



**BUBBLE**  
**OR**  
**REVOLUTION?**





*The Present and Future of Blockchain  
and Cryptocurrencies*

Neel Mehta  
Aditya Agashe  
Parth Detroja

Bubble or Revolution  
Copyright © 2019 Paravane Ventures  
Published by Paravane Ventures  
[bubbleorrevolution.com](http://bubbleorrevolution.com)

1<sup>st</sup> Edition, June 2019

All rights reserved. This book or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of the publisher except for the use of brief quotations in a book review.

The information contained herein is for educational and entertainment purposes only. Every attempt has been made to provide accurate, up-to-date, reliable, and complete information. No warranties of any kind are expressed or implied. Readers acknowledge that the authors are not engaging in the rendering of legal, financial, medical, or professional advice.

By reading this document, the reader agrees that under no circumstances are we responsible for any losses, direct or indirect, which are incurred as a result of the use of information contained within this document, including, but not limited to, errors, omissions, or inaccuracies.

All opinions expressed herein are solely the views of the authors and not those of their employers.

ISBN-13: 978-0-578-52815-1

*To my friends and family, for supporting me no matter how crazy my dreams  
get —Neel*

*To my family and friends, thanks for supporting my passion for business and  
helping me push past my fears to embrace entrepreneurship —Adi*

*To my friends and family for their never-ending support in my seemingly  
ridiculous endeavors —Parth*



# Contents

<b>Introduction</b>	<b>1</b>
The goal	4
What's inside	4
Our first book	5
Who we are	6
Thank you, and enjoy!	6
 <b>Chapter 1. Bitcoin</b>	 <b>7</b>
The trouble with credit cards	8
Decentralized, digital currency	10
Not quite Venmo	10
 <b>Chapter 2. Blockchain</b>	 <b>17</b>
The shared Excel sheet	18
Stone rings	19
Mining	24
Bitcoin's philosophy	27
 <b>Chapter 3. Bitcoin Economics</b>	 <b>31</b>
The \$70 million pizza	32
Growth	35
Inflation and deflation	37

The myth of the solo miner	40
<b>Chapter 4. Bitcoin's Blunders</b>	<b>45</b>
The big crash	46
The \$450 million hack	50
Mining and global warming	55
Dark markets	56
Centralization	59
<b>Chapter 5. Altcoins</b>	<b>65</b>
The Bitcoin hard fork	66
Ethereum	69
Tether and stablecoins	74
Monero and cryptojacking	76
<b>Chapter 6. The Public Blockchain</b>	<b>81</b>
Online voting	82
Decentralized marketplaces	85
An immortal internet	91
Hooters rewards on the blockchain?	96
Trademarks on the blockchain	99
Decentralizing websites	101
<b>Chapter 7. Business on the Blockchain</b>	<b>107</b>
Walmart and preventing foodborne illnesses	108
Stocks and blocks	112
Xbox and game royalties	115
The masters of private blockchains	117
<b>Chapter 8. Cryptocurrency Policy</b>	<b>121</b>
Crypto bans	122
Venezuela's state-backed cryptocurrency	125



ICOs and scams	128
ICO regulation	134
<b>Chapter 9. What's Next</b>	<b>139</b>
Facebook's cryptocurrencies	140
Tokenization	145
China's yuan tokenization	149
The Internet of Things and going beyond the blockchain	152
<b>Chapter 10. Bubble or Revolution?</b>	<b>159</b>
The future of money	160
The real uses of cryptocurrencies	165
Private vs. public blockchains	170
Bubble or revolution?	174
<b>Conclusion</b>	<b>181</b>
<b>Acknowledgements</b>	<b>183</b>
<b>Index</b>	<b>187</b>
<b>Notes</b>	<b>197</b>



# Introduction

*Bitcoin is a tool for freeing humanity from oligarchs and tyrants, dressed up as a get-rich-quick scheme.*

— Naval Ravikant, founder of AngelList<sup>1</sup>

*Bitcoin is probably rat poison squared.*

— Warren Buffett, CEO of Berkshire Hathaway<sup>2</sup>

THE YEAR was 2017, and the United Nations had a problem. Because of Syria's bloody civil war, ten thousand Syrian refugees had fled to a refugee camp in neighboring Jordan.<sup>3</sup> The UN's World Food Program (WFP) had set up supermarkets in the camp where refugees could buy items like olive oil and lentils, and they needed to give refugees some money to buy these items.<sup>4</sup>

