Business Economics
https://doi.org/10.1057/s11369-021-00236-1

NABE
National Association for Business Economics

BOOK REVIEW

# Fabian Schär and Aleksander Berentsen: *Bitcoin, Blockchain, and Cryptoassets: A Comprehensive Introduction*

## The MIT Press, 2020

**Rodney Garratt**[1]



*"Everything you don't understand about money combined with everything you don't understand about computers."* John Oliver's description of Bitcoin on Last Week Tonight with John Oliver, March 2018.

Money is imperfect. Fiat currencies, specifically cash in your pocket, differ from country to country and are typically not directly usable outside national borders. They are available in fixed denominations, which must be aggregated to make transactions and then reaggregated to make change. It is difficult to transport and protect large quantities of cash. Moreover, the receiver must be able to detect counterfeits. Transactions in cash are generally untraceable and anonymous.

Book-entry money (think balances in commercial bank accounts) has the potential to circumvent most of these deficiencies. Banks can transfer balances electronically and cheaply in any amount. But transacting requires the actions of a third party: a central authority that keeps records and ensures validity. Transactions are now traceable and sometimes reversible, which can be a good thing when errors are made or money is stolen.

But book-entry money is not the same as teleporting cash. Imagine you could teleport a 1-dollar bill or 1 billion dollars in cash anywhere in the world, instantly. Would that be better? To some it would be, but is it possible? Teleportation transfers matter from one point to another without traversing the physical space between them, but it only exists in science fiction.[1] I could send a digital image of my bills to a recipient, but how do we solve the double-spending problem? That is, how do we make sure that a particular person is the legitimate owner of the value they are sending, and that, once they send it to someone else, they cannot send it again? Answering this question is the main purpose of this book.

The book is divided into three parts. Part I is a non-technical introduction that includes a discussion of the original motivation for Bitcoin, what makes Bitcoin different from other monies, and how Bitcoin works, in a simplified way. Part II covers the technical aspects of Bitcoin and other cryptoassets. Part III addresses challenges (high price volatility, scalability, energy consumption and regulatory uncertainty) and non-monetary applications. This structure is a wonderful strategy. A reader seeking a broad overview can read Parts I and III. If, in the process of thinking about or dealing with various aspect of cryptocurrencies, you want to really know how something works, then you should be able to find a serious explanation in Part II.

In writing this book the authors grasped a profound concept: to help people understand Bitcoin it is crucial to first help them understand money. The book provides a brief journey though the origins of money, identifying the properties of money, what gives money value, and how this value depends on competition in money creation. The key idea here, of course, is scarcity. Monopolized money systems ensure scarcity by limiting the supply of money. The ability of the monopoly provider to adjust quantities of money, and hence its value, can be socially advantageous. But it can also be a temptation. At this point the authors introduce the most important word in money and banking: "trust." Not surprisingly, attention quickly turns to abuses of this trust: a plot of the real value of money over time in Argentina. The authors point out that while Argentina may be one of the largest abusers of this trust in recent memory, many other countries, including developed ones, have devalued their money over the last 60 years. They refer to this as the Honey Pot

✉ Rodney Garratt
garratt@ucsb.edu

[1] University of California, Santa Barbara, Santa Barbara, CA, USA

[1] I am using the fictional definition of teleportation, not the process of moving an object or person by psychokinesis.

Published online: 12 August 2021

problem. Essentially, central banks are honey pots that are not high enough on the shelf to be out of reach of governments. More literally, they argue central banks do not have sufficient independence from governments, in many cases, to provide "censorship-resistant governance." Bitcoin, in stark contrast, because of its decentralized structure, does.

Before commencing with their discussion of Bitcoin, the authors' conceptual money train makes one last stop. They discuss fractional reserve banking. The authors skillfully describe the distinction between cash and commercial bank money, and recognize a fact that many who are contemplating the creation of central bank digital currency should recognize: most people don't know the difference. Here I would make one very small criticism, which is in the form of identifying a missed opportunity: the authors mention, but do not, I would argue, sufficiently emphasize the importance of the "singleness of the currency" in our fractional reserve banking systems.[2] This is the idea that a dollar is a dollar regardless of the institution that issues it or physical form. This singleness is by no means guaranteed, but rather is a major triumph of central banks.[3]

The initial dialogue on money ends with a discussion of physical versus virtual money. The former is associated with possession, while the latter (at least in complex systems) requires the existence of a ledger.[4] The question of how to maintain this ledger is the launching point for the introduction to Bitcoin.

