What's the Big Deal About Bitcoin?

Steve Patterson

Acknowledgements

Special thanks to my wife Julia for her support, to Isaac Morehouse for his encouragement, and to Matt Gilliland for his detailed feedback.

Thank you to all of my friends and family who volunteered their time to help me: Jason Dreyzehner, Joe Gibbs, Sam Patterson, and James Walpole.

Table of Contents

Introduction

Bitcoin keeps making headlines. Everybody is talking about it, from established financial gurus to twenty-something techies, and they all seem to come to different conclusions. Bitcoin has been called everything from a giant Ponzi scheme to the greatest technological invention in history. But most people, if they have heard of Bitcoin, have no idea what all the fuss is about.

The technology is notoriously hard to explain and understand, especially if you aren't a tech enthusiast. So, this book is meant to clearly explain Bitcoin to the layman. It is conceptual, rather than technical, and my goal is to give every reader a concrete answer to the question, "What's the big deal?"

As you read, it's natural to come up with objections and skepticism about Bitcoin. I ask that you hold your objections until you've read Parts One and Two, which give a thorough conceptual overview of the technology. After that point, please unleash your full skepticism; Part Three deals with common objections to Bitcoin and covers real challenges facing the technology.

My goal is not to endorse Bitcoin, though I have become convinced the technology is beneficial, but rather to provide enough information for readers to form their own opinion.

PART ONE
Bitcoin Clearly Explained

The Confusion

Bitcoin is a confusing subject. It's new technology, so most enthusiasts still speak in technical jargon. News coverage refers to Bitcoin without explaining what it is, and even the word "Bitcoin" has multiple meanings. This makes it difficult to figure out.

Before praising or condemning Bitcoin, the technology should be clearly understood. This book explains it using simple concepts in Part One, explores future possibilities in Part Two, and addresses common objections and challenges in Part Three.

The confusion surrounding Bitcoin can be clarified by breaking it into three distinct parts: computer software, a digital currency, and an online ledger. Together, they form a new type of payment system for the internet. Each of these components will be explained and connected to the others.

To begin, we should clarify our terms: uppercase "Bitcoin" refers to the computer software, and lowercase "bitcoin" refers to the currency.

Bitcoin, the software, can be understood in five words: it maintains an online ledger. The ledger is a public record of transactions, and the entire technology revolves around it.

You might ask, "What kind of transactions are being recorded on this ledger?" Well, the software creates, uses, and tracks its own unique type of currency, called "bitcoin."

So, the ledger is simply a record of bitcoin transactions, and it gets updated by computers running specialized software. Indeed, if you had to summarize the entire technology in one sentence, you might say, "Bitcoin is extremely advanced bookkeeping."

If that doesn't sound like a world-changing invention, don't worry – it's the specific details about the software, currency, and ledger that have so many people excited.

The Context

Before diving into the details, we need to set the stage. Bitcoin was not created in isolation. It was created within a larger context to fix a particular problem: modern payment systems are not suited for the internet.

We can easily send emails and files across the web, but we can't easily send a few dollars. We have to go through middlemen, using credit cards which are insecure and charge fees, bank transfers which are slow and expensive, or services like Western Union which take big percentage cuts of everything we send.

If you live in the United States, you can instantly have a face-to-face conversation online with your friend in England without thinking twice. If you want to send him $20, however, be prepared to jump

through hoops. You have to use a third party who will take anywhere from 3% to 20% of your money, fill out some forms, and hope that the weekend isn't coming up – that adds a few more days to the process. While a low 3% charge might not sound like much, when you're a large firm sending substantial amounts of cash, that can add up to thousands, even tens of thousands of dollars.

Security and Trust

On top of the expense, traditional payment methods are not secure. Think about our current system: every time you hand your credit card to somebody, they immediately hold all the information needed to spend money on your behalf. Forever. They can store this information for later, use it themselves, or even anonymously sell it to somebody else. In addition, many companies store this sensitive information in massive databases. Tens of millions of identities and numbers become centralized in one place, creating a criminal's ultimate jackpot. It shouldn't be surprising that credit card fraud and identity theft are rampant.

Millions of people (myself included) have had their sensitive information stolen from these databases. I am quite careful using my credit cards online, but even using my card *once* at Home Depot resulted in my information being stolen, along with countless other unfortunate customers'.

The current financial system has many moving parts, and therefore, requires a considerable amount of *trust* in third parties. Multiple individuals or companies – whether it's Visa, Western Union, your bank, the waiter swiping your credit card, PayPal, etc. – handle your

money and sensitive data before it reaches its final destination. This is both costly and insecure.

Unsound Currencies

Consider another problem: modern currencies have a consistent track record of losing value due to inflation. Whoever controls the issuance of money tends to create too much. It's not uncommon for currencies to be completely destroyed by inflation in a matter of decades.

Having one group control the printing press *also* requires trust. Whether it's a central bank, a national government, or a private firm, users need to trust that the total supply of their currency won't arbitrarily increase.

The Solution

Bitcoin was created to solve these problems and streamline payments over the internet. It is meant to be the equivalent of digital cash – a fast, easy, "peer-to-peer" payment system, meaning the sender and receiver exchange directly with each other. Paying in bitcoin is akin to personally handing somebody cash, without requiring any middlemen.

Bitcoin also has no central issuer. There's no "Bitcoin Corporation" or "Bitcoin Central Bank" deciding how much bitcoin should exist. The software itself, using mathematics, determines how much bitcoin exists and at what rate it is produced. I'll cover this in more detail later.

The technology was designed to be independent of banks, corporations, governments, or any centralized institution. Bitcoin, being digital cash, is the first *trustless* payment system. It doesn't require third parties handling your financial data, and it uses its own currency to eliminate the possibility of arbitrary inflation.

How was this accomplished? Through an extremely clever use of mathematics and software. The technical details of Bitcoin are not the focus of this book, and other people are more qualified to elaborate on them, but suffice to say a number of problems that had been plaguing computer programmers for years were solved by Bitcoin. Now money can be sent anywhere in the world, for almost no cost, as easily as sending an email.

The Ledger

The first component to understand about Bitcoin is the most important: the online ledger. It's called "the blockchain." That name was chosen for technical reasons which are not relevant to this book. Just understand that, whenever you hear "blockchain," we're talking specifically about the public online ledger which records all bitcoin transactions, and it's at the heart of the Bitcoin ecosphere.

Unlike every other ledger in existence, the blockchain does not reside in one place. It's not stored on one server. The blockchain is found on *every single computer running the Bitcoin software*. This is why it's often called "decentralized." No one group owns or controls the ledger; it's not like the internal bookkeeping at a bank like JP Morgan. The entire, enormous network of computers, spanning every

continent, are all in communication with each other updating and verifying the exact same ledger.

The record goes all the way back to the first bitcoin transaction. Anyone with an internet connection can download the history of every single bitcoin transaction that has ever taken place. As you can imagine, this dramatically reduces (or eliminates) the possibility for fraudulent bookkeeping. Ownership of bitcoin is not murky. If the ledger says you own bitcoin, you do. You can mathematically prove it.

The accuracy of the ledger can be trusted without faith in any one institution, bank, or government. Rather, it's a network of thousands of computers maintaining the ledger in sync with each other. And this network is *enormous*. The amount of computer power dedicated to securing the system is greater than the world's top five hundred supercomputers combined – by at least an order of magnitude. This is partly due to the uniqueness of the Bitcoin software. Specialized computers have been developed to run Bitcoin, and they are far more efficient at running the software than your regular computer or supercomputer.

Once a transaction is recorded, it is set in stone. In fact, it's reasonable to say that a bitcoin transaction, once verified and added to the ledger, is the most secure and certain piece of digital data in existence. It is permanently unalterable by anyone, thanks to a use of applied mathematics.

The power and cleverness of the blockchain invention cannot be overstated. Building such a system is enormously complex – impossible, before Bitcoin was created. People have attempted to create digital currencies for the last few decades without success. You have to solve questions like:

- How do you update everybody's ledger at the same time without a "master" ledger?
- How do you prevent fraudulent transactions?
- What happens if two ledgers ever disagree with each other?
- How do you prevent changes being made after-the-fact?

Bitcoin solves all of these problems for the first time, and it opens up a whole world of new financial innovations built on top of the blockchain (see Part Two).

So in summary, the public ledger is online, accessible and verifiable by everybody, stored in every single computer running the software, updated in sync across the network without directions from a central group or master ledger. And thanks to clever mathematics, it is unalterable and uncrackable for even the world's fastest supercomputers. That's quite an invention, and it's only the ledger.

The Currency

A ledger without a currency is a book without words. Every transaction recorded in the blockchain is denominated in the same currency: "bitcoin" – though occasionally the term "bitcoins" is more appropriate, as when referencing specific units (e.g. "I own five bitcoins" versus "I own some bitcoin")

This currency has a number of unique properties, some of which are unprecedented in the history of money. In fact, as somebody who is interested in economics, it was the properties of bitcoin-the-currency which first grabbed my attention. This section will give an overview of the currency and explain how it works. The economic

implications will be covered in Part Two, in the section entitled "Sound Money."

Digital Gold

Bitcoin as a currency was modeled after gold, because gold has the longest and most successful track record of any currency. The idea was to create, in essence, *digital* gold.

Gold's popularity is not coincidental; it has specific properties which make it useful as a currency. Most importantly, gold is a scarce resource. There is a finite amount of gold in the world, and the supply does not arbitrarily increase. Nobody can declare that more gold exists by law; the supply is not determined by any individual or group. Also, gold is difficult to extract from the ground, which means we can predict with reasonable accuracy what the future supply will be at any given time.

Bitcoin, too, is scarce. Only a finite amount will ever exist: twenty-one million bitcoins total, each of which is divisible down to one-hundred-millionth of a bitcoin.

Scarcity is especially unique in the digital world. With almost any piece of digital data, we can copy and paste, creating as many exact duplicates as we like. But being able to copy and paste digital money would be a catastrophe – everybody could become their own printing press. For reasons I will explain in a minute, you cannot copy and paste bitcoins. The supply is determined by mathematics and software, not by any individual or group.

The rate at which bitcoins are created is also predictable. The supply is based on a mathematical algorithm which *regulates its own*

production at a pre-determined rate. We can estimate to a very precise degree how many bitcoins will exist at any given time. This solves the problem of arbitrary inflation – a recurring flaw with currencies issued by a central group.

Bitcoin mirrors gold in some ways and improves on it in others. While gold has been successful as a currency, it has some drawbacks. For one thing, it's clunky. Try paying for a pack of gum in gold shavings, or for a house in gold bricks. Even worse, try using gold for international business or on the internet. The idea of shipping physical metal through the mail to trade internationally seems archaic, and you can't transmit gold bits through a phone line.

Portability is one area which bitcoin greatly outperforms gold. Because bitcoin is digital, you can send it to anybody on the planet with an internet connection, instantly, for virtually no cost. This is possible because of the special way in which the blockchain and currency relate to each other.

