Alec May, Eder Mazariegos, Patrick Nash, Sean Pratt

Professor Arup Guha

CIS 3362

4 December 2017

**Cryptocurrencies: Bitcoin**

**History of Bitcoin**

On October 31st, 2008, a man by the name of Satoshi Nakamoto published a design paper that describes a purely peer to peer version of electronic cash that solves many issues that plagues previous digital currencies such as copying the currency, this system is referred to as bitcoin. In early 2009, Nakamoto publicly released the bitcoin software which launched the network as well as the first five units of the currency. Much like the early adopters of bitcoin, Nakamoto remains largely anonymous, and many believe the name to be a pseudonym used by other early adopters and developers of bitcoin. Many investigations have been made into uncovering the identity of Nakamoto but all possible candidates have denied the claims. Even though he developed the software and patents for bitcoin, Nakamoto ended all involvement in the currency in 2010, where he handed control over bitcoin to Gavin Andresen the former lead developer at the Bitcoin Foundation(Patron).

Bitcoin stores transactions in what is called a “block chain” which will be explained in greater detail later on, but at the start of this chain, as with the start of any data structure, there must be a starting point. This first block in the chain, called the genesis block, holds the rules for the rest of the blocks to follow, and for bitcoin itself. Nakamoto hard coded this block with certain static laws like a capped supply at 21 million bitcoins, mining difficulty, and rewards for mining being halved over time(Redman).

Many people don’t really understand what a bitcoin is exactly, and while details about mining them will be explained later, the basic idea and exchange system is not too complex. Bitcoins can be purchased or “mined,” but don’t need to be purchased in whole number units as the name might suggest. With the price of bitcoin increasing almost exponentially, bitcoins are divided into subunits of one hundredth and one hundred millionth of a bitcoin. They are transmitted peer to peer, which means there are no middle men like banks or governments slowing things down and adding fees, simply one user authorizing a transaction to another user using a bitcoin addresses that each user can decide to make public or not. Bitcoin addresses function in a similar manner to email addresses but each address should only be used for a single transaction, and users should create more upon further transactions. As mentioned earlier, all transactions are stored in a block chain, which acts as a shared public ledger, which is the backbone of the bitcoin network. The block chain stores transactions in chronological order and is used to verify transfer of funds to fight against the ailments of an entirely digital and internet based currency(Nakamoto).

In early 2010, bitcoin was already getting recognition on the world stage and being used in many online transactions. By now an exchange rate had been established at 1 USD = 1,309 BTC, but increasing press on bitcoin had attracted more users. This press drove the value of bitcoin up 10 times its previous amount to where one bitcoin then was placed at 1 bitcoin to roughly 8 cents USD. Even though a single bitcoin was still not worth very much, many users and companies alike saw great promise in the network and were eager to get involved.

At this point not many online vendors accepted bitcoins as a form of payment so many people attributed the success of bitcoin to an online black-market site called “The Silk Road.” The Silk Road was the first modern darknet market and is best known as a platform for selling illegal items and services, as it was operated through the Tor browser’s IP hiding service. Since many of the transactions on the Silk Road would need to be as private as possible, clients used bitcoin which can only be traced back to a bitcoin wallet address which can be kept separate from all other forms of identity.

Although bitcoin was regrettably adopted by less than legal services like the Silk Road, it was still seeing an explosion of use by everyday upstanding users who simply wished for simpler self-controlled form of currency. One such user by the name of Jed McCaleb, saw how popular bitcoin was becoming, and decided the bitcoin community needed an exchange for trading bitcoin and regular currency. He created a site called Mt.Gox in 2010 where users could do exactly that. Gox worked like any other exchange system where buy and sell orders were placed by users to exchange bitcoins for fiat currency and vice versa. For years Gox grew in popularity to a point where it was the largest company to handle bitcoin exchanges, being responsible for 70% of all bitcoin transactions in the world. Mt.Gox was so pivotal in the price of bitcoin, that when it shut down payment processing for a day for a market cooldown, the value of a single bitcoin dropped 23%, but soon recovered to its earlier standing a few short hours earlier when the site came back online.

