In 2009, an anonymous programmer releases a new method of paying and being paid to the world. No one runs it; no one controls it; no authority verifies it. In this, its creator promises, is a way around banks and governments, around laws and regulations, and around failure itself.

Less than a decade on, the cryptocurrency known as Bitcoin is soaring in demand, and a single unit is valued in the thousands. It has spawned hundreds of clones, and its underlying blockchain technology has created a revolution in computing. It has legally made millionaires of thousands of ordinary people.

Decrypted shows you, in plain, no-nonsense terms, exactly how that happened. Cryptocurrency and startup pioneer Leng Hoe Lon walks you through how cryptos like Bitcoin work and get their value, their strengths and weaknesses, their implications for the world... and how they fit in your investment plans.

Will you join the cryptocurrency revolution, or ignore it as a passing fad? It's up to you to check out the facts, and decide for yourself. This book will show you what you need to know.

The book provides sufficient knowledge for even newcomers to catch up with this seemingly complicated blockchain world without much technical background. I believe the book will help introduce more people to blockchain and cryptocurrency, an exciting innovation of the century.

Loi Luu
Co-founder, Kyber Network

I have always been a huge believer of inclusive finance, where the old and new economy find grounds to collaborate and embrace each others' presence. The first step is to educate ourselves, no matter at what career juncture we are at, and the remaining excitement of cryptocurrency and the sheer potential of blockchain technology will lead the way. *Decrypted*, as narrated by Hoe Lon, is the epitome of life-long learning and embracing of what disruption in his field has to offer.

Professor David Lee
Professor at Singapore University of Social Sciences,
Co-founder BlockAsset and Senior Advisor to Sentinel Chain

visit our website at:
www.marshallcavendish.com/genref

Marshall Cavendish Business

BUSINESS
ISBN 978-981-4828-70-3
9 789814 828703

Leng Hoe Lon

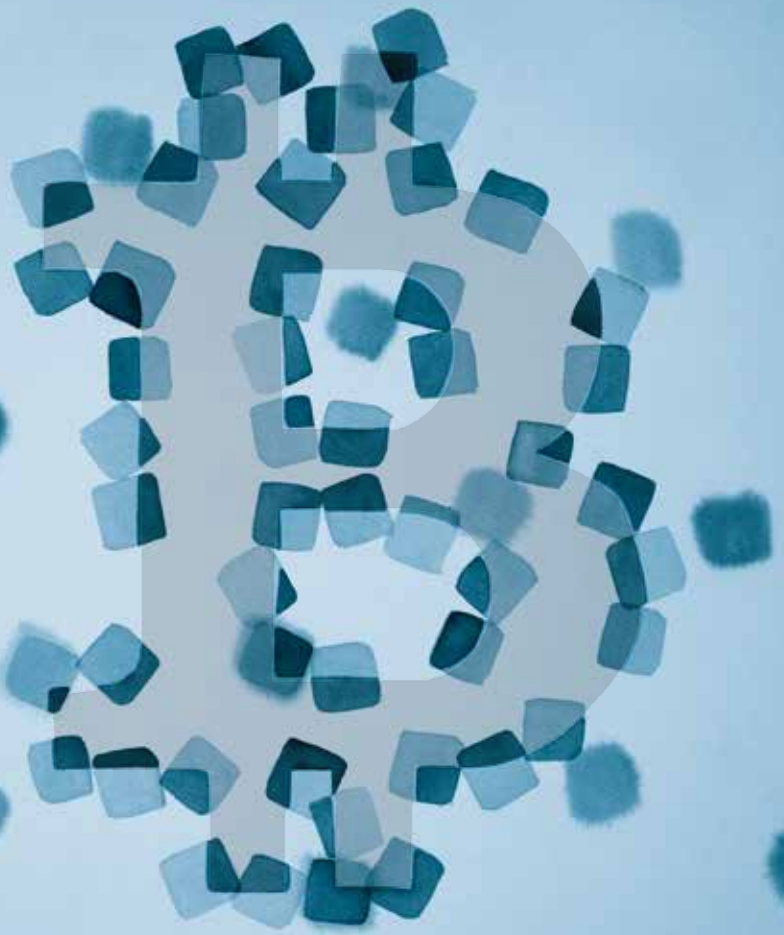
DECRYPTED

A FINANCIAL TRADER'S TAKE ON CRYPTOCURRENCY

Marshall Cavendish Business

DECRYPTED

A FINANCIAL TRADER'S TAKE ON CRYPTOCURRENCY



Leng Hoe Lon

Foreword by **Adam Levinson**

Decrypted is an excellent work by Hoe Lon that explains cryptocurrency from a traditional trader's perspective. The book provides sufficient knowledge for even newcomers to catch up with this seemingly complicated blockchain world without much technical background. I believe the book will help introduce more people to blockchain and cryptocurrency, an exciting innovation of the century.

Loi Luu
Co-founder, Kyber Network

I have always been a huge believer of inclusive finance, where the old and new economy find grounds to collaborate and embrace each others' presence. The first step is to educate ourselves, no matter at what career juncture we are at, and the remaining excitement of cryptocurrency and the sheer potential of blockchain technology will lead the way. *Decrypted*, as narrated by Hoe Lon, is the epitome of life-long learning and embracing of what disruption in his field has to offer.

