FEE's Essential Guide to

CRYPTOCURRENCY & BITCOIN

FEE FOUNDATION *for* ECONOMIC EDUCATION

FEE's Essential Guide to Cryptocurrency and Bitcoin

Essays from the Foundation for Economic Education

Contents

Introduction

What would life be like if our currency wasn't controlled by government and corporate agencies? What if there were no limits on the amount you can transfer to another person, no interference from authorities when those limits are exceeded, and perhaps best of all, no physical cash? It all sounds pretty futuristic.

Thanks to a few industrious entrepreneurs, the monetary future has arrived. Bitcoin is a virtual currency that was created and designed to give total financial autonomy to its users. There's no censorship, it's protected from inflation, and it's cheaper than other payment systems — just you and your coins, however you choose to use them. The use of cryptocurrencies liberates individuals to be able to manage their finances the way they see fit, without any prying eyes.

We have compiled our best articles on bitcoin and cryptocurrency into this essential guide. Bitcoin is a difficult subject to grasp, no doubt, but we hope that after reading this that you will have a more thorough understanding of what bitcoin is, how it works, and why the technology behind it will be the basis of the currency of the future.

Bitcoin for Beginners

Jeffrey A. Tucker

Understanding Bitcoin requires that we understand the limits of our ability to imagine the future that the market can create for us.

Thirty years ago, for example, if someone had said that electronic text — digits flying through the air and landing in personalized inboxes owned by us all that we check at will at any time of the day or night — would eventually displace first-class mail, you might have said it was impossible.

After all, not even the Jetsons had email. Elroy brought notes home from his teacher on pieces of paper. Still, email has largely displaced first-class mail, just as texting, social networking, private messaging, and even digital vmail via voice-over-Internet are replacing the traditional telephone.

It turns out that the future is really hard to imagine, especially when entrepreneurs specialize in surprising us with innovations. The markets are always outsmarting even the most wild-eyed dreamers, and they are certainly smarter than the intellectual who keeps saying: such and such cannot happen.

It's the same today. What if I suggested that digital money could eventually come to replace government paper money? Heaven knows we need a replacement.

Solving Problems a Byte at a Time

Money started in modern times as gold and silver, and it was controlled by its owners and users. Then the politicians got hold of it — a controlling interest in half of every transaction — and look what they did. Today money is rooted in nothing at all and its value is subject to the whims

of central planners, politicians, and monetary bureaucrats. This system is not very modern when we consider a world in which the market is driving innovations in other aspects of our daily lives.

Maybe it was just a matter of time. The practicality is impossible to deny: Gamers needed tokens they could trade. Digital real estate needed to be bought and sold. Money was also becoming more and more notional, with wire transfers, bank computer systems, and card networks serving to move "money" around. The whole world was gradually migrating to the digital sphere, but conventional money was attached to the ground, to vaults owned or controlled by governments.

The geeks went to work on it in the 1990s and developed a number of prototypes — Ecash, bit gold, RPOW, b-money — but they all faltered for the same reason: Their supply could not be limited and no one could figure out how to make them impossible to double- and triple-spend. Normally, reproducibility is a wonderful thing. You can send me an image and still keep it. You can send me a song and not lose control of yours. The Internet made possible infinite copying, which is a great thing for media and texts and — with 3D printing — even objects. But reproducibility is not a feature that benefits a medium of exchange.

After all, a currency is useless unless it is scarce and its replication is carefully controlled. Think of the gold standard. There is a fixed amount of gold in the world, and it enters into economic life only through hard work and real expenditure. Gold has to be mined. All gold is interchangeable with all other gold, but when I own an ounce, you can't own it at the same time. How can such a system be replicated in the digital sphere? How can you assign titles to a fungible digital good and make sure that these titles are absolutely sticky to the property in question?

Follow the Money

Finally it happened. In 2008, a person going by "Satoshi Nakamoto" created Bitcoin. He wasn't the first to solve the problem of double spending. A currency called e-gold did that, but the flaw was that there

was a central entity in charge that users had to trust. Bitcoin removed this central point of failure, enabling miners themselves constantly to validate the transaction record. He had each user download the full ledger of all existing Bitcoins so that each could be checked for its title and not used more than once at the same time. With his system, every coin had an owner, and the system could not be gamed.

Further, Nakamoto built in a system of mining that attempts to replicate the experience of the gold standard. **The math equations CPU power must solve get harder over time**. The early creators had it easy, just like the early miners of gold could pan it out of the river, though later they had to dig into the mountain. Nakamoto put a limit on the number of coins that can be mined (21 million by 2140). (A new coin is currently mined every 20 seconds or so, and a transaction occurs every second.)

He made his code completely open-source and available to all so that it could be trusted. And the payment system used the most advanced form of encryption, with public keys visible to all and a scrambling system that makes its connection to the private key impossible to discover.

No one would be in charge of the system; everyone would be in charge of the system. This is what it means to be open source, and it's the same dynamic that has made Wordpress a powerhouse in the software community. There would be no need for an Audit Bitcoin movement. Trust, anonymity, speed, strict property rights, and the possibility that applications could be built on top of the infrastructure made it perfect.

Bitcoin went live on November 1, 2008. To really appreciate why this matters, consider the times. The entire political and financial establishment was in full-scale panic meltdown. The real estate markets had collapsed, pulling down the balance sheets of the major banks. The investment banks were unloading mortgage-backed securities at an unprecedented pace. Boats delivering goods couldn't leave shore because they could find no backers for their insurance bonds. For a moment, it seemed like the world was ending. The Republicans held the White House, but the unthinkable still happened: Government and the central banks decided to attempt a full-scale rescue of the whole system, spending and creating trillions in new paper tickets to fill bank vaults.