The problem was that just giving refugees prepaid credit cards wouldn't work. This approach had cost the WFP millions in the past due to transaction fees and the need to build partnerships with local banks — money that could have gone toward millions of meals.<sup>5</sup> Giving refugees ID cards that entitled them to goods wouldn't work either; when the WFP had tried this in the past, local tribal leaders had snatched up refugees' cards and began trading them as currency.<sup>6</sup>

So the WFP turned to a fledgling technology called the blockchain, most famous for being the technology behind the digital currency Bitcoin. Each refugee's "account" was credited with some money, and when a refugee went to a store, they'd verify their identities with an iris scanner and then redeem these credits for food and supplies — all without opening their wallets.<sup>7</sup> The shops could then sell their collected coupons back to the UN.<sup>8</sup>

This project, called Building Blocks, was a smashing success. It slashed money-transfer fees by 98%,<sup>9</sup> reduced fraud, and radically simplified the aid process for both the WFP and refugees.<sup>10</sup> The UN quickly grew the program to serve 100,000 refugees,<sup>11</sup> with a plan to eventually serve all refugees in Jordan.<sup>12</sup>

The benefits to the UN go beyond aid: the UN announced that it might one day be able to track refugees' identities and life history using the blockchain, thus helping refugees find jobs and loans in

new countries if their passports or educational records were destroyed.<sup>13</sup>

People around the globe have been incredibly excited about the blockchain and its sister technology, cryptocurrencies (such as the aforementioned Bitcoin). The *Harvard Business Review* wondered if the blockchain could upend the staid banking industry,<sup>14</sup> the famous venture capitalist Marc Andreessen said the blockchain was “the most important invention since the internet,”<sup>15</sup> and analysts worldwide believe cryptocurrencies will revolutionize money and technology as we know them.<sup>16</sup>

On the other hand, these mysterious new technologies have also earned a sinister reputation. Drug lords use Bitcoin to peddle drugs anonymously online,<sup>17</sup> cryptocurrencies have been accused of contributing to global warming,<sup>18</sup> and hackers demand payment in Bitcoin so law enforcement can’t track them.<sup>19</sup> And even the positive hype around these technologies often seems to go too far: an iced tea company, Long Island Iced Tea, added the word “blockchain” to its name<sup>20</sup> and saw its stock price almost quadruple.<sup>21</sup>

So what’s true? Are blockchain and cryptocurrencies a hype-fueled bubble, technologies with no legitimate use cases? Or are they revolutionary inventions that will remake governments, businesses, economies, and societies in their image? In other words: bubble or revolution?

## **The goal**

As the above stories show, blockchain and cryptocurrencies — collectively known as *crypto* — are among the most consequential and yet least understood new technologies of our time. Most public conversations about crypto are dominated by enthusiasts saying crypto will tear down banks and governments and pundits saying crypto is nothing but a scam. Not many people pause to break down how exactly these technologies work and what real potential they have.

In *Bubble or Revolution*, we want to change that. Through real-world examples, plain-English explanations, and unbiased analyses, we want to teach you how crypto works, where it's useful, and where it isn't. We'll tell you what we think of the bubble-or-revolution debate, but we'll also give you the tools you'll need to decide for yourself.

## **What's inside**

In *Bubble or Revolution*, you'll learn about the building blocks of blockchains and cryptocurrencies; explore their strengths and weaknesses using case studies; dive deep into their social, political, economic, and technical implications; and gain insight into their futures from our exclusive interviews with dozens of tech industry leaders.

Just a handful of the things we'll cover:

- The economics of Bitcoin mining
- Famous cryptocurrency hacks and flaws
- Xbox's blockchain for video games
- The SEC's regulation of crypto startups
- Currency tokenization and the future of money
- Facebook's emerging cryptocurrencies

## **Our first book**

When the three of us wrote the business bestseller *Swipe to Unlock: The Primer on Technology and Business Strategy*, we aimed to teach readers everything they'd need to know about the tech world, from the guts of Google's search algorithm to Facebook's high-level business strategies.

Each section in *Swipe to Unlock* is a real-world case study, posing a question you might have had yourself — how Spotify recommends songs, how self-driving cars work, and why Amazon offers free shipping even though it loses them money. We covered a wide range of technologies, from security to cloud computing to machine learning.

But since we wrote *Swipe to Unlock*, cryptocurrencies and blockchains have exploded into the public consciousness in a way that few other technologies have. It's essential that technologists, entrepreneurs, business leaders, and even casual observers understand these technologies — so we decided to write a book about them.

This book will be a deep dive into one key pillar of technology; if you'd like to gain a broader understanding of the tech landscape, frameworks for understanding tech business strategy, and a mental toolkit for evaluating new technologies, you might want to give *Swipe to Unlock* a read as well. Check it out at [swipetounlock.com](http://swipetounlock.com) or find it on Amazon.

