Bitcoin Basics

Over the past few months, cryptocurrencies have dominated headlines. Every day, it seems, another currency is released or another platform for tracking and trading currencies comes on line. Bitcoin, the best-known and best-established cryptocurrency, is still regularly posting increases in value as an ever-growing number of ordinary people become more comfortable with the idea of a democratized monetary system.

For anybody interested in learning the intricacies of cryptocurrencies, there are several outstanding books that go into every detail of Blockchain technology, Bitcoin, and the rise of cryptocurrencies. This book takes a slightly different tack: rather than focusing on the growth of Bitcoin or the technological intricacies of the Blockchain, it looks at the impact of those technologies. What happens when the exchange of wealth — and, on a deeper level, the exchange of goods and services — is taken out of the hands of governments, big banks, and multinational corporations? What happens when individuals can control the value of their work and time? How will they use that power? How can it transform their communities — and their world?

In that context, cryptocurrencies are a truly revolutionary idea. For most of human history, money has been controlled by established authorities and institutions, like kings and warlords, governments and central banks. Needless to say, these authorities had their own agendas which often ran counter to the needs and desires of their citizens. For average people, caught in the web of an economy or a society, there wasn't any way to escape the yoke of centralized currency.

This isn't to say that they didn't try. Private currency isn't a new idea: in fact, today's federally-issued "greenback" dollars only date to 1861, when the US government issued them to help finance the Union army. Before that, states — and even private banks — produced their own currencies. And the tradition of regional currencies continues today: many small towns and regions across the US issue their own community currencies — like Massachusetts' BerkShares or California's Bay Bucks. But these money systems are, for the most part, only useful in a very limited area, and they're usually backed by the US dollar.

Data Is Money

On its surface, the idea behind cryptocurrencies is simple: what if there were an internationally available monetary system that didn't rely on a central bank, was out of the hands of centralized governments, and was controlled by direct actions between individuals? The reality, though, is far more complex. To begin with, if we don't base currency in gold reserves or the "full faith and credit of the US government," what do we base it on?

In the case of Bitcoin, the answer is data. Historically, data are held or controlled by a limited number of people. Take, for instance, the data that someone might compile to make bets during a March Madness basketball tournament. They would start by gathering — or "proliferating" — all the available information on the 68 teams in play, including players, coaches, rankings, history of fouls and scores, and hundreds of other pieces of data. They would then combine the data in a home, such as a spreadsheet, a Word document, or an Access database. Depending on the program they used, they might even be able to make "queries," or ask questions about connections between elements, such as links between the age of player and his number of successful shots.

If our data compiler wanted to share this information with a friend, it would be necessary for both to use the same program, configured the same way. Often companies or organizations do exactly this — share databases and languages across several users. A very common language for databases is SQL (pronounced Sea quell), but there are several others.

Now imagine that our analyst let large numbers of people use the database to make their own queries. It would be tempting to manipulate the data — perhaps adjust the number of shots that a player has made, or the number of fouls that a team received — to influence the bets that the database's users make. If enough people make enough bets based on incorrect information, then it would be possible for the database inventor and his or her friends to make a lot of money.

This, on a broad scale, is what could happen with centralized currencies: companies, banks and governments that have access to classified information can affect the value of a currency. Sharing that information with a few friends and colleagues, they would be positioned to make winning bets on currencies or stocks, or other investments — often to the detriment of uninformed investors who are playing on a more level field.

Accuracy Through Sharing

One way to combat unequal access to information is by sharing information across a much broader group of people. In concept, if a large number of people had access to a database, but had to sign in every time they used it, its information would be very accurate — after all, the more people who transparently share the information, the lower the chance that any single person could introduce errors or exploit holes in it, and the greater the chance that someone else would discover the mistake.

This, by the way, is the concept behind Wikipedia, an online compendium that can be updated or edited by users. At its inception, critics predicted that that users would introduce mistakes, fundamentally flawing the site. In reality, the opposite happened: the large number of users ensured that no single individual could control the information. When errors find their way into Wikipedia, the sheer volume of users ensures that, in most cases, they don't stay long. In fact, repeated studies have shown that Wikipedia is as accurate or more accurate than most traditional reference sources, like dictionaries and encyclopedias.

At its heart, Bitcoin is also a shared database. Invented in 2009 by a consortium of workers who collectively called themselves "Satoshi Nakamoto," the Bitcoin software largely consists of a very secure ledger that lists all the transactions that the coin has ever gone through. The ledger is open sourced, which means that anyone can access it, and that no central authority — like a bank or a government — can control it.