Although Gox was the most popular bitcoin processing site, it was not without its troubles, seeing as how bitcoin and its exchange system were still emerging technologies. From 2010 to early 2013, Gox had a few hiccups in its bitcoin processing from things like identities being spoofed to transactions and their respective funds being lost, but towards the end of 2013, Gox’s problems would come to a head and spell the end times for the company. In June 2013, the bank that handled Gox’s USD exchanges pressured Gox to close its account with them as the US had recently begun cracking down on Gox for acting as an “unregistered money transmitter” in the US. Due to this, Gox had to halt all USD withdrawals for a few weeks but even after withdrawals had resumed, users were not receiving their money in a timely fashion, as some were left waiting for months for their money(Hern).

In February 2014 Gox halted all bitcoin withdrawals claiming it needed to “obtain a clear technical view of the currency processes.(MtGoxTeam)” A few days later Gox announced they had discovered a bug in their bitcoin software that makes it seem like the funds for a transaction were never sent when they in fact were. This essentially created a situation where an attacker could ask Mt.Gox to transfer them bitcoins, capture that transaction and modify it to make it seem like Mt.Gox never transmitted them, when in fact they did. Mere days later, bitcoins prices plummeted 36% as the likelihood of Mt.Gox paying its users became less and less apparent. Only 3 weeks after Gox paused exchanges to assess what was going wrong, its website went offline, the CEO faced multiple lawsuits, and an internal document leaked claiming Gox had been subject to a year’s long hack that had robbed them of 750,000 of its customers bitcoins and 100,000 of its own, totaling 7% of all bitcoins in circulation, worth around 473 million at the time(Stucky).

Despite the leaks and what the CEO of Mt.Gox, Mark Karpeles, said many were not convinced there was hack on their accounts. The possibility of there being a bug that allowed attackers to steal coins from Mt.Gox exists, and most likely did happen but many users claim that it couldn’t have happened often enough and in large enough quantities to rob them of hundreds of thousands of coins. One of the leading theories is that Karpeles or someone at Mt.Gox had something to do with the disappearance of the coins, or that the coins never existed at all, and Gox had always been operated incompetently and never had the funds to back up their transactions. The hack is still being investigated to this day, and even though many are doubtful, the recent information and court cases do point to some sort of hack, though the details are still unknown. In a recent case against Karpeles, he outlined a system that was in place that would inflate a bot’s account with USD and send buy orders for bitcoin. The bot would purchase the coins with the fake currency, and then the coins would be wiped from the bot’s account. This would increase Mt.Gox’s liability in USD but reduce its liability in BTC, and since they banked on the price of bitcoin going up they hoped exchanging debt in BTC for debt in USD would eventually push them out of debt since the bitcoins could be sold for more money than when they were purchased. Somehow Karpeles claims this isn't illegal but it sure sounds like it(Nilsson).

Although not all of bitcoin’s history has been positive, bitcoin has continuously proven that is a legitimate currency and is here to stay. With prices rising as they have been lately, despite the very recent dip and then subsequent recovery, the best time to invest is now, but if the past teaches anything, it’s to be wary of middlemen who may control your bitcoins instead of you, which is against the fundamental value of a peer to peer cryptocurrency currency such as this.

**Bitcoin Mining**

New Bitcoins are introduced to the system through a process known as mining. Mining is the process of adding records of Bitcoin transactions to the Bitcoin public ledger of previous transactions. This public ledger is referred to as the block chain because it functions as a chain of blocks. New blocks are added to the chain when a miner manages to find a hash of all of a block’s information that is either equal to or less than a specified target which every Bitcoin client shares. In exchange for successfully discovering this new block, the miner is rewarded with a certain amount of Bitcoins. In order to ensure that miners are unable to swiftly flood the market with newly generated Bitcoins, the reward for discovering a new block is reduced by 50 percent for every 210,000 blocks discovered. Originally the reward for each block discovered was 50 Bitcoins, now the reward has been reduced to around 12.5 (Coindesk).

Each transaction within the block chain is collected by the blocks. Every block contains a timestamp, a hash of the previous block in the chain, a reduced representation of all of the transactions that have been confirmed with the block, the target that corresponds to the difficulty of finding a new block, an arbitrarily picked number to add entropy to the block’s header, and a hash of all of the previously listed items within the block. All of these details contained within the block are used to ensure the veracity of all of the transactions recorded by the block. If any part of the information within the block were altered in anyway, it was drastically change the block’s resulting hash and therefore be made apparent that an alteration was made; only leaving room for accurate hashes (Mining).

