This means that the software is usually distributed in machine language. Users willing to gain knowledge on what the software is doing must interpret the machine code in a time-consuming process called reverse engineering (Eilam, 2005). Most proprietary licenses forbid the use of these reverse

[1] This computational problem is called the Byzantine Generals' problem, introduced in Lamport et al. (1982).

engineering techniques. Thus under a proprietary license the user is usually not allowed to understand or seek knowledge of what the software is actually doing. In contrast, open source software is always distributed with a copy of the source code. A user who wants to understand what the software is doing can just read the source code. Cryptographic open source software has the advantage that it allows users to check that the code does not contain any backdoor or security vulnerabilities[2].

It is unlikely that Bitcoin could have been released under a proprietary license. Had Bitcoin been released as closed-source, its creator could have easily inserted code that deviated from the specification: say, creating new bitcoins and sending them to an address controlled by him. Most users presumably would not have accepted decentralized cryptographic financial software distributed as a compiled binary and with a proprietary license. It is telling that most competing cryptocurrencies (Chapter 11, section 12.7), have either been launched using an open source license or have switched to an open source license.

Open source licenses grant the user the right to use, copy, modify, and redistribute the software. Different licenses may impose different obligations on the users. Broadly speaking, open source licenses belong to one of two families:

- **"Copyleft."** These licenses impose the obligation to distribute derived works under the same license. If a user of the software makes modifications to it, she is obliged to release the modified software under the same license. This is referred to as the share-alike requirement. Thus "copyleft" licenses preserve the open source nature of the software as it is modified. An example of a "copyleft" license is the **GNU Public License** (**GPL**).
- **"Permissive."** These licenses impose very few restrictions on the redistribution of the software, usually just that the derived software acknowledges the original software and retains the copyright notice. Proprietary software that incorporates software released under an open source permissive license retains its proprietary nature as the license usually only requires that the proprietary software includes the copyright notice. Several common open source licenses belong to this family, such as the BSD license, the MIT License or the Apache License. Bitcoin was released under the MIT license.

Proprietary software requires that the company issuing the software maintains and updates it. In contrast, open source software acquires a life of its own once released. It usually does not matter if an original creator decides to stop working on an open source project, as other developers could take it over. For this reason it does not matter who Satoshi Nakamoto is, or that he has moved on. Open source projects are resilient: even if some developers are forbidden or discouraged to work on a project, other developers from all around the world can take over.

[2] This should not be interpreted that open source code does not contain security flaws or backdoors. Indeed, many security flaws have been found in open source projects (Green, 2014b; Poulsen, 2014). Open source advocates argue that it is more difficult to include flaws and backdoors into open source programs because there is a higher level of scrutiny, and that these flaws are typically discovered and repaired sooner than similar flaws placed in proprietary software (Raymond, 2001).

Under an open source license it is legitimate to start a new independent software project from a copy of an original project. This process is called **forking**. The threat of a fork can often keep the developers of an open source project honest. If the developers of a project introduce changes that are detrimental to the users of the software, anybody can create a fork, undo those changes and continue the development. Users will most likely follow the fork without the undesired features. Thus forking can be seen as a kill switch that prevents developers from evolving a project against their users. Most large open source projects are rarely forked[3]. Bitcoin is somewhat special in this respect, as it has been forked many times by developers wishing to test new concepts. This has given rise to many alternative cryptocurrencies called alt-coins. Alt-coins will be covered in more detail in Chapter 11.

Open source advocates argue that companies releasing proprietary software often lose the incentive to innovate once a product has achieved a dominant market position. Many software markets behave like natural monopolies where a product with first mover advantage can capture a large market share. Thus innovation in many software categories is low, these advocates suggest. In contrast, if an open source software captures the majority of the market this does not bring about the end of innovation, as anybody can keep on adding improvements to the software. Thus the pace of innovation in open source software can be higher than in closed source software.

One problem facing many open source projects is the **tragedy of the commons**. Although many people benefit from an open source project, few developers might have an incentive to contribute to it. Many open source projects face difficulties in getting appropriate funding or development time. There have been some indications that Bitcoin could be facing this problem (Bradbury, 2014b).

An exposition of the merits of open source software can be found in Raymond (2001).

1.3 PUBLIC ASSET LEDGER

The heart of Bitcoin is a distributed database that holds a copy of the common asset ledger. As this database is distributed, each participant in the network (a node) keeps a copy of it. Copies of this database kept by the different nodes are consistent by design.

On the other hand, every user is in control of her own funds, through a cryptographic private key. When a user wishes to spend some funds, she must use this private key to sign a message that states who she wishes to send the funds to as well as the amount to send. The user broadcasts this signed message to the network, and every participant in the network receives a copy of it. Then each node can independently verify the validity of the message and update its internal database accordingly[4].

[3] Most projects are really forked many times by individual users wishing to tinker with them or test new features. However, forks of large open source projects that split the developer base, such as the LibreOffice fork from OpenOffice (Paul, 2011), are rather rare.