Digital Ownership

While a bitcoin owner might casually say, "I have a bitcoin on my computer," or "I have .02 bitcoin on my phone," that's actually not true. Bitcoins are not *literally* stored on your hard drive or phone. *They are stored in the blockchain itself*. If bitcoin is like gold, the blockchain is the gold vault.

Here's how it works: bitcoins are located at "addresses" on the public ledger. You can think of an address as simply an account at the gold vault. Whoever owns the account, owns any bitcoin within.

A bitcoin address is just a very long string of numbers and letters. For example, one of my addresses is "164qx6RhYgXUF2zXjfFWBAvzWMrdT9q8eR." Anybody can check this address on the ledger, and they can see all the transactions to and from the account.

But how can I prove that I am the real owner of that address, and how can I prevent other people from spending my bitcoin or claiming they own the account? The answer: mathematics. Every bitcoin address comes paired with *another* extremely long string of numbers, but this number is not public. It's private, and it's the "key" to the vault.

Bitcoin addresses are created with *only one corresponding private key*. Think of it like a signature. When you write a check to somebody, you have to sign with your particular signature. Somebody else can't sign with their name and draw funds from your account. Your signature is a way to "prove" to the bank that you're the true owner of that account and can authorize funds to be transferred out of it.

In the same way, if you have the private key for a bitcoin address, it's proof that you are the true owner of that account. You mathematically "prove" your ownership to the network. Every bitcoin transaction from every account requires a digital signature – that extremely long string of numbers – in order to take place. But unlike a brick-and-mortar bank, humans don't need to be involved. The proof of ownership is entirely automatic and digital.

So this means that "owning bitcoin" really means *owning the keys* to bitcoin stored in the ledger. But don't worry – the end user does not need to remember these long strings of numbers. The software does it for you. It all happens behind the scenes. Bitcoin

users just click a few buttons or swipe their fingers, and the software does the rest.

This makes the concept of a bitcoin transaction straightforward. Let's say I own the keys to .01 bitcoin at a particular bitcoin address. I want to send all of it to my friend in Japan. So, he shares his bitcoin address with me. All I do is tell the blockchain, "I am the true owner of .01 bitcoin at this address. Draw down my account by .01 bitcoin and send it to this other address." The software then checks my signature to verify I am the rightful owner, confirms there's enough bitcoin in my account to send, and immediately sends the bitcoin from my address to his. Of course, to the end user, that just means scanning a QR code or pasting in a bitcoin address and hitting "send."

Once the transaction is confirmed, every single ledger on the entire network is updated to show the change in ownership. This prevents me from ever trying to re-spend funds which I do not have. If I tried to spend another .01 bitcoin from the same address, every single computer would show in their records that I did not own any more bitcoin, and the transaction would be rejected. This prevents what is called "double-spending," which is a problem that used to plague earlier digital currencies. Bitcoin solved the double-spending problem.

Push Versus Pull

Because of the way this payment process works, Bitcoin is considered a "push system", rather than a "pull system." Meaning, spending bitcoin requires funds to be intentionally "pushed" out of the address, as opposed to a credit card or checking system where

merchants can "pull" money out of your account once you give them your information – like ACH with checking accounts or auto-payments with a credit card. Remember, every single waiter who has swiped your credit card has all the necessary information to pull money out of your account with or without your approval.

When you spend bitcoin, you don't have to worry about anyone stealing your information. You can send and receive digital cash without needing to trust that somebody won't loot you in the future.

The system also eliminates "chargebacks" – when merchants are forced to cover the costs of inaccurate credit card transactions. Say a merchant sells $50 worth of goods online through a credit card transaction. They ship the product out, but three months later, they are contacted by the credit card company. The customer says they never received the product, or they claim that the $50 transaction was the result of identity theft. The merchant is now required to return the funds, eating the entire cost of any shipped goods.

With bitcoin, there are no chargebacks. When you receive bitcoin, it's an irreversible transaction. Merchants receive digital cash that was "pushed" to them from their customer. This reduces overhead costs for companies and will reduce prices for consumers.

Security

One might wonder: if owning bitcoin means owning a bunch of numbers, and you can easily copy those numbers, doesn't that mean you can create more bitcoin? The answer is no. You can copy the digital keys necessary to move the bitcoin, but not the bitcoin itself. Just like making copies of your car key doesn't create a new car,

duplicating your digital keys doesn't make new bitcoin. It does, however, increase the risk of somebody else getting your keys – no different than making a bunch of copies of your car key.

Storing bitcoin safely is thus about storing your private keys safely. Right now, it's not the simplest process. Securing any digital data is hard, though companies are starting to offer ways to secure bitcoin more easily. You can store bitcoin keys anywhere you can store a string of numbers – your hard drive, smartphone, flash drive, smart watch, camera memory card, or even written down on paper.

If someone does get access to your private keys, they can prove their ownership to the Bitcoin network and authorize transactions on your behalf. It's like losing your debit card and PIN at the same time. Except with bitcoin, there's no bank you can call to try to get your money back – once bitcoin is moved out of an address, there's no way to get it back.

New Perks

Since bitcoin is stored in the digital cloud, anybody on the planet can become his own bank. Usually, we use banking services to provide us with security and easy access to our money. But the way Bitcoin was created, anybody can create their own account and be the *sole owner* of the digital keys necessary to spend their funds. And they can spend those funds from anywhere in the world to anywhere in the world.

Also, there's no mechanism to "freeze" accounts on the blockchain. Anybody can create as many bitcoin addresses as they like, and they need not reveal their identity to do so. Each individual is em-

powered to spend, receive, and store his own money, without authorization or permission from anybody.

If these claims sound dubious given that we're talking about computer software, I would recommend diving into the "cryptography" behind Bitcoin – the applied mathematics. This book is meant to be introductory, so we'll simply say that mathematics makes it impossible for unauthorized people to spend your bitcoin. This is also the reason bitcoin is called a "crypto-currency"; it's a currency based on cryptography.

To summarize:

- Bitcoin is modeled after gold; it's scarce, and the supply cannot be arbitrarily inflated.
- Bitcoin is stored in the online ledger; ownership means owning the private key to a corresponding address.
- The keys cannot be forged; they give robust digital security to the funds, and they allow the owner to easily spend from his account.
- Bitcoin must be "pushed" from each address, and they cannot be double-spent.
- Bitcoin transactions are instant and go directly to the recipient.
- Once a transaction is verified, the ledger is immediately and permanently updated.
- The entire system is designed to be trustless; it doesn't require a central company, bank, or government to make it work.

The Software

The final component to understand is the Bitcoin software. The software is what brought the blockchain into existence; it maintains and updates the ledger, secures the network from attacks, and with a little effort, creates new bitcoin.

Bitcoin software comes in different flavors. Some versions are "wallets," meaning they are only a place to store keys to bitcoin addresses and send/receive payments. Other versions store the entire blockchain on your hard drive, while others spend huge amounts of computer power securing the network and bringing new bitcoin into existence.

Your average bitcoin user only deals with wallets. You can download bitcoin wallets onto your phone, straight into your web browser, or as a stand-alone program on your computer. Wallets don't do anything to secure the bitcoin network, but they allow anybody to store, send, and receive bitcoin payments. You can even use bitcoin without running any software – companies exist which host wallets on the web for free. You can login with a regular user name and password to access your wallet online. These services are convenient but less secure.

Much of the heavy lifting on the network is done by software called "Bitcoin Core." Thousands of computers all over the globe run Bitcoin Core, and it forms the backbone of the entire network. Bitcoin Core is the software that updates the blockchain in sync and protects against double-spending. It also requires every computer to download the public ledger in full.

Anybody can download and run Bitcoin Core on their computer. This can be a bit of a hassle, however, since the blockchain is becoming quite large and is constantly growing.

You can think of Bitcoin Core as a new way for computers to talk with each other. It's a computer "protocol" – similar to how the internet is a computer protocol. Email, too, is a computer protocol, and it's almost universal. Bitcoin is the first computer protocol specifically designed for money, and it might become the standard protocol for that purpose.

Bitcoin Core is also *open-source* software, which means the code can be freely inspected by the public. Nothing about it is proprietary; nobody owns it. You and I are free to verify the soundness of the software at any time, and if you are a computer programmer, you are free to contribute to the project and improve it. Creating everything open-source was meant to further reduce the amount of trust needed to use the system.

Mining

The final piece of the puzzle is what's called "bitcoin mining." The process of mathematically verifying that new transactions are legitimate takes a large amount of computer power and energy. So, when computers undertake this process, they are rewarded with a small amount of new bitcoin. These computers and their operators are called "miners."

Miners can also make money by receiving small payments for verifying new transactions. Most bitcoin wallets have optional fees which they add to smaller transactions. The default fee is currently

something like 0.0001 bitcoin. So the more transactions the miner verifies, the more fees they can collect. Right now, those fees don't add up to very much, so the main incentive to "mine" is the software's reward of freshly-minted bitcoin.

The pace at which new bitcoins are created is regulated by the software itself. Based on how much computer power is dedicated to mining on the network, the software adjusts the difficulty of getting new bitcoin. In other words, as computer power flows into the system, the difficulty increases for getting rewarded with new bitcoin. If people stop mining, the difficulty automatically decreases. This regulates, to a very precise degree, the rate at which new bitcoins are created. Currently, twenty-five bitcoins are created every ten minutes.

In the early days, you could easily mine thousands of bitcoin on your home computer because nobody had heard of the technology, and it wasn't valued. Today, it's virtually impossible to receive any bitcoin from mining on your home computer – the power already dedicated to the network is too large.

Bitcoin mining is big business. As the price of bitcoin has increased, the incentive to mine has also increased. As a result, a huge market has developed for creating new hardware and software dedicated to mining with maximum efficiency. The margins for mining are currently razor thin because of its popularity. Miners' competition with each other helps secure the entire bitcoin network.

The software is programmed to gradually reduce the size of the mining reward until it is completely eliminated in the year 2140. At that time, the total number of bitcoins will never exceed 21,000,000, each of which can be divided down to 100,000,000th of a bitcoin.

Development

As impressive as this software sounds, Bitcoin is not a finished product. In fact, Bitcoin Core is still technically a "Beta" version. The software is being refined, and new features are periodically being added.

So, how does the software get updated? By the entire Bitcoin community. Remember, Bitcoin is open-source, so everyone is free to contribute. The thousands of miners are not obligated to run any particular version of the software, which means there's no central organization forcing changes on anyone. This means development is slow, cautious, and with the support of the majority of the Bitcoin community. In a sense, it's up to the entire network to decide how and when it will be updated.

Every computer on the network is free to leave at any time. They can branch off and create their own unique network if they like. For example, if a miner does not agree with one of the updates, he can run his own version of the software and is free to persuade people to join him. This creates a strong incentive to make updates which are beneficial to the entire Bitcoin network, not just a select group of people.

That being said, there is still a core group of developers working on Bitcoin. The creator of Bitcoin, whom I will write about shortly, is no longer working on the project, but those with whom he was closely working still are. So, they have an elevated status in the Bitcoin development community. Ultimately, it's still up to every individual participant to decide if they want to incorporate new ideas, whether they are proposed by the core developers or anybody else.