Professor David Lee, Singapore University of Social Sciences
Co-founder, BlockAsset and Senior Advisor to Sentinel Chain

Decrypted is a trader's view of cryptocurrencies. A hard and uncompromising analysis of what it is, what it is not and most of all whether it will fulfill aspirations of what it can be. Hoe Lon has delved deep into the domain. *Decrypted* is certain to make an engaging read.

Wong Joo Seng
Founder and CEO, Spark Systems

Decrypted took me from the path of least resistance, blissful ignorance, to the path of blissful intelligence. Finally I truly "get it".

Jason Ambrose
Founder and CEO Vanda Securities

Shouldn't one take heed that this book is written by a seasoned money manager working in high finance, who, apart from his day job, pays acute attention to cryptocurrencies? I have not read any other books out there that has distilled the essence of blockchain and its philosophy in such an easy, accessible manner. Anyone wanting to have a good introduction to this fascinating world without feeling as though they are reading a textbook should pick it up. Anyone who wants to be reminded and re-energised as to why they got into cryptocurrencies in the first place should also read it. I know I did.

Kai C Chng
CEO, Digix Global

Decrypted shares an insightful narrative on the uprise of cryptocurrencies, providing a comprehensive view into the multi-faceted interests of cryptoanarchists, bankers, and entrepreneurs. Hoe Lon outlines a thorough history of the blockchain ecosystem, and demonstrates the value of cryptocurrencies and blockchain technology for individuals and institutions. This book describes the potential impact of decentralised applications and provides a vision for how blockchain technology will come to be adopted.

Howard Wu
Co-founder, Dekrypt Capital

Bitcoin, Ethereum, Blockchain, ICOs: the cryptic world of cryptocurrencies is not only tempestuous but polarised. Perspectives are deeply entrenched with both support and opposition driven by almost cultish zeal. Cutting through that sound and fury, Leng Hoe Lon gives the uninitiated amongst us, a dispassionate framework with which to join the debate. He presents the concepts, their recent evolution, their promise and pitfalls in an accessible and engaging way. Using colourful analogies (such as an overbooked restaurant with decentralised management), Hoe Lon explains the mechanics of the underlying technology. Drawing from our experience with more traditional asset classes, he tackles the questions of 'value', 'bubble' and addresses overblown claims on both sides of the debate. *Decrypted* is not designed to be the last word for either enthusiasts or detractors. However, it is the first fair treatment of this field that I have encountered and should serve as a valuable point of reference for investors and regulators.

Lutfey Siddiqi CFA, Visiting Professor-in-Practice,
LSE Adjunct Professor, NUS Risk Management Institute
and former MD, UBS Investment bank

This book provides a great overview on cryptocurrencies and the blockchain industry. The mindset required to understand the fundamental change of the technology is well defined and expressed, which is the core component of conceptualising the benefits of blockchain in the future. A very good source to educate yourself on the subject.

Ronen Kirsh
Co-founder, Dekrypt Capital and Blockchain at Berkeley

DECRYPTED

A FINANCIAL TRADER'S TAKE ON CRYPTOCURRENCY

Leng Hoe Lon

Foreword by **Adam Levinson**

Marshall Cavendish Business

Published by Marshall Cavendish Business
An imprint of Marshall Cavendish International

A member of the Times Publishing Group

Other Marshall Cavendish Offices:
Marshall Cavendish Corporation. 99 White Plains Road, Tarrytown NY 10591–9001, USA • Marshall Cavendish International (Thailand) Co Ltd. 253 Asoke, 12th Flr, Sukhumvit 21 Road, Klongtoey Nua, Wattana, Bangkok 10110, Thailand • Marshall Cavendish (Malaysia) Sdn Bhd, Times Subang, Lot 46, Subang Hi-Tech Industrial Park, Batu Tiga, 40000 Shah Alam, Selangor Darul Ehsan, Malaysia.

Marshall Cavendish is a registered trademark of Times Publishing Limited

National Library Board, Singapore Cataloguing-in-Publication Data

Names: Leng, Hoe Lon. | Levinson, Adam, writer of foreword.
Title: Decrypted : a financial trader's take on cryptocurrency / Leng Hoe Lon ; foreword by Adam Levinson.
Description: Singapore : Marshall Cavendish Business, [2018]
Identifiers: OCN 1048626096 | 978-981-4828-70-3
Subjects: LCSH: Electronic funds transfers. | Money.
Classification: DDC 332.178--dc23

Printed in Singapore

Cover image by Aaron Gan (More on Aaron Gan on pg 165)

To all the traders in the world.
Yes, the machines are here to eat our lunch,
but they will never learn our gut instincts.
Don't stop believing.

This book is dedicated to you,
the reader—for taking a leap of faith
to accept the new world of cryptocurrencies.

CONTENTS

FOREWORD

When Hoe Lon approached me to give a Foreword to his book, the first thing I said was, "This is a fun project", and the courage to take a public stand on such a controversial topic is respectable. In the book, he applies his trading experience to demystify cryptocurrency trading.

Hoe Lon and I often discuss our global macro views, and cryptocurrency became a much greater part of the conversations over the last year. The traders in the financial world didn't care about Bitcoin until 2017. Mind you; the adoption is still pretty low. The parabolic price growth was a social phenomenon.

