An Introduction to Bitcoin

Presentation for Cheyenne's Conservative Corner, April 11th 2021

A version of this can be accessed on the web at: https://github.com/crc32/Intro-Bitcoin

Or as a PDF: https://github.com/crc32/An-Intro-to-Bitcoin.pdf

What is Money

People often confuse currency (dollars, pounds, yen, etc.) with money. Money is actually an abstract concept, with a few attributes, that currency sometimes can satisfy. It is more accurate to say that money is a language that people use to represent, store, and transmit value.

For something to be money, it has to possess (or be able to possess) several attributes.

1. **Store of Value**: A money must be able to store value. As part of being able to store value, money functions as a way of transmitting value both through time (into the future) and space (across distances). Historically, gold has been a good store of value through time, but not all that great through space (it's heavy!). The US Dollar has been great at transmitting value through space, but not time (inflation!). Other things (art, collectibles, real estate, cattle, etc.) also function as stores of value. Usually, a money starts as a store of value.
2. **Medium of Exchange**: A money must be able to be accepted in exchange for other goods. Various things have functioned in this manner throughout history, to greater or lesser degrees.
3. **Unit of Account**: Finally, a money must be able to act as a general unit of account.

In addition to the minimum requirements above, there are several attributes that improve a good's utility as money.

1. **Divisibility**: It is important, but not absolutely necessary, for a money to be able to be divided into small units. Cattle was once a form of money, but it may be impractical to buy a sandwich with a steer.
2. **Recognizability**: One big problem with some forms of money is being sure that what you've received is actually the money! For instance, the difference between a 100% gold coin, and a 90% gold coin may not be easy to determine without special skill or equipment, but it makes a huge difference in the value!
3. **Fungibility**: Money is ideally fungible, where any unit of the money is indistinguishable from any other unit, and therefor has the exact same value as every other unit of the money. Real estate, for instance, does not have this property, since even identically sized lots may have significantly different properties (and hence values).
4. **Durability**: Grain was once used as a money, but it is not ideal, since over time it can rot. Cattle die. Ideal money will exist in its current form through time, and won't decay due to time. You will note that inflation causes the Dollar to fail at this!

What is Bitcoin

At the base, Bitcoin is a **permission-less** and **peer-to-peer** system for the instant and **irreversible** transfer of value between parties. It is based on a **distributed ledger** which represents and records the transfer, in a **trustless**, **secure**, and **censorship resistant** manner. The system depends on **consensus**, not authority, and is built through a durable **proof-of-work** system which prevents cheating.

- **Permission-less**: There is no mechanism by which a central authority allows (or can prohibit) two individuals from exchanging bitcoin. As long as the two parties have (probably independent) access to the bitcoin chain, and they both are in possession of their private keys, value can be sent from one to another.
- **Distributed Ledger**: The entire Bitcoin network exists as a distributed collection of individual nodes, each having a complete copy of the transaction ledger. Any transaction must be validated by the nodes and then secured in a **block** with other transactions by a **proof-of-work miner** before it can be included in the ledger. Once included in the ledger, every node will possess a copy of the transaction.

- **Peer-to-peer**: Every node in the Bitcoin network is considered equivalent to every other node, and no node has any privilege or status above any other node. A transaction may be sent to any node, and the network will transmit the transaction to all nodes for validation.
- **Irreversible**: Once a transaction has been finally committed to the ledger, it is impossible to reverse it without the consent of the recipient. In this sense it is more like handing someone a $1 bill, and not at all like a credit card transaction.
- **Trustless**: The parties to a transaction do not need to depend on a third party to prove that funds are available. Simply examining the ledger will prove to the recipient that the funds are available. Similarly, once the transaction is finally committed to the ledger, the recipient is assured that the transfer is valid (and is also now irreversible). There is no concern for fraudulent checks, stolen credit cards, or counterfeit bills.
- **Secure**: The Bitcoin network is impossible to attack with known computational methods. The entire network depends on complex cryptography which would be exponentially harder to break than trying to find a specific grain of sand on all the beaches everywhere.
- **Censorship resistant**: Due to its permission-less and peer-to-peer nature, Bitcoin is fundamentally resistant to all outside attempts to censor it. It is hard or impossible to block individual transactions, and it is similarly impossible to block general use of it, without going to extreme measures that have significant collateral damage, such as shutting down the entire Internet.
- **Consensus**: The Bitcoin network depends on a majority consensus of the nodes checking local copies of the distributed ledger, to ensure that every new transaction follows the clear and simple rules of the network. For instance, an individual cannot send value that they do not possess, and cannot send the same value to two others (double-spend). If an individual attempts such a double-spend, then the network will automatically adjust (achieve consensus), and only one of the transactions will be recognized.
- **Proof-of-work**: The Bitcoin network is rendered secure by requiring a tremendous amount of work (calculations) be expended to validate a block of transactions. The proof-of-work guarantees that each transaction and **block** has been subjected to the full validation of the Bitcoin network. Also, because each new block depends on all previous blocks, in order to modify even one transaction in the past, someone would have to do all the work from that block forward.

