Bitcoin Overview (v 0.2)

With Bitcoin's recent rise in popularity, I have had trouble finding succinct explanations of what Bitcoin is and how it works intended for intellectually curious, but non-technical audiences. This essay is meant to help bridge that gap. By the end of this essay, you should be able to answer three questions at an advanced beginner level:

- Why is Bitcoin important and how could it change the world?
- How does Bitcoin's underlying technology work?
- How can an an enthusiastic layman get started buying, storing, and using Bitcoin today?

Note that this essay is meant to be a living document. If you enjoy reading it or have any feedback on how to improve it, please let me know at:
cypherperro [at] protonmail.com

Part I: Why Bitcoin Will Change the World

Today, the world's financial system is highly inefficient and highly centralized. Sending money from one part of the world to another is tediously slow and impossibly expensive for most people.[1] The idea of micropayments remains merely an idea because the transaction cost would exceed the actual payment. Governments and corporations retain the ability to seize or devalue (via inflation) financial assets at will. Despite these shortcomings, technological and political limitations have prevented society from developing a drastically better alternative system. Until now.

Enter Bitcoin, a decentralized ledger for the world. That's a fancy way of saying that it is a shared record of accounts that is simultaneously stored on thousands of computers around the globe. It has no formal leader, allows for completely borderless transactions, features a hard coded supply limit and rules that only can be changed if > 50% of the network chooses to accept them.

These claims seem exciting but abstract, so let's examine a few concrete example of how Bitcoin and other cryptocurrencies that it has inspired could soon change the world:

- 1) Incredibly fast and cheap international money transfers - imagine a coffee shop in San Francisco wiring $10,000 to a vendor in China for new equipment in under a few hours for a $1 or less.

[1] Remember the average income around the world is only ~ 1000 USD / year https://www.givingwhatwecan.org

- 2) Micropayments -- imagine paying fractions of a penny to read an article or watch a video without ads.
- 3) Real time, efficient payments for currently bundled services -- imagine paying for the energy you use by the second or being charged by your insurance company only for the minutes you're actually driving a car.
- 4) Smart contracts -- imagine being issued an Airbnb code that unlocks the door of your rental only after your payment has hit the owner's account.
- 5) Censorship resistant money -- imagine living under an authoritarian regime and being able to donate toward a political party that the current regime does not support.
- 6) An inflation free store of value -- imagine living in a country like modern day Venezuela where wheelbarrows worth of your local currency cannot purchase a loaf of bread and now having the ability to save enough value to buy food and medical care for your family.

I believe these last two use cases are the true "killer apps" for Bitcoin and related cryptocurrencies, especially for the billions of people around the world who are currently unbanked or living in countries where the government does not represent their voice. We'll delve much deeper into these use cases in later essays, but for now let's explore a simple yet transformative example that everyone can wrap their head around: borderless transactions between friends in different countries.

We'll illustrate this use case with two dachshund friends, Weenie and Tori. Weenie lives in Tennessee and Tori lives in Mexico City. Weenie wants to send $100 to Tori to buy some tasty crunchies to eat. Until recently, Weenie's only option was to send an international wire from his bank account to Tori's. International wires are typically expensive and slow, taking at least 2-3 business days to clear and costing at least $50 to send and $10 to receive. Say Weenie sends the transfer on a Saturday afternoon. Tori must wait until at least Tuesday to receive only $40 of the original $100 to buy his delicious crunchies (the other ~ $60 went to a bank in the middle). What's more, if Weenie's bank was at all suspicious of either party in the transaction, they could freeze all of his funds indefinitely.

With Bitcoin, Weenie now has the option to send $100 directly to Tori's personal Bitcoin account with no bankers or middlemen. The transaction takes less than an hour and costs on the order of magnitude of a dollar to send.[2] Say Weenie sends the funds at noon on Saturday. By 1pm that same day, Tori now has ~ $99 to spend on his crunchies (and with off-chain Bitcoin solutions like Lightning Network currently under development, the time and costs will soon fall to mere pennies and seconds respectively). Furthermore, no one can freeze these funds under any circumstance. In the words of US Vice President Joe Biden, "This is a big fucking deal!"

