"A great resource for anyone who wants to understand what blockchain and cryptocurrency is really all about."
—Paul Griffin, Associate Professor, School of Information Systems, Singapore Management University

THE BASICS OF BITCOINS AND BLOCKCHAINS

An Introduction to Cryptocurrencies and the Technology that Powers Them

ANTONY LEWIS

The Basics of Bitcoins and Blockchains

“A comprehensive overview of the fundamentals. One of the few recommended readings for my new staff.”
—Yusho Liu, Cofounder, Coinhako

“A useful, usable and enjoyable read. Antony helps us all clearly understand the mechanics of bitcoin and blockchain.”
—Rob Findlay, Founder, Next Money

“A great resource for anyone who wants to understand what blockchain and cryptocurrency is really all about.”
—Paul Griffin, Associate Professor, School of Information Systems, Singapore Management University

“Einstein said that ‘if you can’t explain it simply, you don’t understand it well enough’. Antony clearly understands and articulates the basics of cryptocurrencies and blockchain technologies.”
—Colin Platt, Co-Host Blockchain Insider Podcast & DLT/Cryptocurrency Researcher

“The first book that I’ve seen that really breaks down concepts. An excellent insight into the key concepts and real-world implications of bitcoin and blockchain.”
—Zennon Kapron, Managing Director, Kapronasia

“This is a helpful introductory guide to cryptocurrencies.”
—Tim Swanson, Post Oak Labs and *Of Numbers* blog

“A delightful read that cuts the hype, finds the signal in the noise, and fires on all cylinders from front to back.”

—John Collins, fintech advisor

“My family asked me to explain what I do, I gave them a copy of this book. Antony explains cryptocurrencies and blockchain technologies clearly and articulately, whilst remaining witty.”
—Colin Platt, Co-Host Blockchain Insider Podcast & DLT/Cryptocurrency Researcher

“One of the few credible books I suggest when people ask ‘where can I learn about bitcoin?’ It is an excellent, level-headed primary on everything crypto. I’ve been in the space for quite some time and I still learned from The Basics of Bitcoins and Blockchains.”
—Zennon Kapron, Managing Director, Kapronasia

“An engaging, clear, and authoritative guide to the applications and implications of blockchains.”
—Greg Wolfson, Head of Business Development at Element Group

“If you want a book that over-sells blockchain, go elsewhere. This explains the fundamentals clearly and cuts through the hype.”
—Richard Gendal Brown, CTO, R3

THE BASICS OF BITCOINS AND BLOCKCHAINS

An Introduction to Cryptocurrencies and the Technology That Powers Them

ANTONY LEWIS

Mango Publishing
CORAL GABLES

Published by Mango Publishing Group, a division of Mango Media Inc.

Cover Design: Roberto Núñez
Layout & Design: Roberto Núñez

For permission requests, please contact the publisher at:
Mango Publishing Group
2850 Douglas Road, 3rd Floor
Coral Gables, FL 33134 USA
info@mango.bz

For special orders, quantity sales, course adoptions and corporate sales, please email the publisher at sales@mango.bz. For trade and wholesale sales, please contact Ingram Publisher Services at: customer.service@ingramcontent.com or +1.800.509.4887.

The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them

Library of Congress Cataloging-in-Publication has been applied for.
ISBN: (paperback) 978-1-63353-800-9, (ebook) 978-1-63353-801-6
BISAC category code:
BUSINESS & ECONOMICS / Investments & Securities / Futures

Printed in the United States of America

To my family, my long-suffering wife Sarah and our progeny-chain Toshi and Tosha.

TABLE OF CONTENTS

Part 0

INTRODUCTION

SOME DEFINITIONS

Bitcoin, blockchains, and cryptocurrencies are fascinating to me because there are so many elements to understand. This multidisciplinary nature is one of the reasons I, and so many others, love the industry—it is easy to get sucked into the rabbit hole, and as you try to understand each element, every answer begets more questions. The journey starts with 'What is Bitcoin?' but the explanations and answers come from the disciplines of economics, law, computer science, finance, civil society, history, geopolitics, and more. You could create a pretty comprehensive high school curriculum around Bitcoin and have plenty of material to spare.