Clearly government paper was failing. A digital alternative had to exist. But what gave Bitcoin its value? There were several factors. It was not fixed to any existing currency, so it could float according to human valuation. It was made from real stuff: the very 1s and 0s that were driving forward the global market economy. And while 1s and 0s can be reproduced unto infinity, the new coins could not, thanks to a system in which the coin and its public key were strictly controlled and the ledger updated for every transaction. Its soundness could be checked constantly through instantaneous conversion to other currencies as well as to goods and services. The model seemed impenetrable, the first digital currency that really addressed all the problems that had doomed previous attempts.

A Bitcoin of One's Own

Let's fast-forward in time to March 2013. I had become the proud owner of my first Bitcoin. My wallet lived on my smartphone. Only three years ago, some wonderful applications had already developed around the currency unit. Although I'm a bit techy, I'm not a rocket scientist and I'm quite certain that I would have been out of my league. But this is how digital institutions develop to become ever more user friendly. At the same event at which I became a Bitcoin owner, I also used a Bitcoin ATM. I put in the green stuff, held my digital wallet up to the scanner, and then I felt the buzz on my smartphone. Physical became digital. Beautiful.

But still I wondered what exactly I could do with these things. That's when the consumer world of Bitcoin products appeared before me. We aren't just talking about the Silk Road — a website that became notorious for enabling the easy, anonymous buying and selling of drugs. There are Bitcoin stores everywhere. And there are services in which you can buy from any website with a Bitcoin interface. There was growing talk of Bitcoin futures markets. Some companies were rumored to be going public with Bitcoins, and thereby bypassing the whole of the Securities and Exchange Commission. The implications are mind-blowing.

Sacred Pliers

Still, I'm a tactile kind of guy. I need to experience things. So I went to one of these sites. I bought the first product I saw (why, I do not know). It was a pair of pliers for crimping electric cables. I put in my shipping address and up came a note that said it was time to pay. This was the moment I had been waiting for. A QR code — that funny square design that looks like a 3-D bar code — popped up onscreen. I held up my "wallet" and scanned. In less than 2 seconds, the deed was done. It was easier than Amazon's one-click ordering system. My heart raced. I jumped out of my chair and did a quick song and dance around the room. Somehow I had seen it thoroughly for the first time: this is the future.

The pliers arrived two days later, and even though I have no use for them, I still treasure them.

Bitcoin had already taken off when the surprising Cyprus crisis hit in a big way. The government was talking about seizing bank deposits as a way of bailing out the whole system. During this period, Bitcoin essentially doubled in value. Press reports said that people were pulling out government currency and converting it, not only in Cyprus but also in Spain and Italy and elsewhere. The price of Bitcoin in terms of dollars soared. Another way to put this is that the price of goods and services in terms of Bitcoin was going down. Yes, this is the much-dreaded system that mainstream economists decry as "deflation." The famed Keynesian Paul Krugman has even gone so far as to say that the worst thing about Bitcoin is that people hoard them instead of spending them, thereby replicating the feature of the gold standard that he hates the most! He might as well have given a ringing endorsement, as far as I'm concerned.

Obsession and Resentment

My own experience with Bitcoin during this time intensified. I began to call friends on Skype and scan their QR codes and trade currencies. I began to rope other people into the obsession based on my experience: you have to own to believe. After one full day of buying, selling, and

using Bitcoins, I had the strange experience of resenting that I had to pay a cab fare in plain old U.S. dollars.

How do you obtain Bitcoins? This process can be a bit tricky. You can look up localbitcoins.com and find a local person to meet you to trade cash for Bitcoins. Usually, this exchange takes place at high premiums of anywhere from 10 percent to 50 percent depending on how competitive the local market is. It is understandable why people are reluctant to do this, no matter how safe it is. There is just something that seems sketchy about meeting a stranger in an all-night cafe to do some unusual digital currency exchange.

A more conventional route is to go to one of many online sellers and link up your bank account and buy. This process can take a few days. And then when you set out to transfer the funds, you might be surprised at the limits in the market that exist these days. Sites are rationing Bitcoin selling based on availability, just given the high demand. It could be 10 days or more to go from non-owner to real owner. But once you have them, you are off to the races. Sending and receiving money has never been easier.

Doubts?

As of this writing, a Bitcoin is trading for $88.249. Just three years ago, it hovered at $0.14. Many people look at the current market and think, surely this is a speculative bubble. That could be true, but it might not be. People are exchanging an unstable, fiat paper for something with a real title that cannot be duplicated. Everyone knows precisely how many Bitcoins exist at any time. Anyone can observe the transactions taking place in real time. A Bitcoin's price can go up and down, and that's fine, but there is no real speculation going on here that is endogenous to the Bitcoin market itself.

Is it a pyramid scheme? The defining mark of a pyramid scheme is that more than one person has an equal claim on the same money or good. This is physically impossible with Bitcoin. The way the program is set up, it is a strict property rights regime with no exceptions. In

fact, in early March, there was a brief hiccup in the system when some new coins were approved by one group of developers but not approved by another. A "fork" appeared in the system. The price began to fall. Developers worked fast to resolve the dispute and eventually the system — and the price — returned to normal. This is the advantage of the open-source system.

But what about the vague sense some people have that a handful of coders cannot, on their own, cause a new currency to come in existence? Well, if you look back at what Austrian monetary theorist Carl Menger says, he points out that a similar process is precisely how gold became money. Every new currency is not at first used by everyone. It is at first used only "by the most discerning and most capable economizing individuals." Their successful behaviors are then emulated by others. In other words, the emergence of money involves entrepreneurship — that is, **being alert to opportunities** to discover and provide something new.

Leviathan Leers

But what about a government crackdown? No doubt that attempt will be made. Already, government agencies are expressing some degree of annoyance at what could be. But governments haven't been able to control the cash economy. It would be infinitely more difficult to control a virtual currency with no central bank, with encryption, and with millions of users per day. Controlling that would be unthinkable.