## **Who we are**

Before we jump in, here's a bit more about us.

*Neel Mehta* is a product manager at Google and formerly worked at Microsoft and the U.S. government, where he created the country's first technology internship program for college students.

*Adi Agashe* is a product manager at Microsoft and formerly the founder and CEO of Belle Applications.

*Parth Detroja* is a product manager at Facebook and formerly worked in product and marketing roles at Microsoft, Amazon, and IBM.

## **Thank you, and enjoy!**

Thank you again for choosing to read *Bubble or Revolution!* We hope you find this book informative, interesting, and maybe even fun. From all of us — enjoy!

*Neel Mehta*

[namehta.com](http://namehta.com)

[linkedin.com/in/neelmehta18](https://www.linkedin.com/in/neelmehta18)

*Aditya Agashe*

[adityaagashe.com](http://adityaagashe.com)

[linkedin.com/in/adityaagashe](https://www.linkedin.com/in/adityaagashe)

[quora.com/profile/Adi-Agashe](https://www.quora.com/profile/Adi-Agashe)

*Parth Detroja*

[parthdetroja.com](http://parthdetroja.com)

[linkedin.com/in/parthdetroja](https://www.linkedin.com/in/parthdetroja)



# *Chapter 1.*

# **Bitcoin**

*Trusted third parties are security holes. Anybody in the blockchain space, I would like to get that in their head. That's basically the key to the whole design.*

—Nick Szabo, creator of Bit Gold (a precursor to Bitcoin)<sup>1</sup>

**I**F YOU want to learn about the world of blockchains and cryptocurrencies, you have to start by learning about the most famous cryptocurrency and the most famous technology built on blockchains. That technology is Bitcoin. And if you want to learn about Bitcoin, you have to start by thinking about something as innocuous as a credit card.

## **The trouble with credit cards**

When you pull out your credit card to pay for something, the process seems easy enough: you swipe your Chase Visa card for a \$5 pizza at Pizza Hut, you get the pizza, and at the end of the month Chase sends you a bill for \$5. Credit cards are easy, fast, and accepted everywhere.

But there's a lot more going on behind the scenes. When you swipe your card, Pizza Hut asks its bank to ask Chase to approve the transaction. Once it's approved, Pizza Hut asks its bank for the \$5, its bank asks Visa for \$5, and Visa asks Chase for \$5. Chase gives Visa the \$5 minus a fee called the interchange fee (about 2%), or about \$4.90. Visa gives Pizza Hut's bank \$4.90 minus a small assessment fee of 0.1%, which is about \$4.89.<sup>2</sup> Pizza Hut's bank gives Pizza Hut \$4.89. And at the end of the month, Chase bills you for \$5.<sup>3</sup>

That pizza was worth \$4.89 to Pizza Hut, but you paid \$5 for it. The remaining 11 cents went to fees to Chase and Visa, who mediated the payment between you and Pizza Hut. That 11 cents may not sound like much, but for every million dollars of pizza that Pizza Hut sells, \$20,000 is lost in fees. And those fees are ultimately passed on to you, the consumer.

Meanwhile, if you'd just paid Pizza Hut with a \$5 bill, there would be no Chase and no Visa standing in the middle of the payment,

and hence no fees. (This is why many low-budget shops are cash only, and why gas is often cheaper if you pay with cash than with card.)

The takeaway here is that anyone who stands between buyers and sellers — a *middleman* — charges fees. And it's not just money that flows through middlemen; it's data too. So, when using credit cards, you're trusting banks like Chase and credit card networks like Visa to keep your data safe. But these middlemen have been breached many times: JPMorgan was hacked in 2014,<sup>4</sup> and in 2012 hackers stole the data of thousands of Visa and MasterCard customers.<sup>5</sup>

Meanwhile, cash is totally anonymous, there's nothing to hack, and nobody can steal your money unless they're right next to you (which, to be fair, can happen).

Unless you're using cash, it's tough to get rid of middlemen. Apple Pay is just build on top of your credit card. Paying with Venmo means your money flows through your bank and PayPal, Venmo's parent company. Checks don't come with fees, but you still have to have a bank account in the first place to use them, which is a problem for the world's 2 billion unbanked people.<sup>6</sup>

In short, if you want to avoid the fees, security holes, and accessibility constraints that come with having middlemen, you have to use cash. But cash has its own problems: it's a pain to count, store, and transport, and it fails utterly for long-distance or digital payments. This is all due to the physicality, or *tangibility*, of cash; you can't efficiently make payments in our digitized, globalized world with physical objects you have to haul around. Meanwhile, credit cards and other middlemen-powered payment systems are terrific for long-distance, digital payments.

