2020

Facilitating cross-chain cryptocurrency exchanges: An inquiry into blockchain technology and interoperability with an emphasis on cryptocurrency arbitrage

Samuel Grone

Facilitating cross-chain cryptocurrency exchanges: An inquiry into blockchain technology and interoperability with an emphasis on cryptocurrency arbitrage

Abstract

Since the introduction and proliferation of the blockchain-based cryptocurrency Bitcoin, alternative cryptocurrencies also based on blockchain technology have exploded in number. It was once believed that one, or very few, cryptocurrencies would eventually dominate the market and drive out competitors. This assumption, however, was incorrect. Thousands of cryptocurrencies exist concurrently. The vast number of cryptocurrencies leads to a problem—what if the cryptocurrency that an individual possesses does not meet their current needs as well as another cryptocurrency might? The attempt to solve this problem has led to the rise of many cryptocurrency exchanges and exchange schemes. In this paper, we will discuss the motivations for an individual to be interested in exchanging two or more cryptocurrencies by describing and comparing various popular cryptocurrencies with different desirable attributes. While we will discuss these attributes, this paper will give special focus to arbitrage in particular. In addition, we will describe various cryptocurrency exchange schemes and their advantages and disadvantages. Finally, we contribute to the understanding of cryptocurrency exchangeability and interoperability by comparing the historical price data of several cryptocurrencies to determine how often arbitrage has been possible in the past.

Degree Type
Open Access Senior Honors Thesis

Department
Computer Science

First Advisor
Weitian Tong

Second Advisor
S. Maniccam

Third Advisor
Augustine Ikeji

Subject Categories
Computer Sciences

FACILITATING CROSS-CHAIN CRYPTOCURRENCY EXCHANGES: AN INQUIRY INTO BLOCKCHAIN TECHNOLOGY AND INTEROPERABILITY WITH AN EMPHASIS ON CRYPTOCURRENCY ARBITRAGE

By

Samuel Grone

A Senior Thesis Submitted to the

Eastern Michigan University

Honors College

in Partial Fulfillment of the Requirements for Graduation

with Honors in Computer Science

Approved at Ypsilanti, Michigan, on this date 12/17/2020

Supervising Instructor: Weitian Tong - Date:__12/18/2020__

Departmental Honors Advisor: _S.Maniccam_ ___________ Date:_12/17/2020____

Department Head: _ ___ Date: 12/18/2020

Honors Director: ____________________________ Date:______________

FACILITATING CROSS-CHAIN CRYPTOCURRENCY EXCHANGES: AN INQUIRY INTO BLOCKCHAIN TECHNOLOGY AND INTEROPERABILITY WITH AN EMPHASIS ON CRYPTOCURRENCY ARBITRAGE

By Samuel Grone

A Senior Thesis Submitted to the Eastern Michigan University Honors College in Partial Fulfillment of the Requirements for Graduation with Honors in Computer Science

Abstract

Since the introduction and proliferation of the blockchain-based cryptocurrency Bitcoin, alternative cryptocurrencies also based on blockchain technology have exploded in number. It was once believed that one, or very few, cryptocurrencies would eventually dominate the market and drive out competitors. This assumption, however, was incorrect. Thousands of cryptocurrencies exist concurrently. The vast number of cryptocurrencies leads to a problem—what if the cryptocurrency that an individual possesses does not meet their current needs as well as another cryptocurrency might? The attempt to solve this problem has led to the rise of many cryptocurrency exchanges and exchange schemes. In this paper, we will discuss the motivations for an individual to be interested in exchanging two or more cryptocurrencies by describing and comparing various popular cryptocurrencies with different desirable attributes. While we will discuss these attributes, this paper will give special focus to arbitrage in particular. In addition, we will describe various cryptocurrency exchange schemes and their advantages and disadvantages. Finally, we contribute to the understanding of cryptocurrency exchangeability and interoperability by comparing the historical price data of several cryptocurrencies to determine how often arbitrage has been possible in the past.

Table of Contents

1. Introduction

Blockchain technology exploded onto the computer science scene in 2008 when an anonymous user (or users), writing under the pseudonym Satoshi Nakamoto, sent to a cryptography mailing list a description of a new open-source technology called “Bitcoin”. Bitcoin was the first (successful) digital asset that is now generally known as a cryptocurrency. Popular attributes of cryptocurrencies include the idea that they are completely digital assets or currencies whose transactions do not rely on a third person intermediary, which is true for all conventional currencies. Even United States dollars require a third party in simple cash transactions between a buyer and seller because their value is based on the full faith and credit of the United States government. Other third-party intermediaries include banks who control access to bank accounts as well as notaries that can verify that the terms of a transaction were completed. The promise of cryptocurrencies is to eliminate the reliance on these third parties.

Since the introduction of Bitcoin in Nakamoto’s paper, Bitcoin has flourished and received worldwide attention. In addition, thousands of alternative cryptocurrencies have flooded the market, often using the same fundamental technology as Bitcoin but with modifications that the developers of the alternative cryptocurrencies, or “altcoins,” deem desirable. With the growth in popularity of cryptocurrencies and the massive markets and demand produced for them, it is paramount that research be done to investigate the viability of the technology and of methods to improve upon it. The aim of this paper is to further this mandate via the exploration of multiple facets of blockchain technology including the current state of the technology and its history. It will involve a review of recent literature, related works, current efforts, and a discussion of the technological foundations of cryptocurrencies. We aim to focus on the interoperability and exchange of multiple cryptocurrencies and the implications of multiple blockchains interacting with one-another. In particular, we will complete our investigation by narrowing the focus further by experimenting on the possibility of arbitraging multiple cryptocurrencies.

The paper will be organized as follows. Section 2 describes the background behind cryptocurrencies and discusses why individuals may wish to exchange between cryptocurrencies. Section 3 discusses individual cryptocurrencies in depth and compares them amongst each other. Section 4 expands upon general blockchain concepts and efforts that are important to understand in order to grasp the discussion on interoperability. Section 5 describes schemes and efforts to enable cross-chain cryptocurrency exchanges and interactions. Section 6 involves the description of an experiment we prepared that seeks to shed light on the possibility of arbitrage amongst three or more cryptocurrencies and how an exchange scheme as described in Section 5 could assist in enabling such an arbitrage. Finally, we conclude this investigation in Section 7.

2. Background

While the public at large knows the name “Bitcoin”, the general perception of the public seems to be that this is a standalone entity often used for nefarious purposes. However, it might surprise many that a cryptocurrency named Tether consistently has trades at a higher volume than Bitcoin (“Top 100 Cryptocurrencies by Market Capitalization”)(Kharif, “The World’s Most-Used Cryptocurrency Isn’t Bitcoin”). The main reason for this is that Tether is what is known as a “Stablecoin”, which is a cryptocurrency designed specifically to resist volatility and prevent large price fluctuations as is common with cryptocurrencies similar to Bitcoin (Blenkinsop) .

This example points to a problem prevalent within the Cryptocurrency market—which Cryptocurrency should one invest in? The answer is not so simple because many cryptocurrencies have different goals that they set out to accomplish. Bitcoin was the first cryptocurrency and has thus had time to become prominent in the public consciousness and to proliferate as a result. However, while the value of bitcoin is derived from aspects that create value in fiat currencies, such as its scarcity, utility, transportability, etc., its value is ultimately dependent on what humans believe its value to be (Kelleher). This leaves Bitcoin vulnerable to speculation and leading to massive price fluctuations similar to what one might observe on a stock market. For example, over the course of 2017, the price of one Bitcoin surpassed $1,000 for the first time, eventually growing exponentially to almost $20,000 at its peak (Rudden). Figure 1 below displays the value of Bitcoin over time, with its steep peaks and valleys.

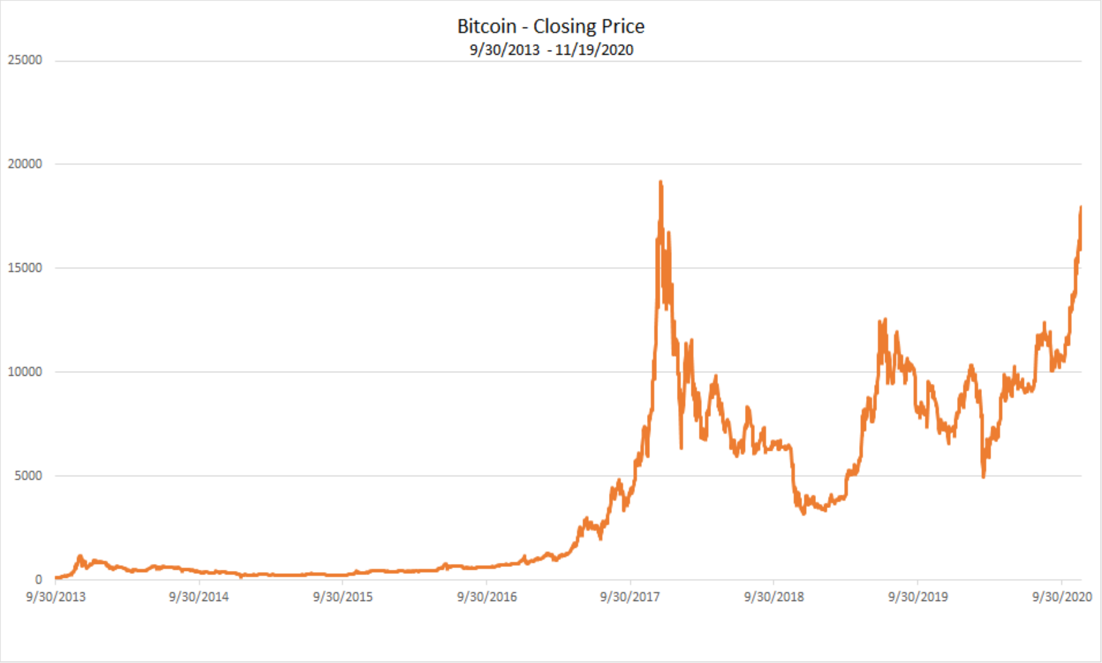


Fig. 1 - Bitcoin closing price over time from: (“Bitcoin Price Index”)

Toward the beginning of this investigation, on June 5, 2020, the price of Bitcoin closed at $9,659.66, roughly half of its 2017 peak. At the time of editing this paper, however, just over five and a half months later on November 20, 2020, Bitcoin is worth over $18,611.74 (“Bitcoin Price Index”). The immense fluctuations can easily be seen in Figure 1. For those investing in cryptocurrencies, such large fluctuations may leave more risk-averse investors wary of investing in Bitcoin. At the same time, however, Tether (originally RealCoin) is an altcoin that does not suffer from speculation in the same way because each token is supposed to be backed by one U.S. dollar or other fiat currency, similar to the way in which the gold-standard used to work (“Stablecoin Cryptocurrencies Based On Golden Standards”) in the United States. While the veracity of this backing is disputed, the idea that one cryptocurrency can be less volatile than another illustrates why a person may wish to exchange one cryptocurrency for another.

