UNION COLLEGE

Currency 3.0: Examining Digital Crypto Currency Markets

by

Jesse E. Grushack

A thesis submitted in partial fulfillment for an interdepartmental degree

in the

Department of Computer Science and Economics

Advisors: Chris Fernandes & Brad Lewis

June 2014

Where I am going is a world where all interaction with our fellow man is entirely voluntary, where you no longer need to rely on government to settle disputes. In fact, decentralized technologies will make governments entirely irrelevant, ineffective at being able to do anything.

Because we now have the ability to communicate with everyone in the world and the ability to reach a global consensus about who owns what and how they settle disputes and how to do co-ordinated decentralized justice without having to rely on taxation or force . . . Its going to be an amazing new world. .”

Dan Larimer, BitShares

UNION COLLEGE

Abstract

Advisors: Chris Fernandes & Brad Lewis
Department of Computer Science and Economics

by Jesse E. Grushack

With the overabundance of data in the twenty-first century, money is still a primitive yet tangible item that can be physically passed from person to person. Money was originally backed by gold, a commodity, but is currently backed by the government. But what if money could be backed by mathematics? The purpose of this project is to explore what may be considered the future of money, a virtual payment protocol known as cryptocurrencies. Bitcoin was the first crypto-coin system and currency which has increased in value by over 500% in the past year. But why should people trust a system when everything else on the internet has the ability to be manipulated? This project explores the security of this network and what makes it unbreakable. The project also examines the economic possibilities of having a global distributed trust network. These new technologies will not only play a major part in shaping our future but have potential to change society as we currently know it.

Acknowledgements

I would like to thank; my advisors, Chris Fernandes and Brad Lewis for joining me on this journey and dealing with all my nonsense. My parents for paying my tuition so I can study incredibly advanced topics like this one. Stephen Wendolowski for always listening to my deep conversations late at night. Nick Goodrich for being one of the few people I can speak to who actually knows what I am talking about. And Union College for whatever that's worth.

Contents

List of Figures

List of Tables

Chapter 1

Introduction: What Are Crypto Coins?

1.1 What is Money?

Everything around you is based in math. The walls that hold up a house rely on physics, the computer that this paper was written on is based in math, everything that surrounds us is based in math. Except for one major aspect of our lives, money. Forms of currency have come and gone throughout history; whether bartering cigarettes and alcohol is acceptable or trading one piece of paper with $20 written on it for a specific good is acceptable. Currency has evolved and continues to do so as the world does too. Today, a green piece of paper with $20 written on it is acceptable. Why? Why is a piece of paper, that has words and numbers on it acceptable? These pieces of paper were once backed by gold, however that is not the case anymore. It is imperative to understand why the money supply is growing and why people accept it. Understanding the history of currency is necessary in answering the aforementioned questions and imperitive in order to understand where currency is going.

1.1.1 Currency 1.0: The Gold Standard

The United States created a formal currency standard in 1785. This was known as the Silver Standard, however it did not last long with the impending gold rush

and excess gold reserves out West. In 1792, a bi-metallic standard was created and set as the standard form of currency in the US. Under Alexander Hamilton, the Coinage Act of April 2, 1792, defined the basic monetary unit of the United States as the dollar and defined subsidiary coinage on a decimal basis
Fifty years later, the Federal government lost power over the banking system with the Treasury Act in 1848. The Gold Standard created a nominal anchor because people believed that using the commodity of gold as a purchasing power was credit worthy. People could exchange gold for paper bills and vice versa; these bills represented a legitimate piece of gold, and thus people had faith in this system.

1.1.2 Currency 2.0: Fiat Money

The Gold Standard became a nominal anchor globally due to actions made by the United States. The Gold Reserve Act of 1934 changed the price of a troy ounce of gold from $20.67 to $35. This change represents the fact that our money is not based in math but in the hands of a few. The Bretton Woods System was set up in 1944 to create a fixed exchange rate in the world. This was beneficial for the US: Because the United States emerged from World War II as the worlds largest economic power, with over half of the worlds manufacturing capacity and the greater part of the worlds gold, the Bretton Woods System of fixed exchange rates was based on the convertibility of US dollars into gold at $35 per ounceThus an important feature of the Bretton Woods System was the establishment of the US as the reserve currency country The Bretton Woods System helped the US to prosper economically as a world power and gave our government significant control over the general global value since most currencies became linked to the US dollar. This shifted in 1971 when President Nixon ended the convertability of dollar bills to gold but gold was not fully removed from the equation until 1977. With the end of the Gold Standard, the U.S. Dollar had become a fully fiat currency. The influence in price was now in the hands of the Treasury. Thus the dollar had evolved from its first version to the next.

1.1.3 Currency 3.0: Crypto Currencies

Money is based on trust, because if anyone could print money it would be worthless. To protect money, governments use different anti-counterfeiting measures

during printing that are incredibly hard to replicate, but not impossible. But how do you protect something that doesn't physically exist?
For centuries people have been encrypting messages and encryption has become somewhat sacred in the digital age. Using cryptography is a way of creating a secure communication channel by using a mathematical formula, usually for the transfer of a message from person to another. This process makes sure that the person sending you a message, is actually who they say they are. Combine the impossible to counterfeit nature of cryptography with money and you get a currency based in math called a cryptocurrency.
These cryptocurrencies are decentralized, electronic systems, which use peer-to-peer networking along with digital signatures to create money. While this may not seem possible, all that is needed is the network, an impossible to counterfeit public system that has peoples trust.

While Bitcoin is not the only digital crypto currency, it is the starting point for learning about cryptocoins. The next sections will attempt to give the reader a better understanding of Bitcoin so that we can truly explore cryptocoins.

1.2 What is Bitcoin?

On November 1st, 2008, a mysterious research paper appeared on a cryptography listserv, a place where fellow cryptotography enthusasits interacted. The man behind the paper was just as mysterious as the paper itself. The man was Satoshi Nakamoto who claimed to be from Japan had an email address from Germany. The proposed system was for an online currency called Bitcoin. The secret to its success would be the creation of a block chain where all users of the currency would each maintain the chain collectively. In the process, users could mine for Bitcoins and Nakamoto mined the first 50 Bitcoins in what is known as the Genesis block on January 3rd, 2009.

Nakamoto revealed little about himself, limiting his online utterances to technical discussion of his source code. On December 5, 2010, after Bitcoiners started to call for Wiki leaks to accept Bitcoin donations, the normally terse and all-business Nakamoto weighed in with uncharacteristic vehemence. No, dont bring it on, he wrote in a post to the Bitcoin forum. The project needs to grow gradually so the software can be strengthened along the way. I make this appeal to Wiki leaks not

to try to use Bitcoin. Bitcoin is a small beta community in its infancy. You would not stand to get more than pocket change, and the heat you would bring would likely destroy us at this stage.

Then, as unexpectedly as he had appeared, Nakamoto vanished. At 6:22 pm GMT on December 12, seven days after his Wiki leaks plea, Nakamoto posted his final message to the Bitcoin forum, concerning some minutiae in the latest version of the software. His email responses became more erratic, then stopped altogether. Gavin Andresen, who had taken over the role of lead developer, was now apparently one of just a few people with whom he was still communicating. On April 26, Andresen told fellow coders: 'Satoshi did suggest this morning that I (we) should try to de-emphasize the whole mysterious founder thing when talking publicly about Bitcoin

Nakamoto stopped replying even to Andresens emails. Bitcoiners wondered plaintively why he had left them. But by then his creation had taken on a life of its own.

1.2.1 Bitcoin Mining

Bitcoins are discovered using computing power in a process called mining. Computers process an encryption algorithm, specifically the SHA-256 hash. A hash function is simply a mathematical formula used to map data. This algorithm was developed by the NSA and has never been cracked. Bitcoins are stored in blocks and every block contains a hash number. To find the next block, you must find a block header that is lower than or equal to the target, which is a hash of the previous block. If the hash number found is not lower than or equal to the previous hash, the algorithm adds nonce or a string of numbers starting at 0 and incrementing from there. The computer keeps looping this until it discovers a hash value that is mathematically related and lower than or equal to the previous hash, when the number is found, the person or miner, processing the algorithm is rewarded with a new block of bitcoins. We can see this process visualized through Figure 1.1

Each new block is directly related to the previous block, and everyone using the bitcoin network keeps a record of every bitcoin transaction. When the miner finds a new block, he announces it to the entire bitcoin network and is rewarded

