



Nicolas de Bontin [Follow](#)

Former advisor with Merrill Lynch, now consulting for businesses centered on Fintech & Crypto. Write on Crypto trends and analysis. @ndebontin @amherstcollege
Dec 5, 2017 · 15 min read

An Introduction to Bitcoin and Cryptocurrency



There is tremendous interest in the cryptocurrency space right now and equal parts confusion, uncertainty and doubt. Bitcoin, cryptocurrencies, blockchain, ICOs. What do these even mean? The natural response to these foreign concepts is usually skepticism and rejection, but beneath the jargon lies a powerful new technology revamping our financial system.

Bitcoin started as an experiment in the depths of the global Financial Crisis of 2008 aiming to build a better financial system. Early on, cryptocurrencies developed a seedy undertone as they were mainly associated with black market trades: drug deals, ransomware payments, money laundering and tax evasion. Cryptocurrency has been described as the most disruptive technology since the internet as well as a fraud or a massive Ponzi scheme.

The pundits say it is a speculative bubble, but that's simply an easy out for those who have failed to find the proper explanations. They have the merits to ask the right questions, but ultimately fail to identify the

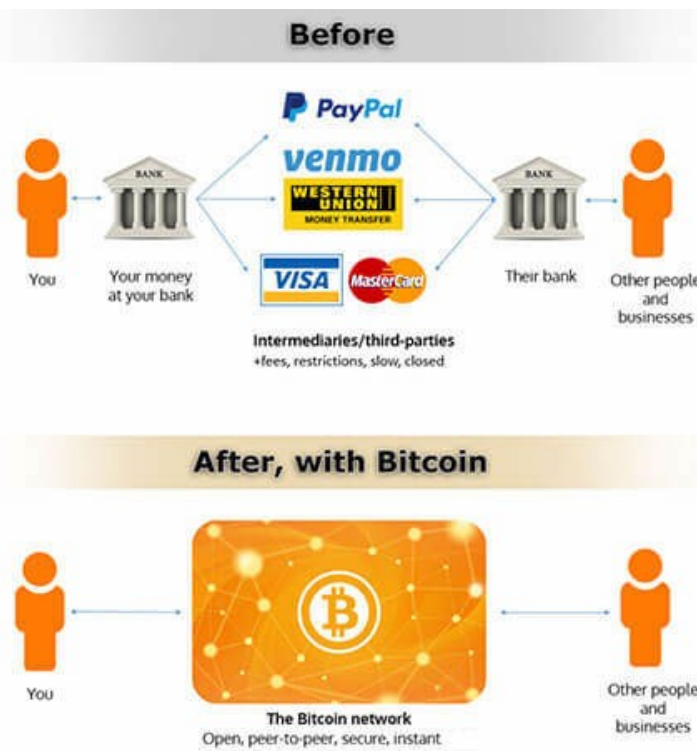
main reasons behind the fast-growing appetite for cryptocurrency. Bitcoin and other cryptoassets are an emerging new asset class experiencing rapid growth as a fundamentally innovative new technology.

We live in a digital era where the new generation prefers to trust the “abstract,” question traditional norms and find a better way forward through technology. Bitcoin brings a multifunctional financial utility to the world by creating an open financial system and allowing us to store and transact value in ways that we never thought imaginable before.

Part 1: Bitcoin

What is it?

Bitcoin is digital money that is not issued or controlled by anyone. It is used to securely store and transfer any amount of value anywhere in the world. It is used to buy goods and services, store wealth, or send value to anyone without the permission of a third party. Often regarded as “Digital Gold,” bitcoin that is stored properly cannot be hacked, stolen or seized by a government. Thus giving people full proprietorship much like having a **Swiss bank account** in their pocket. Unlike physical gold, Bitcoin is cheaper, faster and more efficient to store or send anywhere in the world. Bitcoin is divisible to the eighth decimal place and is completely digital, allowing the transfer of any monetary value. Opposed to government “Fiat” currencies, which can be manipulated and devalued, there is a finite supply of 21 million bitcoins making it a scarce and valuable asset. Bitcoin is the internet of money and will do for finance what the internet did for communication.



How Does it Work?

The Bitcoin network is a peer-to-peer network that runs on a decentralized distributed self-clearing ledger called the blockchain. Units of currency that run on the Bitcoin network are called bitcoins, which are used to store and transmit value among network participants. Unlike most currencies issued by central banks, which can be devalued and manipulated, bitcoins are issued according to a fixed set of rules to create sound money that can't be manipulated by a central authority or malicious actor. Users can buy or sell goods and services, send money to people or organizations, or even extend credit in a fast, secure and borderless manner. The only prerequisite for access to these coins is an internet connection and a private key that forms a pair with public-facing keys to provide access to the coins stored on the Bitcoin network. Unauthorized access to someone's private key is analogous to stealing gold from their vault.