There was a time when the idea that ebooks would replace physical books was an absurd notion. When I first took a look at the early generation of ereaders, I laughed and scoffed. Now I find myself looking for a home for my physical books and loading up on ebooks by the hundreds. Such is the way markets surprise us. Technology without central planners makes dreams come true.

It's possible that Bitcoin will flop. Maybe it is just the first generation. Maybe thousands of people will lose their shirts in this first go-round. But is the digitization of money coming? Absolutely. Will there always be skeptics out there? Absolutely. But in this case, they are not in charge. Markets will do what they do, building the future whether we approve or understand it fully or not. The future will not be stopped.

From Bitcoin to Ether: Today's Blockchain Basics

Billy Silva

Bitcoin and its underlying technology blockchain are game-changing technologies that are reshaping and revolutionizing the world economy.[1]

Often hidden behind the headlines of Bitcoin's meteoric rise in market value and blockchain's technological promise is a basic understanding of what these two technologies are and where they come from.

This brief article examines the digital currencies Bitcoin and Ethereum and introduces Blockchain, the technology that facilitates the digital transfer of value and much more.

Bitcoin: The Beginning?

I think the internet is going to be one of the major forces for reducing the role of government. The one thing that's missing, but that will soon be developed, is a reliable e-cash. — Milton Friedman, '99'

In 2008, a person or group of people acting under the pseudonym Satoshi Nakamoto published a white paper titled *Bitcoin: A Peer-to-Peer Electronic Cash System*. The paper introduced a solution to two puzzling issues.

The first was our inability to transfer money digitally between willing participants without the need of a trusted third party. The second was that a function was needed to transfer money digitally with the ability to establish the order of transactions to avoid double spending.

Nakamoto proposed two solutions:

1. A peer-to-peer currency capable of maintaining its value without a central authority.

2. A decentralized digital ledger capable of establishing the order of transactions.

The ledger would operate much the same as any other, except that the recorded transactions would be distributed to computers around the world.

In 2009 the ability to transfer value digitally was born in what is widely known as Bitcoin. However, it is the second capacity, now known as blockchain that is proving to be of far greater significance.

Although blockchain has scarcely found its way into mainstream thinking and discourse, it is, as mentioned, revolutionizing the world economy.

Bitcoin and Ethereum

Since inception, Bitcoin has captured the attention of an ever-growing, and yet relatively small, number of investors, enthusiasts, companies, and others around the globe.

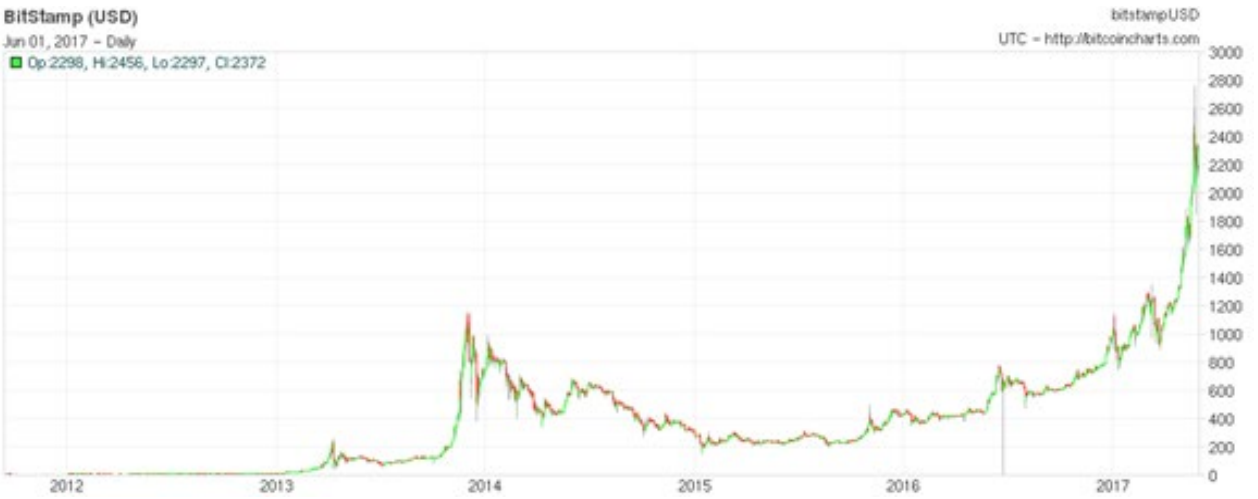
As it has grown, it has served the dual function of acting as proof of concept for a "peer-to-peer version of electronic cash" and simultaneously giving rise to thousands of other digital currencies.

The most well known of these currencies by market value are Bitcoin and Ethereum. Bitcoin's current market value is $37 Billion USD, while Ethereum's is $16 Billion USD.

Any attempt however to compare the two cannot be accurately described as an apples-to-apples comparison. More about this later. First, let's look at what Bitcoin actually is.

Bitcoin

Bitcoin is a decentralized peer to peer electronic version of cash that maintains its value without backing or inherent value. It allows the transference of money digitally without going through a trusted third party such as a bank or credit card.



The first standardized value of Bitcoin was set on October 5th, 2009 at $.0008, calculated using $1USD equals 1309.03 Bitcoin (BTC). It presently trades at more than $2300 USD. This represents 2.9 million x its initial value.[4]

According to the *Washington Post*, if you had purchased $100 in Bitcoin seven years ago, those coins would be worth more than $73 million USD today. To put this into perspective, if you had invested $100 into Amazon.com when it went public in 1997, your investment would be worth just under $64,000. It is worth noting, however, that digital currencies are significantly more speculative than stocks like Amazon.[5, 6]

As the price of Bitcoin goes higher, one question that naturally comes to mind is, Where do Bitcoins come from?

Mining

Where do Bitcoins come from if by definition they are not backed by any central authority? Bitcoins are actually "mined" into existence by Bitcoin miners.

The easiest way to think about this is to consider gold miners. Gold miners work to mine gold from the earth. As it is mined, it then enters the economy. Conceptually, Bitcoin is the same.

