A Mathematical and Economic Analysis of Cryptocurrency

Albert Richard Caputo III

A Senior Thesis.

Applied Mathematics
Brown University
Providence, RI, USA
April 20, 2018

Contents

1 Abstract

In this paper, we seek to understand the fundamental concept of a cryptocurrency. Although a relatively new and widely misunderstood phenomena, cryptocurrency, without a doubt has gained stunning popularity since its theoretical proposal, and with this, exponential growth in valuation. We will first analyze the structure of a cryptocurrency (in particular, Bitcoin) through the lens of Satashi Nakamoto's paper on peer-to-peer (P2P) verification. In addition, we will unravel the concept of "blockchain" and how computer processing power is used to ensure a secure transaction system. Next, we will provide an in-depth economic evaluation of various cryptocurrencies and attempt to answer the following questions: What is cryptocurrency valued as? Who is investing? Who/What are the major drivers? What are the risks? What are the best strategies? Lastly, we will implement mathematical finance strategies and algorithms to determine optimal cryptocurrency portfolios and analyze the Markovity of Bear, Bull, and Stagnant market transitions.

2 Introduction

2.1 What is Cryptocurrency?

A cryptocurrency, in most simple terms, is a currency that relies on trust in its users rather than trust in a centralized authority. Let us first consider using a government regulated currency and compare. When a person swipes his or her credit card, a bank processes the transaction. When a person exchanges cash at a supermarket, the reliance is on the government to print and supply that cash to its users. In the first case, the bank handles verification of the transaction. In the second case, the cash has inherent value and is immediately made available to whom it is owed, so the only verification necessary is that the cash is real (which the government ensures through an extensive and secure printing process).

The commonality in both cases is that the currency is centralized, meaning that it is handled by an authority in charge of its distribution and verification. Banks and governments work together to provide a stable exchange economy for its users. Now imagine removing these authorities from the picture. How would we be able to supply money to users and make sure that transactions are valid? Cryptocurrency answers by giving that same power to the users themselves. By using cryptographic techniques to verify transactions and rewarding those who verify transactions with new currency, we simultaneously provide security and a steady money supply all while creating an inherent form of value. This process is famously dubbed "peer-to-peer" (P2P) verification.

2.2 How does P2P Verification Work?

Satoshi Nakamoto, the mysterious inventor of Bitcoin, the first ever cryptocurrency, published a white paper [1] in 2008 on the proposed structure of a P2P system that is used today by Bitcoin. Nakamoto's identity is to this day unknown, however, he speculated to hold a five percent stake in his invented cryptocurrency.

We will explore in detail the outline of his paper to get a general sense of the system at work, however it is highly encouraged that the reader references the complete paper. Nakamoto "define[s] an electronic coin as a chain of digital signatures ... A payee can verify the signatures to verify the chain of ownership." Think of this chain as a public ledger such that anyone can state a transaction that one has made on it. In order for a transaction on this ledger to be considered valid, the payee must verify that she agreed to the transaction. As such, let her verify this through a digital signature. For now, imagine this as a handwritten signature identical to the one needed after making a transaction with a credit card (we

will clarify the cryptographic function later). So far, we have a ledger in which each transaction listed is considered to be true and in which each person has the net amount that has been transferred throughout the ledger, starting with what that person entered with.

For this system to work, the ledger must be completely trusted. Thus, we need a way to prevent any agent from double spending, or, equivalently, forging signatures. Nakamoto's solution is as follows: encrypt each signature using ECDSA and SHA-256 (we will elaborate more on this in the next section), create a timestamp for each verified transaction, and only trust the largest chain of transactions. The reasoning for this is that the computing power necessary to validate each transaction will always exceed any single agent attempting to redo a proof-of-work. We will later examine the attacker scenario and show that it is probabilistically infeasible.

We have briefly outlined the P2P protocol, but now the question remains: where does Bitcoin (or any cryptocurrency) achieve its value? So far we have represented the ledger with transactions in currency we are familiar with. Now, imagine that the currency is actually the ledger itself! We will supply new currency to anyone who verifies a new list of transactions. This not only incentivizes public verification, but also initiates a value sentiment, such that anyone willing to verify transactions will also be willing to make transactions with her newly supplied currency. Thus, we have a self-fulfilling system where the users are also the authorizers. Any amount of cryptocurrency that a participant on the ledger owns entered the ledger from a previous verification, starting at the epoch, or first ever verified list of transactions on the entire ledger. As such, cryptocurrency achieves its value simply through its users' agreement to its value, as with any form of currency, asset, or commodity.

3 Overview of the Mathematics behind Bitcoin

In this section, we will go over the entirety of the Bitcoin Protocol. Bitcoin, being the oldest and most widely used cryptocurrency, initiated the idea of a decentralized currency. Since then, many new cryptocurrencies have been founded using similar technology, and many still have improved upon the drawbacks of Bitcoin. In this paper, we will focus primarily on Bitcoin to give an overview into the functionality of cryptocurrency in general. This will, by no means, cover every aspect but it will function as a very in-depth introduction to what goes on under the hood in the world of cryptocurrency.

3.1 High Level description of Secure Hashing

The SHA-256 algorithm is a secure hash algorithm (hence the abbreviation) that takes as input a message (some form of data) and sends as output a string of 256 bits, i.e. 1's and 0's. The main heuristic is that even a slight change in the input will lead to an entirely different output, thus making it infeasible to inverse the map quickly. What is amazing about this algorithm is that no matter what the input is, we will always be left with a verifiable string of 256 bits that appears to be random even though it is not. In addition, the reader should note that it is possible for two different inputs to generate the same output, but given that the image of the function has 2^{256} possibilities, it is incredibly unlikely. Thus, in function notation:

$$\begin{aligned} &\text{SHA256} : M \to (\mathbb{Z}_{/_2})^{256} \\ &\text{SHA256}(m) = b \\ &m \in M, b \in (\mathbb{Z}_{/_2})^{256} \end{aligned} \tag{3.1}$$

Where M is the space of all possible messages, m is a message in M, and b is a binary string of length 256. As previously noted, the function is surjective since the space of possible messages is infinite while the image space is finite. There has been no inverse function correctly implemented to date and it is assumed that breaking a SHA-256 hash is close to impossible bar quantum computing, which we will harp on later. The actual process is incredibly complex and outside the scope of this paper so we will leave it to the reader to explore the exact steps if he or she wishes to.

The use of SHA-256 is a step included in the overarching Bitcoin protocol to enhance the security of transactions. A second hashing algorithm, known as RIPEMD160, is used in conjunction with the SHA-256 hashing algorithm to generate Bitcoin addresses. We will discuss this in more detail later on, but the heuristic is the same. RIPEMD160 generates a shorter output than SHA-256, thus the combined use allows for users to have shorter Bitcoin addresses and makes it even less likely to have collisions, i.e. two different addresses with the same hash.

3.2 Elliptic Curve Digital Signature Algorithm (ECDSA)

The elliptic curve digital signature algorithm, or ECDSA, is the bread and butter of Bitcoin. It is the technique used to verify that transactions between users. Elliptic curve cryptography is a form of cryptography that allows for messages to be sent and verified securely contingent on the sender keeping her private key, which is a very large random integer, secret. In the case of Bitcoin, this message would contain the transaction between two parties where the private key would belong to the sender. If we can verify transactions and ensure that senders spend willingly only once, then we can maintain a secure network of transactions.

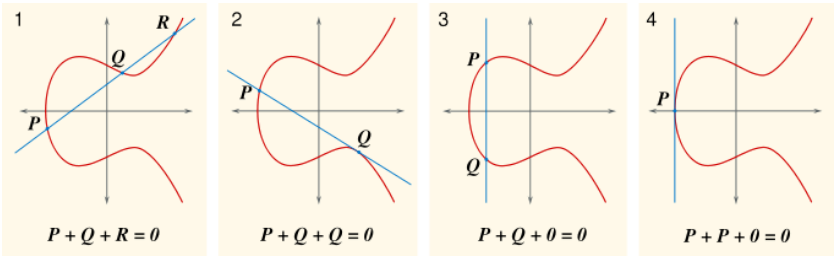
We must first clarify the definition of elliptic curve and its operation.

Definition 1. Elliptic Curve
An elliptic curve (under ECDSA parameters) is a plane algebraic curve defined by an equation of the form

$$y^2 = x^3 + ax + b \tag{3.2}$$

that is non-singular, i.e. it has no cusps or intersections. It has a multiplication defined algebraically with respect to which it is an abelian group, meaning that its multiplication is commutative.

When we add points on on elliptic curve, we draw a line between them, pick the third point of intersection, and reflect across the x-axis to achieve the result. Thus, scalar multiplication draws a tangent line from the original point, and continues the process iteratively based at that point.



Visually, we can observe that reflecting the final point will yield the result of the operation. The above visually represents an elliptic curve with the real domain, however, when used for cryptography, we usually define the curve over the field of integers modulo a large prime. In fact, primes are usually chosen to be pseudo-Mersenne, or of the form $p \approx 2^d$. This allows for faster computation when verifying digital signatures. We want to have a large enough field to ensure cryptographic security, but finiteness is a necessary aspect of computational feasibility.

3.2.1 Elliptic Curve Fields

We define our elliptic curve over the field $\mathbb{F}_p$ where p is a large prime as previously discussed. Let us briefly go over the properties of $\mathbb{F}_p$ and the operations defined on it.

Definition 2. Finite Prime Field

A finite prime field $\mathbb{F}_p$ has p elements such that $\{0, 1, ..., p-1\} \in \mathbb{F}_p$. For all $a, b \in \mathbb{F}_p$, if $a + b, a \times b \in \mathbb{F}_p$,

$$a + b \equiv a + b \bmod p$$
$$a \times b \equiv a \times b \bmod p.$$

Here $+$ and $\times$ denote regular addition and multiplication respectively. Note if $a + b = k \cdot p$ for some integer k, then $b \equiv -a \bmod p$ and $a + b \equiv 0 \bmod p$. In the case of (3.2), $y, x, a, b \in \mathbb{F}_p$.

When we define scalar multiplication over a elliptic curve, such as an integer m multiplied by a point $P = (x_1, y_1)$, we mean $m \times P = \underbrace{P + P + ... + P}_{m \text{ times}} = (x_2, y_2)$ where each $x, y \in \mathbb{F}_p$ and $+$ is elliptic curve addition of two points as previously defined. Since $\mathbb{F}_p$ is a finite field, we have finitely many possible (yet very many) points (x, y) on the elliptic curve defined over $\mathbb{F}_p$. For more information on prime fields, see [2].

3.2.2 ECDSA Recipe

We will now go over the general recipe for ECDSA and provide the parameters specific to Bitcoin. Suppose person A wants to send a signed message to person B. Both people must first agree on and have access to the following parameters:

1. An elliptic curve field, Ω, and the equation used, E.
2. The curve base point, G, a generator of the elliptic curve with large prime order n.
3. Integer order of G, denoted n, such that $n \times G = 0$ where $\times$ denotes elliptic curve scalar multiplication.

Once persons A and B have agreed on these parameters, person A creates a key pair, consisting of a private key and a public key.

1. The private key, d_A, is an integer randomly chosen on the interval $[1, n-1]$. Person A must keep d_A secret to maintain cryptographic security.
2. The public key, Q_A, is a curve point and is equivalent to $d_A \times G$ (note that the interval we choose d_A on avoids a public key equivalent to the identity). The public key is known by everyone.

3.2.3 Signature Generation

Now that we have settled preliminary definitions, we explore the steps person A takes to sign message m:

1. Calculate $e = \text{HASH}(m)$ where HASH is a cryptographic hash function.
2. Let z be the L_n leftmost bits of e, where L_n is the bit length of the group order, n.
3. Select cryptographically secure random integer k from $[1, n-1]$.
4. Calculate the curve point $(x_1, y_1) = k \times G$.
5. Calculate $r = x_1 \bmod n$.
6. Calculate $s = k^{-1}(z + rd_A) \bmod n$. If $s = 0$, go back to step 3.
7. The signature is the pair (r, s).

The string z resulting from $\text{HASH}(m)$ is converted to an integer. z can be greater than n but not longer, hence why step 2 is necessary.

k must be cryptographically secure for the signature to be valid, otherwise we can reverse calculate d_A through step 6 by solving $d_A = \frac{ks-z}{r}$. Furthermore, k should vary for each signature. Otherwise, given two signatures (r, s) and (r, s'), an attacker could calculate $s - s' = k^{-1}(z - z')$ which leads to $k = \frac{z-z'}{s-s'}$ which leads to d_A being compromised (the previous operations are all mod n).

3.2.4 Signature Verification

Now that person A has signed her message, it is up to person B to verify the signature. It is assumed person B has a copy of person A's public-key curve point Q_A in addition to her signature pair (r, s).

First, some preliminary steps

1. Check that Q_A is not equal to the identity element O, and its coordinates are otherwise valid.
2. Check that Q_A lies on the curve.
3. Check that $n \times Q_A = O$.

Now that the public key is considered valid, we begin verifying the signature:

1. Verify that r and s are in $[1, n-1]$. If not, the signature is invalid.
2. Calculate $e = \text{HASH}(m)$, where HASH is the same function used in signature generation.
3. Let z be the L_n leftmost bits of e.
4. Calculate $w = s^{-1} \bmod n$.
5. Calculate $u_1 = zw \bmod n$ and $u_2 = rw \bmod n$.
6. Calculate the curve point $(x_1, y_1) = u_1 \times G + u_2 \times Q_A$. If $(x_1, y_1) = O$ then the signature is invalid.
7. The signature is valid if $r \equiv x_1 \pmod n$, invalid otherwise.

Claim. *The above algorithm is correct: Let $C = (x_1, y_1) = u_1 \times G + u_2 \times Q_A$. Then $C = k \times G$ as well.*

Proof.

$$C = u_1 \times G + u_2 \times Q_A$$

Under the definition $Q_A = d_A \times G$,

$$\begin{aligned} C &= u_1 \times G + u_2 d_A \times G \\ &= (u_1 + u_2 d_A) \times G. \end{aligned}$$

Expanding the definition of u_1 and u_2,

$$\begin{aligned} C &= (zs^{-1} + rd_A s^{-1}) \times G \\ &= (z + rd_A)s^{-1} \times G. \end{aligned}$$

Under the definition $s = k^{-1}(z + rd_A)$, we have that $s^{-1} = (z + rd_A)^{-1}(k^{-1})^{-1} = (z + rd_A)^{-1}k$. Therefore,

$$\begin{aligned} C &= (z + rd_A)(z + rd_A)^{-1} k \times G \\ &= k \times G. \end{aligned}$$

□

Thus, ECDSA is cryptographically secure and signatures are verifiable using only the public key.

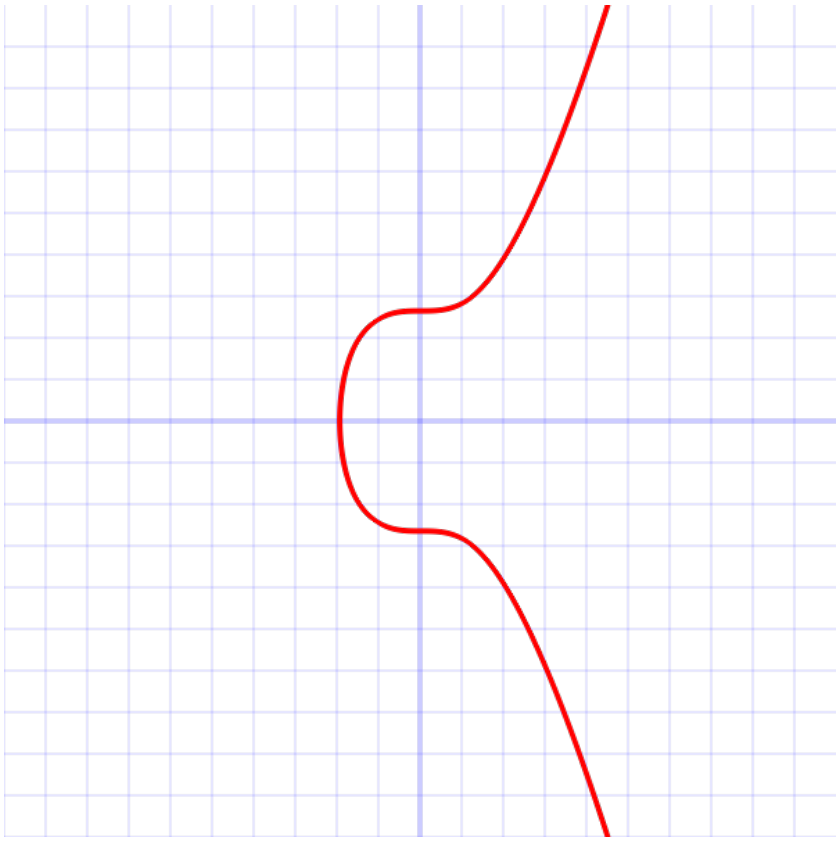
3.2.5 The Bitcoin Specific Paramaters of ECDSA

With ECDSA defined, we can now assign the parameters that Bitcoin uses. Although these values appear arbitrary, they are selected so that signing and verification may occur quickly. This research predates the founding of Bitcoin in the paper *Standards For Efficient Cryptography* [3] and the parameters used by Bitcoin are known as secp256k1.

We define the parameters as follows: [4]

1. The hash is defined by HASH = SHA-256.
2. m is a message containing a transaction amount.
3. The elliptic curve field Ω is defined as the field of integers mod a large (pseudo-Mersenne) prime:
   (a) $\Omega = \mathbb{Z}_p$
   (b) $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^6 - 2^4 - 1$
4. The curve equation is defined as
$$E : y^2 = x^3 + 7.$$
5. The base point, in compressed hexadecimal form, is
$$G = 02\ 79BE667E\ F9DCBBAC\ 55A06295\ CE870B07\ 029BFCDB\ 2DCE28D9\ 59F2815B\ 16F81798$$
6. The order of G, in hexadecimal, is
$$n = FFFFFFFF\ FFFFFFFF\ FFFFFFFF\ FFFFFFFE\ BAAEDCE6\ AF48A03B\ BFD25E8C\ D0364141$$

Visually, our curve looks as follows:



This is a representation over the real numbers, however if we were to represent the curve as previously defined, the curve would look like random scattered points. Since we define the curve over a finite field, we still have the same properties when defining point multiplication, although now the problem of signature generation and verification is computationally feasible.

3.3 Blockchain - Proof of Work

For each individual transaction, the sender and receiver use ECDSA: the sender signs the transaction and the receiver verifies the signature. This ensures that there is security between individuals. But how do we know exactly how many Bitcoin are in possession by the sender? What if the sender is trying to send more than what she owns or "double spend" her Bitcoin? This is where the blockchain comes into effect. The blockchain works as a ledger containing every Bitcoin transaction ever made. In this way, we can keep track of how much Bitcoin anyone owns at a given time, thus enabling us to have an effective and valid system of transactions.