"The Blockchain"

What literally is a blockchain? A blockchain is a tamper-proof, encrypted database secured by cryptography (*the study of encryption*) that acts as an accounting ledger keeping track of digital assets. Instead of being maintained by a single server like traditional databases,

blockchains are **decentralized** and maintained by a **distributed** network of computers around the world. This database tracks every bitcoin in the network and each transaction since the very first bitcoin. You can think of Bitcoin as an accounting system. Through the blockchain, it is a way of recording transactions and value digitally in an open and distributed self-clearing ledger.

Decentralized: *There is no central entity or one person with control.*

Distributed: *Instead of one central server owned and operated by a singular entity, Bitcoin's ledger is distributed across the globe making it impossible to shut down as there is no central point of failure. There is no Bitcoin HQ address for someone to raid; there is no central server to hack.*

Bitcoin Mining

The database is maintained by **miners**: people or businesses who have set up specialized computers to process transactions by contributing their electricity and computer processing power to the network. In exchange, they receive transaction fees and/or new bitcoins that are released into the network by the protocol when a new block is added to the chain. Miners provide a public service by securing the network and the network rewards them for their work.

For this to work, users broadcast transactions to the network and miners record them with specialized compute power by racing to complete complex mathematical puzzles, which *prove* that they are working for the Bitcoin network. Each new block is added to the blockchain and those transactions are confirmed and recorded every 10 minutes. Then the miners' race for the next block begins. This is all dictated by the rules of the Bitcoin algorithm/protocol and its underlying NSA cryptographic hashing algorithm (SHA-256) as outlined in the original [Bitcoin white paper](#).

Value of Blockchains

Before blockchains it wasn't possible to actually *own* a digital asset. If I send you an mp3 file you only have a copy, while the original remains with me—there are two copies. When it comes to money, if I send you \$10 it's very important that I no longer possess the \$10 and it's now yours. With blockchain technology, we now have a way to prove and

enforce the concept of digital scarcity and track the ownership of digital assets in a decentralized way.

The idea that we can have money living on the internet is a breakthrough. We now have the same open access architecture we saw on the internet for communication but for finance.

The first set of internet protocols enabled global permission-free exchange of information which has completely changed the world. This new set of blockchain based protocols or “cryptoassets” enable global permission less exchange of value. The ability to exchange value on the internet is a game changer. We will see vastly improved ways of organizing capital, new markets, or even decentralized autonomous organizations as blockchains will be making decisions, and allocating resources and capital in ways that no human can match.*

Blockchain Not Bitcoin

There has been plenty of hype amongst banks and businesses about the promises of the underlying technology of blockchain, but not Bitcoin itself. This represents firms building “private blockchains” similar to the narrative in the early days of the internet of private intranets vs. the public internet. For the same reasons as the internet, blockchain’s real value will be in open public blockchains, which offer free and open global access as they’re not in closed private systems. Decentralized public blockchains are building an entirely parallel system of finance rather than using the technology to update archaic infrastructure.

Bitcoin being digital in and of itself is not entirely revolutionary as the vast majority of the wealth in the world is already digital. When we check our bank account balances online we don’t actually have that amount of physical money sitting in a bank vault. Money is simply an accounting system. The bank runs its own private internal ledger (*accounting mechanism*) that keeps track of all the ones and zeros in the system (*account balances*).

Until now the only way to operate such a system was through the rules of a trusted third party. Now Bitcoin is governed in a decentralized way through the agreement of a fixed set of rules and people are starting to trust the laws of mathematics much more than the faith of their institutions.

"In its purest form, currency is confidence. It's a network effect around an agreed-upon medium of exchange that has some promise of scarcity. Bitcoin enforces its scarcity through a combination of cryptography and economic incentives ("cryptoeconomics"). A lot of people find that more comforting than relying on the good faith of a government. In math we trust."

- David Sacks Founder of Paypal

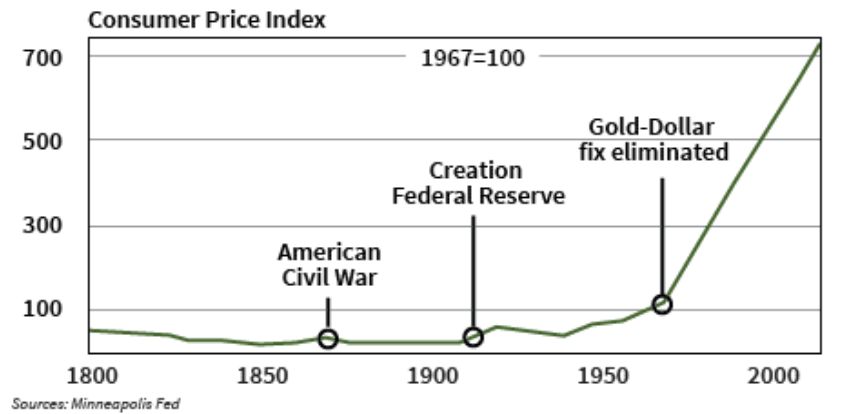
Evolution of Money

In the very early days people exchanged value via a barter system of trading goods followed by the development of commodity money (*i.e. silver and gold coins*) as they were easy to carry and divide, and had a level of scarcity that provided value. With the rise of banking arose a debt-based system where we deposited gold with the bank and they issued us a piece of paper representing how much gold we had with the bank. After all, it's much easier to carry around paper bills than a bag of gold.