[2] Note that the cost of transactions fluctuates based on network demand. In late 2017, the cost of Bitcoin transactions surged to > $50 / transaction. While this is certainly very high, it's still a small cost relative to the amount you could send (100s of millions of dollars or more). And there are numerous solutions which already exist or are in the works to help keep this fee at a dollar or less today, including second layer networks like Lightning and alternative cryptocurrencies like Litecoin.

Part II: How Does Bitcoin Work?

The impacts of Bitcoin -- uncensorable, unlimited, borderless transfers of value -- are relatively easy to grasp. The underlying technologies, however, are a bit more complicated. The Bitcoin network uses multiple cryptographic technologies and well designed game theory to function. We'll start with an overview of how each is used in Weenie's $100 transaction to Tori.

Note: if you prefer to skip the technical overview and are ready to get started using Bitcoin, you may skip to section 3.

In order to use Bitcoin, Weenie and Tori must download software for their computers or smartphones called a wallet.[3] This wallet contains two critical numbers: a public key, which is used as an address for receiving funds, and a private key, which is used to authorize sending funds. In our example, Weenie chooses to send 0.01 btc (worth about $70 in April 2018) to Tori's public address[4]. In order for the transaction to be sent and recognized by the Bitcoin network, Weenie's wallet must sign the transaction with his private key, a sort of secret signature that Weenie has not shared with anyone and that is stored securely in his wallet.

The big breakthrough with this public/private key technology is that the pair results from what is known as a trapdoor or one-way function. In such a function, a private key is picked randomly from an unfathomably large set of numbers (~10^77 possibilities) and converted into a public key using a special one way algorithm. The function works such that if someone has your private key, they can easily find your public key. If they have only your public key, however, they can functionally never find your private key. Thus, it is said to function only one way.[5] This means that Tori can publish his public key for the world to send him money, but no one can use this information to derive the private key needed to send money away from his wallet.

Once Weenie's wallet has signed the transaction for 0.01 btc, the funds are sent to the Mempool (memory pool), which is sort of like a purgatory for proposed transactions waiting to be confirmed. The transaction is only considered valid if it is successfully confirmed and added to the Bitcoin blockchain. To understand this process of adding a transaction to the blockchain, we must first examine what is a blockchain.

The Bitcoin blockchain is an immutable ledger (essentially a giant accounting book) of every transaction that has ever happened on the Bitcoin network from the very first Bitcoin transaction until today. It is an identical file that stored and hosted by thousands of computers around the world updating continuously to reflect the addition of new transactions. This ledger is called a

---

[3] There are a variety of wallets on the market today, many of which are free and open source.
[4] The public key is actually the source of a public address and requires a few operations to derive. But for simplicity, we'll refer to his public key as his address.
[5] These key pairs are derived from a complicated trapdoor function called the Elliptic Curve Digital Signature Algorithm (ECDSA), based on branch of cryptography called Elliptic Curve Cryptographic (ECC). See here for more detail on how this works.

blockchain because it is literally a chain of blocks. Every block in the chain consists of a few key pieces of information, each of which is stored as a hash.[6]

Each block in the chain contains the following information (each stored as a hash):

- A timestamp of when the block was added to the chain
- A special random number called a nonce used in mining (more on this in a moment)
- A hash pointer which is just the hash of the previous block in the chain (i.e. a label of which block came before it)
- A hash identifier of this new block (i.e. a label for the next block to use as a pointer)
- A hash representing the hundreds of individual transactions to be added to the chain in the current block (known as Merkle tree)

Although this seems complex (and you should definitely dig deeper on each topic mentioned above), the core idea is that this blockchain full of hashes creates a decentralized, immutable ledger. If anyone tries to change ANY input in an old block (say for example the amount or recipient of even one single transaction), it will change the hash identifier of that block which will also change the hash pointer in the following block, which will in turn change that block's hash identifier, which will change the hash pointer in the next block, and so on until every subsequent block following the first change is also changed. Basically, any small change anywhere in the blockchain results in a completely different version of the blockchain, which the rest of the network would spot and reject.

Thus far we have explained how the use of cryptographic technologies allows Weenie and Tori to send and receive money that no one can tamper with and how the blockchain prevents anyone from changing the history of earlier transactions. But we still have one well-known challenge to overcome known as the double spend problem.