As a macro trader, I always evaluate various factors and put on a trade when a compelling opportunity arises. Several years back, when I was involved with Bitcoin at around $100, the bear thesis was around hacking of exchanges, links to nefarious activities and the 21st-century "tulip mania". On the other hand, the bull thesis was on three distinct arguments. First, a libertarian view on currencies free from government influence. Secondly, the discovery of digital gold. Lastly, the likely demand from China as a channel of capital outflow. The miners in China converted electricity to crypto that could be turned into foreign currencies outside of China, and everyone wants that. The rapid technological advances in the blockchain world were only the kicker to the long crypto trade.

Is it over? Emphatically no! History repeated itself when a futures market launch ended a strong rally. Bitcoin experienced that in December 2017, when many of the positions front running the event were liquidated. While you never know precisely where you are in a cycle, it is not over until crypto is institutionalised in some shape or form. Very rarely have I seen a cycle end with a narrow slice of participation. The hyper-realists are probably right that this market makes no sense, but be careful not to get stuck in an anchoring bias. It is hard and unlikely to be rewarding to fight the growing population's collective imagination. Most great trades are going with a major trend and sociological force.

The research team in my office calls this a Polymorphic Financial Instrument. It seeks to alter 5,000 years of global financial evolution, which tended towards increased centralisation since Hammurabi, King Croesus and more lately Bretton Wood. We believe the millennials will drive investment philosophy for the next two decades. The silent generation bought gold, boomers bought equities, genX put most in hedge funds, and millennials have already shown a distinct preference for digital assets.

This book is a great way to start your journey into crypto-currency investment. Hoe Lon shares his fortunate experience and makes you understand from the financial trader's point of view. Whether or not you are involved already is not important. The decentralised revolution and the trust minimisation movement have many more chapters to play out. While this is by no means a comprehensive list, one should think about the following developments.

1. How utility tokens gain greater acceptance going forward.
2. The ETF-isation of cryptocurrency to allow older generation non-millennials to participate at ease and comfort.
3. The emergence of nationally sponsored fiat-crypto like the J-Coin ahead of the 2020 Tokyo Olympics.
4. The post regulation validation wave of adoption.
5. The institutionalisation of crypto assets that will come with the development of custody solutions.

This is too important as an emerging technology to ignore. Spending time is worthwhile. Hoe Lon's insight is a great aid in that exploration.

Adam Levinson
Managing Partner and CIO
Graticule Asset Management Asia (GAMA)

INTRODUCTION

CRYPTO AND YOU

> Television won't be able to hold on to any market it captures after the first six months. People will soon get tired of staring at a plywood box every night.
>
> *—Darryl Zanuck,*
> *Executive at 20th Century Fox (1946)*

Suppose two great financiers strongly disagree on some great new money product that's taking the world by storm—and they don't mince words. The first one (let's call him 'James') declares it to be "a fraud" and "worse than tulip bulbs," referring to the sixteenth-century 'tulip mania' in Holland.[1] James is so serious, he threatens to fire anyone in his bank caught trading in it. "It's against our rules, and it's stupid. And both are dangerous."

The second is a billionaire venture capitalist (we'll call him 'Timothy') who backed crypto from the very beginning, and sees incredible potential in it—so incredible, he's invested more than almost anyone else in its startups and exchanges.

"[It] frees people from trying to operate in a modern market economy with weak currencies," he has said. "We expect to be able to create new services that can provide liquidity and confidence to markets that have been hamstrung by weak currencies."

He's so confident in it that he buys massive quantities of it on auction for a few thousand dollars... and sees their value to grow to US$70 million over the mere three years he's held them.

Both James and Timothy have seen the trends. Both have presumably done the math. Both are responsible for the smooth transaction and use of billions of dollars ... and yet, they've arrived at vastly different convictions on the same issue. (Given their language and actions, I'm sure you'll agree that 'conclusions' is too weak a word.)

I haven't even changed their names. 'James' is Jamie Dimon, chairman and CEO of JPMorgan Chase. 'Timothy' is Bitcoin proponent Tim Draper, whose belief in its growing value over the coming years has led him to support crucial pioneering work in the creation and trade of bitcoins, such that each of them is worth thousands of dollars as I write this.[2]

What divides them—and millions of people worldwide—is a new way of thinking about money and its exchange.

The Name Is Currency, Cryptocurrency

Enter cryptocurrency, or *crypto* for short.

At its most basic definition, it's a financial product that, like stocks and bonds, doesn't physically exist; instead, it consists of a public record of transactions made, updated in real-time and secured using industrial-grade mathematical cyphers to protect it from being changed by anyone after the fact.

This immutable record, stored as a distributed ledger known as a *blockchain*, is entirely anonymous, with no personal information appended to it. This is where cryptocurrencies get their name; it's got nothing to do with mystery, unintelligibility or secrecy of any kind.[3]

I'll certainly admit that crypto is something of an odd duck, as far as investment instruments go. (For reasons I'll explain later, it's a slight misnomer. Crypto more resembles stocks and shares than it does the spendable, liquid money implied by the term 'currency'.)

For one, its creator was the first to lay out a system of money as a series of unchangeable 'agreements' between account numbers that would be stored in servers worldwide and synchronised regularly so that each had a ledger bearing the same 'content'... rather than assets held by actual, identifiable people.

He (or they) remains anonymous, going by the handle '*Satoshi Nakamoto*'—perhaps as a means of showing how you can hold large amounts of money in such an instrument, while remaining untraceable by banks, governments and other authorities.