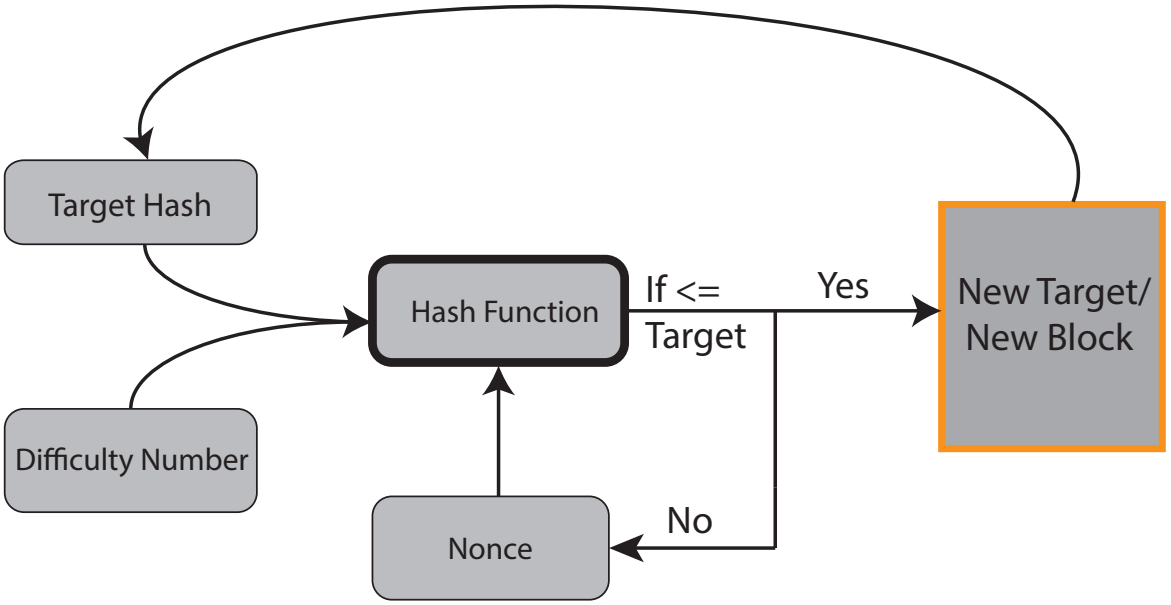

FIGURE 1.1: A Simple Diagram of Bitcoin Mining

with (currently) 25btc. This number is halved every two years to compensate for inflation. In 2016, the number of bitcoins found per block will be reduced to 12.5. All the transactions and creations of bitcoins are stored in a public ledger called the Block Chain. The Block Chain is public record where all blocks are based off of the previous block and any transaction is made public as soon as it is confirmed. Once a miner discovers the next block, it is added to the chain, and everyone who is using the network automatically updates their ledger and the miners begin looking for the next block. These miners are the ones that maintain the network and verify transactions which is why they need to be rewarded for their contributions to the network.

1.2.2 Difficulty

At first, these blocks were easy to discover, but since Bitcoins have become more popular, the difficulty to mine has increased. A new block is discovered every ten minutes but in order to find the block, you are competing against everyone in the network. The more miners, the harder it is to find a block. Because there is a finite amount of Bitcoins, 21 million by 2140, the difficulty of mining changes depending on how long it takes to find 2016 blocks. This difficulty is a number that is factored into the mining equation. Since this should roughly take two weeks, if it

takes longer than two weeks to find 2016 blocks, the difficulty number is reduced. If it occurs quicker, the difficulty number is increased. This is calculated through the formula: difficulty = difficulty 1 target / current target (target is a 256 bit number). Difficulty 1 targer is the difficulty of finding the first block, which was preset in the bitcoin whitepaper. [2] We can think of difficulty as a target that shrinks over time as seen in Figure 1.2.

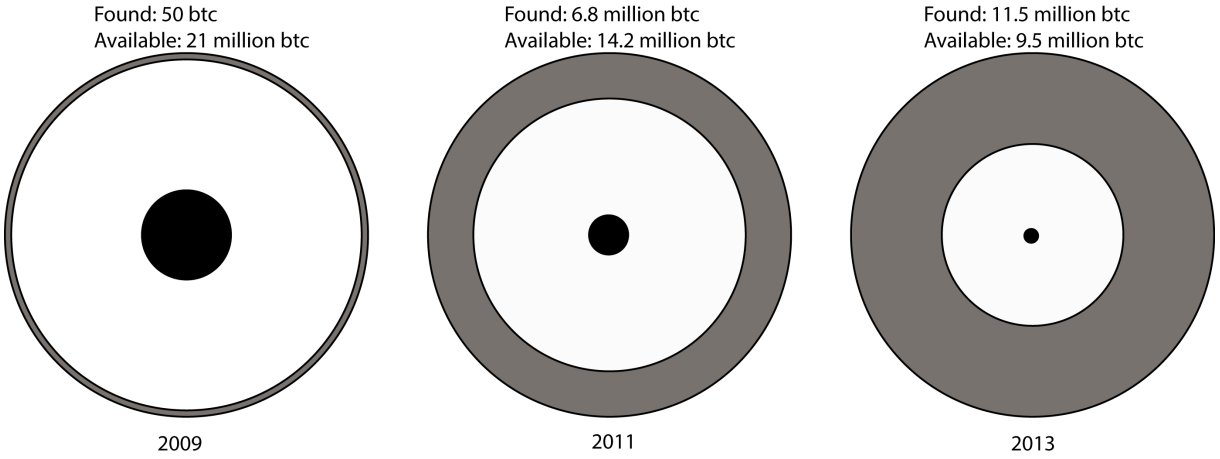

FIGURE 1.2: A Basic Representation Of Bitcoin Difficulty

We can see the increase in difficulty over time in Figure 1.3 At the time of writing, the current difficulty number is about 4.25 trillion. [3]

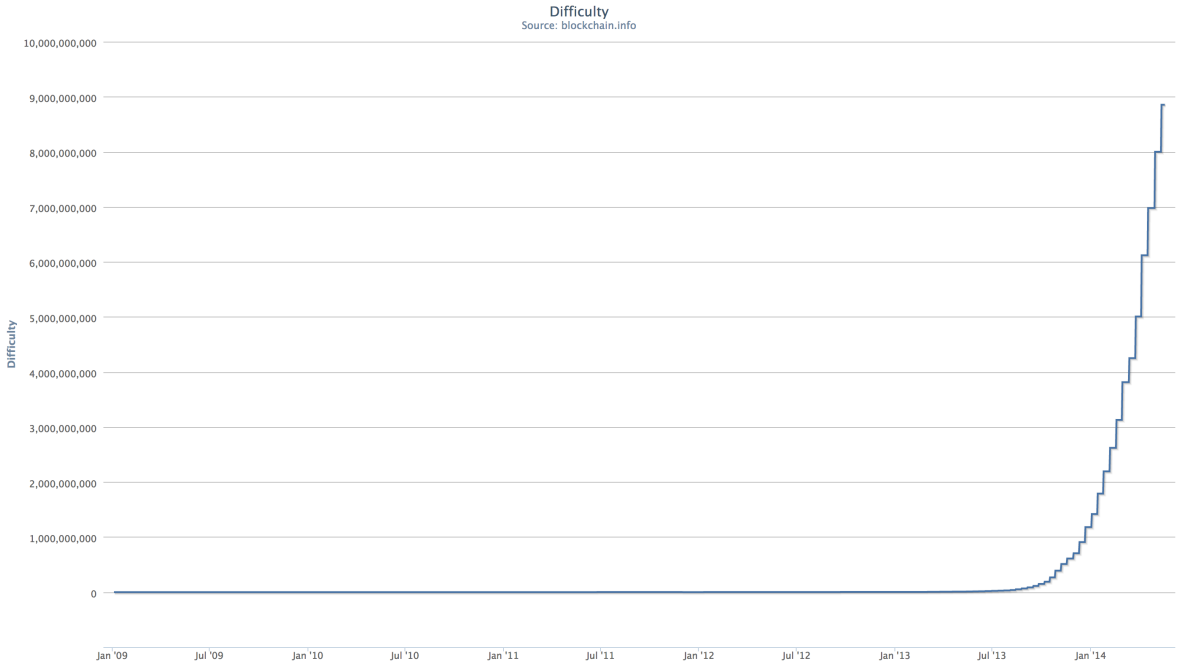

FIGURE 1.3: Difficulty of Bitcoin Mining from 2009- Present [3]

1.2.3 Computer Implications

As of May 2013, the power of the Bitcoin network has become the most powerful computer network on the planet. If you combined the power of the 500 most powerful supercomputers on earth, their power still wouldnt match the Bitcoin network. The thousands of computers that are linked together generate over 1,000 petaflops of processing power. This is the first time anyone has achieved exascale computing which makes it possible to compute quantum calculations. In comparison, the fastest super computer, Titan, achieves 18 petaflops of processing over. To achieve this power, it takes over $5,000,000 a day in electricity costs. At the day of writing however, the profit from this mining is worth $2,500,000, which gives a profit margin on mining of 50%.

1.2.3.1 CPU Mining

When Bitcoin first launched, it was possible to run the mining software on a regular computer and produce results. Using the Central Processing Unit (CPU) the software would run calculations and try to guess an answer. CPUś are only capable of around 1400 kilohashes a second (kH/s). Meaning that they can make about 1,400,000 hashes a second. If one of these hashes is correct then the program has found a block, however this has become increasingly difficult. As bitcoins became more popular, difficulty increase and people figured out that you could use Graphics Processing Units (GPU) to mine bitcoins.

1.2.3.2 GPU Mining

Once the programs were written to hash using a GPU, difficulty increased exponentially. GPU's are capable of producing around 8 megahashes a second (mH/s) of calculations. This is almost 8 times greater than a CPU and a single computer can support up to 6 GPUs. So a single machine GPU mining can make up to 50 times the calculations CPU mining can. This increases the chances of finding the next block but GPUs require about 350watts of power per card. Making this a very power hungry operation. We will explore network power consumption later in paper.