So you can avoid either the tangibility problem (physical objects are poor forms of currency in this day and age) or the middleman problem (they come with fees, security holes, and accessibility constraints). You can't have both. Right?

## **Decentralized, digital currency**

Another way to phrase that tradeoff is between *decentralization* (another word for not having middlemen) and *digitization* (another way of saying intangibility). *Centralization* is just another way of saying there are middlemen; in a *decentralized* system like cash, there are no middlemen, and money goes straight from buyer to seller, or *peer-to-peer*. Credit cards (and Venmo, Apple Pay, etc.) are digitized but not decentralized; cash is decentralized but not digitized.

In 2008, a computer scientist calling himself Satoshi Nakamoto announced he had created a payment system that was *both* decentralized and digital. There were no banks or credit card companies standing between buyers and sellers, and hence he promised lower fees and no single points of failure or targets for hackers. And, at the same time, his payment system worked great for long-distance, digital payment. In fact, it was a purely digital currency.

He called it Bitcoin.<sup>7</sup>

## **Not quite Venmo**

The first question to answer about Bitcoin is: how does this thing work, anyway?

At first glance, Bitcoin looks a lot like conventional money-sending apps like Venmo. You can buy bitcoins to load into your account,

## Bitcoin

send bitcoins to others, receive bitcoins from people, and “cash out” to send your bitcoins back to your bank.

The screenshot displays the Coinbase 'Buy' interface. The top navigation bar is blue with the 'coinbase' logo and a user profile icon. Below the navigation bar, there are links for 'Dashboard', 'Buy/Sell', 'Accounts', 'Tools', and 'Settings'. A green button labeled 'Invite friends, earn \$10' is on the right.

The main content area is divided into two sections: 'Buy' (active) and 'Sell'. The 'Buy' section shows the following details:

- Cryptocurrency:** Bitcoin (BTC) at a price of \$6,302.45.
- Payment Method:** Bank of America.
- Amount:** 5 USD, which is equivalent to 0.00063626 BTC. A daily bank limit of \$25,000.00 remaining is shown.
- Repeat this buy:** Options for Daily, Weekly, Every two weeks, and Monthly.
- Buy Bitcoin - \$5.00** button.

The right section, titled 'YOU ARE BUYING', shows the summary of the purchase:

- 0.0006 BTC** at \$6,302.45 per BTC.
- Payment Method:** Bank of America.
- Deposit to:** BTC Wallet.
- Available to trade on Coinbase:** Instantly.
- Available to send off Coinbase:** In 7 days. A link 'Need to send instantly?' is provided.
- Summary:**
  - 0.00063626 BTC ..... \$4.01
  - Coinbase Fee ..... \$0.99
  - Total ..... \$5.00**

A link 'Learn more about our fees [here](#).' is at the bottom of the summary section.

*Loading \$5 worth of bitcoins into an account using the Bitcoin exchange Coinbase.*

Send BTC

Wallet Address Email Address

A miner fee will be added for sends to BTC addresses. Miner fees do not go to Coinbase. To avoid miner fees, send to an email address. [Learn more.](#)

Recipient

Available to send [Don't see all your funds?](#)

BTC Wallet 0.0006 BTC  
= \$3.98

Amount

1 USD ⇌ 0.00015997 BTC

Note

Thank you, Internet Archive!

Continue

© 2019 Coinbase

*Sending bitcoins with Coinbase. In this case, we are sending \$1 worth of bitcoin to the Internet Archive as a donation.*

If you look a bit closer, however, you'll notice some distinctions:

First, instead of loading dollars into your account, you convert them into bitcoins (the coins themselves are lowercase-b *bitcoins*; the currency is uppercase-B *Bitcoin*) at a particular exchange rate. This is similar to how you can convert dollars to euros (or any

other normal, or *fiat*, currency). This conversion is done at a website known as a *Bitcoin exchange*; there are dozens of these around the world, such as Coinbase and Bittrex.<sup>8</sup>

Your money is kept in a *wallet* instead of an account. What's more, instead of usernames, Bitcoin runs on *addresses*, which are long, garbled-looking strings of numbers and letters. In our example screenshots, we sent money to *1ArchiveIn2C579dMsAu3iC6tWzuQJz8dN*, which is the address of the nonprofit Internet Archive,<sup>9</sup> a site that saves past versions of webpages so they don't get lost to the ravages of time. Wikileaks has a somewhat famous address, too: *1HB5XMLmzFVj8ALj6mjBsbjRoD4miY36v*.<sup>10</sup>

And, instead of passwords, Bitcoin uses *private keys*. You can run a private key through a mathematical function to get an address, but you can't go the other way (much like how you can easily figure out a person's initials if you know their full name, but you can't determine someone's full name for sure if you only know their initials). This way, Bitcoin users can prove their identity without having to trust their private key to some company's database, which you have to do with your passwords for conventional services.