He named it *Bitcoin*, and today it serves as the 'gold standard' for cryptocurrencies worldwide. Where once inventors sought fame, licensing fees and fortune, Nakamoto has gone the opposite route by avoiding media attention and paying himself in his own product.

Will cryptos like Bitcoin and its competitors (which we'll meet later in the book) go big and stay big, or flame out? Perhaps it's too early to say; as I write this, the concept of crypto itself is less than a decade old. That isn't a long time to hold a financial product like a stock, and the value of crypto could go in either direction.

But let me ask you a few questions. Would a poor investment attract so many startups, so much capital? Would it accrue thousands of dollars over a short time, such that what you spent on a pizza in 2010 would buy you a house and retire you for life?

(This has actually happened; in the first ever sale of something for bitcoins, programmer and Bitcoin enthusiast Laszlo Hanyecz

paid 10,000 bitcoins for two pizzas on 22 May, an amount worth $5 million just four years later, and $20 million in 2017.)[4]

Personally, I knew that Loi from Kyber Network used his scholarship money to buy 5,000 ETH at ETH/USD 1.00 which he later sold for US$7,500 at ETH/USD 1.50, a 50% gain. Back then as a poor student, he was happy as he thought he had made some money. The value of his ETHs then would have been worth over US$3 million today!

Would important VCs like Draper pay much attention to it, much less fund it so thoroughly?

Would it attract committed users all over the world, and leave governments and banks scrambling to control pieces of the pie?

Would major banks like Goldman Sachs set up trading desks for it, and declare it a form of money to its clients?[5]

And would governments all over the world, including one that oversees one-sixth of humanity, get so heavily involved?

That hasn't just attracted dozens of startups to create literally hundreds of new cryptos, but also set up a market worth US$170 billion as of August 2017... and growing every day. Not bad for a concept that, as I write, hasn't even reached its ninth birthday.

Like the paper in your wallet, the data that makes up cryptos and their blockchains has no value in and of itself—it's only useful because everyone agrees that it holds some certain amount of value that can be exchanged for real-world goods and services. As of this writing, a single bitcoin is worth thousands of dollars, but this is because that's the average price across the various exchanges that dot the Internet.

As with government-issued currency (or *fiat*) it's not the dollar value that's important, but its buying power. There's no point in

having hundreds of dollars if the necessities of life, like food, water and shelter, cost thousands.

The Reason For This Book

Why this book? Not because I want you to agree with me or anyone else, but to share the facts and why they happened... and only then invite you to decide whether cryptos like Bitcoin, Ether, Litecoin or something else are products you want in your portfolio. Cryptocurrencies are a completely new class of asset, built on technology that literally did not exist only a short time ago.

You may have heard of crypto before, whether in the financial pages; or when some criminal organisation threatened computer users worldwide and demanded ransoms in bitcoins. *That's* set off a firestorm of scepticism that I believe doesn't give crypto a fair chance. What if you or I missed out on something good simply because we believed its critics? There is no new invention under the sun that didn't have its share of them, and crypto is no different. I'm not going to sell crypto (or the blockchain technology it is built on) as the next quantum leap in finance, or otherwise dictate what you think about it. No one can—or should. But I believe that's a great reason to research the field for yourself, gather the facts and make up your own mind.

That said, some patience is needed as we tease out the intangible, uncontrolled nature of crypto. You can't see or touch it, and transactions work so differently in crypto that it looks like a whole new ball game.

That's why I wrote this book. I want to demystify the concept of cryptocurrency so anyone with no prior knowledge can understand how it works. I'll share how its decentralised structure

works without the need for banks, government action or, indeed, verifiable authority of any kind—and show its relation to the real money we see and handle every day.

The fact that its creator is unknown, and its systems often invisible and unaccountable, doesn't have to be a barrier to your use and investment in it, any more than you have to know about internal combustion or who Henry Ford was every time you start your car. As the Bitcoin website puts it:

> Just like current developers, Satoshi's influence was limited to the changes he made being adopted by others and therefore he did not control Bitcoin. As such, the identity of Bitcoin's inventor is probably as relevant today as the identity of the person who invented paper [...] Nobody owns the Bitcoin network much like no one owns the technology behind email.[6]

I do this by sharing the 'pillars' of crypto operations, with an inside look at how new cryptos are planned, differentiated and sold, and what this means for the financial and political worlds... and by extension, you the individual trader and investor.

Like any specialised field, crypto has its own evolving 'language' that coins (no pun intended) new words and repurposes existing ones. I'll introduce new terms in italics, and give short explanations in the glossary at the end of this book.

Why Take Me Seriously?

I'm a banker and fund manager by profession, but have a keen interest in technology startups. While I got my start in Deutsche

Bank in 1997, I was told that foreign exchange trading (FX) would soon become obsolete.[7] I was still trading FX in JPMorgan Chase, ABN AMRO and Goldman Sachs through to 2011—but after managing fiat money in Tudor Investment Corp for five years, I grew more and more interested in ways to combine human and machine learning to solve problems that are beyond the reach of either working alone.