Even if the core developers turned malicious and greedy and decided to change the code to specifically benefit them, their changes would have *no* control over the version of the software that the rest of the network runs. In this way, the Bitcoin community has many checks and balances to ensure Bitcoin remains beneficial for all users.

The Creator

Naturally, we'd like to know about the creator of this invention. It turns out, when he released his work to the world in 2009, he chose to remain anonymous. We don't know his real identity. He communicated with people online through the pseudonym "Satoshi Nakamoto." Many have speculated about his true identity, but nobody knows for sure.

Newsweek magazine famously ran an article in March 2014 claiming they had uncovered the identity of Satoshi. His name, the journalist claimed, was actually "Dorian Satoshi Nakamoto" – not a clever disguise after all. Newsweek turned out to be terribly wrong, and Dorian Nakamoto is not the real creator of Bitcoin. The magazine is still wiping egg off their face.

With such an elusive creator, shouldn't we be worried about the security of the software? Might Satoshi have planted a secret backdoor or weakness that nobody knows about? Not likely, because every part of Bitcoin is open-source and can be freely scrutinized. Many developers and programmers have searched the code, and nobody has ever found a backdoor.

Given the openness of the code, we don't actually need to know who the creator was at this point. It would be interesting, for sure, to

be able to hear his thoughts about the current state of the software, or to know more about him, but it's ultimately irrelevant; the software is far more important than the person. It remains to be seen if he can keep his identity secret forever. (I'd advise him not to use his credit card at Home Depot.)

PART TWO
So What's the Big Deal?

Programmable Money

The basic facts about Bitcoin have caused plenty of buzz, but it's the future possibilities which cause the most excitement. I'd like to go through a number of different examples to show how Bitcoin might be used in the future.

Put yourself back in the 1990s. Everybody used landline phones to communicate with each other, and landline phones were good for one thing: making calls. But today, we expect our phones to do a lot more. We walk around with smartphones in our pockets and take for granted that they take pictures, navigate roads, surf the internet, play games, read books, and become flashlights. In a short period of time, the smartphone has become the Swiss Army knife of technology.

The software running on our cell phones makes these innovations possible. Hundreds of thousands of different apps can all be created and run *within the same programming environment*. This freedom is what allows your phone to be used for various purposes –

the same device can stream music, access your bank account, and record a video all at the same time.

Bitcoin, too, is a programming environment, allowing for different "apps" to be created in a similar way. It is essentially *programmable money*. We wouldn't expect phones to only make phone calls anymore, and we shouldn't expect currency to only be used as a medium of exchange.

Microfinance, Remittances, and the Unbanked

Before covering purely technological possibilities, we need to realize that Bitcoin could bring financial tools to the underdeveloped world in a big way. Currently, more than 2.5 billion people do not have access to basic financial services – not even a bank account. Bitcoin can be used by every single person with an internet connection. Everyone from rural sub-Saharan farmers to techies on Wall-Street can be his own bitcoin bank, able to secure, transmit, and receive payments from anywhere in the world. Even if a small fraction of the world's unbanked ever use bitcoin, that would be tens of millions of people given control of basic financial tools for the first time.

This opens up new doors in terms of lending and microfinance. Getting capital to underdeveloped countries is notoriously difficult, and it requires going through lots of middlemen who charge big fees. Little infrastructure exists to connect lenders with rural farmers, businessmen, or regular citizens needing a loan. Bitcoin requires minimal infrastructure.

Anybody on the planet can lend, borrow, or give *directly* to anyone else, from the Congo to Shanghai without fees, delays, or authorization from any company. A farmer doesn't need to set up a bank account, provide anyone with information, or have a credit score or proof of income to participate in financial markets. Workers in Kenya can now receive money from an entrepreneur in New York City as easily as they can send money to their neighbors. They have access to the exact same public ledger.

This could also dramatically change the remittance market. "Remittances" are payments that workers in one country send home to their families in another country. The global remittance market is estimated around $550 billion annually, and the system is complicated. Companies take huge cuts – often more than 10% – out of the amount being sent. Bitcoin allows for seamless remittances, instantly, for almost no cost, and without any interference from middle men. Companies like Western Union would have virtually no comparative advantage to offer workers sending remittances *directly* back to their families in bitcoin. This benefits the workers, the families, and also their local economies. As cliché as it sounds, Bitcoin could help bring communities and countries out of poverty.

If it seems absurd to imagine rural farmers using bitcoin, consider two things: bitcoin can be sent and received using basic text messaging services, and underdeveloped countries have extremely high ownership rates of cell phones which are already being used to send money to each other. A company called "M-Pesa" currently provides money transmission services in Kenya, India, Tanzania, Afghanistan, South Africa, Egypt, Mozambique, and a number of smaller countries. Users can send and receive money using only their

cell phones. The service is immensely popular and growing. However, it still requires a middleman – M-Pesa – who needs to make money. Transaction fees can range anywhere from less than 1% to more than 60%. There's no reason why Bitcoin could not be used instead, with less friction, cost, and trust required, and with much greater access to a global market.

International trade also democratizes the world a bit more. Strong borders have created very sharp differences in countries' financial systems, and as a result, workers in different countries are artificially separated from each other; they aren't permitted to benefit from trade. But, if you can easily communicate and exchange *across* borders, those borders become less steep and less relevant.

Colored Coins and the Global Asset Register

The smallest unit on the public ledger is 0.00000001 bitcoin; that's one-hundred-millionth of a bitcoin. This unit has been named one "satoshi," after the technology's creator. But one satoshi does not need to equal one satoshi, nor does it need to reside only in the blockchain. Here's what I mean: units on the ledger can be assigned to real-world goods. Meaning, ownership of a real-world good can be transmitted and tracked on the public ledger as securely as a bitcoin.

For example, say you want to establish ownership of a car. Instead of going to lawyers and sorting through paper records, you could assign a specific fraction of a bitcoin *to* the car. Whoever owns that bitcoin would be the legitimate owner of the car. No forgery, no clunky paperwork, no confusion. Ownership becomes quite simple: if you own the keys to a specific satoshi on the blockchain, you own that

corresponding good. Recording ownership on the public ledger means you can change ownership of any good instantly, internationally, and without involving a bunch of lawyers.

The idea of assigning real-world goods to bitcoin is called "colored coins." It's as if those particular fractions of bitcoin that correspond to physical goods have "color" – they represent more than just bitcoin on the blockchain. Colored coins blend digital and physical ownership together. Imagine all the important goods that need titles: houses, cars, boats, stocks, bonds, etc. Ownership of a boat on the blockchain would be indisputable and unforgeable to the entire world. Anybody with access to the blockchain would immediately have access to stock markets and other financial markets. The buyer of a house could *instantly* send $150,000 to the seller and receive his title *instantly*. The transaction could even happen on their cell phones, if they desired.

Using bitcoin and the blockchain this way creates what's called a "global asset register," where anybody can immediately verify the ownership of any good tied to the blockchain, whether it's a house, a gold bar, a mortgage, or even smaller goods like a lawn mower. Think your neighbor stole your lawn mower? You can imagine a world where disputes over ownership can be easily resolved by referring to the global blockchain.

In addition, whenever bitcoin is transferred, the transaction is time-stamped. This means the blockchain can be used for signing important contracts or proving that a particular exchange happened at a particular time. Whenever the "colored" coin was exchanged, at that exact moment, the ownership changed, the contract was signed, or the deal was made. No forgery is possible.

Smart Property, Smart Money

Owning something on the blockchain might be more secure than our current system, but the idea is still abstract. "Smart property" makes ownership concrete.

Imagine you purchase a car with bitcoin. Your title is provable on the blockchain. Now, imagine the *physical keys* that you use to drive the car are also programmed: they will only work for whomever owns the correct colored coin. In other words, the car will only start for the true, mathematically provable owner(s). This would make auto theft immensely more difficult. Thieves would have to access your coins on the blockchain in order to steal your car.

Imagine being able to send digital car keys to somebody. You, and only you, could create self-expiring keys to your car, from the other side of the planet, and send them directly to whomever you choose. And you could do it from your cell phone. A valet might only have access to your car until you choose to digitally revoke permission. Your kid might be able to drive until a certain time of night, or within a specified geographic region. The possibilities are endless.

Computers might start for only one true owner. Doors might only open with digital permission. Who knows – perhaps some property could self-destruct if used by people without corresponding ownership on the blockchain.

This is why it's called "smart property." We could, in essence, *program physical goods* to behave in certain ways for those with the correct digital key. Those keys would be traded and secured on the blockchain, further shrinking the gap between digital and physical.

A company might set up a digital wallet for employees and specify: only $300 can be spent on particular office supplies. The money literally couldn't be spent for anything else. Or, instead of handing an employee the company credit card for his business trip, you could give him a digital wallet which could only work within a specified time-frame, for a specified amount, or at specified locations. After that time ends, any remaining balance could be automatically returned to the company's funds.

A father might set up a college fund for his daughter and specify that the funds will only be usable after she turns eighteen. This kind of specification could literally be programmed into the money itself.

Even the mundane grocery run could be improved with this technology. Bitcoin allows for long-distance payments, enabling users to simply wave their smartphones in front of a scanner to pay. They're called "NFC payments". So, imagine walking into a grocery store, pulling anything you need off the shelf and loading it into your cart, which automatically reads the items you've selected. You then walk straight out of the store to your car, passing by an NFC scanner on the way out. No need to take out your wallet, hand over your personal information to anybody, worry about your identity being stolen, or even interact with anybody.

Programmable money even seeps into the legal profession. Usually, we don't think of lawyers' jobs as being easily automated. But consider a simple example involving a death certificate and the execution of a will. Imagine a program which searched the web for news articles and obituaries, cataloging who died and when. Once enough evidence was gathered, a death certificate could be automatically issued, and the estate could automatically be dispersed to the

appropriate recipients, publicly verifiable on the blockchain. Lawyers might not need to be involved at all; legal documents, payments, and contracts could all be automatically created and executed, without trusting any third party in the process. It's a wild idea, distant in the future, but it's possible with the technology.

Try programming a regular dollar bill to automatically transmit itself into the appropriate bank account upon somebody's death. You'll quickly see why techies are excited about the idea of programmable money.

Multisignature

As explained in Part One, every bitcoin address has two corresponding strings of numbers: one public address and one private key. But this is only the default setting. If desired, the software allows multiple private keys per address. This is called a "multi-signature wallet" or "multisig" for short. A multisig wallet requires multiple digital signatures in order to spend any funds – like a check which must be signed by multiple people in order to be valid.

The software can create a bunch of different combinations. For example, it can create a wallet which requires 2-of-3 digital signatures in order to send payments. Meaning, the wallet creates three corresponding private keys, and it would absolutely need at least two of those keys in order to recognize a transaction as valid. Or, it could create a 4-of-5 wallet, 1-of-6, 7-of-7, 10-of-15 or any other combination.