1.2.3.3 ASIC Mining

There is an even faster way to hash then using a GPU. An Application Specific Integrated Circuit (ASIC) is a chip that is specifically designed to do one thing, run the SHA-256 algorithm. These new chips are capable of extreme hash speeds with minimum power consumption. When people realized they could build ASIC's, the game shifted. These ASIC's are capable of incredibly higher speeds, which are currently approaching 1 terrahash of computing power. If there are 1000 kh/s in 1 mh/s, there are 1000mh/s in a gigahash per second and 1000 gH/s equals 1 tH/s. The ASIC computers are capable of almost two thousand times the processing power as a GPU and consume as little as 500W. Making a much more efficient system but unbalancing the playing field and turning Bitcoin mining from a basement project to a commercial application
Table 1.1 shows a comparison of different types of bitcoin miners and the time it takes for a return of investment. Since the invention of ASIC miners, the competition has been decreased significantly and the initial investment for mining equipment has increased.

Type	Hashes/sec	Cost	Break even
CPU	1451 kH/s	$125	3700 years
GPU	7.3 mH/s	$250	7200 years
ASIC	600 gH/s	$4600	60 days

Table 1.1: A Comparison of Bitcoin Miners

1.2.4 Sending Bitcoins

Bitcoins can be sent almost instantly to anyone in the world. They are stored in a bitcoin wallet, which is designated by a public key. The public key is a 34 bit alpha numeric character, for example: *1CC3X2gu58d6wXUWMffpuzN9JAfTUWu4Kj*. This public key can be attached to a computer program designed to send and receive bitcoins or simply written on a piece of paper. In order to release these coins from the wallet, you need to be in possession of the private key. The public key and private key are both related to each other through a mathematical relationship such that the public key can be derived from the private key but not the other way around. Suppose Alice wants to send Chris bitcoins. Chris must send his public address to Alice, Alice then adds Chris's address, the amount of bitcoins

to transfer, a transaction fee and a possibly a transaction message. Alice then signs then transaction with his private key and then announces his public key for signature verification, then it gets broadcasts to the entire Bitcoin network. A miner sees this transaction, and verifies that it is legitimate. This verification process usually goes through a minimum of 6 different miners. The miner then collects the transaction fee and adds the bitcoin transactions to the newest block when it is created. This keeps a ledger of every transaction in the block chain that everyone can see. We can see this in Figure: 1.4 If the transaction is found to be invalid, it is rejected and not added to the chain. To prevent double spending, this system uses proof of work showing that the Bitcoins existed in the network and that the person who they belong to is spending them. If you wanted to create a false block, you would have to change every following block after it, something that is not truly feasible. Only the longest chain of blocks is accepted by the network. If a shorter version of the block chain is attempted to be used, the transaction will be denied. These security measures help maintain the trust within the network.

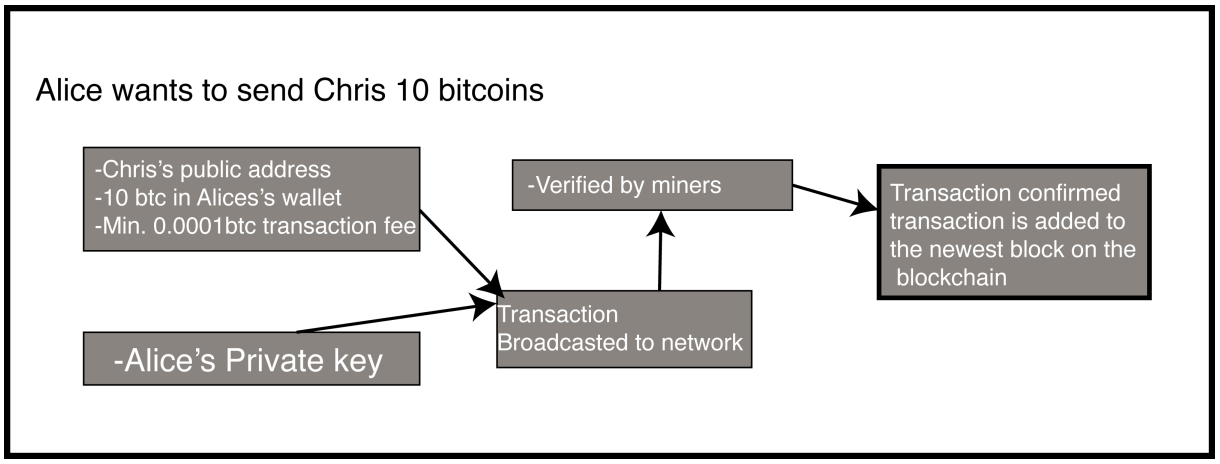

FIGURE 1.4: A visual representation of sending bitcoins

1.2.5 Storing Bitcoins

A common misconception is that because Bitcoins are virtual, they are very secure. Bitcoin however, behaves more like cash. If you were to announce that you have a lockbox on the street corner full of money, you can bet someone will try to steal it. The same goes for Bitcoin. Since the wallet applications on computers hold the private key, if someone hacked into your computer they could steal your bitcoins unless your wallet is encrypted. The most secure way to store bitcoins are in a cold wallet. A cold wallet means that both the public and private key were generated

offline and have never been available on an internet connected machine. You can then send as many bitcoins to the public key and your bitcoins are 'offline'. The only way to 'reactivate' the bitcoins is to enter the private key on an internet connected device which you can then transfer the bitcoins to a 'hot' wallet. If you lose this private key there is no way to retrieve your bitcoins and they are considered 'orphaned'.

1.2.5.1 Orphaned Bitcoins

Because bitcoins can be stored offline, it is possible to lose a private key, effectively 'orphaning' the bitcoins. There have been numerous stories of people losing bitcoins due to hard drive crashes or even throwing them away. [4] It is believed that almost 1 million bitcoins will never be moved or used again . This is a pretty significant figure because there are only 21 million in existence.

1.2.5.2 Bitcoin Days Destroyed

Another measure of activity in the bitcoin network is the 'Bitcoin Days Destroyed' calculations. If one bitcoin is in a wallet, for every day that it sits there, one bitcoin day is created. If you were to move that bitcoin after one year, 365 Bitcoin days would be destroyed. This helps to see how much Bitcoin is in circulation and how much activity is occurring within the network. There have been a few times that a significant amount of Bitcoin days are destroyed, like in January 2014 when 134 million bitcoin days were destroyed. After tracing a few transactions through the blockchain, the users of Reddit.com were able to figure out that $58 million dollars was moved between wallets. We can see the total bitcoin days destroyed in Figure 1.5

1.2.6 Buying/Trading Bitcoin

1.3 A Brief Bitcoin Timeleine

Bitcoin has been on a turbulent ride for the past five years and there have been numerous stories which have contributed to the rise (and fall) of the price of bitcoin to USD.

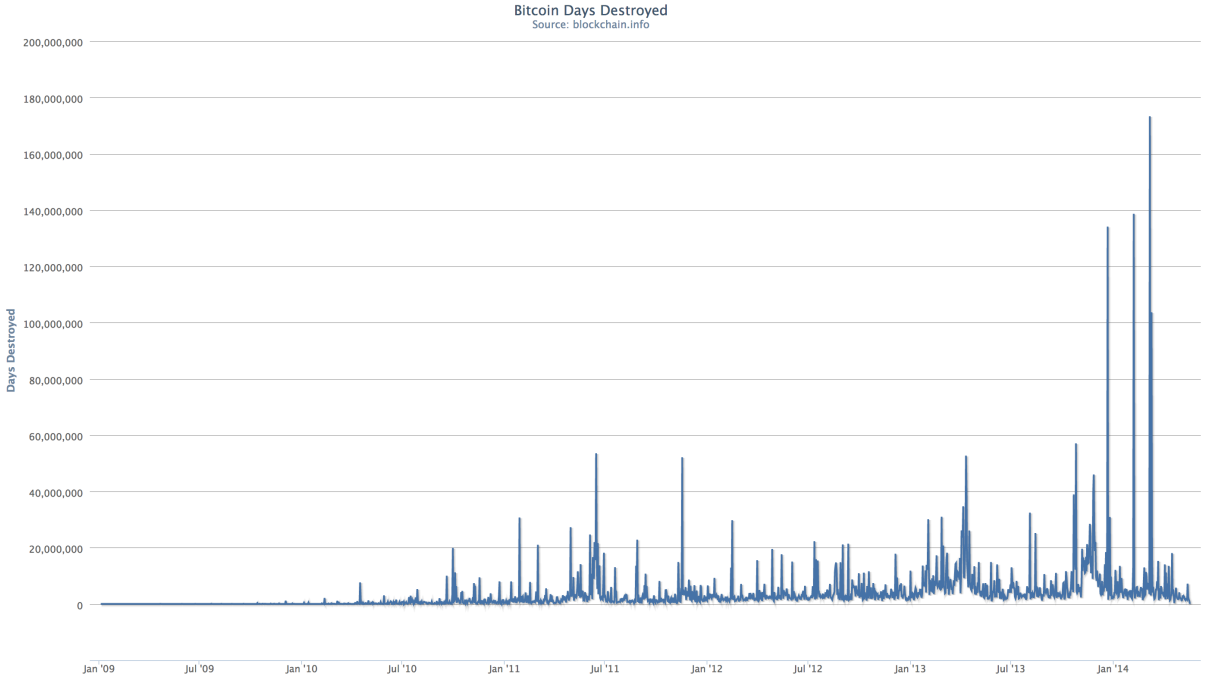

FIGURE 1.5: Bitcoin Days Destroyed [3]

1.3.1 Genesis Block

On January 3rd, 2009 at 18:15:05 GMT, the first block or the 'genesis' block was mined by Satoshi himself.