New Bitcoins are generated through a competitive process called mining. Miners are given Bitcoins as rewards for their services processing transactions and securing the network using highly specialized hardware.[7]

Investopedia offers a more in-depth explanation of the **process of mining**.

How Are Bitcoins Used?

After Bitcoins are mined into existence, how are they used and what are they used for?

Bitcoins are traded on exchanges like stocks, bonds, and currencies, and are also used as currency in the exchange of goods and services.

The number of vendors and merchants accepting Bitcoins for the exchange of goods and services is expected to grow from the 1000's to the 100,000's now that Japan is accepting Bitcoins as currency.

Japan is the first nation to officially accept Bitcoin for payments. More than 300,000 merchants will begin accepting Bitcoin payments in that country alone.[8]

Here is a list of **100 major US-based retailers** currently accepting Bitcoin.

Bitcoin, however, is not the only digital currency growing in value and capturing global attention. Ethereum shares many of these characteristics with Bitcoin while also possessing several unique qualities.

Ethereum

I would say Ethereum boasts features and opportunities to things Bitcoin doesn't. It's like saying a telephone can beat an orange. — Vitalik Buterin, 2014[9]

While Bitcoin was first to market and has drawn most of the media attention, many believe that the Ethereum blockchain, and its currency Ether, is a much more powerful tool.

In 2013, then-19-year old Vitalik Buterin proposed Ethereum in a **white paper** titled "Ethereum White Paper: A Next Generation Smart Contract and Decentralized Application Platform."

The development of the protocol was crowd-sold in 2014, raising over $150 million USD. The system itself was finally launched on July 30, 2015.

Ethereum is an open source blockchain platform and its fundamental contention is this, that blockchains can be used for more than just the transfer of money.

Additional use cases include currencies, financial instruments, property, domain names, along with more sophisticated cases like exchanges, derivatives, peer to peer gambling, and identity and reputation systems.[10]

Smart Contracts

"Smart contracts" are one of Ethereum's most important contributions to the rapidly expanding universe of digital currencies and blockchains.

They can be thought of as a digital means of facilitating the exchange of anything of value in a way that is transparent and removes middlemen such as lawyers, notaries, and others. Smart contracts perform this function by carrying out the terms of the digital contract itself.[11]

Another of Ethereum's unique characteristics is its digital currency Ether.

Ether

Ethereum, like Bitcoin is a digital currency. However, unlike Bitcoin, it is also a blockchain platform. Ethereum's currency, Ether is used primarily to access the Ethereum network.

The Ethereum Foundation defines Ether as a *fuel* or a form of payment that is used by clients of the Ethereum platform to pay for the machines that are executing the requested operations.[12]

Unlike Bitcoin, Ethereum has two digital currencies trading in the market. The first is Ethereum which trades under the symbol — ETH. While the other, known as Ether Classic, trades under the symbol ETC.

In June 2016 a large scandal rocked the Ethereum community. A still-unknown hacker attempted to steal more than $50 million dollars due to a software bug. The end result was the creation of a second Ether trading currency.

If it is of greater interest here are two articles that explain the hack in more detail **Article 1** & **Article 2**. For a more technical explanation **read this article** by Maria Paola Gelvez Gomez, former head of Coinbase in Latin America.

Where Does Ether Come From and What Is It Used For?

Similar to Bitcoin, Ethereum is also mined. Groups of "miners" work to validate and store the transactions taking place on the Ethereum platform. The *Huffington Post* presented a clear and coherent article on **Ethereum mining**.

While Bitcoin and other digital currencies can be used to purchase goods and services, as mentioned, Ether is primarily used for transactions associated with accessing the Ethereum network and trading.

What is most important to remember about Ethereum is that it is not only a digital currency, it is also blockchain based platform with smart contracts, and it allows for the building of apps, of which digital currencies are but one expression.

Blockchain

The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value. — Don and Alex Tapscott [13]

What is a Blockchain?

Nakamoto Satoshi's initial description of the framework needed to facilitate the movement of online payments between two willing participants without an intermediary has become known as blockchain.

In its most simple form blockchain is a decentralized ledger. The implications of blockchain however, are far greater than the simplicity its name implies.

Blockchain facilitates the digital transference of value itself. Sally Rivers, *Financial Times* technology writer describes the relationship between blockchain and digital currencies like Bitcoin: "[Blockchain] is to Bitcoin, what the internet is to email."

In the same way the internet facilitates the digital transfer of information, blockchain facilitates the digital transfer of value.

Industries in which blockchain technology is being rapidly explored and deployed include the capital markets, financial services, payments and remittances, derivatives, identity and reputation management, governance, sharing economy, supply chain, auditing, stock trading, internet of things, insurance, healthcare, and others.

A Few Takeaways

Digital currencies and Blockchain technology are truly reshaping the world economy. We may, however, be too close to their inception to accurately assess their importance or ultimate impact.

A few key thoughts from this post:

- Bitcoin was founded in 2008 and launched in 2009. Bringing with it digital currencies and the underlying technology, blockchain.
- There are thousands of new digital currencies of which Bitcoin ($30bil) and Ethereum ($16bil) are the largest in terms of market value.
- These currencies are created through a process of digital mining akin to mining for gold.

- Many of these currencies are traded on exchanges like stocks, and used for the purchase of good and services.
- Ethereum recognized blockchains can be used for more than digital currencies, and introduced smart contracts.
- Blockchain is to Bitcoin, as the internet is to email.

One of the best and most insightful presentations on Blockchain is a **30-minute video** created by Farzam Ehsani, Blockchain Lead at the Rand Merchant Bank in South Africa. I highly recommend it to everyone.

Referring to the unfoldment of this new technological development, in a polite and slightly prophetic tone Mr. Ehsani shared in his closing statement, "We are on that journey, and there's no turning back."