In 1971, President Nixon abolished the **gold standard** ending the ability for people to redeem U.S. dollars for gold at the Federal Reserve, allowing the government full autonomy to freely print money, thus making the USD a **fiat currency** (*Fiat is Latin for "it shall be"*). Fiat currencies, which are now commonplace around the world, are not backed by tangible assets, only the promise from a government. Unfortunately, this led to currency manipulation and devaluation by governments to erode massive federal deficits at the expense of the consumer.

Goodbye Gold Standard, Hello Inflation

The gold standard, even in its partial form up to 1971, helped to control inflation. Since the switch to a fully fiat system, inflation has pushed prices about six times higher than they were 45 years ago.



The dollar has lost 90% of its purchasing power since the mid-Twentieth Century as a result of inflation. This is why many financial planners stress investing in assets like stocks, gold, real estate, etc., rather than holding cash: to preserve and grow wealth given fiat loses its store of value over time.

U.S. Dollar vs. Bitcoin

It's important to understand that the USD is the best transactional currency in the world. If I were stuck in the middle of the rainforest in South America I would want U.S. dollars as it is the reserve currency of the world. The USD is accepted nearly anywhere, but it is a terrible store of value.

For a long time, gold has been considered the ultimate store of value. Now people are turning to cryptocurrencies as they are more secure, easier to store and transport, cheaper to use, and easier to subdivide than any asset known today. It is disrupting the international payments and transfers business by cutting out the exorbitant fees of banks/middlemen, the global remittance market (people working in one country and sending money back home to their families), as well as becoming the currency of the internet and fueling a new wave of global e-commerce.

The underlying point here is that Bitcoin is not meant for paying for your Starbucks coffee instead of U.S. dollars. Most would rather use their Starbucks card and earn stars than use Bitcoin.

Bitcoin and the Developing World

People in the U.S. continue to underestimate Bitcoin because they live in the comfort of the most secure and stable financial system in the world. This is a much more real picture for those in other countries where there is rampant hyperinflation as a result of either government corruption or lack of economic growth (Venezuela, Argentina, Zimbabwe, etc.). Cryptocurrency provides an escape for those stuck under oppressive monetary regimes.

Another powerful way Bitcoin is changing the developing world is by providing financial services to those who don't have access. There are billions of people without access to financial services or a bank account, but do have access to a smartphone. Because all that is required to use Bitcoin is a smartphone with an internet connection, Bitcoin brings financial services to those who need it most. There is value in empowering people to "be their own bank" giving them the means to access, store and transfer value regardless of where they are in the world.

Bitcoin's Core Value Proposition

One of the first things that people think about when they learn about Bitcoin is **payments**. Every financial transaction we make, either with Venmo or our banks, has at least one intermediary that sits in the middle and takes a little cut. What if we could transact with one another in a peer-to-peer way without needing permission? All we need is an internet connection and we can send money to anyone, without anyone's permission, in the same way that the internet allows us to send information. Philosophically, Bitcoin assures that the money you have earned is yours and enforces the idea that you can truly own your wealth.

Payments and being a medium of exchange is an important part of Bitcoin's value proposition, but it's not the only part. Bitcoin is a highly censorship-resistant and permission-less **store of value**. Using the Swiss bank account analogy, there is around \$20 trillion dollars' worth of wealth in the world stored in offshore bank accounts and shell companies by major companies and many individuals. This is not illegal, rather it's to lawfully shield those assets from creditors, taxation, legal jurisdictions or even corruption. **Bitcoin and other**

cryptoassets fulfill this void and many others to a much greater extent as the first un-censorable and un-seizable asset in history.

Why You Should Own Bitcoin

You should own some bitcoin for the same reasons why you should invest in anything: to maintain or increase your standard of living over time. This is especially important in the face of inflationary pressures and the fact that fiat currencies are a terrible store of value. Everyone should build a diversified portfolio to secure their financial futures and enable them to achieve what they want most in life. Cryptoassets will play an important role in that as I believe Bitcoin and blockchain based assets are one of the greatest technological innovations and will represent the greatest wealth creation event of our time.

Part 2: What about Ethereum and all the other Cryptocurrencies?