1.3.2 The 10,000 Bitcoin Pizza

On May 22nd, 2010 a man was looking to use his bitcoins on a tangible item. He found someone online willing to order him two large pizzas in exchange for 10,000 bitcoins. At the time, this was worth about $25.

1.3.3 August 2011 Collapse

Bitcoin went to new records, breaking $1 USD in February, and then $31 on June 8th .The market value was now $206 million. On June 12th, 2011, Mtgox.com, the largest (and one of few) bitcoin exchange, faced a security breach. This caused the market price to decrease from $17 to $0.01. Mt.Gox halted trading for seven days, foreshadowing future problems.

1.3.4 Reward Halved

On November 28th, 2012, the reward for finding a block of bitcoins decreased from 50 btc to 25 btc.

1.3.5 April 2013 Bubble

Due to an increase in price and publicity, the value of bitcoin started to skyrocket. Increasing from $50 to $266 in a matter of days. People saw this as a bubble and many cashed out causing the price to tumble to around $100.

1.3.6 Enter Altcoins

The first Altcoin was created in October 2011 however, since the price and difficulty of bitcoin increased, people looked towards alternatives to bitcoin. This created a market for Altcoins which are based almost completely on speculation and incorporation of 'new and innovative' features.

1.3.7 August 2013

The Winklevoss twins, famous for their initial involvement with Facebook, publicly endorse bitcoin and announce the development of a Bitcoin Exchange Traded Fund (ETF). Current price of bitcoin fluctuates from around $60 to $120.

1.3.8 November 2013 Rise

After all the press and public recognition, the price of bitcoin skyrockets from $150 to over $780. The price continued to rise until it hit a peak of $1260 in December 2013. The price then decreased from the bubble to around $750

1.3.9 The Implosion of Mt. Gox

At one time, MtGox.com handled 80% of all bitcoin transactions. However problems started to arise and withdrawing money from the site became more difficult.

The price on MtGox continued to hold as most other exchanges decreased realizing their was an issue in the network. 'a supposedly leaked document from an internal Mt. Gox discussion posted online Monday by a Bitcoin-focused blogger Wired has identified as Ryan Selkis claims that Mt. Gox has been severely hacked, with a massive reserve of its bitcoins stolen. The document, whose authenticity I couldnt verify, blames the transaction malleability issue for allowing 744,000 bitcoins to be taken from both Mt. Goxs active accounts and its cold storage.' [5] The transaction malleability problem had been known since 2011, MtGox claimed that this was the issue but it was most likely an internal issue of their system. The case is still open as MtGox faces bankruptcy charges and fraud.

1.3.10 Current State

At the time of writing, Bitcoin is valued at $650. The amount of Venture Capitalists investing in Bitcoin was over $76 million dollars in 2013, and is on track to break over $200 million in 2014. [6] This is not only a massive boost to public hesitation but more investment also helps the network evolve and adapt to current conditions. The more systems and ways to use bitcoin, the more value it starts to hold.

Bitcoin value history (comparison to $)

Date	Price for 1 BTC	Notes
Jan 2009 – Jan 2010	basically none	No exchanges or market, users were mainly cryptography fans who were sending bitcoins for low or no value.
Feb 2010 – May 2010	less than $0.01	User "laszlo" made the first real-world transaction – he bought 2 pizzas for 10,000 BTC.[72][73] User "SmokeTooMuch" auctioned 10,000 BTC for $50 (cumulatively), but no buyer was found.[74][75]
June 2010	$0.08	In five days, the price grew 1000%, rising from $0.008 to $0.08 for 1 bitcoin.
Feb 2011 – April 2011	$1	Bitcoin takes parity with US dollar. [76]
8 July 2011	$31	top of first "bubble", followed by the first price drop
Dec 2011	$2	minimum after few months
Dec 2012	$13	slowly rising for a year
April 11, 2013	$266	top of a price rally, during which the value was growing by 5-10% daily.
May 2013	$130	basically stable, again slowly rising.
June 2013	$100	in June slowly dropping to $70, but rising in July to $110
Nov 2013	$350 – $1250	from October $150–$200 in November, rising to $400, then $600, eventually reaching $900 on 11/19/2013 and breaking $1000 threshold on 27 November 2013.
Dec 2013	$600 – $1000	Price crashed to $600, rebounded to $1,000, crashed again to the $500 range. Stabilized to the ~$650–$800 range.
Jan 2014	$750 – $1000	Price spiked to $1000 briefly, then settled in the $800-$900 range for the rest of the month.[77]
Feb 2014	$550 – $750	Price fell following the shutdown of MTGOX before recovering to the $600-$700 range.
Mar 2014	$450 – $700	Price continued to fall due to a false report regarding Bitcoin ban in China [78] and uncertainty over whether the Chinese government would seek to prohibit banks from working with digital currency exchanges. [79]
Apr 2014	$340 – $530	The lowest price since the 2012–2013 Cypriot financial crisis had been reached at 3:25 AM on April 11th[80]
May 2014	$440 – $630	The downtrend first slow down and then reverse, increasing over 30% in the last days of May.

FIGURE 1.6: Bitcoin's value history from [1]

Chapter 2

The BlockChain

2.1 Sending Secure Data over a Network

An age old problem in computer science is being able to trust information received from another computer in a network. If someone sends you an email for example, there is nothing that guarantees that person it claims to be from is the person that sent the email. Someone could have hacked your computer or email address and could be sending false data while posing as the sender. This is an issue that can only really be handled with encryption. The problem with any type of encryption is that you need to decrypt the message. For example. Pretty Good Privacy or PGP, has been the staple of p2p encryption for the past twenty years. However, in order to send someone a PGP encrypted message, you need their public key to encrypt the message and they need your public key to decrypt the message. If you have never communicated with a person before, you have no way of making sure you have a secure line to that person. This is something that cannot exist between two strangers unless their is a trusted third party involved. With financial transactions, we aren't willing to risk any type of false transaction but currently there is no way to pay a stranger without a third party. When sending money over the internet, users turn to services like PayPal to guarantee that their transaction meets the receiver without being altered. In order to provide this service, PayPal charges users as much as 4%. So you either have to risk having your credit card stolen, or compensate PayPal to use their service. Not only does this pose a risk to users, but a massive corporation has access to your accounts and essential

information. As a user, you have no option but to trust this service because there is no other option.

2.1.1 The Byzantine General's Problem

> Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals. (From The Byzantine General's White Paper)

2.1.2 Solving the Byzantine General's Problem

While the problem has been solved, you need three or more generals to validate the message. If there are less than three, we again face the same problem of validation. This is where Bitcoin comes in. While old digital payment systems require a third party to validate transactions, Bitcoin uses its own network. But what exactly makes that Bitcoin so secure and how exactly do we verify transactions between two users without a third party. This is where the Blockchain comes into play and solves this problem.

2.2 SHA-256

'For encryption to work, it needs a steady supply of random numbers to throw attackers off the scent. Traditional computation often has a hard time providing the necessary chaos. It's a problem that crypto coders have dealt with over and over, developing lots of answers that each come with their own unique weaknesses'

[7] At the very heart of Bitcoin sits the Secure Hashing Algorithm 256-bit or SHA-256. This encryption algorithm is used in almost all government institutions for encryption and was considered the pinnacle of encryption until the creation of SHA-3 in 2012. Although possible, there have been no known collisions during hashing of the SHA-256 algorithm and even using the fastest supercomputers on Earth, it would take more time to break the encryption than you would be alive.

2.2.1 A Technical View of SHA-256

2.2.1.1 Preprocessing

Before the algorithm even starts working its black magic, it needs to process the message so that it works with the algorithm. It takes any message or value and needs to make it 512 bits long so that it can run through the algorithm. It accomplishes this by adding the bit "1" to the end of the message and then padding the rest of the message with zeros. If message M, lets use 'abc' as an example, is of length l bits, in this case 24 bits, then it will need to have 'k' bits added, so that

$$l + 1 + k \equiv 448 \; modulo \; 512$$

In our example that would mean $448 - (24 + 1) = 423$ zero bits need to be added to create a 512 bit message. Although longer messages would be padded into multiples of 512. The number 64 comes from the the length of the original message in bits as 64-bit big-endian integer.

$$\underbrace{01100001\ \ 01100010\ \ 01100011}_{\text{message in bits}}\ \underbrace{1}_{1bit}\ \underbrace{00\ldots0}_{\text{423 zero bits}}\ \underbrace{0\ldots011000}_{\text{64 bits}}$$

The message is then broken into N 512-bit blocks which are then initialized as $M^1, M^2 \ldots, M^n$. The first 32-bits of the message block i are stored as ${M_0}^{(i)}$ then the next 32-bits are stored, up to ${M_1}5^{(i)}$. The bits are stored big-endian meaning the left most bit is stored in the most significant position.