To understand why this is different from standard money, let's imagine that I sold you a bicycle. If you paid me via credit card, somewhere a bank gets a three percentage transaction fee. Similar things would happen with PayPal or Venmo, or almost any system of payment: the payment platform would get a fee, as well as interest-free use of our money while it sat in their online account. There could also be wire fees, handling fees, taxes, and other charges.

By comparison, Bitcoin allows you and I to transact directly, without having a bank — or a government — touch our money. What's more, our Bitcoin transaction would be transparent to everyone with access to the system. Because we both would need to sign in, there could be no question about whose wallet the money came from, and whose wallet it went into. If there were a problem with the bike, or if there were an issue of nonpayment, it would be easy for both of us — as well as any third-party observer — to track the transaction.

To understand how this information would play out on a broad scale, it helps to contrast it with the 2008 housing crisis. In the years leading up to the crisis, analysts combined thousands of mortgages into mortgage-backed securities, then sold slices — or “tranches” — of the securities to investors. Because the mortgages were all combined into a sort of mortgage casserole, the investors couldn’t be sure about the quality of what they were buying. Neither, for that matter, could the insurance companies that promised to back the securities if they failed. On a fundamental level, every player in the transaction was flying blind.

We all know what happened: as the interest rates on many of these mortgages rose, the mortgages failed, and houses faced foreclosure. Unfortunately, it often wasn’t clear who owned the mortgages, who held the homes, who held the debt, or who needed to pay it back. By the time the crisis hit full swing, the people who had written the mortgages and those who had put together the securities were long gone, their profits locked up in bank accounts. As for the investors who had trusted them and the homeowners who hadn’t fully understood their mortgages, they were left holding the bag.

In a blockchain-based transaction, this disaster may have been averted. Since every coin contains a record of every transaction, it would be easy to see who wrote a mortgage, who held it, who had sold it, and how much they had charged. The money would have a trail, which would have led all the way to the doors of the speculators who created the bubble and ended up benefitting from it. It’s not surprising that the first Bitcoin block, the Genesis block, contains a hidden message: “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks,” suggesting that the creation of Bitcoin was directly inspired by these speculative mortgage activities.

Software Versus Hard Currency

One of the major things that distinguishes Bitcoin is that, for the most point, it only exists in the virtual world. Unlike a quarter or a dollar bill, most people will likely never ever physically touch a Bitcoin. But just because it's not tangible doesn't mean that it's not real: it can be bought and sold, and it can be used to purchase real, tangible things.

The value of bitcoin is supported by two things: the supply of coins and their security. As of this writing, there are just over 16.8 million Bitcoin, and supply will ultimately be capped at 21 million. In an interesting way, supply and security go together: new coins are "mined" by users who solve complex cryptographic equations, called hashes, which are connected to the Bitcoin blocks that preceded them, as well as to the Bitcoin blocks that follow them. In that way, all Bitcoins are connected, much like a family tree.

The number that solves a Bitcoin hash equation, called a "nonce," serves as the basis of each new coin. The math is very hard to do — as of March 2015, miners had to try 20.5 quintillion nonces to find one that fit a hash. As time goes on, and the value of Bitcoins increase, the hash equations become more difficult, a process that limits supply, and ensures that the value of Bitcoin doesn't drop. However, once a nonce is found, the math is very easy to check, which means that the numerical basis of a Bitcoin can be easily verified. For every equation that they solve, miners get a certain number of coins.

In addition to controlling supply, this mathematical complexity does another thing: it ensures that Bitcoins are very secure. As a new step in the Bitcoin Blockchain, hashes are very complex. And, once they're solved, they begin a new block in the Blockchain, which tracks what happens to every Bitcoin that's mined.

A Note on Investor Prejudice

To understand how Bitcoin flies in the face of traditional investment, it helps to look at how traditional investors like Warren Buffett have dealt with it. In February 1998, Buffett, the CEO of Berkshire Hathaway, purchased 130 million ounces of mined silver via Phibro, a subsidiary of Solomon Brothers, in which he had a large stake.[i] At the time, commodities analysts saw this as a bold move, but also recognized it as a classic, bare-knuckles investment. Basically, it looked like Buffett was cornering the silver market. He ended up pushing the price up, but eventually was forced to drop his holdings. Ironically, his move put a little tarnish on his golden halo.

