SAIFEDEAN AMMOUS

THE BITCOIN STANDARD

The DECENTRALIZED ALTERNATIVE to CENTRAL BANKING

WILEY

THE BITCOIN STANDARD

THE BITCOIN STANDARD

The Decentralized Alternative to Central Banking

Saifedean Ammous

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data is Available:

ISBN 9781119473862 (Hardcover)
ISBN 9781119473893 (ePDF)
ISBN 9781119473916 (ePub)

Cover Design: Wiley
Cover Images: REI stone © Danita Delimont/Getty Images; gold bars © Grassetto/Getty Images; QR code/Courtesy of Saifedean Ammous

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

To my wife and daughter, who give me a reason to write.
And to Satoshi Nakamoto, who gave me something worth writing about.

Contents

About the Author

Saifedean Ammous is a Professor of Economics at the Lebanese American University and member of the Center on Capitalism and Society at Columbia University. He holds a PhD in Sustainable Development from Columbia University.

Foreword

by Nassim Nicholas Taleb

Let us follow the logic of things from the beginning. Or, rather, from the end: modern times. We are, as I am writing these lines, witnessing a complete riot against some class of experts, in domains that are too difficult for us to understand, such as macroeconomic reality, and in which not only is the expert not an expert, but he doesn't know it. That previous Federal Reserve bosses Greenspan and Bernanke, had little grasp of empirical reality is something we only discovered too late: one can macroBS longer than microBS, which is why we need to be careful of whom to endow with centralized macro decisions.

What makes it worse is that all central banks operated under the same model, making it a perfect monoculture.

In complex domains, expertise doesn't concentrate: under organic reality, things work in a distributed way, as F. A. Hayek has convincingly demonstrated. But Hayek used the notion of distributed knowledge. Well, it looks like we do not even need the "knowledge" part for things to work well. Nor do we need individual rationality. All we need is structure.

It doesn't mean all participants have a democratic share in decisions. One motivated participant can disproportionately move the needle (what I have studied as the asymmetry of the minority rule). But every participant has the option to be that player.

Somehow, under scale transformation, a miraculous effect emerges: rational markets do not require any individual trader to be rational. In fact they work well under zero intelligence—a zero-intelligence crowd, under the right design, works better than a Soviet-style management composed of maximally intelligent humans.

Which is why Bitcoin is an excellent idea. It fulfills the needs of the complex system, not because it is a cryptocurrency, but precisely because it has no owner, no authority that can decide on its fate. It is owned by the crowd, its users. And it now has a track record of several years, enough for it to be an animal in its own right.

For other cryptocurrencies to compete, they need to have such a Hayekian property.

Bitcoin is a currency without a government. But, one may ask, didn't we have gold, silver, and other metals, another class of currencies without a government? Not quite. When you trade gold, you trade "loco" Hong Kong and end up receiving a claim on a stock there, which you might need to move to New Jersey. Banks control the custodian game and governments control banks (or, rather, bankers and government officials are, to be polite, tight together). So Bitcoin has a huge advantage over gold in transactions: clearance does not require a specific custodian. No government can control what code you have in your head.

Finally, Bitcoin will go through hiccups. It may fail; but then it will be easily reinvented as we now know how it works. In its present state, it may not be convenient for transactions, not good enough to buy your decaffeinated espresso macchiato at your local virtue-signaling coffee chain. It may be too volatile to be a currency for now. But it is the first organic currency.

But its mere existence is an insurance policy that will remind governments that the last object the establishment could control, namely, the currency, is no longer their monopoly. This gives us, the crowd, an insurance policy against an Orwellian future.

Nassim Nicholas Taleb
January 22, 2018

Prologue

On November 1, 2008, a computer programmer going by the pseudonym Satoshi Nakamoto sent an email to a cryptography mailing list to announce that he had produced a "new electronic cash system that's fully peer-to-peer, with no trusted third party."[1] He copied the abstract of the paper explaining the design, and a link to it online. In essence, Bitcoin offered a payment network with its own native currency, and used a sophisticated method for members to verify all transactions without having to trust in any single member of the network. The currency was issued at a predetermined rate to reward the members who spent their processing power on verifying the transactions, thus providing a reward for their work. The startling thing about this invention was that, contrary to many other previous attempts at setting up a digital cash, it actually worked.