The blockchain works as a public network. Each new transaction must be broadcast to every node in the network. Now comes the interesting part: each time a new transaction is added, it is first confirmed between the two parties involved via ECDSA. It must then be confirmed a second time via a proof-of-work algorithm. The proof-of-work algorithm involves doing a large amount of computational work to essentially create a timestamp that proves something existed at a certain time.

For Bitcoin, this involves using SHA-256 to hash the list of transactions to a string of 256 bits that must begin with a preset number of zeros. The process has been famously dubbed "mining" since each new verified block rewards the node with the correct hash with new Bitcoin. Let all non-hashed transactions be contained in a string B. This is known as a new block. Then each node in the network has an opportunity to hash this block to the correct string. The following pseudo-code describes the mining process:

while HASH(B) $\neq$ Correct # of Zeros:
    Add new transactions to B
    Add random symbols to end of B
    HASH(B)

Once B is hashed to the desired number of zeros, it is considered to be verified and each transaction receives a second confirmation. We then append B to the chain of all preceding blocks and continue the process. The most fascinating process about blockchain technology is its main heuristic: We need only trust the longest chain of blocks i.e. the one with the most computational work done on it. If an attacker were to try to add a false transaction to the blockchain, then she would have to redo the proof-of-work for *every* single block in the chain since each transaction must be traceable to the source.

3.3.1 Mining: Rewards and Increasing Difficulty

Since Bitcoin's founding in 2008, computers have increased in power exponentially. Mining Bitcoin is a sheer force process. Therefore, the user with the most computing power is the most likely to win the block reward since the block reward is designated to the miner who first hashes to the correct number of zeros. Thus, Satoshi implemented a clever way to combat the ever increasing nature of computing power. The difficulty of mining increases exponentially in the number of zeros required at the front of the hash. Let z be the number of required zeros. Then the probability of hashing to the correct number of zeros is $\frac{1}{2^z}$. So to increase difficulty, we must merely increase the number of zeros required at the front of the hash. A zero is added to the required number of zeros every 2016 blocks, or roughly every 2 weeks [5]. Note that difficulty can *decrease* under certain circumstances, such as if the latest 2016 blocks took longer than 2 weeks to mine [6].

In addition, the number of Bitcoin rewarded to each successful hash is cut in half rougly every four years. In 2008, the hashing reward was 50 BTC. Since then, it has scaled down to 25, and today is 12.5. In fact, the total number of Bitcoin in circulation is capped at 21,000,000, which is projected to occur in 2140. As a further incentive to mine, miners also receive a small percentage of each transaction as a transaction fee. This is to make up for the incredibly unlikely nature of actually receiving the block reward and the immense cost of electricity required to mine. Miners will usually

collaborate in guilds to increase the likelihood of receiving new Bitcoin; guilds, then, will share the reward amongst its users proportional to each user's contributed computing power.

3.3.2 Attacker Scenario

Satoshi outlines in his whitepaper an attacker scenario where an attacker attempts to create a new chain faster than the honest chain. We have previously recognized that, due to ECDSA, an attacker cannot forge a transaction out of thin air or "steal" from an unwilling address (since it would be unsigned). Rather, an attacker must create a completely new chain that can be traced to the root such that the transaction is considered legitimate. Otherwise, an attacker can attempt to take back any Bitcoin that she recently spent so to double spend. For this to happen, she must find the next block faster than the majority mining party.

The idea is that this is computationally infeasible. Given that the incentive to "honestly" mine exceeds the incentive to defect from the true blockchain, we can safely assume that an attacking party would have significantly less computing power than the majority of miners. We will outline this scenario mathematically as from the whitepaper.

We characterize this race as a binomial random walk. The success event is the honest chain being extended by one block, increasing its lead by $+1$, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1. The probability of an attacker catching up from a given deficit is identical to the Gambler's Ruin problem. Suppose a gambler has unlimited cash starting at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We model this scenario as follows:

$$
\begin{aligned}
p &= \text{probability an honest node finds the next block} \\
q &= \text{probability an attacker finds the next block} \\
q_z &= \text{probability the attacker will ever catch up from z blocks behind} \\
q_z &= \begin{cases} 1 & \text{if } p \leq q \\ (\frac{q}{p})^z & \text{if } p > q \end{cases}
\end{aligned}
$$

Given our assumption that $p > q$ (in practice, much, much greater than), the probability becomes exponentially smaller as the number of blocks the attacker is behind of increases.

3.3.3 How long do we need to wait to trust a new block?

Satoshi Nakamoto outlines the answer to this question beautifully in the whitepaper. We assume a situation where we have a villain, V, and an unsuspecting, yet skeptical, user, U. Here, V is sending Bitcoin to U, except he wants U to believe he has received the transaction only to then reverse this transaction after some time has passed. U will know once this happens, but V hopes it will be too late.

U generates a new key pair and gives the public key to V shortly before signing. This ensures V cannot prepare a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead and then execute the transaction at that moment. Only after the transaction is sent can V begin to work in secret on a parallel block that reverses the transaction.

U then waits until the transaction has been added to a block and z blocks have been linked after it. Assuming honest blocks take an average expected time per block, V's potential progress will be a Poisson distribution with expected value

$$\lambda = z\frac{q}{p}.$$

Thus, the probability P that V could still catch up now is the Poisson density for each amount of progress he could have

made multiplied by the probability he could catch up from that point, i.e.

$$P = \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot f_z$$

where

$$f_z = \begin{cases} (\frac{q}{p})^{z-k} & \text{if } k \leq z \\ 1 & \text{if } k > z \end{cases}$$

which we can rewrite as

$$P = 1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \big(1 - (\frac{q}{p})^{z-k}\big).$$

Even if V had computational power such that $q = 0.1$ i.e. V has a 10% chance to find the next block, we would only need to wait until $z = 5$ until $P < 0.001$. Realistically, any attacker would have an exceptionally small probability of finding the next block, so it is commonplace to accept a transaction is valid after $z = 2$ where two more blocks have been mined on top of the block your transaction lives in. Additionally, we only need to trust the longest blockchain since this chain has had the most computational work done it. Since we assume the majority of computing power belongs to honest nodes, the longest chain will be honest with the highest probability. The incentive given by mining honestly ensures that this is the case. For some simulations of this scenario, see [1].

4 Economic Analysis of Cryptocurrency

Since its founding, Bitcoin has surged in popularity at an exponential rate, giving rise to immense valuation increase. Up until this point in the paper, we have used Bitcoin to describe the underlying mathematics of what is really going on behind cryptocurrency. Of course, there are many other cryptocurrencies that have immerged in the wake of Bitcoin, many of which have significantly different proposed functionality and use cases. As of April 2018, the top 5 cryptocurrencies in order of market cap are:

1. Bitcoin (BTC)
2. Ethereum (ETH)
3. Ripple (XRP)
4. Bitcoin Cash (BCH)
5. Litecoin (LTC)

Each of these coins differ in functionality in a number of ways, however the underlying systems are based on the foundation of Bitcoin. We will briefly outline the use cases for some of the top coins in market cap later on.

The following section will focus on these questions:
Why has cryptocurrency surged in value? How do you get it? Why is there so much variance day-to-day? Are there any significant advantages to using cryptocurrency over legal tender?

There are massive discrepencies over the opinions surrounding cryptocurrency, which based on several schools of thought. We will do our best to remain unbiased in providing the correct insight and evaluation of cryptocurrency in general.

4.1 Exchanges: How to Acquire and Trade Cryptocurrency

Cryptocurrency is strange in that the most difficult and time consuming aspect of acquiring it comes from transitioning from fiat currency to cryptocurrency. Only a few exchanges in the world offer this platform and usually allow purchase of

cryptocurrency through linking a bank account or credit/debit card. Coinbase[1] is a San Fransisco based crypto-exchange and is the most popular exchange in the United States as it offers purchase of major cryptocurrencies using USD. We will use Coinbase to explain the process of acquisition throughout this section, although user experience may differ depending on the platform he or she chooses.

Let's examine the case where a user, call her Alice, wishes to purchase Bitcoin. She hears about Coinbase through the internet and decides to set up an account. Coinbase requires identity verification before allowing its users to purchase cryptocurrency. Alice sends an image of her driver's license and receives confirmation roughly three days later (this time varies depending on external circumstances). She then links her bank account and credit/debit cards allowing her to purchase Bitcoin at Coinbase's price. This process usually takes up to five business days when buying or selling. In addition, the price may or may not differ from prices on certain other major exchanges, such as Bitfinex, a EU based exchange, or OKEx, a Korean based exchange. Coinbase charges a 3% fee, making it suboptimal.

In fact, Coinbase has its own exchange known as GDAX[2] [7] where any user can buy/sell major cryptocurrencies to any other user on the exchange. GDAX has no "maker" fees, meaning that if a user makes a limit order that differs from market price, she will be charged no fee. If a user buys or sells at market price, which would designate them as a"taker", they are charged a 0.25% fee (this fee decreases if the user exceeds a large 30-day volume). When an order is made on GDAX (or any exchange), the order is filled as soon as possible, and it is filled almost instantly at market price. Any Coinbase user can make a GDAX account once her identity is verified. Alice, knowing that GDAX offers little to no fees, decides to create her own GDAX account.

To transfer funds (in USD) from Coinbase to GDAX, a user must first either transfer USD from her bank account to a USD wallet on Coinbase, which operates similar to a Bitcoin wallet in that transfers only require two addresses, or transfer directly to GDAX from her bank account using a bank wire or bank transfer. Wires usually have a $10 fee and are usually same-day while transfers take 5-10 business days. Alice decides that time is not an issue and proceeds with a bank transfer of $500 to GDAX. Her $500 arrives in her GDAX account five days later.

Up until this point, Alice has spent eight days getting her account set up and still has not yet purchased or traded any Bitcoin. Well, she is now in luck, as GDAX allows for extremely quick transactions between users at little to no cost. She now places a limit order of Bitcoin slightly below market price for all $500 she has in GDAX and her order is filled five minutes later. Now, all her USD has been traded for Bitcoin and she may withdraw her Bitcoin to any of her other Bitcoin addresses. As of now, her Bitcoin is "located" in the Bitcoin address provided by GDAX, meaning that the amount she purchased has been transferred from another address within GDAX using ECDSA, broadcast to all other nodes in the blockchain network, and is awaiting or has received blockchain verification using proof-of-work. It is important to note that any crypto-exchange merely keeps track of the purchases an individual has made since actual verification takes on average ten minutes. In addition, users making a transaction using Bitcoin will have their transaction verified faster if they pay a small fee to incentivize miners.

What separates exchanges like GDAX from the vast majority of other crypto exchanges is that they offer **fiat-to-crypto** conversion. There are thousands of other exchanges operating with similar functionality that only allow trading once a user has sent **cryptocurrency** to their exchange account's relevant address. This creates a massive liquidity bottleneck such that when users want to enter or exit the crypto markets, i.e. convert from fiat to crypto and vice versa, there are large delays and some fees depending on the exchange and cryptocurrency being used. Coins with smaller market cap are much harder to liquefy since many of them are only offered on exchanges that do not have fiat conversion.

Alice's value is now determined by the volatility of the market, which is driven by the supply and demand for Bitcoin. When supply exceeds demand, the price for Bitcoin decreases. Similarly when demand exceeds supply, the price for

[1] https://www.coinbase.com/dashboard
[2] https://www.gdax.com

Bitcoin increases. The price therefore indicates the ever changing supply and demand for Bitcoin.

4.2 Valuation of Cryptocurrency

Unlike stocks, cryptocurrencies lack many useful underlying measurements of performance such as Revenue, Profit Margin, Price to Earnings, etc. Therefore, it is difficult to measure the true value of any cryptocurrency. This gives way to massive fluctuations and overall speculative value. Anyone willing to purchase cryptocurrency most likely assumes that the value will increase in the future since the aforementioned liquidity bottleneck leads to suboptimal usage as an actual currency. A cryptocurrency is therefore (in the vast majority of cases) merely a store of value similar to a commodity like gold with the functionality of a true currency for anyone on the same cryptocurrency network. Many cryptocurrencies do, however, seek to solve a pre-ordained problem or apply to a specific use case. These problems / killer-applications include but are not limited to file storage (Filecoin), computing power (Ethereum: ETH, Golem: GNT), internet of things (IOTA), data (Datacoin: BTC), anonymity (Zcash: ZEC, Monero: XMR) etc. Thus, it is also the case that a user interested in one of these killer-applications may invest in a corresponding cryptocurrency. In this way, cryptocurrency can also be seen as an application of market dynamics to a problem, i.e. a public decree of value sentiment regarding one of the aforementioned use-cases.

A secondary usage of cryptocurrency is for the purchase of illegal goods on online black markets. Cryptocurrency transactions are incredibly difficult to trace back to a source user making them ideal for illegal trade. It is difficult to measure the exact percentage volume of cryptocurrency transactions that are allocated to the black market, but when major black-market exchanges are shut down by governments, large amounts of digital assets are often seized. For this reason, cryptocurrency has received backlash, however black markets have existed long before the existence of cryptocurrency and we can safely assume that it is not causing a surge in online crime, but merely aiding it. It may be the case, however, that online black markets are causing a surge in the value of select cryptocurrencies such as Monero, which are founded on transaction anonymity.

As of 2018, there exist nearly 1500 different cryptocurrencies and over 8200 crypto markets and exchanges. Given that the number of exchanges is over five times the number of cryptocurrencies being traded, there is a great deal of price disparity between exchanges. This, among the many following reasons, gives way to the large volatility of the cryptocurrency market. Most of these exchanges are unregulated and trade 24/7. There is no limit as to how large an order can be, thus these markets are subject to heavy price manipulation by parties with large enough capital. Any new cryptocurrencies released via an "ICO," or Initial Coin Offering, are extremely vulnerable to price manipulation given that any large capital investor can drive the price up and down at her whim. These schemes have been commonly dubbed "pump and dump" schemes performed by "whales," or any investor with a large amount of capital staked (roughly $5+ million) in cryptocurrency. The whale will inject, or pump, large amounts of capital into a new and vulnerable coin, causing an immediate surge in price, bringing in outside buyers who wish to "ride the wave" ending with the whale selling-off, or dumping, to the hopefuls that have been brought on board; this leads to a large drop in the price. Such schemes are far more difficult in the stock market since wealth is distributed across a far wider array of participants. Thus, the crypto markets move much faster and with far more volatility than any other publicly traded market worldwide:

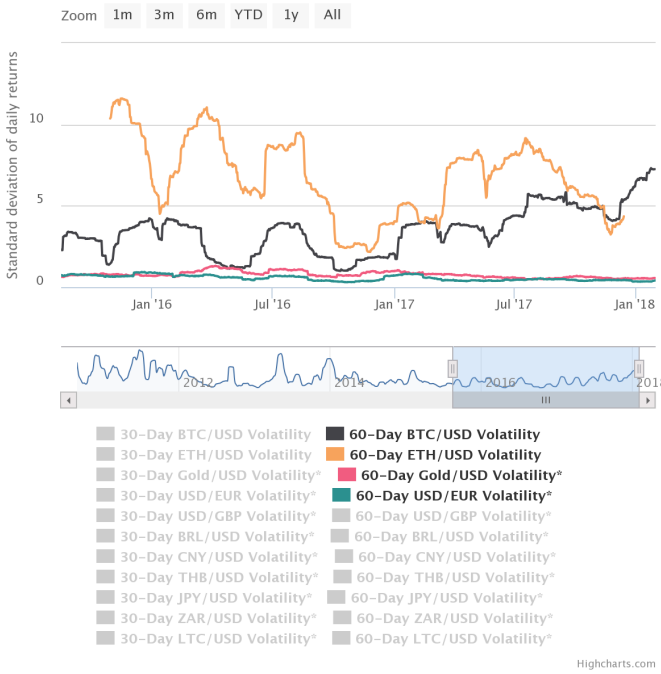


Figure 1: Source: https://www.buybitcoinworldwide.com/volatility-index/

While most commodities and currencies have a volatility of about 1%, The two largest cryptocurrencies by market capitalization, Bitcoin and Ethereum, average about 7.5%.

4.3 Major Investors

There are few large financial entities who have publicly declared major investments into cryptocurrency. It is true, however, that over 95% of Bitcoin are owned by roughly 4% of addresses. This can be confirmed via blockchain.info [9] which publicly displays the worth of any Bitcoin address. Since Bitcoin, as of April 2018, dominates over 40% of the entire cryptocurrency market capitalization, we will assume that the majority of all cryptocurrency holdings belong to a small group.

Satoshi Nakamoto, the mysterious inventor of Bitcoin, is assumed to have mined 1 million BTC, roughly 5% of all Bitcoins ever to be mined, in the early days of Bitcoin distributed over a small number of addresses. It is of course impossible to confirm this given the anonymity of Satoshi's true identy, however, many addresses that hold over 100,000 BTC exist on the blockchain.

To achieve a better understanding of wealth distribution in the cryptocurrency space, we will use a chart provided by bitinfocharts.org which aggregates data from blockchain.info:

Bitcoin distribution

Balance	Addresses	% Addresses (Total)	Coins	$USD	% Coins (Total)
0 - 0.001	15301386	55.95% (100%)	2,663 BTC	27,135,905 USD	0.02% (100%)
0.001 - 0.01	5406088	19.77% (44.05%)	23,137 BTC	235,725,318 USD	0.14% (99.98%)
0.01 - 0.1	4228843	15.46% (24.29%)	135,235 BTC	1,377,818,086 USD	0.81% (99.85%)
0.1 - 1	1719601	6.29% (8.82%)	548,311 BTC	5,586,390,001 USD	3.27% (99.04%)
1 - 10	544346	1.99% (2.54%)	1,446,420 BTC	14,736,640,139 USD	8.63% (95.77%)
10 - 100	132184	0.48% (0.55%)	4,373,770 BTC	44,561,531,850 USD	26.09% (87.14%)
100 - 1,000	15701	0.06% (0.06%)	3,710,851 BTC	37,807,472,831 USD	22.13% (61.06%)
1,000 - 10,000	1512	0.01% (0.01%)	3,362,974 BTC	34,263,180,441 USD	20.06% (38.92%)
10,000 - 100,000	108	0% (0%)	2,738,466 BTC	27,900,465,181 USD	16.33% (18.86%)
100,000 - 1,000,000	3	0% (0%)	424,393 BTC	4,323,865,707 USD	2.53% (2.53%)

Addresses richer than

1 USD	100 USD	1,000 USD	10,000 USD	100,000 USD	1,000,000 USD	10,000,000 USD
19,371,768	6,732,356	2,452,983	721,913	153,716	18,247	1,715

Figure 2: Source: https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html

Other Major Bitcoin investors who have been publicly identified include (but are not limited to):

1. The Winklevoss Twins - Former Olympic rowers, angel investors, and co-founders of cryptocurrency exchange Gemini - Claim to own 1% of all Bitcoin in circulation, or roughly $1.3 Billion worth.
2. The US Government - Seized 144,336 BTC from Ross Ulbright in 2013, former leader of online black market Silk Road. Worth roughly $ 1.2 Billion - They since auctioned off their Bitcoin to the Public
3. Barry Silbert - Venture Capitalist and founder of Digital Currency Group - Purchased 48,000 BTC at the same US Government auction
4. Tim Draper - Venture Capitalist Billionaire who invested early in Skype - Purchased 30,000 BTC from US Government auction
5. Charlier Shrem - Early Bitcoin adopter - reportedly has a few thousand BTC although the actual amount is undisclosed.
6. Tony Gallippini - Cofounder and chairman of Bitpay, a platform for coin storage and processing - Speculated to own Bitcoin in the thousands although true amount is undisclosed.