Since one of the core purposes of Bitcoins is that it is decentralized, each user of Bitcoins has their own copy of the block chain. Whenever a user records a transaction made, that transaction is then broadcasted to all other users in order to update their own block chain. The goal of miners is to listen to these broadcasts while searching for a new block. Once the block is found, the miner then broadcasts that new block to all other Bitcoin users and it is added to their own block chain. Often more than one viable new block is found for the chain so in order to ensure every user’s copy of the block chain is the same the block chain will only add the set of block which has the greatest length.

Bitcoin mining is designed to be a highly difficult and resource-intensive process to do in order to maintain a steady amount of blocks being discovered. As mentioned above, the hash of a block’s header found by a miner must correspond with a specified target. This target is a particular format in which the hash must be in line with; specifically this format is a set amount of zeros that the hash must start with. There is a very low probability of generating a hash that begins with many zeros therefore a vast amount of attempts must be made. The difficulty involved in discovering a new block is calculated based on the specified target in place. Every 2016 blocks this difficulty is recalculated such that the previous 2016 blocks would have been generated in exactly two weeks if every user had been mining at this new difficult, and the target is adjusted accordingly. On average this adjustment of difficulty guarantees a new block will be discovered every ten minutes (Coindesk).

Bitcoin users have utilized many different types of hardware in order to mine new blocks. In very early versions of the Bitcoin client users were readily able to use their CPUs to mine. However as the Bitcoin network expanded and more and more users began switching to GPU mining, CPU mining began to produce less income in Bitcoins then it consumed in cost of power; making CPU mining outdated and inefficient. Then there is GPU mining; GPU mining is immensely faster and far more efficient than that of CPU mining. This is because GPUs are on average capable of executing many more instructions per clock tick than the average CPU. The popularity of GPU mining has given rise to users engineering contraptions such as mining rigs. Mining rigs are computer systems that are designed either entirely or at least partially for mining Bitcoins. These rigs tend be equipped multiple GPUs in order to maximize the amount of mining that can be done at once. Unfortunately, the difficulty in mining Bitcoin has risen so drastically at this point that even in a scenario where electricity is free it is unlikely that most GPU mining rigs will be able to generate enough income to pay for themselves. Currently perhaps the most popular and potentially most lucrative method of Bitcoin mining is through the use of an application-specific integrated circuit, or ASIC. An ASIC is a microchip which has been manufactured for a very particular purpose. A Bitcoin ASIC is designed in a way that, in most cases, it can be used exclusively for the mining of Bitcoin and nothing else. As a result of the specificity of a Bitcoin ASIC, it is capable of mining Bitcoins at rate that is exponentially faster and more efficient than any hardware utilized before it. It is because of ASIC mining that GPU mining is no longer viable (Mining).

Today Bitcoin mining has developed into a proper career for some individuals with the creation of entire Bitcoin mining factories. These factories consist of thousands of computers manufactured for the sole purpose of mining Bitcoins. Many have managed to amass substantial personal fortunes through Bitcoin mining alone, further expanding the Bitcoin market (Coindesk).

**Investing in Bitcoin**

Investing in Bitcoin or any cryptocurrency for that matter, may be just as, if not more lucrative than investing in your average stock. Investing in Bitcoin can be simple, easy to do, but very hard to comprehend. Bitcoin varies immensely in price range on a day to day basis and changes patterns in split seconds. One could say that this statement remains true for any given stock within the stock market, however Bitcoin is no stock and is very much a currency of its own. Bitcoin is a risky investment, but provides a fair return for both short-term and long-term growth with very little capital necessary.

These days, you can buy a stock for as little as a penny and as much as $279,000, but you cannot buy ¼ of a $100,000 stock on the stock exchange market if you do not have enough money to put into buying a full share. This is exactly why investing in currency is so popular, because you can by pieces of that currency and hold onto it as its value rises. The only problems with this is you are essentially investing in something that isn’t based on one or any proprietary object, concept, or matter and instead are putting money into something that will bring you very little return due to the lack of fluctuation and government regulation. Cryptocurrency, however allows the investor to bypass this by providing a decentralized network to which you may trade, deposit, and withdraw freely without government intervention and plenty of price fluctuation.