[4] The process is actually more involved to prevent double-spending attacks where a user sends different messages to different parts of the network. How Bitcoin prevents double-spending attacks is the subject of Chapter 7.

In traditional financial systems, value is represented in ledgers (databases) managed by financial institutions. Users must place trust in these financial institutions that these databases will not be subverted either by insiders or by outside attackers. The protocols and procedures that safeguard traditional financial databases are not generally revealed to the public. In contrast, Bitcoin makes the database public and creates an open source software protocol to secure it. This protocol is designed to be resilient against attackers participating in the network. Bitcoin users do not need to place trust on any entity: the system is said to be trust-less.

All the financial information flowing through the Bitcoin network is public, except the identities behind the transactions. Bitcoin does not use personal information to identify the holders of funds, but Bitcoin addresses. Addresses are long strings of seemingly random letters and numbers, such as “13mckXcnnEd4SEkC27PnFH8dsY2gdGhRvM”. Bitcoin is like making everybody’s bank statements public online, but with the identity blacked out (Back, 2014b).

Although in principle there is no way to associate addresses to identities, there are many techniques to analyze the information flowing through the network and acquire different grades of knowledge about Bitcoin addresses and the users behind them (Chapter 13).

Bitcoin is not anonymous, and it can sometimes be less anonymous than the traditional payment systems. In the traditional payment system, for instance, an employer does not gain knowledge of where an employee spends her wage, although the employee’s bank has that information. If an employee were paid in bitcoins, her employer could see where she spends the money simply following the trail of transactions emerging from the address where the wage was sent to. The employee could follow some practices to hide this trail of transactions (Chapter 13).

In other cases, this transparency can be an advantage. One such example is the case of public entities where a transparent destination of funds could help increase the quality of the administration and help avoid corruption. In the case of commercial enterprises some level of transparency can be beneficial, for example financial statements that could be verified against the public ledger. There has been some technological progress towards achieving different levels of transparency in a public ledger system (section 8.5).

1.4 IT’S NOT ONLY THE CURRENCY, IT’S THE TECHNOLOGY

Transfer of value has traditionally been a slow and highly manual process. In essence, Bitcoin is a protocol to create distributed consensus. This protocol allows transferring value securely in a trust-less way: it is an open platform for money. But it is not only restricted to money: Bitcoin and similar protocols can transfer any digital asset (Chapter 12). The technology is cheaper and faster than most of the alternatives, creating opportunities for new applications.

The digital transfer of value enables the adoption of smart contracts. **Smart contracts** are contracts that do not require human interpretation or intervention to complete. Their settlement is done entirely by running a computer program. Smart contracts are math-based contracts, as opposed to law-based contracts. A trust-less digital transfer of value opens the door to new applications that make use of smart contracts.

One such application is autonomous agents. Autonomous agents should not be confused with artificial intelligence. Autonomous agents are just straightforward computer programs, created for a specific task. One example is a computer program running in the cloud that rents storage space and offers end users file-sharing services. Up until now computer programs could not hold value: a computer program presumably could not open a bank account in its name. With the introduction of Bitcoin, computer programs can control their own funds and sign smart contracts with cloud service providers to rent cloud storage and computing power. Similarly a storage agent could enter into smart contracts with its end users. The storage agent can settle these smart contracts, making bitcoin payments to the cloud provider and receiving bitcoin payments from its end users (Garzik, 2013a). A more extensive discussion of autonomous agents can be found in section 12.4.

Autonomous agents are just one example, and many more innovative ideas are being devised (Chapter 12). Some of these ideas may turn out not to be practical, but maybe a few could become mainstream. A decentralized system is an ideal test ground for these technologies, as innovators do not need the approval of anybody to try out their ideas: a decentralized system enables **permissionless innovation**.

Bitcoin is an API (Application Programming Interface) for money and bitcoin the currency is just the first application. Bitcoin could be used as an open platform for the exchange of value in much the same way that the internet is an open platform for the exchange of information. It can be used as a protocol on top of which applications can be built, much like email, web browsing, or voice-over-IP are built on top of the TCP/IP protocol. This is where most of the excitement around Bitcoin and related technologies comes from. Regardless of whether bitcoins have a future as currency, the technology has shown that many applications are now possible and innovators will continue to push forward with new ideas. Bitcoin could become a platform for financial innovation.

One of Ronald Coase's most important economic insights in *The Nature of the Firm* (Coase, 1937) was that one factor that contributed to the creation of firms was high transaction costs. If there were no transaction costs, an entrepreneur could contract any good she needs in the open market, and this would be efficient, as an efficient market would always achieve the best price for that good. However, transaction costs, such as information gathering, bargaining, policing the contract, keeping secrets and so on, can be a significant portion of the total cost of contracting out to the market. For this reason, it might be cheaper for an entrepreneur to hire some employees to produce the goods internally, thus starting a corporation. Transaction costs are also at the root of public goods and government action.

Bitcoin's technological breakthrough creates an opportunity to lower the costs of entering and upholding contracts, say through smart contracts. More efficient contracts thus have the potential to change corporations and government action.