- **Block**: The Bitcoin ledger is called a *blockchain* since it is literally a chain of blocks. Every 10 minutes (on average), a set of transactions is organized into a block. The **proof-of-work miners** append the new block to the existing blocks and the new block becomes part of the **distributed ledger**.
- **Miner**: The miners are specialized computers that competitively work to solve a complex cryptographic problem (called a hash). The solution to the problem provides **proof-of-work**, demonstrating that the block was made through the competitive process, and that it was guaranteed to pass through the rigorous validation required for a valid block.

Hard vs. Easy Money

The fundamental difference between hard and easy money is right there in the name. Easy money is money that can be created 'easily', while hard money requires significant effort to create.

Gold is the quintessential hard money. Locating, mining, and refining it is a difficult process, requiring significant effort to create. This results in a limited amount of new supply, which helps guarantee that the existing *stock* will always exceed the amount that can be created (the *flow*).

By contrast, the US dollar (and other paper or debt-backed monies) represents some of the easiest money. Since it can be created costlessly on a whim (or *by fiat*, hence its other name - Fiat money), there is no limit on how much can be created, or how quickly new money can be created.

The speed at which new money can be created directly impacts the ability of a money to hold its purchasing power. As new money is created (such as through the various COVID stimulus packages), the purchasing power of the existing money decreases. This is how we get inflation. So basically **the harder a money is, the better it is at storing value through time**. Easy money always results in an eroding purchasing power over time.

Other Cryptocurrencies

When you start learning about Bitcoin, you will discover that there are many other cryptocurrencies. Be extremely careful here! Nothing else comes close to Bitcoin, even though there is usually much marketing hype about them.

Opinions on the other cryptocurrencies differ, but they are all significantly more risky than Bitcoin. In addition, none of them possess the hard money aspects of Bitcoin, and so are not likely to retain their value long term.

Before we go further here, keep in mind that there is only one true Bitcoin, and it is represented on exchanges (like a stock ticker) as either BTC or XBT.

Alt-coins (non-Bitcoin cryptocurrencies) like Etherium (ETH), Ripple (XRP), Cardano (ADA), & Tron (TRX), all attempt to provide other utilities than what Bitcoin does. The main problem with these is that every one sacrifices one or more of Bitcoin's fundamental core attributes in the name of efficiency or to build in needless complexity. Trading these can be very dangerous, and is beyond the scope of this document.

You will also discover that there are Bitcoin clones (also called forks) like Bitcoin Cash (BCH), Bitcoin Gold (BTG), and Bitcoin Satoshi Vision (BSV). **THESE ARE WIDELY REGARDED AS TOTAL SCAMS** and you should definitely avoid anything trying to pass itself off as Bitcoin.

If you want to go down this path, there is ample information on the Internet that can help, but you should definitely do your homework, because much of what has been discussed herein won't apply to the alt-coin market.

Common Objections

There's no intrinsic value to Bitcoin / "I can't touch it!" / It's backed by nothing

There are several different ways to look at this objection. The concept of intrinsic value basically means that an object or thing itself possesses a value that is part of its fundamental makeup.

1. On a practical level, *nothing* has intrinsic value. All value depends on what other people value it for. Value is entirely based on a combination of circumstances and what other people assign to it. How valuable would a gold brick be if you were stranded alone on an island with no drinkable water?
2. On a more philosophical level, Bitcoin does have intrinsic value. Its value is in the fact that the network generates a low-friction, high fidelity, extremely divisible 'token' that can be exchanged for anything else of value. Not even gold can claim to have these values.
3. Similarly, what is the intrinsic value of the United States Dollar? It hasn't been backed by gold since 1971, so it is entirely backed by "faith and credit". In one sense, that is exactly what Bitcoin is backed by, but instead of "faith and credit" in the Unites States Government, Bitcoin is backed by faith in mathematics.
4. On the "you can't touch it" front, while you can touch a paper dollar bill, that isn't actually what a dollar is. A dollar is a liability (debt) generated by a bank somewhere, and the vast majority of them are digital already. So while a dollar bill is a representation of a dollar, holding one is not actually holding a dollar. In that same sense, one could print out a wallet code that holds a bitcoin, and hold (and spend!) that piece of paper.