Weenie is an upstanding dachshund who would never try to cheat the system. But other potentially malicious actors like his notoriously misbehaved brother Bully would love to get away with sending a transaction to Tori and then trying to send that same bitcoin transaction to another merchant to get even more crunchies (effectively stealing by sending the same money twice).

How can we protect the network from such an unethical attack? Bitcoin uses game theory to solve this problem with an ingenious "proof of work" system known as mining. Recall that Weenie has sent his transaction to Tori's address, but that the transaction is currently sitting in the transaction limbo known as the mempool. In order for the transaction to be added to the

[6] A hash is simply the result of a as special function where you can feed inputs of any length and always receive a fixed length output. E.g. Bitcoin uses a hashing algorithm known as SHA256, which means anything you feed into the SHA256 algorithm (from the letter "a" to the entire contents of *Hamlet*) will always yield a unique 256 bit (64 character) output.

blockchain, the transaction must be added to a block as part of a Merkle tree during the mining process.

You can think of mining as similar to mining for gold. Only instead of mining with picks and axes, miners use extremely fast computers. And instead of searching for gold, they're searching for a solution to a puzzle that will yield a large Bitcoin reward if they find it. Miners can also earn money based on fees that transactors like Weenie attach to their transactions for priority inclusion in future blocks.

Said another way, miners are service providers paid in Bitcoin to secure the Bitcoin network. To get paid, miners must assemble a block of transactions in a merkle tree along with the other information mentioned above (a timestamp, a hash pointer pointing to the most recent block in the chain, etc.). Miners can choose to add whichever transactions they like to their proposed block (up to 1 MB worth of transactions, as specified by the current rules of the Bitcoin network)[7] and will typically choose transactions based on the size of the fee attached. Once they have their proposed block prepared, they create a hash of all of this information and begin playing the mining puzzle game. In this game, they append random numbers to the hash of their block and hash these two numbers together again and again until they find a solution to the network puzzle that produces a final hash starting with a specified number of zeros.

The Bitcoin network is designed to automatically adjust its difficulty to ensure a new block gets added every ~10 minutes. The network auto-adjusts puzzle difficulty (according to hard-coded rules) by requiring more or fewer zeros to successfully solve the puzzle and stay within the ~10 minute window for a adding a new block (e.g. a solution starting with 10 zeros is harder to find than one with 9 zeros is harder to find than one with 5 zeros, etc.). Once a miner finds a solution with the appropriate number of zeros, she publishes a solution to the network and so long as she followed the rules correctly, her new block will be appended to the existing blockchain and she will receive two rewards: 1) the fees appended to the transactions in her block (e.g. whatever fee Weenie chose to include to entice the miner in including his transaction in a block) and 2) a standard reward from the Bitcoin network that halves every ~4 years (the reward started as 50 btc in 2009 and is currently 12.5 btc as of 2018). This network reward is the only way that new bitcoin come into existence. The reward halves over time to introduce fewer and fewer bitcoin into circulation. Note that the system was designed to only ever create 21 million bitcoin to prevent future monetary inflation (we'll explore why this is important in future essays).

If the miner discovers that the transaction from Weenie has ever been used before in any previous block, she will NOT include the transaction in her block because the block will be rejected by the network which can identify where in the existing blockchain the transaction currently lives and the miner will earn nothing (this is true as long as at least 51% of the Bitcoin nodes are running a copy of the blockchain where this transaction has been spent before). Thus all of the electricity and time the miner spent trying to solve the puzzle will have been for naught

[7] This is ~500-2000 transactions / block depending on transaction size

because of one poorly chosen transaction in her block. This is the genius of the game theory of the Bitcoin -- miners secure the network by merely following their own self interest. Note that there are still ways that miners could try and collude to allow themselves to double spend (e.g. the 51% attack where one entity attempts to control 51% of all mining nodes on the network), but these attacks are incredibly costly and unlikely to occur. We may discuss these scenarios in more depth in future posts.