And this is the very reason why it is so hard to explain. This book is an attempt to cover the basics. It is aimed at the thinking person but assumes that the reader doesn't have a detailed background in the various disciplines mentioned previously. Different people will find different parts interesting. I try to use analogies where I think they help explain some concepts, but be gentle with me: all analogies break down if stretched too far. And although I have tried to be accurate, there will still be oversimplifications, errors and omissions. What is true today may not be tomorrow: the pace of change is rapid. I am the first to admit that there are limits to my own technical expertise. Nevertheless, I hope that every reader comes away learning something new.

With that, let's start by defining at a basic level some of the words and concepts we will be exploring later in the book.

Bitcoin' and Ether are two of the better-known *cryptocurrencies* or *coins* (note that the coin on the Ethereum network is called Ether, though is often misnamed in the media as 'Ethereum'). These are *assets* or items of

value that exist digitally, not physically, and are created by software. They have no issuer as such. No person, company, or entity backs these, and there are no terms of service or guarantees associated with them. Like physical gold, cryptocurrencies simply exist, and are created or destroyed according to the rules articulated in the code that creates and governs them. If you own some cryptocurrency, and we'll see what that actually means later, it is your asset that you control. It has value, and can be exchanged for other cryptocurrencies, US dollars, or other global sovereign (or fiat) currencies. Its value is determined within marketplaces called *exchanges* where buyers and sellers come together to trade at mutually agreed prices.

As well as 'coins,' units of cryptocurrencies may be described as digital assets. That is, unique data items whose ownership can be passed from account to account. These accounts are technically called addresses, and we will explore what addresses are later. When these digital assets move from one account to another they are all recorded on their respective transaction databases known, because of some unique shared characteristics which we will look into later, as blockchains.

Just to confuse everybody, some digital assets are described as tokens, as in 'Is it a cryptocurrency or a token?'. Cryptocurrencies and tokens are both types of cryptographically secured digital assets, sometimes known as *cryptoassets*. These tokens have different characteristics from cryptocurrencies and from each other. Tokens can be fungible (one token being more or less replaceable by another), or non-fungible (where each token represents something unique). Unlike cryptocurrencies, these newer tokens are usually issued by known issuers who stand behind them, and the tokens can represent legal agreements (like financial assets), physical assets (like gold), or future access to products and services.

Where the underlying item is an asset you could think of the token as a digital version of a cloakroom ticket, issued by a cloakroom clerk and redeemable for your coat. Indeed, these tokens are sometimes called DDRs—Digital Depository Receipts. Where the underlying item is an agreement, product or service, you can think of the token as something like a concert ticket issued by a concert organiser and redeemable for entry to a concert at a later date.

To give some real examples, there are tokens that represent everything from gold bullion sitting in a vault somewhere[2], through to tokens representing unique 'CryptoKitties'—collectable digital cats with specific visual attributes determined by their 'DNA' code.

A CryptoKitty[3]

What do all of these coins and tokens have in common? All transactions related to them, including their creation, destruction, changes of ownership, and other logic or future obligations, are recorded on *blockchains*: replicated databases that act as the ultimate books and records—the 'golden source' that represents the universal understanding of the current status of all units of the digital asset.

Bitcoin's blockchain is an ever-growing list of every Bitcoin transaction that has ever happened, right from the creation of the very first Bitcoin on 3 January 2009, through to the most recent transfer or payment from one account to another. Ethereum's blockchain is a list of transactions involving the cryptocurrency Ether, a multitude of other tokens (including those representing CryptoKitties) and other related data, all of which is recorded on Ethereum.

Different blockchains have different characteristics, so much so that nowadays it is almost impossible to make a general statement about 'blockchain' without being wrong for some particular example. Some blockchains, like the well-known Bitcoin and Ethereum chains, are *public*, or *permissionless*, meaning that their list of transactions can be written to by anyone, with no gatekeepers to approve or reject parties who want to create blocks or participate in bookkeeping. Self-identification is not a requirement to create blocks or validate transactions. Other blockchains can be *private* or *permissioned*, in that there is a controlling party who allows participants to read or write to them.