Other coins have other advantages compared to Bitcoin and Tether. One prominent example is Ether, which is the cryptocurrency that exists within the Ethereum software platform. Ethereum will be discussed in much greater detail, but the aspect worth noting now is that personalized programs and applications can be written by programmers and then hosted directly on the Ethereum blockchain with a Turing-complete language. This feature is not available on Bitcoin and makes Ethereum attractive to developers and investors that wish to exchange coins using Ether (Hayes, “Is Ethereum More Important Than Bitcoin?”). Other coins, such as XRP developed by Ripple, do not require coins to be “mined” and all coins that will ever exist, already do (“Ripple Vs. Bitcoin: Key Differences”). Litecoin is similar to Bitcoin but was designed so that mining could be done on household computers. Libra, a coin set to launch within the next year was created by

Facebook, and thus already has an established mega-corporation backing it which should ensure that it has every resource at its disposal to ensure its resilience and stability long-term. These same issues that might be enticing to some investors, however, will also turn off others, notably being owned by Facebook specifically (Posner).

Naturally, there are also more practical considerations to take when choosing a cryptocurrency to purchase. Some cryptocurrencies may be more accessible to users, or a good that a user wishes to buy may only be purchasable by one specific cryptocurrency. Other attributes worth considering include efficiency, ease of access, value, security, privacy, and the size of the cryptocurrency's user-base. The fact that no one coin has emerged to dominate the cryptocurrency market suggests that multiple coins may continue to exist simultaneously. As of today, there are more than 5,000 cryptocurrencies (Redman). The wide availability of different cryptocurrencies with varied uses and advantages leads us to believe that, until a single coin comes to dominate all the rest, we should actively pursue reasonable exchange schemes because the value of each coin's advantage will change daily depending on the needed use of the coin. Before diving into the mechanisms of exchanging one cryptocurrency for another, however, it is important to have background knowledge of prominent competing coins in order to understand the necessity and inner working of the exchange protocols described below.

3. Cryptocurrencies

While the most successful to date, Bitcoin was not the first attempt to create a digital currency. As early as 1983. David Chaum at the University of California Santa Barbara proposed digital signatures that could provide privacy and allow for proof of payment for online payments. His published works argued that two-key digital signature systems could be used for anonymous payment verification (Chaum 199). Fast forward to 1995, and Chaum rolled out DigiCash which allowed for anonymous transactions. While DigiCash was not successful in the end, it provided some key ideas that would be foundational to blockchain-based cryptocurrencies that would eventually be developed.

Similarly, Wei Dai at the University of Washington, proposed in a paper what he called B-money. He described using public keys as pseudonyms in B-money to keep transactions anonymous and suggested a "proof-of-work" system, similar to modern cryptocurrencies, and which would free B-money from the constraints of a trusted third-party acting as an intermediary (Dai).

In order to go in-depth about various cross-chain cryptocurrency schemes, it is first important to discuss commonalities amongst (most) cryptocurrencies as well as what distinguishes them. The obvious place to start is with Bitcoin since all other modern cryptocurrencies derive at some level from this early model. For this reason, also, we will delve quite deeply into the inner workings of the Bitcoin blockchain. This will give us a reference when speaking to the differences of other chains, as well as helping us to describe the way in which different cross-chain communication schemes work.

3.1 Bitcoin

Bitcoin claims to be the first successful implementation of a digital cryptocurrency that was originally described by Wei Dai ("Bitcoin Wiki"). On November 1, 2008, a pseudo-anonymous person, or possibly a group of people, claiming to be a Japanese man named Satoshi Nakamoto submitted a research paper (known as the Bitcoin whitepaper) proposing the outline for a new form of digital currency. The timing of the release, as well as a cryptic message that is written into the first block of the bitcoin blockchain: "The

Times 03/Jan/2009 Chancellor on brink of second bailout for banks" may suggest that the release had something to do with the global financial crisis that began that year (Tardi, "Genesis Block"). As evidence, the first sentence of Nakamoto's white paper reads:

> "Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model." (Nakamoto 1)

This is the core function of a modern cryptocurrency: to provide a means of conducting transactions without the need of a third party to verify the legitimacy of the transaction. Further, Bitcoin is an attempt to solve the "double-spending" problem which has plagued earlier digital currencies. The double-spending problem involves the possibility of spending a single token multiple times from the same originator because it exists in the form of data that can be modified or copied (Chohan 1). In general, the only way to solve this problem would be for a trusted third party, in effect a middleman, to keep a record of transactions that can be audited at a later time. Nakamoto proposed using cryptographic proofs to avoid this problem instead of third parties (Nakamoto 1).

In order to avoid the need for a trusted third party, Bitcoin publishes all transactions publicly so that they can be verified by anyone. This is partially accomplished via a timestamp server, which adds a timestamp to all transactions and publishes the timestamp publicly. The public also needs to be sure that the information that has been entered cannot later be changed. This is accomplished with a proof-of-work scheme, and this is where the idea of a blockchain begins to form.

First, we must describe a “block”. A block is a set of data that includes, among other things, a nonce, the previous block’s hash, and recent transaction data. We will go over other important features of a Bitcoin block, but these are the key items needed to understand a proof-of-work scheme. First, a hash value is a bit-array of a fixed length that is formed when some piece of data is fed into a mathematical algorithm known as a hash function. Bitcoin uses the SHA-256 hash function. An equivalent hash value will always be formed when the same data is input into the hash function. However, a hash value cannot be reversed (practically) back into the original data. Consider the following image, which demonstrates the hash value formed given similar input data using the SHA-1 hash function:

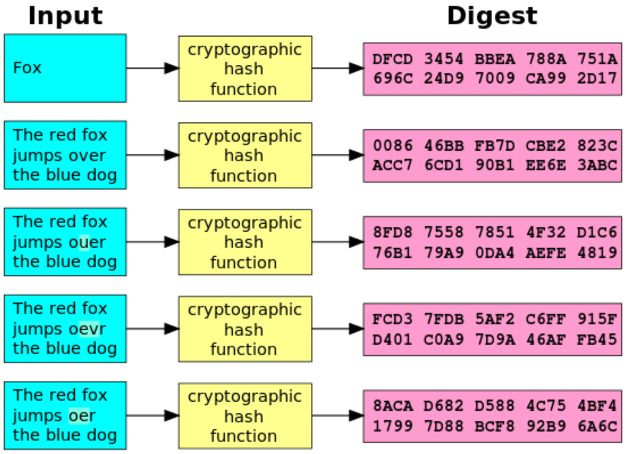

Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

Fig. 2 - Hash-value derivation example from: (“Cryptographic Hash Function”)

The key point to notice is that very minor changes in the input create vastly different and more importantly, unpredictable, hash values. In fact, the only reasonable way to produce a hash value with specific properties is to change the input data until a hash with the desired attributes is formed.

This is the basis by which a block is “solved” and added to a chain in the Bitcoin blockchain through proof-of-work. In Bitcoin’s proof-of-work scheme, blocks are added to a chain when the hash value of the data contained within the block begins with a specified number of zeros[1]. Because it is extremely unlikely to the point of near impossibility that the block's hash value will begin with the specified set of zeros, the data within the block must be altered to change the hash of the current block. The data that is altered is known as the "nonce", which is just an arbitrary number. The only feasible way to find the nonce that creates the desired hash-value is through a brute-force method of testing random nonce values and their effect on the hash. This requires CPU power and is what is known as "mining". Miners are incentivized to use their CPU power to "solve" blocks by being awarded with Bitcoin upon their successful finding of the nonce that generates the needed hash value and adding a block to the chain. Bitcoin is programmed so that a new block will be mined approximately every ten minutes. The speed at which a block is mined depends on the total CPU power being used to mine the new block so the Bitcoin blockchain will increase or decrease the difficulty of mining a block according to how long the previous block took to mine. Mining difficulty is increased or decreased by changing the number of zeros that are needed at the beginning of the block's hash-value. You can see the hash of the latest block that has been solved, as well as the difficulty that was required, via https://btc.com/.

When a block has been "solved" or "signed", it is added to the blockchain, which can be described as a series of blocks that are linked together. The primary way in which

[1] The exact number of zeros that will be required is based on how long the Bitcoin software determines the next block should take. In order to be "deflationary", the difficulty of Bitcoin blocks is often altered so that new blocks are created on a more-or-less specified timeframe.

they are linked is that the hash of each block is calculated, in part, based on the hash of the previous block. Any change to one of the precedent blocks in the blockchain will change the hash of that block. And, because the hash-value is composed of all the data in a block (including the hash-value of that preceding block), the hash-value of every subsequent block will be changed (Nakamoto 3). The longest chain of blocks that is broadcast is the one that is accepted. Therefore, if someone changed transactional information from a precedent block, each block after would have to be re-mined and then new blocks in a separate branch of the blockchain would have to be added. This becomes exponentially more difficult the further down the chain you attempt to alter a block, so it is extremely unlikely to occur in reality. This provides much of the security inherent in Bitcoin's blockchain technology. Furthermore, the blockchain is available publicly, so any alternative chain that does not match the chain that is accepted by the majority users can be safely disregarded as a chain with incorrect transactional data. The publicly available is generally referred to as the public ledger.

Another feature of Bitcoin worth exploring is its use of Merkle Trees to store transaction data in older blocks (Nakamoto 4). Merkle Trees, similar to blocks, make use of hash functions. A typical Merkle tree involves creating a hash value for the transaction data of every transaction that occurred within that block. Then, pairs of the hash values created from the transactions are run through the hash function again to create a new hash value for the pair of transactions. This is repeated for each pair until a binary tree is formed with each node containing the hash value of a pair of hash values below it in the tree. The root of this binary tree is called the "merkle root" and is stored in the header of the block. The merkle root contains the hash value based on every other paired hash value. Because each hash value of the nodes above the leaves are based on the hash values of a pair of nodes below them, if any transaction data in any node below the Merkle root is changed, then the hash values of all of the nodes above that transaction would also change, including the Merkle root. This allows users to compare only the Merkle root of each block instead of comparing each individual transaction from every block when searching for where a change in a prior block occurred. The Merkle root does not contain any information about the depth of the tree. However, given the speed that blocks are currently being mined, approximately 2,200 transactions occur within every block, so the ability to only compare one value instead of thousands makes the system as a whole much more efficient ("Average Transactions Per Block"). This also has the benefit of saving a lot of storage space on the blockchain itself.

Privacy is another major concern with blockchain-based cryptocurrencies. Bitcoin attempts to achieve a level of privacy by utilizing a system of public and private keys (Nakamoto 6). Public keys are derived from a private key that is held by each user and known only to that user. The private key can be used to "digitally sign" a transaction, and the public key can be used to verify that signature. This allows transactions to be authenticated. Finally, a hashed version of the public key is created and shared in the form of an "address". These addresses are shared between users that wish to initiate a transaction and can be used as a "bank account number" of sorts to identify users (Frankenfield, "Public Key"). These addresses do not contain identifying information, so there is no direct way to know the identity of the user from this address alone.

With a general understanding of the computational foundations of Bitcoin, an important question remains: Why does Bitcoin have value? According to the Bitcoin organization, it is because there are several factors that influence the value of any currency including durability, portability, divisibility, scarcity, recognizability, and fungibility ("FAQ: Why Do Bitcoins Have Value?"). Bitcoin satisfies all of these criteria. Bitcoin is clearly durable, because as long as the internet continues to exist, Bitcoin can continue to exist. In fact, it will exist even after no one wishes to trade for it anymore. Similarly, Bitcoin is extremely portable because anyone with access to the internet can trade it between any two places in the world very rapidly. Bitcoin is very divisible, with one token being able to be divided and traded down to 8 decimal places ("FAQ: How Divisible Are Bitcoins?"). It is also scarce in the sense that an upper limit of 21 million Bitcoins is hard coded into the blockchain. Once that many Bitcoins exist, no more will ever be created. In addition, as time goes on, the reward for mining Bitcoin becomes smaller and smaller, providing even more scarcity. As for recognizability, a Harris poll determined that as of April 2019, over 89% of people had at least heard of Bitcoin (Spencer).