The previous valuations use prices as of April 2018.

Given that the number of wallets exceeding 10,000 BTC is in the hundreds, there are likely to be many anonymous Bitcoin "whales" out there, but of course there is no way of knowing for sure. Anonymity provides several benefits to these large holders, such as protection from hacking and taxation. It is likely that anyone holding a large amount of cryptocurrency would prefer to store their funds in an external wallet, meaning that their private key would be stored in a physical hard drive such that only the user would have access to it.

Major investors outside of Bitcoin would include many creators of other cryptocurrencies which have reached a large market cap. Most of the time, creators of new cryptocurrencies hold a large number of their creation.

Some of these publically identified creators include (but are not limited to):

1. Vitalik Buterin - Co-Creator of Etheruem (ETH) - Prospected to own roughly 500,000 ETH ($450 mil).
2. Chris Larsen - Creator of Ripple (XRP) - Prospected to own roughly 5.9 bil XRP ($6.8 bil).
3. Charlie Lee - Creator of Litecoin (LTC) - 5-10% stake in LTC ($1.5 bil). Has since sold his stake[3].
4. Charles Hoskinson - Co-Creator of Ethereum and Creator of Cardano (ADA) - Unknown Stake

[3]https://www.cnbc.com/2017/12/20/litecoin-founder-charlie-lee-sells-his-holdings-in-the-cryptocurrency.html

5. David Sonstebo - Creator of IOTA (IOTA or MIOTA) - Unknown Stake

The irony of cryptocurrency creators holding a large stake in their own coin is that it takes away from the decentralization aspect of what cryptocurrency was founded on. Of course, anyone who creates a form of value is entitled to an amount of that value. However, keeping a large chunk of money supply from reaching the public creates a sense of centralized control. For instance, if at any point a creator sells their stake, she can dramatically affect the value of her own currency. Furthermore, holding indefinitely leads to the problem of artificial rarity, such that no matter what the money supply is, a certain fraction will never be available for public transaction. This, in theory, inflates the price of said asset, benefiting the holder. Cryptocurrency thus by no means diverges from the common saying, "the rich get richer."

4.3.1 Cryptocurrency: Commodity or Currency

Cryptocurrency functions as a currency in that at any point its value can be traded for something of equal worth. However, that value moves exceptionally quick and with large deviations, making this store of value unsafe. Fiat currency, on the other hand, does not change in value quickly or with large deviations, making it safe for long term storage. Any risk averse person would likely avoid cryptocurrency. However, despite its volatility, cryptocurrencies in the top tier of market capitalization still seem to have long-term growth potential, unlike fiat currency, which loses value over time due to inflation. Cryptocurrencies are also less liquid: if at any point one wishes to spend her cryptocurrency, she must first convert to fiat, unless of course the transacting party agrees to accept cryptocurrency, which is uncommon. Thus, cryptocurrencies do function as currencies, but not in the same way as fiat currencies other than in tradability.

Undoubtedly, cryptocurrency is a store of value, but it functions in a way never before seen by the current economy. It is backed by no other form of value, in most cases has no inherent use other than tradability, and is always available to trade. The most common comparison to cryptocurrency, especially Bitcoin, is gold. Gold functions primarily as a store of value, but it also has functional use, such as in jewelry, wiring, and dental implants. Gold is seen as a safe investment, as its value moves somewhat independently of the stock market and fiat inflation. Gold can be mined but is also rare and limited, thus making it difficult to acquire without trading. Lastly, and perhaps more importantly, it is decentralized, meaning transacting in gold does not necessarily rely on a central authority or bank. So, in all ways except practical, Bitcoin and gold are quite similar.

Compared to other cryptocurrencies, Bitcoin is the most "gold-like" since it carries, by an order of magnitude, the most value per unit and rarity. Litecoin has been quoted by its founder, Charlie Lee, to be "the silver to Bitcoin's gold," meaning that it is meant to mimic the store of value in a "lighter," more achievable manner. Litecoin is cheaper, easier to mine, and faster to transact. Similarly, silver is cheaper, more abundant, and literally lighter than gold. These comparisons of cryptocurrency to precious metals is thus perhaps the best way to analogize these digital assets. However, it is true that cryptocurrencies are more liquid than precious metals, especially if the metals are stored tangibly.

Cryptocurrency thus has similarities to both commodities, especially precious metals, and fiat currency. It is a digital asset that grows with time, bar a crash, and can be traded in exchange for goods in a semi-liquid fashion. It is important to note that the U.S. Commodity Futures Trading Commission (CFTC) has ruled that cryptocurrencies like Bitcoin are commodities[4].

4.4 Major Drivers

What drives the value of cryptocurrency? Why does it dominate the news as of 2018? Up until this point in the paper, we have focused on what defines cryptocurrency from a mostly functional standpoint, but in this section we will focus on how the public has shaped the cryptocurrency space into what it is today. Fall 2017 saw an exponential surge in cyrptocurrency value. Following this surge was a large correction that caused most cryptocurrencies to dip down to 60% of their peak

[4]http://fortune.com/2018/03/07/bitcoin-cftc-commodities-coin-drop-markets/

value.

4.4.1 Momentum

As cryptocurrencies began to see more attention from the public eye, their value surged with it. This brought in even more attention, leading to more buying volume and more price surging. Those who held were ecstatic and those who didn't were beginning to fear missing out. This phenomenon drives the momentum of any asset, in this case cryptocurrency. Momentum in markets seems to be a psychological factor, but works nearly identically to its physical definition. In physics, we have that

$$p = mv$$

where $p =$ momentum, $m =$ mass, and $v =$ velocity. In an economic setting, we define market momentum as

$$p = mv$$

where $p =$ momentum, $m =$ some market index, usually change in price from a start date, and $v =$ trading volume within said market index, i.e. number of shares traded in a market over a given period of time. Market momentum can be either positive or negative and indicates the sentiment of a market. The underlying assumption is that what grows will likely keep growing and what shrinks will likely keep shrinking. Momentum played a central role cryptocurrency's skyrocket in value toward the end of 2017. Let's take some measurements starting with the early stages of cryptocurrency and compare these with the measurements from the latest surge. We will use 10-day momentum, i.e.
$(\text{Change in \$ price over last 10-days}) \cdot (\text{Trading volume over past 10 days})$.

In late 2013 - early 2014, we saw the first ever surge in Bitcoin price. This was back when cryptocurrency was first beginning to gain major traction, yet Bitcoin was by far the most dominant cryptocurrency as the space was very new and the term "altcoin" was barely breaking the surface. In November, 2013, momentum began to grow from roughly 0 to 430 in a matter of 3 weeks. It then surged to 630 in a week after that. These record heights, however, were broken after Mt. Gox, then the largest exchange platform, was hacked, losing all stored cryptocurrency on the exchange. This led to a massive reversal in momentum, declining to as low as -351 a month later. This major event completely stopped Bitcoin, and thus the entire cryptocurrency market, in its tracks, leading to widespread mistrust and overall deprecation of cryptocurrency sentiment. Momentum was a great measurement in determining how major events can shape the market ever so quickly. Here is a plot of momentum from November-December 2013:

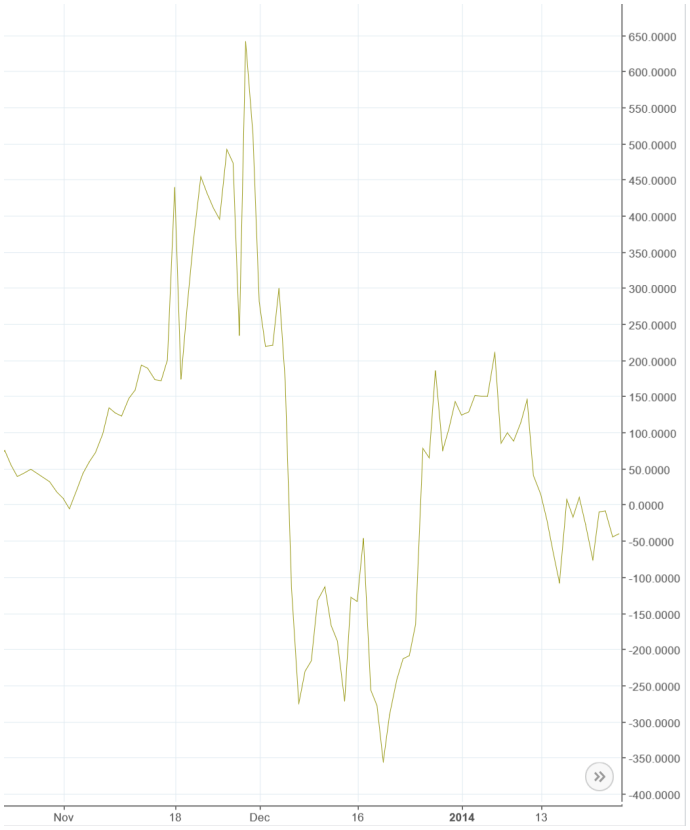


Figure 3: Source: https://www.tradingview.com/chart/LmduOjEx/

This major event put a halt on resurgence of cryptocurrency valuation for roughly three and a half years. Such dangerous swings in momentum combined with risks of hacking were too much for the public to handle for a long time. However, despite this, the space began to grow behind the scenes. New "altcoins," or cryptocurrencies alternate to Bitcoin, such as Ethereum, Litecoin, and Ripple began to gain popularity as these coins brought new functionality to the cryptocurrency space. By the summer of 2017, cryptocurrency began to see some rapid growth in momentum. By Fall 2017 leading into 2018, four years after the crash of Mt. Gox, we begin to see a similar pattern:

Figure 4: Source: https://www.tradingview.com/chart/LmduOjEx/

What caused this nearly identically shaped, much larger momentum swing? On December 10th, Cboe Global Markets launched Bitcoin futures [10]. A week later, on December 17th, CME Group launched its own Bitcoin futures. Over the next two days, momentum swung from roughly 6000 to -4000. Furthermore, prices had reached an all time high of nearly $20,000 a few days earlier. These futures allow users to purchase a contract that enables them to buy or sell Bitcoin at a set price (either higher or lower than the current price) on a set date. Futures have certain advantages over trading assets themselves since they are secured once they are purchased, so the user knows exactly what they are getting and when. Additionally, the user does not need ever hold any Bitcoin if she chooses to purchase a Bitcoin future since both firms settle in USD. Finally, and most importantly, these futures were the first universal implementation of the ability to bet against cryptocurrency due to the fact that most exchanges do not allow short selling. The main heuristic is that futures would attract Wall Street and the like. By betting against or for cryptocurrency without holding cryptocurrency itself, firms can take advantage of speculative value while minimizing their associated risk.

Bitcoin futures instilled fear in the cryptocurrency markets in a way nearly identical to the Mt. Gox incident. When Bitcoin is undergoing large growth in momentum and price, especially at all-time highs, history shows that it is actually a vulnerability in the cryptocurrency market as any fear-promoting news leads to massive corrections.

4.4.2 Metcalfe's Law in Relation to Cryptocurrency

Metcalfe's law is a very unique law in that it discusses the value of a telecommunications network. While cryptocurrency functions somewhere in between a commodity and a currency as previously discussed (although is legally classified as a commodity), it has very similar properties to a network. Any user of a cryptocurrency, let's say Bitcoin, is a member of a transaction network on the Bitcoin blockchain. The value of each user is determined by the net flux of received and sent Bitcoins. The volume of transactions between users affects the growth of the price of a single Bitcoin. The number of miners participating on the Bitcoin blockchain affects the speed of these transactions and the rate at which new Bitcoins are added to the network. Could there perhaps be "value" given to the network itself and not just the price of a single Bitcoin? Many economists, such as Tom Lee[5], co-founder of Global Fundstrat Advisors, believe this is the case.

Theorem 1 (Metlcalfe's Law)**.** *The value of a (telecommunications) network is proportional to the square of it's users. This relates to the fact that the unique number of connections in a network of n nodes is $\frac{n(n-1)}{2}$ which is asymptotically proportional to n^2.*

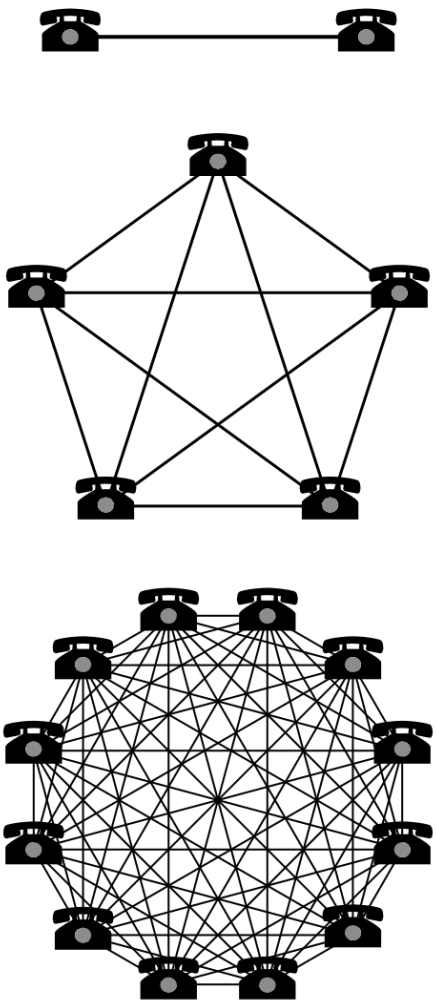
Proof. By induction, we start with the fact that a single node network has no connections. A two node network has one connection, a three node network has three, four has six, etc. An n node graph must have added $n-1$ nodes to the previously existing graph. Thus, we have

$$\sum_{i=1}^{n} i - 1 = \frac{n(n-1)}{2} \approx n^2$$

as $n \to \infty$. □

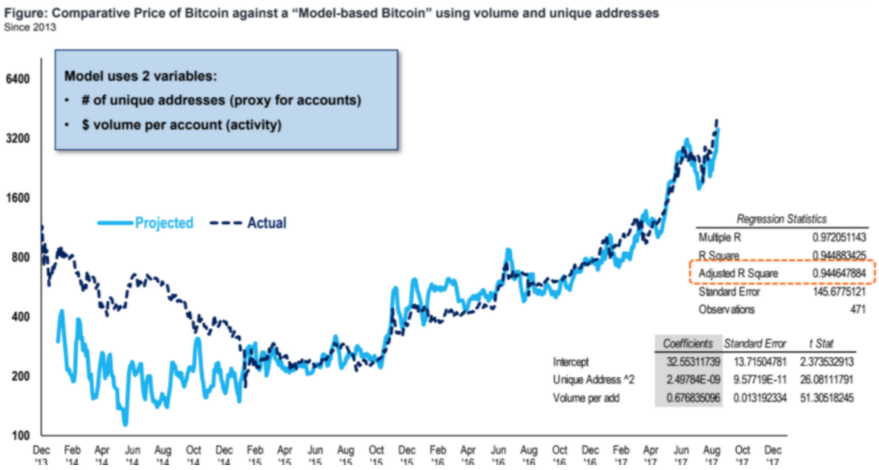
Visually, we can express how adding new nodes to a network increases the number of connections at a rate equivalent to triangle numbers such that the ith new node adds $i-1$ connections to the previously existing network:

[5] www.businessinsider.com/bitcoin-price-movement-explained-by-one-equation-fundstrat-tom-lee-metcalf-law-network-effect-2017-10



Here, we represent nodes as telephones, yet in the context of cryptocurrency we can think of these nodes as addresses on a cryptocurrency network. Two nodes can only make one connection, five can make 10 connections, and twelve can make 66 connections. Removing a node from any of these networks would result in the number of connections decreasing by the amount of original nodes minus one.

Metcalfe's law therefore shows not only how "valuable" a network is in its current state, but also how quickly one can grow. As more and more users join various cryptocurrency networks, the value of these networks and thus the value of the corresponding asset grow very quickly. In theory, applying Metcalfe's law to cryptocurrency in an economic sense works beautifully. In fact, Tom Lee's firm published their findings after applying Metcalfe's law to predict price growth of Bitcoin in October 2017. They modeled a function consisting of both the square number of unique Bitcoin addresses at the given time as well as the volume per address. Adding this second variable is important since it is crucial in weighing the true value of an address. For example, if an address joins the network, but rarely participates, it isn't really adding much value to the network. A graph of their model fits very nicely when plotted against the price of bitcoin, achieving an R^2 of 0.94:



The price of bitcoin compared with the projected value of bitcoin. This is based on the FundStrat model using unique addresses and transactions. FundStrat

This model works wonderfully when plotted against areas of growth, but seems to falter during large sell-offs. Since this research has been published, Bitcoin achieved its largest percentage drop in history as previously discussed. Additionally, we can see that the projected model trails actual pricing from roughly late 2013 - early 2014 after the Mt. Gox crash. Some hypotheses as to why this might be: Perhaps domination of a few number of addresses (the aforementioned "whales") on the Bitcoin network far exceeds any new value added from a new user and thus can move prices at greater speeds than the masses. Furthermore, we have shown that hysteria-generated momentum swings can wipe out massive climbs in a matter of days. Lastly, there is never any sure way to measure the effect of the size and power of a mining population on a blockchain, but it is a fact that this affects the speed of transaction confirmation and thus may have an effect on price.

4.4.3 "Halvenings" and the effect of mining

Mining drives the Bitcoin network. Without it, transactions would be meaningless as there would be no way to know which blocks to trust. Ethereum is also powered by a minable blockchain, and together these cryptocurrencies make up the majority of the entire combined cryptocurrency market cap. Many more cryptocurrencies operate under a minable platform. Thus, mining determines the money supply for the majority cryptocurrency. As such, mining is proportional to price.