Sending money doesn't incur any credit card fees, but it does incur a *mining fee*. In our example, the mining fee was 80 cents (pretty hefty when you consider we were only donating \$1!). We'll explore what mining fees are in later chapters.


Finally, in Venmo, each dollar in your account is always worth \$1 — but here, the conversion rate between dollars and bitcoins fluctuates, just like a stock price does. That means you can buy bitcoins, hold on to them, and sell them when the price goes up.

Confirm BTC Send

Transaction Details

To	1A1... 1A1... 1A1... 1A1...
Amount	0.00015997 BTC \$1.00
Coinbase fee	\$0.00
Miner fee ?	0.00012843 BTC \$0.80
Total	0.0002884 BTC \$1.80
Note	Thank you, Internet Archive!

Enter the 2-step verification code provided by SMS to your phone



0 0 0 0 0 0 0

Didn't receive the SMS?

[Re-send SMS](#)

Go Back

Confirm

*Sending bitcoins requires you pay a “mining fee.”*



# Bitcoin

coinbase

Dashboard Buy/Sell Accounts Tools Settings Invite friends

Buy Sell

Don't see all your funds?

Sell From BTC Wallet 0.00034789 BTC ~\$2.76

Deposit To How to withdraw funds from Coinbase Cash (USD)

Amount 2.74 USD ⇌ 0.00034789 BTC

Sell Bitcoin Instantly - \$1.75

YOU ARE SELLING 0.0003 BTC @ \$7,876.05 per BTC

Withdraw From BTC Wallet

Available Instantly

Deposit To Cash (USD)

0.00034789 BTC ..... \$2.74  
Coinbase Fee ..... \$0.99  
Total Payout ..... \$1.75

Learn more about our fees [here](#)

*You can sell bitcoins for dollars much like you can sell stocks and bonds.*

So, at this level, Bitcoin looks like a strange hybrid of Venmo and a stock-trading app: you can use it to send and receive money, but you can also use it as a pure investment vehicle. It's almost as if you could send your friends shares of stock on Venmo.

But that's not the main reason why Bitcoin is so different from normal monetary systems, and it's not why we're learning about it. For that, we'll need to understand the technology that Bitcoin is built on: the *blockchain*.



## Chapter 2.

# Blockchain

*Bitcoin gives us, for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer. The consequences of this breakthrough are hard to overstate.*

—Marc Andreessen, co-founder of Andreessen  
Horowitz<sup>1</sup>

THE BIG technological innovation behind Bitcoin, and the thing that makes it so unique, is the *blockchain*: a public, shared list of every Bitcoin transaction that's ever happened. It's a straightforward enough idea, but there's a lot to inspect under the hood.

## **The shared Excel sheet**

The remarkable thing about Bitcoin is that no banks, credit card companies, or other mainstream institutions are involved in transactions (besides converting bitcoins to and from fiat money). That is, you can send money to any Bitcoin user without a middleman standing in the way — and so, the usual fees, constraints, and security holes don't apply.

In Bitcoin, instead of a single entity (like a bank) verifying that a transaction happened, *everyone* collectively agrees that a transaction happened. At a high level, whenever you send someone bitcoins, your payment gets added to a giant shared list of all past transactions — known as a *shared ledger* or *blockchain*. It's as if all payments were stored on a giant public Excel spreadsheet and anybody could add a “row” for a payment, but nobody could erase or change a row once it was added.

This ledger is the official record of all past payments. Everyone can see every past transaction and thus prove to themselves that the payment happened. Because the ledger is shared, no one person owns it and nobody can censor it. And, as long as at least one person has a copy of the ledger, it'll never die.

## **Stone rings**

To make this definition of a blockchain concrete, let's look at a society whose traditional money system works strikingly similarly to the blockchain.

In the tiny Micronesian island of Yap, the traditional currency is giant stone rings, known as *rai stones*.<sup>2</sup> These stones are massive, with some reaching ten feet across and weighing as much as a pickup truck.<sup>3</sup>



*A rai stone, a traditional form of money on the Pacific island of Yap. Source: Wikimedia<sup>4</sup>*

What's unusual about these stones is that they change ownership, but they never physically move (imagine lugging one of these rocks to your house!). This is radically different from most traditional societies, where you couldn't buy anything without physically giving something — coins, shells, cows, you name it — to the

seller. You couldn't just say, "that rock over there now belongs to you," and expect to get something in return.