The question of fungibility is a little different. In theory, there is no difference between two Bitcoin tokens, much like there is no difference between two $20 bills. Consider, however, the value of that $20 bill if every good or service that had ever been purchased with it could be seen. If it had been used for illicit transactions, assumptions might be made about one's personal involvement with those transactions. This is a feature of Bitcoin and many other cryptocurrencies. In fact, companies have begun selling newly mined Bitcoins with no transaction history, known as "virgin Bitcoin", which have been sold at a premium. Virgin Bitcoins have increased value because they cannot be connected to nefarious activities and transactions that may have occurred in the past (Lielacher). That said, for an average user, this may not be a problem, so the degree of fungibility of Bitcoin seems to be situational. This question of the fungibility of cryptocurrencies will have implications in the need to exchange different cryptocurrencies, as we will discuss below.

Even despite the question of Bitcoin's fungibility, its price on the open market leaves no doubt that Bitcoin does have value. While Bitcoin has most of the qualities that create value in a currency, however there are other attributes that could alter the value of Bitcoin relative to other altcoins. Vitalik Buterin, the founder of Ethereum, writes in his paper *Chain Interoperability* that "[w]ithin the public blockchain space, different projects have been staking out different regions of the tradeoff space between security, privacy efficiency, flexibility, platform complexity, developer ease of use and even what could be described as public values" (Buterin 1). In the next sections, we will discuss several, mostly popular, altcoins in order to demonstrate their value compared to Bitcoin in order to both provide background information and to showcase examples of when cryptocurrency transactions would be desired by users.

3.2 Bitcoin Forks

We began this section with a discussion of Bitcoin because it was the original blockchain-based cryptocurrency and because many of the underlying technologies carry over into other cryptocurrencies. We will begin the discussion on alternative cryptocurrencies by describing altcoins that are direct derivations of Bitcoin itself.

Bitcoin is not run by a corporation, but rather by a dedicated community of developers and interested parties. In fact, Satoshi Nakamoto himself is no longer involved with the project and has disappeared (Bernard). Bitcoin is still evolving, however, so there needs to be a system to allow change and for the community to initiate potential changes, receive feedback and community approval, and to implement the changes. With Bitcoin, these changes are introduced by the community in the form of a Bitcoin Improvement Proposal (BIP). While BIPs must meet certain standards, they can be submitted by anyone. Before they are approved and implemented, BIPs must be approved by an editor and should include the code that would be used to update Bitcoin software. In the case of most BIPs, if 95% of the last 2,016 miners approve a BIP, then that proposal is approved and Bitcoin is updated, or forked[2] (Agrawal).

Forks come in the form of either softforks or hardforks. A softfork is a fork that involves changes to the Bitcoin protocol that are backward-compatible on the chain, meaning that old blocks will treat new blocks that are added after the fork as valid ("Softfork"). A hardfork, on the other hand, is not backward-compatible. The bitcoin wiki describes hardforks as "[a]ny alteration to bitcoin which changes the block structure (including block hash), difficulty rules, or increases the set of valid transactions is a hardfork" ("Hardforks"). In order for hardforks to be instituted within the protocol, every user must upgrade their software. If users do not upgrade their software to reflect the changes of the hardfork, they will effectively be conducting transactions and adding blocks to a blockchain that is separate from the chain that users that did upgrade will be using. If a large enough majority of the community embrace the changes brought on by a hardfork, then the hardfork will become the defacto blockchain.

Occasionally, a hardfork will be proposed that divides the Bitcoin community. Some users will adopt the change, and others will not. As noted earlier, the users that adopt the change will update their software and effectively create a new blockchain, identical to

[2] This is the approximate number of miners that it would take to mine blocks every 10 minutes for 14 days based on Bitcoin.

the original up to the last block before the changes were made. This phenomenon has driven the Bitcoin community to create several derivative Bitcoin blockchains, modified and running concurrently with the original Bitcoin blockchain, which is referred to as Bitcoin Core.

An early example of this forking is exemplified in the creation of Bitcoin XT. Bitcoin has a scalability problem that arises because, as stated before, the difficulty of mining a new block allows for an average of one block to be produced every 10 minutes. Because each block can only be as large as one megabyte, and each transaction takes up a certain amount of space, there is a limit to the number of transactions that can happen in a given time. The math works out to Bitcoin allowing about 7 transactions to occur every second, with a theoretical maximum of 27 transactions per second (Evangelos 5). Comparing this to Visa, which claims to have the capacity to process 24,000 transactions per second (“Visa Acceptance for Retailers”), one is presented with a clear problem that will only get worse with widespread adoption of Bitcoin—it cannot process large numbers of transactions quickly enough. The main idea behind Bitcoin XT, therefore, was to increase the size of a Bitcoin block from 1 megabyte to 8 megabytes. This would, in effect, allow for a faster transaction rate than Bitcoin core allowed because more transactions could be stored on one block, but they would still be mined and added to the chain at the same rate (Reiff). Miners were given the ability vote on whether to adopt Bitcoin XT by mining and producing new blocks with a new version number (indicating that they adopted Bitcoin XT rather than Bitcoin Core). If 75% of the last 1,000 blocks had been mined using this version number, then those miners would automatically abandon the old Bitcoin blockchain and begin mining on the new Bitcoin XT blockchain. However, only a small number of the miners adopted Bitcoin XT ("Bitcoin-XT News"). While it is technically still available, it has fallen out of favor and is largely abandoned.

Other Bitcoin forks that were not successful include Bitcoin Classic, Bitcoin Unlimited, and Bitcoin Gold. Bitcoin Classic was a proposal similar to bitcoin XT except that it proposed only increasing the size of a block to 2 megabytes (Frankenfield, "Bitcoin Classic"). Bitcoin Unlimited, on the other hand, proposed allowing miners to dictate their own block size via voting. Unfortunately, Bitcoin Unlimited had major security concerns (even being hacked at one point) (Frankenfield, "Bitcoin Cash Definition"). Bitcoin Gold was an attempt to limit mining to consumer GPU's in an attempt to make mining more egalitarian. Bitcoin Gold, however, suffered from security concerns and was never adopted. Similarly, neither Bitcoin Classic nor Bitcoin Unlimited were fully adopted by a large enough community and no longer have an active enough following (Won) to cement these forks as legitimate competitors. There is an ongoing, heated debate within the extended Bitcoin community about how to address the scalability problems inherent in Bitcoin's original design (Elliot-Ennis and O'Leary).

Some forks, however, have become popular in their own right alongside Bitcoin Core. The most notable example is known as Bitcoin Cash, which launched in July 2017 and is the largest and most successful bitcoin fork. Bitcoin cash was proposed after the failure of Bitcoin Ultimate and also allows for adjustable block sizes. Because it was a fork of Bitcoin Core, anyone that held tokens on the Bitcoin Core blockchain held the same amount of tokens on the Bitcoin Cash blockchain, so there was an immediate initial interest, with the opening price on August 1, 2017 being $294.60. By the end of 2017, Bitcoin Cash was worth as much as $3,909 ("Historical Data for Bitcoin Cash"). Bitcoin

Cash was also given a boost because it was supported by the world's largest cryptocurrency mining platform, Bitmain, as well as receiving support from Chinese mining operations (Frankenfield, "Bitcoin Cash Definition")(Popper). Currently, Bitcoin cash is valued at $260.68 as of November 20, 2020 ("Historical Data for Bitcoin Cash").

While this price is quite a bit lower than its historical high, its price does demonstrate that there is still a demand for Bitcoin Cash tokens years after its launch. Bitcoin Cash supporters argue that by allowing for larger block sizes, and thus a higher capacity for more transactions per second, that Bitcoin Cash is better suited to be used as a currency, compared to Bitcoin Core which is better suited as a store of value (Jeffries). Interestingly, Bitcoin cash *itself* has undergone a recent fork, in effect creating two Bitcoin altcoins out of one. The original Bitcoin Cash blockchain is now known as Bitcoin Cash ABC, while the forked version of bitcoin Cash is known as Bitcoin Cash SV (Satoshi's Vision). This fork came about due to a disagreement amongst bitcoin Cash developers on the incorporation of smart contracts, as well as further increases to block sizes (Frankenfield, "Bitcoin Cash Definition"). Both forks remain competitive and are actively traded today.

3.3 Other Cryptocurrencies

In this subsection, we will describe some of Bitcoin's most prominent competitors in the cryptocurrency market. While Bitcoin is still the dominant cryptocurrency, several altcoins are beginning to cut into Bitcoins market capitalization. You can see this visually in Figure 3, which is taken from coincapmarket.com.

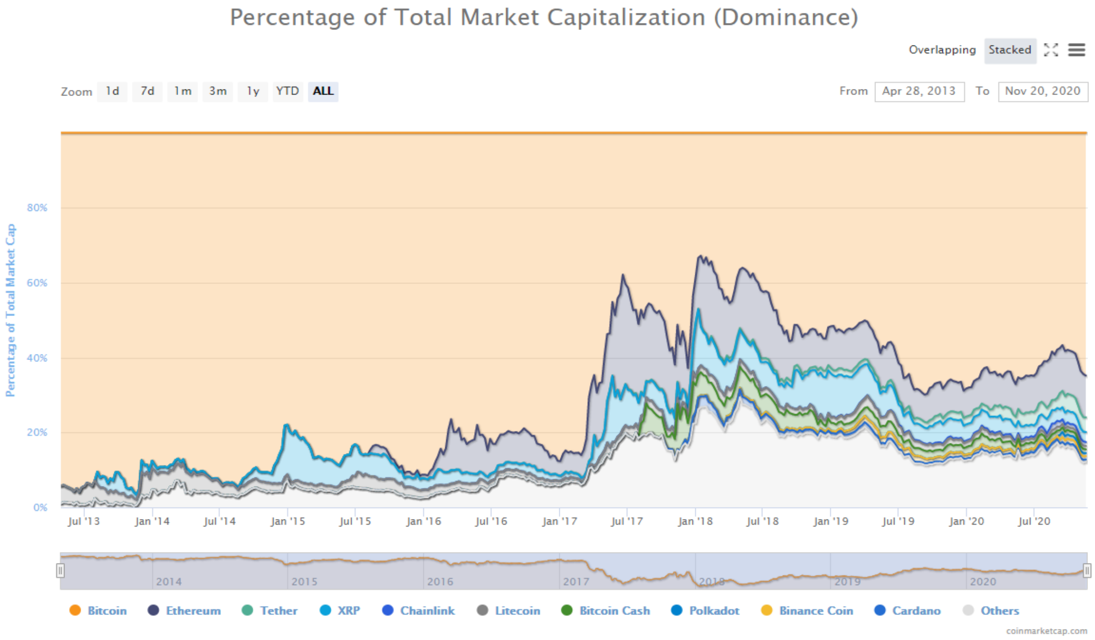


Fig. 3 - Market capitalization of various cryptocurrencies from: ("Global Charts")

3.3.1 Altcoins

Litecoin is an example of an early altcoin that was released in 2011 and has distinct, situational advantages over Bitcoin. While it is largely based on the Bitcoin source code, similar to the Bitcoin forks discussed above, its creator Charles Lee wanted to create an altcoin on a distinct blockchain that could boast faster transaction speeds. One key difference is that new blocks are mined every 2.5 minutes, instead of 10 minutes as on the Bitcoin Blockchain (Steadman). It also has a larger maximum number of coins that can exist on the blockchain compared to Bitcoin.