And finally, we need to distinguish between *protocols*, *code*, *software*, *transaction data*, *coins*, and *blockchains*. Bitcoin is a bunch of *protocols*: rules that define and characterise Bitcoin itself—what it is, how ownership is represented and recorded, what constitutes a valid transaction, how new participants can join the network of operators, how participants should behave if they want to be kept up to date with the latest transactions, and so on. These protocols, or rules, can be described in English or any other human language, but are best articulated in computer *code*, which in turn can be compiled into *software*—Bitcoin software—that enacts those protocols, i.e. makes them operate. When the software is run, Bitcoin *coins* are generated and can be sent from one account to another. These actions are recorded as *transaction data*, and this transaction data is bundled into bundles or *blocks*, and linked together to form the Bitcoin *blockchain*.

So, to recap, Bitcoin *protocols* are written out as Bitcoin *code* which is run as Bitcoin *software* which creates Bitcoin *transactions* containing data about Bitcoin *coins* recorded on Bitcoin's *blockchain*. Got it? Good. Not all other cryptocurrencies or tokens work this way, but it is as good a basis as any to start the journey.

Some people think of Bitcoin as the next evolution of money—it is described as a (crypto) *currency* after all. So we need to understand a little more about money. What is money? Has it always been the same? How successful has money been? Are some forms of money better than others? Can the nature of money ever change, or is what we have going to be the same for evermore? Do cryptocurrencies sit easily alongside today's money, fulfilling a niche or purpose that existing forms of money cannot serve, or are cryptocurrencies competitors to today's money that threaten the status quo of state-issued currency?

This book should give you a good well-rounded education into the basics of bitcoins and blockchains and assumes no specific starting expertise. We start by defining and understanding the nature of money. Then we dive into digital money and how value is really transferred around the world. We then explore a few key concepts from a branch of mathematics called cryptography, so that we can then move to cryptocurrencies themselves. In the cryptocurrencies section, we dive into the Bitcoin and Ethereum networks, and the Bitcoin and Ether digital tokens—what they are, how to buy, store, and sell them, how to explore their blockchains, and the risks in managing them, including the unique challenges in moving this new digital money around the world. Finally, we discuss the types of blockchain technology that are being explored by banks and big businesses to join up their databases and do more efficient business.

Although I have my personal biases and interests, throughout the book I try to maintain a neutral position on the cryptocurrencies, tokens, and blockchain platforms. I try not to neither over-sell them nor be overly critical. I leave it up to readers to conclude for themselves whether these technologies are a trend or a fad, useful or useless, good or bad.

Part 1

MONEY

PHYSICAL AND DIGITAL MONEY

Cash—physical money—is wonderful. You can transfer (or spend or give away) as much of what you have as you want, when you want, without any third parties approving or censoring the transaction or taking a commission for the privilege. Cash doesn't betray valuable identity information that can be stolen or misused. When you receive cash in your hand, you know that the payment can't be 'undone' (or charged back, in industry jargon) at a later date, unlike digital transactions such as credit card payments and some bank transfers, which is a pain point for merchants. Under normal circumstances, once you have cash, it is yours, it is under your control, and you can transfer it again immediately to somebody else. The transfer of physical money immediately extinguishes a financial obligation and leaves nobody waiting for anything else.

But there is a big problem with traditional physical cash: it doesn't work at a distance. Unless you carry it in person, you can't transfer physical cash to someone on the other side of the room, let alone on the other side of the planet. This is where digital money becomes highly useful.

Digital money differs from physical money in that it relies on bookkeepers who are trusted by their customers to keep accurate accounts of balances they hold. To put it another way, you can't own and directly control digital money yourself (well, you couldn't until Bitcoin came along, but more on that later). To own digital money, you must open an account somewhere with someone else—a bank, PayPal, an e-wallet. The 'someone else' is a third party whom you trust to keep books and records of how much money you have with them—or, more specifically, how much they must pay you on demand or transfer to someone else at your request. Your account with a third party is a record

of an agreement of trust between you: simultaneously how much you have with them, and how much they owe you.