Bitcoin uses too much energy / Bitcoin will boil the Earth's oceans with it's CO2

While it is true that Bitcoin uses a tremendous amount of energy, this line of objection is extremely misleading. Bitcoin mining always seeks the lowest cost energy. Here in the US, the cheapest energy is what's known as stranded energy. Stranded energy includes things like flare gas and renewable curtailment (such as when a wind farm produces more than can be consumed). This is effectively free energy, since without pushing it through a Bitcoin miner, it would otherwise be totally lost.

Specifically for Wyoming, the use of Bitcoin miners to supplement the energy production infrastructure is very interesting. With all the wind, solar, hydro, and flare-gas resources present in Wyoming, energy producers can utilize Bitcoin mining as a supplemental income stream to tap into otherwise lost energy (such as flare-gas), or to level out the unreliable production of renewable energy.

Bitcoin is money for criminals/terrorists/drugs/money laundering

This is my personal favorite objection, in part because there is actually some truth to it, but it totally misses the point.

The fact that Bitcoin is based on a permission-less and censorship resistant system means that there is no way to stop anyone from using it for any purpose — even if that purpose is illegal. So that does mean that it can be used by criminal organizations. But it also means that it can be used by anyone *without the permission of the central authority*.

Consider the current administration in Washington. President Biden recently enacted several executive orders aimed at damaging the Second Amendment. What happens if the Biden administration tries to de-bank gun stores? In an environment like that, gun stores could add censorship resistant Bitcoin to their arsenal so that citizens who wish to exercise their Constitutional rights can still do so, in the face of a deeply hostile administration.

Similarly, Bitcoin has been extremely helpful in other countries where the central government is outwardly hostile to their citizens rights. In Venezuela, Hong Kong, Russia, Burma, and many other places, Bitcoin is seen as the best escape hatch from a tyrannical regime.

Bitcoin does not care what you use it for! So, yes, Bitcoin can be used for "criminal activity," but what happens if that "criminal activity" is something that really shouldn't be illegal to begin with?

Finally, it should be mentioned that this argument contains the assumption that governmental money *isn't* used for criminal activity. Of course this is absurd. In 2018, Danske Bank laundered about €200 billion in Russian money. And US banks have been reported to have knowingly laundered over $2 Trillion between 1999 and 2017, with almost $400 billion alone to Mexican drug cartels by Wachovia (now Wells Fargo).

The Government will ban it

This is both highly unlikely, and also not actually a problem for Bitcoin! First, it is highly unlikely that the United States will ban Bitcoin, since over the past year major financial institutions have taken huge positions in Bitcoin. With companies like Goldman Sachs, Fidelity, MassMutual, Microstrategy, and Tesla making hundred-million or billion dollar purchases of Bitcoin, the amount of political pressure from the financial world to keep Bitcoin legal will be tremendous.

Second, where national governments have tried to ban Bitcoin, that ban has backfired. Nigeria recently stated that Bitcoin was a danger to their local currency (the Naira), and moved to ban it. Since that ban, there has been a massive increase in person-to-person trading of Bitcoin, actually accelerating adoption of Bitcoin by regular Nigerians.

What the US Government *could* do is try to confiscate Bitcoin. This would likely look like what the Government did on April 3rd, 1933, under Executive Order 6102. With Order 6102, the Government attempted to confiscate all "gold coin, gold bullion, and gold

certificates within the continental United States." The net effect was that all gold held in banks and other institutions became the property of the Government, replaced with Federal Reserve Notes (ie: debt). This is why it is so important to actually take personal possession of your Bitcoin! The common refrain here is "not your keys, not your crypto!"

Bitcoin was designed from the beginning to be able to survive a ban. As open-source cryptography, the entire thing is basically speech. Also, it is designed to function even under extreme authoritarian conditions such as in China and Venezuela. About the only way to totally destroy Bitcoin would be to shut down all computers, everywhere, and in that scenario, humanity likely has bigger problems!

Sources, Extended Reading, and Tools

Getting Bitcoin

1. Strike, possibly the easiest and cheapest way to get bitcoin, and send to others. https://invite.strike.me/8JZ9XT (affiliate link)
2. Cash App, not the best or cheapest, but easy to use https://cash.app
3. River Financial, another low-fee place to buy Bitcoin https://river.com/signup?r=WBG4T5EB (affiliate link)

Holding Bitcoin

Software Wallets

1. BlueWallet, good basic wallet for iOS or Android. Can do both Lightning and On-Chain. https://bluewallet.io
2. Wallet of Satoshi, another good basic lightning wallet. https://www.walletofsatoshi.com/
3. Sparrow Wallet, one of the best desktop wallets. https://sparrowwallet.com/

Hardware Wallets

1. **NOTE: ALWAYS buy hardware wallets from the manufacturer! Otherwise you will not be sure it hasn't been tampered with!**