2.2.1.2 Initializing Hash Values

The first thing the algorithm needs to do is initialize the hash values. These values are obtained by taking the fractional parts of the square roots of the first eight

prime numbers. So the initial hash value is equivalent to:

$$H_1{}^{(0)} = 0x6a09e667 \equiv hex(modf(\sqrt{2}))$$

$$H_2{}^{(0)*} = 0xbb67ae85 \equiv hex(modf(\sqrt{3}))$$

$$\vdots$$

$$H_8{}^{(0)} = 0x5be0cd19 \equiv hex(modf(\sqrt{19})) * denotes$$

After the initial hash values are initiated, we need to initialize the array of round constants. These are equivalent to first 32 bits of the fractional parts of the cube roots of the first 64 prime numbers. These numbers create a randomness which isn't perfectly random, but in order to break the encryption it would take about 2^256 years.

2.2.1.3 The Main Loop

for $i = 1$ to N where N =the number of 512-bit blocks in the message. **do**

Initialize hash values as stated above and assign them to registers $a \dots h$ where $H_1^{(i-1)} \rightarrow a$

Apply the SHA-256 Compression Algorithm to update registers $a \dots h$

for $j = 0$ to 63 **do**

function $(C)h(e, f, g),\ Maj(a, b, c),\ \Sigma_0(a),\ \Sigma_1(e),\ and\ W_j$

$Ch(e, f, g) = (e \wedge f) \oplus (\neg e \wedge g)$

$Maj(a, b, c) = (a \wedge b) \oplus (a \wedge c) \oplus (b \wedge c)$

$\Sigma_0(a) = S^2(a) \oplus S^{12}(a) \oplus S^{22}(a)$

WHERE S^i = RIGHT ROTATION BY i BITS.

$\Sigma_1(e) = S^6(e) \oplus S^{11}(e) \oplus S^{25}(e)$

end function

$T_1 \leftarrow h + \Sigma_1(e) + Ch(e, f, g) + K_j + W_j$

$T_2 \leftarrow \Sigma_0(a) + Maj(a, b, c)$

$h \leftarrow g$

$g \leftarrow f$

$f \leftarrow e$

$e \leftarrow d + T_1$

$d \leftarrow c$

$c \leftarrow b$

$b \leftarrow a$

$a \leftarrow T_1 + T_2$

end for

NOW WE NEED TO COMPUTE THE i^{th} INTERMEDIATE HASH VALUE, $H^{(i)}$

$H_1^{(i)} \leftarrow a + H_1^{(i-1)}$

$\vdots$

$H_8^{(i)} \leftarrow h + H_8^{(i-1)}$

end for

We can see this loop visualized below in Figure 2.1. The $\boxplus$ denotes modulo 2^{32} addition.

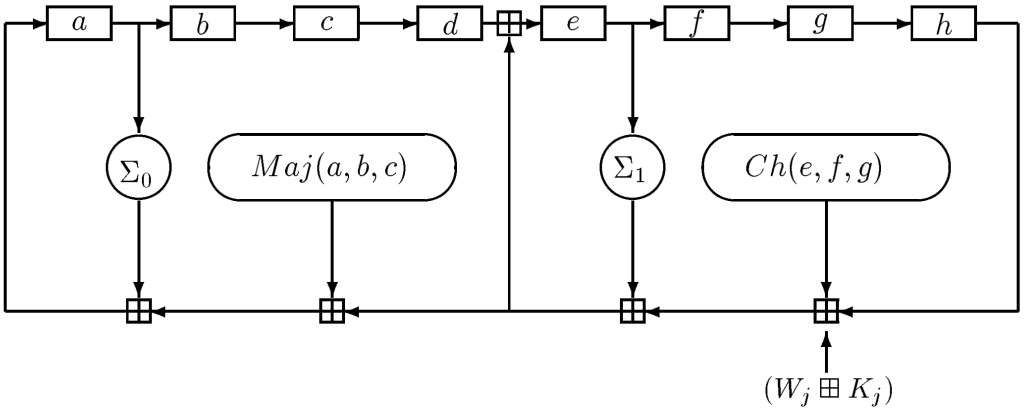

FIGURE 2.1: The Main Loop of SHA-256 [8]

The Hash of our original message is equal to:

$$H^N = H_1^N, H_2^N \dots H_8^N$$

2.3 Merkle Trees

Now even though this complicated algorithm changes the data, how does mining bitcoin become difficult and how is SHA-256 being used inside the protocol? All of the hashs are combined in what is known as a Merkle Tree. A Merkle Tree is a version of a binary tree except it moves from the bottom up. As seen in Figure 2.2, the bitcoin transactions are stored at the bottom, Tx0, Tx1, etc. We take the hash value of these transactions, concatenated them, then process the hash value of both transactions until we get to the root hash. This is called the Merkle Root and is stored in the Block Header. The block header is a combination of the

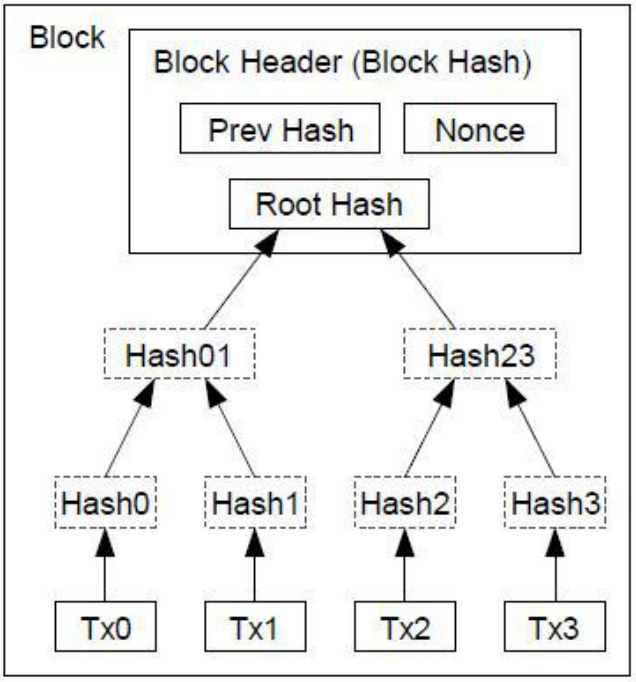

FIGURE 2.2: A Merkle Tree diagram with Bitcoin block header [8]

Merkle Root with the previous hash and a Nonce. All of these values are hashed together to achieve a 'block hash' which must be less than the difficulty target. If the value is not less than the target, the miner would add another nonce and hash again. 'Nonces are used in proof of work systems to vary the input to a cryptographic hash function so as to obtain a hash for a certain input that fulfills certain arbitrary conditions. In doing so, it becomes far more difficult to create a "desirable" hash than to verify it, shifting the burden of work onto one side of a transaction or system.' [9] Since changing any part of an input changes the output hash, making any unauthorized change to the blockchain will result in a rejection of the block. This allows the computer to have a checksum along every step of the way, guaranteeing the security of the network. All bitcoin transactions must be checked six times before they are completely confirmed by the network. This forces false transactions to not verify and makes it very difficult to trick the network.

2.3.1 Why Difficulty Matters

As stated earlier, bitcoin difficulty is equal to difficulty = difficulty 1 target / current target (target is a 256 bit number). However, it is possible that blocks

can be found in less than 10 minutes, since the difficulty is only calculated once every two weeks. To explain in simpler terms, if the hash values can only be 0 to 1000 and the difficulty starts at 1 then difficulty would be 100. (1000/1) At a rate of 1 hash per minute, the chances of you finding a block are 100%. If the difficulty increases to 4, your chances of finding a block are 25%. If a friend came over and your hashrate went up to 2 hashes a minute, you would be able to find double the amount of coins in half the amount of time. Bitcoin recalculates for the amount of people on the network and the amount of hashes per second the network is outputting, in order to combat this issue. This is computed in another algorithm and broadcasted to the network automatically. Without calculating difficulty, there would be no way to regulate the amount of bitcoins so that there are 21 million by 2140. Since SHA-256 runs in constant time, difficulty is needed to make this constant time function take longer. This is another reason why finding bitcoins has become a computer power arms race.

2.4 SHA-2 versus SHA-3

Since SHA-256 is considered so secure, why has it been succeed by SHA-3 'Keccak'? In 2007, the National Institute of Standards and Technology (NIST) found a number of weaknesses and possible attacks for SHA-1. It was feared that SHA-2 would soon be broken and a competition was held to find a successor. However it took five years to name an algorithm worthy of SHA-3 and the NIST chose the algorithm that was the most different from SHA-256 so that both would not be broken simultaneously. During these five years, SHA-256 proved to be more robust than originally thought and no crack in the armor has yet to be found. SHA-3 has essentially become a backup for SHA-2 incase someone does find a flaw.