Without the third party, you would need to keep bilateral records of debts with everyone, even people who you may not trust or who may not trust you, and this is not feasible. For example, if you bought something online, you could attempt to send the merchant an email saying 'I owe you $50, so let's both record this debt'. But the merchant probably wouldn't accept this; firstly, because they probably have no reason to trust you, and secondly, because your email is not very useful to the merchant—they can't use your email to pay their staff or suppliers.

Instead, you instruct your bank to pay the merchant, and your bank does this by reducing how much your bank owes you, and, at the other end, increasing how much the merchant's bank owes them. From the merchant's point of view, this extinguishes your debt to the merchant, and replaces it with a debt from their bank. The merchant is happy, as they trust their bank (well, more than they trust you), and they can use the balance in their bank account to do other useful things.

Unlike cash, which settles using the transfer of physical tokens, digital money settles by increasing and decreasing balances in accounts held by trusted intermediaries. This probably seems obvious, though you may not have thought of it this way. We'll come back to this later, as bitcoins are a form of digital money which share some properties of physical cash.

There is a big difference between *online* card payments, where you type the numbers, and physical card payments, where you tap or swipe the *physical* card. In the industry, an online credit card payment is known as a 'card *not* present' transaction, and swiping your card at the cashier's till in a shop counts as a 'card present' transaction. Online (card not present) transactions have higher rates of fraud, so in an effort to make fraud

harder, you need to provide more details—such as your address and the three digits on the back of the card. Merchants are charged higher fees for these types of payments to offset the cost of fraud prevention and the losses from fraud.

Cash is an anonymous bearer asset which does not record or contain identity information, unlike many forms of digital money that by law require personal identification. To open an account with a bank, wallet, or other trusted third party, regulations require that the third party can identify you. This is why you often need to supply information about yourself, with independent evidence to back that up. Usually that means a photo ID to match name and face, and a utility bill or other 'official' registered communication (for example from a government department) to validate your address. Identity information is not just collected when opening accounts. It is also collected and used for validation purposes when some electronic payments are made: when you pay online using a credit or debit card you need to supply your name and address as a first gateway against fraud.

There are exceptions to this identity rule. There are some stored value cards that don't require identity, for example public transport cards in many countries, or low-limit cash cards used in some countries.

Do payments *need* to be linked to identity? Of course not. Cash proves this. But *should* they? This is a big question that raises legal, philosophical and ethical issues that remain subject to ongoing debate. Credit card information is frequently stolen, along with personally identifying information (name, addresses, etc) which creates a cost to society.

Is it a fundamental right to be able to make payments which are shielded from the eyes of the state governments? And should people have the

ability to make anonymous digital payments, as they do with physical cash? To what extent should our financial transactions be anonymous or, at the very least, private? And what, if any, are the reasonable limits to that privacy? Should the public sector or the private sector provide the means for electronic payments and financial privacy? Should a nation state be able to block an individual's ability to make digital payments, and with what limits? How can we reconcile financial privacy with the prevention of support for illegal activities, including the funding of terrorism? I won't provide answers to these big questions in this book, but the fundamental questions concerning financial privacy are inevitably raised when understanding the game-changing innovation that is Bitcoin.

HOW DO WE DEFINE MONEY?

We all know what money is, but how might we define it? The generally accepted academic definition of money usually says that money needs to fulfil three functions: A medium of exchange, a store of value, and a unit of account. But what does this really mean?

Medium of exchange means it is a payment mechanism—you can use it to pay someone for something, or to extinguish a debt or financial obligation. To be a good medium of exchange, it doesn't need to be *universally* accepted (nothing is), but it should be widely accepted *in the particular context* for which it is being used.