Another difference that differentiates Litecoin and Bitcoin is Litecoin's use of the "Scrypt" hashing algorithm for its proof-of-work scheme instead of using SHA-256 as used by Bitcoin. Scrypt lowers the advantage of miners that are using GPU-intensive computers by being memory intensive as well. This means that the nonce values generated are stored in the computer's RAM which must be accessed in order to submit a result (Fernando).

The intent of Scrypt is to allow more common users to mine for cryptocurrencies, whereas Bitcoin mining is largely dominated by large firms that set up “mining farms”. In January of 2020, five mining operations controlled 49.9% half of the Bitcoin’s hashrate (Redman), meaning that those five companies mined about half of the blocks available to be mined in that month. The relative distributions of some of the largest mining farms over the past three years is displayed in Figure 4 taken from blockchain.com[3].

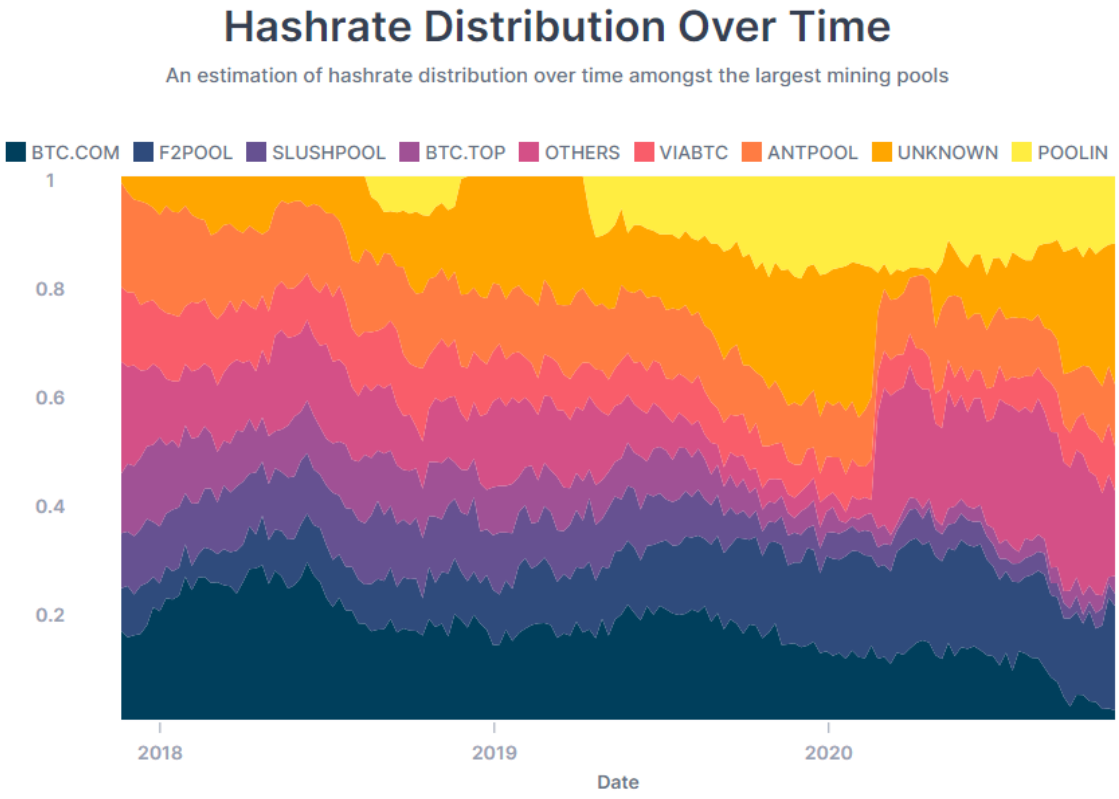


Fig. 4 - Hashrate Distribution over time from: (“Hashrate Distribution Over Time”)

[3] BTC.COM is operated by Bitmain Technologies Ltd. Bitmain was mentioned in Section 3.2 and is the company that gave credence to the viability of Bitcoin Cash.

In addition to transaction speeds, another consideration for a cryptocurrency user when choosing a cryptocurrency user may be whether they require total, or as close to total as possible, anonymity. Bitcoin is what is known as a pseudo-anonymous cryptocurrency. While your Bitcoin wallet address is not directly tied to your identity, the fact that there is a public ledger that details *all* public transactions means that any movement of Bitcoin can be detected forever on the chain. In some cases, access to all of this transaction history between accounts can provide a lot of unintended information to sources that are looking through the ledger, such as law enforcement (Orcutt). Consider the instance where a single user's identity was matched to their public key. Now, every address that has ever transacted with them will be less anonymous than before because someone viewing the chain knows a new piece of information about you—specifically that you are someone that has interacted at some point with the identified user. Some users, for better or worse, may wish to move closer toward full anonymity, and there are blockchain-based cryptocurrencies that hope to achieve this, such as the coin known as Monero.

Monero is different from Bitcoin in several respects that make it more private. While in many cryptocurrencies such as in Bitcoin users can have multiple addresses, in Monero every transaction is sent over a single-use (stealth) address and these addresses are stored on the blockchain (Kurt Magnus). Further, Monero utilizes ring signatures to perform account verification. This means that instead of a single private, public key pairing, every private key in a Monero transaction will have a "ring" of public keys that are all equally likely to be part of the matching pair of keys. An outside observer would not be able to tell which was the correct public key that corresponds to the private key in question (Kurt Magnus). This allows a sender plausible deniability that they are the true address that was involved in a Monero transaction. Monero is seen as a sort of “testing ground” for new cryptographic privacy techniques (such as “bulletproofing”)[4] that may one day be adopted by other cryptocurrencies if there is some degree of success (Nuzzi).

While the privacy technology under the hood of Monero is impressive, there are drawbacks to the amount of privacy it affords. Because of its privacy, Monero is an obvious choice for money-laundering and is beginning to become a coin of choice for purchasing illicit goods (Greenberg). Also, Monero can be mined using more common computers than Bitcoin, so it is common for Malware that infects a computer to use the infected computers resources to mine Monero instead of other cryptocurrencies. In fact, 44% of all cryptocurrency-based ransom-ware attacks involved demanding Monero (Rooney) or exchanged other currencies into Monero such as in the example of the infamous WannaCry ransomware attack (Neutrino Research Team). Once this Monero has been obtained, it is extremely difficult to trace back to the attacker. This is not, however, to say that Monero should be demonized and that illicit uses are the only benefit. Along with its inherent privacy, Monero is much easier to mine than Bitcoin, is very technologically advanced even by cryptocurrency standards, and has a large, dedicated development team behind it

[4] Bulletproofing is “non-interactive zero-knowledge proof” that allows users to see whether a secret value exists within an interval without having the interval having to be set up beforehand. This system can allow public validation of a transaction on a public ledger without revealing any information about the users involved with the transaction. Bulletproofs are shorter than similar existing proof methods which will make a blockchain platform that implements it more efficient. (Bünz et al.)

(Saurel). However, illicit uses also may incentivize users to divest from Monero and exchange their coins with a different cryptocurrency.

Another reason to choose one specific cryptocurrency coin over another is that, in the future, coins may begin to be distributed by governments. On July 23, 2020, Lithuania became the first country to release a state-backed digital currency in the market, a cryptocurrency called LBCOIN. LBCOIN is largely a trial to determine the efficacy of a state-backed cryptocurrency. In fact, the Bank of Lithuania discourages its use as a means of payment and simply considers LBCOIN a digital collector's coin. The release and endorsement by a central government marks a turning point in trust of digital currencies by governments ("Regulations for LBCOIN and Its Issue Date Approved"). China's central bank is similarly experimenting with and plans to roll out its own digital currency based on blockchain technology which will be distributed to consumers via large institutions and corporations (del Castillo). However, while LBCOIN may suggest that state-backed cryptocurrencies are on the way, there is reason to believe that these coins may not be released—both Japan and Russia have put their state-backed digital currency aspirations on hold (Tassev). It is clear though that if government-back cryptocurrencies become popular, however, that they would have clear advantages (travel, monetary-policy, trust, etc.) that would make exchanges desirable.

Finally, in recent years cryptocurrencies have been created with the sole purpose of facilitating charitable donations. A company known as smARTOFGIVING has created a coin called AOG which is an ERC-20 token (discussed below) on the Ethereum blockchain. The idea is that instead of mining, new coins are generated through reaching checkpoints on free-to-play mobile games (Whitepaper: SmART OF GIVING (AOG)). When the checkpoint is reached, the user can decide which charity to donate the generated coins to. By going about generating new tokens in this way, coins will be donated to charity without smARTOFGIVING ever having to actually ask for donations. In order for a functioning ecosystem to exist before the coin generation began, smARTOFGIVING held an Initial Coin Offering (ICO), which is similar to an Initial Public Offering that occurs when a corporation begins offering its shares to the public. Fifty percent of all AOG coins existed before the games went live on cryptocurrency exchanges, with the other fifty percent being donated fully to select charities afterward. Cryptocurrency users may wish to invest in this coin as popularizing it means that the donations created by users playing games will be worth more to the charities receiving donations (Whitepaper: SmART OF GIVING (AOG)) .

3.3.2 Stablecoins

As described earlier in this paper, Tether is what is known as a "stablecoin" which is a cryptocurrency designed with the intention of having low price volatility. The premise is that Tether tokens will be pegged to a fiat currency, in Tether's case the U.S. dollar. This is made possible by Hong Kong based Tether Limited maintaining one-to-one reserves of U.S. dollars for every token of Tether issued ("Tether: Fiat Currencies on the Bitcoin Blockchain" 1). In theory, a user should be able to exchange Tether for U.S. dollars (or Bitcoin) at any time. More risk averse cryptocurrency users may prefer this to other cryptocurrencies, which have experienced over 50% reductions in value within the span of a day (Young). Tether also benefits from a high level of security as it runs on the Omni Protocol Layer of Bitcoin (originally known as Mastercoin). The Omni layer protocol is essentially a scheme whereby sending very small amounts of Bitcoin to specific addresses and providing transaction data for Altcoins within the notes of Bitcoin transactions can allow for other cryptocurrencies to exist and be exchanged on top of the Bitcoin blockchain (Willet et al.). This allows Coins based on the Omni protocol to enjoy many of the advantages of Bitcoin's blockchain, such as its anonymity, rigorous testing, and integration with merchants and wallets ("Tether: Fiat Currencies on the Bitcoin Blockchain" 4).

While a stablecoin's advantage is the low risk of wild price fluctuations, an efficient exchange method is also necessary. In Tether's case, the fact that Tether Limited is required to hold reserves of a fiat currency necessarily means that Tether is no longer decentralized in the same way as Bitcoin. This is problematic because the use of Tether requires trust in Tether Limited, and trust in a third-party is one of the main issues that the creation of Bitcoin was meant to avoid. Cryptocurrency users may wish to avoid placing trust in a third party completely or may be incentivized to exchange their tokens if the third party breaches their trust. An example of such a breach includes a report that Tether Limited only backs Tether with 74 cents for every dollar worth of the Tether token, which prevents a guaranteed exchange of Tether for U.S. dollars being strictly possible (Kharif, "Tether Says Stablecoin Is Only Backed 74% by Cash, Securities").