Multisig wallets can be used for company funds, family budgets, or even for basic bitcoin security. A husband and wife, for example,

could set up a 2-of-2 wallet for their vacation together. They could specify: for any big expenditures, the software would need both of their signatures, requiring them to agree unanimously. Or, say they simply want to secure their funds. They could create a 2-of-3 wallet. The husband could hold one key, the wife another, and a trusted friend could hold the third in case anything happened to them. The trusted friend couldn't steal their money (he only has one of the two required keys), and if either of them lost a key, they would still be able to access their funds.

This is how some online bitcoin wallets secure their clients' money. They create 2-of-3 wallets, give two keys to their client, and only keep one themselves. That way, even if the company gets hacked, users still retain control over their funds.

Bitcoin escrow and arbitration services work the same way. Say you're a contractor who's being paid in bitcoin. A 2-of-3 wallet is created by your employer. You have one key, your employer holds one key, and an escrow/arbitration service holds the third. Your employer would deposit money into the wallet, which couldn't be withdrawn without a second party's agreement. If the work goes smoothly, the employer and contractor authorize the transaction, and the money is immediately sent. If, however, a dispute arises – either the work wasn't finished properly or the employer refuses to pay – either party can contact the escrow service, which holds a third key. The arbitrator could review the dispute and decide whether to authorize a transaction paying the contractor or returning the employer's funds.

The security of a multisig wallet is very flexible. If you want to be extremely secure with your digital money, you could create a 5-of-5 wallet, keeping one key on your computer, one on your smartphone,

another on a flash drive deposited in a safety deposit box at a bank, one on a camera memory card, and one with the numbers physically written down on a piece of paper. Then, in order to spend your money, somebody would require access to every single one of those keys – an absurd scenario unless you're the rightful owner. It would be quite tedious to ever spend money from the wallet, but the security would be extraordinary.

Of course, such security wouldn't be required for everyday use, but that's the flexible nature of programmable money; you can use whatever level of security you need. For this reason, multisig wallets are already being used in the Bitcoin ecosphere.

Sound Money

As neat as the technology is, it was the economics behind bitcoin which originally caught my eye. Currencies are important to any modern economy, and successful currencies tend to share similar properties. To understand the benefits of bitcoin-the-currency, we need to dive a little bit into basic economics.

First, a definition: currency is simply a tool used for "indirect" exchange. Meaning, the currency is used as a middleman to get what we want. Instead of directly bartering with my local farmer – trading my shoes for his eggs – I can trade my shoes for US dollars, then trade my dollars for his eggs. In that example, we would say the US dollar was used as a "medium of exchange." So when people buy computer parts online with bitcoin, they've used bitcoin as a medium of exchange.

The most successful currencies usually share the same five properties: they are scarce, divisible, portable, durable, and remain valued over time. I'll briefly explain each of these properties and how bitcoin relates to them.

The first property has already been mentioned, but it's arguably the most important: successful currencies must be *scarce*. Meaning, there can't be an unlimited supply of currency units. Think of Monopoly money – why isn't it used as currency outside of the board game? Simple: anybody with a scanner can print up as many copies of the currency as they like. I might be a Monopoly billionaire, but that doesn't mean much if everybody else is also a billionaire. A billion units of a worthless currency won't buy you a pack of gum.

Bitcoin, like gold, is fundamentally scarce. No more than twenty-one million bitcoins will ever exist. That limit is written straight into the software. This scarcity is mathematical, not physical; it's ultimately based on software and computer programming.

It's one thing to say, "The supply of bitcoin cannot be arbitrarily inflated." It's another to understand how historically significant this is. Currency after currency has been destroyed because of inflation. When a central authority gets out of control and prints too much money, whoever holds on to cash gets decimated. On average, currencies that aren't backed by hard assets don't last more than a few decades, because their central issuers can't help but print money. This is true from the days of the Roman Empire through modern day Argentina and Zimbabwe.

The United States has been experimenting with so-called "fiat" money since the 1970's (money which is not backed by any hard asset). Since then, the price of gold – a traditional measure of infla-

tion – has gone from $32 an ounce to currently over $1,200 an ounce, with ominous signs on the horizon. Countries in Latin America have experienced round after round of double-digit inflation, and Zimbabwe notoriously had inflation so severe they were printing $100,000,000,000,000 notes! Being inflation-proof has very large benefits, especially for smaller, developing countries with unstable money supplies.

The second property of successful currencies is *divisibility*. You have to be able to easily divide a currency into smaller units. Take a scarce resource, for example: cows. It would be very difficult to make precise exchanges using cows as a medium of exchange. What might a loaf of bread cost: a hundredth of a cow? And which hundredth, the ears or the tail? As you can imagine, trying to meaningfully divide a cow up into currency units would not only be gross, but impractical.

Bitcoin is eminently divisible, down to 100,000,000th of a bitcoin – that's 0.00000001 bitcoin. This means that once all the bitcoins are mined, 2.1 quadrillion (2,100,000,000,000,000) individual units will exist. If somehow that weren't enough – if the value of each unit was too high to make tiny transactions – then a simple change to the code could allow bitcoins to be divided into even smaller fragments.

The next property of successful currencies is *portability*. You need to be able to easily transport a currency around. Imagine using something clunky like cinder blocks as a currency. How would you pay for your groceries? By rolling a wheelbarrow full of cinder blocks through the aisles?

Bitcoin is extremely portable, given its digital nature. In fact, bitcoin might be the most portable currency ever. You can carry an

unlimited amount with you on your phone, on a laptop, on a flash drive, or even on the web. Remember, owning a bitcoin doesn't come with any physical possession; it's owning the digital keys required to move the bitcoin on the public ledger. So, you can store bitcoin keys anywhere you can store numbers – even on physical paper, if you choose.

Plus, not only can you store bitcoin without physical encumbrance, you can also send them anywhere on the planet instantly. Transacting with somebody on the other side of the globe takes a few clicks or swipes of a finger. No other currency in history has ever been so portable.

The next property of popular currencies is *durability*. You can't have your storage of currency significantly degrade over time. Imagine using something like bananas as currency. They are scarce, useful, somewhat portable, but they have a lifespan. Bananas turn to mush after a few weeks, and nobody wants to trade rotting fruit with each other.

Bitcoin, being mathematical, is entirely durable. Remember, owning a bitcoin means you own the digital keys tied to that bitcoin, and numbers do not degrade over time. Hardware, however, might. Still, with simple precautions, it's safe to say bitcoins will never lose their durability, and they certainly won't rot.

This particular combination of scarcity, portability, and durability has never been seen in the history of money. There's usually a trade-off between the security of money and its convenience. Carrying around paper bills, for example, is more convenient than carrying around gold nuggets. But, paper bills can be printed off a press; gold nuggets cannot. Bitcoin happens to combine both these properties

and even improve on them. Paper is clunky when compared to bitcoin – you can't instantly send paper directly to another person on the other side of the planet.

The final property of successful currencies is that they remain valued over time. Goods can lose their value for many different reasons. They can degrade, become less useful, or be discovered to have an undesirable property. Take lead paint for example. It used to be a highly valuable good, until people discovered that it was dangerous. Then, its value plummeted.

Whether or not bitcoin will remain valuable over time is an open question; it was created only a few years ago. It took around a year before one bitcoin had any market value whatsoever. Many years will need to pass before we can confidently answer whether or not people continue to value it. But, within the limited time that bitcoin *has* existed, its value measured in terms of price has been growing. The price has gone from essentially zero, to less than a penny, to a few dimes, through the $1 mark, past $10, $100, $200, $500, and all the way up to over $1,200 per bitcoin! As I write, the price for one bitcoin is around $300. Thus, it has a very strong track record so far.

A common objection to bitcoin is that the price is *too volatile*. I will address this in Part Three, along with the popular misconception that a currency must have "intrinsic" value.

Bitcoin scores highly on the traditional properties for a sound currency, but it also adds a few new ones. It's digital; the issuance is decentralized, and it's programmable. Never before have such properties existed in a currency. Because it resides on the internet, and is even accessible through text messaging, bitcoin destroys any barriers to entry for owning a sound currency; anybody with a phone

on the entire planet can own bitcoin and trade internationally, and there's no clear way to stop them. That's potentially life-changing value created for billions of people.

Meta-Currency, Sidechains, and Mesh Networks

The current international financial system is very clunky. Dealing with multiple currencies is a bookkeeping nightmare. Bitcoin could become a universal medium of exchange for dealing with multiple currencies at once – a kind of currency-of-currencies. Instead of trying to convert US dollars to ten different currencies to send internationally, you simply send bitcoin and allow the recipient to settle in the currency of their choice. In that way, bitcoin could become a kind of standard for international trade that wouldn't rely on the politics and good governance of any particular nation.

In fact, given all the benefits, it's not unreasonable to imagine a time when bitcoin becomes the *preferred* medium of exchange in contrast to centralized currencies. With such a stable money supply, we might even end up denominating traditional currencies in terms of bitcoin. Many countries have used a "gold standard," formally declaring a fixed exchange rate between their currency and the precious metal. This was used to protect their currencies from arbitrary inflation. Well, if bitcoin is digital gold, might some countries want to denominate their currency with a "bitcoin-standard" for the same purpose? It sounds wild, but it's certainly possible.

Bitcoin might also end up being the reserve currency for future technological innovations built on top of the blockchain. Right now,

programmers across the globe are building new services and platforms to be used with the blockchain that could be integrated with Bitcoin as so-called "sidechains." This means they would offer additional services not allowed by the basic Bitcoin software, but could still seamlessly transfer in and out of the same blockchain.

Take micropayments as a concrete example. Bitcoin is not well-suited for transactions involving only a few cents at a time. It can be done, but it's inefficient for technical reasons. The blockchain, however, is perfectly suited for micro-transactions. So, a programmer might create software – call it BitcoinMicro – that easily processes transactions dealing with pennies or even fractions of pennies. Those tiny transactions could be recorded "on the side" of the main blockchain, on a separate protocol, and then added back in to the blockchain after the fact, without tampering with or disrupting the main Bitcoin system.

Sidechains would allow programmers to continue to innovate in ways which Bitcoin does not allow, while still accessing the same blockchain. The possibilities are extremely advanced, and beyond the speculation of this book. Sidechains are not currently implemented, but the Bitcoin community is working on them and debating their pros and cons as I write.

Another futuristic invention incorporating bitcoin is called "mesh networks." A mesh network is created when one person shares his internet connection with other people through WiFi. The recipients then re-share that connection with more people, creating a web of peer-to-peer internet access. Bitcoin can be integrated to allow seamless behind-the-scenes payments for this service.

For example, if you don't have internet access, you could pull up an app on your phone, see which networks were available, and pay a small fraction of bitcoin to whomever shared their internet with you. The payment might be per-minute or per-kilobyte, and it would be as easy as swiping a finger. Similarly, if you have access to the internet, you could make money by simply swiping your finger and sharing your connection with people. Everyone with a cell phone could become a paid WiFi router for complete strangers if they wanted. This technology, too, is being developed as I write.