While a clever and neat design, there wasn't much to suggest that such a quirky experiment would interest anyone outside the circles of cryptography geeks. For months this was the case, as barely a few dozen users worldwide were joining the network and engaging in mining and

[1] The full email can be found on the Satoshi Nakamoto Institute archive of all known Satoshi Nakamoto writings, available at www.nakamotoinstitute.org

sending each other coins that began to acquire the status of collectibles, albeit in digital form.

But in October 2009, an Internet exchange[2] sold 5,050 bitcoins for $5.02, at a price of $1 for 1,006 bitcoins, to register the first purchase of a bitcoin with money.[3] The price was calculated by measuring the value of the electricity needed to produce a bitcoin. In economic terms, this seminal moment was arguably the most significant in Bitcoin's life. Bitcoin was no longer just a digital game being played within a fringe community of programmers; it had now become a market good with a price, indicating that someone somewhere had developed a positive valuation for it. On May 22, 2010, someone else paid 10,000 bitcoins to buy two pizza pies worth $25, representing the first time that bitcoin was used as a medium of exchange. The token had needed seven months to transition from being a market good to being a medium of exchange.

Since then, the Bitcoin network has grown in the number of users and transactions, and the processing power dedicated to it, while the value of its currency has risen quickly, exceeding $7,000 per bitcoin as of November 2017.[4] After eight years, it is clear that this invention is no longer just an online game, but a technology that has passed the market test and is being used by many for real-world purposes, with its exchange rate being regularly featured on TV, in newspapers, and on websites along with the exchange rates of national currencies.

Bitcoin can be best understood as distributed software that allows for transfer of value using a currency protected from unexpected inflation without relying on trusted third parties. In other words, Bitcoin automates the functions of a modern central bank and makes them predictable and virtually immutable by programming them into code decentralized among thousands of network members, none of whom can alter the code without the consent of the rest. This makes Bitcoin the first demonstrably reliable operational example of *digital cash* and *digital hard money*. While Bitcoin is a new invention of the digital age, the problems it purports to solve—namely, providing a form of money that is

[2]The now-defunct New Liberty Standard.

[3]Nathaniel Popper, *Digital Gold* (Harper, 2015).

[4]In other words, in the eight years it has been a market commodity, a bitcoin has appreciated around almost eight million-fold, or, precisely 793,513,944% from its first price of $0.000994 to its all-time high at the time of writing, $7,888.

under the full command of its owner and likely to hold its value in the long run—are as old as human society itself. This book presents a conception of these problems based on years of studying this technology and the economic problems it solves, and how societies have previously found solutions for them throughout history. My conclusion may surprise those who label Bitcoin a scam or ruse of speculators and promoters out to make a quick buck. Indeed, Bitcoin improves on earlier "store of value" solutions, and Bitcoin's suitability as the sound money of a digital age may catch naysayers by surprise.

History can foreshadow what's to come, particularly when examined closely. And time will tell just how sound the case made in this book is. As it must, the first part of the book explains money, its function and properties. As an economist with an engineering background, I have always sought to understand a technology in terms of the problems it purports to solve, which allows for the identification of its functional essence and its separation from incidental, cosmetic, and insignificant characteristics. By understanding the problems money attempts to solve, it becomes possible to elucidate what makes for sound and unsound money, and to apply that conceptual framework to understand how and why various goods, such as seashells, beads, metals, and government money, have served the function of money, and how and why they may have failed at it or served society's purposes to store value and exchange it.

The second part of the book discusses the individual, social, and global implications of sound and unsound forms of money throughout history. Sound money allows people to think about the long term and to save and invest more for the future. Saving and investing for the long run are the key to capital accumulation and the advance of human civilization. Money is the information and measurement system of an economy, and sound money is what allows trade, investment, and entrepreneurship to proceed on a solid basis, whereas unsound money throws these processes into disarray. Sound money is also an essential element of a free society as it provides for an effective bulwark against despotic government.

The third section of the book explains the operation of the Bitcoin network and its most salient economic characteristics, and analyzes the possible uses of Bitcoin as a form of sound money, discussing some use

cases which Bitcoin does not serve well, as well as addressing some of the most common misunderstandings and misconceptions surrounding it.