We have previously discussed how mining becomes more difficult with time. Additionally, rewards are cut in half every four years for Bitcoin, and these cuts are dubbed "halvenings." Ethereum also reduces block rewards over time but in a less systematic way. The idea is that as computers become more powerful, there needs to be ways to ensure that no one party can have a mining majority, as this would lead to possible malicious behavior on the relevant blockchain. While this is indeed a threat, these measures lead to massive amounts of inefficiencies. For any miner to keep up with increasing block difficulty profitably, she must either be constantly upgrading her hardware or adding more of what she already has. This, more often than not, also leads to more energy consumption and thus more marginal cost. Here is a nice info-graphic depicting the cost of mining a single Bitcoin in the United States as of December 2017:

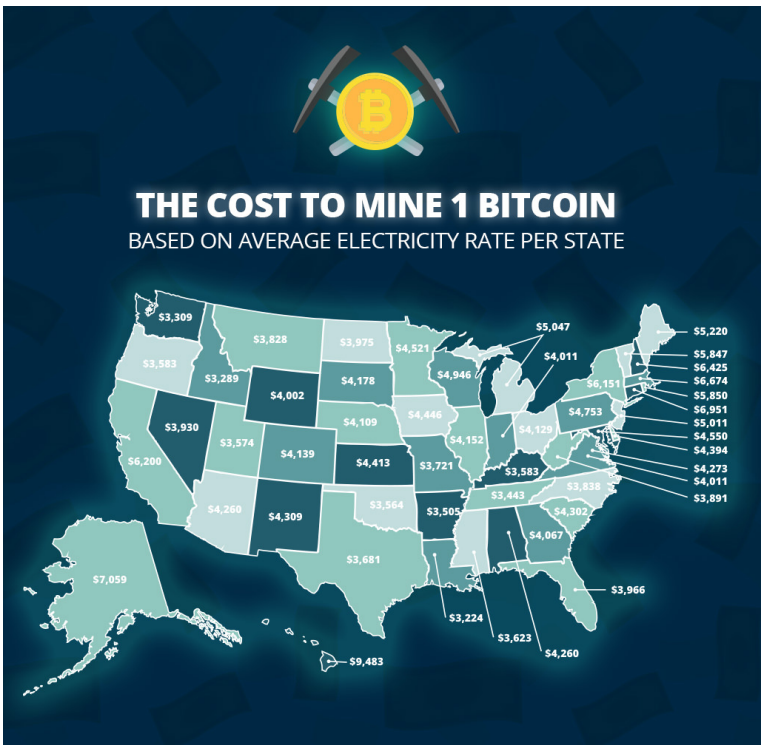


Figure 5: Source: https://www.marketwatch.com/story/in-one-chart-heres-how-much-it-costs-to-mine-bitcoin-in-your-state-2017-12-15

This is still profitable, but one must factor in the cost of hardware and the time needed to mine a single Bitcoin. With the cost of hardware and the difficulty of mining both simultaneously and constantly increasing, the risk involved in mining is dependent entirely on the current price trend and market sentiment. For example, a dedicated miner may pull the plug if the cryptocurrency market is bearish. If enough miners leave the network for this reason, the time it takes to verify transactions will decrease proportionally, thus decreasing cryptocurrency liquidity. Note that this will hold for all cryptocurrencies that are not offered fiat conversion since Bitcoin and Etheruem are the most liquid. Decreased liquidity can instill fear in the market, further decreasing prices. On the other hand, if the cryptocurrency market is bullish, this will incline new miners to join the network and already-dedicated miners to enhance their current equipment, further increasing prices. For these reasons, we should assume that the size and power mining population proportionally affects the cryptocurrency market trend.

4.4.4 Global Commercial Implementation

Many companies are willing to accept Bitcoin as payment as of March 2018. Some of these companies[6] include Overstock.com, Subway, Microsoft, OkCupid, Expedia.com, and many more. However, few companies are willing to endorse or promote the cryptocurrency space. In fact, major tech companies Google and Facebook, have banned or plan to ban cryptocurrency advertising on their respective platforms[7]. This has mainly to do with the unregulated and speculative nature of new Initial Coin Offerings, or ICOs. However, companies like Facebook and Google who have massive dominance and control over the internet's data, perhaps see cryptocurrencies, and decentralization in general, as a threat to that control.

Last year alone, there were over 900 ICOs which raised billions for their promoters, but in doing so caught the attention of the Securities Exchange Commision (SEC) [11]. The SEC views certain ICOs not as new currency offerings, but as securities offerings, which therefore fall under the SEC's jurisdiction. According to the SEC, already half of the ICOs from 2017 have failed. From the standpoint of Google and Facebook, it seems their move to ban cryptocurrency advertising is

[6]https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/
[7]https://www.npr.org/sections/thetwo-way/2018/03/14/593553255/google-follows-facebook-in-banning-cryptocurrency-ads

less about discounting the entire cryptocurrency space as it is avoiding false advertising.

The consensus of major companies is such that cryptocurrencies that have already been around for a long time, like Bitcoin and Ethereum, seem to be more legitimate forms of payment than those that came after. While many new cryptocurrencies entering the market seek to improve upon the fallbacks of larger cryptocurrencies, many are merely "get rich quick" scams. It can be difficult to tell the difference, which is why major companies are choosing only to recognize Bitcoin and Ethereum while avoiding promotion of ICOs. This skeptical nature will help evolve the cryptocurrency space in a good way: only the strong will survive.

4.5 Major Risks

4.5.1 The Bubble

If the word "cryptocurrency" appears on the news, it is very likely the word "bubble" will follow. What is a bubble in economic terms? To understand the meaning of this term, we begin with the story of what is considered the first major recorded economic bubble in history[8].

4.5.2 Tulip Mania

In 1593, tulips were introduced to the Dutch from Turkey. The novelty of the new flower made it desirable and expensive. After some time, the tulips contracted a non-fatal virus known as mosaic, which left the tulips unharmed but altered their appearance, causing flame-like color patterns to appear on the petals. These color patterns varied widely from flower to flower, increasing the rarity of the already unique tulip. Thus, tulips, which were already selling at a premium, began to rise in price further according to the unique color patterns. Everyone wanted to join the tulip market for these reasons; tulips were believed to never stop increasing in value.

Soon, people were trading their land, life-savings, and anything else they could liquidate to get more tulip bulbs. Dutch traders filled up inventories for the growing season, further depleting supply, increasing scarcity and demand. These traders believed they would be able to unload these tulips onto the market once demand reached all-time highs. This market manipulation caused the value of a single tulip bulb to increase twenty times in value in a single month.

Prices were obviously completely out of proportion to the true value of a tulip bulb. Thus, some people decided to sell and take their profit from the investment. Progressively, this caused a domino effect as prices began to decline, causing more people to sell. Eventually, panic set in and prices reached a nosedive; demand for tulip bulbs had become almost non-existent. Just as fast as greed drove prices to the moon, panic pulled prices back to the ground. Poor traders who had bought into the hype had realized they sold their house for a plant.

Tulip Mania, as this event has been labeled, was the first of its kind and caused a major economic crash for years to come. No matter if a trader had been lucky enough to sell at the right time, she still suffered from the depression that followed. This event led to major skepticism in the Dutch markets, leading traders to become more hesitant and careful with their investments.

Other major bubbles include the Florida real-estate craze (1927), the dotcom bubble (2000-02), and the housing market bubble (2007-08).

4.5.3 Is Cryptocurrency a Bubble?

Cryptocurrency has seen the likes of tulip-mania-esque price fluctuations. In fact, given that it has no true underlying value, any cryptocurrency in its entirety is a speculative bubble. Prices reflect simply the belief of those involved, including the miners, holders, sellers, and those who accept cryptocurrency as a valid transaction. This is identical to tulips

[8] https://www.investopedia.com/features/crashes/crashes2.asp

in the early 1600's. However, what differs is the ease of transaction, ever increasing supply, and use cases surrounding decentralization. Cryptocurrencies, being digital, are easy to transact and take up no physical space apart from the devices required to store and mine them. Furthermore, there is unlikely ever to be a shortage of cryptocurrency given the constant influx of supply from mining and ICOs. Lastly, cryptocurrency has a tendency to survive major crashes. Bitcoin survived the Mt. Gox crash of 2014 and is currently stabilizing after the most recent and futures crash of late 2017. Only time will tell if cryptocurrency will ultimately reach its demise due to its purely speculative value, but given the public's willingness to participate, this may end up never being the case.

Ultimately, as time goes on, there seems to be only two possibilities. The first and most common belief is that cryptocurrency will eventually be worth nothing. The current state of the market is indeed purely speculative and, given the current trends, it seems as though the long term fate of the space is dying. Furthermore, mining is unsustainable as it consumes massive amounts of electricity and yields diminishing returns independent of market behavior. Although not all cryptocurrencies rely on mining, the vast majority of the space by market cap does. If the crypto-space continues to be dependent on minable cryptocurrencies, it may be the case that no matter how innovative new ICO's become, they will be tethered to the lesser functional, yet dominant cryptocurrencies, Bitcoin and Ethereum.

On the other hand, there are those who believe cryptocurrency will survive and even surpass fiat currency in usability. Given that our world is headed toward digital dominance, there seems to be less of a need for printed money. Additionally, if any major world governments were to collapse due to war, global warming, or other major disasters, the fiat currency driven economy may, in turn, collapse as well. Cryptocurrency could be seen as a hedge against such major disasters. Furthermore, with the dominance of artificial intelligence imminent, it is widely believed that most forms of basic human labor will be replaceable in the next 50 years. Cryptocurrency could be used as a form of basic income for citizens who can no longer find employment. By serving as an owner of computational equipment, any citizen would be able to conduct verification of transactions and earn fees, thus supplying steady income. Additionally, data storage and GPU power are in massive demand as "big data" contains so much valuable and profitable information, yet requires heavy lifting to extract such information. Citizens could be paid basic income in exchange for supplying storage and computational power under certain cryptocurrency models. Golem (GNT) is a cryptocurrency that already implements a similar model[9]. Decentralization of data has incredible long-term merits given the direction the world is headed, however the powers at be, i.e. governments, big data companies, computer companies, and banks may see cryptocurrencies and decentralization in general as a threat. Thus, these powers may work against cryptocurrency's possible rise.

4.5.4 Government Intervention

Governments have many reasons to be against cryptocurrency:

1. It is very difficult to tax cryptocurrency earnings.
2. Cryptocurencies are used for illegal transactions.
3. Cryptocurrencies threaten government sanctioned currencies.
4. Cryptocurrencies consume needless amounts of energy.
5. Deregulation and decentralization are at odds with any form of government.

World governments, for these reasons, have already been attempting to find ways to either ban or somehow regulate the cryptocurrency space. The Chinese government has already implemented a soft ban on cryptocurrency, although this has not completely stamped out trading[10]. The South Korean government has been discussing ways to regulate the space as well[11]. The US government has placed a subpoena on cryptocurrency exchange Bitfinex under the charge that they have

[9] https://golem.network/
[10] http://www.scmp.com/business/banking-finance/article/2132009/china-stamp-out-cryptocurrency-trading-completely-ban
[11] https://www.forbes.com/sites/elaineramirez/2018/01/23/why-south-korea-is-banning-all-foreigners-from-trading-cryptocurrency/#28da19327345

pumped $2.3 billion artificially backed US dollars (Tether or USDT) into the cryptocurrency market[12].

Indeed, it is the case that governments of countries heavily involved in the exchange of cryptocurrency have been seeking ways to regulate or ban such trading. However, this has not been easy. If it were, cryptocurrencies would most likely not exist today. The threat of government regulation is always imminent in the cryptocurrency world but does not seem to ever be a solid or guaranteed risk. Therefore, most cryptocurrency markets today still run without regulation. In fact, certain governments, especially those with crippled monetary systems, are in favor of cryptocurrencies. As of 2018, Venezuela has implemented their own cryptocurrency, Petro, to combat the highly over-inflated Bolívar[13]. Other countries that have implemented their own national cryptocurrencies include Ecuador, China, Senegal, Singapore, and Tunisia[14]. Many other countries have voiced plans to do the same.

Since worldwide governments have a polarized stance on cryptocurrencies, it is impossible to tell whether government regulation will ever completely eradicate cryptocurrencies from existence. However, it is always a considerable threat to the space.

Perhaps the most interesting case of government intervention is that of the US government in relation to USD Tether and the Bitfinex exchange. USDT was introduced in 2014 as a way for users interested in purchasing cryptocurrency to exchange easily from fiat to crypto. Tether is claimed to be backed one-to-one such that for every USDT in existence, there is 1 USD held in reserve. As of April 2018, there are nearly 2.3 billion USDT in circulation.

While representatives from Tether and Bitfinex claim the two are separate, the Paradise Papers leaks in November 2017 named Bitfinex officials Philip Potter and Giancarlo Devasini as responsible for setting up Tether Holdings Limited in the British Virgin Islands in 2014[15]. According to Tether's website, the Hong Kong based Tether Limited is a fully owned subsidiary of Tether Holdings Limited. Furthermore, Bitfinex is the largest Bitcoin exchange by volume in the world. To make matters more convoluted, Bitfinex banned trading for users based in the US as of November 9th 2017[16]. This is apparently due to troubles with US banking regulations.

Indeed, the activity of Bitfinex is suspicious and the apparent sweeping under the rug of ties with Tether makes matters all the more telling that there is something deeper going on here. Tether does not get released on a basis such that for every dollar inputted, a single tether is outputted. Rather, hundreds of millions of USDT are released into the market every few months or so. $850 million worth of USDT were released in January alone[17]. Furthermore, Tether has failed to release an audit to confirm its reserves do in fact contain $2.3 billion in USD. As of December 6th 2017, the US Commodity Futures Trading Commission sent subpoenas to both Tether and Bitfinex to testify on their behalf regarding the matter.

The influx of USDT into the crypto market has undoubtedly inflated the prices of all cryptocurrencies, Bitcoin in particular. While the current market cap of Tether is roughly $2.3 billion (13th out of all cryptocurrencies), it is consistently second to Bitcoin in 24 hour volume, averaging close its entire market cap. This is indicative that Tether is more of a vessel of buying and selling power rather than any sort of store of value. As such, despite having small market cap relative to major cryptocurrencies, Tether most likely has a larger effect on the market. The outcome of Tether's court hearings is perhaps the largest government risk in that much more than $2.3 billion of market cap could be wiped from the market very quickly.

[12] https://www.bloomberg.com/news/articles/2018-01-30/crypto-exchange-bitfinex-tether-said-to-get-subpoenaed-by-cftc

[13] https://www.washingtonpost.com/news/wonk/wp/2018/03/05/venezuelas-cryptocurrency-is-one-of-the-worst-investments-ever/?utm_term=.79cac331eb18

[14] https://www.fxempire.com/education/article/the-next-cryptocurrency-evolution-countries-issue-their-own-digital-currency-443966

[15] https://www.nytimes.com/2017/11/21/technology/bitcoin-bitfinex-tether.html

[16] https://www.bitfinex.com/posts/227

[17] https://arstechnica.com/tech-policy/2018/02/tether-says-its-cryptocurrency-is-worth-2-billion-but-its-audit-failed/

4.5.5 Quantum Computing

Quantum computers are a theoretical and very powerful alternative to classical computers. Rather than operating in deterministic bits, i.e. 1's and 0's, they operate in qubits, which act as a superposition of 1's and 0's. What does this mean? Well, the exact aspects of quantum theory are outside the scope of this paper, but we hope to give a high level description so that the reader understands the threat they pose to cryptocurrency. A superposition of 1's and 0's means that a qubit *simultaneously* contains information as a 1 and 0. While a classical bit has only two possibilities, a qubit has infinitely many. Certain problems that are extremely difficult for classical computers to solve would be much easier for a quantum computer. Today, quantum computers exist mainly as a theoretical phenomena, although quantum computers with a very small number of qubits have been successfully implemented by the likes of Microsoft, IBM, and Google[18].

Despite being a long way from mainstream implementation, numerous quantum algorithms have already been discovered. This means that once quantum computers with a large enough number of qubits are manufactured, we will be able to use them for tasks involving optimization, artificial intelligence, and most importantly in our case, encryption.

4.5.6 Shor's Algorithm

Shor's algorithm is a quantum computer algorithm which can quickly factor numbers. On a classical computer, this is easy to do if the number is relatively small, say 10 digits. But what if the number has thousands, or even hundreds of thousands of digits? This becomes infeasible for a classical computer. Shor's algorithm on a quantum computer, however, significantly speeds up this process. A modified version, called Shor's discrete logarithm quantum algorithm for elliptic curves, can crack ECDSA. In the case of Bitcoin, Shor's algorithm can simply take a user's public key and signature as input, and find the associated private key. On a classical computer, runtime for this is $O(2^{\frac{k}{2}})$, while on a quantum computer, it is $O(k^3)$, which is much, much smaller. Since a Bitcoin public key is 256 bits long, the number of computational steps to crack the private key goes down from 300 trillion trillion trillion to a few hundred million[19]. The only case in which a Bitcoin address is quantum-safe is if it has not broadcasted a transaction from itself, or is "unused." This means that its public key has not been broadcasted to the network. However, for anyone to spend Bitcoin from their address requires them to make transactions from it, and these transactions include their public key and signature. Thus, anyone with a quantum computer would be able to impersonate a user after they made a transaction by recovering their private key from their public key and forging their signature.

Luckily, the largest number factored on a modern quantum computer is 21, which is a 5 bit number, and, as we've seen, is dwindled in comparison to a 256 bit number. True quantum computing in the above sense is most likely decades away, bar a massive leap in computer science research. Additionally, there are measures that could provide quantum safety to Bitcoin addresses. Certain cryptocurrencies such as Cardano and IOTA have already implemented quantum safe protocols. An idea, called Lamport signatures, would be to provide a single user with two hashes rather than a single elliptic curve point as their public key. All functionality would be the same except now a user has "multiple locks" (see [12] for more details). This signature would be infeasible to forge even for a quantum computer. The difficulty for a massive network like Bitcoin or Ethereum would be converting from the current protocol to a quantum safe protocol such as Lamport signatures in an effective manner.

While quantum computers do pose a threat to the current cryptocurrency space, it is unlikely that the threat requires addressing in the near future. Additionally, the threat can be mitigated using quantum-safe encryption. The main heuristic is that algorithms evolve much faster than the hardware required to run them...

[18] http://www.bbc.com/news/technology-43580972

[19] https://bitcoinmagazine.com/articles/bitcoin-is-not-quantum-safe-and-how-we-can-fix-1375242150/

4.6 Interview with Tyler Winklevoss

The following contains an interview we had with Tyler Winklevoss on April 12th 2018, who, along with his twin brother Cameron, are widely considered the most influential people in cryptocurrency. We ask him a few questions regarding certain aspects of the previous section. Tyler's answers really help us understand the space from a perspective that deals with its inner workings from day to day.

How has your opinion of Cryptocurrency evolved since you first became involved?

Tyler: Good question... Initially when I first came across Bitcoin, I felt like it was the first money that was truly built for the internet. A money that worked like email. If you think of Bitcoin as a money protocol like SMTP (Simple Mail Transfer Protocol) and IMAP (Internet Message Access Protocol) as email protocol and VoIP (Voice over internet Protocol) as a voice protocol, Bitcoin, at the time when I first discovered it in 2012, was the first of its kind in that sense. It was the only thing like that out there. The 'aha' moment was this is money over internet protocol, built to work over the internet by the same people who built the internet as opposed to the money we had, which was built by bankers before the Internet ever existed and never really contemplated working on the Internet. Over time, Bitcoin became known as the first use case; the MVP of cryptocurrency. The killer-application is Gold 2.0, or a better gold. From there, there are all these other possibilities of re-architecting the internet itself. Whether its storage, things like Filecoin, or computing power, things like Ether, all of the sudden all of these different problems of the internet could be attacked by cryptocurrency and its market forces and dynamics. Today, I think the thing you see is the problem of de-centralizing the internet since data is centralized by a only few companies. The criticism of the internet today is that it's not open and that it's very much siloed off to these data cartels. Cryptocurrencies could help push centralized data on the application layer down into the protocol layer and give it back to the users.