Libra, a cryptocurrency in the works by Facebook, Inc. is another stablecoin that is based upon non-digital assets. Libra was originally planned to be pegged to a basket of currencies, rather than a single fiat currency. Facebook acknowledges, however, the potential for interfering with the monetary policies of the entities whose fiat currencies are involved. It has responded by also allowing single-currency stable coins to exist on its network ("Libra Whitepaper" 1), Facebook has since revised what will constitute the basket of currencies saying

> "'The Libra Reserve is expected to be a fungible pool of cash and very short-term government securities that are expected to be denominated in U.S. dollars, euros, Japanese yen, British pound sterling and Singapore dollars,' a Libra association spokeswoman said in a statement to Barron's. 'We are not commenting on the specific breakdown of the Libra Reserve.'" (Walsh).

Additionally, Facebook has no intention of keeping Libra decentralized. Libra will be a permissioned blockchain meaning that the organization known as the Libra Association, composed of businesses and NGOs, will be the only entities able to mine Libra. Having all of the mining power allows the Libra Association to act as "a de facto central bank" (Ip). While Libra benefits from being created with the funding and resources available to a mega corporation such as Facebook, it may suffer from a lack of public trust in Facebook.

One final stablecoin worth mentioning in Terra. Terra, while also being pegged to fiat currencies, maintains its stability in part by programming supply adjustments directly into its core programming. More specifically, Terra is backed by another cryptocurrency within its protocol, Luna. Luna is rewarded to miners of the Terra blockchain, but the amount awarded is changed to make mining more or less valuable which indirectly affects the value of Terra and keeps its price stable (Kereiakes et al. 5). Users may wish to exchange for Terra if they are traveling. Similar to exchanging for a foreign country's fiat currency, Terra is currently most popular and is being accepted by merchants in Southeast Asia so a user traveling to Southeast Asia may wish to exchange for this coin. Additionally, Terra is a blockchain implemented on Tendermint as opposed to Ethereum, which may have advantages as described in Section 4 below (Platias).

3.4 Ethereum

In the previous subsections, we discussed Bitcoin, along with its technological foundations as well as several alternative cryptocurrencies and their advantages and disadvantages compared to Bitcoin. Ethereum, meanwhile, is a blockchain technology that deserves a section all to itself. In one of the forthcoming sections, we will discuss in depth a particular scheme for achieving efficient exchanges of cryptocurrencies that relies heavily on Ethereum technology. In order to make sense of that scheme, we will dedicate a section to covering Ethereum technology and why it facilitates such schemes.

Ethereum was originally developed in order to create a new blockchain that addressed what the developers of Ethereum considered to be a serious limitation in Bitcoin. While Bitcoin has very basic stack-based scripting that can be used to create limited programs, there are several weaknesses according to the developers of Ethereum: lack of Turing-completeness, value blindness, lack of state, and blockchain blindness (Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform" 12). According to the Vitalik Buterin, the founder of Ethereum, the main concept missing from Bitcoin's scripting implementation is the lack of ability to create loops. Without loops, creating many programs becomes infeasible. Ethereum, however, was created with the aim of allowing for programming on the Ethereum blockchain using fully Turing-complete languages such as Solidity or Vyper, both of which allow for loops and other functions common in high-level languages. Value-blindness refers to the idea that the balance of Bitcoins owned in an account is determined by summing all of the transactions throughout Bitcoin's entire history that have affected the balance of an account (Chakravarty). Fine-grain control is not possible with Bitcoin scripting--Ethereum aims to fix this issue by allowing the Ethereum network to keep track of state objects called "accounts" that store ether balance so that fractional values can be easily transferred between accounts. Further, the accounts taken together serve as the state of the Ethereum platform. Finally, unlike Bitcoin, Ethereum allows you access to the data contained in the block header (Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform" 13) as well as external information not available natively on the blockchain (Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform" 20).

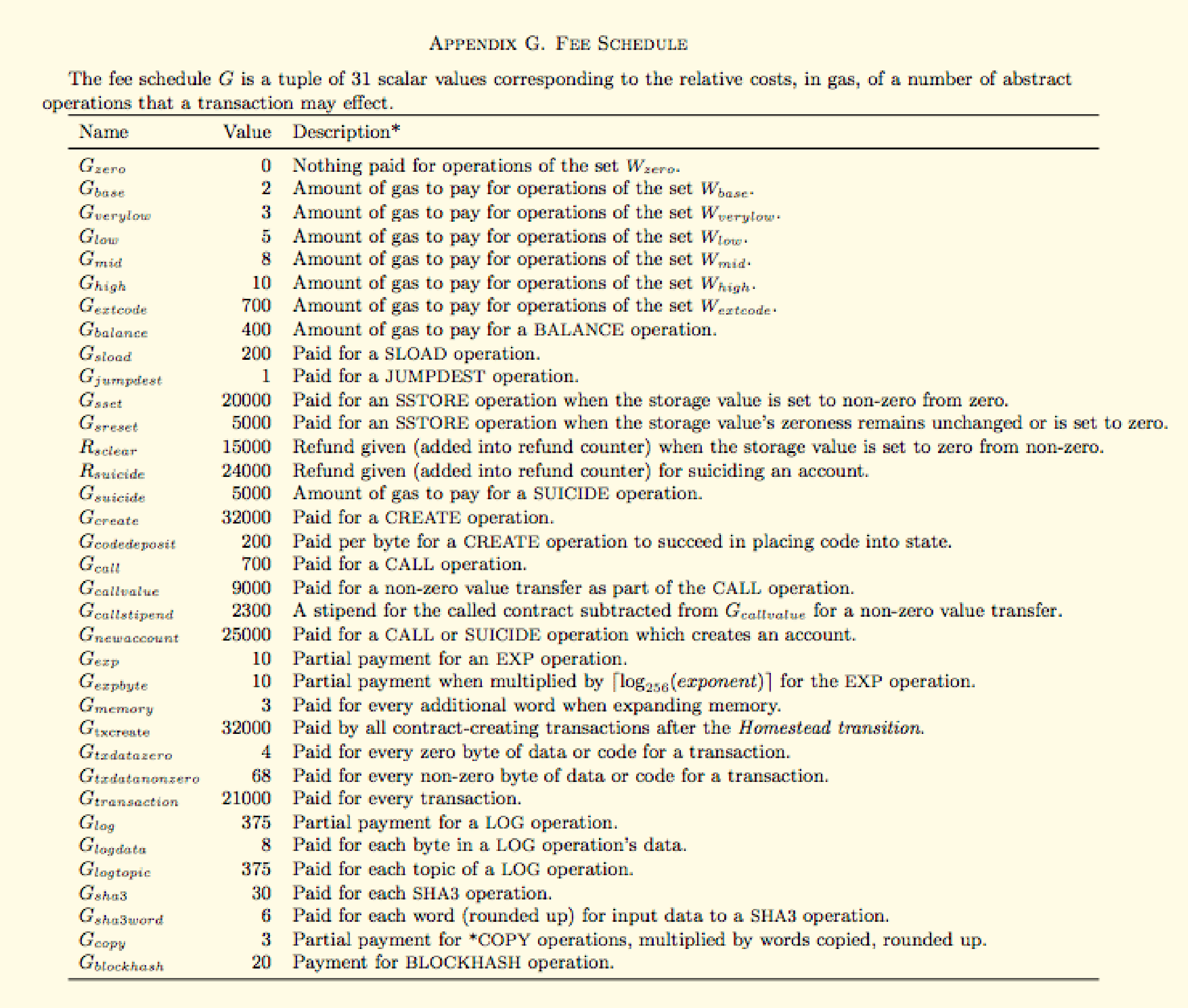
The driving force, and primary goal of Ethereum, is to allow for the writing and execution of robust and complex "smart contracts" on the platform. Buterin describes smart contracts as "systems which automatically move digital assets according to arbitrary pre-specified rules" (Buterin 1). These contracts allow for exchanges that do not rely on trust between parties ("Contract") and that can be coded by anyone and executed automatically when certain conditions are met. The concept of smart contracts was originally conceived of by Nick Szabo in 1997 (Szabo) but was not implemented in any true form until the introduction of the Bitcoin blockchain. As discussed earlier, however, the Bitcoin scripting system is not as robust as it could be, and Ethereum tries to fix that through its platform. In addition, it is important to note that Ethereum also differs from Bitcoin in that it sends "messages" rather than "transactions". Buterin explains the difference concisely:

> "'Messages' in Ethereum are somewhat similar to "transactions" in Bitcoin, but with three important differences. First, an Ethereum message can be created either by an external entity or a contract, whereas a Bitcoin transaction can only be created externally. Second, there is an explicit option for Ethereum messages to contain data. Finally, the recipient of an Ethereum message, if it is a contract account, has

> the option to return a response; this means that Ethereum messages also encompass the concept of functions" (Buterin 14)

The way that Ethereum allows this to happen is that instead of storing the current ledger for all Bitcoins, the Ethereum platform holds the current state of all smart contracts executed on the system as well as all transaction information. In order for nodes to have an incentive to mine the new blocks that will store all of the data, miners need to have some incentive. This is achieved through Ether, which is the actual cryptocurrency token that exists on the Ethereum blockchain. 5 ether is earned for miners when a new block is created which is programmed to happen on average every 12 seconds (Hertig). Much like Bitcoin, consensus is achieved through a proof of work system (though Ethereum may transition to a proof-of-stake system in the future). This ether allows the system to work, as each transaction and smart contract has a 'fee' that incentives miners to use computational power to process the transaction or contract.

These fees are possible thanks to the Ethereum Virtual Machine (EVM) which is the translation of high-level code (such as in Solidity) to low-level byte-code that runs in an assembly language using opcodes that control different actions that the code can take. Virtual machines are written in order to provide portability and to allow the code to run on the platform instead of being handled by the host (Hollander). Every opcode that is run has a cost that is referred to as "Gas". Different opcodes and their gas prices can be seen in Figure 5 below, borrowed directly from the Ethereum yellow paper.



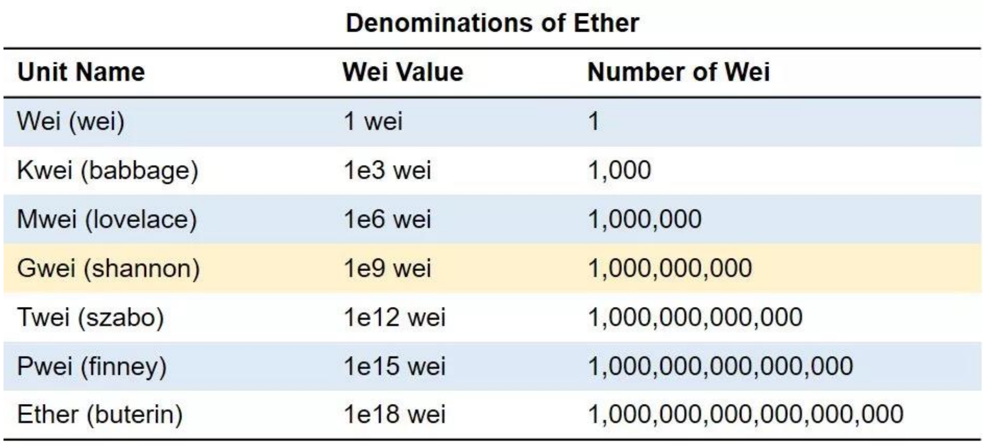
Appendix G. Fee Schedule

The fee schedule G is a tuple of 31 scalar values corresponding to the relative costs, in gas, of a number of abstract operations that a transaction may effect.

