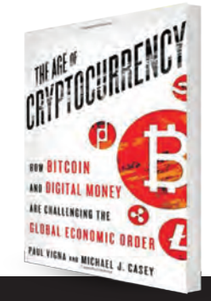
NEW MONEY

Digital cash—cryptocurrencies—could be the key to a decentralised currency writes **Darcy Allen**

> THESE NEW FORMS OF 'DIGITAL CASH' HOPE TO REVOLUTIONISE OUR FINANCIAL SYSTEM BY RETURNING THE CONTROL OF MONEY TO INDIVIDUALS.

DARCY ALLEN
Research Fellow at the Institute of Public Affairs



The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order

Paul Vigna and Michael J. Casey
St Martin's Press, 2015, 368 pages

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.

CONTINUED

The latter is precisely what *The Age of Cryptocurrency* provides. This new book by Paul Vigna and Michael J. Casey offers a clear and concise explanation of what bitcoin is and how it works. The authors offer a balanced and easy-to-read journalistic account of the volatile rise of cryptocurrencies.

This book is a refreshing addition to the small body of work on cryptocurrency. Their prose is unashamedly neutral and comes across as informative, rather than proselytising. *The Age of Cryptocurrency* book provides an accurate account of bitcoin, its potential benefits and its downfalls, as well as some clearly delineated conjectures of future cryptocurrency applications.

Bitcoin is a form of digital cash. It requires neither central banks nor trustworthy intermediaries to function. Bitcoin is created, exchanged, and maintained through the mathematics of cryptography—the study of techniques for secure communication when third parties are present.

Bitcoin is based on a technology called the blockchain. The blockchain is a chronological, tamper-proof, and decentralised ledger of all bitcoin transactions in history. Before bitcoin, we went to banks to clarify previous transactions and account balances (i.e. 'who owns what'). But with bitcoin the intermediary is no longer required—all individuals consult the most recently updated public ledger.

Rather than trusting banks to maintain 'ledgers', bitcoin users trust the 'blockchain' ledger. The blockchain is stored across a distributed network of computers and is downloadable and accessible to anyone. This decentralised model makes it less susceptible to the risks of centralised control.

There are two main technical achievements that were crucial in the emergence of bitcoin: the creation of a distributed, public ledger of transactions, and an incentive mechanism to maintain that ledger.

We are well accustomed to paying account or transaction fees to banks. Banks require these often exuberant fees to maintain up-to-date account balances. The bitcoin blockchain also requires continual and reliable updating, a process which uses copious amounts of expensive computing power. And therein lay one of Bitcoin's biggest challenges: how to maintain the blockchain in an affordable way.

Bitcoin's solution is ingenious: those individuals who offer to maintain the ledger—individuals known as bitcoin 'miners'—are periodically rewarded with 'new' bitcoins for contributing their computing power. Therefore the incentive mechanism behind maintaining the blockchain ledger is inexplicably linked with bringing bitcoins into circulation (the 'creation' of bitcoins).

This incentive mechanism effectively solves two problems. First, it makes the whole system cheaper to use by avoiding expensive banks. And, second, the underlying algorithm to create bitcoins is set and cannot be tampered with. This makes bitcoin 'inflation proof' and puts it out of the hands of state manipulation.

Anyone may buy bitcoins on bitcoin currency exchanges. To do this, users create a unique bitcoin 'wallet'—which is similar to a conventional bank account number. But it is pseudonymous because no real names are attached. The equivalent of an account password is a 'digital signature', created when users combine their 'public' key and their 'private' key together. The transaction is then permanently and publically recorded on the blockchain.

But the blockchain is not limited to money or currency. For free markets what is most exciting are additional applications of the block chain technology. In the same way that the bitcoin block chain addresses centralisation and trust issues in financial exchange, the blockchain also creates similar opportunities in many institutional domains that are afflicted by over-centralisation.

> 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 block chain—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—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.