Buffett isn't quite so bullish on non-tangible commodities. In the autumn of 2017, discussing mined cryptocurrencies, he said that "almost with certainty that they will come to a bad ending."[ii] Buffett's comments appear to be based on the tangible, commodity-based value of the token, rather than on the technology or community trust level driving the value. The thing is, in this economy, large-scale encryption is becoming more and more a valued commodity. While Buffett — like any World War II history buff — might be able to recognize the economic value of cracking Enigma, Nazi Germany's encryption device, he may be unable to see how this kind of computing power, and the security it yields, has become a commodity itself.

Playing With Blocks

To understand how blocks work, it helps to imagine three children, Ted, Ann and Sam, sitting in a sandbox. Ann picks up the block with the letter A. She calls it A and Ted and Sam agree. They place the block into the center of the sandbox. That's a finished block that they agreed upon. They then move on to the next block, B. And so on.

Eventually, though, they come to a fork. When they get to the letter F, Ted and Sam disagree with Ann about the next letter. Ann wants it to be G, while Ted and Sam want to use numbers instead. Ultimately, they part ways: Ted and Sam create their new alternate sequence using numbers and Ann continues building her order with the letter G. Sam and Ted's sequence becomes ABCDEF1, while Ann's becomes ABDEFG. Later, they and their friends might create increasingly complex, byzantine sequences, but they'll all begin with the same ABCDEF sequence, memorializing the early days of their blockchain.

Bitcoin is only one of many blockchains. Another popular one is Ethereum, which is based on "smart contracts." A smart contract, in short, is a piece of computer code that enables automatic execution of a transaction based on pre-defined arrangements between two parties. Going back to our friend Ann, imagine that she's playing on her father's computer. She opens an app, like Seamless, that shows her a lot of foods, arrayed on little tiles. She clicks on a Burger King Whopper and, a few minutes later, a delivery man shows up at the door with a burger.

In a manner of speaking, Ann has just executed a smart contract. In this case, the tile would be a "token," which automatically sets in motion a series of events that lead to a burger showing up at her door. In the crypto world, we'd say that she used a "crypto currency" to buy Burger King. She used no actual money, just a code that she activated by clicking on the square. Burger King had a smart contract attached to the code, meaning they had to automatically execute on the order. Calling the customer is not something Burger King does normally, but if it defined in the contract as something that they must do then they do it. The Ethereum smart contracts enable automatic execution of transactions that follow the protocols designed by their creator.

A Note on Consensus

For all the complex math underlying their security and supply, the exchange value of Bitcoin — or of any cryptocurrency — is ultimately based on a shared consensus. If a person wants to buy a Bitcoin for $1, it's worth $1. If someone else is willing to pay $2, it's worth $2. And so on. If people gain faith in the currency, and if the supply doesn't outstrip the demand, the value will rise. This, incidentally, works in much the same way as a stock.

On the surface, this might seem like a tenuous link to reality, the kind of thing that could easily lead to inflation or panics, bubbles and crashes. And – to be honest – it's likely that, as cryptocurrencies come into broader uses, those events will occur. Some cryptocurrencies won't have sufficient faith and will collapse. Others, like Bitcoin, will have stops and starts, times when their value increases or falls based on hiccups in the system and insecurities in the market.

While the faith underlying cryptocurrencies might seem shaky, it isn't all that different from the faith underlying regular US currency. Ultimately, the US government says that a dollar is worth a certain amount of money, the international financial markets go along with it, and the dollar maintains its value. As long as that happens, the world economy stays fairly secure, people continue to get paid, food continues to go on tables, and the world continues to turn.

But that stable dollar comes with a cost: because of the widespread need for a secure currency, governments around the world must work to keep the dollar's value consistent. China, for example, buys millions of dollars of US debt to keep the economy going, ensuring that US consumers will continue to buy Chinese products.

The most powerful people in the world know how to navigate that system: behind the scenes, politicians and businessmen wheel and deal over tariffs and trade, tax rates and interest rates, US debt purchases and bond issues, all knowing that the global financial system will bend over backwards to keep the dollar strong.

By comparison, imagine a system that's based on transparency and agreement, in which there's never any question about where a currency came from or how it was traded. A system in which people who use a currency agree on its value and how it should be traded. A system in which faith and clarity are at the forefront. That, at its heart, is the idea behind cryptocurrencies — and the dream of the currency creators that you're going to meet on the following pages.

[i] https://www.washingtonpost.com/archive/business/1998/02/04/buffett-discloses-big-silver-purchases/bc2c4d12-e997-4932-8a10-d62ec4ede139/?utm_term=.a90c336d2937

[ii] https://www.cnbc.com/2018/01/10/buffett-says-cyrptocurrencies-will-almost-certainly-end-badly.html