Cryptocurrency can be bought in pieces and sold in pieces. For example, if you were to buy an entire Bitcoin today, it would cost you $11,200 (At the time of this writing), but if you only plan to invest $1,000, you can and will be given 0.08% of that share of Bitcoin. With this investment, you may then expect interest to accrue on you money put in and with that interest, you can use Bitcoin as money to purchase everyday items. This is an important factor of Bitcoin because it has been the underlying factor for the price increasing, and cuts out many middle-men stockbrokers who tend to cheat clients out of the money they invest by charging fees and only giving certain percentages of the money earned.

Do not be confused however, investing in cryptocurrencies like Bitcoin may be very risky and are this way due to drastic fluctuations, that being said, they can also be very profitable. When a cryptocurrency price fluctuates, it can go either up or down, and just like in stocks an investor either chooses to sell or buy whenever he or she deems necessary. A common occurrence of a Bitcoin price going up is after a recent development, such as a Bitcoin debit card being released or funding for a poverty stricken country by replacing its currency with Bitcoin being announced, or a big named company stating they are investing in Bitcoin. When Bitcoin raises in value, there are many factors in play, but there is always a reason as to why it rises, you just have to do your research.

Anyone can be a part of Bitcoin and buy or sell it freely as they wish. When you own a piece of Bitcoin, you are essentially an owner of that share within the market. Therefore, you are trading and making either a profit or a loss in value every second of the day and as Bitcoin value rises, that fluctuation stands to become more and more stable, meaning people can use Bitcoin freely without having to worry about any loss in value and it may be used as intended, a decentralized currency for the masses.

**Bitcoin today and the future of the Bitcoin**

Bitcoin today is doing better than ever, as their value continues to soar. As bitcoin has gained immense popularity in 2017, many alternate cryptocurrencies, also known as altcoins, have been created to try to compete with the success of the bitcoin(. These altcoins start by making an Initial Coin Offering, or ICO. In basic terms, this is when a startup company shows possible investors their plan to create their cryptocurrency, and people who investor are given some of the first coins of this currency, similar to buying shares (Initial). ICO’s avoid the traditional legal restrictions on how to raise capital, and because of this, ICO’s began to appear all over. China was one of the first countries to take action against this legal avoidance, by banning Chinese investors from participating in ICO’s. This action had a large impact on the market, sending the value of the bitcoin and many other cryptocurrencies down quite a bit, since they were often the currencies used to buy tokens from ICO’s. While many countries are scrambling to place regulations to fight against these transactions, China’s has had one of the biggest impacts thus far. The value of the Bitcoin is still climbing, however, and has been on a rapid incline since late 2016. At the end of 2016, the value of a bitcoin was just under $1000, and when we started writing this paper, it’s value was hovering around $7000. Bitcoin’s value has been fluctuating greatly as of late, and since we began this paper, the value of the bitcoin went from $6500 to almost $12000! However, it certainly was not a straight shot. A few months ago, the bitcoin community was considering switching to a network that supports larger blocks, which would make it faster and more efficient. While this idea was being debated, many people switched to an altcoin called “Bitcoin Cash”, which supports these larger blocks. A few weeks ago, the decision was finally made that Bitcoin wouldn’t make those changes, and the value fell significantly for a brief time (Titcomb). The value of the bitcoin shows promise for even more growth, but there is some concern that foreign restrictions will stunt its growth. Overall, the bitcoin is a promising but risky investment.

The future of a bitcoin is a bit of a question mark still. While they do currently still have the largest market share of any cryptocurrency, there are so many other altcoins waiting to take the throne away from them as soon as they slip up. Bitcoin's largest advantage still remains that it is anonymous, and that transactions can occur with nearly no record. As long as the bitcoin can maintain its control of its market share, it will remain the most widely accepted cryptocurrency in the world, and will succeed. Security breaches and regulation also remain as large threats to the success of the bitcoin, as we try to improve the online transaction system, we introduce the possibility for new security breaches. The future of mining is moving away from the more traditional methods such as CPU and GPU mining as cloud mining and mining hardware take off. With cloud mining, people can buy hardware in a warehouse to mine bitcoins, and get a share of the profits. This allows a consumer to mine coins without paying for the overhead costs such as heating and hardware wear (Bitcoin.com). Mining specific hardware is also becoming popular, which is just circuit boards specifically made to mine. They are by far the fastest way to mine currently, and have blown away CPU and GPU mining. Many people worry that the Bitcoin is a fad that will die out, or that it will be similar to gold was many years ago, but as long as Bitcoin is widely accepted and remains easy to use for transactions, it will likely stay as a relevant cryptocurrency.