It is indeed true. We are on a new digital journey, and no, there is no turning back!

Bitcoin Technology: A Festival of the Commons

Andreas Antonopoulos

Open-source technologies such as bitcoin are a combination of open-source software, common technology standards, and a participatory decentralized network. These layers create a three-tiered commons where innovation contributed by users adds to the common platform, which makes it better for everyone.

But for the last few hundred years, we have generally thought of goods as best belonging to the private domain. Consider that, in economic terms, the "tragedy of the commons" is a market-failure scenario where a shared public good is overexploited. In this scenario, each user has an incentive to maximize his or her own use until the good is depleted.

The example used to illustrate this economic theory is a grassland (a "village commons" in British English) that is unregulated and overgrazed by cattle until it deteriorates to a muddy field. The tragedy of the commons occurs when individual self-interest combined with a large economic externality (the cost to the commons) create a market failure for all.

The opposite of the tragedy of the commons is called a "comedy of the commons," but I prefer to use the term "festival of the commons," which conjures a better visual example: a grassland used to hold a community festival that benefits everyone. The **comedy of the commons** was first stipulated as an economic theory governing public goods such as knowledge, where individual use of the common good does not deplete the good but instead adds to it.

The **sharing economy**, which consists of open-source software (for example, Linux), participatory publishing (Wikipedia), and participatory networks (BitTorrent), creates conditions where increased participation

adds to the good's underlying value and benefits all participants. In such cases, the underlying good is knowledge, software, or a network, and its availability is not depleted by individual use.

Software applications are themselves open-sourced and add to the commons, offering new capabilities for all subsequent innovators. Enhancements to the protocol bring new features across the entire network, allowing the ecosystem to build new services around them. Finally, as more users adopt the technology and add their resources to the P2P network, the scalability and security of the entire network increases.

Open-source currencies have another layer that multiplies these underlying effects: the currency itself. Not only is the investment in infrastructure and innovation shared by all, but the shared benefit may also manifest in increased value for the common currency. Currency is the quintessential shared good, because its value correlates strongly to the economic activity that it enables. In simple terms, a currency is valuable because many people use it, and the more who use it, the more valuable it becomes. Unlike national currencies, which are generally restricted to use within a country's borders, digital currencies like **bitcoin** are global and can therefore be readily adopted and used by almost any user who is part of the networked global society.

The underlying festival-of-the-commons effect created by open-source software, shared protocols, and P2P networks feeds into the value of the overlaid shared currency. While this effect may be obscured in the early stages of adoption by speculation and high volatility, in the long run, it may create a virtuous cycle of adoption and value that become a true festival of the commons.

The festival is now open. Who will join it?

Bitcoin: Currency of Currencies

Steve Patterson

Bitcoin's creation represents a watershed moment in monetary history. For the first time, a currency combines the strengths of commodity money with the convenience of fiat money, while avoiding the problems with both. Bitcoin is a new type of currency created for a new type of world: the digital world. And as more people trust bitcoin, it has the potential to completely overturn the established financial system.

Around the globe, nearly everybody uses fiat money — paper currency not redeemable in anything. But this wasn't always the case. With few exceptions, paper emerged as a popular currency for a specific reason: it was redeemable in precious metals. Only recently has this not been the case. This concept of *redeemability*, when applied to bitcoin, suggests that history might repeat itself in a big way.

For the last millennium, a key storyline in the history of money has been the relationship between precious metals and paper. Gold, silver, and paper have all been used as currencies. At times, precious metals were used directly as currency; circulating coins were stamped in gold or silver. At other times, paper bills were used as currency — either redeemable in gold or silver, or not backed by anything at all.

Given enough time, all experiments with fiat paper money have ended in failure. So I want to focus on the success story: paper currency, redeemable in precious metals, emerging as the dominant form of money. How did it happen?

The story goes like this: several centuries ago, gold and silver were the most popular currencies in the Western world. (For the sake of brevity, I will refer to "gold and silver" as just "gold" in this article.)

People often stored their gold in vaults with goldsmiths to keep it safe. On depositing their gold, they would be issued a paper receipt, which they could redeem on demand — like a coat check at a fancy hotel.

So, if person A wanted to trade with person B, he could pick up his gold from a goldsmith and exchange it for whatever good or service he wanted with person B. Then, person B could take his new gold back to a goldsmith who would issue him a new receipt. Not the smoothest process, but it worked.

As you can imagine, people found a way to streamline this system. Instead of trading physical gold, person A could simply trade his paper receipt — his claim for the gold — to person B. That way, gold ownership transferred without the hassle of lugging physical gold around. The paper receipt was essentially *as good as gold*.

Person B could also now avoid carrying metal around by trading his paper receipt. He might exchange it with person C, who could turn around and trade it again with person D, and so on. Physical gold needed not actually circulate, unless people wanted to redeem their receipts for it. Thus, paper receipts emerged as a popular form of currency. And as I'll argue in a moment, this system has huge implications for bitcoin.

In theory, under this system, the total supply of paper currency was limited by the amount of gold stored in vaults. But in practice, the goldsmiths would sometimes create fake receipts, not backed by anything; it's called "fractional-reserve lending," and it's a topic for another time. The important part is this: the monetary system relied on trust placed in goldsmiths. You had to believe that the paper receipts were tied to something concrete — that they weren't just created out of thin air.

Under this system, paper currency is valuable because it represents a claim to a finite amount of gold. If the supply of currency becomes unlimited, detached from the finite supply of gold, that currency eventually becomes worthless. The paper is no longer as good as gold; it's only as good as paper, which isn't very good at all. Unfortunately, this process of currency devaluation has happened dozens of times throughout history.

Governments have also denominated their currencies in relation to precious metals. For example, during half of the 20th century, one US dollar could officially be redeemed for 1/35th an ounce of gold. But, due to political mischief, the United States canceled its policy of redeemability during the 1970s, and the dollar has been a fiat currency ever since.