I became intrigued by crypto after learning that famous hedge fund managers Michael Novogratz and Adam Levinson from Fortress Investment Group had bought US$20 million of bitcoins in 2013. Today, that stash is worth close to US$200 million. In 2016, I created technology startups (such as Shentilium Technologies), but kept in touch with a colleague from Goldman Sachs named Mona El Isa, who would go on to create a crypto software provider called Melonport, and whom you'll meet at the end of this book.[8]

Perhaps in time to come, 2016 will be remembered as a watershed year for crypto, and less for the highly unlikely election of US President Donald Trump. Over and over again I would hear news about some new development in Bitcoin or the hundreds of new cryptos (and exchanges) seemingly popping up overnight. Many were appreciating in value, such as Ethereum; since I first heard of it, it's grown more than 40 times in value! And in fairness, Dimon has since changed his position on Bitcoin from hostility to neutrality.[9]

I experimented here and there with crypto, dipping my toe into the waters and learning what I could. Together with my crypto compatriot, Lee Hong, we had several meetings late at night teaching each other about blockchain technologies and cryptocurrency. We decided to go to DevCon 2 in Shanghai in

September 2016. I didn't make it in the end but Lee Hong did and befriended Loi Luu of Kyber Network.

My dual background in banking and tech caught the eyes of Kyber Network's development team, who approached me to advise on their new crypto exchange and help build it from the ground up by working alongside some of the best coders and engineers in the industry.

To that end, I spent several months immersed in what it truly takes to build and trade in crypto, especially in the days leading up to an *initial coin offering* (ICO). This is when a startup begins offering its own cryptocurrency to raise funds, potentially bypassing traditional forms of fundraising like offering shares or working with venture capitalists.

That means I know a promising information product when I see one, and in the case of crypto, I can actually show you how it works—and why it attracts the attention it does.

What You'll Learn

Think of me as a tour guide to the basics of crypto, giving you a knowledge base you can start out with as you decide whether or not to take the plunge into crypto trading. When our time together is done, you'll be able to:

- Follow a conversation or financial pages report about crypto and its value, and understand what it bodes for various cryptos such as Bitcoin, Ethereum, Dash, Litecoin and others.
- Set up an account for crypto buying, selling and mining, complete with your own *wallet* and set of transaction records, or blockchains.

- Understand the key issues that make crypto so alluring yet controversial (like any new technology), and its implications for investors, governments and banks.
- Tell what differentiates one crypto from another, in terms of their product positioning, accessibility, level of oversight and risk factor.
- See how and why half-truths and myths form so easily around crypto—and bust them with the truth.

Like any current financial instrument, crypto is here to stay, for better or worse. Even if there is indeed a crash (more on that later in the book) it's not going to wipe crypto out—only change the way it's dealt with.

Everyone is free to embrace it as the biggest revolution since Gutenberg's printing press; shrug and add some to their portfolios 'just in case'; dismiss it as a fraud; or completely ignore it in favour of 'safer' transactions and financial products. I can easily point you to even more intelligent, savvy and well-informed people who've taken each position. All I ask is that we decide from knowledge, not ignorance.

Of course, the usual boilerplate that this book doesn't constitute investment advice applies here. But I hope it'll equip you with what you need to make the most of it.

Whatever you decide, I wish you all the best in your financial journey. See you ahead!

Notes

[1]For more on the Dutch tulip craze and subsequent market crash in the 1630s, see: Andrew Beattie, "Market Crashes: The Tulip and Bulb Craze," *Investopedia*, (no date), at http://www.investopedia.com/features/crashes/crashes2.asp.

[2] Dimon quotes in: Hugh Son, Hannah Levitt and Brian Louis, "Jamie Dimon Slams Bitcoin as a 'Fraud,'" *Bloomberg*, 13 September 2017, at https://www.bloomberg.com/news/articles/2017-09-12/jpmorgan-s-ceo-says-he-d-fire-traders-who-bet-on-fraud-bitcoin. Draper quotes in: Laura Lorenzetti, "Venture capitalist Tim Draper wins government bitcoin auction," *Fortune*, 2 July 2014, at http://fortune. com/2014/07/02/venture-capitalist-draper-wins-bitcoin-auction.

[3] An example of the latter use: 'Cryptozoology' is the study of unknown or speculative organisms, like the Sasquatch, the Yeti, modern dinosaurs or the Loch Ness Monster.

[4] Rob Price, "Someone in 2010 bought 2 pizzas with 10,000 bitcoins — which today would be worth $20 million," *Business Insider UK*, 22 May 2017, at http://uk.businessinsider.com/bitcoin-pizza-day-passes-2000-20-million-2017-5/?IR=T. The Bitcoin community marks 22 May as Bitcoin Pizza Day.

[5] Kenneth Rapoza, "Goldman Sachs Caves: Bitcoin Is Money," Forbes, 10 January 2018, at https://www.forbes.com/sites/kenrapoza/2018/01/10/goldman-sachs-caves-bitcoin-is-money.

[6] "Frequently-asked Questions and Myths," *Bitcoin.org*, (no date), https://bitcoin.org/ en/faq.

[7] For the uninitiated, FX is foreign exchange trading—that is, where international currencies like the US dollar, the euro or the Chinese renminbi are traded.

[8] For more on Melonport and the services it provides, see: Melon, "What Is Melon?" *Medium. com*, 28 June 2017, at https://medium.com/melonport-blog/what-is-melon-f9bf41600b7e.