So returning to Weenie and Tori's transaction -- assuming that Weenie is not trying to double spend and has appended a reasonable miner fee[8] relative to what other network participants are offering, then his transaction should be added to a block relatively quickly. Once several blocks have been added on top of the block in which Weenie's transaction was included (say 6), then the transaction is said to be secure (this should take ~ 1 hour if Weenie's fee is competitive).[9]

One important thing to note is that unlike with traditional physical or digital money, Weenie's money that he sends to Tori is not actually stored in his wallet. His wallet only stores his public and private keys which give him access to specific pieces of the public blockchain. By signing a transaction he can give Tori ownership to one such piece of the blockchain. Here's how the transaction for 0.1 btc would actually look: Weenie's wallet software searches for pieces of the blockchain associated with Weenie's public key. Each of these portions of the ledger account for specific amounts of bitcoin (~.005 btc, 0.02 btc, .75 btc). Each of these discrete amounts is called an unspent transaction output (UTXO). Weenie's wallet identifies his 0.02 btc UTXO as the easiest to send to Toribio (different wallet software may have different criteria for choosing UTXOs).

Weenie's wallet then initiates a transaction requesting that 0.01 of this 0.02 btc go to Tori and signs the request with Weenie's private key. This proposed transaction includes a time stamp when the transaction was initiated, the input UTXO, and 3 output UTXOs -- the .01 UTXO that goes to to Tori, a small .001 UTXO paid to the miner as a fee to process the transaction, and a 0.009 UTXO that comes back to Weenie as change. Note that these three UTXOs should add up to the same amount as the input UTXO.

And that's it! Once Weenie's transaction is officially confirmed on the blockchain by the miners, Tori now has access to 0.1 btc which he can happily use to buy his crunchies!

---

[8] Bitcoin users can set whatever transaction fee they like. Typically, a user's wallet will either propose or select a target fee based on how urgently one wants her transaction confirmed.

[9] This transaction is said to be secure because of how the Bitcoin network recognizes what is the "true" Bitcoin blockchain. The real blockchain is that which A) meets criteria laid out by the software run by at least 51% of participating nodes on the network (those computers running full copies of the Bitcoin blockchain) and B) has the longest proof of work chain (i.e. the chain that has the most correctly added blocks). Thus, the more blocks on top of an existing block in the chain, the harder it is for a future chain to emerge with a longer proof of work history that does not contain that block.

Part III: How To Buy, Store, and Use Your First Bitcoin

Acquiring some bitcoin can be a great first step down the crypto rabbit hole. Once you have skin in the game, you'll want to learn much more about the underlying technology, societal implications, and maybe even start using crypto in your day to day life. That said, I must begin with a few words of caution:

1) This is not investment advice and I recommend that no one invest anything before doing their own deep dive and due diligence on any individual crypto asset. If you want to go deeper on Bitcoin's underlying technology, you can start with this comprehensive list of resources by developer Jameson Lopp.

2) Even after conducting due diligence, I still recommend that one only invest what she can easily afford to lose (e.g. this might represent 1-10% of your total net worth, depending on your risk tolerance).

Ok, so now that we have that out of the way, let's get started! You'll need two things: A) an online exchange to buy your bitcoin and B) a wallet to store your bitcoin.

How To Buy Your First Bitcoin

You can buy Bitcoin directly with fiat currency (dollars, pesos, etc.) from an online exchange. In the United States, I recommend Gemini. You'll need to submit some identification, but should be up and running within a few weeks, depending on signup traffic. I like this exchange for a few reasons: 1) you can instantly credit up to $500 a day with ACH transfers from your bank (this means you can buy quickly in case of a price dip instead of waiting for a wire transfer that takes at least 2 days) and 2) your cash deposits (note: NOT crypto assets) are FDIC insured like they would be in a normal bank.

If you'd like to buy in Mexican pesos, then I recommend using Bitso. Like Gemini, you need to submit identification to move large amounts of money. If you don't live in the U.S. or Mexico, email me your location and I can try to add some thoughts on exchanges in your locale.

Once you've bought your Bitcoin, I recommend moving it to a wallet asap. Leaving assets on an exchange creates unnecessary risk. All of the massive crypto heists you've heard about in the news (e.g. Mt. Gox) have happened with assets on an exchange, never in your own safely secured cold wallet. The first crypto rule of thumb: if you control your private keys, then the asset is yours. If someone else, like an exchange, controls your keys, then the asset is NOT yours.