What does this have to do with bitcoin? Here's my theory: the same phenomenon that happened with gold and paper can happen again with bitcoin and paper. The *redeemability* of bitcoin will give it incredible use as a currency. It's more convenient to use than paper — just as paper is more convenient to use than gold — but unlike paper, it is inflation proof.

If that sounds like a bunch of abstract mumbo jumbo, here it is in more concrete terms: right now, people across the world are accepting bitcoin through payment processors like Bitpay, and they immediately convert their bitcoin into local currency. They might sell a product for 1 BTC, but they instantly *redeem* that bitcoin for, say, dollars, euros, or yen. It's this process that I imagine will change in the future, with huge implications.

Naturally, people are redeeming their bitcoin right now because they're unsure; it's a new type of currency, and they don't want to get stuck holding something worthless. But what happens when the fear and uncertainty around bitcoin diminish? If you know you can immediately redeem your bitcoin safely, the incentive to actually do so lessens. It's like holding a goldsmith's receipt; yes, you can go to the vault and get your gold, but it's an unnecessary hassle when you could just hold on to the receipt instead.

Bitcoin is easier to transact than paper; you can send it anywhere on the planet. Plus, it is protected from counterfeiting, unlike paper money. And nobody has to worry about fractional-reserve bitcoin receipts — every bitcoin is publicly viewable by visiting the corresponding address on the blockchain. And, *you,* not a goldsmith, have final access to your bitcoin if you hold the keys. With all of these advantages, the incentive to redeem your bitcoin shrinks.

Here's where it gets really exciting: if bitcoin is held as this sort of meta-currency, one feature cannot be overstated: it is inflation proof. Paper is way more convenient than gold, but it has a catastrophic Achilles' heel: it can be printed out of thin air. Bitcoin is way more convenient than paper, *and we don't have to worry about its inflation*. It merges super portability with super security. Historically speaking, no currency has ever existed with both of these properties.

And this convenience says nothing about the technical potential for bitcoin; keep in mind, bitcoin is software, and it can evolve even greater properties in the future. You can't say that about gold.

Just as paper emerged on the back of gold, bitcoin might emerge on the back of paper. If redeeming bitcoin for local currency becomes superfluous, the monetary world might be turned on its head. Instead of denominating bitcoin in fiat currency, fiat currency might end up being denominated in bitcoin. After all, it was the connection with precious metals that protected paper currency from inflation and gave it significant appeal. And it could be argued that bitcoin has an even more strictly limited supply than precious metals.

It might sound idealistic, but bitcoin could represent the beginning of a new financial world built on a solid, digital, noninflationary foundation. As with the emergence of gold, silver, and paper as money, the market will ultimately decide which currency is best.

What Gave Bitcoin its Value?

Jeffrey A. Tucker

Many people who have never used bitcoin look at it with confusion. Why does this magic Internet money have any value at all? It's just some computer thing that someone made up.

Consider the criticism of goldbugs, who have, for decades, pushed the idea that sound money must be backed by something real, hard, and independently valuable.

Bitcoin doesn't qualify, right?

Maybe it does. Let's take a closer look.

Bitcoin first emerged as a possible competitor to national, government-managed money nearly six years ago. Satoshi Nakamoto's **white paper** was released October 31, 2008. The structure and language of this paper sent the message: This currency is for computer technicians, not economists nor political pundits. The paper's circulation was limited; novices who read it were mystified.

But the lack of interest didn't stop history from moving forward. Two months later, those who were paying attention saw the emergence of the "Genesis Block," the first group of bitcoins generated through Nakamoto's concept of a distributed ledger that lived on any computer node in the world that wanted to host it.

Here we are six years later and a single bitcoin trades at $500 and has been as high as $1,200 per coin.The currency is accepted by many thousands of institutions, both online and offline. Its payment system is **very popular** in poor countries without vast banking infrastructures but also in developed countries. And major institutions — including the Federal Reserve, the OECD, the World Bank, and major investment houses — are paying respectful attention.

Enthusiasts, who are found in every country, say that its exchange value will soar in the future because its supply is strictly limited and it provides a system vastly superior to government money. Bitcoin is transferred between individuals without a third party. It is nearly costless to exchange. It has a predictable supply. It is durable, fungible, and divisible: all crucial features of money. It creates a monetary system that doesn't depend on trust and identity, much less on central banks and government. It is a new system for the digital age.

Hard lessons for hard money

To those educated in the "hard money" tradition, the whole idea has been a serious challenge. Speaking for myself, I had been reading about bitcoin for two years before I came anywhere close to understanding it. There was just something about the whole idea that bugged me. You can't make money out of nothing, much less out of computer code. Why does it have value then? There must be something amiss. This is not how we expected money to be reformed.

There's the problem: our expectations. We should have been paying closer attention to Ludwig von Mises' theory of money's origins — not to what we think he wrote, but to what he actually did write.

In 1912, Mises released *The Theory of Money and Credit*. It was a huge hit in Europe when it came out in German, and it was translated into English. While covering every aspect of money, his core contribution was in tracing the *value and price* of money — and not just money itself — to its origins. That is, he explained how money gets its price in terms of the goods and services it obtains. He later called this process the "regression theorem," and as it turns out, bitcoin satisfies every condition of the theorem.

Mises' teacher, Carl Menger, demonstrated that money itself originates from the market — not from the State and not from social contract. It emerges gradually as monetary entrepreneurs seek out an ideal form of commodity for indirect exchange. Instead of merely

bartering with each other, people acquire a good not to consume, but to trade. That good becomes money, the most marketable commodity.

But Mises added that the value of money traces backward in time to its value as a bartered commodity. Mises said that this is the only way money can have value.