[9] Quoted in Omkar Godbole, "Jamie Dimon says he regrets calling Bitcoin a fraud," *Coindesk*, 10 January 2018, at https://www.coindesk.com/jamie-dimon-says-he-regrets-calling-bitcoin-a-fraud

CHAPTER 1

THE NEW GOLD MINING

> Is a man not entitled to the sweat of his brow? "No," says the man in Washington, "it belongs to the poor." "No," says the man in the Vatican, "it belongs to God." "No," says the man in Moscow, "it belongs to everyone." I rejected those answers; instead, I chose something different. I chose the impossible. I chose... Rapture.
>
> *—Bioshock (2007)*

In this chapter, you'll see:

- How and why the idea of crypto was birthed
- The processes and thinking that shaped its creation
- How Bitcoin (and most crypto) differs from cash, stocks and bonds

It is said that when then-California Governor Ronald Reagan visited a university in the 1960s, a student told him there was no way people like Reagan could understand young people. "You grew up in a different world," he said. "Today we have television, jet planes, space travel, nuclear energy, computers."

Reagan simply replied, "You're right. It's true that we didn't have those things when we were young. We invented them."[1]

Perhaps blockchain technology, and the cryptocurrencies and other applications that run on it, is our own generation's answer to Reagan. It might seem that crypto is entirely new, and indeed few people understand how money can be transacted safely without a single authority (like a bank) to make sure it's sent in the right amount, to the right person, at the right time.

As crypto took off, Satoshi Nakamoto himself would wonder how to explain it to others.

"Writing a description of this thing for general audiences is bloody hard," he once wrote. "There's nothing to relate it to."[2]

The best way to grasp the birth of crypto is to look into the past. It all starts with people trying to solve a defined problem—be it making fire, working out the speed of light or learning the structure of the DNA molecule.

The birth of the blockchain concept, and Nakamoto's rise to fame, can be compared (believe it or not) to the work being done on DNA in the 1950s. The iconic double helix was deduced by the work of biologists James Watson and Francis Crick, who noted in their famous 1953 paper, "A Structure for Deoxyribose Nucleic Acid": "It has not escaped our notice that the specific pairing we have postulated immediately suggests a possible pairing mechanism for the genetic material."[3]

That discovery won them the Nobel Prize. Notice that Watson and Crick were simply studying the DNA molecule to learn its structure—in hopes of unlocking the chemical basis of life, as one of many teams to do so. With their discovery came a promising new avenue, a means by which cells replicated their genetic material. Nearly all of what we know about genetic science stems from that single discovery, and the paper that followed.

Similarly, Nakamoto was working on a widespread, well-known problem among software engineers when he made the proposal that changed everything.

Cash Is King

Today, we send money to vendors and each other via bank transfer, PayPal or some other system that we take for granted. But we're using the winners of a competition held decades ago, when it was realised that financial transactions could indeed be made over the Internet. It may seem remote to us now, but the eighties were a time of great technological uncertainty as many of the things we take for granted today were still being figured out.

The idea of digital cash isn't new; it dates back to proposals made in the 1980s by mathematician David Chaum, whose paper "Untraceable Electronic Cash," outlined ecash, a system of anonymous cash transfers over the then-new Internet. He found partners in cryptography (that is, the science of encoding information so it can only be seen by its intended recipients) and started his own company, DigiCash, in an attempt to commercialise the idea.

"At this moment in history," observes finance writer Dominic Frisby, "credit cards were still considered unsafe and insecure. It was not clear who was going to win the battle to control internet payments."[4]

Of course, no prizes for guessing which system won out in the end. Despite much interest from partners like Microsoft (which wanted to integrate ecash into Windows 95) and major banks such as ING, Chaum insisted on holding out for more money—refusing to sign lucrative deals that might have sealed his product as a pioneer of electronic cash transfer. In the end, his backers

lost interest and the offers dried up as they sought a less obstinate partner. Credit cards won that battle, and in 1999 Digicash went out of business entirely.

Other models would be tried. Frisby cites e-gold, which allowed users to buy physical gold using accounts on its website, and sell portions of it to others. Its pioneering firm grew into a success story from its founding in 1996, until its widespread use by criminals led to the FBI taking an interest in the late 2000s. "It fell victim to hacking, fraud and identity theft [...] By 2009, it had been shut down. Its founders faced all sorts of legal calamities—and are still dealing with the fall-out." [5]

Perhaps, Frisby notes, this is one reason why Nakamoto remains completely anonymous. If he were conclusively identified, it would make Bitcoin far more susceptible to regulation, and therefore much less empowering than he envisioned it to be.

Nakamoto definitely had the fates of ecash and e-gold on his mind when he wrote:

> A lot of people automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990s. I hope it's obvious it was only the centrally controlled nature of those systems that doomed them. I think this is the first time we're trying a decentralised, non-trust-based system.[6]

Because the past attempts at digital cash were set up by established companies with names, faces and identities to them, they were tied entirely to the people that produced them. In other words, they had a central point of failure—something Bitcoin,

with its peer-to-peer, networked nature doesn't have. Because no one can be said to administer Bitcoin, there's no single entity whose trouble will spell the end.

Double-Spending

Why are banks still needed when you transact digitally? Because their authority is needed to verify that you haven't spent money you don't (or no longer) have.

You see, electronic payments have a vulnerability that physical ones don't, namely the problem of *double-spending*—the possibility that a packet of data representing a given transaction is sent, but a copy kept by the sender so they appear not to have sent anything. When money is sent in the form of electronic data, it's far easier to duplicate, as it's simply a matter of copying and pasting code. Physical currency by definition is more difficult to fake, needing expensive counterfeiting equipment to defeat the measures that mints have put into place.[7] Also, a genuine coin or note can only exist in one place at a time. Once you've spent it, it's gone from your possession.