Store of value means that in the near term (however you define this) your money will be worth the same as it is today. To be a good store of value, you need to be reasonably confident that your money will buy you more or less the same amount of goods and services tomorrow, next month, or next year. When this breaks down, the money's value is quickly eroded, a process often referred to as hyperinflation. Individuals quickly

develop alternative ways to denominate value and undertake transactions, for example bartering or using a ‘hard’ or more successful and stable currency.

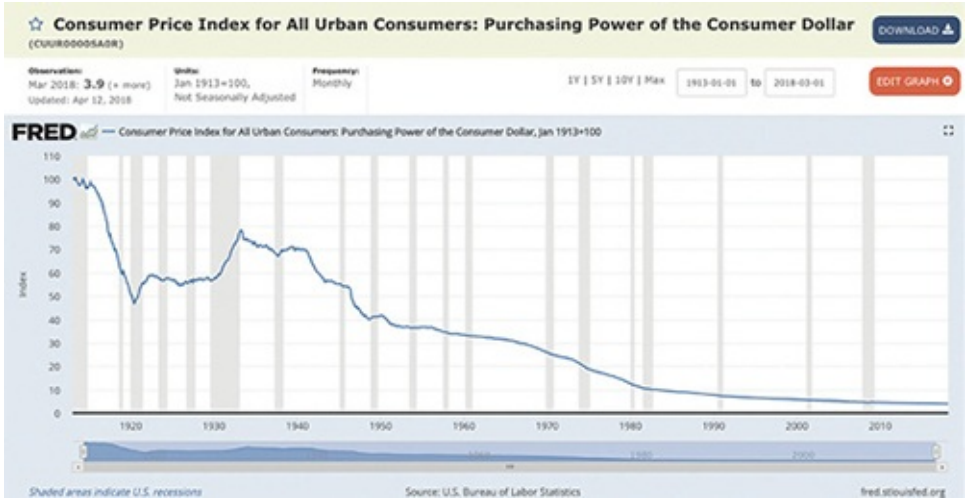
Unit of account means it is something that you can use to compare the value of two items, or to count up the total value of your assets. If you record the value of all of your possessions, you need some unit to price them in, to get a total. Usually that is your home currency (GBP or USD or whatever), but you could in theory use any unit. The last time I counted, I had 0.2 Lamborghinis worth of gadgets in my study. To be a *good* unit of account, the money needs to have a well-accepted or understood price against assets, otherwise it is hard to figure out the total value across all your assets and, if you need to do so, to convince others of that value.

While some believe that ‘good money’ should fulfil all of these functions, others think that the three functions can be fulfilled by different instruments. For example, there is no real reason why something used as a medium of exchange (i.e., something that can be used to immediately settle a debt) must also be a long term store of value.

Is Today’s Money Good Money?

It is debatable how well the forms of money we generally regard as ‘good money’ stack up against these properties. The US dollar is arguably the most prominent form of money we have today, and can be considered the best, at least for the time being. But how *good* is it? The dollar is generally acceptable for payment, certainly in the USA, and even in other countries, so it is an excellent medium of exchange in those contexts (but less so in Singapore). And it is an excellent unit of account, because many assets are priced in dollars, including global commodities such as crude oil and gold.

But how has it fared as a store of value? According to the St Louis Fed, the purchasing power of the USD from a consumer's perspective has fallen by over 96% since the Federal Reserve System was created in 1913.



Source: St Louis Fed[4].

Given that purchasing power of the USD over time has decreased significantly, it has been a poor store of value over the long term. Indeed, people don't tend to keep banknotes under their mattress for decades, because they know cash is not a good store of value. And if they did, they would find that the purchasing power has decreased, or worse, that the banknotes have been pulled out of circulation and are no longer accepted in shops. In fact, the dollar, as with almost all government currencies, consistently loses value by design, driven by policy. We can predict, more or less, that the USD will lose its purchasing power by a few percentage points each year. This is known as price inflation (as opposed to currency inflation which is an increase in the number of dollars in circulation). Price inflation is measured by CPI (Consumer Price Inflation)—an index measuring the changes in the price of a theoretical basket of goods that are reportedly chosen to represent typical urban household spending[5]. The makeup of the basket changes over time, and policymakers are not