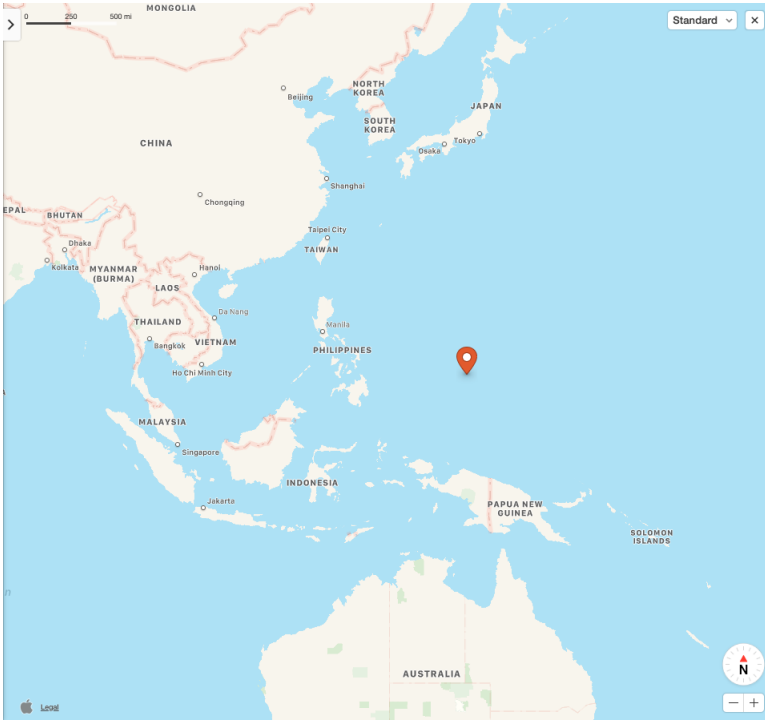
In a Yap village, dozens of rai stones are scattered around town, and everyone in the village agrees who owns each stone. There's an oral history of each stone's past ownership (e.g. "three years ago, the elder's son gave the rai stone by the beach to the carpenter's daughter") that each villager keeps in their heads. You can imagine that each villager gossips regularly with other villagers to keep their records of transactions up-to-date.<sup>5</sup>

Whenever someone buys something with a rai stone, the buyer announces that one stone they own now belongs to the seller. All the villagers update their mental records to account for the stone's new ownership, and the seller now owns the stone. The stone didn't physically move — nothing physically changed about it at all — but it changed ownership!<sup>6</sup>

It's hard to overstate how different this is from other traditional societies, where all changes of ownership involved physically moving things from one person's house to another.

In fact, you can even trade rai stones if they can't be physically seen. Hundreds of years ago, a ship carrying a rai stone sunk off the coast of Yap. But the villagers reasoned that the stone must still exist somewhere on the ocean floor, so people continued to own and trade the stone like nothing had happened.<sup>7</sup> (Meanwhile, try paying someone with coins that fell into the ocean!)

## *Bubble or Revolution?*



*The location of Yap in Micronesia. Source: Apple Maps<sup>8</sup>*

### *Intangible and decentralized*

In short, there are two really remarkable things about rai stones. First, they can be used as money without being moved, and indeed they don't even need to be accessible. In other words, they're *intangible*.

And second, the official history of the stones lives in villagers' heads, so that as long as the majority of villagers agree that a payment happened, it officially happened. If the village's chieftain disapproves of a transaction, there's not much they can do about it short of bullying half the population into agreeing with them. (Meanwhile, if the chieftain kept a log book of all



payments and that was the source of truth, the chieftain could easily delete payments they didn't like.) In other words, the rai stone system is consensus-driven and hence *decentralized*; the chieftain is the would-be middleman that gets cut out.

Yap's rai stone system is both intangible and decentralized. Remember that cash is decentralized but tangible, while credit cards are intangible but centralized — yet rai stones get both because they're consensus-based.

*Bitcoin, blockchain, and consensus*

Bitcoin works similarly to rai stones in that it's consensus-based. A Bitcoin transaction happened if a majority of people agree that it happened, just as a rai stone transaction happened if a majority of villagers agree that it happened.

And just as Yap villagers have a shared oral history of past payments, Bitcoin users have a shared history of past payments — that's the blockchain, which is stored as a giant list of payments on people's computers. And while Yap villagers gossip to synchronize their versions of history with others, Bitcoin users' computers constantly talk to each other to make sure they have the latest version of the blockchain.