Besides processing the payment, computers belonging to your issuing bank need to verify that you're you and that you actually have the money you're sending. After you've sent it, they must confirm that it's no longer in your possession. Those are the tests your transaction needs to pass before you can see that comforting green tick on the screen.

Investopedia outlines the problem as follows:

> Double-spending is a problem unique to digital currencies because digital information can be reproduced relatively easily. Physical currencies do not have this issue because they cannot be easily replicated, and the parties involved in a transaction can immediately verify the bona fides of the physical currency. With digital currency, there is a risk that the holder could make a copy of the digital token and send it to a merchant or another party while retaining the original.[8]

A simpler explanation is offered by Ofir Beigel of 99Bitcoins.com. Suppose a sender has only one bitcoin. He makes a transaction sending that bitcoin to recipient A, sending it into a pool of unconfirmed transactions. Before Transaction A can be confirmed, the sender makes another one-bitcoin transaction, sending it to recipient B.

Now both transactions are in the pool, awaiting confirmation by the network. The transaction that gets confirmed first is treated as final, and the second is discarded. But what if the confirmation process for the two happened simultaneously? "Both transactions will show that I have the money needed," Beigel points out. In other words, the same bitcoin (or dollar) can be spent twice! [9]

I'll say more about how Nakamoto dealt with this problem in the next chapter. Traditionally, the problem of double-spending has been solved through financial institutions (which Nakamoto called '*mints*') setting their services up as intermediaries that verify that each party in the transaction

is who they say they are, and that all monies successfully sent are received in good order.

But there is one very, very serious flaw with this approach: That you have to entrust your money with a financial authority, and as history has shown, it leaves that money vulnerable to poor risk management on their part.

When They Let You Down

Nakamoto and his fellow coders were deeply sceptical of the central control wielded by said trusted authorities—and the possibility that they were taking unwarranted risks with money they did not own. The concept of Bitcoin grew out of the 2008 financial crisis, a time when many people lost faith in banks and central authorities.

As 'Prypto', the author of *Bitcoin for Dummies*, tells it:

> As the global financial system teetered on the brink of collapse, many central banks engaged in quantitative easing—or in simple terms, turned on the printing presses. Central banks flooded the markets with liquidity and slashed interest rates to near zero in order to prevent a repeat of the Great Depression of the 1930s.
>
> The effect of this was large-scale fluctuations in fiat currencies and what has since been termed currency wars—a race to competitively devalue so that an economy can become more viable simply by its goods and services being cheaper than those of its neighbors and global competitors.[10]

The result? Currencies lost value as more of it got printed, and governments were forced to pay billions of taxpayer dollars to save failing banks. The entire financial market took many terrible shocks that are still being felt today, nearly a decade on. It became suspected by many that central bankers:

> ... were taking many economies into the unknown and were prepared to devalue their fiat currencies at will just to keep the wheels turning. In doing so, they bailed out the very same institutions and bankers whose reckless behavior had brought about this crisis in the first place.[11]

To Nakamoto, currency control was too critical to be left completely to bankers and financial institutions. By believing that financial institutions knew better and entrusting such authority to them, entire populations (and their governments) were setting themselves up for failure. "The root problem with conventional currency is all the trust that's required to make it work," he told forum users at the P2P Foundation. "The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust."[12]

Rather, he believed that a secure, tamper-proof payment system that bypassed the need for central verification (while replicating the ability of mints to handle transactions) was the solution. He realised that the key was not to trust anyone or anything but the sheer power of industrial-grade encryption and the ability to break it.

Nakamoto's plan would rest on *decentralisation*, or breaking up the load of creating, decrypting and distributing the money

into smaller processes performed by different entities. To do this, he would have to solve four key problems:

- How can identities be verified in a way satisfactory to both parties?
- How can everyone agree on what transactions have been made, and when?
- How can everyone be sure that they have the latest information?
- How can the records, once set, be protected from being tampered with?

We don't know if Nakamoto actually set out to create a new currency with the same agreed-on worth as others, but that was the natural direction his discovery took him to. The result was his 2008 white paper "Bitcoin: A Peer-to-Peer Electronic Cash System,"[13] which he first published to the cryptography mailing list of metzdowd.com. Its architecture was simple in its construction, and I'll go through the basics of Nakamoto's paper and Bitcoin, the first cryptocurrency, in the next chapter.

Bitcoin's birthday is regarded to be 3 January 2009, when Nakamoto released the first-ever 'block' of Bitcoin, a package of 50 coins known to this day as the Genesis Block. At the same time, he released the full source code of the Bitcoin software on open-source distribution site SourceForge—all 31,000 lines of it. The first recipient of bitcoins was one of Nakamoto's closest collaborators, a programmer named Harold 'Hal' Finney. (Sadly, Finney died in 2014 of motor neurone disease; if he knew who Nakamoto really was, he has taken the secret to his grave.)

It's possible, even likely, that Nakamoto is actually an entire development team hiding behind a single pseudonym. This is the conclusion reached by several researchers who have studied Bitcoin's source code, including cybersecurity pioneer Dan Kaminsky, who attacked it in every way he knew—only to give up when the code resisted every attempt.