Works Cited

“Bitcoin.com's Cloud Mining Begins, Now Anyone Can Mine Bitcoin.” *Bitcoin News*, Bitcoin.com, 17 May 2017, news.bitcoin.com/bitcoin-coms-cloud-mining-allowing-anyone-mine-bitcoin/.

Coindesk. “How Bitcoin Mining Works.” *CoinDesk*, 22 Dec. 2014, [www.coindesk.com/information/how-bitcoin-mining-works/](http://www.coindesk.com/information/how-bitcoin-mining-works/).

Hern, Alex. “How a bug in bitcoin led to MtGox's collapse.” *The Guardian*, Guardian News and Media, 27 Feb. 2014, [www.theguardian.com/technology/2014/feb/27/how-does-a-bug-in-bitcoin-lead-to-mtgoxs-collapse](http://www.theguardian.com/technology/2014/feb/27/how-does-a-bug-in-bitcoin-lead-to-mtgoxs-collapse).

“Initial Coin Offering (ICO).” *Investopedia*, 5 Sept. 2017, [www.investopedia.com/terms/i/initial-coin-offering-ico.asp](http://www.investopedia.com/terms/i/initial-coin-offering-ico.asp).

Kotevski, Peter. “Basics For Buying And Investing In Bitcoin” *Investopedia*, 24 Aug. 2014, <https://www.investopedia.com/articles/investing/082914/basics-buying-and-investing-bitcoin.asp>

Langager, Chad. “Start Investing With Only $1,000” *Nasdaq*, 4 Dec. 2017, http://www.nasdaq.com/investing/start-investing-1000.stm

Lielacher, Alex. “Bitcoins as an Investment: Oppurtunities and Risks” *Nasdaq*, 31 Jan. 2017, <http://www.nasdaq.com/article/bitcoin-as-an-investment-opportunities-and-risks-cm740800>

“Mining.” *Mining - Bitcoin Wiki*, 22 Oct. 2014, en.bitcoin.it/wiki/Mining.

MtGoxTeam. “MtGox.” *Wayback Machine*, 2014, [web.archive.org/web/20140210122955/https://www.mtgox.com/press\_release\_20140210.html](http://web.archive.org/web/20140210122955/https://www.mtgox.com/press_release_20140210.html).

Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System.” 31 Oct. 2008.

Nilsson, Kim. “Breaking open the MtGox case, part 1.” *WizSec*, 27 July 2017, blog.wizsec.jp/2017/07/breaking-open-mtgox-1.html.

Nilsson, Kim. “Comments on the Mark Karpeles Trial.” *WizSec*, 12 July 2017, blog.wizsec.jp/2017/07/comments-on-mark-karpeles-trial.html.

Patron, Travis. “Who Is Satoshi Nakamoto?” *Diginomics*, 14 Oct. 2017, [www.diginomics.com/2014/11/09/who-is-satoshi-nakamoto/](http://www.diginomics.com/2014/11/09/who-is-satoshi-nakamoto/).

Redman, Jamie. “Bitcoin's Quirky Genesis Block Turns Eight Years Old Today.” *Bitcoin News*, 3 Jan. 2017, news.bitcoin.com/bitcoins-quirky-genesis-block-turns-eight-years-old-today/.

Roberts, Jeff John. “China's Crackdown on Digital Currency: What It Means for Bitcoin.” *Fortune*, 5 Sept. 2017, fortune.com/2017/09/05/china-bitcoin-ban-icos/.

Stucky, Jake Adelstein Nathalie-Kyoko. “Behind the Biggest Bitcoin Heist in History: Inside the Implosion of Mt. Gox.” *The Daily Beast*, The Daily Beast Company, 19 May 2016, [www.thedailybeast.com/behind-the-biggest-bitcoin-heist-in-history-inside-the-implosion-of-mt-gox](http://www.thedailybeast.com/behind-the-biggest-bitcoin-heist-in-history-inside-the-implosion-of-mt-gox).

Titcomb, James. “Bitcoin price drops 29pc in four days.” *The Telegraph*, Telegraph Media Group, 13 Nov. 2017, www.telegraph.co.uk/technology/2017/11/13/bitcoin-price-drops-29pc-four-days/