2. ColdCard, a great wallet, but harder to use, better for more advanced users. https://coinkite.com/ (As of 06/01/2023, this is the only one I can currently recommend)

Websites

1. Jameson Lopp's Bitcoin Resources https://www.lopp.net/bitcoin-information.html
2. Jameson Lopp's Lightning Network Resources https://www.lopp.net/lightning-information.html
3. The Why Bitcoin Only repository https://whybitcoinonly.com/

Books

1. The Bitcoin Standard, Saifedean Ammous: http://bit.ly/Bitcoin-Standard
2. Layered Money, Nik Bhatia: http://bit.ly/Layered-Money
3. Thank God for Bitcoin, Jimmy Song: http://bit.ly/Thank-God-for-Bitcoin
4. The 7th Property, Eric Yakes: https://bit.ly/7thProp
5. Bitcoin Clarity, Kiara Bickers: https://amzn.to/3aekZtG

Articles

1. The Bullish Case for Bitcoin, Vijay Boyapati: http://bit.ly/Vijay-Boyapati
2. Allen Farrington Series
    2.1 Wittgenstein's Money: http://bit.ly/Wittgensteins-Money
    2.2 Capital Strip Mine: http://bit.ly/Strip-Mine
    2.3 Bitcoin is Venice: http://bit.ly/Bitcoin-is-Venice

3. The Fraying of the US Global Currency Reserve System, Lyn Alden: http://bit.ly/LynAlden
4. Bitcoin is Time, Dergigi: http://bit.ly/dergigi
5. Parker Lewis Articles
    5.1 Gradually, Then Suddenly: http://bit.ly/Parker-Suddenly
    5.2 Bitcoin is Not Backed by Nothing: http://bit.ly/Parker-Backed
    5.3 Bitcoin Obsoletes All Other Money: http://bit.ly/Parker-Obsoletes
    5.4 Bitcoin is the Great Definancialization: http://bit.ly/Parker-Definancialization
6. Why Bitcoin, The Series, Tomer Strolight: https://bit.ly/Strolight
7. Masters and Slaves of Money, Robert Breedlove: https://bit.ly/MastersAndSlaves

Podcasts / Interviews

(Links are to the first episode if it's a series)

1. BTC005: Bitcoin & Michael Saylor (single interview): https://fountain.fm/episode/EzFb9JLOroSfEO8nYfCp
2. BitcoinTINA on Bitcoin (4+ part series): http://bit.ly/BitcoinTINA
    2.1 Bitcoin Audible (Guy Swann - Basically the best reader of Bitcoin Material): https://bitcoinaudible.com
    2.2 Guy's Take #49: https://fountain.fm/episode/wP7ILvwe2nAoQ6pVuFjG
    2.3 Fraying of the Petrodollar System Part 1, by Lyn Alden: https://fountain.fm/episode/uEoES7jIN5Dmcyk93HKj
    2.4 Fraying of the Petrodollar System Part 2, by Lyn Alden: https://fountain.fm/episode/5Zis86Vqj4RPHru6W1j7
    2.5 The Cantillion Effect 2.0, by CK_snarks & Deniz Saat: https://fountain.fm/episode/WvSsWNOuFXh1xElgNaWY

3. Bitcoin Audible - Bitcoin Basics Series: https://fountain.fm/episode/DCVP9EDYmpAaUTwTcU21
4. What is Money - The Saylor Series (17 part series): https://fountain.fm/episode/eumqR5JSyLx9ZPx9uoyv (This is a LONG one, over 26 hours of content, with tons of historical aspects, so not explicitly Bitcoin focused)

YouTube & Videos

1. BTC Sessions https://www.youtube.com/c/BTCSessions
    1.1 Getting Started: https://www.youtube.com/playlist?list=PLxdf8G0kzsUWe-rG0X6LDJAMXL7761B42
    1.2 Hardware Wallets: https://www.youtube.com/playlist?list=PLxdf8G0kzsUVkZ5*Jc6PyG*j4K8htg-i3
    1.3 Bitcoin Privacy: https://www.youtube.com/playlist?list=PLxdf8G0kzsUXZUbsVrUHYKSu3XAzV0lS3
    1.4 Mobile Wallets: https://www.youtube.com/playlist?list=PLxdf8G0kzsUUE7HHNTGTWBFxzt2oudiyS
2. BitcoinTV (this can be a bit of a grab-bag): https://bitcointv.com/

The Bitcoin Whitepaper

Satoshi Nakamoto's initial description of Bitcoin is the most important document in the history of Bitcoin — it is the document that started everything, after all! However, it is a highly technical piece, and is not the best place for most people to start. https://crc32.com/bitcoin.pdf