2.4.1 Why Do Different 'Altcoins' Use Different Algorithms?

When Bitcoin was first created in 2009, anyone could mine using their personal computer since difficulty was so low. However if you were to use your personal computer today, you probably never find a bitcoin. This is why ASIC's were created, to further the arms race and find bitcoins even quicker. In order to even compete now, you need to be calculating a minimum of 1 trillion hashes a second. This requires an incredibly high initial investment and unless you keep reinvesting

your money, it becomes very hard to continually profit. Figure 2.3 shows the hashrate of the bitcoin network and Figure 2.4 shows the average miners profit. It is important to remeber that every four years, the reward for finding a bitcoin block is halved. This last occurred in November 12th, 2012. Cutting the reward from 50 btc to 25 btc and is scheduled to happen again in 2016. We can see this in Figure 2.4

FIGURE 2.3: The Hash rate of the Bitcoin Network [3]

FIGURE 2.4: Miner Revenue [3]

In order to level the playing field, developers started looking into different algorithms that SHA-256 ASIC's could not solve. The first Altcoin was Litecoin created in 2011, which uses Scrypt as proof-of-work. Newer Altcoins use Keccak, Adaptive-n (which is incredibly memory intensive), and any combinations of these to keep their own blockchains secure. Now while many people were trying to 'level' the playing field, other coins were created simply because the creators promised something new and exciting which usually led to said coin spiking in value and then becoming almost worthless. A classic 'pump and dump' scheme which is illegal in real world markets. A 'pump and dump' is when you get people to believe that your coin is worth something, so that they purchase it then when the price is high, then you dump all of your holdings in the coins maximizing on profit. At the time of writing, their are 426 Altcoins in existence.

2.4.2 CryptoCurrencies 2.0

Many of the Altcoins consider themselves Bitcoin 2.0, 3.0, etc. There are new projects that are in the works that plan on using the underlying bitcoin technology and blockchain to create a new currency or even a new type of system. These systems show promise to revolutionize the way we interact, creating new ways for trust to exist. Economically, this could become a revolution where money is pulled away from massive multibillion dollar corporations and back into the hands of consumers.

Chapter 3

Changing The Financial Landscape

3.1 The Implications of Decentralization

Decentralization is a very interesting concept because almost everything that we do on a day to day basis relies on a centralized authority. Whenever we make a financial transaction, there is almost always at least one third party involved, which creates the trust between the two people and allows a transaction to be completed.

If we were to use cash, the government is still a third party that defines what the money is worth and gives the trust that the transaction requires for an exchange of goods. On the internet, we have to use many different services to transfer money between people because you cannot exchange cash digitally. So in addition to the bank that holds your money, a service like Paypal, Visa, or Western Union, must be used as a guarantee that the transaction has been completed. These services have high fees because they require a lot of work to transfer money from one bank to another. Unlike Bitcoin, banks do not share a public ledger so funds must be verified and moved physically from one location to another. This process is slow and can take days to transfer money from one bank account to another unless you share the same bank.

3.1.1 Decentralized and Distributed

We can examine the different types of networks in Figure 3.1. A centralized

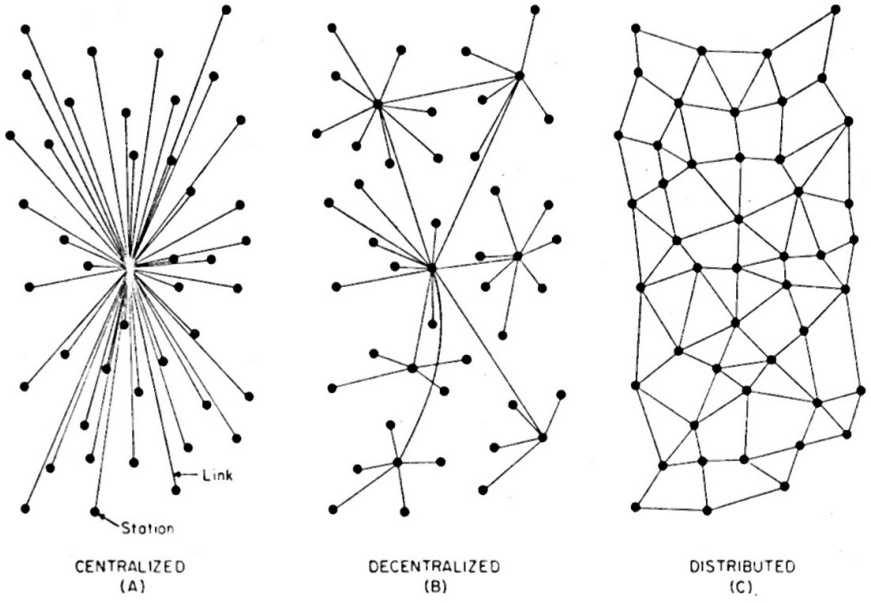

FIGURE 3.1: Types of Networks [10]

network would be where one person or company owns the servers and the only way to get the information that you need is from that one location. The internet is currently a centralized network because in order to connect, you need to go through a company that provides internet, unless you tap directly into the network but that is usually not possible. If a company were to no longer exist, the network that it controlled would most likely cease to exist also.

A decentralized network is a network in which there is no central authority but information can still flow as it would in a normal network. If some of the people on the network leave, the network can still function because it can connect to other nodes. This is the definition of Peer 2 Peer (P2P) and illegal music sharing was able to exist. Instead of the files being held on a central server, they were held on any computer in the network and you would download from other peoples computers. This makes shutting a system like this very hard. It also allows the network to function if one of more servers or 'nodes' go offline.

A distributed network is a network in which every node in the mesh contains the same information creating a system that can be stretched across the globe. Bitcoin is both a decentralized and a distributed network. You do not need to have the entire Blockchain to send bitcoins to anyone but the miners must have to have

a copy of the Blockchain in order to verify data. Every time the Blockchains is edited, all of the nodes connected must update their copy so that the network is able to stay in sync.

The reason Bitcoin miners get rewarded for their efforts is because in order for the network to function there has to be many miners able to verify the transactions. As it is becoming harder to find Bitcoins, there is less incentive for miners to leave nodes on the network because the hardware requires a significant investment and requires constant reinvestment in order to continue profiting. We can see in Figure 3.2 that the number of nodes on the Bitcoin network has decreased by almost 1000 in the 60 days from March 12, 2014 to May 15, 2014. There has been discussion of launching Bitcoin Nodes into space so the network could never go down and would be out of reach from government hands. Just like any system, if no one uses it, it won't work. If people aren't mining for bitcoins or maintaining the network, it will collapse.

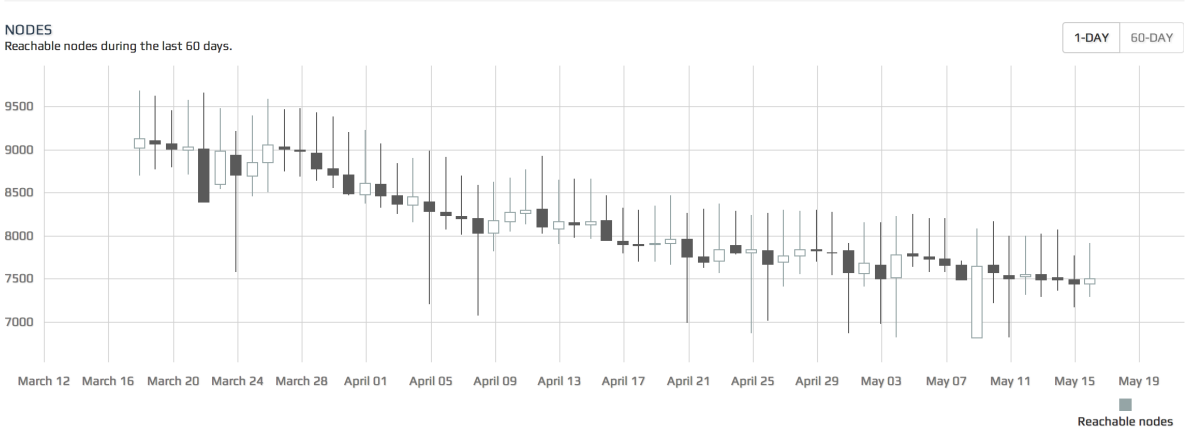

FIGURE 3.2: Number of Reachable Bitcoin Nodes

3.2 Smart Property

The idea of 'Smart Property' was first introduced by Nick Szabo in 1997 and gives the idea that ownership is controlled by a Blockchain using contracts. Ownership would be validated using the secure hashing algorithms and timestamps and if a hash did not check out, the owner would not be correct. This would allow for property to be traded with almost zero trust, eliminating most fees and fraud. For example you could loan someone money for a project and if they didn't pay

it back, whatever collateral or smart property they agreed to in the original deal would now become yours.