> The theory of the value of money as such can trace back the objective exchange value of money only to that point where it ceases to be the value of money and becomes merely the value of a commodity.… If in this way we continually go farther and farther back we must eventually arrive at a point where we no longer find any component in the objective exchange value of money that arises from valuations based on the function of money as a common medium of exchange; where the value of money is nothing other than the value of an object that is useful in some other way than as money.… Before it was usual to acquire goods in the market, not for personal consumption, but simply in order to exchange them again for the goods that were really wanted, each individual commodity was only accredited with that value given by the subjective valuations based on its direct utility.

Mises' explanation solved a major problem that had long mystified economists. It is a narrative of conjectural history, and yet it makes perfect sense. Would salt have become money had it otherwise been completely useless? Would beaver pelts have obtained monetary value had they not been useful for clothing? Would silver or gold have had money value if they had no value as commodities first? The answer in all cases of monetary history is clearly no. The initial value of money, before it becomes widely traded as money, originates in its direct utility. It's an explanation that is demonstrated through historical reconstruction. That's Mises' regression theorem.

Bitcoin's use value

At first glance, bitcoin would seem to be an exception. You can't use a bitcoin for anything other than money. It can't be worn as jewelry. You can't make a machine out of it. You can't eat it or even decorate with

it. Its value is only realized as a unit that facilitates indirect exchange. And yet, bitcoin already is money. It's used every day. You can see the exchanges in real time. It's not a myth. It's the real deal.

It might seem like we have to choose. Is Mises wrong? Maybe we have to toss out his whole theory. Or maybe his point was purely historical and doesn't apply in the future of a digital age. Or maybe his regression theorem is proof that bitcoin is just an empty mania with no staying power, because it can't be reduced to its value as a useful commodity.

And yet, you don't have to resort to complicated monetary theory in order to understand the sense of alarm surrounding bitcoin. Many people, as I did, just have a feeling of uneasiness about a money that has no basis in anything physical. Sure, you can print out a bitcoin on a piece of paper, but having a paper with a QR code or a public key is not enough to relieve that sense of unease.

How can we resolve this problem? In my own mind, I toyed with the issue for more than a year. It puzzled me. I wondered if Mises' insight applied only in a predigital age. I followed the speculations online that the value of bitcoin would be zero but for the national currencies into which is converted. Perhaps the demand for bitcoin overcame the demands of Mises' scenario because of a desperate need for something other than the dollar.

As time passed — and I read the work of **Konrad Graf**, **Peter Surda**, and **Daniel Krawisz** — finally the resolution came. I will cut to the chase and reveal it: Bitcoin is both a payment system and a money. The payment system is the source of value, while the accounting unit merely expresses that value in terms of price. The unity of money and payment is its most unusual feature, and the one that most commentators have had trouble wrapping their heads around.

We are all used to thinking of currency as separate from payment systems. This thinking is a reflection of the technological limitations of history. There is the dollar and there are credit cards. There is the euro and there is PayPal. There is the yen and there are wire services. In each case, money transfer relies on third-party service providers. In order to use them, you need to establish what is called a "trust relationship"

with them, which is to say that the institution arranging the deal has to believe that you are going to pay.

This wedge between money and payment has always been with us, except for the case of physical proximity. If I give you a dollar for your pizza slice, there is no third party. But payment systems, third parties, and trust relationships become necessary once you leave geographic proximity. That's when companies like Visa and institutions like banks become indispensable. They are the application that makes the monetary software do what you want it to do.

The hitch is that the payment systems we have today are not available to just anyone. In fact, a vast majority of humanity does not have access to such tools, which is a major reason for poverty in the world. The financially disenfranchised are confined to only local trade and cannot extend their trading relationships with the world.

A major, if not a primary, purpose of developing Bitcoin was to solve this problem. The protocol set out to weave together the currency feature with a payment system. The two are utterly interlinked in the structure of the code itself. This connection is what makes bitcoin different from any existing national currency, and, really, any currency in history.

Let Nakamoto speak from the introductory abstract to his white paper. Observe how central the payment system is to the monetary system he created:

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate

the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

What's very striking about this paragraph is that there is *not even one mention of the currency unit itself*. There is only the mention of the problem of double-spending (which is to say, the problem of inflationary money creation). The innovation here, even according to the words of its inventor, is the payment network, not the coin. The coin or digital unit only expresses the value of the network. It is an accounting tool that absorbs and carries the value of the network through time and space.

This network is called the blockchain. It's a ledger that lives in the digital cloud, a distributed network, and it can be observed in operation by anyone at any time. It is carefully monitored by all users. It allows the transference of secure and non-repeatable bits of information from one person to any other person anywhere in the world, and these information bits are secured by a digital form of property title. This is what Nakamoto called "digital signatures." His invention of the cloud-based ledger allows property rights to be verified without having to depend on some third-party trust agency.

The blockchain solved what has come to be known as the **Byzantine generals' problem**. This is the problem of coordinating action over a large geographic range in the presence of potentially malicious actors. Because generals separated by space have to rely on messengers and this reliance takes time and trust, no general can be absolutely sure that the other general has received and confirmed the message, much less its accuracy.

Putting a ledger, to which everyone has access, on the Internet overcomes this problem. The ledger records the amounts, the times, and the public addresses of every transaction. The information is shared across the globe and always gets updated. The ledger guarantees the integrity of the system and allows the currency unit to become a digital form of property with a title.

Once you understand this, you can see that the value proposition of bitcoin is bound up with its attached payment network. Here is where you find the use value to which Mises refers. It is not embedded in the currency unit but rather in the brilliant and innovative payment system on which bitcoin lives. If it were possible for the blockchain to be somehow separated from bitcoin (and, really, this is not possible), the value of the currency would instantly fall to zero.

Proof of concept

Now, to further understand how Mises' theory fits with bitcoin, you have to understand one other point concerning the history of the cryptocurrency. On the day of its release (January 9, 2009), the value of bitcoin was exactly zero. And so it remained for 10 months after its release. All the while, transactions were taking place, but it had no posted value above zero for this entire time.

