When governments lavishly print money, citizens are helplessly left watching their savings erode. This is the cost of centralised government monopoly over currency. But cryptocurrencies, such as the burgeoning bitcoin, have set out to solve this problem. These new forms of ‘digital cash’ hope to revolutionise our financial system by returning control of money to individuals.

The cryptocurrency revolution was launched by a group of fed up computer scientists, mathematicians, and engineers. Their aim was both simple and profound: eliminate the need for intermediaries—the middle-man—in the monetary exchange. Even imagining such a world is difficult: a world where currency is freed from the shackles of supposedly omnipotent governments. Money would be transferred instantly, costlessly and pseudonymously. No more transaction fees, clearing delays, or bank holidays.

But there has always been one stumbling block for a digital currency: trust. For many decades we have used banks and intermediaries to solve the trust problem. Traditionally, ledgers of ‘who owns what’ have been maintained by banks. And thus banks became the trusted gatekeepers of exchange, holding an indispensable and powerful link with the money we use. To be successful, cryptocurrencies such as bitcoin need to solve the ‘trust’ problem. But how do we generate trust in something that only exists in bits and bytes?

There are many facets to this trust problem. The first is a technical one—how do you create the system? The second, and currently perhaps more important, is in creating a level of understanding with the public.
IPA Review

Volume 67 | 3

MONEY HAS NOT BEEN GENERATED BY LAW. IN ITS ORIGIN IT IS A SOCIAL, AND NOT A STATE, INSTITUTION. SANCTION BY THE AUTHORITY OF THE STATE IS A NOTION ALIEN TO IT. —CARL MENGER

The additional technological innovations using the blockchain—known as ‘blockchain 2.0’ technologies—are the topic of chapter eight of The Age of Cryptocurrency. Here the authors describe the use of blockchain technology in any transaction where it is important to know who owns what, and when ownership of a particular asset was obtained. Having a publically stable and secure system for recording this information presents enormous potential. These all use the underlying technology of the blockchain as a ‘trustless’ consensus-driven proof mechanism for exchange—which whether it be contracts or currency. Currently entrepreneurs are bringing the block chain technology to: peer-to-peer crowd funding, escrows and trusts, public records; smart contracts with self-executing clauses, decentralised voting platforms, and so on. While this book appropriately highlights the concerns over trust and power—which are certainly important—the authors may be obscuring a more vital point about the origin of money. The focus on Milton Friedman’s widely cited definition of money—as a unit of account, a store of value, and a medium of exchange—begins from the premise that money is state-granted. In such a context, the idea that money could be created and sustained by private entrepreneurs in a market is almost impossible to grasp. The origins of cryptocurrencies are decidedly ‘non-state’. Bitcoin was a surprising development to many mainstream economists. But the heterodox schools of economic thought—such as the Austrians, the institutionalists and the evolutionary economists—would almost predict this to be the case. For instance, in 1892 Carl Menger wrote: ‘Money has not been generated by law. In its origin it is a social, and not a state institution. Sanction by the authority of the state is a notion alien to it.’

What is most interesting about The Age of Cryptocurrency is that the technologies described in it provide an optimistic future for limited governments and free markets. We are decidedly coming into an era where exchange out of the watchful eye of the state is more possible than at any other time in all of human history. Given the ever-expanding reach of the state, such an innovation may be priceless.