This book is written to help the reader understand the economics of Bitcoin and how it serves as the digital iteration of the many technologies used to fulfill the functions of money throughout history. This book is not an advertisement or invitation to buy into the bitcoin currency. Far from it. The value of bitcoin is likely to remain volatile, at least for a while; the Bitcoin network may yet succeed or fail, for whatever foreseeable or unforeseeable reasons; and using it requires technical competence and carries risks that make it unsuited for many people. This book does not offer investment advice, but aims at helping elucidate the economic properties of the network and its operation, to allow readers an informed understanding before deciding whether they want to use it.

Only with such an understanding, and only after extensive and thorough research into the practical operational aspects of owning and storing bitcoins, should anyone consider holding value in Bitcoin. While bitcoin's rise in market value may make it appear like a no-brainer as an investment, a closer look at the myriad hacks, attacks, scams, and security failures that have cost people their bitcoins provides a sobering warning to anyone who thinks that owning bitcoins provides a guaranteed profit. Should you come out of reading this book thinking that the bitcoin currency is something worth owning, your first investment should not be in buying bitcoins, but in time spent understanding how to buy, store, and own bitcoins securely. It is the inherent nature of Bitcoin that such knowledge cannot be delegated or outsourced. There is no alternative to personal responsibility for anyone interested in using this network, and that is the real investment that needs to be made to get into Bitcoin.

Chapter 1

Money

Bitcoin is the newest technology to serve the function of money—an invention leveraging the technological possibilities of the digital age to solve a problem that has persisted for all of humanity's existence: how to move economic value across time and space. In order to understand Bitcoin, one must first understand money, and to understand money, there is no alternative to the study of the function and history of money.

The simplest way for people to exchange value is to exchange valuable goods with one another. This process of *direct exchange* is referred to as barter, but is only practical in small circles with only a few goods and services produced. In a hypothetical economy of a dozen people isolated from the world, there is not much scope for specialization and trade, and it would be possible for individuals to each engage in the production of the most basic essentials of survival and exchange them among themselves directly. Barter has always existed in human society and continues to this day, but it is highly impractical and remains only in

use in exceptional circumstances, usually involving people with extensive familiarity with one another.

In a more sophisticated and larger economy, the opportunity arises for individuals to specialize in the production of more goods and to exchange them with many more people—people with whom they have no personal relationships, strangers with whom it is utterly impractical to keep a running tally of goods, services, and favors. The larger the market, the more the opportunities for specialization and exchange, but also the bigger the problem of *coincidence of wants*—what you want to acquire is produced by someone who doesn't want what you have to sell. The problem is deeper than different requirements for different goods, as there are three distinct dimensions to the problem.

First, there is the lack of coincidence in scales: what you want may not be equal in value to what you have and dividing one of them into smaller units may not be practical. Imagine wanting to sell shoes for a house; you cannot buy the house in small pieces each equivalent in value to a pair of shoes, nor does the homeowner want to own all the shoes whose value is equivalent to that of the house. Second, there is the lack of coincidence in time frames: what you want to sell may be perishable but what you want to buy is more durable and valuable, making it hard to accumulate enough of your perishable good to exchange for the durable good at one point in time. It is not easy to accumulate enough apples to be exchanged for a car at once, because they will rot before the deal can be completed. Third, there is the lack of coincidence of locations: you may want to sell a house in one place to buy a house in another location, and (most) houses aren't transportable. These three problems make direct exchange highly impractical and result in people needing to resort to performing more layers of exchange to satisfy their economic needs.

The only way around this is through *indirect exchange*: you try to find some other good that another person would want and find someone who will exchange it with you for what you want to sell. That intermediary good is a *medium of exchange*, and while any good could serve as the medium of exchange, as the scope and size of the economy grows it becomes impractical for people to constantly search for different goods that their counterparty is looking for, carrying out several exchanges for each exchange they want to conduct. A far more efficient solution will

naturally emerge, if only because those who chance upon it will be far more productive than those who do not: a single medium of exchange (or at most a small number of media of exchange) emerges for everyone to trade their goods for. A good that assumes the role of a widely accepted medium of exchange is called money.