The first posted price of bitcoin appeared on October 5, 2009. On this exchange, $1 equaled 1,309.03 Bitcoin (which many considered overpriced at the time). In other words, the first valuation of bitcoin was little more than one-tenth of a penny. Yes, if you had bought $100 worth of bitcoin in those days, and not sold them in some panic, you would be a half-billionaire today.

So here is the question: What happened between January 9 and October 5, 2009, to cause bitcoin to obtain a market value? The answer is that traders, enthusiasts, entrepreneurs, and others were trying out the blockchain. They wanted to know if it worked. Did it transfer the units without double-spending? Did a system that depended on voluntary CPU power actually suffice to verify and confirm transactions? Do the rewarded bitcoins land in the right spot as payment for verification services? Most of all, did this new system actually work to do the seemingly impossible — that is, to move secure bits of title-based information through geographic space, not by using on some third party but rather peer-to-peer?

It took 10 months to build confidence. It took another 18 months before bitcoin reached parity with the U.S. dollar. This history is essential to understand, especially if you are relying on a theory of money's origins that speculates about the pre-history of money, as Mises' regression theorem does. Bitcoin was not always a money with value. It was once a pure accounting unit attached to a ledger. This ledger obtained what Mises called "use value." All conditions of the theorem are thereby satisfied.

Final accounting

To review, if anyone says that bitcoin is based on nothing but thin air, that it cannot be a money because it has no real history as a genuine commodity, and whether the person saying this is a novice or a highly trained economist, you need to bring up two central points. One, bitcoin is not a stand-alone currency but a unit of accounting attached to an innovative payment network. Two, this network and therefore bitcoin only obtained its market value through real-time testing in a market environment.

In other words, once you account for the razzle-dazzle technical features, bitcoin emerged exactly like every other currency, from salt to gold, did. People found the payment system useful, and the attached accounting was portable, divisible, fungible, durable, and scarce.

Money was born. *This money has all the best features of money from history but adds a weightless and spaceless payment network that enables the entire world to trade without having to rely on third parties.*

But notice something extremely important here. The blockchain is not only about money. It is about any information transfers that require security, confirmations, and total assurance of authenticity. This pertains to contracts and transactions of all sorts, all performed peer-to-peer. Think of a world without third parties, including the most dangerous third party ever conceived of by man: the State itself. Imagine that future and you begin to grasp the fullness of the implications of our future.

Mises would be amazed and surprised at bitcoin. But he might also feel a sense of pride that his monetary theory of more than 100 years ago has been confirmed and given new life in the 21st century.

What Cryptocurrency Can Teach Us About Political Governance

Skyler J. Collins

It's a marvel to me to witness what is happening on planet Earth as it regards **cryptocurrencies**. Satoshi Nakamoto, whoever or whatever he/she/zhe is, began a revolution as big as the wheel and the printing press and the Internet that came before it, or so it seems to me.

Over $93 billion, and counting, have poured into the cryptocurrency market since Bitcoin was **released in 2009**. Millions of individuals have come together without central direction to build this worldwide phenomenon.

Changes are happening every day that have global ramifications, all of which are happening without permission by governments, and often in spite of governments' supposed authority to control other people. That is truly *awesome*.

Decentralized Governance

There is governance, to be sure, as it regards cryptocurrencies, but such governance is without centralized structure. Cryptocurrency manipulation must follow specific rules, and changing those rules requires popular acceptance by users and stakeholders of each given cryptocurrency. Nobody can implement their preferred change arbitrarily. The only thing arbitrary about cryptocurrencies is one's desire to get involved in the hundreds of different systems, and once involved, they must follow the rules.

I think there's a model here for political governance, or in others words governance around the idea that people have rights, and those rights should be protected, with physical violence if necessary. While people mostly agree that behaviors such as murder, rape, robbery, assault, and battery are undesirable and we all should be protected

from them, there's a lot of disagreement on the smaller stuff, like who's entitled to what, provided by others that haven't themselves committed any of the foregoing behaviors (ie. crimes). That's not to say that people don't disagree on the big stuff, but the disagreement is more **a matter of definition than of undesirability**.

Who should decide which entitlements should be enforced? The current model says that for a given **arbitrarily-derived** geographical area, one entity should decide, even when a party to the dispute and that entity may be influenced in any number of ways. In other words, *one size fits all*, like it, leave it, or hope you get enough popular support to change it.

Spontaneous Order

Alternatively, using the cryptocurrency model, there would be no single entity per arbitrarily-derived geographical area to force one set of rules onto everyone else. Instead, individuals would pick and chose which rules they wish to engage with. When someone violates their rules, they have the option of dealing with it personally or calling on their rights protection agency to do so.

Everyone involved now has a strong financial incentive to remedy the dispute as peacefully as possible. How so? Because everyone involved is bearing the costs of resolution personally. There's no forcing those costs on to innocent third parties. Any attempt to do so will be met with the same type of response the original dispute was met with.

Of course, I can't predict how all of this will develop, spontaneously, just as I couldn't predict the effects of the wheel, the printing press, the Internet, and of the emergence and spread of cryptocurrencies. But I can say that I'd prefer governance based on this model over governance based on the old model. Seems far more effective, efficient, justified, and just plain 'ole *right*, to me.

In any event, to what extent the cryptocurrency phenomenon pushes against old models in the financial industry, and beyond, should be a welcome change for anyone tired of getting "landline government in a cell phone world," quoting Michael Malice. I don't think it can be stopped. I think that now that it's begun, it's here to stay.

FEE's mission is to inspire, educate, and connect future leaders with the economic, ethical, and legal principles of a free society.

Find us online at:

FEE.org

Facebook.com/FEEonline

Twitter.com/FEEonline (@feeonline)

The Foundation for Economic Education

1819 Peachtree Road NE, Suite 300

Atlanta, GA 30309

Telephone: (404) 554-9980

FEE

FEE.org