Would you classify cryptocurrency as a currency, a commodity, or something in between?

Tyler: I would classify it as a commodity and the CFTC (Commodity Futures Trading Commision) classifies it as a commodity per the Coinflip order in September 2015. So it's in the same class, in the eyes of the CFTC, as gold. The Fed does not classify it as a currency since its not centrally issued or issued by a government. The SEC, while they won't come out and say it, will probably not reach over and try to classify it as a security. If you do a Howey test analysis, the test used by courts to determine whether or not something is a security, I don't think bitcoin would fall under the definition of a security. The regulation has been pretty clear for Bitcoin for quite some time even though in the press it's often called a virtual currency, digitial currency, or digital asset. These names can be misleading and confusing because the media uses them interchangeably even though they have dramatically different consequences from a tax or commerce standpoint. I feel strongly as do government regulators that Bitcoin is a commodity, but you'll never see a newspaper come out and label Bitcoin as a virtual commodity.

Do you think governments view cryptocurrency as a threat?

Tyler: Depends on which government. The rhetoric out of most of the US government is that they believe in the innovation, the merits, and the promise of cryptocurrencies. There are obvious natural concerns such as money laundering, activity in dark markets, but it doesn't feel like any of them are so outsized or dominant over the positive aspects. I think that as a whole that cryptocurrency is an important innovation that should be regulated thoughtfully but allowed to thrive. Certainly, the cynical position is that it's very hard to stop, so it's better to work with it than against it. It works over the internet, so in order to control cryptocurrency you'd have to somehow censor the internet itself and that's a very hard thing to do... If you were to fight things like Bitcoin, you may not win, and if you were to be somewhat successful in that, you'd push a lot of human capital and innovation offshores. So you're better off working with it, fostering it, but putting in the right safeguards so that there are not bad actors using it. That has been pretty much the way the US government has approached this for a while now.

Gemini is regulated as a New York Trust company in the state of New York. Just like a bank, we have to make sure bad actors aren't able to open an account. We're confident and we think New York State is confident that the tried and true money laundering policies with regards to cash will work with cryptocurrencies. There are governments that are allergic to cryptocurrencies because they want to have more control over their financial system. Russia, Venezuala, countries that you'd expect to want to have strong capital controls are much more threatened by cryptocurrency because of the financial independence, autonomy, and freedom it confers on users. I'm sure that's more threatening to more autocratic governments, but it feels like the US has embraced cryptocurrency a lot more than its repelled it.

Your exchange, Gemini, currently offers only Bitcoin and Ethereum. Do you prefer these cryptocurrencies over others?

Tyler: We try and be agnostic about which cryptocurrencies we support for trading and custody. At the end of the day we are a service platform and an infrastructure business. So we do not give investment advice to our customers, but Bitcoin was the logical place to start since it was the first and only. It's difficult for us to support cryptocurrencies in a secure and thoughtful way since it takes time and resources. We want to definitely support the trading of cryptocurrencies that have large developer communities, that have technical merit and differentiation and that will be around in the long run. We don't want to be in the business of listing and de-listing. Because we are the most regulated cryptocurrency exchange in the world, we require regulatory approval, so there is a certain bar that must be met before Gemini can consider listing something. We don't list things with the idea, 'oh this must go up' or as an endorsement, but rather there must be a community that can upkeep the protocol. When we do list something, we custody it in cold storage, which costs a lot of resources and developer hours to do right so it's not of interest for us to throw resources at something that is a fly-by-night. The other thing is legal characterization of what we are listing. We believe Bitcoin and Ether are virtual commodities and we are licensed to list virtual commodities for trading, however, we are not licensed to list securities for trading. If we were to list something classified as a security some day, we would need additional licensing, so we need to be very careful in listing only the things we are licensed to. We will be adding more cryptocurrencies in the next couple of months that meet our criteria.

With the recent subpoena on Bitfinex and Tether by the CFTC, what is your opinion on the steps that need to be taken toward making cryptocurrency universally legitimate?

Tyler: What's important to legitimizing cryptocurrencies is making sure there's a clear path for legitimate companies to become licensed and compliant with laws. In addition, there needs to be enforcement actions taken by regulators against operators that don't want to be legitimate and are running a foul of regulations and other laws. The culmination of a clear path for licensing for legitimate operators and enforcement against bad actors are critical for the mainstreaming and legitimizing of the space. What we've seen is that there have been legitimate paths forward, as Gemini became a New York trust company in 2015, but there hasn't been enough enforcement. I think what we'll see in 2018 is more enforcement from regulatory bodies such as the SEC and CFTC, and maybe even states. Enforcement does have a longer tail since it takes time to build a case. Things that were done wrong a year ago may be just getting addressed a year later. Overall, those who want to become involved should have a clear path toward doing so, and those responsible for regulation should continue to make the space safe.

5 Mathematical Analysis of Cryptocurrency Markets

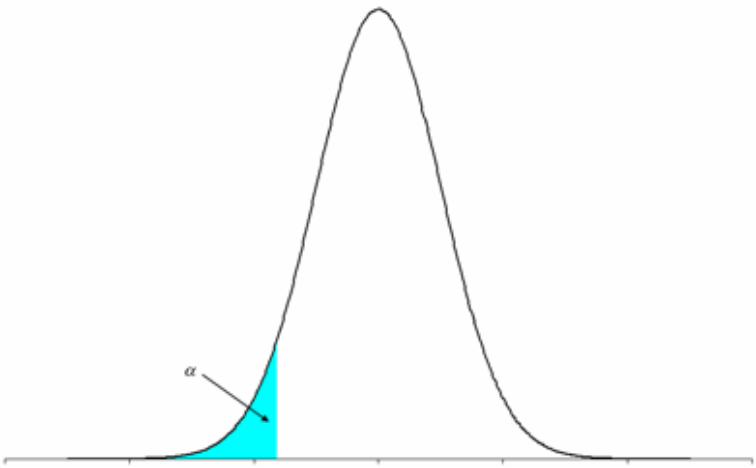
So far we have outlined the functionality of and economic drivers behind cryptocurrency. We will now delve into some aspects of mathematical finance when applied to cryptocurrency. Mathematical finance involves using purely mathematical techniques to attempt understand and predict market movement. These techniques have been used in stock market trading for decades and has yielded tremendous success. Is it possible to use mathematical finance to predict cryptocurrency

fluctuation? Indeed, but with far greater risk than in the stock market.

DISCLAIMER: The following section involves strategies that are for academic purposes only. Trade at your own risk.

5.1 Value at Risk

A common mathematical finance strategy is calculating value at risk (VAR). On any given day, a portfolio carries with it a measure of risk. A common strategy to assess this risk is to ask the question, "how much value can I expect to lose with 1% probability on any given day?" To answer this, we must first measure the distribution of returns for each asset in our portfolio over a certain time period. This will visually look something like a normal distribution:

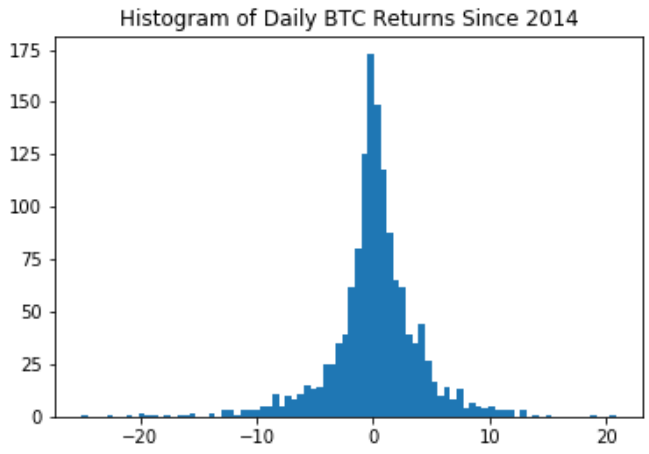


To measure a 1% risk, we would assess values that are roughly 2.33 standard deviations to the left of the mean ($Z_{0.01} \approx 2.33$).

A notable difference between VAR of cryptocurrency and VAR of stocks is that cryptocurrency has *very* wide tails when it comes to returns. This means that on any given day we will have to take on far more risk than if we were holding stocks. Additionally, stocks have many decades of historical data while most cryptocurrencies only go back a year or two. This can cause biased measurements. We can acquire price data from quandl.com containing BTC-USD from Bitfinex. To measure daily percentage returns R, we simply assess the daily close price p over a given time period $1, ..., n$ and calculate

$$R_i = \frac{p_i - p_{i-1}}{p_{i-1}} \cdot 100$$

for $i = 2, ..., n$. Let's assess daily price data of Bitcoin from January 2014 to April 2018 ($n = 1402$), plotting a histogram of our result:



We can see that most of our returns are centered around 0, but indeed there are some cases where returns skyrocket to $+20\%$ and plummet to -20%. Let's calculate the sample standard deviation of our returns, i.e.

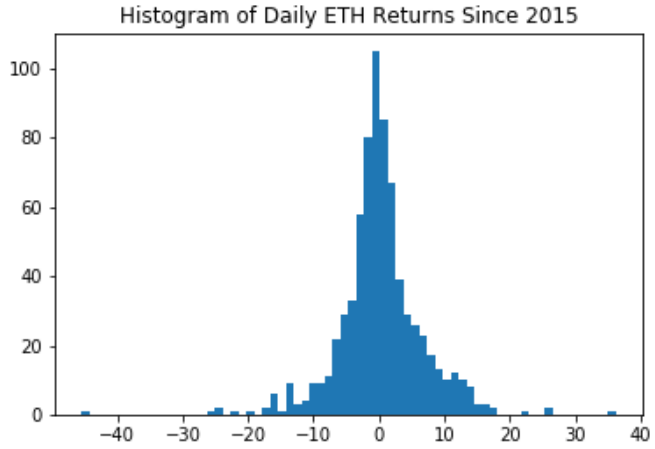
$$\hat{\sigma}_n = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}\left(R_i - \bar{R}\right)^2}$$

where

$$\bar{R} = \frac{1}{n}\sum_{i=1}^{n} R_i$$

is the sample mean of our returns. We find that $\bar{R} = 0.1\%$ and $\hat{\sigma}_n \approx 4.054\%$. This means that our 1% value at risk is $2.33 \cdot \hat{\sigma}_n \approx 9.45\%$. We can conclude that on any given day, we can expect to lose no more than 9.45% of the value of our position 99% of the time. This is immensely high. For some perspective, the S&P 500 has a current 1% Value at Risk of 2.52%[20].

What about other cryptocurrencies? Let's again turn to Bitcoins younger sibling Ethereum. If we run the same calculations as above, we achieve the following histogram of returns since March 2016:



We can immediately see that this distribution has more variance. In this case, we find that $\bar{R} \approx 0.245\%$ and $\hat{\sigma}_n \approx 6.5$. This means that our VAR is approximately 15.15%! Ethereum is quantitatively almost twice as risky as Bitcoin. This is captured in the figure of BTC and ETH volatility from section 5.2. It is important to note that since Ethereum is newer than Bitcoin, we don't have as much price data, leading to a more biased measurement. This can make VAR appear higher than it might actually be. The following is a table of VAR calculated for a few popular cryptocurrencies in terms of USD:

Cryptocurrency	Symbol	Number of Days Measured	Value at Risk (%)
Bitcoin Cash	BCH	124	26.41
Litecoin	LTC	1423	14.26
Iota	IOT	287	24.38
Ripple	XRP	312	21.55
Monero	XMR	485	17.78
Dash	DSH	392	17.76

We see that many alternate cryptocurrencies carry far more value at risk than Bitcoin and Etheruem, but again see that cryptocurrencies with less data points have higher VAR.

[20]https://www.macroaxis.com/invest/technicalIndicator/%5EGSPC–Value-At-Risk

5.2 Portfolio Theory applied to Cryptocurrency

Portfolio theory is a subsection of mathematical finance that covers the optimization of wealth over a basket of stocks. In this section, we will apply certain aspects of portfolio theory to the world of cryptocurrency, attempting to optimize wealth purely within the space. Note that in this section we will use the terms security and cryptocurrency interchangeably, although a cryptocurrency is not necessarily considered by regulatory bodies to be a security. We will make the following (somewhat unrealistic) assumptions:

1. *Investors*: All investors are rational.
2. *Equilibrium*: Supply equals demand.
3. *Access to Information*: Rapid availibility of accurate information on securities exist.
4. *Efficiency*: A security's price adjust quickly to new information.
5. *Liquidity*: Any number of units of a security can be bought and sold quickly.
6. *No transaction costs*: Fees for trading are negligible.
7. *No taxation*: Ignore taxes.
8. *Borrowing and Lending*: Borrowing and lending are at risk the risk-free rate r.

5.2.1 Information Theoretic Aspects of Portfolio Theory

To introduce the concept of portfolio theory, we will begin with an abstraction that will help us later in defining optimal investment strategies. In particular, we will use models from *Elements of Information Theory* by Thomas M. Cover and Joy A. Thomas [13] which cover the information theoretical aspect of portfolio theory.

Some notation: the cryptocurrency market is represented as a vector $X = (X_1, X_2, ..., X_m), X_i \geq 0, i = 1, 2, ..., m$, where m is the number of cryptocurrencies and the price relative X_i is the ratio of the price at the end of the day to the price at the beginning of the day. In the case of stocks, this value is usually close to 1, but as we have outlined in the previous section, cryptocurrencies carry more volatility. As an example, if $X_i = 1.03$, the price of the ith cryptocurrency went up 3 percent that day.

Let $X \sim F(x)$, where $F(x)$ is the distribution of the vector of price relatives. A *portfolio* $b = (b_1, b_2, ..., b_m), b_i \geq 0, \sum b_i = 1$, is an allocation of wealth accross cryptocurrencies. b_i is simply the fraction of wealth associated to cryptocurrency i. If one uses a portfolio b over cryptocurrency vector X, the wealth relative (ratio of wealth at the end of the day to the wealth at the beginning of the day) is $S = b^T X = \sum_{i=1}^{m} b_i X_i$. Our goal is to maximize S. The difficulty in this is that S is a random variable dependent on X and we can never precisely measure the distribution $F(x)$.

The *growth rate* of a portfolio b within respect to the distribution $F(x)$ is defined as

$$W(b, F) = \int \log(b^T x) dF(x) = \mathbb{E}[\log(b^T x)].$$

If we use log base 2, the growth rate can also be called the doubling rate. The *(log) optimal growth rate* $W^*(F)$ is defined as

$$W^*(F) = \max_b W(b, F) = \max_b \mathbb{E}_{F(x)}[\log(b^T x)]$$

w.r.t. the constraint $b_i \geq 0, \sum_i b_i = 1$. This problem is solvable by knowing exactly what $F(x)$ is. However, we can only make our best guess at $F(x)$ through what we observe. We will outline ways to measure $\hat{F}(x)$, i.e. an estimate of the

true distribution F, in later sections. Our goal is to get as close as possible to understanding the day-to-day distribution of cryptocurrency returns. In fact, we can show that believing in a distribution g when f is true loses

$$\Delta W = W(b_f^*, F) - W(b_g^*, F) \leq D(f||g) \tag{5.1}$$

where b_f^* is the log optimal portfolio corresponding to f, b_g^* is the log optimal portfolio corresponding to g, and $D(f||g)$ is the Kullback-Leibler divergence of f w.r.t. g, which is defined as

$$D(f||g) = \int f(x)\log\big(\frac{f(x)}{g(x)}\big)\mathrm{d}x \geq 0.$$

One can think of $D(f||g)$ as the "distance" between the distribution f and g. We state without proof that $D(f||g) \geq 0$. Note that in general $D(f||g) \neq D(g||f)$.

Proof of (6.1). Let $b^* = b$.

$$\begin{aligned}
\Delta W &= W(b_f^*, F) - W(b_g^*, F) \\
&= \int f(x)\log(b_f^T x)\mathrm{d}x - \int f(x)\log(b_g^T x)\mathrm{d}x \\
&= \int f(x)\log\big(\frac{b_f^T x}{b_g^T x}\big)\mathrm{d}x \\
&= \int f(x)\log\big(\frac{b_f^T x}{b_g^T x} \cdot \frac{g(x)}{f(x)}\big)\mathrm{d}x + D(f||g) \\
&\overset{\text{(a)}}{\leq} \log \int f(x)\big(\frac{b_f^T x}{b_g^T x} \cdot \frac{g(x)}{f(x)}\big)\mathrm{d}x + D(f||g) \\
&= \log \int g(x)\big(\frac{b_f^T x}{b_g^T x}\big)\mathrm{d}x + D(f||g) \\
&\overset{\text{(b)}}{\leq} \log(1) + D(f||g) \\
&= D(f||g)
\end{aligned}$$

where (a) follows from Jensen's Inequality (see [21]) and (b) follows from Kuhn Tucker conditions and the fact that b_g is log optimal for g. To expand on (b), note that $S_g = b_g^T X$ and $S_f = b_f^T X$, but $\mathbb{E}_g[\frac{S_f}{S_g}] \leq 1$ under the log-optimality of b_g. □

This is indeed an abstract concept, but we can certainly enhance our understanding of investment in a market under the light of information theoretic portfolio theory. In the case of cryptocurrency, this is no different. We want to maximize wealth, but in doing so we also must minimize the divergence between our understanding of the market $g(x)$ and the true distribution $f(x)$. But this task is still very difficult: we can never predict with certainty the behavior of any given cryptocurrency. To simplify, we will re-introduce the concept of risk.

5.2.2 Markowitz Portfolio Theory

Measuring risk is the key in determining a good portfolio. Rather than attempting to know *exactly* how the market is going to behave, we can understand the level of risk associated with a portfolio (similar to as outlined in VAR) and maximize expected returns under this level of risk. This idea was pioneered by Harry Markowitz in 1952 and is dubbed Markowitz Portfolio Theory. Markowitz's idea centers around the fact that the major contributor to risk of a portfolio with a sufficiently large number of securities is not the risk of each security alone, but rather the movement of securities returns relative to each other (their covariances). The world of cryptocurrencies is highly covariant, especially given the circumstances under which they trade as outlined in previous sections.

[21] http://mathworld.wolfram.com/JensensInequality.html

Given the unpredictable nature of cryptocurrency, it is in our best interest to introduce *short selling*. Short selling involves borrowing cryptocurrency from a broker and immediately selling it. We then buy back the cryptocurrency at a later date and return it to our broker, keeping the profit (or loss). Short selling requires margin, or a certain amount of required funds, in our account in case we are unable to return the borrowed assets. It is important to note that in practice, not many cryptocurrency exchanges offer short selling, or margin trading, to all of its users. Rather, one must have a large amount of capital devoted to the exchange to enable short selling opportunities. We will nonetheless assume we have this capability.