3.2.1 Contracts

The idea of smart property is incredibly innovative but unless contracts are understood, the idea may seem complicated although it doesn't make anything possible that wasn't already. What it does accomplish is removing human judgement by minimizing the amount of trust needed and allowing for automation. If you have no reason not to trust a system, you would be much more inclined to use it. In contrast, you probably wouldn't use a system that has had a history of corruption and issues. Even though the majority of major financial institution all have this history, they still exist so people trust them to hold their money.
Contracts allow for smart property, transferring digital property or assets, creation of agents, and even distributed financial markets. These contracts use the same checks that the Blockchain uses in addition to timestamps and other signifying factors that validate the information.
An example of a contract could be if you wanted to trade with someone that you don't know or don't trust. You could set up a contract which would require a third party mediation service to verify if the contract has been fulfilled. This third party mediation service could be anything from a trusted company, a mutual friend, or a computer program that verifies the information. Or if a grandparent wanted to set up a will, they could have a contract that verifies if they are still alive before releasing the coins or assets to the designated receive.

3.2.1.1 Assurance Contracts

Public goods are a hard thing to create because their is always the question of who is responsible for the good. Directly no one profits from a public good but indirectly everyone profits. In order to fund these projects, usually a government steps in to provide the good. Crowdfunding websites like Kickstarter.com are currently the best example of assurance contracts. You find a product or service that someone wants to create, purchase that product for a set price and if the product or good does not reach their funding goal, your money is returned. However this system does not currently work as efficiently as it could because the credit card

isn't charged until funding is met. If a person cancels their card or something along those lines, they will not be able to pay for the product or service when the time comes. With a Blockchain system, you can have an assurance contract that either acts as an escrow service and can refund your purchase instantly if funding is not met with zero fees. If you were to use a credit card, there would be approximately 3% fee on all charges, even refunds. Current banks and credit card systems were not designed to handle services like this and aren't flexible enough for the digital world. If people could pay for the services they needed instead of paying taxes, it would be a very different landscape, one being pushed forward by innovation.

3.2.2 Agents and Distributed Autonomous Corporations

Another incredible innovation of the Blockchain is the creation of Agents which was suggested by Gregory Maxwell in 2011. An agent is a program designed to sell services for bitcoins and then use the proceeds to pay for the power consumption and maintenance. For example an Agent could provide a file hosting site in the cloud where you would pay in bitcoin for hosting. The computer would automatically find the best server price and be as efficient as possible. If the program starts to make more money than it needs to survive, it can clone itself a 'child.' If the child is successful it will pay back the parent and eventually go on to clone itself. If the child is unsuccessful and starts to lose money, when it's bank account hits zero, it will die or be deleted.

If you were to create a bunch of agents and form a corporation, it could become a distributed autonomous corporation or DAC as suggested by Vitalik Buterin with his bitcoin like protocol, Ethereum. He is creating a bitcoin like system that will have a new turing-complete programming language built on top of it making it easy for anyone to start a distributed system. In colloquial usage, the terms 'Turing complete' or 'Turing equivalent' are used to mean that any real-world general-purpose computer or computer language can approximately simulate any other real-world general-purpose computer or computer language. The reason this is only approximate is that within the bounds of finite memory, they are only linear bounded automaton complete.' [8]

While this sounds like Skynet, it is completely possible with a system like Bitcoin or a system like it. There is one thing that computers cannot do, be creative. This is why humans will always have the upper hand because these systems are not capable of designing themselves or coming up with a creative way to improve. So humans may be working or machines in the future but we will still have control over them. Any job that requires no creativity can always be replaced by a machine.

3.2.3 Distributed Markets

What if you could issue shares of a company without going public? The only way this is currently possible is if the company has a private equity sale but really, they could use a Blockchain based system to distribute shares of their company and the computer would automatically be able to check if the funds were there and issue returns back to the investors original address. A system like this is possible and would allow for fee free transactions while maintaing the security and trust of an established institution like the Dow Jones.

3.3 Attempting Complete Efficiency

Economists generally study 'perfect' economies because it is hard to interpret data with too many variables. These crypto coin markets do not respond to outside forces mostly because the system is controlled by formulas that cannot be changed. If the building blocks of these systems were to change, any change would need to be accepted by 2/3 of the network. If only 1/3 of miners were to adopt the change, their transactions would be stopped by the network because they fell within the minority. Bitcoin is the perfect tool for economists to study because not only are all the systems already set in stone but every transaction is visible on the blockchain. If you know where the money is coming from you can study how it moves. While bitcoin might not be the most stable market presently, in theory it is a perfect market. Figure 3.3 shows inflation Vs. Time as it was presented in the original white paper.

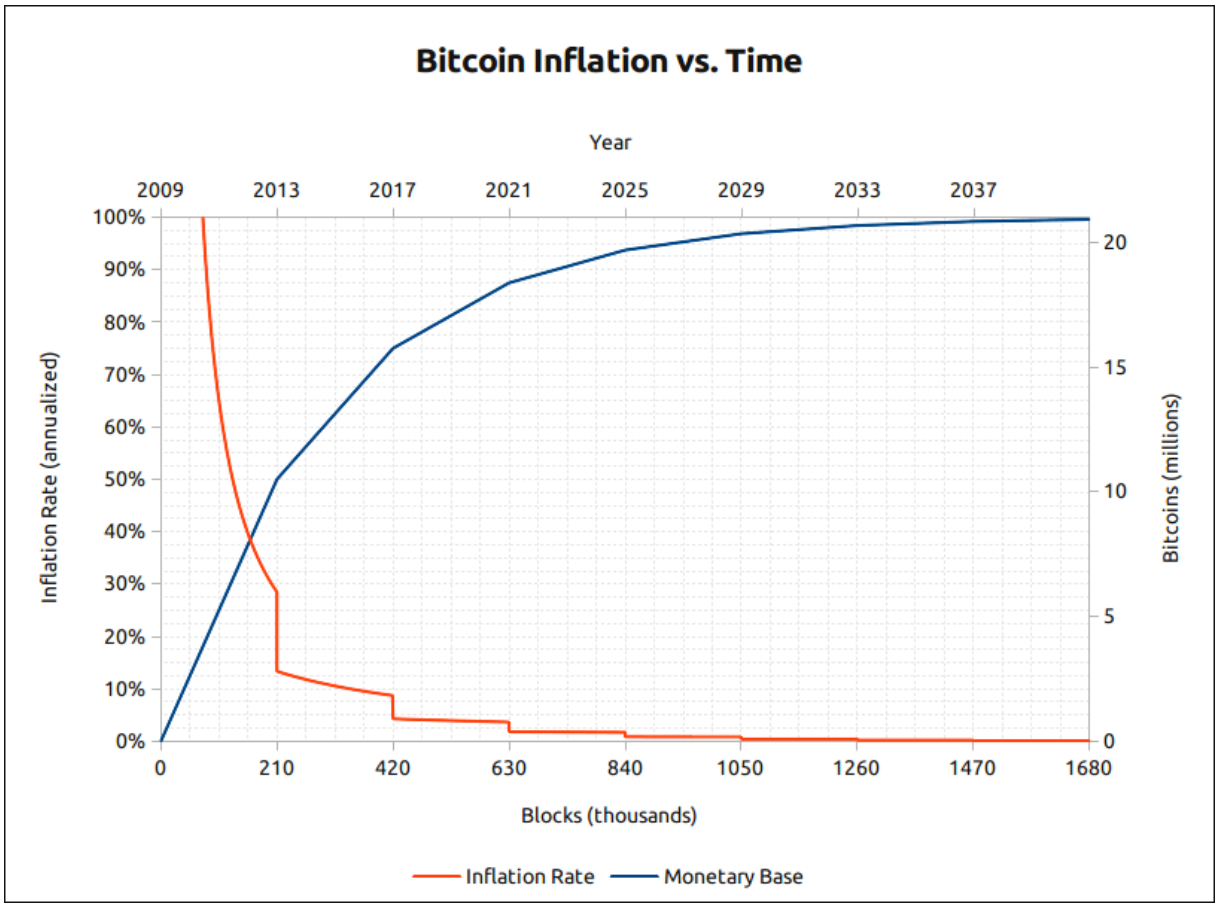

FIGURE 3.3: Bitcoin Inflation vs Time

3.4 Adapting Current Systems

Many current computer systems were designed years ago before most realized the security issues with the internet. Since the uncovering of the NSA's surveillance policies, many people have been concerned with the safety of their virtual data. Every year millions of accounts and credit cards are compromised by hackers because people trust these third parties to hold ones data. But why should a company own someone else's credit card information or know everything about their lives? Implementing a blockchain protocol into our current systems would not only be more efficient but also help secure our data.

3.4.1 The Ticketing Market

One example of a system that could be made more efficient with a cryptographic blockchain is event ticketing. As the worlds largest provider of tickets, TicketMaster essentially owns ticketing. But there are issues associated with their system that they do not seem to address. Not only would this improve the customer experience, but it would most likely result in higher revenue.

3.4.1.1 Reselling Tickets

If you purchase a ticket and cannot attend the event, you will probably turn to StubHub to sell your tickets. StubHub charges a 25% fee on all sales. This is a huge proportion and although they will guarantee that the ticket is real, if you get to the event and it doesn't, you're out of luck. You will still receive your money back but you will not get into the event that night. In order to cut down on ticket fraud, the company likes to make sure that the name on the ticket is the person who purchased it and that it matches their identity upon entering. If you want to give it to a friend or sell it, this data no longer lines up. If a blockchain system was implemented, it would allow seamless transfers between users while maintaining security and preventing fraud. It would also allow for tickets to be on cellphones, paper, or on wristband chips. Allowing for seamless transfer between platforms. We can see this plan illustrated in Figure 3.4

3.5 The Future is Connected

Cryptography is going to start being a lot more prevalent in today's society. With the current massive surveillance attacks and computer hacking, society is ready to own their data and protect themselves. The internet was once a free place where any information could be shared. It has become a pawn of large corporations and it is time that distributed technology helps the world break away from this system. With Net Neutrality looking grim it seems that the only way to break free is to connect to one another. Once we can share information freely without the use of third parties, the world will become a much fairer place.