Being a medium of exchange is the quintessential function that defines money—in other words, it is a good purchased not to be consumed (a consumption good), nor to be employed in the production of other goods (an investment, or capital good), but primarily for the sake of being exchanged for other goods. While investment is also meant to produce income to be exchanged for other goods, it is distinct from money in three respects: first, it offers a return, which money does not offer; second, it always involves a risk of failure, whereas money is supposed to carry the least risk; third, investments are less liquid than money, necessitating significant transaction costs every time they are to be spent. This can help us understand why there will always be demand for money, and why holding investments can never entirely replace money. Human life is lived with uncertainty as a given, and humans cannot know for sure when they will need what amount of money.[1] It is common sense, and age-old wisdom in virtually all human cultures, for individuals to want to store some portion of their wealth in the form of money, because it is the most liquid holding possible, allowing the holder to quickly liquidate if she needs to, and because it involves less risk than any investment. The price for the convenience of holding money comes in the form of the forgone consumption that could have been had with it, and in the form of the forgone returns that could have been made from investing it.

From examining such human choices in market situations, Carl Menger, the father of the Austrian school of economics and founder of marginal analysis in economics, came up with an understanding of the key property that leads to a good being adopted freely as money on the market, and that is *salability*—the ease with which a good can be

[1] See Ludwig von Mises' *Human Action,* p. 250, for a discussion of how uncertainty about the future is the key driver of demand for holding money. With no uncertainty of the future, humans could know all their incomes and expenditures ahead of time and plan them optimally so they never have to hold any cash. But as uncertainty is an inevitable part of life, people must continue to hold money so they have the ability to spend without having to know the future.

sold on the market whenever its holder desires, with the least loss in its price.[2]

There is nothing in principle that stipulates what should or should not be used as money. Any person choosing to purchase something not for its own sake, but with the aim of exchanging it for something else, is making it de facto money, and as people vary, so do their opinions on, and choices of, what constitutes money. Throughout human history, many things have served the function of money: gold and silver, most notably, but also copper, seashells, large stones, salt, cattle, government paper, precious stones, and even alcohol and cigarettes in certain conditions. People's choices are subjective, and so there is no "right" and "wrong" choice of money. There are, however, consequences to choices.

The relative salability of goods can be assessed in terms of how well they address the three facets of the problem of the lack of coincidence of wants mentioned earlier: their salability across scales, across space, and across time. A good that is salable across scales can be conveniently divided into smaller units or grouped into larger units, thus allowing the holder to sell it in whichever quantity he desires. Salability across space indicates an ease of transporting the good or carrying it along as a person travels, and this has led to good monetary media generally having high value per unit of weight. Both of these characteristics are not very hard to fulfill by a large number of goods that could potentially serve the function of money. It is the third element, salability across time, which is the most crucial.

A good's salability across time refers to its ability to hold value into the future, allowing the holder to store wealth in it, which is the second function of money: *store of value*. For a good to be salable across time it has to be immune to rot, corrosion, and other types of deterioration. It is safe to say anyone who thought he could store his wealth for the long term in fish, apples, or oranges learned the lesson the hard way, and likely had very little reason to worry about storing wealth for a while. Physical integrity through time, however, is a necessary but insufficient condition for salability across time, as it is possible for a good to lose its value significantly even if its physical condition remains unchanged.

---

[2]Carl Menger, "On the Origins of Money," *Economic Journal*, vol. 2 (1892): 239–255; translation by C. A. Foley.

For the good to maintain its value, it is also necessary that the supply of the good not increase too drastically during the period during which the holder owns it. A common characteristic of forms of money throughout history is the presence of some mechanism to restrain the production of new units of the good to maintain the value of the existing units. The relative difficulty of producing new monetary units determines the hardness of money: money whose supply is hard to increase is known as *hard money*, while *easy money* is money whose supply is amenable to large increases.

We can understand money's hardness through understanding two distinct quantities related to the supply of a good: (1) the *stock*, which is its existing supply, consisting of everything that has been produced in the past, minus everything that has been consumed or destroyed; and (2) the *flow*, which is the extra production that will be made in the next time period. The ratio between the stock and flow is a reliable indicator of a good's hardness as money, and how well it is suited to playing a monetary role. A good that has a low ratio of stock-to-flow is one whose existing supply can be increased drastically if people start using it as a store of value. Such a good would be unlikely to maintain value if chosen as a store of value. The higher the ratio of the stock to the flow, the more likely a good is to maintain its value over time and thus be more salable across time.[3]

If people choose a hard money, with a high stock-to-flow ratio, as a store of value, their purchasing of it to store it would increase demand for it, causing a rise in its price, which would incentivize its producers to make more of it. But because the flow is small compared to the existing supply, even a large increase in the new production is unlikely to depress the price significantly. On the other hand, if people chose to store their wealth in an easy money, with a low stock-to-flow ratio, it would be trivial for the producers of this good to create very large quantities of it that depress the price, devaluing the good, expropriating the wealth of the savers, and destroying the good's salability across time.