Bitcoin is a store of value for the digital economy. It was the first major cryptocurrency and is only a precursor to the broader potential of blockchains.

The second largest cryptocurrency is Ethereum and it's main use case is to expand beyond the money use-case of Bitcoin. Ethereum is a much more programmable, general purpose blockchain that uses smart contracts (legal, financial, social, etc.) expressed in code. This allows other developers to build applications on top of Ethereum rather than building their own blockchain. A good comparison is to think of Bitcoin as “**Digital Gold**” and Ethereum as “**Digital Oil.**” Think of Ethereum as a massive global decentralized super computer that can process all

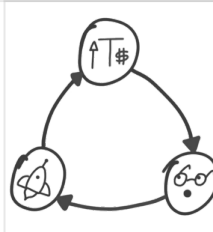
types of complex transactions or applications. Ethereum's native currency "Ether" is the oil in this analogy. It is used as fuel to pay for the costs of computation allowing other businesses, developers and individuals to build applications and process transactions on the Ethereum blockchain.

2017 and the Rise of Initial Coin Offerings (ICOs)

As a result of the rise of Ethereum, the barrier to entry for developers to create new networks has been lowered. In 2017 we saw a surge of ICOs on the Ethereum network. An ICO is where a group of developers builds a decentralized network with a token on the Ethereum blockchain and crowd-funds development by selling this token to the community in exchange for money to develop the protocol. On the other hand, the users have purchased a piece of the protocol itself and now own tokens to use as an investment for speculation, or pay for services and access on that network. These networks can power anything from decentralized file storage to prediction markets or a decentralized casino.

Blockchain technology and the underlying decentralized applications it enables are the internet's next frontier. The internet created tremendous amounts of value and changed the world yet the underlying fundamental internet protocols that we rely on to make the internet work, such as TCP/IP HTTP SMTP, accrued none of the value.

The thesis for this is called Fat Protocols by USV:

<p>Fat Protocols Union Square Ventures</p> <p>This relationship between protocols and applications is reversed in the blockchain...</p> <p>www.usv.com</p>	
---	---

Josh Brown from Reformed Broker summarizes this well:

There's a concept called Fat Protocols, which goes something like this: Tim Berners Lee, who effectively invented the World Wide Web in 1989, didn't really reap much of the financial benefit for his creation. All the monetary rewards went to the companies who built things on top of the HTTP

protocol or the FTP protocol etc. Yahoo, Google, AOL, Facebook—those were the winners. The protocols that actually run the web didn't retain any value in and of themselves. The Fat Protocols theory says that in crypto currencies it will be the other way around—most of the value will accrue to the network itself (in the form of the coins' values) and there will be a very thin layer of value on top for companies that create things.

Blockchains bring markets to networks by building a marketplace to price scarce resources, allocate those resources more efficiently and provide an incentive for trade. Because blockchains create digital scarcity they can monetize protocols via a cryptographic digital token, which essentially acts as a currency within each networks' own private digital economy. This allows people to directly invest in the protocol itself rather than a company building off of it. During the early stages of the internet, investing in the technology required one to make an early stage investment as a venture capitalist in companies like Amazon or Yahoo!, which build applications on top of these underlying internet protocols.

So what?

Cryptoassets represent the democratization of venture capital and the wealth generation of future technologies down to the users of the networks rather than elite groups of investors.

The rise of Bitcoin is the first time that we can monetize open source technologies, meaning everyday investors can participate in its growth rather than just those who invest in early stage companies. This produces viral network effects allowing networks to overcome the bootstrap problem because the users have a financial incentive in the networks' success similar to being an early investor in Facebook or Twitter.

Bootstrap Problem: Networks only become valuable after reaching a critical mass of users. i.e a social network with 10 people vs. a social network with one million.

Returning the Internet to its roots and Web 3.0

The first iteration of the internet originated in the 1960s as a survivable communications system for the military in the event of a nuclear attack on the United States. The key to its resilience was decentralization.

Unfortunately, over time the internet became increasingly centralized and monopolized as internet titans such as Google and Facebook profited by controlling users' personal data. Blockchain and decentralized technologies are returning the internet to its decentralized roots, putting users back in control of their data and eliminating the controls, restrictions and security limitations of for-profit entities.

By enabling the development of new open networks, tokens could help reverse the centralization of the internet, thereby keeping it accessible, vibrant and fair, and resulting in greater innovation. — Chris Dixon

Still with me?

Understanding blockchain technology today is a bit like understanding the internet in 1995. It wasn't until Netscape and the world wide web that the internet saw mainstream adoption as the ability to browse the web was one of its first mainstream applications. In the same way that you know how to use Safari to surf the web, soon enough you will interact with blockchains in your everyday life as the underlying infrastructure scales to support a plethora of mainstream user applications even beyond Bitcoin.