Decentralized Markets, Blockchain Voting

The concept of decentralization can be applied to more areas than just money. One complementary technology being built alongside Bitcoin is called "OpenBazaar," and it applies decentralization to an online marketplace. The idea is to create a peer-to-peer marketplace to use alongside our peer-to-peer currency, connecting buyer and seller directly, without middle men, fees, or overseers controlling who trades with whom. A farmer in China could set up an online store with OpenBazaar and be connected *directly* with his customers all over the world, and because the technology would be decentralized – without a central point of failure – overreaching governments could do little to shut his store down. This could be particularly powerful in countries with strict, stifling economic regulations that prevent people from freely trading with each other.

The blockchain might even be applied to the functioning of government. One idea is to bring *voting* onto the blockchain, to benefit from the openness, security, and transparency of decentralized

record-keeping. Imagine votes were cast by moving specific tokens along the public ledger. Each voter would have his own secure digital signature that would be used to cast a vote, and he could personally verify it was tallied correctly. Voter fraud could be seriously diminished. If implemented correctly, the level of transparency would be exponentially greater than modern voting systems.

The Rate of Adoption

An entire industry has sprung up around Bitcoin. Companies are trying to radically disrupt financial markets with bitcoin; merchants are accepting bitcoin for their products, and venture capitalists are pouring hundreds of millions of dollars into new Bitcoin startup companies.

The current development around Bitcoin is often compared to the early days of the internet. Back in the 90s only a handful of geeks knew about the internet and could use it. The internet was slow, incredibly clunky, and nearly impossible to navigate before search engines were created. Nowadays, the internet is easy to use and ubiquitous. Because the Bitcoin ecosphere is still in the early days of development, it's not yet easy to use for beginners. Though, this has started to change over the last two years.

A now-legendary article was written for Newsweek in 1995 entitled "Why the Web Won't Be Nirvana." The author laments the chaos of the internet and is entirely unconvinced that business will ever happen online. He wrote:

> "Every voice can be heard cheaply and instantly. The result? Every voice is heard. The cacophony more closely resembles citizens band radio, complete with handles, harassment, and anonymous threats... How about electronic publishing? Try reading a book on disc. At best, it's an unpleasant chore: the myopic glow of a clunky computer replaces the friendly pages of a book. And you can't tote that laptop to the beach. Yet Nicholas Negroponte, director of the MIT Media Lab, predicts that we'll soon buy books and newspapers straight over the Internet. Uh, sure..."[1]

Twenty years later, we laugh at his shortsightedness. Yet, in the midst of these criticisms, many entrepreneurs saw the potential of the internet. Only a few decades later, the internet has become essential to the global economy and universal in developed countries. Young people especially spend enormous amounts of time online working, connecting with each other, shopping, and for recreation.

Further comparing the early internet to Bitcoin, venture capital is being invested in Bitcoin startups at a similar pace to internet startups in the early 90's. As of March 2015, over $550 million has been invested in Bitcoin startups, more than 80% of which was invested since the start of 2014 alone.[2] The industry is now worth several billion dollars between the companies, capital investment, and speculation surrounding Bitcoin.

Naturally, tech companies have been the first to accept bitcoin for payment. Companies like Microsoft, Dell, Newegg, Tiger Direct, and Zynga all accept bitcoin in some way. But acceptance is not

[1] Stoll, Clifford. "Why the Web Won't Be Nirvana." Newsweek, 26 Feb. 1995. Accessed 8 Dec. 2014. <http://www.newsweek.com/ clifford-stoll-why-web-wont-be-nirvana-185306>

[2] "Bitcoin Venture Capital Funding." CoinDesk. Accessed 5 March 2014. <http://www.coindesk.com/bitcoin-venture-capital/>

limited to the tech world. Dish Network, Expedia, Virgin Galactic, and even the Sacramento Kings accept bitcoin for their services. Non-profits like the American Red Cross, Greenpeace, United Way, and Wikileaks accept bitcoin for donations. The payment processor giant PayPal allows some of its merchants to sell digital products for bitcoin.

Some US political candidates have also begun accepting bitcoin donations for their campaigns, like Jeff Kurzon from New York City.

At this point, most merchants use payment processors to handle their bitcoin transactions and immediately convert bitcoin to their local currency. BitPay is the largest bitcoin payment processor; in 2013, they processed more than $100 million in transactions, and in 2014, they crossed $1 million *per day* in bitcoin transactions.

Microsoft CEO Bill Gates recently called Bitcoin a "technological tour-de-force," and Virgin CEO Richard Branson has been one of the leading venture capitalists investing in Bitcoin startups. Overstock.com CEO Patrick Byrne is such a Bitcoin enthusiast that he gives public speeches on the topic. His company doesn't immediately convert all the bitcoin from their sales to cash; they hold on to a portion in bitcoin.

The comparison between Bitcoin and the internet has one more important parallel. Right now, around three billion people use the internet – almost half the world's population. But only a tiny fraction of them understand how it works. I, for one, have no idea how the computer protocol TCP/IP works, but that's the protocol which everybody uses to access the internet. Not only do most people not understand TCP/IP, *they don't care to understand*. The internet just works. The same can be said for Bitcoin. At some point, people will

neither understand nor care to understand the protocol. If it works, that's what matters.

Imagine you're writing somebody an email. Next to their email address, there's a little box where it says "enter amount to send." You have the option of zapping them money, if you want, just by typing in the amount. Assuming it works, do you really care *how*? Or perhaps more accurately: will the vast majority of people really care how this payment system works? I think the answer is no, and that's a good thing. Advanced technology is supposed to work quietly in the background, and Bitcoin can do just that.

One major reason there's so much hype around Bitcoin is because global markets are massive, even without including all the currently inaccessible markets. The potential for a radical new technology is huge. Simple online commerce is large and growing, and the traditional financial system is not well suited for the digital environment. Bitcoin, by contrast, is literally made for the internet. Now that Bitcoin is entering the mainstream a bit more, the excitement is no longer limited to a tiny group of tech geeks.

PART THREE
Common Objections, Real Challenges

Common Objections

Bitcoin has been criticized a hundred different ways. Some objections are good; some are not so good. This part is broken up into two sections. The first deals with the most popular objections – nearly all of which are misguided – and the second covers the real challenges facing Bitcoin. The technology isn't perfect, and we need to be careful discerning good objections from bad.

Intrinsic Value

Perhaps the most common objection is this: "Bitcoin has no intrinsic value!" You can't eat bitcoins. You can't wear them. They have no industrial use. Heck, you can't even see a bitcoin. So why would anybody value one in the first place?

This criticism rests on a fundamental misunderstanding of value and a limited understanding of bitcoin. Technically speaking, it's true

that bitcoin has no intrinsic value. But this is not a meaningful objection. *Nothing* has intrinsic value.

"Intrinsic value" is a contradiction in terms. It implies that certain goods contain value in themselves, separate from humans' evaluation of them.

Water is a popular example. Supposedly, water is intrinsically valuable all by itself because of its properties. But imagine a world without life. If water were *intrinsically* valuable – if value was an internal property of water – then even in a world without living creatures, it would remain valuable. But this idea is absurd. Without living things, who would be around to value water, and for what reason? It's just hydrogen and oxygen, after all.

The confusion resolves itself when you understand that value is subjective, by definition. Goods are valued by human minds; they don't "possess" value. Value is not an objective property of something; it's a human evaluation, and humans have wildly different preferences and reasons for valuing one thing over another.

To me, bright orange nail polish is ugly, stinky, and unhealthy. I don't value it at all. But other people do. Some people think bright orange nail polish is beautiful and smells nice. I think they're crazy, but that's beside the point. Nail polish is valued differently by different people.

So yes, it's true, bitcoin has no intrinsic value. Neither does anything else. Bitcoin, gold, silver, and every other currency are only valuable because of human minds, not by virtue of their internal composition.

To be fair, what most people probably mean when they say "Bitcoin has no intrinsic value" is something like "Bitcoin has no

tangible use-value." You can't do anything with it other than send to somebody else, and a currency must have at least one other use.

This objection fails both empirically and theoretically. Lots of different things have been used as currency throughout history, some more useful than others. In the Micronesian islands, for example, gigantic stones were used as money. Some stones weighed more than four tons and were over twelve feet in diameter. These stones changed ownership orally – the stones never needed to physically move. One stone even fell off a canoe and ended up in the ocean, but its ownership still circulated through the economy because everybody agreed the stone still existed, just somewhere underwater. Of what use-value is a two-ton stone at the bottom of the sea? None. But, such a currency worked by convention; they simply agreed to use it.

Paper currency does not get its value because you can use it as kindling. Gold is not used as currency because it can also make pretty jewelry. While it's true that most currencies have some kind of use-value, this is only a side-effect of traditional currencies being *physical*.

Bitcoin is not physical, so naturally it doesn't have physical use-value. It does, however, have lots of digital use-value, as explained in Part One and Two. It represents ownership on the biggest, most secure public ledger in the world. It can be used to track the legitimate ownership of any asset on the planet and transfer it instantly to anybody else. It is transparent bookkeeping on a global level, accessible to everybody. If people value these properties, and the supply of bitcoin is limited, then each unit must have some value.

Now, it's a completely different question to ask, "What should the price of one bitcoin be?" Nobody knows the answer. Markets are

currently trying to figure that out. Remember, the base unit of bitcoin is one satoshi, and as of March 2015, one US dollar can buy around 360,000 satoshis. Should it be more or less? I haven't a clue.

Ponzi Scheme

What about the popular criticism: "Bitcoin is nothing but a Ponzi scheme!" This objection can be easily refuted: no, Bitcoin is not a Ponzi scheme, by definition.

A Ponzi scheme is a financial instrument designed to pay out returns to investors based on the future influx of new investors. For example, say I tell you about an offshore investment which pays high returns. An initial $100 investment yields $10 dividends every quarter. Sounds great, right? So, you invest $100 and start receiving your dividends as promised. Where does the $10 keep coming from? The investors who enter the scheme after you. And where do their dividends come from? The investors who enter after them. And so on. Ponzi schemes like this can run for a long while, making early adopters enormous amounts of money, until finally the whole scheme falls apart. Whoever entered the market last gets stuck holding the bag.

Bitcoin has little in common with such a scenario. There's no Bitcoin company, no central control or dividends being paid out; there are no promises of returns being made. Quite simply: bitcoin is an appreciating asset. It's true that, if you got in early, you could have made a huge amount of money selling your bitcoin to somebody after you, but that's no different than buying Apple stock early and selling it to somebody else. Or buying a home and watching the price appre-

ciate because your local real estate market is growing. It's an asset which has, so far, appreciated in value because of increased demand. It's that simple. Criticizing early holders of bitcoin is no more sensible than criticizing owners of gold when it was under $100/oz. Bitcoin is in no way a Ponzi scheme.

Not a Real Currency

One fashionable criticism of bitcoin is to say it's not a *real* currency, or that it shouldn't be called money. But this simply stems from a lack of clear definitions. "Currency" and "money" are often used interchangeably in our common vocabulary, but if we want to be precise, they do indeed have different definitions.