Name	Value	Description*
G_{zero}	0	Nothing paid for operations of the set W_{zero}.
G_{base}	2	Amount of gas to pay for operations of the set W_{base}.
$G_{verylow}$	3	Amount of gas to pay for operations of the set $W_{verylow}$.
G_{low}	5	Amount of gas to pay for operations of the set W_{low}.
G_{mid}	8	Amount of gas to pay for operations of the set W_{mid}.
G_{high}	10	Amount of gas to pay for operations of the set W_{high}.
$G_{extcode}$	700	Amount of gas to pay for operations of the set $W_{extcode}$.
$G_{balance}$	400	Amount of gas to pay for a BALANCE operation.
G_{sload}	200	Paid for a SLOAD operation.
$G_{jumpdest}$	1	Paid for a JUMPDEST operation.
G_{sset}	20000	Paid for an SSTORE operation when the storage value is set to non-zero from zero.
G_{sreset}	5000	Paid for an SSTORE operation when the storage value's zeroness remains unchanged or is set to zero.
R_{sclear}	15000	Refund given (added into refund counter) when the storage value is set to zero from non-zero.
$R_{suicide}$	24000	Refund given (added into refund counter) for suiciding an account.
$G_{suicide}$	5000	Amount of gas to pay for a SUICIDE operation.
G_{create}	32000	Paid for a CREATE operation.
$G_{codedeposit}$	200	Paid per byte for a CREATE operation to succeed in placing code into state.
G_{call}	700	Paid for a CALL operation.
$G_{callvalue}$	9000	Paid for a non-zero value transfer as part of the CALL operation.
$G_{callstipend}$	2300	A stipend for the called contract subtracted from $G_{callvalue}$ for a non-zero value transfer.
$G_{newaccount}$	25000	Paid for a CALL or SUICIDE operation which creates an account.
G_{exp}	10	Partial payment for an EXP operation.
$G_{expbyte}$	10	Partial payment when multiplied by $\lceil \log_{256}(exponent) \rceil$ for the EXP operation.
G_{memory}	3	Paid for every additional word when expanding memory.
$G_{txcreate}$	32000	Paid by all contract-creating transactions after the *Homestead transition*.
$G_{txdatazero}$	4	Paid for every zero byte of data or code for a transaction.
$G_{txdatanonzero}$	68	Paid for every non-zero byte of data or code for a transaction.
$G_{transaction}$	21000	Paid for every transaction.
G_{log}	375	Partial payment for a LOG operation.
$G_{logdata}$	8	Paid for each byte in a LOG operation's data.
$G_{logtopic}$	375	Paid for each topic of a LOG operation.
G_{sha3}	30	Paid for each SHA3 operation.
$G_{sha3word}$	6	Paid for each word (rounded up) for input data to a SHA3 operation.
G_{copy}	3	Partial payment for *COPY operations, multiplied by words copied, rounded up.
$G_{blockhash}$	20	Payment for BLOCKHASH operation.

Fig. 5 - Ethereum opcode gas fees from: (Wood 25)

When miners use their computational resources, they receive a fee based on the amount of gas that was required to be used for a smart contract. The miners receive a payment based on the speed at which contracts need to be executed as well as the "going-rate" for gas at the time. The price of the gas itself is set by the sender of a message, so the price that they set will dictate the priority of their smart contract for a miner (thus the speed of its execution) (Rosic). Gas prices are generally measured in either billions of "Wei" or "Gwei", which is 1e-9 Ether.



Denominations of Ether

Unit Name	Wei Value	Number of Wei
Wei (wei)	1 wei	1
Kwei (babbage)	1e3 wei	1,000
Mwei (lovelace)	1e6 wei	1,000,000
Gwei (shannon)	1e9 wei	1,000,000,000
Twei (szabo)	1e12 wei	1,000,000,000,000
Pwei (finney)	1e15 wei	1,000,000,000,000,000
Ether (buterin)	1e18 wei	1,000,000,000,000,000,000

Fig. 6 - Denominations of Ether from: (Tardi, "Gwei Definition")

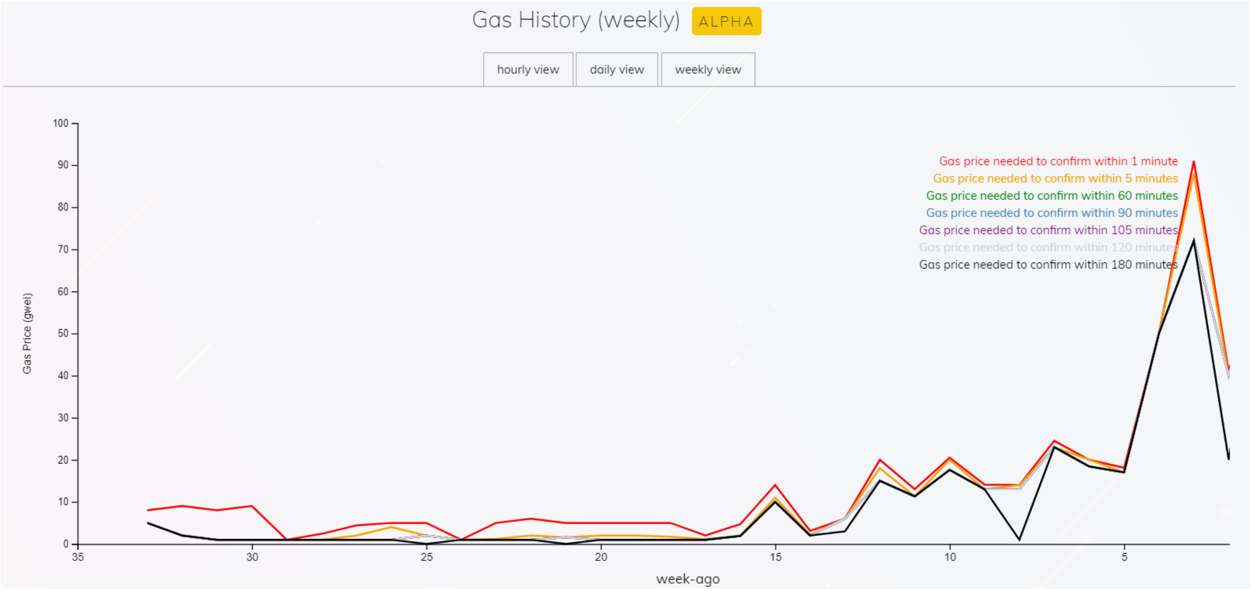


Fig. 7 - Historical gas price in Gwei from: ("Live Ethereum (ETH) Gas History")

At the time of writing, gas is currently priced at an average of 68.36 Gwei ("Ethereum Average Gas Price").

While Ether itself is one of the most valuable tokens in the cryptocurrency market and is often traded on exchange markets, the Ethereum platform has allowed for many other altcoins to exist and proliferate. Firstly, much like Bitcoin, there have been several hard forks in Ethereum that have brought about different cryptocurrencies existing in sync.

The most notable example is Ethereum Classic, which forked off from the primary Ethereum blockchain due to a dispute over whether the Ethereum developers should return over $50 million dollars' worth of stolen Ether to its owners. Ethereum Classic is the original, unaltered blockchain while what is generally simply referred to as "Ethereum" is the blockchain with the stolen ether transaction reversed (Vigna).

In addition, creating new cryptocurrencies that run on the Ethereum blockchain is quite simple. To date, over 345,844 tokens are hosted on the Ethereum platform ("Token Tracker"), including many coins that are extremely popular such as Tether, discussed above. These tokens are known as ERC-20 tokens, which are tokens that follow certain rules pre-defined by the Ethereum developers and can exist alongside Ether on the Ethereum platform. A new type of token, known as ERC-223 is currently being developed, but is not yet available (William).

4. Other Miscellaneous Blockchain Concepts

Proof of Stake

As blockchain technology continues to expand and proliferate, there will inevitably be innovation. Concepts that at one time seemed revolutionary will give way to newer ideas. One such concept, which is surprising because it is one of the major backbones that made Bitcoin possible, is the proof-of-work consensus algorithm. While it prevents double-spending attacks for the most part, it does suffer from some flaws that newer consensus algorithms are attempting to improve upon. For example, blockchains with proof-of-work consensus algorithms encourage mining pools (such as Bitmain discussed earlier) because they can pool their processing power together to improve the chances that they mine a block and split the profit. Also, newer coins are susceptible to 51% attacks, wherein malicious users can incorrectly verify transactions that are incorrect (such as double spending). Finally, proof-of-work has the potential to have delays in transaction verification when nodes are down (Nguyen et al.).

One consensus algorithm that has recently emerged as a viable successor to proof-of-work is known as proof-of-stake. In proof-of-stake, instead of computing power being the main determinant in a user's likelihood to create a new block via finding the correct nonce, a user will have a higher chance to create a new block based on their stake in the cryptocurrency. This "stake" is based on how many tokens in a particular cryptocurrency an account holds. In general, proof-of-stake protocols are based on an algorithm called "find-the-satoshi" wherein every base fraction of a token is indexed. A pseudorandom index will be chosen, and the owner of the token at that index will be chosen as the next individual to create a block. If you have more coins, you have a larger chance to be chosen (thus, you have a larger stake). (Nguyen et al.) Block creators are incentivized with monetary rewards, similar to how the miner that solved the nonce first would receive a reward for doing so.

Proof-of-stake based blockchains already exist. Peercoin is the name of the first token to implement this feature, though it was more of a hybrid proof-of-work and proof-of-stake system. However, there are several protocols, each with applications that use them, that utilize proof-of-stake. These include the Ouroboros, Chain-of-Activity, Algorand, Casper, and Tendermint protocols. Casper is a mixed proof-of-work and proof-of-stake consensus algorithm that is being adopted by Ethereum, so there are clearly big names in the blockchain industry adopting this technology.

There are several benefits that make proof-of-stake systems worth investigation. Firstly, they do not require users to buy any special hardware, because increased processing power no longer gives users an advantage. This is especially important, as blockchain mining is responsible for an estimated 0.2% of the world's energy consumption. While not a tremendous proportion, newer tokens and increased profitability will further exacerbate climate change (Parkhouse) so any attempts to reduce this impact should be considered. It also takes away some incentive to create mining pools, again because combining computing power will not offer any advantage. Finally, proof-of-stake allows for faster transaction speeds than does proof-of-work which is important for any blockchain that wishes to function as a currency rather than a store of value.

Blockchain Oracles

Blockchains cannot, on their own, access information that exists outside of the blockchain itself. Outside information, however, may be critical when it comes to smart contracts which may require that some outside condition be met before they can execute or continue with execution. For example, a smart contract that transfers Bitcoin may delay running until the ratio of prices between Bitcoins and dollars reaches a pre-specified level, at which point the contract will execute. The blockchain itself cannot determine the price of a U.S. dollar, so it looks to a "Blockchain Oracle" to receive that information. Blockchain Oracles are simply services that provide outside information to (or from) the blockchain itself which can be used by scripts and smart contracts (Mou).