I like to call this the *easy money trap*: anything used as a store of value will have its supply increased, and anything whose supply can be easily

[3]Antal Fekete, *Whither Gold?* (1997). Winner of the 1996 International Currency Prize, sponsored by Bank Lips.

increased will destroy the wealth of those who used it as a store of value. The corollary to this trap is that anything that is successfully used as money will have some natural or artificial mechanism that restricts the new flow of the good into the market, maintaining its value across time. It therefore follows that for something to assume a monetary role, it has to be costly to produce, otherwise the temptation to make money on the cheap will destroy the wealth of the savers, and destroy the incentive anyone has to save in this medium.

Whenever a natural, technological, or political development resulted in quickly increasing the new supply of a monetary good, the good would lose its monetary status and be replaced by other media of exchange with a more reliably high stock-to-flow ratio, as will be discussed in the next chapter. Seashells were used as money when they were hard to find, loose cigarettes are used as money in prisons because they are hard to procure or produce, and with national currencies, the lower the rate of increase of the supply, the more likely the currency is to be held by individuals and maintain its value over time.

When modern technology made the importation and catching of seashells easy, societies that used them switched to metal or paper money, and when a government increases its currency's supply, its citizens shift to holding foreign currencies, gold, or other more reliable monetary assets. The twentieth century provided us an unfortunately enormous number of such tragic examples, particularly from developing countries. The monetary media that survived for longest are the ones that had very reliable mechanisms for restricting their supply growth—in other words, *hard money*. Competition is at all times alive between monetary media, and its outcomes are foretold through the effects of technology on the differing stock-to-flow ratio of the competitors, as will be demonstrated in the next chapter.

While people are generally free to use whichever goods they please as their media of exchange, the reality is that over time, the ones who use hard money will benefit most, by losing very little value due to the negligible new supply of their medium of exchange. Those who choose easy money will likely lose value as its supply grows quickly, bringing its market price down. Whether through prospective rational calculation, or the retrospective harsh lessons of reality, the majority of money and wealth will be concentrated with those who choose the hardest and most

salable forms of money. But the hardness and salability of goods itself is not something that is static in time. As the technological capabilities of different societies and eras have varied, so has the hardness of various forms of money, and with it their salability. In reality, the choice of what makes the best money has always been determined by the technological realities of societies shaping the salability of different goods. Hence, Austrian economists are rarely dogmatic or objectivist in their definition of sound money, defining it not as a specific good or commodity, but as whichever money emerges freely chosen on the market by the people who transact with it, not imposed on them by coercive authority, and money whose value is determined through market interaction, and not through government imposition.[4] Free-market monetary competition is ruthlessly effective at producing sound money, as it only allows those who choose the right money to maintain considerable wealth over time. There is no need for government to impose the hardest money on society; society will have uncovered it long before it concocted its government, and any governmental imposition, if it were to have any effect, would only serve to hinder the process of monetary competition.

The full individual and societal implications of hard and easy money are far more profound than mere financial loss or gain, and are a central theme of this book, discussed thoroughly in Chapters 5, 6, and 7. Those who are able to save their wealth in a good store of value are likely to plan for the future more than those who have bad stores of value. The soundness of the monetary media, in terms of its ability to hold value over time, is a key determinant of how much individuals value the present over the future, or their *time preference*, a pivotal concept in this book.