And thus the new currency was born. A cash exchange system not issued by a central bank, and with records maintained by computers around the world, not a single entry point where hackers could enter and steal. Once Bitcoin came online, it was indestructible from any single point; no government, hacker or power can shut Bitcoin down, because as long as even one node is active, Bitcoin will continue to exist.

Crypto Today

Just as genetic science in the post-double helix world exploded, so did financial markets when the true implications of Nakamoto's work emerged. I'll share more about why Bitcoin is so controversial, but the result has been the proliferation of new forms of electronic currency (Bitcoin alternatives, or *altcoins*) that claim to do what Bitcoin does, or better. Some even have the backing of the very same banks that Nakamoto worked to cut down to size.

At the very least, you'll be hard-pressed to find a modern bank that doesn't take the idea of crypto very, very seriously, to the extent of publishing about it, partnering with crypto startups or introducing laws to protect people from scams and crashes. As the fintech chief of Singapore's Monetary Authority, Sopnendu Mohanty, has said: "We know exactly when to intervene, based on the market size and the demand and transaction volume, and

we will come in at the right time. So, I'm not overly worried about getting to some large financial system crisis."[14]

Will the Real Satoshi Nakamoto Please Stand Up?

What has become of Nakamoto himself? He quietly handed over his websites and Bitcoin programming assets, then vanished from the community in 2010, citing his move to "other projects".

Whoever Nakamoto really is, he (or they) would never assume the identity again. However, there is no guarantee that he will not resurface or be unmasked—whether by his own hand or some brilliant detective work—at some point in the future.[15]

The secrecy is not for want of trying, and when the value of Bitcoin increased sharply over the years, journalists took great pains to try to expose him.

None have succeeded. A recent rumour has it, however, that he may be working with blockchain startup Ethereum.

Whether Nakamoto truly succeeded in eroding the power of central banking and mint-verified payment remains to be seen. What he did do was kick off an entirely new market worth hundreds of billions of dollars that did not even exist a decade ago. You'll find crypto used by everyone from well-known businesses to criminals on the Dark Web, and thousands of merchants accept payment in Bitcoin and other cryptos—wherever it is allowed as legal tender.

What's the Big Deal, Anyway?

The birth of Bitcoin and the entire cryptocurrency movement is ushering in a new era of technological independence, with people participating in it as they choose—rather than being hand-held, or arm-twisted, into accepting terms and conditions that may not be to their liking. One way of thinking about it is considering that crypto and blockchains are to Uber or Grab as banks are to traditional taxi and car rental firms.

In both cases, the former provides convenience and participation at each person's own discretion, though one must necessarily give up some control, safety and a formal accountability structure. Instead, you're the sole decision-maker of what happens to your crypto—though what you learn in this book and from the community will be a great help in storing, investing and using it.

A look at the market shows how popular Bitcoin has become. Since 2011, Bitcoin's value has shot up thousands of times, and is steadily increasing to this day. This is a credit not just to Bitcoin, but the model itself; altcoin Ethereum's value has been rocketing up since mid-2016.

This freedom must be responsibly used, though—because once you lose access to your crypto or make a transaction you later regret, there's no way to reverse it, short of the recipient willingly sending it back to you. In this book, I'll share not only the processes, but the thought patterns you must bring to the party so as to handle crypto safely.

Just turn the page to get started.

Your New Blocks

- Bitcoin was conceptualised as a means of electronic cash transfer which eliminated the need to trust any centralised entity or institution.
- Double-spending is a problem unique to electronic cash transfer; because the money exists only as computer code, there must be a way to prevent a single dollar from being copied and spent over and over again.
- The double-spending problem in electronic cash transfer was traditionally solved by a trusted party (such as a bank) declaring the transaction complete; Bitcoin achieves this by decentralising the process and having multiple Internet-connected computers compete to do so.
- Owners are the sole decision-makers of what happens to their cryptocurrencies—there is no authority over the system itself.
- Despite its anonymous origin, Bitcoin has now become a commodity worth millions of dollars in its own right.

Notes

[1] Quoted in Ronald Reagan, "Remarks and a Question-and-Answer Session With Senior Citizens in Los Angeles, California," *UCSB American Presidency Project*, 6 July 1982, at http://www.presidency.ucsb.edu/ws/?pid=42708.

[2] Satoshi Nakamoto, post in "Slashdot Submission for 1.0," 5 July 2010, Bitcoin forum, at https://bitcointalk.org/index.php?topic=234.msg1976#msg1976.

ABOUT THE AUTHOR

Leng Hoe Lon, CFA serves as Executive Advisor of Kyber Network (www.kyber.network), a decentralised cryptocurrency exchange powered by Ethereum smart contracts and is also an angel investor of Digix Global (https://digix.global), a company that aims to tokenise physical assets and make them fungible on the Ethereum blockchain in order to increase the pool of liquidity in a decentralised marketplace. Before this, he was CEO of machine-learning startup Shentilium Technologies, and co-founder of trading and mentoring firm TrackRecord Asia.

Before his foray into entrepreneurship, his 19-year financial trading career saw him holding the positions of Portfolio Manager at Tudor Investment Corporation (2011-2016); CEO at Tudor Capital Singapore (2013–2015); Managing Director at Goldman Sachs (2007–2011); ABN AMRO (2004–2007); JP Morgan (2003–2004); Deutsche Bank (1997–2003). He holds a Bachelor's Degree in accounting and finance from the University of Warwick, England.