Blockchain oracles come in several variants that each provide different functionality. The oracle can be software based which retrieves data from other sources and provides it to the blockchain. It can also be hardware based, meaning that it translates information and events that occur in the physical world into data usable by a blockchain. Similar to cryptocurrency exchanges, it can be either centralized or decentralized. Finally, even humans can technically be oracles by providing outside information known to them to a smart contract. How trustworthy a smart contract is depends on the nature of the oracle and its implementation (Mou).

Byzantine Fault Tolerant Consensus Algorithms

A term that one will come across often when researching blockchain technology is “Byzantine Fault Tolerance”. This concept is named after a thought experiment proposed in a paper by Leslie Lamport, Robert Shodtak, and Marshall Please titled “The Byzantine Generals Problem”. The thought experiment is as follows:

> “...imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger. After observing the enemy, they must decide upon a common plan of action. However, some of the generals may be traitors, trying to prevent the loyal generals from reaching agreement. The generals must have an algorithm to guarantee that
>
> A. All loyal generals decide upon the same plan of action. The loyal generals will all do what the algorithm says they should, but the traitors may do anything they wish. The algorithm must guarantee condition A regardless of what the traitors do. The loyal generals should not only reach agreement, but should agree upon a reasonable plan. We therefore also want to insure that

> B. A small number of traitors cannot cause the loyal generals to adopt a bad plan." (Lamport et al. 206, 207)

As it applies to blockchain technology, this allegory can describe how nodes in a blockchain system can continue to be trusted and function even if some nodes may have malicious intentions. In other words, we need a consensus method, such as proof-of-work, in order for a blockchain to achieve Byzantine Fault Tolerance. Bitcoin has, for example, a theoretical 50% Byzantine fault tolerance (Patel) because its proof-of-work consensus algorithm requires that a majority of nodes need to be malicious in order to control of and add false information to the Bitcoin blockchain.

Tendermint

Tendermint is a consensus algorithm that solves the Byzantine Generals Problem with a proof-of-stake based algorithm with a 33.3% byzantine fault tolerance (Kwon). There are two main components that make up Tendermint: Tendermint Core and Cosmos (discussed in Section 5.2). The difference between Tendermint Core and other Proof-of-Stake consensus algorithms is that Tendermint is intended to be used as a framework and consensus algorithm for which blockchain-based applications can be created using any programming language. This is possible via the "Application Blockchain Interface" which is an interface that allows the separation of the peer-to-peer layers of a blockchain application from the consensus algorithm. Tendermint strives to be a modular blockchain framework instead of a monolithic one as is common in most blockchains so that application-level technology can be developed on top of Tendermint without developers having to worry about implementing a consensus algorithm ("What Is Tendermint"). This has broad implications for interoperability as will be discussed in the section regarding Cosmos below.

5. Cross-Chain Cryptocurrency Communication and Interoperability

5.1 Technical Background

Research into the field of communication between two blockchains has demonstrated that actual direct communication is not possible without a third party that can be trusted by users on both sides of an exchange (Zamyatin et al. 7). There are many schemes and solutions that attempt to take the place of this third party in the most safe, secure, and decentralized way possible. These generally fall into one of three categories which describe the basic way that the scheme will work. They include notary schemes, relays, and hash-locking schemes.

Notary Schemes

Notary schemes involve the use of a trusted third party that is used to ensure that events that are being claimed to have happened on one chain truly occurred. This requires the trusted third party to make claims to one chain that events on another chain did in fact take place (Buterin, “Chain Interoperability” 4). The notaries would have to come to some sort of agreement through a consensus protocol similar to the way mining a cryptocurrency works (Larsen) and would be held on a ledger operated by the notaries themselves (Koens and Poll 7). Notary schemes are noteworthy because they are the simplest cross-chain interoperability strategy that currently exists (Buterin, “Chain Interoperability” 4).

A common example of Notary schemes exists in the form of “federated pegged sidechains”. Sidechains are blockchains that exist that allow for some form of interoperability. They work by “locking” some amount of a cryptocurrency on one blockchain and then releasing an equivalent amount of a cryptocurrency on the sidechain that can then be spent. These sidechains can then be destroyed, and an equivalent amount of the original cryptocurrency will then be “unlocked” (“Sidechain”). Federated, meanwhile, refers to a group of nodes that controls some amount of cryptocurrency tokens that can only be accessed and transacted upon if the keys from everyone involved in the group are granted. Therefore, a federated pegged sidechain simply means that a group can freeze and create cryptocurrencies on an original chain and a sidechain. In practice, this is how the cryptocurrency Liquid created by Blockstream works (Nick et al. 1). Liquid coins are created when Bitcoin tokens are “frozen” and are pegged to that amount of Bitcoin which is controlled by the “Liquid Federation”.

Relays

Relays describe one blockchain being able to read the distributed ledger of another blockchain. This allows a blockchain to verify for itself whether an event or state of another blockchain exists and cuts out the trusted notary that is necessary in a notary scheme. The most prominent example of a real-world relay is BTCRelay, which is a smart contract on the Ethereum blockchain that can view the Bitcoin public ledger and monitor it for verified transactions (“FAQ — BTC Relay 1.0 Documentation”). This can allow for exchanges because a user of Ethereum could write a smart contract that sends Ether to another user after BTCRelay verifies that the second user has sent an equivalent amount of Bitcoin to the first user. Bitcoin, however, has no way of viewing the Ethereum ledger and therefore BTCRelay only works one way (and is known as a one-way relay) (Koens and Poll 5).

Relays work by one blockchain copying a miniature version of another blockchain ledger and extracting information from the other ledger by analyzing this miniature copy. Buterin, once again, summarizes the problem quite concisely:

> "it is impossible for a mechanism inside chain A to fully validate chain B and a mechanism inside chain B to fully validate chain A at the same time, for the same simple mathematical reason why two boxes cannot simultaneously contain each other: A would need to re-run the part of B that re-runs A, including the part of A that re-runs B, and so forth." (Buterin, "Chain Interoperability" 5)

There are, however, schemes that attempt to solve this inherent problem with creating two-way relays. One solution is to create a centralized blockchain known as a "relay chain" that tracks ledger information from multiple blockchains which can then interact with this relay chain instead of other chains directly. These relay chains, or "light clients" can be made even more useful by giving them power over the blockchains they monitor (Larsen). Cosmos and Polkadot are two interoperability schemes that attempt to set up two-way relays through the use of a relay chain.

Hash-Locking

The final interoperability strategy is known as hash-locking. Hash locking involves exchanging assets between two blockchains by "locking" assets within a smart contract that can only be unlocked if certain conditions have been met before a pre-specified time-period runs out. Lightning Network uses this scheme in order to allow cross-chain transfers of cryptocurrency. In general, the condition that has to be met by both parties is the revelation of a randomly generated "secret" or preimage that is hashed and stored (locked) in the hash-lock (Buterin, "Chain Interoperability" 11).

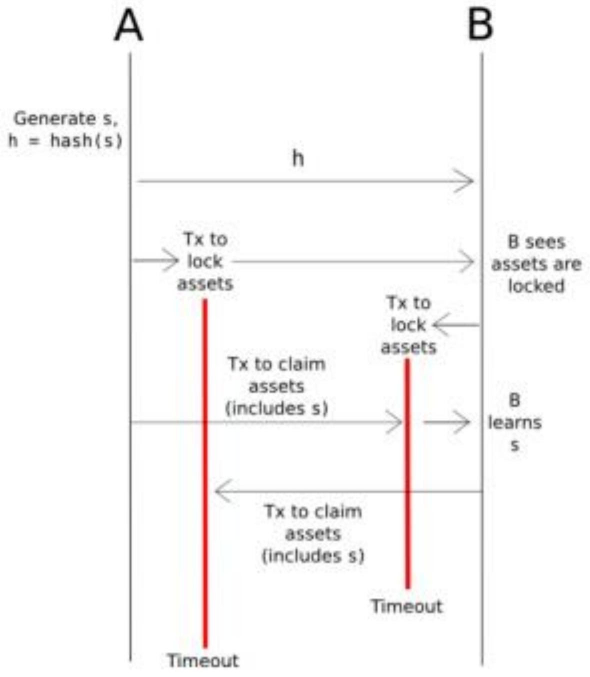


Fig. 8 - Execution of an HTLC from: (Buterin, "Chain Interoperability" 11)

The main function of hash-locking in the sphere of cross-chain communication involves combining hash-locks with timelocks within a contract to create what is known as a hashed timelock contract (HTLC). This will allow for atomic swaps (or Atomic cross-chain swaps)—a distributed, decentralized exchange method that utilize hash-locking and timelocks to enable cross-chain asset transfers that will either occur completely or will not occur and no party involved in the transaction will be worse off, thus achieving atomicity. These contracts can involve two or more parties though some modification will need to be made to accommodate swaps involving more than two parties. The idea for atomic swaps originated in a Bitcoin discussion forum in 2013 by a user known as TierNolan (TierNolan) but the first successful atomic swap actually occurred in 2017 and was brought about by the founder of Litecoin, Charlie Lee (Lee; "What Are Atomic Swaps?"). Early adopters of Atomic Swaps include the Komodo and Rubix (Fitzpatrick).

Atomic cross-chain swaps work by having both parties publish a hashed timelock (smart) contract that takes control of the assets that they wish to exchange between blockchains. If both parties reveal their secret within a specified time period, then the transaction will be executed. Otherwise, all assets will be refunded. The benefits of conducting a cross-chain swap include the decreased risk and lack of exchange fees brought about by the lack of a centralized entity controlling the assets being exchanged. In addition, a true atomic swap protocol will guarantee that:

- If all parties uphold their personal requirements as specified by the contract in the specific time period, then all swaps contained within the contract must and will take place
- If any party does not uphold their personal requirements, all parties will have their assets returned to them
- The atomic nature of the swap does not allow for any incentives for a party to not uphold their end of the contract (Herlihy 246).

5.2 Current Iterations and Examples of Cross-Chain Exchanges

There are many current efforts to introduce a widely-used system to allow for the interoperability and exchange of data, and even tokens, between cryptocurrencies operating on different blockchains. Most of these efforts are implemented via one of the schemes introduced in Section 5.1. This section will be a review of several current efforts that seek to allow such interoperability. It should be noted, however, that this list is far from exhaustive.

Interledger

Interledger is an attempt to enable interoperability between different currencies (including cryptocurrencies) that was originally developed by Ripple, the creator of the XRP token. However, in an effort to allow Interledger to exist without being controlled by a single entity, Ripple released control of Interledger and designated it as an open-source project. The current group overlooking the development of Interledger is the World Wide Web Consortium (W3C), which is the group that designates standards for the World Wide Web to allow universal compatibility.

Interledger works via the implementation of a protocol that can, through a network of “connectors”, view information on multiple public ledgers simultaneously. It uses this information to enable interoperability between the blockchains represented by these ledgers. Interledger has two primary modes of interoperability: “Atomic” and “Universal” modes (Frankenfield, “Interledger Protocol”), each of which is an example of a different interoperability scheme described above in Section 5.1. Atomic mode functions as a notary scheme, with a group of notaries that is selected by participants involved in a cross-chain operation (Thomas and Schwartz). The notaries will, in general, collect fees for being parties to the transaction. Universal mode, meanwhile, functions as a hashed timelock contract and uses Ripple’s cryptocurrency, XRP, to facilitate the transfers. This exchange relies also on packets that are sent through the connector network in the form of packets that include “prepare”, “fulfill”, and “reject” packets that correspond to the steps involved in setting up and executing an HTLC as described above (Schwartz and Pestritto).