To enable short selling, let us redefine our notation a little bit to incorporate time dependence. We will use notation as outlined in *An Introduction to Mathematical Finance with Applications* by Arlie O. Petters and Xiaoying Dong [14]. Let us consider a portfolio holding N securities. We will define $b = w$ such that

$$w_1 + ... + w_N = 1$$

are the weights of securities $1, ..., N$ and $w = [w_1 w_2 ... w_N]^T$ is the portfolio weight vector at time t_0. Assume that the percentage of initial capital $V_p(t_0)$ invested in the ith security is w_i. Then the total investment spreads among the securities as follows:

$$V_p(t_0) = w_1 V_p(t_0) + ... + w_N V_p(t_0)$$

where $w_i V_p(t_0)$ is the amount of capital invested in the ith security. Before we defined S_i as the price relative of the ith security on a single day. We shall now define $S_i(t_0)$ as the price of the ith security at time 0. Then, the number of units of cryptocurrency money buys is

$$n_i = \frac{w_i V_p(t_0)}{S_i(t_0)} \quad i = 1, ..., N$$

Note that $n_i \in \mathbb{R}_+$. We can then equivalently define $V_p(t_0)$ as

$$V_p(t_0) = n_1 S_1(t_0) + ... + n_N S_N(t_0).$$

Our portfolio is constructed at time t_0 by obtaining the following specific number of units of N securities,

$$n(t_0) = (n_1, ..., n_N)$$

which we will call our trading strategy at time t_0. $n_i < 0$ indicates a short position on security i while $n_i > 0$ indicates a long position on (meaning we buy n_i units of) security i. $n_i = 0$ means we take no action on security i. Hence, we can define w_i as

$$w_i = \frac{n_i S_i(t_0)}{V_p(t_0)}$$

and see that w_i can be positive, negative, or zero, indicative of n_i. The property $\sum_i w_i = 1$ still holds assuming we take short positions on a proper subset of w! This is because when we short sell a security, we receive the capital associated to it. Only sometime in the future do we buy back and return it. We return now to the concept of returns R, whereas we now define

$$R_p(t_0, t_f) = \frac{V_p(t_f) - V_p(t_0)}{V_p(t_0)}$$

as the return of our entire portfolio over time period $[t_0, t_f]$. For simplicity, let the previous interval be fixed such that $R_p = R_p(t_0, t_f)$. Let R_i be the return of security i and $R_p = \sum_{i=1}^{N} R_i$. The expected portfolio return rate for the period $[t_0, t_f]$ is therefore

$$\mu_p = \mathbb{E}[R_p] = \sum_{i=1}^{N} w_i \mu_i$$

where

$$\mu_i = \mathbb{E}[R_i]$$

is the expected return of the ith security. We can now think of determining w in terms of finding the best μ_i, a similar

goal as in last section. We can only approximate μ_i using historical return rates, similar to the section on value at risk. Thus, define sample mean $\hat{\mu}_i^m = \frac{1}{m}\sum_{j=1}^m R_i(t_{j-1}, t_j) = \bar{R}_i$ over some discretization of time $t_0 < t_1 < ... < t_m$ (this can be by minute, day, week, etc.). In section 6.1, we used daily time periods. The choice of time period depends greatly on the type of investment strategies we want to use, but for ease of notation assume we are using day-to-day returns.

We can now define the *risk of a portfolio* as the standard deviation of its return rate, i.e.

$$\sigma_p = \sqrt{\mathbb{E}[(R_p - \mu_p)^2]}$$

This is nearly identical to the measurement of risk in VAR, except now we consider a portfolio containing more than one asset. An equivalent definition of σ_p is the volatility of a portfolio. The sample volatility of a portfolio over m days is defined as

$$\hat{\sigma}_p^m = \sqrt{\frac{1}{m-1}\sum_{i=1}^m \big(R_p(t_{i-1}, t_i) - \hat{\mu}_p^m\big)^2}.$$

We define the covariance of two securities A and B as

$$\sigma_{AB} = \mathbb{E}[(R_A - \mu_A)(R_B - \mu_B)]$$

and sample covariance

$$\hat{\sigma}_{AB}^m = \frac{1}{m-1}\sum_{i=1}^m \big(\hat{R}_A(t_{i-1}, t_i) - \bar{R}_A\big)\big(\hat{R}_B(t_{i-1}, t_i) - \bar{R}_B\big).$$

Lastly, define the correlation coefficient of two securities as

$$\rho_{AB} = \frac{\sigma_{AB}}{\sigma_A \sigma_B}$$

where the sample correlation uses sample risk and covariance of A and B. The correlation coefficient is a unit-independent measure that will help in quantifying how two random variables vary relative to one another.

In section 6.1, we observed how to quantify risk of a single cryptocurrency. Assume now that we wish to invest in two cryptocurrencies. The fundamental question we must ask is, "what percentage of money $V_p(t_0)$ should we allocate today to each cryptocurrency in order to create an efficient portfolio?" Once we observe how to do this with two cryptocurrencies, we will be able to generalize to larger portfolios.

Let's assume we wish to invest in Bitcoin and Ethereum as these are the two largest cryptocurrencies by market cap and are relatively less risky than other cryptocurrencies according to our VAR model. Let w_1, w_2 be the (non-zero) weights of Bitcoin and Ethereum in our portfolio respectively. Thus,

$$w = \begin{bmatrix} w_1 \\ w_2 \end{bmatrix}$$

such that $w_1 + w_2 = 1$, or in matrix form, letting

$$e = \begin{bmatrix} 1 \\ 1 \end{bmatrix},$$

$$1 = w_1 + w_2 = w^T e$$

To further our notation, we have that

$$R = \begin{bmatrix} R_1 \\ R_2 \end{bmatrix}$$
$$\boldsymbol{\mu} = \mathbb{E}[R] = \begin{bmatrix} \mu_1 \\ \mu_2 \end{bmatrix}$$
$$\Sigma = \begin{bmatrix} \sigma_1^2 & \sigma_{12} \\ \sigma_{12} & \sigma_2^2 \end{bmatrix}$$

where $\sigma_{12} = \rho_{12}\sigma_1\sigma_2$ is the covariance of Bitcoin and Ethereum, μ is the expected return of Bitcoin and Ethereum, and Σ is the covariance matrix of Bitcoin and Ethereum. Thus, the expected portfolio return $\mu_p(w)$ and portfolio risk $\sigma_p(w)$ are defined as

$$\mu_p(w) = w_1\mu_1 + w_2\mu_2 = \mu^T w$$
$$\sigma_p(w) = \sqrt{w_1^2\sigma_1^2 + w_2^2\sigma_2^2 + 2w_1w_2\rho_{12}\sigma_1\sigma_2} = \sqrt{w^T\Sigma w}.$$

We assume that $\mu \neq 0$ and $\mu_1 \neq \mu_2$. Furthermore, we claim that the $n \times n$ (in this case 2 by 2) covariance matrix Σ is positive definite, i.e.

$$x^T\Sigma x > 0 \quad \forall x \neq 0 \in \mathbb{R}^n$$

In this case,

$$\sigma_1^2, \sigma_2^2 > 0$$

and

$$|\Sigma| = (1 - \rho_{12})(\sigma_1\sigma_2)^2 > 0$$

where $|\Sigma|$ is the determinant of Σ. This means that the eigenvalues λ_1, λ_2 of Σ are positive since $\lambda_1 + \lambda_2 = tr(\Sigma) = \sigma_1^2 + \sigma_2^2 > 0$ and $\lambda_1\lambda_2 = |\Sigma| > 0$. A matrix is positive definite if and only if its eigenvalues are positive, thus Σ is positive definite. We now define the following properties:

1. Since $w \neq 0$, the positive definiteness of Σ implies that the portfolio always has risk since

   $$\sigma_p(w) = \sqrt{w^T\Sigma w} > 0$$

   for all w.

2. The positive definiteness of Σ implies that Σ is invertible and its symmetric inverse

   $$\Sigma^{-1} = \frac{1}{|\Sigma|}\begin{bmatrix} \sigma_2^2 & -\rho_{12}\sigma_1\sigma_2 \\ -\rho_{12}\sigma_1\sigma_2 & \sigma_1^2 \end{bmatrix}$$

   is also positive definite.

3. We introduce the following quantities which will come in handy later:

   $$A = e^T\Sigma^{-1}e = \frac{\sigma_1^2 + \sigma_2^2 - 2\rho_{12}\sigma_1\sigma_2}{|\Sigma|}$$
   $$B = \mu^T\Sigma^{-1}e = \frac{(\sigma_2^2 - \rho_{12}\sigma_1\sigma_2)\mu_1 + (\sigma_1^2 - \rho_{12}\sigma_1\sigma_2)\mu_2}{|\Sigma|}$$
   $$C = \mu^T\Sigma^{-1}\mu = \frac{\sigma_1^2\mu_2^2 + \sigma_2^2\mu_1^2 - 2\rho_{12}\sigma_1\sigma_2\mu_1\mu_2}{|\Sigma|}$$
   $$AC - B^2 = \frac{(\mu_1 - \mu_2)^2}{|\Sigma|}$$

Our goal now is to attempt to *minimize* the risk of our portfolio containing Bitcoin and Ethereum. That is, we wish to solve the following optimization problem:

$$\min_w \sigma_p(w) = \sqrt{w^T \Sigma w}$$

w.r.t

$$w^T e = 1, \quad w^T \boldsymbol{\mu} = \mu$$

or equivalently,

$$\underbrace{\begin{bmatrix} 1 & 1 \\ \mu_1 & \mu_2 \end{bmatrix}}_{K} \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} = \begin{bmatrix} 1 \\ \mu \end{bmatrix}.$$

and we can solve for w:

$$\begin{bmatrix} w_1 \\ w_2 \end{bmatrix} = K^{-1} \begin{bmatrix} 1 \\ \mu \end{bmatrix}.$$

such that

$$K^{-1} = \frac{1}{\mu_2 - \mu_1} \begin{bmatrix} \mu_2 & -1 \\ -1 & \mu_1 \end{bmatrix}.$$

Thus,

$$w^* = \begin{bmatrix} w^* \\ 1 - w^* \end{bmatrix} = \frac{1}{\mu_1 - \mu_2} \begin{bmatrix} \mu - \mu_2 \\ \mu_1 - \mu \end{bmatrix} \tag{5.2}$$

We will generalize without proof that this equates to

$$w^* = \big(\frac{C - \mu B}{AC - B^2}\big)\Sigma^{-1} e + \big(\frac{\mu A - B}{AC - B^2}\big)\Sigma^{-1}\boldsymbol{\mu}.$$

Let us now solve for the minimum risk diversification of our BTC, ETH portfolio. We can solve for the global minimum of $\sigma_p^2(w^*)$ (since it is quadratic) such that

$$\sigma_p(w^*) = \sigma_p(\mu)$$

i.e.

$$\sigma_p^2(\mu) = w^{*T}\Sigma w^* = \big(\sigma_1^2 + \sigma_2^2 - 2\rho_{12}\sigma_1\sigma_2\big)w^{*2} + 2\big(\rho_{12}\sigma_1\sigma_2 - \sigma_2^2\big) + \sigma_2^2.$$

Substituting (5.2) we achieve

$$w^* = \frac{\mu - \mu_2}{\mu_1 - \mu_2}$$

which yields

$$\sigma_p^2(\mu) = \frac{A\mu^2 - 2B\mu + C}{AC - B^2}.$$

We can complete the square to achieve

$$\sigma_p^2(\mu) = \frac{A}{AC - B^2}\big(\mu - \frac{B}{A}\big)^2 + \frac{1}{A}$$

and solve for (σ_p, μ_p) on their respective plane. Thus, let $\sigma_p(\mu) = \sigma_p$ and $\mu_p = \mu$. We can write the above formula in hyperbola notation:

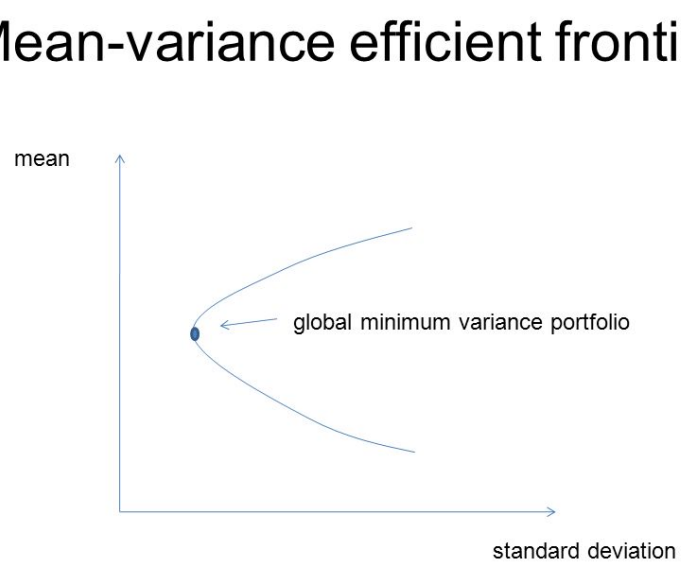
$$\frac{\sigma_p^2}{\frac{1}{A}} - \frac{\big(\mu_p - \frac{B}{A}\big)^2}{\frac{AC - B^2}{A^2}} = 1.$$

Since $\sigma_p > 0$, we can solve for the vertex of this is equation, which is equivalent to the global minimum-variance portfolio, denoted $(\sigma_G, \mu_G) = (\frac{1}{\sqrt{A}}, \frac{B}{A})$. If we solve for w^* we get

$$w^* = \frac{\Sigma^{-1} e}{e^T \Sigma^{-1} e}$$

where $w^* = [w_1^* \;\; w_2^*]^T$ is our minimum-risk weighting of Bitcoin and Ethereum respectively. Note that if we plot this

curve, it should look something like this:



Let's apply this using real data. Note that we have to convert to the empirical world, i.e. let $X_i \in \mathbb{R}^2$ such that $X_i(1)$ and $X_i(2)$ are the *weekly* returns of Bitcoin and Ethereum respectively on week $i = 0, ..., n$. If $p(1)_i, p(2)_i$ are the prices of Bitcoin and Ethereum respectively, then

$$X(j)_i = \frac{p(j)_i - p(j)_{i-1}}{p(j)_{i-1}}, \quad j = 1, 2$$

is the weekly return on week i. To construct the mean of each asset, we apply the formula

$$\hat{\mu_j} = \frac{1}{n} \sum_{i=1}^{n} X(j)_i$$

for $j = 1, 2$ such that $\hat{\mu} = \begin{bmatrix} \hat{\mu}_1 \\ \hat{\mu}_2 \end{bmatrix}$ and

$$\hat{\Sigma} = \frac{1}{n-1}(X - \hat{\mu}^T)^T(X - \hat{\mu}^T) = \begin{bmatrix} \hat{\sigma}_1^2 & \hat{\sigma}_{12} \\ \hat{\sigma}_{12} & \hat{\sigma}_2^2 \end{bmatrix}$$

are the empircal mean and covariance matrix respectively. We can then solve for $(\sigma_G, \mu_G) = (\frac{1}{\sqrt{A}}, \frac{B}{A})$ and w^* such that

$$A = e^T \hat{\Sigma}^{-1} e$$
$$B = \mu^T \hat{\Sigma}^{-1} e$$
$$w^* = \frac{\hat{\Sigma}^{-1} e}{e^T \hat{\Sigma}^{-1} e}$$

Using our data, we achieve the following values:

$$\hat{\mu_1} = 3.575\%$$
$$\hat{\mu_2} = 5.361\%$$
$$\hat{\sigma_1} = 12.51\%$$
$$\hat{\sigma_2} = 20.23\%$$
$$\hat{\sigma}_{12} = 0.748\%$$
$$\hat{\rho}_{12} = \frac{\hat{\sigma}_{12}}{\hat{\sigma}_1 \hat{\sigma}_2} = 1.209\%$$

Solving for our minimum-risk portfolio, we achieve the following values (rounded to 4 figures):

$$\mu_G = 3.926\%$$
$$\sigma_G = 11.85\%$$
$$w^* = \begin{bmatrix} 0.8035 \\ 0.1965 \end{bmatrix}$$

We find that our optimal portfolio contains 80.35% BTC and 19.65% ETH, achieving a slightly higher expected monthly return than Bitcoin alone and slightly less expected risk as well. Of course, since this is based on historical data, we must proceed with caution since the past cannot always accurately depict the future. That being said, using empirical measures help us better understand how to diversify our investments, especially when dealing with high variance assets.

If we want to increase our portfolio to more than two cryptocurrencies, we can easily generalize by increasing the number of columns in X and proceeding with the same calculations!

5.2.3 Python Code

```
# The following code is used to determine
# the minimum risk portfolio containing BTC and ETH
import quandl
import pandas as pd
import numpy as np
import matplotlib.pyplot as plt

# Import Data from Quandl
btc = quandl.get("BITFINEX/BTCUSD", authtoken="nyEaBHLDxQ7WB6GX5mbt")
eth = quandl.get("BITFINEX/ETHUSD", authtoken="nyEaBHLDxQ7WB6GX5mbt")
'''
writer = pd.ExcelWriter('BTC.xlsx')
btc.to_excel(writer,'Sheet1')
writer.save()
'''
# Extract Close Prices
btc = btc['Last']
btc = btc[-730::]
btcR = btc.copy()
eth = eth['Last']
eth = eth[-730::]
ethR = eth.copy()
```

```
# Specify Time Range
t = 7

# Iterate over days to achieve returns
for i in range(1,int(len(eth)/t)):
        btcR[i] = (btc[i*t] - btc[(i-1)*t])/btc[(i-1)*t]
        ethR[i] = (eth[i*t] - eth[(i-1)*t])/eth[(i-1)*t]

# Convert to array
btcR = np.array(btcR[1:int(len(eth)/t)])
ethR = np.array(ethR[1:int(len(eth)/t)])

# Aggregate Returns and create Covariance Matrix
X = np.matrix(np.vstack((btcR,ethR)).transpose())
Xhat = X - np.mean(X,0)
Cov = (1/(np.size(X,0)-1))*Xhat.transpose()*Xhat

# Calculate Minimal Risk Portfolio:
mu = np.mean(X,0).transpose()
CovInv = np.linalg.inv(Cov)
rho = Cov[0,1]/np.sqrt(Cov[0,0])*np.sqrt(Cov[1,1])
e = np.matrix([1,1]).transpose()
A = float(e.transpose()*CovInv*e)
B = float(mu.transpose()*CovInv*e)

sigmaG = 1/np.sqrt(A)
muG = B/A

wG = (CovInv*e)/(e.transpose()*CovInv*e)
```

5.3 The Markovity of the Cryptocurrency Market

5.3.1 Simplification to a Three State Market

Markov chains are very useful tools in measuring how random variables evolve over time. For the following section, we will assume that market sentiment i.e. bearish (-1), bullish (+1), or stagnant (0), is a Markov chain with respect to time. To clarify, let $Y = \{Y_0, Y_1, ..., Y_n\}$ be the sequence of market sentiment and let Y_i be the market sentiment at time i. We assume that at any given discrete time $t = 0, ..., n$,

$$\mathbb{P}(Y_t|Y_{t-1}, ..., Y_1, Y_0) = \mathbb{P}(Y_t|Y_{t-1})$$

i.e, the probability of Y_t is only conditional on the previous Y_{t-1}. we will also assume that this Markov chain is stationary in time, meaning

$$\mathbb{P}(Y_t|Y_{t-1}) = \mathbb{P}(Y_{t+l}|Y_{t+l-1})$$

for $l = 0, 1, 2....$ These assumptions will allow us to measure the "Markovity" of the cryptocurrency market through observations of price data. We can consider any cryptocurrency alone or a combination of many. For simplicity, we will consider the case where we only own Bitcoin. First, let us consider the case when Y is an observable variable defined

arbitrarily as

$$Y_t = \begin{cases} 1 & \text{if } R_t > 2\% \\ -1 & \text{if } R_t < -2\% \\ 0 & \text{otherwise} \end{cases}$$

where R_t is the weekly return at time t. Using daily price data, we can construct each R_t for a given time interval and define the probability transision matrix Q such that $Q_{ij} = \mathbb{P}(Y_t = y_j | Y_{t-1} = y_i)$ where i and j are indexed according to the above definition of Y. Since we assume Y is stationary, we have that Q is a stationary transition matrix. Using the same dataset as in the previous section, we can construct a transition matrix for Bitcoin's weekly market sentiment. We will proceed in MATLAB since this platform suits Markov chain analysis very well.