Beyond the stock-to-flow ratio, another important aspect of a monetary medium's salability is its acceptability by others. The more people accept a monetary medium, the more liquid it is, and the more likely it is to be bought and sold without too much loss. In social settings with many peer-to-peer interactions, as computing protocols demonstrate, it is natural for a few standards to emerge to dominate exchange, because the gains from joining a network grow exponentially the larger the size of the network. Hence, Facebook and a handful of social media networks

[4]Joseph Salerno, *Money: Sound and Unsound* (Ludwig von Mises Institute, 2010), pp. xiv–xv.

dominate the market, when many hundreds of almost identical networks were created and promoted. Similarly, any device that sends emails has to utilize the IMAP/POP3 protocol for receiving email, and the SMTP protocol for sending it. Many other protocols were invented, and they could be used perfectly well, but almost nobody uses them because to do so would preclude a user from interacting with almost everyone who uses email today, because they are on IMAP/POP3 and SMTP. Similarly, with money, it was inevitable that one, or a few, goods would emerge as the main medium of exchange, because the property of being exchanged easily matters the most. A medium of exchange, as mentioned before, is not acquired for its own properties, but for its salability.

Further, wide acceptance of a medium of exchange allows all prices to be expressed in its terms, which allows it to play the third function of money: *unit of account*. In an economy with no recognized medium of exchange, each good will have to be priced in terms of each other good, leading to a large number of prices, making economic calculations exceedingly difficult. In an economy with a medium of exchange, all prices of all goods are expressed in terms of the same unit of account. In this society money serves as a metric with which to measure interpersonal value; it rewards producers to the extent that they contribute value to others, and signifies to consumers how much they need to pay to obtain their desired goods. Only with a uniform medium of exchange acting as a unit of account does complex economic calculation become possible, and with it comes the possibility for specialization into complex tasks, capital accumulation, and large markets. The operation of a market economy is dependent on prices, and prices, to be accurate, are dependent on a common medium of exchange, which reflects the relative scarcity of different goods. If this is easy money, the ability of its issuer to constantly increase its quantity will prevent it from accurately reflecting opportunity costs. Every unpredictable change in the quantity of money would distort its role as a measure of interpersonal value and a conduit for economic information.

Having a single medium of exchange allows the size of the economy to grow as large as the number of people willing to use that medium of exchange. The larger the size of the economy, the larger the opportunities for gains from exchange and specialization, and perhaps more significantly, the longer and more sophisticated the structure of production

can become. Producers can specialize in producing capital goods that will only produce final consumer goods after longer intervals, which allows for more productive and superior products. In the primitive small economy, the structure of production of fish consisted of individuals going to the shore and catching fish with their bare hands, with the entire process taking a few hours from start to finish. As the economy grows, more sophisticated tools and capital goods are utilized, and the production of these tools stretches the duration of the production process significantly while also increasing its productivity. In the modern world, fish are caught with highly sophisticated boats that take years to build and are operated for decades. These boats are able to sail to seas that smaller boats cannot reach and thus produce fish that would otherwise not be available. The boats can brave inclement weather and continue production in very difficult conditions where less capital-intensive boats would be docked uselessly. As capital accumulation has made the process longer, it has become more productive per unit of labor, and it can produce superior products that were never possible for the primitive economy with basic tools and no capital accumulation. None of this would be possible without money playing the roles of medium of exchange to allow specialization; store of value to create future-orientation and incentivize individuals to direct resources to investment instead of consumption; and unit of account to allow economic calculation of profits and losses.

The history of money's evolution has seen various goods play the role of money, with varying degrees of hardness and soundness, depending on the technological capabilities of each era. From seashells to salt, cattle, silver, gold, and gold-backed government money, ending with the current almost universal use of government-provided legal tender, every step of technological advance has allowed us to utilize a new form of money with added benefits, but, as always, new pitfalls. By examining the history of the tools and materials that have been employed in the role of money throughout history, we are able to discern the characteristics that make for good money and the ones that make for bad money. Only with this background in place can we then move on to understand how Bitcoin functions and what its role as a monetary medium is.

The next chapter examines the history of obscure artifacts and objects that have been used as money throughout history, from the Rai stones of Yap Island, to seashells in the Americas, glass beads in Africa,

and cattle and salt in antiquity. Each of these media of exchange served the function of money for a period during which it had one of the best stock-to-flow ratios available to its population, but stopped when it lost that property. Understanding how and why is essential to understanding the future evolution of money and any likely role Bitcoin will play. Chapter 3 moves to the analysis of monetary metals and how gold came to be the prime monetary metal in the world during the era of the gold standard at the end of the nineteenth century. Chapter 4 analyzes the move to government money and its track record. After the economic and social implications of different kinds of money are discussed in Chapters 5, 6, and 7, Chapter 8 introduces the invention of Bitcoin and its monetary properties.