Unequivocally, bitcoin is a real currency. But that's not saying much. Lots of things are used as currency and have been throughout history. Sea shells, wheat, salt, stones, paper, gold, cigarettes, sugar – all of these things have been used as currency. As explained in the section "Sound Money," a currency is simply a medium of exchange.

In different situations, different things are used as currency. In prison, cigarettes are a popular currency. In Washington D.C., Tide detergent is used as a black market currency. Online, bitcoin is used as currency. Factually speaking: bitcoin is traded for goods and services online, and goods and services online are traded for bitcoin. Therefore, it is a real currency.

Does bitcoin also qualify as "money"? The answer, equally clear at this point, is no. "Money" is just a word we use to reference the most popular currency in an economy. And, in almost every circum-

stance, bitcoin is not the most popular currency. This should be no surprise, given that bitcoin didn't exist a few years ago.

The only difference between "currency" and "money" is the degree of popularity. So, it's no criticism to point out that bitcoin is not money. This might change in the future if it becomes more popular and widely accepted, but it's not there yet.

Bitcoin is Not Backed by Anything!

Another common criticism is that bitcoin isn't "backed" by anything. Because it's not redeemable in any commodity, detractors say it's unsuitable as a currency. I am very sympathetic to this idea. Hard-money enthusiasts are right to point out that currencies not backed by anything often collapse within decades. The best solution, so far, has been to tie currency to something with a physically limited supply – gold and silver are prime examples.

But we need to take a step back and ask, "*Why* do unbacked currencies collapse?" The answer is universal: inflation. They don't collapse because they are unbacked; they collapse because they are easily inflated. This is a key distinction.

Granted, it's reasonable to assume that unbacked currencies can easily be inflated, especially given their history, but it's not a *necessary* connection. We can envision a currency not redeemable in any commodity and yet safe from inflation. As explained in Part One, that currency is bitcoin.

In fact, it's safe to assume that bitcoin is the first currency which solves the problem of inflation without relying on its physical scarcity. Bitcoin is inflation-proof thanks to mathematics and the absence of a

central issuer. So if we don't have to worry about inflation, whether or not bitcoin is "backed" by anything becomes irrelevant.

Volatility

Another common criticism is to say the price of bitcoin is too volatile for it to be used as a currency. Nobody wants their money to fluctuate up and down 10%+ every day. Sound currencies are supposed to have a relatively stable purchasing power, and bitcoin has gone through a series of enormous booms and busts.

There is a lot of truth to this objection. The price of bitcoin has unquestionably been volatile for the last four years. To give you an idea, here are some of the past swings in the market price for one bitcoin[3]:

July 2010:	$0.05
February 2011:	$1.00
June 2011:	$29.59
November 2011:	$2.05
August 2012:	$13.50
April 2013:	$230.00
July 2013:	$66.08
October 2013:	$116.82
November 2013:	$1147.08
April 2014:	$360.84
December 2014:	$381.01

[3] "Bitcoin Price Index" CoinDesk. Accessed 5 March 2015. <http://www.coindesk.com/price/>

January 2015:	$172.43
March 2015:	$284.14

If the price never stabilizes, it's safe to say that bitcoin will not be the most attractive option to use as a long-term currency. But if we understand why the price has fluctuated so wildly in the first place, it's not unreasonable to think that it will eventually stabilize.

The most important reason is this: even after all the hype, the bitcoin market is still small. Tiny, by comparison to other markets. The market capitalization of bitcoin (the number of bitcoins in circulation times the price) is currently just under $4 billion. To put that in perspective, global stock market capitalization is over $63 trillion. Bitcoin has less than 0.01% of the capitalization of global stock markets. That means small amounts of money – a few million entering or exiting the market – causes huge swings in the price.

Thus, it shouldn't be surprising that the price has behaved erratically, and it will likely continue to do so in the near future. The amount of money currently sitting in bitcoin could increase a hundredfold, and it would still be a fraction of larger markets.

While the price is still volatile, companies have developed ways to mitigate the risk of holding bitcoin. A company called Coinapult has created a system called "Locks," where customers can permanently lock in the purchasing power of their bitcoin. They tie the value of your bitcoin to another asset like USD or gold. So, a $1000 purchase of bitcoin would be worth $1000 next year, regardless of the nominal price of bitcoin. This prevents holders of bitcoin from either losing or gaining money due to volatility.

The company BitPay has completely eliminated volatility risk for businesses accepting bitcoin. They allow companies to accept bitcoin and *immediately* cash it in for the domestic currency of their choice. In other words, the merchant can enjoy all of the benefits of bitcoin, especially for international transactions, while not needing to hold bitcoin directly. BitPay provides this service for free, allowing payments to be accepted from anywhere in the world with 0% transaction fees.

Also, let's not forget: traditionally stable assets like gold and silver have also been volatile in recent years. In January of 2006, one ounce of gold was around $515. By September of 2011, it was up to $1,826. That's more than tripling in price. As of March 2015, one ounce of gold is around $1,200. Silver has been even more volatile. In January of 2006, an ounce of silver was worth around $8.80. By March 2008, the price shot up to $20. Then, by that November, it crashed back to $9.35. The price then shot up five-fold by April of 2011 to $47.50 an ounce. As of March 2015, the price is back to around $16. That's a drop of more than 66%. This kind of volatility does not suddenly mean gold and silver make bad currencies. There's simply been a lot of speculation in these markets.

Until the market capitalization of bitcoin grows substantially, holding bitcoin carries risk. It's a speculative asset at this point. But we should not mistake volatility in a small, new market as an intrinsic problem with the currency.

Create Your Own Currency

Bitcoin is open-source, which means anybody can take the code, tweak it however they want, and then run their own version. As a result, many people have concluded, "Well, if anybody can create their own currency, the total supply is unlimited!" This objection collapses under scrutiny.

First of all, it's true that anybody can create his own crypto-currency. Over 1,000 alternative crypto-currencies exist besides bitcoin. But here's the difference: *alternative currencies operate on different blockchains and different networks.* This means all the computer power – the entire security of the Bitcoin network – is being used to secure one blockchain, not 1,000. Practically all of the new development, too, is being focused on the bitcoin blockchain.

However, there's more here than meets the eye. Alternative crypto-currencies (called "altcoins") actually benefit Bitcoin in a big way. They are laboratories for experimentation. Any of the algorithms in Bitcoin can be tweaked to try to create the best currency possible. If, for some reason, somebody creates an extremely beneficial tweak, there's no reason why it couldn't be incorporated into Bitcoin.

Out of the 1,000+ altcoins which exist, only a handful have any meaningful changes to the code. The vast majority are simple pump-and-dump schemes. Fraudsters will create a new altcoin, greatly overstate its benefits (the "pump"), and then sell all their coins while the price is temporarily high (the "dump"). There's even a coin called "BBQ-coin." Remember, no altcoin can access the bitcoin blockchain, and the security of their networks is tiny by comparison. The amount of bitcoin in existence will never change due to somebody creating

alternative software, an alternative blockchain, and an alternative network.

Some altcoin enthusiasts have argued that bitcoin is just too expensive to buy. But this argument doesn't hold water either. As stated earlier, $1 will currently buy over 250,000 units on the bitcoin ledger.

The freedom for anybody to create his own currency is a wonderful thing, and everybody benefits in the process. Say you don't like the idea of twenty-one million bitcoins, and you don't like that it will take around a hundred years to mine them all. You can, right now, create your own currency which has, say, ninety-seven billion units that come into existence all at once. Or, you could have them mined over a millennium. Afterward, you are free to persuade as many people as you like to use your currency.

Imagine that somebody does manage to create something superior to Bitcoin, and it's so radically different that the developers of Bitcoin can't merge it into their network. That's a wonderful thing! Such innovation benefits everybody except speculators in bitcoin. This creates radical, beneficial competition – something the monetary world has not seen in a very long time.

One success story has been an altcoin called "Dogecoin." It was created as an absurdist internet meme, but it caught on. Enough people got involved with Dogecoin that the community ended up raising over $25,000 to send the Jamaican bobsled team to the 2014 Winter Olympics. Compared to bitcoin, the community is still small, but that's what we'd expect in a market without any barriers to entry. Perhaps large companies will start issuing their own coins in the future. We can't really predict how the technology will be used.

So yes, anybody is free to create his own currency. But in doing so, they create an entirely separate public ledger and network. And unless they offer significant advantages, altcoins serve little purpose. Criticizing bitcoin because of the existence of altcoins is like saying, "If anybody can create their own car, then GM won't be able to compete." Actually, if GM produces a good product, they won't be harmed at all by your competition.

What About Mt Gox?

But what about the infamous Mt. Gox fiasco? For those who aren't familiar, Mt. Gox was a popular online bitcoin exchange that went bankrupt, and a lot of people lost their bitcoin in the process. The media has been especially harsh in criticizing bitcoin because of the virtual bank run on Mt. Gox.

This scenario, too, is easily cleared up. While it is a shame so many people lost their money, the failure of Mt. Gox has absolutely nothing to do with the soundness of bitcoin as a currency. Mt. Gox was a company that went bankrupt. Criticizing bitcoin because of a company bankruptcy would be like criticizing gold because a warehouse went bankrupt and people lost their gold.

In particular, Mt. Gox was terribly managed by its CEO Mark Karpeles, who may or may not be an outright criminal. Investigations are currently underway to figure out the answer.

To put it into perspective, understand that Mt. Gox was the first online exchange, ever, to swap bitcoin for fiat currency. It was essentially run by hobbyist nerds who wanted to trade their (at the time) quirky online money. In fact, "Mt. Gox" was originally a plat-

form to exchange trading cards with each other – MTGOX stands for "Magic: The Gathering Online eXchange." This was a company run by Magic card traders who picked up another hobby – no surprise the company eventually folded. Nearly all these first-generation bitcoin companies are dead. As bitcoin has grown, more legitimate businesses have taken their place.

To add more controversy to the Mt. Gox scandal, the company claimed that their failure was due to an actual problem with the Bitcoin software – an important claim, if true. They cited "transaction malleability" as the culprit. Unfortunately for them, transaction malleability was a well-known, well-documented part of the Bitcoin software, which every well-constructed bitcoin business knew about. There was even an entire Wikipedia article on the topic over a year prior to the failure of Mt. Gox. So, either they intentionally misled the public and blamed a scapegoat for their failure, or they were plagued by poor software engineering. Either way, in the long run, it's a good thing that the company doesn't exist anymore, though it is a shame so many people lost their funds.

Ultimately, Mt. Gox was a case of bad management, bad technical use of bitcoin, bad accounting, and potentially criminal leadership. It had nothing to do with Bitcoin being flawed, just like Enron's failure had nothing to do with electricity being flawed.