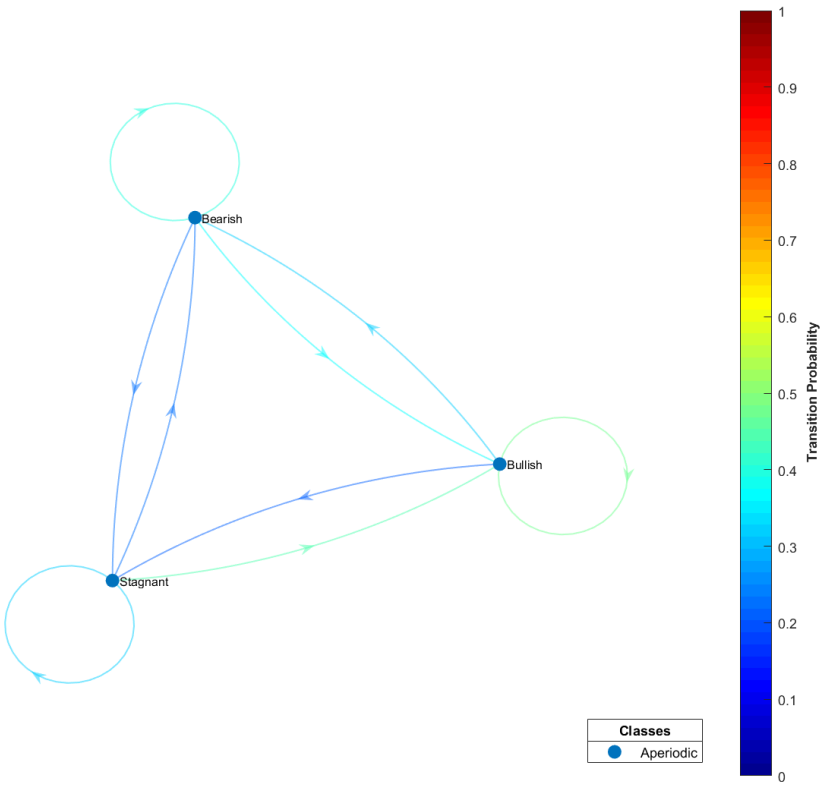
To begin, when we import our data we must convert from R_i to Y_i for all i as previously mentioned. Then, we construct a rolling window matrix such the ith row contains the i^{th} and $i + 1^{th}$ Y values, which visually looks like this:

$$\begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ \vdots \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 2 \\ 2 & 3 \\ 3 & 4 \\ 4 & 5 \\ 5 & 6 \\ \vdots & \vdots \end{bmatrix}.$$

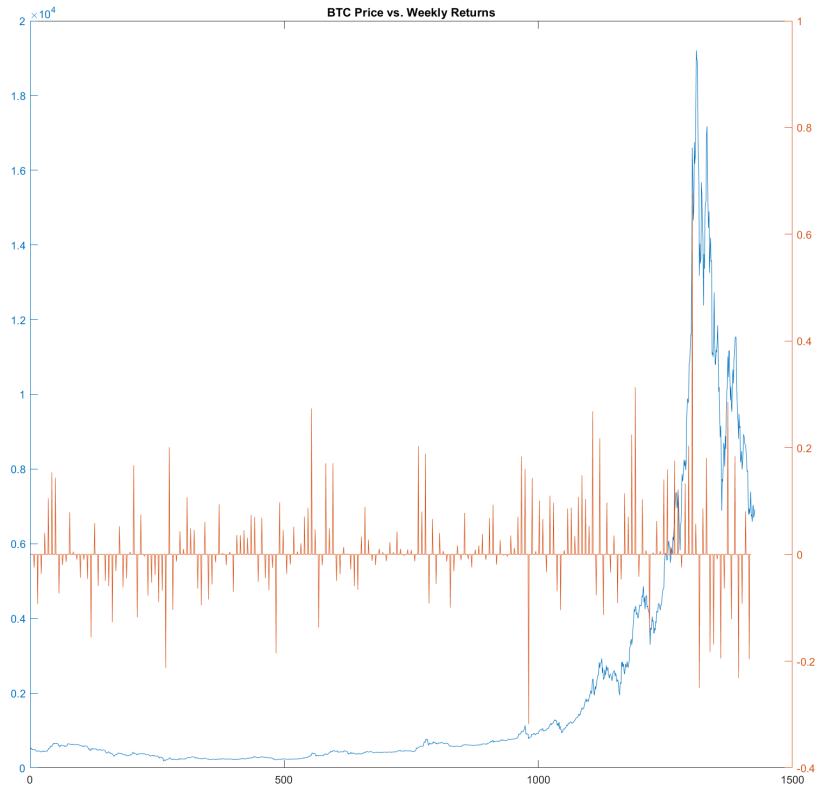
From here, we can easily compute Q. We obtain the following:

$$Q = \begin{bmatrix} 0.4030 & 0.2239 & 0.3731 \\ 0.2340 & 0.3191 & 0.4468 \\ 0.3182 & 0.2045 & 0.4773 \end{bmatrix}.$$

Note that $\sum_{j=1}^{3} Q_{ij} = 1$ where the row of Q indicates the preceding Y value and the column indicates the probability of transition to the next Y value conditional on the preceding one. This is indexed in the order -1,0,1. We can plot the directed weighted graph associated to this Markov chain to get a better idea as to what's going on:



We see that in a bearish market, we are most likely to continue being in a bear market; in a bull market, we are most likely to stay in a bull market; and in a stagnant market, we are most likely to transition to a bull market. Interestingly, it seems as though no state is entirely dominant. This is most likely due to the high variance of BTC returns. If we plot weekly returns vs. price, we get the following:

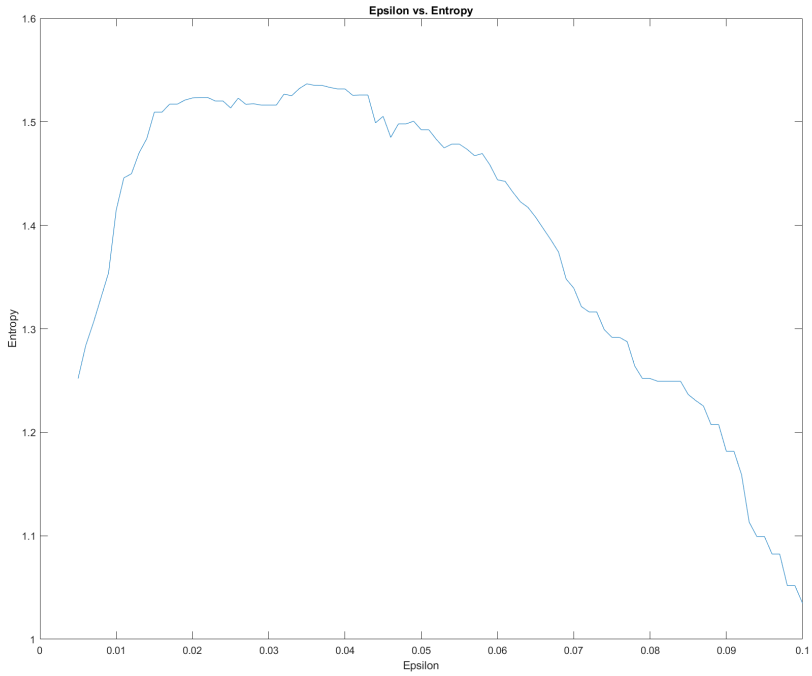


We see how we can have very good returns one week but quickly transition to losses, giving way to high uncertainty. To quantify this uncertainty, we can calculate the entropy rate of this Markov chain, i.e.

$$H(Y) = -\sum_{ij} \mu_i Q_{ij} \log_2(Q_{ij})$$

where μ is the stationary distribution of Q such that $\mu Q = \mu$. In our case, we can calculate μ using the probability of each state unconditioned on the previous state. We get that $H(Y) = 1.5238$ bits, which nearly the maximum possible value of entropy! This is because entropy is maximized over a uniform distribution, which in this case would yield $H(Y) = \log_2(3) = 1.585$ bits. Therefore, Bitcoin returns discretized in terms of market sentiment are very uncertain.

Let us define ϵ as the threshold for stagnant market, i.e. $Y_t = 0$ if $-\epsilon \leq R_t \leq \epsilon$. In the above calculations, we chose $\epsilon = 0.02$. Let's now discover how changing ϵ affects $H(Y)$. If we plot $H(Y)$ over a range of many choices ϵ, we achieve the following plot:



We find that the entropy rate is maximized at 1.5368 bits when $\epsilon = 0.035 = 3.5\%$. This is a helpful way to tune our parameter for defining a stagnant market. If ϵ is too small, then we will rarely every get $Y_t = 0$. On the other hand, if ϵ is too large, we will get $Y_t = 0$ too much of the time. $\epsilon = 3.5\%$ gives us the most uniformity over the three states and is therefore the most informative in separating what defines a bearish vs. bullish market. Given that market sentiment is relatively subjective, we must attempt to figure out the best possible mathematical definition, and using entropy helps us do so.

5.3.2 MATLAB Code

```
% Import BTC Daily Price Data
btc = xlsread('BTC.xlsx');
btc = btc(:,5);

% Convert to time frame t
t = 7;

% Init Parameters
R = zeros(length(btc)-t,1);
Y = R;
e = 0.001*(5:100);
entropy = zeros(length(e),1);

% Iterate over all e
for j = 1:length(e)
        for i = (t+1):t:(length(btc)-t)
                R(i) = (btc(i) - btc(i-t))/btc(i-t);
                if R(i) >= e(j)
                        Y(i) = 1;
                elseif R(i) < -e(j)
```

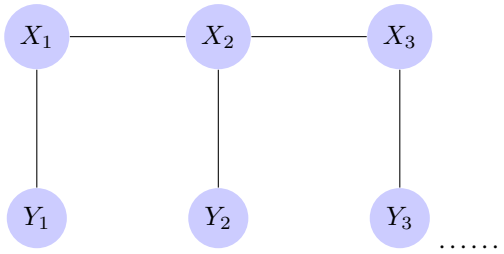
```
                Y(i) = -1;
            else
                Y(i) = 0;
        end
end

% Create Y and Q
Y = Y(1:t:end);
Q = createQ(Y);

% Calc entropy
mu = tabulate(Y);
mu = mu(:,3)/100;
entropy(j) = -sum(mu'*(Q.*log2(Q)));
end

% Plotting
plot(e,entropy)
title('Epsilon vs. Entropy')
ylabel('Entropy')
xlabel('Epsilon')
%{
mc = dtmc(Q,'StateNames',["Bearish","Stagnant","Bullish"]);
figure;
graphplot(mc,'ColorNodes',true,'ColorEdges',true);
%}
%{
R = R(1:t:end);
yyaxis right
plot(R)
yyaxis left
plot(btc)
title('BTC Price vs. Weekly Returns')
%}

function [tranMatrix] = createQ(Z)
%createQ generates the transition matrix of the sample distribution.

Y = createRollingWindow(Z,2);
tranMatrix = zeros(3);

for i = -1:1
        I = Y(Y(:,1) == i,:);
        M = tabulate(I(:,2));
        tranMatrix(i+2,:) = M(:,3)./100;
end

function output = createRollingWindow(vector, n)
% CREATEROLLINGWINDOW returns successive overlapping windows onto a vector
```

```
%   OUTPUT = CREATEROLLINGWINDOW(VECTOR, N) takes a numerical vector VECTOR
%   and a positive integer scalar N. The result OUTPUT is an MxN matrix,
%   where M = length(VECTOR)-N+1. The I'th row of OUTPUT contains
%   VECTOR(I:I+N-1).
l = length(vector);
m = l - n + 1;
output = vector(hankel(1:m, m:l));
end
```

5.4 Hidden Markov Model for Price Prediction

To improve our previous model, let's now assume that market sentiment is a *hidden* Markov chain. This means that while we observe the price of Bitcoin over time, we assume that we cannot directly observe market sentiment. Rather, the set of observables, i.e. returns over a certain time period, depend only on the hidden random variables. Additionally the ith random variable conditioned on the $(i-1)$th hidden variable is independent of previous hidden variables. This model works well when applied to stock prices since although we can observe price fluctuations, there is so much more going on "behind the scenes." We therefore attempt to figure out what is going on that we cannot see.

Graphically, the model will look something like this:



Here, the hidden variables are $X_1, ..., X_n$ while the observed variables are $Y_1, ..., Y_n$. In this case, will consider a similar discrete Y as before, however, we now consider the case where time t is discretized *daily* and R_t is the daily return at t:

$$Y_t = \begin{cases} 1 & \text{if } R_t > \epsilon \\ 2 & \text{if } -\epsilon \leq R_t \leq \epsilon \\ 3 & \text{if } R_t < -\epsilon \end{cases}$$

In the last section, we defined $\epsilon^* = \underset{\epsilon}{\text{argmax}}\ H(Y;\epsilon)$, and we will do the same here. We find that for daily returns over the past 200 days, $\epsilon^* = 0.019 = 1.9\%$. $Y_t \in \{1,2,3\}$ translates roughly to "bearish, stagnant, and bullish," respectively. We use Y_t as our observable both for simplicity and so that we may use the Baum-Welch algorithm, which relies on discrete observables.

5.4.1 The Baum-Welch Algorithm

We assume that X_t is a discrete hidden random variable with N possible states. For simplicity, let $N = 3$ such that X has the same number of states as observable Y. We assume $\mathbb{P}(X_t|X_{t-1})$ is independent of time t, leading to the following definition of the time-independent stochastic transition matrix

$$A = \{a_{ij}\} = \mathbb{P}\big(X_t = j | X_{t-1} = i\big).$$

The initial state distribution ($t = 1$) is given by

$$\pi_i = \mathbb{P}\big(X_1 = i\big).$$

We assume the observation given the "hidden" state is time independent. The probability of a certain observation y_i at time t for state $X_t = j$ is given by

$$b_j(y_i) = \mathbb{P}\big(Y_t = y_i | X_t = j\big).$$

If we take into account all possible values of Y_t and X_t, we obtain the 3×3 matrix $B = \{b_j(y_i)\}$ where b_j belongs to all the possible states and y_i belongs to all the observations.

The observation sequence is given by $Y = (Y_1 = y_i, Y_2 = y_2, ...Y_T = y_T)$. In our case, we wish to observe data over the last 200 days, thus $T = 200$. We can describe a hidden Markov chain by $\theta = (A, B, \pi)$. The Baum-Welch algorithm finds a local maximum for $\theta^* = \text{argmax}_\theta \mathbb{P}(Y|\theta)$.

The Algorithm:
Set $\theta = (A, B, \pi)$ with random initial conditions. In our case, we will attempt to set up a good initialization to speed up the algorithm and steer it toward the desired local maximum.

Forward Propagation:
Let $\alpha_i(t) = \mathbb{P}(Y_1 = y_1, ..., Y_t = y_t, X_t = i|\theta)$ be the probability of seeing $y_1, ..., y_t$ being in state i at time t. We find α_i recursively:

1.
$$\alpha_i(1) = \pi_i b_i(y_1)$$

2.
$$\alpha_i(t+1) = b_i(y_{t+1}) \sum_{j=1}^{N} \alpha_j(t) a_{ji}$$

Backward Propagation:
Let $\beta_i(t) = \mathbb{P}(Y_{t+1} = y_{t+1}, ..., Y_T = y_T | X_t = i, \theta)$ be the probability of ending the partial sequence $y_{t+1}, ...y_T$ given the starting state i at time t. We calculate $\beta_i(t)$ as

1.
$$\beta_i(T) = 1$$

2.
$$\beta_i(t) = \sum_{j=1}^{N} \beta_j(t+1) a_{ij} b_j(y_{t+1})$$

Update:
We can now calculate the following temporary variables, according to Bayes' Theorem:

$$\gamma_i(t) = \mathbb{P}(X_t = i|Y, \theta) = \frac{\mathbb{P}(X_t = i, Y|\theta)}{\mathbb{P}(Y|\theta)} = \frac{\alpha_i(t)\beta_i(t)}{\sum_{j=1}^{N} \alpha_j(t)\beta_j(t)}$$

which is the probability of being in state i at time t given the observed sequence Y and the parameters θ.

$$\eta_{ij}(t) = \mathbb{P}(X_t = i, X_{t+1} = j|Y, \theta) = \frac{\mathbb{P}(X_t = i, X_{t+1} = j, Y|\theta)}{\mathbb{P}(Y|\theta)} = \frac{\alpha_i(t) a_{ij} \beta_j(t+1) b_j(y_{t+1})}{\sum_{i=1}^{N} \sum_{j=1}^{N} \alpha_i(t) a_{ij} \beta_j(t+1) b_j(y_{t+1})}$$

which is the probability of being in state i and j at times t and $t+1$ respectively given the observed sequence Y and parameters θ. The parameters of the hidden Markov model θ can now be updated:

1. $\pi_i^* = \gamma_i(1)$.
2. $a_{ij}^* = \frac{\sum_{t=1}^{T-1} \eta_{ij}(t)}{\sum_{t=1}^{T-1} \gamma_i(t)}$.

3. $b_i^*(v_k) = \frac{\sum_{i=1}^T \mathbb{1}_{y_t=v_k}\gamma_i(t)}{\sum_{t=1}^T \gamma_i(t)}$.

If we initialize

$$A^0 = B^0 = \begin{bmatrix} 0.5 & 0.25 & 0.25 \\ 0.25 & 0.5 & 0.25 \\ 0.25 & 0.25 & 0.5 \end{bmatrix}$$

and

$$\pi^0 = \begin{bmatrix} \frac{1}{3} \\ \frac{1}{3} \\ \frac{1}{3} \end{bmatrix}$$

we converge after about two hundred iterations to

$$A^* = \begin{bmatrix} 0.5022 & 0.1133 & 0.3845 \\ 0.5372 & 0.0055 & 0.4573 \\ 0.5237 & 0.0307 & 0.4455 \end{bmatrix}$$

$$B^* = \begin{bmatrix} 0.7301 & 0.2699 & 0.0000 \\ 0.3792 & 0.4017 & 0.2191 \\ 0.0037 & 0.2758 & 0.7205 \end{bmatrix}$$

$$\pi^* = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

The algorithm works as we would have hoped and converges to hidden parameters that contain a good amount of information about the observed variable. $Y_t = 1$ has a large chance of occuring given $X_t = 1$ and $Y_t = 3$ has a large probability of occurring given $X_t = 3$. Meanwhile, Y_t is more uniform given X_2, however $Y_t = 2$ is most probable. Additionally, as we can see by A, the probability of $X_t = 2$ conditioned on $X_{t-1} = x_{t-1}$ is rather small, so this hidden variable is less probable than the others. We see that under this convergence, $\mathbb{P}(X_1 = 3) = 1$.

We can now use dynamic programming and attempt to uncover the most likely configuration for $X_1, ..., X_T$ given $Y_1, ..., Y_T$. Using Bayes' Rule and Markovity, we have

$$\mathbb{P}(X_1, ..., X_t | Y_1 = y_1, ..., Y_t = y_t) = \frac{\prod_{i=1}^t \mathbb{P}(Y_i|X_i = x_i)\prod_{i=2}^t \mathbb{P}(X_i|X_{i-1} = x_{i-1})\mathbb{P}(X_1 = x_1)}{\mathbb{P}(Y_1 = y_1, ..., Y_t = y_t)}$$

for $t = 2, ..., T$. To solve for the above quantity up to T, we can maximize the likelihood given the data Y and our previously calculated parameters $\theta^* = (A^*, B^*, \pi^*)$. Define $L(P)$ as the log-likelihood of the above probability (which we use for numerical stability). We have that

$$L(P) = \log(\mathbb{P}(X_1 = x_1)) + \sum_{i=2}^T \log(\mathbb{P}(X_i|X_{i-1} = x_{i-1})) + \sum_{i=1}^T \log(\mathbb{P}(Y_i|X_i = x_{i-1})) - \log(\mathbb{P}(Y_1 = y_1, ..., Y_T = y_T)).$$

Since the last term is constant (we are given Y), we will ignore it. Thus, substituting our parameters, we have

$$L(P) = \log(\pi^*) + \sum_{i=2}^T \log(\mathbb{P}(A^*(X_{i-1}, X_i)) + \sum_{i=1}^T \log(B^*(X_i, Y_i))$$

We wish to maximize the above quantity over X. Searching over all possible vectors X is computationally infeasible, so we will do so using the following method.

5.4.2 Dynamic Programming Most Likely HMM Configuration

Let $(A^*, B^*, \pi^*) = (A, B, \pi)$.

1. Let

$$M_1(X_2) = \max_{X_1} \quad \log(A(X_1, X_2)) + \log(B(X_1, Y_1)) + \log(\pi)$$
$$R_1(X_2) = \operatorname{argmax}_{X_1} \quad \log(A(X_1, X_2)) + \log(B(X_1, Y_1)) + \log(\pi)$$

   be lookup tables for every possible X_2.

2. For $t = 2, ..., T-1$, let

$$M_t(X_{t+1}) = \max_{X_t} \quad \log(A(X_t, X_{t+1})) + \log(B(X_t, Y_t)) + M_{t-1}(X_t)$$
$$R_t(X_{t+1}) = \operatorname{argmax}_{X_t} \quad \log(A(X_t, X_{t+1})) + \log(B(X_t, Y_t)) + M_{t-1}(X_t)$$

   be lookup tables for every possible X_{t+1}.

3. On the last step T, we have that

$$R_T = \operatorname{argmax}_{X_T} \quad \log(B(X_T, Y_T)) + M_{T-1}(X_T).$$

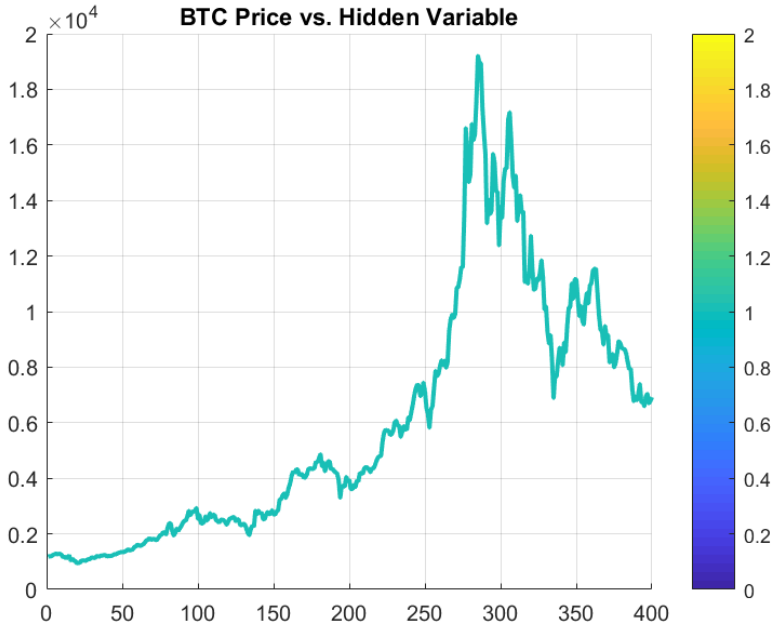
4. We now solve backwards:

$$X_T^* = R_T$$
$$X_t^* = R_t(X_{t+1}^*)$$

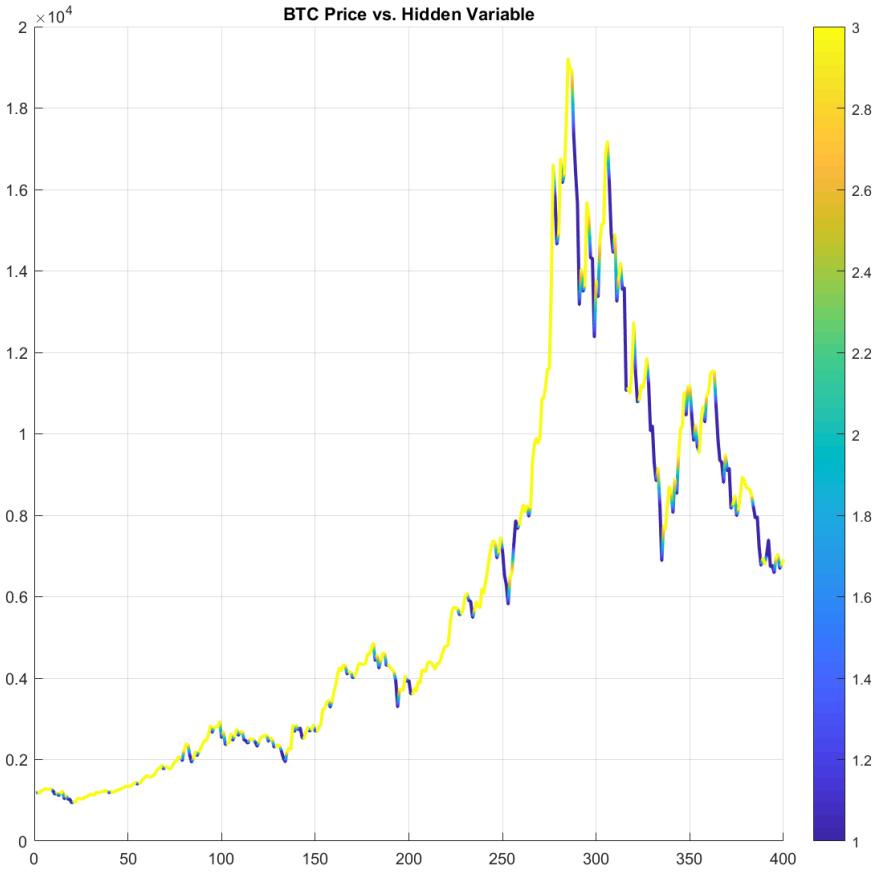
   for $t = T-1, ..., 1$.

Setting $\epsilon = \epsilon^*$ yields $X_t^* = Y_t$ for nearly all t. This makes sense since we have shown that B is dominant along the diagonal. What happens when we tune ϵ? How about if we change the time scale T? This provides more interesting results. Note that we initialize θ^0 the same as before.

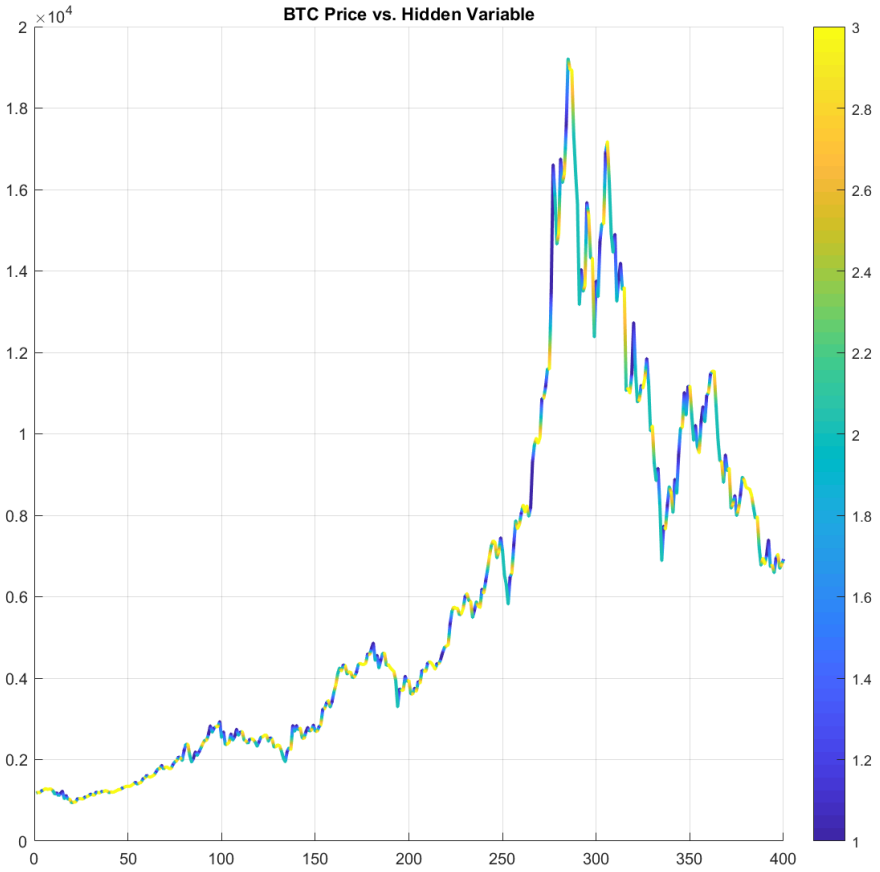
Let's set $T = 400$ and define $\epsilon = c\epsilon^*$ for some constant c and defining Y the using this new value of ϵ. Recall that ϵ^* leads to Y having maximum entropy when it is itself defined as a Markov chain. Setting $c = 1$ and plotting X^* by color over the plot of Bitcoin price, we achieve the following plot:



We see that $X_t = 1$ for all t. Let's now increase c. For $c = 1.2$:



We begin to see some diversification in X^*! In fact, X^* takes only values 1 and 3 where 3 seems to indicate a bearish trend while 1 indicates a bullish trend. For $c = 1.4$:



We see that $X^* = 2$ indicates a bearish trend, $X^* = 3$ indicates a somewhat stagnant trend, and $X^* = 1$ indicates a bullish trend. Given the abstraction of X, the trend provided by each value depends greatly on the value of c and requires analysis of the plot. Furthermore, the ordering of X is independent from Y. These hidden Markov models, when studied visually, are very informative when applied to trend analysis. By increasing the value of c (decreasing $c < 1$ leads to $X_t = 1$ for all t), we gain different segmentations of X, each containing a moderate to completely different output than the associated observed Y variable. The hope, from a trading standpoint, would be to utilize HMM's on a prefered time scale to predict future trends. It seems, in our case, that these HMMs contain sticky hidden variables, meaning that they will last at least a few days. For instance, if we were to see a transition from a bearish or stagnant hidden variable to a bullish hidden variable at the latest time T, we could view this as a good point to enter the market. A forewarning is that solving for X^* using dynamic programming merely computes the *most likely* configuration, and is thus subject to error. A way to expand this model would be to try a different number of observed and hidden states and compare results.

5.4.3 MATLAB Code

```
function [A,B,p] = BWalgo(Y,A,B,p)
%BWalgo uses the Baum Welch Algorithm. It takes as input observables Y,
% matrices A,B and p and outputs optimal values for each.

T = length(Y);
[N,K] = size(B);

alpha = zeros(N,T);
beta = zeros(N,T);
```

```
gamma    = zeros(N,T);
eta      = zeros(N,N,T-1);

% Forward prop
alpha(:,1)   = p.*B(:,Y(1));
for t = 2:T
        alpha(:,t)   = B(:,Y(t)).*(A*alpha(:,t-1));
end

% Backward prop
beta(:,T) = 1;
for t = fliplr(1:(T-1))
        beta(:,t) = A*(beta(:,t+1).*B(:,Y(t)));
end

% Update
for t = 1:T-1
        gamma(:,t) = alpha(:,t).*beta(:,t)/sum(alpha(:,t).*beta(:,t));
        eta(:,:,t) = alpha(:,t).*A.*(beta(:,t+1).*B(:,Y(t+1)))';
        eta(:,:,t) = eta(:,:,t)/sum(sum(eta(:,:,t)));
end

gamma(:,T) = alpha(:,T).*beta(:,T)/sum(alpha(:,T).*beta(:,T));

p = gamma(:,1);
A = sum(eta,3);
A = A./sum(A,2);

for k = 1:K
        B(:,k) = sum(((Y==k).*ones(N,1)')'.*gamma,2)./sum(gamma,2);
end


function [X] = HMMdp(Y,A,B,p)
%HMMdp solves for the most likely configuration of X given theta parameters
% using dynamic programming

[N,~] = size(B);
T = length(Y);
M = zeros(N,T-1);
R = zeros(N,T-1);
X = zeros(T,1);

% Forward Prop

for i = 1:N
        [M(i,1),R(i,1)] = max(log(p) + log(A(:,i)) + log(B(:,Y(1))));
end
```

```
for t = 2:T-1
        for i = 1:N
                [M(i,t),R(i,t)] = max(log(A(:,i)) + log(B(:,Y(t))) + log(M(:,t-1)));
        end
end

% Backward Prop

[~,RT] = max(B(:,Y(T))+M(:,T-1));
X(T) = RT;

for t = fliplr(1:(T-1))
        X(t) = R(X(t+1),t);
end



[~,I] = max(entropy)
eStar = entropy(I);

% FIT HMM BY TUNING C

Y = zeros(length(btc)-1,1);
R = Y;
c = 1.4;
        for i = 2:length(btc)
                R(i) = (btc(i) - btc(i-t))/btc(i-t);
                if R(i) > c*eStar
                        Y(i) = 1;
                elseif R(i) < -c*eStar
                        Y(i) = 3;
                else
                        Y(i) = 2;
                end
        end
Y = Y(2:end);

% Init HMM

A = 0.25*(ones(3)+eye(3));
B = A;
p = (1/3)*ones(3,1);


% Solve for optimal hidden variable prob
iter = 200;
for i = 1:iter
        [A,B,p] = BWalgo(Y,A,B,p);
end
```

```
X = HMMdp(Y,A,B,p);

x = 1:length(X) ; % extract "X" column
y = btc(2:end);
z= X; % everything in the Z=0 plane

% Draw the surface (actually a line)
hs=surf([x(:) x(:)],[y(:) y(:)],[z(:) z(:)], ... % Reshape and replicate data
'FaceColor', 'none', ... % Don't bother filling faces with color
'EdgeColor', 'interp', ... % Use interpolated color for edges
'LineWidth', 2);

view(2);
colorbar
title('BTC Price vs. Hidden Variable')
%{
yyaxis right
plot(btc)
yyaxis left
p1 = plot(X,'LineWidth',1);
title('BTC Price vs. Hidden Variable')
%}
```

6 Conclusion

We have delved deep into the world of cryptocurrency by studying its inner workings, analyzing it from an economic standpoint, and applying mathematical finance techniques to its market. Overall, cryptocurrency is an incredibly diverse space, offering decentralized solutions to abstract problems. However, it is very a risky venture for those used to the usual stock market from an economic standpoint. Furthermore, it is difficult to forecast the functional evolution of cryptocurrency given its ties to the dynamics of a new and immature market.

Nonetheless, the foundation, application, and evolution of cryptocurrency since its inception are a phenomenon unlike anything ever seen in history. The fate of cryptocurrency, as it has been until now, is in the hands of the public; its rise or fall will depend purely on whether or not a majority prefers one or the other. That being said, the mathematical underpinnings as to what makes things like Bitcoin so amazing are without a doubt here to stay. Using cryptography and proof-of-work, the idea of blockchain is highly applicable to fields like medicine, insurance, identification, task-management, and artificial intelligence. Additionally, the intention of solving domain specific problems behind certain cryptocurrencies is unparalleled when combined with the forces of a market consensus. Ultimately, it is up to the people to decide what they consider most important in the realm of cryptocurrency and blockchain, as this world has no one ruler; no central authority.

This is perhaps the most revolutionary aspect of cryptocurrency: the fact that, using complex mathematics and computer science, a society can come together without any form of governance. Rather than relying on a separate entity, the cryptocurrency community relies only on its own users to maintain security and trust. Meanwhile, its non-deterministic, highly impressionable market conditions give way to extreme variance, all the while maintaining quite strong persistence and stubbornness. Thus, cryptocurrency is both beautiful and chaotic; both trustworthy and unpredictable; both independent and interconnected.

References

[1] Satoshi Nakamoto: Bitcoin Whitepaper.
https://bitcoin.org/bitcoin.pdf

[2] Herstein, I. N. *Abstract Algebra*. 1999.

[3] Standards for Efficient Cryptography.
http://www.secg.org/sec2-v2.pdf

[4] Bitcoin specific sepc256k1.
https://en.bitcoin.it/wiki/Secp256k1

[5] Bitcoin mining and difficulty.
https://en.bitcoin.it/wiki/Difficulty

[6] Bitcoin target (256-bit number).
https://en.bitcoin.it/wiki/Target

[7] GDAX support
https://support.gdax.com/

[8] Cryptocurrency market information
https://coinmarketcap.com/

[9] Blockchain Info
blockchain.info

[10] Implementation of Bitcoin Futures
http://cfe.cboe.com/cfe-products/xbt-cboe-bitcoin-futures

[11] SEC's warning on ICO's.
https://www.sec.gov/ICO

[12] Lamport Signatures.
https://csrc.nist.gov/
csrc/media/events/first-cryptographic-hash-workshop/documents/preneel_nist_v2.pdf

[13] Thomas M. Cover, Joy A. Thomas. *Elements of Information Theory, 2nd Edition*. Wiley-Interscience, New Jersey 2006.

[14] Arlie O. Petters, Xiao-Ying Dong. *An Introduction to Mathematical Finance with Applications*. Springer, Switzerland 2016.