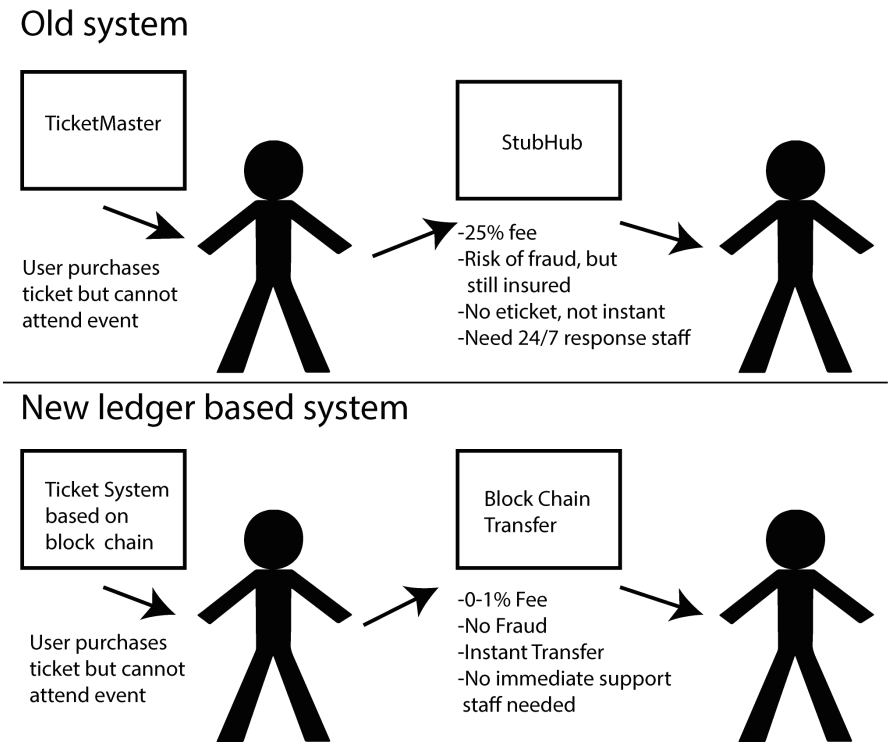

FIGURE 3.4: A Comparison of Ticket Systems

Bibliography

[1] Wiki. History of bitcoin. URL http://en.wikipedia.org/wiki/History_of_Bitcoin#Theft_and_exchange_shutdowns.

[2] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. URL https://bitcoin.org/bitcoin.pdf.

[3] Many. Blockchain.info. URL https://blockchain.info/.

[4] Alex Hern. Missing: hard drive containing bitcoins worth 4m in newport landfill site. URL http://www.theguardian.com/technology/2013/nov/27/hard-drive-bitcoin-landfill-site.

[5] Andy Greenberg. Bitcoin's price plummets as mt. gox goes dark, with massive hack rumored, . URL http://www.forbes.com/sites/andygreenberg/2014/02/25/bitcoins-price-plummets-as-mt-gox-goes-dark-with-massive-hack-rumored/.

[6] Saumya Vaishampayan. Bitcoin is like the early internet, minus the vc money. URL http://www.marketwatch.com/story/bitcoin-venture-capital-money-hasnt-kept-up-with-buzz-2014-04-28.

[7] Russel Brandom. Your cellphone camera might be the most random thing you own. URL http://www.theverge.com/2014/5/16/5723252/mobile-cryptographers-tap-into-quantum-chaos.

[8] Many. Bitcoin wiki, March 2014. URL https://en.bitcoin.it/wiki/Main_Page.

[9] Cryptographic nonce, May 2014. URL http://en.wikipedia.org/wiki/Cryptographic_nonce.

[10] Rand. On distributed communications series. URL http://www.rand.org/pubs/research_memoranda/RM3420/RM3420-chapter1.html.

[11] N Y Times. An abridged history of bitcoin. URL http://www.nytimes.com/interactive/technology/bitcoin-timeline.html?_r=0.

[12] Felix Martin. Bitcoin is pointless as a currency, but it could change the world anyway. URL http://www.wired.com/2014/03/bitcoin-currency_martin/?mbid=social_twitter.

[13] Loomio. Decentralised decision making for decentralised currencies. URL http://blog.loomio.org/2014/04/07/decentralised-decision-making-for-decentralised-currencies/.

[14] Andy Greenberg. Dark wallet is about to make bitcoin money laundering easier than ever, . URL http://www.wired.com/2014/04/dark-wallet/?mbid=social_twitter.

[15] Tristan Winters. Web 3.0: A chat with ethereum's gavin wood, . URL http://bitcoinmagazine.com/12596/web-3-0-chat-ethereums-gavin-wood/?utm_content=bufferb149f&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer.

[16] many. Bitcoin magazine.

[17] Gavin Wood. Insights into a modern world: What web 3.0 looks like. URL http://insightsintoamodernworld.blogspot.co.uk/2014/04/apps-what-web-30-looks-like.html?m=1.

[18] Vinny Lingham. Finding equilibrium: Searching for the true value of a bitcoin. URL https://medium.com/crypto-currency/ba5f3fcce103.

[19] Mainak Ghosh, Miles Richardson, Bryan Ford, and Rob Jansen. A torpath to torcoin proof of bandwidth altcoins for compensating relays.

[20] Tim Swanson. Bitcoin is facing a potentially fatal paradox. URL http://www.businessinsider.com/bitcoin-is-facing-a-potentially-fatal-paradox-2014-5.

[21] Eric Calouro. State regulators working to pen first bitcoin rulebook, 2014. URL http://newsbtc.com/2014/05/18/state-regulators-working-pen-first-bitcoin-rulebook/.

[22] Tim Swanson. Learning from bitcoins past, 2014. URL http://www.ofnumbers.com/wp-content/uploads/2014/04/Learning-from-Bitcoins-past.pdf.

[23] Coindesk, May 2014. URL www.Coindesk.com.

[24] Gavin Wood. *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER*. Ethereum, 2014.

[25] Rob Wile. Satoshi's revolution: How the creator of bitcoin may have stumbled onto something much bigger. URL http://www.wired.com/2014/03/decentralized-applications-built-bitcoin-great-except-whos-responsible-outc

[26] Primavera De Filippi. Tomorrow's apps will come from brilliant (and risky) bitcoin code. URL http://www.wired.com/2014/03/decentralized-applications-built-bitcoin-great-except-whos-responsible-outc

[27] Leslie Lamport. The byzantine generals problem. URL http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf.

[28] Lex Rieffel. Could the imf have built bitcoin? URL http://www.ft.com/intl/cms/s/0/9aaec458-aadc-11e3-83a2-00144feab7de.html?siteedition=intl#axzz2wRfpDhPv.

[29] Cryptocurrencies world. URL http://com-http.us/.

[30] Bitcoin. Block explorer. URL http://blockexplorer.com.

[31] Elaine Shi Simon Barber, Xavier Boyen. Bitter to better- hot to make bitcoin a better currency. *Financial Cryptography and Data Security*, 7397:399–414, March 2012.

[32] Dorit RonÃdi Shamir. Quantatative analysis of the full bitcoin transaction graph. *Financial Cryptography and Data Security*, 7859:6–24, April 2013.

[33] Tristan Winters. Bitcoin 2.0: Is a political revolution inevitable?, . URL http://bitscan.com/articles/bitcoin-2.0-is-a-political-revolution-inevitable/.

[34] Scott Rose. Current criticisims to bitcoin are at least 10 years too early. URL http://www.coindesk.com/current-criticisms-bitcoin-10-years-too-early/.

[35] Vitalik Buterin. Ethereum: A next-generation smart contract and decentralized application platform, . URL https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-White-Paper.

[36] Vitalik Buterin. Bootstrapping a decentralized autonomous corporation, . URL http://bitcoinmagazine.com/7050/bootstrapping-a-decentralized-autonomous-corporation-part-i/.

[37] Nicholas Tomaino. What are the consumer benefits of spending bitcoin? URL http://www.coindesk.com/consumer-benefits-spending-bitcoin/.

[38] Pete Rizzo. Dogecoin foundation to raise $50k for kenya's water crisis. URL http://www.coindesk.com/dogecoin-foundation-raise-50k-kenya-water-crisis/.

[39] Nermin Hajdarbegovic. Goldman sachs: Bitcoin isn't a currency but underlying tech holds promise. URL http://www.coindesk.com/goldman-sachs-bitcoin-isnt-currency-underlying-tech-holds-promise/.

[40] Jason Kolb. 5 technologies that will change the world. URL http://www.jasonkolb.com/5-disruptive-technologies-that-will-change-the-world/.