At the heart of this discussion is the explanation of proof-of-work. Proof-of-work was the final piece of the puzzle that allowed Bitcoin to function as a completely decentralized system. Proof-of-work eliminates the need for a trusted book-keeper. Instead of trusting an individual to keep an honest and accurate record of transactions, this faith is placed in the blockchain. The description here is clear and comprehensible, and it provides a very natural segue into a discussion on origin and governance. The authors start with a discussion of David Chaum's DigiCash, which is a great choice because it speaks not only to original uses of cryptography, but also the broader intent of, and in some eyes need for, Bitcoin.[5] DigiCash provided privacy (my transactions could not be attributed to me), but it did not provide anonymity (the bank still knew who I was) and, perhaps more importantly to some, there was a bank; i.e., it was still a centrally operated system. Bitcoin, in contrast, is decentralized—no one is in charge and perhaps surprisingly to some, the creator has "no privileges within the system and has become irrelevant owing to the disclosure of the information as well as subsequent technological development by other people" (p. 49). The authors' discussion of how protocol changes are made with no one in charge is excellent. It skillfully draws in the human aspect and explains how organizational structures still seem to be present. But ultimately changes are made through group acceptance. Individuals can suggest but not impose changes. There is no one who as the authority to implement a change. Changes are initiated and they succeed or fail depending on the collective will of the Bitcoin community.

Throughout the book, the authors return to the theme of trust. In centralized systems, confidence is obtained through a trust relationship between users and the center that is carefully cultivated over time and supported by regulation, supervision, and procedural safeguards. Such a relationship is also enforced by economic incentives: financial institutions recognize that trust is hard to gain, and easy to lose. In decentralized networks "reputational effects are practically nonexistent…The network participants will only comply with the consensus protocol if it is in their own interests" (p. 70). Much of what the book covers in the middle chapters can be described as the authors' successful attempt to explain why participants in the Bitcoin system do what they are supposed to.

The willingness of participants to do things that help the network (e.g., run a full node) is nicely formulated as a private provision of public goods problem. The authors explain how failure to provide the public good pushes the system in the direction of becoming more centralized. In fact, the authors explain that there seem to be many forces that are pushing Bitcoin in the direction of centralization. Most clients connect to centralized subnetworks that provide wallet services.[6] Pool mining also leads to centralization as miners sell power to the pool operator and no longer have to run a full node. Tendencies toward centralization conflict with the goal of censorship-resistant governance. In fact, in explaining the process by which Bitcoin transactions are validated the authors point out that while there is no central authority in the Bitcoin network, there is still a potential for blacklisting (p. 122).[7]

[2] The phrase "singleness of the currency" appears in Bank for International Settlements (2003).

[3] In fact, the singleness of the currency is so ingrained in many banking systems that the indemnity of deposit insurance contracts is an equivalent value of deposits at another (solvent) institution. The authors mention that this is true in Switzerland, and it is also true in other countries.

[4] Kahn and Roberds (2009) were the first to highlight that a key distinction between physical and virtual forms of money is that in the former case transaction verification requires verifying the object while in the latter case it requires verifying the identity of transactors.

[5] I take some pleasure in reporting that David Chaum's affiliation in the 1982 paper cited by the authors is the University of California, Santa Barbara, although we never overlapped.

[6] In such cases the user does not have direct access to the Bitcoin network and instead relies on their "host" (p. 77).

[7] See Garratt (2015) for a related discussion.

There are several other worthwhile aspects that emerge from the discussion of the technology that makes proof-of-work cryptocurrencies work. These include the economic incentives of miners, a description of equilibrium in mining and the economic incentives for a 51% attack, whereby a group that controls more than 50% of a network's hashing power attempts to alter the blockchain.[8] One aspect of this technical discussion that deserves highlighting is the implications for real-time payments. The move toward faster payments is something that is at the forefront of modernization efforts of conventional payment platforms. As the authors explain, until a payment is encoded in a block it is easy for someone to double-spend the coin, which leads to a non-negligible chance that the original transaction will be invalidated (p. 170). The authors identify some solutions to this problem, but the acceptance of some delay remains a necessary burden of trustless payments.

While much of the book addresses how Bitcoin works, there is ample discussion of its performance. One issue they address is the fact that the Bitcoin protocol is open-source and hence it can be duplicated. In fact, there are many close substitutes in existence that compete with Bitcoin. The authors argue Bitcoin still maintains scarcity, as there can only be one original Bitcoin and copies are easy to identify. However, price volatility is still a problem. As demonstrated in Garratt and Wallace (2018), kindly cited by the authors, there is great indeterminacy in the price of Bitcoin units and 0 is always going to be one option.[9] Even sticking to one equilibrium path, an inherent feature of Bitcoin's inelastic supply (there is no stabilization mechanism in the protocol) is that fluctuations in market demand necessarily lead to unhampered price fluctuations. This leads the authors to a discussion of stablecoins.