Mt. Gox was a big story, but it wasn't the only bitcoin bank run. Dozens of different companies have either gone bankrupt or disappeared with their clients' money. In every case, these failures happen for the same reason: bitcoin keys are held by third parties. At Mt. Gox, one person controlled all the keys to everybody's wallets – an obviously dangerous idea. The whole point of bitcoin is to allow users

to be the sole, secure owner of their money. Outsourcing this ownership to a third party is a big risk; once bitcoin is spent, there's no getting it back.

Bitcoin should be thought of as cash; you wouldn't leave a pile of cash lying around for a third party to watch. You'd put your cash in your wallet, where it belongs. The same is true of bitcoin: do not let somebody else hold your keys. At the end of this book, I will share some resources where you can find more information about how to properly secure bitcoin.

Deflation

One criticism is strictly economic. Some argue that bitcoin is a *deflationary* currency, and therefore won't work. A deflationary currency gains value over time, and therefore prices denominated in bitcoin would steadily fall. The overall price-level falling is what they are concerned about.

The textbook worry about deflation goes something like this: as prices fall, consumers realize their money can purchase more stuff in the future. So, they choose to hold on to their cash rather than spend it, which causes prices to fall even faster. Then, wage rates supposedly fall alongside consumer prices, further reducing how much money people spend. This, in turn, reduces the amount of goods produced in the economy, creating a downward spiral.

This story is inaccurate, both theoretically and empirically. The very foundation of the argument is wrong: when prices fall, consumers don't all refrain from spending. Take the electronics industry, for example. Everybody knows that the price of computers falls rapidly. If

you wait a year, that laptop you're eying will be heavily discounted from its current price. Yet, laptops and computers still get sold. The electronics industry is booming, even though consumers know prices will be much cheaper if they only wait a few months or a year.

Falling prices don't paralyze the economy for a simple reason: at some point, consumers will spend their money. Nobody holds on to cash indefinitely. The whole purpose of saving your money is to spend it in the future. As prices fall, more people get enticed to purchase stuff. Personally, I think computer graphics cards are too expensive, so I haven't purchased a nice one. But if the right deal comes along – if prices drop far enough – I will buy one. For this reason, falling prices draw buyers into the market, they don't push them out.

If all consumers don't radically change their behavior because of falling prices, the hypothetical scenarios about dangerous deflation don't hold much merit. And historically speaking, falling prices are almost always accompanied by an increase in production and standards of living. Prices fall because entrepreneurs find more efficient ways to produce. Falling prices should be *an expectation* in a competitive market.

Deflation isn't benign, however. Customers and merchants still have to deal with adjusting prices and negotiating contracts to take into account an appreciating currency. But this is not an insurmountable problem. The electronics industry has been dealing successfully with falling prices for many decades now. Furthermore, because the production of bitcoin is predictable, it's reasonable to expect the rate of deflation to be slow and predictable, in proportion to the natural rate of growth in the economy. Of course, this could only happen after the volatility of bitcoin stabilizes.

The astute reader might say, “But what about the Great Depression – wasn’t that caused by deflation?” The answer, without going into detail, is yes and no. The word “deflation” is ambiguous. In the most popular sense, “deflation” simply refers to falling consumer prices. But “deflation” can also mean *a contraction of the money supply*. And, when the money supply shrinks, less money circulates through the economy, and prices tend to fall. So, a “deflation” of the money supply results in a “deflation” in prices.

This is what happened during the Great Depression. Consumer prices fell, but it was *caused* by a contraction in the money supply. This contraction devastated the financial world, largely because the system was built on top of so-called “fractional-reserve lending.”

In a fractional-reserve system, banks only hold on to a fraction of their customers’ deposits, and they lend out the rest. This system works fine – unless customers start worrying about their deposits. If depositors withdraw their money from banks all at once – if they create a bank run – a fractional-reserve system can quickly implode. All deposits aren’t held in reserve, so when a bank runs out of money, some deposits essentially disappear – shrinking the total money supply. And that is what happened during the Great Depression. There were nation-wide bank runs, caused by worries about different banks’ financial health.

Of course, even the contraction of the money supply wasn’t the ultimate cause of the Great Depression. It was just one part. A full elaboration is not appropriate for this book, but keep in mind one often-overlooked fact: the entire decade prior to the Great Depression was marked by an *inflation* of the money supply. During the 1920’s, the United States’ central bank expanded the money supply and

helped create an unsustainable economic boom which infamously burst in the stock market crash of 1929. Of the many contributing factors to the Great Depression, the US central bank was a large one.

Bitcoin, however, does not face these systemic problems; it is not a fractional-reserve currency. You cannot lend bitcoin you do not have. Any bitcoin "bank runs" (like the failure of Mt. Gox) won't result in the kind of system-wide collapse which plagues fractional-reserve systems. And deflation measured by falling prices certainly poses no threat. On the contrary, it would be a sign of increased productivity. The disaster-scenarios constructed about deflation are largely based on economic and historical confusion.

Criminals and Terrorists

Another common objection is: what about criminals and terrorists? Won't they be drawn to bitcoin? The answer is yes, though probably more so in the future. Digital cash, if it becomes anonymous, will undoubtedly interest those with ill purposes, but in its current form, bitcoin is *not* anonymous. Every transaction is recorded in the blockchain, and law enforcement has had reasonable success identifying the owners of addresses on the ledger.

In its current state, bitcoin is more easily traceable than cash. Several underground black markets using bitcoin have already been busted and shut down by law enforcement.

However, let's say bitcoin became anonymous. In a few years, it's reasonable to assume that somebody will develop a reliable way to make it anonymous (people are currently working hard at this). So let's assume people could safely launder money, purchase illicit

goods, fund terrorism, etcetera, with bitcoin. We need to ask ourselves: is it worth it? Should all the benefits of bitcoin be thrown away to try and hamper the efforts of a very small group of people who will use bitcoin illicitly? I'd say no. Keep in mind: physical cash is by far the most popular currency for criminals. They use it almost exclusively to launder money, fund terrorism, and buy illicit goods. But that's no criticism of physical cash.

If we wanted to, say, "ban" bitcoin because criminals may use it, that would put regulators in a very awkward position. The same exact argument could be used to ban all cash, credit cards, bank accounts, the entire internet, casinos, and even Tide detergent, which is used as a black market currency in Washington, D.C.

The fact is this: criminals will *always* find a way to exchange currency with each other. It doesn't make sense to turn around and criticize the currency for it. Just like we shouldn't try to ban email because criminals use it to communicate with each other, we shouldn't try to ban bitcoin because criminals exchange it with each other.

And to be realistic, bitcoin by its nature is difficult to ban. The technology is already online, and it's not going away. It would be far, far more productive to think about how we can benefit from the currency and protect ourselves from any bad actors. We should indict the criminals, not the currency.

Real Challenges

Now that the most common misconceptions about Bitcoin are cleared up, I'd like to address the realistic challenges that Bitcoin faces.

Bitcoin supporters have a tendency to see the technology as invincible and perfect; it is neither. If we want to clearly understand Bitcoin, we must see the real obstacles it needs to overcome.

The 51% Attack

The most plausible challenge to the Bitcoin network is called the "51% attack." The details are technical, but the concept is fairly straightforward. As explained in Part One, the ledger is maintained by a decentralized group of computers running the Bitcoin software. These computers – called "miners" – contribute a massive amount of computer power verifying transactions and securing the network. The 51% attack could happen if one group controlled a majority of this computer power.

Part of the brilliance of Bitcoin is that the system works by *consensus*. The ledger is not maintained by a central authority; it's maintained by a decentralized group of miners who must rely on majority agreement. This has great benefits, but it also comes with risks. If a single group were to contribute the majority of computer power to the network, they could tamper with some important parts of the system.

For example, such a group could get away with "double-spending," allowing the same bitcoin to be spent twice in a short

period of time. Because miners determine which transactions are legitimate, a *majority* of miners could allow double-spending to happen. They could also block certain transactions from being verified – potentially blacklisting specific bitcoin addresses from spending funds.

They could not steal bitcoin from users' wallets, reverse transactions which had already been confirmed in the blockchain, or create new bitcoin out of thin air. The record of past bitcoin transactions wouldn't change, but they could meddle with pending and future transactions.

The greatest damage, however, would be the resulting loss of public confidence. A 51% attack might not ruin the technology, but it would certainly shake everybody's trust in the system. This is especially important in the early years of Bitcoin, while people are still evaluating its trustworthiness.

Now, some Bitcoin enthusiasts will respond, "A 51% attack wouldn't happen, because the miners involved would be shooting themselves in the foot. The bitcoin price would plummet along with their revenue." They often add, "Any group with such a massive amount of computer power would make more money legitimately mining than by orchestrating a 51% attack."

These claims are partially true, and in fact, we've already witnessed economic incentives regulating miners' behavior. Thousands of miners currently pool their computer power together. These "mining pools" contribute huge percentages to the overall computer power on the network. One mining pool briefly crossed the 50% mark, and many of its members voluntarily left and joined other

pools to quell any worries. As of December 2014, that mining pool now contributes around 20% of the overall computer power.

But these economic arguments overlook a crucial possibility: what about malicious actors? Right now, miners motivated by profits gain nothing by launching a 51% attack, but it's not difficult to imagine powerful groups in the future wanting to ruin the system outright.

Bitcoin could be perceived as a threat to powerful entities, whether governments, established corporations, or organized crime. Monetary loss would be irrelevant to a large government creating thousands of computers designed to mess with the Bitcoin network. It's unclear what would happen in such a scenario, but if a successful attack did happen, it would seriously reduce the amount of trust in the system.

Developers are aware of this, however, and they are currently working on potential software changes which would lessen the risk of a 51% attack. In addition, Bitcoin is an open-source project, which further limits the amount of damage malicious actors can cause. The rest of an uncompromised network could immediately "fork" the software – creating an alternative version along with a new network.

The 51% attack is not a big enough vulnerability to render Bitcoin technology useless, but if it were successfully executed, I believe the short-term consequences would be severe.

Governments

Perhaps the biggest unknown factor in Bitcoin's future is the response of governments. Nobody knows how governments across the

globe will react to Bitcoin, and the few countries that have commented on the technology have waffled on their positions. China, Russia, Germany, and Mexico have all issued warnings about bitcoin, and at one point, it was unclear whether or not Thailand had banned the currency outright. In the United States, bitcoin is considered "property" similar to a commodity for tax purposes, and regulators are in the process of creating more definite rules.

Given enough time, it's safe to assume that all governments will regulate Bitcoin in some way. The current size and growth of the market is too large to ignore. We can imagine a number of different governmental responses, some more threatening than others. Some countries might only lay out basic rules for taxation; others might demand strict consumer financial protection. A few might outlaw it and place strict penalties on using or accepting the currency. In China, it was illegal at one point for banks to use bitcoin – but legal for citizens.

One possible scenario is for governments to universally end up hostile towards Bitcoin, especially if the currency becomes popular for evading taxes. Instead of merely regulating it, they might try to shut down the entire system. If that happens, it's unclear what would result. The technology won't disappear, but it might render bitcoin essentially useless for regular citizens and drive it underground.