I recommend Exodus as a good starter desktop wallet because of their intuitive interface, excellent customer support, and large volume of different crypto assets that they support. A desktop wallet is much more secure than leaving your money on an exchange or a strictly online / in-browser wallet. That said, as long as your computer is still connected to the Internet, even a wallet like Exodus is not completely safe. Clever hackers can infect your computer with Malware that records your keystrokes when entering your wallet. Therefore, once you start making a larger investment into crypto, I recommend moving your funds over to a hardware wallet like a Trezor or Nano Ledger S (both seem to be well funded and well respected within the crypto community). These wallets are an example of "cold" storage because they are designed to never touch the Internet. You can also make a paper wallet if you want a cheaper alternative for cold storage, although I'm personally a bit nervous about keeping my keys on just a piece of paper (note: this is merely an unfounded personal bias; many people do this successfully).

One very important note: for most people the greatest risk of losing your bitcoin is not getting robbed, but rather losing your password and recovery seed phrase for your wallet. Therefore regardless of what wallet you're using, I highly recommend that you take some time to write down your 12 or 24 word seed recovery phrase on a few sheets of paper or offline computers which you store in different physical locations. This seed recovery phrase is magic. Even if you lose your computer or hardware wallet, as long as you have this list of words, you can always download a new copy of your desktop wallet or buy a new hardware wallet and reboot your old funds. If you lose this phrase, however, you are -- as they say in France -- shit out of luck. This is one of the greatest lessons of crypto. With great power -- the ability to be your own bank -- comes great responsibility -- the responsibility of securing your assets and not losing your seed phrase. Note: in the future, it will become easier and easier to store your assets. But part of the adventure and excitement of being an early adopter means taking some of the early risk.

How To Use Your First Bitcoin

So, now that you've got a wallet and a little bit of bitcoin, what can you do? It obviously depends on why you acquired it. Some speculators want to trade it for a quick profit. Many long-term believers want to HODL.[10] Still others want to use it to acquire real goods and services like you would with a "normal" state-backed currency.

I'll cover a quick example of a real use case. Say you and your friends had a weekend retreat and you want to settle up bills. You owe your buddy $25 but want to pay him in Bitcoin. First, do a quick conversion to find that equivalent amount in BTC (you can use the exchange rate from your personal exchange or an aggregator like CoinMarketCap). Next, get a copy of your friend's friend's address. For example, my Bitcoin address is:

1752ATKUcGndbNqFAY1ttK6FCwj5eCGUhg

[10]HODL is a common meme on the Bitcoin Reddit sub. It's a misspelled acronym of "HOLD" frequently translated as on "Hold On for Dear Life." As in never sell your crypto no matter what happens.

Then go to your wallet of choice (say Exodus) and click on the Bitcoin tab (you may have many currencies featured here). NOTE: MAKE SURE YOU SELECT THE CURRENCY THAT MATCHES THE ADDRESS OF YOUR FRIEND AND CHECK THAT YOU COPY/PASTED HIS ADDRESS CORRECTLY. If you try to send Bitcoin to an Ethereum address, at best it won't work, at worst you've lost your money. Again, remember the mantra that with great power comes great responsibility. Always double check that you have the correct address before sending. Never type it, always copy/paste.

Once you've selected Bitcoin, you should see a button that says "send." Select "send" and paste your friend's address into the corresponding window. And that's it! You're ready to start using Bitcoin :)

It's important to note while I've written this guide for Bitcoin, there may be a better cryptocurrency for you to use depending on the use case. For example, as of April 2018, it is still cheaper and faster to use a currency like Ethereum or Litecoin for small transactions like in the $25 case above. This is changing, however, as Bitcoin is implementing a second layer called Lightning Network that promises to offer much faster and cheaper transactions on top of the Bitcoin blockchain. You may also wish to send your payment anonymously which cryptos like Monero allow (more to come on this in a future post!).

Thanks so much for reading! If you enjoyed this article or have feedback on how to improve it, please let me know. You can shoot me a note at **cypherperro [at] protonmail.com**