And just as Yap chieftains can't easily interfere with rai stone payments, banks (and other potential middlemen) can't touch Bitcoin payments. While Bitcoin relies on thousands or millions of people agreeing on a history of payments, no single person or entity controls the payment history the way a bank or credit card company can for normal payment mechanisms.

In fact, you can track the exchange of anything on the blockchain if you want to; it doesn't have to be bitcoins. There are thousands of other digital currencies — known as *cryptocurrencies* — that use

consensus-based blockchains to track payments without a middleman. You can even track the movement of things that aren't money on a blockchain; blockchains can be used to track the movement of goods through supply chains, track healthcare data, and even track votes in digital elections. And it all starts with a concept pioneered by the villagers of Yap.

## **Mining**

When you pay with a Chase Visa credit card, Chase and Visa take care of checking that you're under your credit limit, verifying your identity, and making sure the transaction's metadata (the store's name, the date, etc.) is valid. In Bitcoin-land, there's no central authority to do these checks, so members of the Bitcoin community need to do them.<sup>9</sup>

But, of course, people won't do the computational work of verifying transactions for free, so Bitcoin has to throw in some money to incentivize people. These transaction-verifiers are known as *Bitcoin miners*.<sup>10</sup> (Bitcoin thinks of itself as a digital version of gold, hence the borrowed terminology.) Bitcoin miners verify batches of payments, known as *blocks*.

For their trouble, miners earn some fees from the payments in the block, and the Bitcoin software rewards them with a fixed chunk of bitcoins for every block of transactions they verify, or mine. At the time of writing, this reward — known as the *block reward* — is 12.5 bitcoins, but it gets halved every four years (it dropped from 25 to 12.5 in 2016 and is slated to drop to 6.25 in 2020).<sup>11</sup> Besides incentivizing miners to do the computational work, block rewards are also the only way new bitcoins get added to the economy.

The blockchain is just a chain of blocks — each block is mathematically tied to the one before it (this uses cryptography,

hence *cryptocurrency*), and miners' job is to attach a new block to the end of the chain. Each block depends on all the blocks before it, so if a single block earlier in the chain is tampered with, each following block will be invalid. (It's like a novel: if someone tore out the third chapter, every following chapter wouldn't make sense.) This way, Bitcoin users can be sure past transactions weren't tampered with.<sup>12</sup>

### *Proof-of-work*

The catch, though, is that mining a block isn't as easy as running a small snippet of code. If it was, a cheating miner could easily create a chain of fake transactions as long as the real blockchain, and nobody would be able to tell which chain was the legitimate one. To prevent this, Bitcoin actively makes it hard to mine a block; on average, it would take a computer working nonstop about 57 years<sup>13</sup> to mine a block!<sup>1415</sup>

How? Mining is basically a high-stakes guessing game. Anyone can do the verification computations and generate a block, but for that block to be accepted and added to the blockchain, the miner has to guess a magic number. Guessing this magic number is about as hard as rolling a 30 billion trillion-sided die and hoping you get a 1.<sup>16</sup> (This is a simplified model; see the footnotes for the gory details about mining.<sup>17</sup>)

Each "roll of the die" is called a *hash*, and miners just need to compute hashes nonstop in the hopes that one of them is the lucky one that gets their block approved.<sup>18</sup>

Because it takes so much work to mine a block, would-be fraudsters would have an extremely difficult time out-mining all the honest miners. (The longest blockchain is the official one, so a fraudster would have to make a longer chain — but, as we just saw, that's nearly impossible. This is the *longest chain rule*.<sup>19</sup>) This

mining system is known as *proof-of-work* because mining a block requires you to prove that you've done a whole lot of work.<sup>20</sup>

Proof-of-work is incredibly wasteful — it literally requires you to waste time and energy until you guess the right number — but it's only secure because it's so wasteful. (It's like having a giant lawn: it's a huge waste of water and takes a ton of energy to maintain, but it proves you're wealthy because only a wealthy person could afford to waste so much.<sup>21</sup>)

### *Difficulty*

Though it might take a solo miner decades to mine a block, there are millions of miners competing for the right to mine a block, so it only takes an average of 10 minutes for someone, somewhere to mine a block.<sup>22</sup> In Bitcoin-speak, this means the *block time* is 10 minutes.<sup>23</sup>

Over time, though, computers get more powerful and miners join or leave the network. This means that the total number of hashes, or “rolls of the dice,” per second is always changing; it increases if computers get stronger and miners join, and it decreases if miners leave. So, if the odds of getting the right hash stayed constant, the block time would constantly change.