If it seems conspiratorial to imagine governments outlawing bitcoin, remember: during the Great Depression, the US government criminalized private possession of gold. They put people in jail for owning it and confiscated the metal on multiple occasions. It is not unrealistic to imagine bitcoin being outlawed.

This range of potential regulations is the reason many consider governments to pose a real challenge to Bitcoin. Some countries will be lenient, drawing bitcoin businesses into their countries. Others will undoubtedly make using bitcoin difficult.

In the United States, for example, regulators in New York City are currently drafting a "BitLicense" proposal requiring commercial holders of bitcoin to follow a large amount of financial regulations, bookkeeping rules, and know-your-customer requirements. The BitLicense, in its first iteration, has been almost universally criticized by industry leaders as being too stifling for the new technology. It's unclear what the final version of the BitLicense will be, but it's plausible that the United States will not end up being the most bitcoin-friendly country for businesses.

But one thing is clear: no government can effectively "ban" Bitcoin. There's no central organization to shut down. It's simply a piece of software – international and peer-to-peer. Anybody can access the network if they have an internet connection. Domestic governments might be hostile towards bitcoin and criminalize users, but their rules will not extend beyond their borders.

Ultimately, if people can access the internet, there's no feasible way to prevent them from using bitcoin, even if it's declared illegal.

Transaction Limits, Confirmation Times

Scalability is another real challenge facing Bitcoin. Right now, the Bitcoin network can only process a maximum of seven transactions per second. By comparison, PayPal processes over a hundred per second, and Visa processes over two thousand; Visa's infrastruc-

ture can handle a peak capacity of over forty thousand transactions per second.

The current frequency of bitcoin transactions doesn't come close to seven per second, but it's reasonable to assume this number will be reached and surpassed in the future. The transaction limit is changeable, but it requires careful software development, which the Bitcoin community is currently debating.

This particular change in the software will be significant, and it will come with trade-offs. For example, one proposed solution could end up inadvertently centralizing mining power by making it difficult for smaller players to compete – contrary to the original vision of the Bitcoin network.

Another challenge facing Bitcoin is what's called "confirmation time" – the time it takes for transactions to be verified as legitimate and safe from double-spending. While sending and receiving bitcoin is instant, its confirmation can take a while.

On average, one miner's confirmation takes around ten minutes. For best security, it's recommended for a transaction to be verified at least *six* times before being considered permanent. That's an hour's worth of work. In comparison to traditional payment methods, waiting an hour to securely transmit a million dollars is lightning quick. But waiting an hour to get a cup of coffee would be absurd. It's not realistic to imagine a successful payment system requiring customers to wait around for even one minute after their transaction, much less one hour.

Fortunately, there are solutions to this problem. Small-scale transactions are usually safe even with zero confirmations. Executing a double-spending attack takes a lot of effort, and it wouldn't be

worth it for trivial amounts of bitcoin. Companies like BitPay which process merchant transactions will accept "unconfirmed" transactions on their clients' behalf, taking on the risk of double-spending and allowing instant transaction speeds. However, by not waiting for several confirmations, the risk of fraud becomes higher. It's possible that a company like BitPay could be subject to an elaborate double-spending attack, given their high transaction volume.

This trade-off between speed and security will remain a legitimate challenge for Bitcoin. Developers are currently discussing ways this could be improved.

Worth noting: one *false solution* to the issue of confirmation times has been advocated by some altcoin creators. Instead of ten-minute confirmations, they might change the code to allow one or two-minute confirmations. Some are even shorter. But these changes are entirely superficial. An altcoin with a one-minute confirmation requires ten times less computer power to verify; it is ten times easier to manipulate, and it is ten times less secure. Instead of waiting for six confirmations to be super secure, you would need sixty. The security of crypto-currency transactions does not come from the nominal amount of confirmations, but rather the *amount of work* put into the verification process.

Neither the transaction limits of the Bitcoin network nor the confirmation times are insurmountable problems. But in order for Bitcoin to successfully scale, both of these areas will need to be addressed by developers and Bitcoin companies in the future.

The Year 2140

As explained in Part One, the rate at which new bitcoins are created gets incrementally slower until the year 2140, when the very last bitcoin will be mined. At that point, miners will only be rewarded for their work with transaction fees, not newly minted bitcoin. So the question is: will transaction fees be a large enough incentive for miners to continue securing the network?

We're talking about more than a century in the future, so we can't predict with any certainty what will happen, but we can imagine a few different scenarios. In the simplest scenario, transaction fees might indeed be large enough to sustain a decentralized group of miners. The transaction fees would likely be tiny per transaction, but the volume would be sufficient to make up for it.

If transaction fees aren't significant enough, the Bitcoin community will need to find new ways to support mining. Businesses will have a strong incentive to keep providing easy and secure payment options for their customers, so perhaps they will process their own transactions in-house. Or, companies might contribute to the maintenance of the bitcoin network simply for good PR.

Whatever happens, the industry will not be hit by any abrupt changes, because the transition to transaction-fee-only mining will be gradual. Miners will have many decades to prepare for it, and if Bitcoin is still popular a hundred years in the future, it's reasonable to assume entrepreneurs will figure out how to make the system work.

However, making any predictions about payment systems a century from now is entirely speculative – it's doubtful that anybody

reading this book will be alive by then. Given all the unknowns, concern about what happens in the year 2140 is reasonable.

Cryptography, Bugs, Hackers

The pillar supporting the entire Bitcoin infrastructure is mathematics. If the mathematical "cryptography" behind Bitcoin were faulty, the entire system would collapse. So, is the cryptography perfectly secure? I don't know. Neither does anybody else.

At the bottom of Bitcoin's architecture is a mathematical algorithm. Specifically, it's a very complex function. The stronger the function, the stronger the security. To date, nobody has found weaknesses with Bitcoin's algorithm, but other cryptographic algorithms have been found faulty and exploitable.

Fortunately, these flaws have not been catastrophic or resulted in immediate collapse. Any flaw with Bitcoin's algorithm would likely be discovered long before it became an issue for bitcoin users, and the software, being open-source, would allow miners to change the underlying algorithm without too much difficulty.

But let's be realistic: few people understand all the technical details behind Bitcoin. I am not one of them. Cryptographers have spoken very highly of Bitcoin's security, but most people are unable to verify for themselves that the mathematics is indeed solid.

Of course, the same could be said for almost any technology. Windows is ubiquitous software (though it's often full of bugs), but few people inspect the code themselves. We end up trusting the computer programmers.

The software, not just the underlying mathematics, might also contain flaws. No malicious code or backdoors have ever been found. However, back in 2010 – when Bitcoin was still new and practically unknown – one significant bug was discovered. It allowed an invalid transaction to occur which essentially created new bitcoins, and it was exploited by somebody with a sense of humor. The transaction didn't just create a handful of new bitcoins – it created 184 billion! Needless to say, this immediately raised red flags.

While it sounds like a worst-case scenario, the error was corrected within hours. The software was immediately patched to fix the bug, and the blockchain was successfully "forked." Meaning, the miners agreed to reset the ledger back to the point just before the invalid transaction occurred, effectively erasing the error. Even without centralized coordination, the network was able to handle this situation smoothly.

No other significant bugs have been found to date, but that doesn't mean they won't be in the future. Software bugs, by their nature, are often discovered after-the-fact.

Furthermore, even if it's true that the mathematics and software are sound *right now,* we can't predict what kind of technology will be invented in the future. What happens when young hackers have a decade to work on exploiting Bitcoin? What happens if governments spend billions of dollars researching ways to break the technology? Governments, in particular, have enormous amounts of money to spend on projects like this, and it's unclear whether the software can withstand such a challenge.

Quite simply, we don't know how Bitcoin will be attacked in the future, and we shouldn't act like we do. So far, the technology has

been incredibly resilient and trustworthy, and I am very optimistic about Bitcoin's future. But, the ultimate security of the system is not guaranteed.

OTHER INFORMATION

Buying, Using, and Storing Bitcoin

The purpose of this book was to give a conceptual overview about what Bitcoin *is*, not necessarily how to use it. For the interested reader, however, I will share a few resources and tips for how you can buy, use, and store bitcoin.

Purchasing bitcoin has become simple. If you want to buy bitcoin, you can easily set up an account at websites like Coinbase.com or Circle.com. You sync up your bank account, as you would an ACH deposit, and the company will sell you bitcoin by automatically drawing money from your bank account. These services also serve as online wallets, though they are less secure than storing the bitcoin yourself.

Using bitcoin is quite easy. It requires opening up your wallet, pasting in a bitcoin address, entering an amount, and hitting "send." If you store bitcoin on your phone, you can scan a QR code instead of pasting in a bitcoin address. Services like Coinkite.com also allow you to send bitcoin through email. That way, the recipient doesn't even need a bitcoin address to start off with. A word of warning: once you

start using bitcoin, you may find yourself frustrated by the traditional payment system. After sending and receiving instant payments, it can be difficult to go back.

The most important part of owning bitcoin is proper storage, and right now, it is by far the most difficult part. Nearly all the methods for super-secure storage require a number of steps that aren't easy for somebody unfamiliar with technology. Undoubtedly, there is a learning curve at this point in Bitcoin's development.

For the technophobe, keeping small amounts of bitcoin with online companies like Coinbase or Circle might be the best option, though one must realize the risks are dramatically higher for loss or theft. Large amounts of bitcoin should *not* be kept with third parties. For those interested in securely storing their bitcoin, or for those wanting to store large amounts, I recommend Googling "paper bitcoin wallets" and "cold bitcoin storage" and following the instructions. Or, you can contact a reputable Bitcoin consultant online who can help you out. Many other people have written in-depth guides on how to safely store bitcoin, but such walkthroughs are not part of the "what-is" nature of this book.

In 2015, a bitcoin ETF is expected to come out, essentially allowing investors to own bitcoin indirectly – like owning a stock. This will further reduce the barriers to entry for ownership. As the technology grows, it's reasonable to assume bitcoin storage won't require much technical skill, but we aren't there yet. In its current form, Bitcoin is not friendly for the non-tech-savvy consumer. This shouldn't be surprising: from a broader perspective, the technology is still in its infancy.

Conclusions

Understanding a new type of payment system is not an easy task – imagine trying to concretely understand all the moving parts of our current financial system, including all its networks, clearinghouses, intermediaries, regulations, security features, and weaknesses.

Most of us, myself included, don't know how the current system works in detail, just *that* it works, which is what we ultimately care about. I expect the same will happen with Bitcoin: the system works, and most people will neither understand nor care how it functions.

Bitcoin might end up being the payment system of the future, or it might not. It remains to be seen. Hopefully this book has provided enough information to help you make an informed opinion either way.

Postscript and Author Information

I sincerely hope you found this book helpful. Please feel free to share it with anyone you like, free of charge, and do consider leaving a review at the marketplace where you purchased it.

You can find my other work and contact information at stevepatterson.com. If you appreciate the information in this book, you can send me a bitcoin tip at: 164qx6RhYgXUF2zXjfFWBAvzWMrdT9q8eR: