Joseph Gao
EAS 499: Senior Thesis
Advisor: Brett Hemenway
[DRAFT]

Introduction to Cryptocurrencies for Retail Investors

1. ABSTRACT

In the year 1998, roughly seven years before the smartphone revolution, (2007 marked the release of the iPhone, which arguably kicked off the 'always online' era that we live in today), Wei Dai published a proposal for an "anonymous, distributed electronic cash system".(http://www.weidai.com/bmoney.txt). In the paper, Dai introduced two protocols to achieve his proposal - the first using a proof of work function as a means of creating money, and the second defining a set of servers responsible for keeping accounts, which must be regularly published, and verify balances for the other participants in the decentralized system. While B-money never took off, in part due to the impractical requirement of the first protocol that asks for a broadcast channel that is synchronous and unjammable, Wei Dai's proposal planted the seeds of an idea that would later inspire Satoshi Nakamoto to publish the Bitcoin: A Peer-to-Peer Electronic Cash System white paper. This publication sparked a renewed wave of interest in distributed payment systems and resulted in thousands and thousands of new proposals and protocols to be developed in the next ten years.

2. INTRODUCTION

The year of 2017 showed immense mainstream adoption in a number of cryptocurrencies. However, while mainstream chatter of these various cryptocurrencies has become nearly impossible to avoid, many retail investors are unfamiliar with the underlying technology powering each coin, according to studies performed by CoinDesk, Blockchain Capital, and The University of Cambridge[1]. This paper performs a technical literary review of the Bitcoin, Ethereum, and Ripple whitepapers, and introduces the readers to each cryptocurrencies protocols and specifications in how transactions are verified between peers. Then, several research studies regarding the impact cryptocurrencies has had on the worldwide economy are analyzed and presented to the reader, as the main target audience is the causal cryptocurrency retail investor, the primary impetuous force behind the mainstream popularization of the word 'blockchain'. Following the economic impact and implications analysis, we will explore the benefits and consequences born from a decentralized, peer-to-peer monetary system, such as the value of anonymity and the scaling challenges a peer-to-peer (p2p) network may encounter in the face of tremendous growth. Finally, two case studies are presented that serve as both a warning to new retail investors as well as a reminder to all that despite all the research and efforts currently revolving around cryptocurrency and blockchain in general, it exists within a speculative bubble that could pop at any given moment, and that there still exists a myriad of ways to utilize a p2p, decentralized currency that circumvents the legal system, a problem which still has no solution. In 2014, Mt. Gox, the world's leading bitcoin exchange, announced that it had lost roughly $450

[1] http://www.survey.blockchain.capital/, https://www.coindesk.com/research/who-really-uses-bitcoin/, https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf - turn these into real citataions later

million worth of customer bitcoins. The Silk Road was an online black market that shared the same name as the historically famous trade route between Europe and China, providing a platform for the sale of illicit materials and drugs using bitcoins. While one case study covers the dangers of a decentralized currency, where the lack of a central authority enforcing regulations provides a platform for institutions with shady or poor technical practices could result in negative repercussions for the casual investor, the other case study highlights the dangers an unregulated and anonymous currency can have on society as a whole.

3. CONCEPTS

Before the literary review of the four cryptocurrencies, it is first necessary to establish a solid understanding of the mathematical concepts and computer science algorithms that act as the foundations of these cryptocurrencies, and the blockchain as a whole.

3.1 Cryptographic Hash Functions

A general hash function is a mathematical function with the following traits[2]:

1. One or more inputs of various size
2. An output of fixed size n
3. An efficient runtime, i.e. the computation of the output should not take longer than $O(n)$.

For a hash function to be cryptographically secure, three additional conditions must be met[3]:

1. Collision-resistance
2. Hiding
3. Puzzle Friendliness

A collision is defined as two inputs producing the same output when given to a hash function. A function $F(x)$ is collision-resistant if no two inputs can produce a collision. In other words, a hash function F is collision resistant if it is computationally difficult to find two values a and b such that $F(a) \neq F(b)$, and $a \neq b$. By the pigeon-hole principle, one would conclude that it is impossible for there to be no collisions given the fact that the domain is of fixed output size. Unfortunately, there do not exist any truly collision-resistant hash functions. The hiding property dictates that if we're given the output y of a hash function, there's not feasible way to figure out what the input was. Puzzle Friendly means that if someone wishes to target the hash function to some particular output value, given that the input value was chosen in a randomized way, it would be extremely difficult to find another value that hits that exact output value. SHA-256 is a particular cryptographic hash function that is used by Bitcoin.[4]

3.2 Hash Pointers and Block Chains

A hash pointer is data structure that contains a pointer to where some information is stored along with a cryptographic hash of said information. This gives clients a method to verify the information referenced by this pointer hasn't changed. Hash pointers are used as the strings that tie together the basic linked list structure of a block chain. At its core, a block chain adheres to

[2] Bitcoin and Cryptocurrency technologies

[3] ibid

[4] Ibid

the linked list abstract data type. However, in addition to the pointers to the next and previous nodes, each node also contains a hash that allows us to verify that the previous value pointed to has not changed, and the 'head' of the list contains a pointer to the most recent node. The head pointer can detect tampering when its hash does not correlate to the most recent node, i.e. the contents of the most recent node changed for whatever reason. For example, Bitcoin makes use of a block chain by appropriating it as a tamper-evident log.[5] If an application needed to keep track of a history of transactions, it would be sensible to ensure that a previous transaction suddenly doesn't change or alter itself. Should an adversary attempt to reuse or double-spend, they would have to modify a block k. Doing so would then invalidate the hash of block k+1, and so on until the attacker reaches the head node, which they cannot modify. As a consequence, should an attacker wish to modify the contents of a block chain, they would have to start at the very first block, as well as figure out a method to override the head pointer.

3.3 Digital Signature

A digital signature scheme consists of the following three algorithms:

1. *generateKeys(n) => (privateKey, publicKey)* – this method takes in a size parameter n and generates a key pair. The privateKey is known only to the generator and is used to sign messages, while the public key is known to all clients, and used to verify the signature on a message.
2. sign(privateKey, message) => signed_message – this method takes in both a message to sign and a private key, and outputs a signature for the message using privateKey
3. *verify(publicKey, message, signed_message) => is_valid* – this method takes in a publicKey, message, and signed_message, and uses the publicKey if it determines that the signed_message is a valid signature for message.

Now that the primary building blocks of a cryptocurrency have been defined, we are able to being our analysis.

4. BITCOIN

4.1 Relevant Sources

- Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto
- A History of Bitcoin by Usman Chohan
- An Explanation of Nakamoto's Analysis of Double-spend Attacks

4.2 Brief History and Motivation

Before Bitcoin's specifications and protocols were published, there existed other digital monetary instruments that made its rounds in various online forums and special interest groups.[6] These instruments could be considered 'distant cousins' of Bitcoin, with the concepts of proof-of-work and digital scarcity acting as their bloodline. The earliest known proof-of-work

[5] ibid
[6] History of Bitcoin

implementations was found in ecash, proposed by David Lee Chaum, and Wei Dai incorporated both a proof-of-work system as well as a proposal for distributed digital scarcity in his B-Money paper. While none of these ideas took off to the mainstream, they laid the foundation for what later became Bitcoin. Bitcoin itself was authored and developed by an anonymous person or entity known as Satoshi Nakamoto. Bitcoin's whitepaper laid out the framework for a peer-to-peer network that would foster a system for electronic transactions without relying on trust.

In a traditional online transaction between two entities A and B, a trusted, or verified arbiter exists to ensure the validity of that transaction occurring between A and B, with the arbiter usually being some well-known financial institution. The need for the arbiter exists because otherwise, an entity might engage in double spending, or the act of using funds to perform a transaction with B to obtain some services, reversing the payment, and then repeating with some entity C. The presence of a third party acting as a witness or ledger would essentially prevent entity A from partaking in fraudulent behavior. This model is otherwise known as the trust-based model. While widely implemented, this model does not come without problems. If some dispute were to occur between A and B, the arbiter would be required to use their time and resources to resolve any disputes. As a remedy, the third parties usually require a great deal of personal, publicly verifiable information from both entities who wish to partake in a transaction before that transaction takes place. With the world wide web changing the way humans live their lives, it is inevitable that the number of online transactions will continue to rise, and as a consequence, more time, resources, and information having to float around the internet. Bitcoin attempts to solve this problem by introducing mechanism to make payments over a communications channel without the need for a trusted arbiter.[7] In the stead of a third party, Bitcoin utilizes a cryptographic, peer-to-peer distributed timestamp server to generate computation proof of the chronological order of transactions. The proof of work scheme would be computationally impractical to reverse, thus solving the double spending problem.

4.3 Transactions

Bitcoin defines an electronic coin as a chain of digital signatures. To transfer the coin from owner A to owner B, owner A must digitally sign a hash of the previous transaction as well as the public key of the next owner and add these signatures to the end of the chain, or coin. The person whom the coin is being transferred to can then verify the signatures to verify the chain of ownership.[8]

4.4 Timestamp Server and Proof-of-Work

To address the problem of double spending, Bitcoin makes use of a peer-to-peer distributed timestamp server. The timestamp server aggregates several transactions into a data structure, or block, and generates a new hashed timestamp with the current block and the previous hashed timestamp. Since each timestamp includes the previous timestamp, the server has effectively built a block chain of timestamps. Once a timestamp has been generated, it is publicized to all

[7] Bitcoin whitepaper
[8] Bitcoin whitepaper

peers on the server. The generation of this timestamp, however, is not a trivial task. In order to ensure the validity and accuracy of the peer-to-peer distributed timestamp server, Bitcoin employs an exponential time proof-of-work system that scans for a particular nonce value such that the resulting hash of the block begins with some number of zero bits. Assuming the output from the hash is of length n, then our search space is 2^n, and our worst-case runtime of this process is O(2^n), an exponential endeavor. Thus, the amount of CPU effort needed to determine a valid nonce value is exponentially proportional to the amount of zero bits the bitcoin network seeks. The process of finding that nonce value is otherwise known as *mining*. Once a valid nonce bit has been found, a new timestamp block is tentatively added to the timestamp block chain, and the node originally found the nonce and accepted the block would be rewarded with some bitcoin. This information is then disseminated throughout the network, and the new block is accepted by a node if all the transactions can be verified as valid, i.e. no double spending is detected. Should a node receive a block and realize that the current block it is working on conflicts with the block the just came in the node will accept the block that was harder to generate, i.e. the block with a longer chain, and all the transactions that were present in the block it was previously working on will be thrown out. Once a node accepts a block, it begins working on the next block using the timestamp of the newly accepted block. Thus, adhering to the *eventual consistency* model of the internet, after some period of time *x*, a single, accepted chain of timestamp blocks will be accepted by a majority of nodes in the network. In other words, after a certain age, transactions on the block 'clear', and cannot be negated, much like how a check takes a few days to deposit.

4.5 Probability of Double Spend Attacks

To understand how the Double Spend attack works, consider the following scenario. Some merchant M is offering its services for some amount of bitcoin. Let B_0 be the latest block on the accepted and honest blockchain. A malicious user X is attempting to commit fraud by taking the following steps[9]

1. X sends transactions T to the bitcoin network
2. Merchant M waits for T to accepted in block B_1, where B_1 has B_0 as its previous block, and then waits some time until it sees block B_z where z >= 1until accepting the transaction
3. M exchanges its services with X
4. X immediately releases a chain of blocks B_1` … B_z+1`, where B_1` has B_0 as its previous block. However, inside B_1` is transition S, which moves the bitcoin supposedly used in transaction T from its source wallet address to the address of another wallet that user X owns.
5. If the honest chain has not yet accepted block B_z+1`, the X is done. All miners that receive the chain of B_1` to B_z+1` will recognize that as the honest chain, since it is longer. The B_1 that was originally the honest block will be deemed out of date and thrown out. Merchant M is now left with having given away a service and no funds to show for it.

[9] Explanation of Nakamoto's Analysis of Double Spend Attacks

6. If the honest chain did reach block B_z+1`, X can continue to try and find blocks further ahead that would invalidate the honest block or admit defeat.

For such an attack to even be feasible, we must assume that X controls a sizable portion of miners on the network. Thus, let the fraction of honest miners on the network be denoted by q, and the fraction of miners controlled by the malicious user X be $q = 1 - p$. Now, consider the following probabilities associated with the scenario above.

p = probability honest node finds next block
q = probability X finds next block
Q_z = probability X catches up to the honest chain given that it is z blocks behind honest chain

Let q_i denote the probability that X catches up with the honest block given than it is managed to successfully find i blocks after B_0, such that $0 < i < z$. If z manages to found a nonce that accepts block i, then q_i+1 would be the probability that X catches up with the honest block, and the q_i-1 would be the probability if the honest chain were to accept a new block. The following recurrence relation can be derived:

$$q_i = (q)(q_i+1) + p(q_i-1)$$

Since $p + q = 1$, we know that

$$q_i = p(q_i) + (1 - p)(q_i) = p(q_i) + q(q_i)$$

which when substituted into the former equation gives us

$$p(q_i) + q(q_i) = (q)(q_i+1) + p(q_i-1)$$

After some clever algebraic manipulation, we end up with

$$q_i+1 - q_i = q_1 * sum(k=1, i)\ (p / q)^k$$

Noticing that this is geometric series, we can write the above equation as

(insert latex equation here)

To express our answers not in terms of q_1, simply solve for q_1 and plug it back in

(insert next latex equation here)

TO BE CONTINUED…

*Note – since this is a draft, I won't bother extending the mathematical details more here. In my final draft I plan on having a very nice step through in latex but found it too painful to write it out in word. This is a draft anyway. My derivations come from the source in footnote 9. In the interest of time, I will move onto the next topic. The rest of the section on bitcoin wraps up the mathematical discussion of 4.5 and then quickly wraps up with some final thoughts on bitcoin.

4.6 Summary

The proof-of-work mechanism present in Bitcoin solved two problems vital to the successful operation of Bitcoin. First, it provided an effective consensus algorithm, allowing participating nodes in the network to collectively agree on a set of updates to the state of the ledger. Next, it allowed anyone who was able to enter the consensus process while still protecting it from attack due to the computational complexity associated with the consensus mechanism. Therefore, the amount of influence a certain group of new nodes n bring to the network is directly proportional to the amount of computational power they bring into the network. While the blockchain these protocols were built on allowed Bitcoin to flourish, several other coins began appearing with different takes on how to appropriate the blockchain.

5. ETHEREUM AND ETHER

5.1 Relevant Sources

- Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform
- The Idea of Smart Contracts by Nick Szabo

5.2 Brief History and Motivation

Following the introduction of Bitcoin in 2008, the blockchain that powered Bitcoin garnered increasing interested in several online groups. As Bitcoin began attracting greater attention, separate blockchains which improved on the protocols introduced in Bitcoin began appearing, each having their own cryptocurrencies associated with them. Soon, these separate blockchains gained the nickname of 'alt coins'. In 2013, Vitalik Buterin published the Ethereum white paper, where he described in detail the technical design and rationale for Ethereum – an open source distributed computer platform backed by a blockchain and smart contracts. Ethereum also proposed a cryptocurrency named ether, which served as a sort of payment for computers on the Ethereum platform that ran smart contracts, or code, and is directly analogous to the payment miners on the Bitcoin network received when they successfully confirmed a new block. Taking a step back, it is important to realize that Ethereum itself is not a coin or cryptocurrency, it is in fact a decentralized virtual machine that is backed by blockchain and powered by ether. While Bitcoin aimed to remove the need for a trusted third-party arbiter in a transaction between two parties, Ethereum attempts to use the internet and blockchain to build the world's first truly decentralized computer.

5.3 Smart Contracts

In the context of Ethereum, a smart contract can be thought of as a unit of code, with the goal of allowing developers to program their own functionalities. In fact, by tooling together multiple smart contracts, developers could theoretically build their own application. To better illustrate what a smart contract is, consider the famous scenario presented by Nick Szabo in 1993, where we wish to purchase a soft drink from a vending machine. A vending machine takes in payment, and after a selection, distributes a drink to the buyer. The various phases of interacting with a vending machine can be modeled as some finite state automata, and one can think of a vending machine as a contract: anyone with money is able to participate in a transaction with the vending machine.[10] A smart contract takes the simple contract example with a vending machine and proposes that we apply it to any valuable digital property. Thus, Ethereum is a platform that exists specifically to create and run smart contracts. Ethereum smart contracts are compiled down to bytecode readable by the Ethereum Virtual Machine, or EVM, which acts as the runtime environment for smart contracts.

5.4 Ethereum Accounts

[10] The Idea of Smart Contracts

Ethereum accounts makes up the overall state of Ethereum and play a central role in Ethereum. A state transition is triggered when information is transferred from one account to another. Each account contains four fields: (1) a nonce value, which is a counter used to make sure each transaction is processed only once, (2) the account's ether balance, (3) the account's smart contract code if present, and (4) the account's storage. There exist two types of accounts, an externally owned account, and contract accounts. Externally owned accounts are controlled by private keys, do not have any associated code, but are able to send messages by creating and signing a transaction like in Bitcoin to trigger code associated with a contract account. Contract accounts do have associated code and are able to trigger other contract accounts to run their code or can have their code triggered when they receive a message from an external account and are also able to read and write from internal storage. Both types of accounts have an ether balance.[11] Ether is the token used by Ethereum to pay fees associated with transactions and is often referred to as fuel for the decentralized network to operate.

5.5 Messages and Transactions

A transaction in Ethereum refers to the signed data structure that stores a message to be sent from an externally owned account. Unlike a Bitcoin transaction, which involves a series of verifications and validations, transactions in Ethereum contain two values central to the operation of Ethereum – startgas and gasprice. Startgas represents the maximum number of computation steps a transaction execution can take, whereas gasprice represents the ether fee the sender is paying per computational step. The other fields are the standard sender, receiver, and data fields necessary in any cryptocurrency. Gas is the fundamental unit of computation in Ethereum, and in addition to ensuring that the Ethereum network does not DDOS itself by passing around a message that has a hostile infinite loop, the startgas and gasprice act as sort of time-to-live (TTL) parameter. If a transaction contains data in the data field, this will also cost the sender 5 gas per byte. Thus, the gas price for each transaction must be paid by anyone who wishes to participate in a network, causing attackers to have to pay a proportionate amount to the network resources they consume[12]. Contract accounts are also able to send messages to other contracts, and in the context of Ethereum can be thought of as a piece of code calling another piece of code as a sub-procedure via a message. Each message sent out by a contract also has a startgas value, which counts towards the startgas value received by the first contract either in a message or transaction.

5.6 State Transitions

Since the state of Ethereum is made up of all the accounts, state transitions correspond to direct transfers of value and information between accounts. Note that when a transaction occurs, it is up to the smart contracts that are ran to determine whether any value will be transferred between two accounts. Perhaps one account is simply relaying some information to another. However, a

[11] Ethereum whitepaper

[12] Ethereum whitepaper

transaction fee consisting of the startgas * gasprice must be paid in ether nonetheless. An Ethereum state transition function, APPLY(S, TX) -> S` can be defined as follows.[13]

1. Check if the transaction is well formed
2. Calculate the transaction fee as startgas * gasprice. Subtract this fee from the sender's ether balance and increment the sender's nonce.
3. Initialize gas = startgas, and subtract out the quantitiy of gas per byte of data present in the data field to pay for the bytes in the transaction.
4. Transfer the transaction value from the sender's account to the receiving account. Note that this value may be zero. If the receiving account doesn't exist simply create it. If the receiving account is a contract account, run the code associated with the contract either to completion or until the execution is out of gas.
5. If the sender did not have enough money, or if the code execution ran out of gas, revert all state changes, except the payment of the ether fee, and add that payment to whatever node ran the code.
6. Otherwise, refund the fees for all remaining gas to the sender, but not the transaction fee, which still goes to the miner.

5.7 Blockchain and Mining

The Ethereum blocks in the blockchain are similar the blocks found in the Bitcoin blockchain. In addition, they contain a copy of the transaction list, the most recent state, the block number, and the difficulty. The proof-of-work used by Ethereum is very similar to the one described in the Bitcoin section as well. Once a valid hash has been found, a node must verify that the block is indeed valid. To verify or accept a block, a participating node must:[14]

1. Check if the previous block referenced exists and is valid
2. Ensure the timestamp of the block is greater than the referenced block, and not into the future by more than 15 minutes
3. Ensure that the various low-level Ethereum constructs are valid (gas limit, difficulty, block number, etc.)
4. Ensure the proof of work on the block is valid
5. For each transaction in this block, and S_0 being the state at the end of the previous block, APPLY(S[i], TX[i]) for I in 0 to n-1.
6. S_n is the resulting final state of the Ethereum network, with the account that mined this block obtaining the reward, i.e. the gas fees for each of the transactions

Once the verification step is complete, the accepted block is broadcast to all nodes participating on the Ethereum network, and as in the Bitcoin network, most of the nodes must reach a consensus as to whether this block is accepted. If the majority of nodes do agree the block is valid, then what we essentially have is a state transition from S_0 to S_n.

5.8 Summary

Ethereum came about as a sort of response to the variations of blockchains being built to address specific issues. The hope is that by using smart contracts running on the Ethereum blockchain, a

[13] Ethereum whitepaper
[14] Ethereum whitepaper

developer could decide to build another currency like Bitcoin or build an app completely unrelated to anything financial. Thus, while similar in ideas to Bitcoin in idea, Ethereum has a different goal altogether – become the world's computer. Although the creation of apps on the Ethereum platform is theoretically possible, it is still unclear which apps will prove to be useful, and which ones will be nothing more than just simple fun.

6. Ripple Transaction Protocol and XRP

6.1 Relevant Sources

- The Ripple Protocol Consensus Algorithm
- The Byzantine Generals Problem by Lamport et. al
- Re: Bitcoin P2p e-cash paper by Satoshi Nakamoto (email chain)

6.2 Brief History and Motivation

In a way, the relationship between Ripple and XRP mirrors that of Ethereum and Ether. Ripple is more of a catchall name for the platform backed by The Ripple Transaction Protocol that facilitates the trading of XRP. XRP is the actual cryptocurrency, and thus is the unit that has actual value when it comes to exchanges. In this section we explore in detail the Ripple Transaction Protocol, and conclude with a brief overview of how XRP stacks up to Ether and Bitcoin as a cryptocurrency.

Long before the rise of modern distributed computer systems, a problem known as the "Byzantine Generals Problem" was detailed in a paper published by Leslie Lamport, Robert Shostak, and Marshall Pease.[15] This problem drew an analogy between a distributed computer system running on a network and some number of generals attempting to reach a consensus on whether or not to attack or retreat from an imminent battle. In both contexts, miscommunication or malicious intent could result in disastrous consequences. Before the Ripple payment protocol, RipplePay was developed in 2004 by Ryan Fugger. Fugger aimed to create a monetary system that was decentralized and allowed individuals and communities to create their own money. His payment system debuted in 2005 as a financial service to provide payment options to members of his online community via a global network. In 2011, after Bitcoin's now famous initial proposal of a blockchain based digital currency, RipplePay served as the inspiration and foundational framework for a new digital currency system in which transactions were verified by consensus among select members of a network, rather than the proof-of-work mining method used by Bitcoin. The new system was designed to be quicker and more efficient than Bitcoin, and eventually became the new version of the Ripple System, after its creators got in contact with Fugger and his community. By 2014, a whitepaper titled "The Ripple Protocol Consensus Algorithm" was released to the public by Ripple Labs, and that same year Ripple became the world's second biggest cryptocurrency.

6.3 Byzantine Generals Problem

[15] Ripple Protocol Consensus Algorithm

For a computer system to be reliable, it must be able to adapt to the failure of one or more of its components. The problem of adapting and coping with this type of failure can be expressed abstractly as the Byzantine Generals Problem.[16] Consider the following fictional scenario: Several divisions of the Byzantine army are planning to attack an enemy city, with each division headed by its own general. The generals have no reliable method of communication, and are only able to utilize a messenger who must travel on foot to relay tactics. In order to successfully lay siege to the city, the generals must come to an agreement on the battle tactics. However, some of these generals may be traitorous, and maliciously attempt to sabotage the battle tactics by doing the exact opposite of an agreed upon plan of attack. Thus, in order to solve this problem, the generals must have some algorithm to guarantee that (a) all loyal generals agree upon the same plan of action that is reasonable, and carry that plan out accordingly, and (b) in the case that a small number of generals are traitors, those traitors are unable to influence the loyal generals to adopt an unreasonable plan.[17] Since the term reasonable plan has a variable number of interpretations, the crux of the problem lies in how the generals reach a consensus of attack. Let v be the vector of length n defined as the information communicated by each general, with the *ith* entry correspond to the information communicated by the *ith* general, with a total of n generals. The naive method one might propose for each general to know each other's plans would be for each general to disseminate their plans to the other $n - 1$ generals. However, because traitorous generals may send different values $v(i)$ to different generals, we notice that in order for condition (a) to be satisfied, all *loyal* generals must obtain the same vector v. In order to obtain the same vector v among all loyal generals, a general m cannot simply take at face value a value he or she receives from general i. There must be some sort of mechanism for consensus on the vectors v each general received. In other words, any two loyal generals will use the same value of $v(i)$. Thus, we arrive at the formal Byzantine Generals Problem[18]:

A commanding general must send an order to his n - 1 lieutenant generals such that

1. *All loyal lieutenants obey the same order*
2. *If the commanding general is loyal, then every loyal lieutenant obeys the order the commanding general sends*

Accordingly, the term *Byzantine Failure* is defined as arbitrary deviations of a process from its assumed behavior based on the algorithm it is supposed to be running and the inputs it receives. There exists a number of solutions to the Byzantine Generals Problem. Bitcoin solves it via its proof-of-work mechanism. The Ripple Protocol attempts to take an alternative consensus approach that enables its own cryptocurrency, XRP, or Ripples, to have faster and more energy efficient transactions.

6.4 Bitcoin's Proof-of-Work Solution

In a email chain dated November 13, 2008, Satoshi Nakamoto responded to an email pointing out that Bitcoin's consensus algorithm fell victim to the Byzantine General's Problem, because it is not sufficient to know that everyone knows some information X. In addition to that, it is necessary for everyone to know that everyone knows X, and that everyone knows that everyone

[16] The Byzantine Generals Problem p.1
[17] The Byzantine Generals Problem p.2
[18] The Byzantine Generals Problem p.3

knows that everyone knows X, and so on. Nakamoto responds with the claim that the proof-of-work block chain is a solution to the Byzantine Generals problem.[19] Consider Bitcoin's method of block discovery and acceptance in the context of the Byzantine Generals' problem. Each general would like to attack a juicy Facebook database by brute forcing the password to the database. However, this password change at random time intervals *x*, and so they only have enough CPU power to brute force the password in their limited timeframe if the majority of them work together. In addition, their only method of communication is a very inefficient multicast channel in which they are all subscribed to. It is decided that whatever start time is seen first will be the time at which they will collectively begin brute forcing the password to the database. Unfortunately, since their network communication is not instantaneous like the buggers in Ender's Game, if two generals decide to announce a time at relatively the same instance, some partition of the generals will receive times that do not correspond to the times received by the other partition. To remedy this, each general knows that if they receive a timestamp to attack, they will first tell their computer to solve a complex and intensive computation task that involves finding a hash that includes the time of attack in that hash. The first general to find a solution *s* will then broadcast his success and the time *attack_time* they received to the rest of the network, and everyone who sees this will change their own proof-of-work computation to include that time. Anyone working on a different attack timestamp will drop working on that one, and switch to the received on via broadcast. After some time *t*, the *attack_time* should have been hashed by a chain of some number of proofs-of-works. Each general can then verify the difficulty of the proof-of-work chain and can estimate how much parallel CPU power was necessary to obtain this chain, and conclude that a majority of the computers must have been working on this *attack_time* in order to obtain this proof-of-work chain. Thus, each general can agree that *attack_time* is indeed a safe time to all begin their brute force attack on the Facebook database. Notice that even if some of the generals were 'good', i.e. traitorous, and refused to search for hashes that included *attack_time*, so long the generals can determine that a majority of the generals were indeed searching for *attack_time* they are able to remain confident their brute force attack will succeed.

6.5 The Ripple Consensus Algorithm

The Ripple Protocol aims to achieve a consensus algorithm of correctness, agreement, and utility. The protocol defines a state of consensus as "the state in which nodes in the network reach correct agreement".[20] Correctness is defined as the ability for a distributed system, in this case a distributed payment network, to be able to identify bad transactions and facilitate honest transactions. As explained in the Bitcoin section, correctness is traditionally enforced by a third party arbiter, such as a trusted bank. Agreement is defined as the ability to reach a single, global truth amongst all the nodes participating in a decentralized system. Decentralized systems, at their core, are prone to faults in the network. The problem of how to adapt in the face of faults is addressed by the Ripple protocol. Finally, utility is defined as the usefulness of a solution. In the case of Bitcoin, one could argue that the length of time it takes for a transaction to be verified detracts from the utility of Bitcoin as a payment option. The Ripple protocol thus presents a

[19] Bitcoin p2p e-cash paper email chain

[20] The Ripple Protocol Consensus Algorithm

solution that speeds up the transaction time while maintaining the same level of correctness and security offered by Bitcoin, resulting in more utility.

6.5.1 Definitions

Ripple has several terms that need defining before we are able to dive into how the consensus algorithm works. First off, a server is any entity running the Ripple Server software, which enables a node to participate in the consensus process. Nodes that do not run this software but still participate in the Ripple network run software known as the Ripple Client software. In a sense, the computers that run the software can be deemed "trustworthy", since some central authority vets each node that runs the server software. The ledger is a record of the amount of currency in each user's account on the Ripple network, and it represents the "ground truth" of the network. Any transaction that passes the vetting of the consensus algorithm legally updates the ledger. The last-closed ledger is the most recent ledger that was deemed correct by the consensus protocol, and thus is the last known state of the network. The open ledger is the current operating status of a node in the Ripple network. Transactions by client nodes of a given server node are applied to that server node's open ledger. Thus, each node running the server software may have differing open ledgers depending on the distribution of the client nodes throughout the network, but the transactions in the open ledger are not final until they have been vetted and agreed upon by the consensus process, which then converts that open ledger into the next last-closed ledger. The unique node list (UNL) is a list maintained by each server node *s* which contains a set of the servers that *s* will query when determining consensus. Only the votes from the servers contained in *s'* UNL will be considered as trusted by *s* not to be participating in any collusion in an attempt to defraud the network. When a new server node joins the Ripple network, a curated, default UNL is provided. The default list is chosen in order to minimize and mitigate the case where traitorous nodes are attempting to collude and agree on fraudulent transactions. Finally, any server, or proposer, can broadcast transactions to be included in the current consensus process, and each server that receives these broadcasts will make their best effort to include every valid transaction in their open ledger when a new consensus round starts. During the consensus process, only proposals from servers on the UNL of a server *s* will be considered by *s*.[21]

6.5.2 Consensus Algorithm

The consensus algorithm is run every few seconds by all participating nodes, and proceeds in rounds. In each round, each server takes all valid transactions it has seen before the start of the consensus and creates a public list known as the candidate set. The server then merges all candidate sets set forth by each server in its UNL, and votes on the validity of all transactions in the master list. All transactions that meet some minimum threshold of "yes" will be considered valid and be passed onto the next round. Transactions that do not make the cut are either discarded, or given a second chance during the next consensus wave. In the next round, each transaction must achieve a 80% threshold of the UNLs voting "yes" to be applied to the ledger. Once this process is complete, that ledger is closed and becomes the new last-closed ledger.[22] In order for the consensus algorithm to achieve correctness, even in the face of a maximal amount

[21] The Ripple Protocol Consensus Algorithm p.2 - 3
[22] The Ripple Protocol Consensus Algorithm p.4

of tolerable Byzantine failures, we must show that a fraudulent transaction cannot be passed to the final ledger. If the majority of server nodes have been compromised, however, this is clearly impossible to show. In the case that a majority of server nodes are still honest and functioning correctly, we can show correctness as follows. In order for a transaction to be added to the final ledger, 80% of a server's UNL must agree on that transactions validity. For any given UNL with *n* nodes, the number of traitorous nodes must be less than *(n - 1) / 5*. Let p_c be the probability that a server node is traitorous and is part of a gang of server nodes attempting to override the honest consensus. The probability of correctness, i.e. the probability that the gang of traitorous server nodes are unable to influence the honest consensus is then

p* = sum(i=0, (n-1)/5) (nCr(n, i) * p^i_c * (1 - p_c)^(n-i))

Since the UNLs are not chosen completely at random, but with the intent to minimize p_c. As the number of nodes *n* in the UNL increases, we see that the p* only gets larger, or in other words, the probability of correctness increases.[23] Due to the fact that each server node has its own UNL that *may* be different, it must be shown that by the end of the consensus algorithm, all honest nodes reach a consensus on the same set of transactions. In other words, the protocol must be in agreement. A fork is defined as a cut of nodes A coming to a different consensus as B, the remainder of the cut. Given a scenario where two cliques arise due to the selections of the server's UNL, the potential for forks arises. A clique of nodes is formed if the UNL's for a set of servers are exactly the same, and because two cliques do not share any members, it is entirely possible that both cliques achieve a correct consensus independently of each other. Thus, to ensure agreement, the UNLs must be chosen in a way such that the situation of sparsely connected cliques does not arise.[24] The final consensus goal the Ripple protocol attempts to achieve is that of utility. Convergence is defined as the ability for the consensus process to terminate in a reasonable amount of time. To ensure convergence, the consensus protocol enforces a latency heuristic. Response times of server nodes on the Ripple network is monitored, and any node whos latency exceeds some threshold are deactivated and removed from all UNLs containing that node. Coupled with the fact that the consensus algorithm has a finite number of rounds, the latency heuristic thus guarantees convergence termination with an upper bound of

*number of rounds * latency threshold*[25]

In addition, there are a slew of other heuristics Ripple employs to optimize the utility of the consensus algorithm.

6.6 XRP

Finally, we arrive at the cryptocurrency of Ripple, XRP. Apart from being classified as a cryptocurrency, XRP has a number of differences from its peers. First off, XRP transfers are effectively immediate, and compared to the sometimes ten minute transaction time of Bitcoin, an XRP transaction is immediate by comparison. Furthermore, while Bitcoin has an ever growing number of coins in circulation until that number hits an eventual cap, and Ether has no theoretical limit, XRP has a hard limit of 100 billion tokens, all available immediately. The majority of the XRP tokens are held by Ripple Labs, the organization that formally released the

[23] The Ripple Protocol Consensus Algorithm p.4 - 5

[24] The Ripple Protocol Consensus Algorithm p.5

[25] Ibid

specification of the Ripple Protocol Consensus Algorithm. While Ripple Labs holds a large share of XRP tokens, they do not plan on releasing them all into the wild immediately, since such an action would cause the value of XRP to tank. Ripple Labs aims to leverage the Ripple consensus algorithm introduced in its paper to facilitate financial organizations around the world in making faster transactions. As a result, Ripple is backed by a large number of the world's most influential financial institutions, such as Santander, UBS, and American Express. The primary factor that sets Ripple apart from the rest of the cryptocurrencies available is the fact that Ripple has the support of so many worldwide banks. Such a standing brings inherent centralization to a supposedly decentralized system, and unlike Bitcoin and Ethereum, who both rely on blockchain to empower the authenticity of their decentralized networks, Ripple has the luxury of not needing to rely on complex and computationally intensive proof-of-works to verify transactions - its brings back the trusted third-party arbiter as the catchall insurance to its consensus network.

6.7 Summary

Since no new XRP is being created through the efforts of mining, coupled with the fact that a worldwide coalition of banks back Ripple, many are uncertain about the future of Ripple. Should governmental regulation begin clamping down on decentralized payment systems, Ripple might be one of the few to survive if the banks were to lobby for technology. However, since mining has effectively no incentive and not everyone can simply become a Ripple server node, adoption has been slow. Only time will be able to tell the success of this particular cryptocurrency.

7. Economic History of Cryptocurrency

7.1 The Rise of Mainstream Cryptocurrency Exchanges

By 2013, Bitcoin was beginning to emerge as the clear face of cryptocurrency, and academic research on the topics of Bitcoin and cryptocurrency as a whole reached new heights. As cryptocurrency began to take on a more mainstream media appearance instead of being relegated to online email chains and research groups, financial institutions and retail investors alike began to ponder the potential economics of cryptocurrency. The most popular use of mainstream cryptocurrencies today is currency exchange. Currency exchanges allow for users to trade Bitcoin and other cryptocurrencies for traditional fiat currencies, or other virtual currencies. The majority of currency exchanges operate in a similar manner to traditional financial markets, with bids and asks and commission fees.[26] Mt. Gox was a Bitcoin exchange based in Japan that launched in 2010, and by 2014 it was handling over 80% of all Bitcoin (BTC) transactions worldwide, and was the world's leading Bitcoin exchange.[27] Mt. Gox ultimately went bankrupt as a result of a security break with led to the theft of millions of Bitcoins, and the legal disputes revolving around Mt. Gox's downfall continues to this day. However, Mt. Gox's success as an exchange proved that there existed a marketplace for Bitcoin, where its users had somehow assigned value to a cryptocurrency and gave life to its stock-like behavior. By 2016, a company named Coinbase rebranded its cryptocurrency exchange to the Global Digital Asset Exchange, or GDAX, and offered the ability to trade Bitcoin and Ether. Coinbase is a startup based in San

[26] Bitcoin: economics, technology, and governance p. 8
[27] Bitcoin: economics, technology, and governance p. 8

Francisco, and was arguably in the right place at the right time. Founded during the golden age of entrepreneurship and focused the burgeoning field of cryptocurrency, Coinbase has become a fundamental starting point for any new retail investor looking to get their feet wet with cryptocurrency. In the United States, currency exchanges are registered with the Financial Crimes Enforcement Network, which impose fees for certifications and other legal reasons, resulting in an exchange having to pay hundred of thousands of dollars to legally operate. Apart from the regulatory and technical requirements necessary to create an exchange nothing else stops one from setting up another cryptocurrency exchange. However, as currency exchanges inherently bring about an aspect of centralization - i.e. a trusted third party, (in this case the exchange itself) oversees a transaction between two entities. What was once a vision for a global decentralized payment systems seems to be tied down by the familiarity of having some trusted party in the picture. As a result, an interesting question arises - will Bitcoin and cryptocurrency as a whole ever become an actual currency, or will it forever be relegated to act as a means of investment, or will it simply remain an alternative payment platform similar to Venmo, where the assets you have on this platform aren't truly useful unless you "cash out" back to fiat currency?

7.2 Cryptocurrency During its Formative Years

The first notable adopters of Bitcoin were businesses that required features not easily offered through other avenues - in other words - black market businesses that sold illegal services and wished to be paid with a currency that had little regulation and high anonymity.[28] The Silk Road was a online black market part of the dark web that facilitated the sale of illicit substances and narcotics to anonymous buyers, and was one of the first online businesses to accept Bitcoin. Coupled with Tor, a browser that protects a users identity, Bitcoin suddenly became the preferred method of payment on the Silk Road marketplace. As a result, Bitcoin, and cryptocurrency in general was regarded by the mainstream media and public as a method to payment for illegal activities.

7.3 Cryptocurrency Today

Following the FBI shutdown of The Silk Road marketplace, the community around Bitcoin and cryptocurrency in general began to their potential to act as an alternative to credit card and debit card networks, due to Bitcoins lower transaction fees. In January 2014, Overstock.com began accepting Bitcoin payments, and following a positive response, Expedia, Newegg, and other large merchants began accepting Bitcoin in order to offer a lower-cost method of payment.[29] Thus, the benefits that merchants gain from accepting Bitcoin is clear - however, the benefit of spending cryptocurrencies as a consumer is less clear. Today, many credit card companies offer competitive sign up bonus' and reward consumers for swiping their card at terminals. A percentage of the transaction fee usually paid by merchants is often translated to rewards given back to the consumer. Should a user use Bitcoin or some other cryptocurrency to pay for services and goods, the consumer effectively loses out on the benefits of using a credit card. In addition, due to the fluctuating valuation of cryptocurrencies, consumers are better off converting a

[28] Bitcoin: economics, technology, and governance p. 10
[29] Bitcoin: Economics, Technology, and Governance p.13

cryptocurrency to hard fiat currency and then using that to pay off a credit card bill rather than spending the cryptocurrency directly. As a consequence, cryptocurrencies are treated as financial assets and are bought and sold as such, with many consumers buying a large quantity of Bitcoin and other cryptocurrencies simply to hold onto them and hope they appreciate in value over time, before selling them off for fiat gains. Interestingly enough, the forces behind how a particular value associated with a certain cryptocurrency are both invisible and mysterious. Whether it was the original fiat valuations of narcotic substances that inspired the first valuation of Bitcoin, or just dark magic, the formation of value behind cryptocurrencies is indeed an interesting question to consider.

7.4 Cryptocurrency Value Formation

As of 2016, the value of all Bitcoins in existence represented approximately $7 billion, and more than $60 million worth is exchanged each day.[30] Since many cryptocurrencies rely on proof-of-work mining to reach consensus and produce new units of the cryptocurrency in a similar manner as Bitcoin, we attempt to use Bitcoin as a generic example to elaborate on a more general scope of cryptocurrencies in value formation. There exist a few common variables amongst all cryptocurrencies that are baked-in to the coin at creation. Most notably, most coins have a maximum number of coins that is able to be mined, or created. In the context of Bitcoin, this number caps out at 21 million. In addition, the time it takes to find a block and the reward a node receives when it finds a correct block is known as the block time and block reward, respectively. By 2016, the Bitcoin reward for finding a block was 12.5 Bitcoins per block, and it took roughly 10 minutes for a new block to be discovered. Depending on the speed at which the network wishes to discover new blocks, the network has the ability to change the difficulty of the proof-of-work each node must perform to confirm a new block. This is known as the difficulty variable. Finally, the market price is the observable price on exchanges where trading pairs are listed between various currencies.[31] A few observations can now be drawn from these common variables. Notice that any user who controls a large amount of computational power appears to have a higher chance at discovering blocks and thus may be able to hoard the majority of the block rewards for themselves. While earlier in this paper we addressed the problem of malicious users, and showed that it is unlikely and unprofitable for a user to tamper with the blockchain ledger, the problem of having more computational power to gain a competitive advantage compared to the rest of the network is mitigated by the problem difficulty variable. If a large group of nodes appears to be adding valid blocks too quickly, the network will agree that a harder proof-of-work problem must be assigned. However, as a consequence, by creating an even harder problem to solve, the user who had a majority of the computational power is simply slowed down, while everyone else on the network has even less of a chance at solving a block.[32] As a result, blockchain consensus and proof-of-work networks follow the mantra "to the victor belong the spoils". The network can do its best to ensure the value of a coin is not destroyed by quick mining or an influx of malicious users, but it cannot provide a platform where each user as an exactly equal chance of obtaining the next block reward. This holds true for both Bitcoin and

[30] Cryptocurrency Value Formation: An empirical analysis leading to a cost of production model for valuing Bitcoin
[31] Cryptocurrency value formation p.6
[32] Ibd

many other cryptocurrencies. Interestingly enough, because XRP is premined, it does not have to deal with the phenomena of mining for value or the like. Instead, its value is backed by the worldwide banking organizations that support it. The reason a cryptocurrency would be motivated to limit the number of new blocks verified in a timespan relates to the law of diminishing marginal utility. The law states that as the consumption or abundance of a product increases, the utility one gains from consuming or obtaining an additional unit of that product decreases. All this talk of mining ultimate boils down to the hypothesis that the more aggregate computation power in a network being consumed by mining for a particular cryptocurrency, the more valuable that cryptocurrency is. Since mining is actually the process of solving a computationally hard puzzle to verify transactions in a block, it stands to reason that if there is no mining going on for a cryptocurrency, with the exception of coins that do not require mining such as XRP, then there are no transactions being performed on that cryptocurrency network.[33] Perhaps it's due to the lack of acceptance for that cryptocurrency, as a number of cryptocurrencies exist simply as a proof-of-concept or for general amusement. As an aside, many cryptocurrencies are open-source, hence the effort it takes to create a similar alternate currency, or altcoin, is minimal and can be done by simply taking an existing coin's implementation and modifying some of the variables mentioned earlier in this section. In addition, because all cryptocurrencies are motivated by profits, that would mean the electricity and computational costs associated with mining that currency are outweighed by the marginal product of mining. The following hypotheses, among others, can be drawn[34]:

Hypothesis 7.1 - The amount of computational power devoted to finding a valid block is positively correlated to a coin's value.

Hypothesis 7.2 - Due to the law of diminishing returns, the rate of blocks found per minute is negatively correlated to a coin's value

Hypothesis 7.4 - The longer a cryptocurrency has been around, the more valuable it is.

The two hypotheses are derived from the earlier talking points regarding computation power and block verification times, and the final hypothesis is more or less an obvious statement in the context of how simple and easy it is for altcoins to be created today - if a coin is older, it would have had a chance to be adopted by businesses, and if it didn't die out already, then it must have some value to some community of users. In light of the low barrier of entry for altcoins, the question of whether or not it would be profitable to mine a newly created altcoin rather than well known currencies such as Bitcoin and Ether should be considered. Since the ability to mine a cryptocurrency is consolidated entirely in the owner of a particular machine, it is not hard to switch contexts should the situation arise where mining a certain altcoin would yield a higher marginal profit. Should there be an opportunity where a machine could mine an altcoin at a much cheaper rate than the cost of mining for Bitcoin, and then find an exchange where Bitcoin could be bought in exchange for the altcoin, there lies a chance for arbitrage. Since Bitcoin remains the de-facto digital currency of the masses, we will attempt to assign valuation to it using the

[33] Ibd

[34] Ibd

hypotheses stated above and take into consideration the opportunity to mine altcoins instead. The analysis used to obtain a production cost model for valuing Bitcoin can also be used for any other cryptocurrency. Assume that if we were to actually set our machines to mine Bitcoin, the actual rate of return we get from doing so is measured in expected Bitcoins per day per unit of mining power. If we estimate the average hashing power be 1000 GigaHashes per second. The expected number of Bitcoins to be produced per day can be found by the following equation[35]:

$$BTC/day* = (\beta * \rho * 3600 * 24)/(\delta * 2^{3}2)$$

where *\beta* is the block reward, *\rho* is the hashing power, 3600 * 24 representing the number of seconds in an hour multiplied by the number of hours in a day, *\delta* is the difficulty of the block (in units of GH/block), and 2^32 is the normalized probability of a single hash solving a block in the case of Bitcoin, and results from the Bitcoin mining algorithm. Factoring in all the constants leaves us with[36]

$$BTC/day* = (\beta * \rho) * \theta/(\delta)$$

To model the event in which there exists an arbitrage opportunity, let epsilon represent the exchange rate between the altcoin that we would rather mine and Bitcoin. Assuming that we would be able to use the same hashing power to mine the altcoin, we have the equation[37]

$$BTC/day* = (\frac{\beta_{altcoin} * \rho_{altcoin}}{\delta_{altcoin}}) * \theta * \epsilon$$

From the equation, if the exchange rate ϵ is greater than or equal to 1, then there exists no benefit in actually mining an altcoin. However, if the exchange rate is less than 1, that is, for each altcoin, we are able to exchange it for more than one Bitcoin or are able to find a series of exchanges that reliably result in more Bitcoin, then it would make sense to mine the altcoin for some time, so long the ϵ remains at a favorable ratio. Due to the fluctuating nature of the difficulty δ, overpriced altcoins tend to readjust quick enough so that opportunities for arbitrage for an ephemeral amount of time.[38] Finally, to complete our cost of production model that aims to assign value to Bitcoin, we must consider a few more variables. The cost of electricity, measured in cents per kilowatt-hour, the energy consumption per unit of mining effort, measured in watts per gigahash per second, the market price of Bitcoin, and the current difficulty to mine a block in the Bitcoin network.[39] Our previous equation can then be expressed as

$$E_{day} = \frac{\rho}{1000} * Electricity_Cost * Energy_consumption$$

where E_{day} represents the cost per day for us to run our mining hardware. Since we now have an expression for Bitcoins per day the cost to produce Bitcoins per day, the appropriate price, or the MSRP, if you will, can then be found[40]:

$$P = \frac{E_{day}}{BTC/day*}$$

[35] Cryptocurrency Value Formation p.11
[36] Ibd
[37] Ibd
[38] Cryptocurrency Value Formation p.12
[39] Ibd, p. 13
[40] Ibd, p.14

where *P* represents the fair price in dollar amount a single Bitcoin should have, based off of the efforts and incentives offered to a miner.

7.5 Summary

While digital currency concepts have been around for decades at this point, it was not until Bitcoin made a name for itself, and began to be accepted by a number of large merchants did the concept of mining really begin to take off. Digital currency exchanges like Mt. Gox only fawned the flames of speculation, and as the mainstream hordes of speculative investors began to arrive via the likes of Coinbase and GDAX, an interesting phenomena begins to unfold regarding the value of said digital currencies. While it was shown that the cost of production and the incentives offered to a miner for a cryptocurrency ultimately determine a fair price for a unit of a digital currency, due to the limited circulation of most cryptocurrencies, or the backing of some digital currencies by trusted international organizations, we observe that many cryptocurrencies may have constantly fluctuating valuations pegged to them that are in fact higher, or in some cases lower, than what the fair price is. As speculative retail investors, we must do well to remember that depending on the pace of global adoption and whether or not newer technologies end up reducing the cost of mining, these seemingly positive factors do not necessary directly correlate to a positive force on the price of a digital currency.

9 Closing Remarks

While many believe the present day hype revolving around to be smoke and mirrors, the undeniable fact is that early cryptocurrencies enabled the existence of several burgeoning economies since their creation, ranging from sites like the Silk Road Marketplace to the thriving exchange market we see today. The absence of a regulating body and the factor of anonymity are just two factors that contribute to reasons cryptocurrencies have thrived in certain contexts, and only time will tell the impact this will have on the speculative bubble surrounding them. In this paper we saw how a blockchain was the impetuous force behind each cryptocurrency, and as a consequence of most cryptocurrencies being open source, we saw how low the barrier of entry was for new, young, and sometimes even outright fraudulent altcoins backed by a blockchain could appear on almost seemingly out of thin air. Regardless of the motive behind all these new coins, the common theme they all shared was their championing of how the blockchain was a revolutionary new technology that could be used in many ways to circumvent centralized authority. While we saw that Ethereum was the only platform that comes closest to reaching the purported goal of what a blockchain technology can offer, the influence of blockchain technologies has already begun to trickle into the various industries that originally had no interest in working with blockchains. Small startups here and there, iced tea companies, and even traditional camera companies have begun to dabble with blockchains, but the overall impact blockchain technology has yet to be measured in contexts outside of what we analyzed here. Which efforts will actually yield meaningful results, and which will prove utterly futile? Only time will tell. Finally, the speculative bubble currently revolving around the values of each cryptocurrency appears to have little to do with the differences between the underlying technologies the currencies are built upon. We saw how the pricing of each cryptocurrency has some fundamental structure to it regarding the supply, demand, and cost to mine the coin, but it seems even then the prices of certain coins defies all earthly logic and skyrockets well beyond what one might deem the “fair price”. While enough money is floating around the current ecosystem to encourage the long-term exploration of and development on cryptocurrencies, and more generally blockchain technologies, it is important for us speculative retail investors to not only understand just what we are buying when we exchange our hard earned fiat currency for an ether token or an XRP coin, but also that the economies revolving around these cryptocurrencies are highly volatile and seemingly unpredictable. No amount of proper research can be done to predict the ‘next Bitcoin’, as with any form of gambling, we should be wise to only invest what we are willing to lose.