To keep the block time at 10 minutes, the Bitcoin software adjusts the odds of getting the right hash every two weeks. By adjusting the *difficulty* like this, Bitcoin can ensure that the block time stays consistent.<sup>24</sup> (It's like a lottery: if you want to choose a winner every month, you need to constantly adjust the odds of a particular ticket winning when the number of tickets sold changes.)

## Bitcoin's philosophy

If we take a step back, the rough outline of Bitcoin takes shape. Payments are verified and approved by other people in the Bitcoin network (not a bank or credit card company), money is paid out by the mining algorithm (not some central institution), and the official history of payments lives on Bitcoin users' computers (not some bank's database). This is how Bitcoin promises to be a decentralized, digital money system; the people, not institutional middlemen, own the system.

It's hard to be sure exactly what Satoshi Nakamoto, the creator of Bitcoin, intended for Bitcoin to be, but one clue is hidden in the very first Bitcoin block ever mined. In this *genesis block*, Satoshi awarded himself 50 bitcoins and included this cryptic message:<sup>25</sup>

*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.*

This message referenced an article in the British newspaper *The Times*,<sup>26</sup> which mentioned that the Chancellor of the Exchequer (the head of the UK's treasury<sup>27</sup>) was considering pumping taxpayer money into failing British banks amidst the heights of the 2008 financial crisis. Bitcoin analysts have interpreted this to mean that Nakamoto distrusted the banking system and was angry that citizens were paying for banks' mistakes. Thus, the thinking goes, Satoshi created a currency that no bank or government could control — no taxes, no bank losses, no bailouts.<sup>28</sup>

Some of Satoshi's posts in internet forums hinted that he was a libertarian, expressing skepticism of government authority and seeking to "gain a new territory of freedom" with Bitcoin.<sup>29</sup> Beyond that, however, little is known about Satoshi's political leanings.

*The mystery man*

The reason we know so little about Satoshi's philosophy is simple: nobody knows who Satoshi really is!

The name "Satoshi Nakamoto" is almost certainly a pseudonym. The name has only been used for forum posts, a handful of emails, and the academic paper that introduced Bitcoin; Satoshi has never appeared in person and in fact hasn't written anything since 2011. Nobody has yet proven that they are Satoshi.<sup>30</sup>

Still, many Bitcoin fans have sought to learn Satoshi's true identity to gain insights into his vision for Bitcoin (and just out of sheer curiosity). Some people think Satoshi might be an alias for Wei Dai or Nick Szabo, computer scientists who created proto-cryptocurrencies that predated Bitcoin but never took off. (We asked Nathaniel Popper, the author of *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*, and he thought Satoshi was Szabo.) Others think Satoshi is actually a group of scientists.<sup>31</sup> The eccentric security entrepreneur John McAfee has claimed he's met Satoshi and threatened to expose him but quickly called off the plan; most people think McAfee was just blustering.<sup>32</sup>

The most substantial theory, in our minds, is that Satoshi is really British, and not Japanese, as he claimed. His original Bitcoin paper was full of British spellings ("favour" instead of "favor"<sup>33</sup>), and his forum posts were full of Britishisms ("bloody hard"<sup>34</sup>). He also rarely posted on forums between midnight and 6am GMT<sup>35</sup>, which would be the middle of the day in Japan but nighttime in the UK. Plus, he cited the British newspaper *The Times* in the genesis block.

Whoever Satoshi was and whatever his intentions were, his invention has had far more impact than he probably ever thought possible.





*Chapter 3.*

# **Bitcoin Economics**

*There are 3 eras of currency: Commodity based, politically based, and now, math based.*

—Chris Dixon, co-founder of Hutch (acquired by eBay)<sup>1</sup>

THERE'S NO denying it: Bitcoin is a major currency, and a multibillion-dollar economy has developed around it. But just as Bitcoin is very different from the dollars and euros we're familiar with, the Bitcoin economy operates with rules very different from those of the economies we usually interact with.

## **The \$70 million pizza**

In May 2010, a Florida man named Laszlo Hanyecz posted on a Bitcoin forum offering 10,000 bitcoins (then worth \$41) to anyone who would send him a pizza. A British man gladly obliged, ordering him two large pizzas from Papa John's.<sup>2</sup> It was the first time anyone had ever bought a real-world item with bitcoins.<sup>3</sup>

Those 10,000 bitcoins are now worth over \$70 million.



*The pizzas that Laszlo Hanyecz bought for 10,000 bitcoins in 2010.*

*Source: Laszlo Hanyecz<sup>4</sup>*