Different stablecoin concepts are discussed. The overarching lesson is that centralization tends to creep into most stablecoin concepts. The conclusion is that no privately-created stablecoin concept is perfect. Does this open the door for central bank digital currency (CBDC)?

Given the high level of current interest in CBDCs, it is appropriate that the authors weigh in on the issue. In fact, this is one part of the book where the authors exercise their prerogative to express an opinion. They offer multiple reasons why central bank money for all (think conventional accounts for the public at the central bank) make more sense than a central bank cryptocurrency. I will not debate this point here, but the reader should be aware that others have taken a contrary view (e.g., Kahn *et al.* 2020).

The last big topic is scalability. Many people will have heard that Bitcoin transactions can only occur at a rate of roughly 10 transactions per second. In this regard the authors discuss two solutions: block size increases and payment channels (e.g., the lightning network). The former solution would lead to fewer full nodes and more centralization (p. 197), longer propagation times, more block races, and other problems. The latter allows large numbers of micropayments to made off of two blockchain transactions. The trick here is doing this without requiring the counterparties to trust each other. The authors explain how this can be done using multiple-signature authorization and time locks, but suffice it to say it seems a lot more complicated than other closed loop systems like Venmo. Perhaps the final lesson here is that trust in institutions can be really useful. Unless there is good reason why this trust cannot work, the alternatives seem to be dominated.

I have not addressed all aspects of the book. There are several important issues the authors put significant effort into describing that I did not even touch on. One of these issues is the energy cost of maintaining the Bitcoin network. As the authors illustrate, proof-of-work uses the energy consumption of a small country (see Table 6.6). The authors point out that conventional platforms also use a lot of energy, but I do not believe this provides absolution for Bitcoin. Many cryptocurrencies are transitioning to proof-of-stake and other, far less energy-intensive, protocols. The authors do not discuss these alternatives, as perhaps it is too early to tell whether these alternative protocols will be as trustless and secure as proof-of-work. However, the reader should be aware that proof-of-work cryptocurrencies are coming under increased scrutiny for their energy use and it is highly likely that proof-of-stake based protocols will become increasingly popular in the future.[10]

To conclude, let me strongly encourage anyone interested in, exactly as the title of this book suggests, a comprehensive introduction to Bitcoin, blockchain and cryptoassets to read this book. Developments in this space are evolving fast, and following these exciting developments is not possible without a solid foundation. This book, which could also serve quite nicely as an introductory textbook for an undergraduate/graduate course on cryptoassets, provides both the contextual and technological background anyone needs to keep up with crypto and overcome John Oliver's comedic description provided in the epigraph.

[8] In this discussion, the authors state that fixed costs can be ignored in assessing the short-run behavior of miners. Recent work by Garratt and van Oordt (2020) reveals that fixed costs can matter, even in the short run, and that the combination of a high fixed cost and a low alternative use value for specialized mining equipment can lead to a more resilient network.

[9] Garratt and Wallace (2018) point out that the existence of many close substitutes increases the price indeterminacy.

[10] See the announcement by Elon Musk that Tesla will no longer accept Bitcoin: https://twitter.com/elonmusk/status/1392602041025843203/photo/1.

## References

Bank for International Settlements. 2003. *The Role of Central Bank Money in Payment Systems*. Committee on Payment and Settlement Systems https://1lib.us/book/948577/1e5c23?id=948577&secret=1e5c23.

Garratt, Rod. 2015. A Distributed Version of Repugnance as a Constraint on Markets. *Liberty Street Economics*, Federal Reserve Bank of New York. https://libertystreeteconomics.newyorkfed.org/2015/09/a-distributed-version-of-repugnance-as-a-constraint-on-markets/.

Garratt, Rodney, and Maarten van Oordt. 2020. *Why Fixed Costs Matter for Proof-of-Work Based Cryptocurrencies*. Bank of Canada Staff Staff Working Paper 2020–27.

Garratt, Rodney, and Neil Wallace. 2018. Bitcoin 1, Bitcoin 2,…: An Experiment in Privately Issued Outside Monies. *Economic Inquiry* 56 (3): 1887–1897.

Kahn, Charles, and William Roberds. 2009. Why Pay? An Introduction to Payments Economics. *Journal of Financial Intermediation* 18 (1): 1–23.

Kahn, Charles M., Francesco Rivadeneyra, and Tsz-Nga. Wong. 2020. Should the Central Bank Issue e-Money? *Journal of Financial Market Infrastructures* 8 (4): 1–22.