Lightning Network

The lightning network began as an attempt to solve Bitcoin’s scalability problem, yet it has real potential for enabling interoperability for several reasons. The Lightning

Network works by creating a channel between a few transactors and which exists as a single node on the Bitcoin network. Instead of every individual transaction being broadcasted to the entire blockchain, the channel will record micropayments between the transactors. When the users are finished and close the channel, the final balance between the transactors will be broadcast as a single transaction that is made public on the blockchain. The micropayments within the channel are made trustless via HTLCs (Poon and Dryja 5).

While this system was not conceived of necessarily to facilitate interoperability between chains (in fact, it was designed for use specifically with Bitcoin), the technology does have implications for the existence of interoperability. Firstly, the Lightning protocol could be replicated on blockchains other than Bitcoin. In this case, there is potential for each Lightning network to transact with each other, then reporting the new balance of each coin to the respective blockchain (“What Is Lightning Network And How It Works”). The other, more indirect way, in which the Lightning Network facilitates interoperability is that some schemes rely on the blockchains involved in the exchange to independently verify that a transaction is legitimate before the exchange can be made. For example, the Bitcoin client lists transactions as unconfirmed until six blocks have been added to the chain after the block in which the transaction occurred (“Confirmation”). This decreases the likelihood that the block that contains the transaction information was not double-spent. However, with an average time of ten minutes between blocks, this means that Bitcoin transactions are not considered confirmed for at least an hour after the transaction has actually taken place. For schemes that rely on each blockchain involved in an exchange establishing trust, the lightning network can vastly accelerate the speed at which cross-chain transfers can occur.

Liquid

The Liquid Network—created by the company Blockstream—is another example of technology built to coexist and enhance Bitcoin and promises to allow for cross-chain exchanges. Particularly, Liquid is worth mentioning because it is an example of a federated-pegged sidechain as discussed in Section 5.1. Liquid works by running a blockchain in parallel to Bitcoin with tokens known as L-BTC (Bitcoin used in the Liquid network). Bitcoin (BTC) can be exchanged to L-BTC by sending actual Bitcoins to a trusted account operated by the Liquid network. This account will "lock" the Bitcoin and will "release" an equivalent amount of L-BTC on the sidechain to a user's associated account. The reverse scenario is utilized to exchange L-BTC for BTC (Nick et al. 5). Although Liquid was designed specifically to interoperate with the Bitcoin blockchain, it is possible for users to use Liquid as a mechanism to exchange different cryptocurrencies. This is done via creating "collateralized cryptocurrencies" that can also be held in trusted nodes on a blockchain and exchanged for L-BTC. In theory, this L-BTC could then be exchanged for a different cryptocurrency locked away on another chain. However, cryptocurrencies other than Bitcoin will not be natively compatible with the Liquid Network, so these exchanges will have to be organized by entities that exist outside Blockstream ("Technical Overview").

XCLAIM

XCLAIM, pronounced cross-claim, is an effort by Alexei Zamyatin, Dominik Harz, and others at the Imperial College London to produce an alternative to atomic cross-chain swaps (e.g., through the use of HTLCs). This is accomplished by defining "cryptocurrency-backed assets" which are simply any asset backed by a cryptocurrency and are trustless

(Alexei Zamyatin et al. 6). They can be swapped to other blockchains via chain relays. Zamyatin and Harz have formed a company together known as Interlay that works with blockchain networks to implement XCLAIM features within the networks themselves to assist in facilitating cross-chain communication.

Cosmos

Cosmos is a blockchain network architecture based on the Tendermint Byzantine Fault Tolerant consensus algorithm that allows for multiple blockchains to interoperate. Each blockchain in the Cosmos network is known as a “zone” and operates on the Cosmos Hub, which is itself a cryptocurrency with tokens called atoms. Tokens can be exchanged between blockchains hosted on this hub via an internal messaging protocol, with the hub itself keeping track of the state of each zone (Kwon and Buchman).

Cosmos achieves interoperability through the use of its Inter Blockchain Communication protocol, which is essentially a relay that allows chains operating on the Cosmos network to read data that exists on other blockchains. Cosmos makes it easy for new chains to interoperate as long as they follow this protocol. In addition, it is also possible for the Cosmos network to facilitate interoperability between blockchain within and without the Cosmos network through the use of a “privileged zone” acting as a bridge. This “bridge-zone” runs a node on the blockchain outside the Cosmos network as well as the Tendermint-based blockchain.

Polkadot

Polkadot, founded by Ethereum cofounder Dr. Gavin Wood, is similar to Cosmos in that it is intended to be a network of chains that are interoperable because they are implemented on the same network. The Polkadot network is divided into three pieces: the main relay chain, parachains, and bridges. The Polkadot blockchain itself is a “relay-chain” that hosts data structures including but not limited to blockchains that run in parallel to each other (Redman, “A Deep Dive Into Polkadot”). Polkadot refers to these parallel data structures as “parachains” (Wood, *Polkdadot: Vision for a Heterogenous Multi-Chain Framework*)(. This is accomplished via a technique known as “heterogeneous sharding”. Sharding in cryptocurrencies involves breaking up a total set of transactions and dividing those transactions amongst committees that handle only a portion of the total set in parallel (Wang et al. 44). Each parachain in the Polkadot network is a shard. Bridges, meanwhile, are the connection between parachains that allow them to interoperate. These bridges are not all implemented in exactly the same way. For example, the Bitcoin bridge includes XCLAIM as a primary component in its implementation (“BTC Parachain at a Glance”). The Ethereum bridge, however, would be implemented via a smart contract (Wood, “Polkadot, Substrate and Ethereum”). In theory, any blockchain can join the Polkadot network and transfer any type of data across the network to other chains via bridges.

Komodo

Komodo claims to be an implementation of what it calls the fourth era of blockchain technology (with Bitcoin being the start of the first era, Ethereum and smart contract platforms representing the second era, and Cosmos and Polkadot representing the third era). The central aim of Komodo is to have it be a “composable” solution that provides a system that allows for the creation of independent blockchains, rather than side chains that exist parallel to a primary chain (“Technology Overview”). Komodo allows for turing-complete smart chains that, while interoperable within the ecosystem, do not rely on the main Komodo chain to be functional.

6. Arbitrage

6.1 Introduction

This discussion on blockchain technology and interoperability will culminate with our contribution to the discussion. Specifically, we will investigate the possibility of engaging in triangular arbitrage using publicly available cryptocurrency exchange-rates and prices to determine how often triangular arbitrage is possible. We will test the feasibility of triangular arbitrage given at least three currencies, with a minimum of two cryptocurrencies using historical cryptocurrency price-data. Triangular arbitrage, described in more depth below, can be described as a riskless exchange of three or more currencies that guarantees some amount of profit. Generally, this is possible due to market inefficiencies that affect exchange rates in such a way as to make them disproportionate. In typical currencies, these inefficiencies will only exist briefly. Our work will look through historical prices to determine how often this type of arbitrage would have been possible in the past (Chen).

6.2 Related Work

There has been much research done on the subject of arbitrage within cryptocurrency markets. Makarov and Schoar in their article "Trading and arbitrage in cryptocurrency markets" use historical exchange data to calculate the arbitrage index across cryptocurrency exchanges. They largely focus on arbitrage derived from purchasing a single cryptocurrency (i.e., Bitcoin) with a fiat currency on one market and selling that same cryptocurrency back on a new market with a different exchange rate. They take special note of selling Bitcoin on exchanges located in different regions and demonstrate that moving across regions increases the potential profit margins of arbitrage opportunities.

They also compare arbitrage spreads between Bitcoin and Ethereum and conclude that “arbitrage opportunities are much less pronounced and persistent between different cryptocurrency markets than between cryptocurrency and fiat currency markets” (Makarov and Schoar 315). However, they did not compare coins besides Bitcoin and Ethereum, and their data only covered a four-month window of time.

Another form of arbitrage that is unique to the cryptocurrency world is described by Adam Hayes whereby Bitcoin miners may mine a proof-of-work based altcoin and exchange that coin directly for Bitcoin rather than mining Bitcoin itself (Hayes, *The Decision to Produce Altcoins*). This would occur in instances where the miners calculate that there is a likelihood that due to the exchange rate of Bitcoin and the altcoin that the miners would, overall, receive more Bitcoin than they would by mining it directly. Hayes shows, however, that this avenue is generally unprofitable and unpredictable.

To our knowledge, there has been little research on the potential for triangular arbitrage. This will be of particular importance should one of the cryptocurrency exchange schemes detailed in Section 5.2 gain prominence over the others. In particular, we specifically are interested in arbitrage in situations where cryptocurrencies are purchased in one market, exchanged for another cryptocurrency, and finally sold in a different market (see Figure 9 below). We do not attempt to determine which exchange scheme is best suited for this task, though we acknowledge that a scheme that charges an arbitrary flat fee for the exchange will be the most profitable when trading in large quantities.

6.3 Methodology

To envision the type of arbitrage that we are attempting to measure, consider an arbitrageur, Jane. Jane has assets in the amounts of $10,000, 3 Bitcoin (BTC), and 40 Ether

(ETH). How can she use these assets at a given time to guarantee a profit? We will consider two hypothetical markets at an arbitrary time as an example. We will compare two exchanges, Exchange A and Exchange B.

At a particular time, Exchange A is offering Ether at $1\frac{ETH}{\$248.26}$ while Exchange B is offering Bitcoin at $1\frac{BTC}{\$3956.92}$. Both Exchange A and Exchange B also offer an exchange between Bitcoin and Ether, at $0.07235\frac{BTC}{ETH}$ and $0.0722\frac{BTC}{ETH}$ respectively. In addition, we will imagine that we can use a third-party exchange enabled by an interoperability scheme as discussed in Section 5.2 which offers a market price, ideally for a fixed fee. As long as the fee is not calculated as a proportion of the amount exchanged, the actual amount of this fee will not affect the ability to arbitrage these exchange rates given that a user chooses to move a large enough sum.

Jane, seeing an opportunity for arbitrage, spends her \$10,000 on Ether from Exchange A. Given that Exchange A charges a 0.1% fee on exchanges, she would have collected $(\$10{,}000 * 0.999) * \left(\frac{1\,ETH}{\$284.26}\right) = 35.14388\,ETH$

At the same time, Jane will exchange an equivalent amount of Ether for Bitcoin on the pseudo exchange-platform representing a cross-chain exchange via one of the schemes above. For simplicity, we will assume that the exchange scheme will charge a rate that is the average of the going rate between the different exchanges, in this case $0.072275\frac{BTC}{ETH}$. Exchanging her 35.14388 ETH for BTC will increase the amount of Bitcoin that she owns by 2.54002 BTC.

The final move that Jane will make will be to exchange an equivalent amount of Bitcoin to the amount she received in Exchange A simultaneously in Exchange B for dollars. Exchange B charges a higher fee at 0.25%, so she will net $(2.54002\ BTC + 0.9975) * \left(\frac{\$3956.92}{BTC}\right) = \$10{,}045.81$. These three exchanges, done simultaneously, net Jane a guaranteed profit of $45.81 through her arbitrage efforts while her cryptocurrency assets remain the same. Figure 9 is a graphical depiction of the concurrent transactions in which Jane will engage.

Exchange	Rate: ETH/BTC (Direct)	Rate: BTC/USD	Rate: ETH/USD
Exchange A	0.07235	3964.92	284.26
Exchange B	0.0722	3956.23	285.79

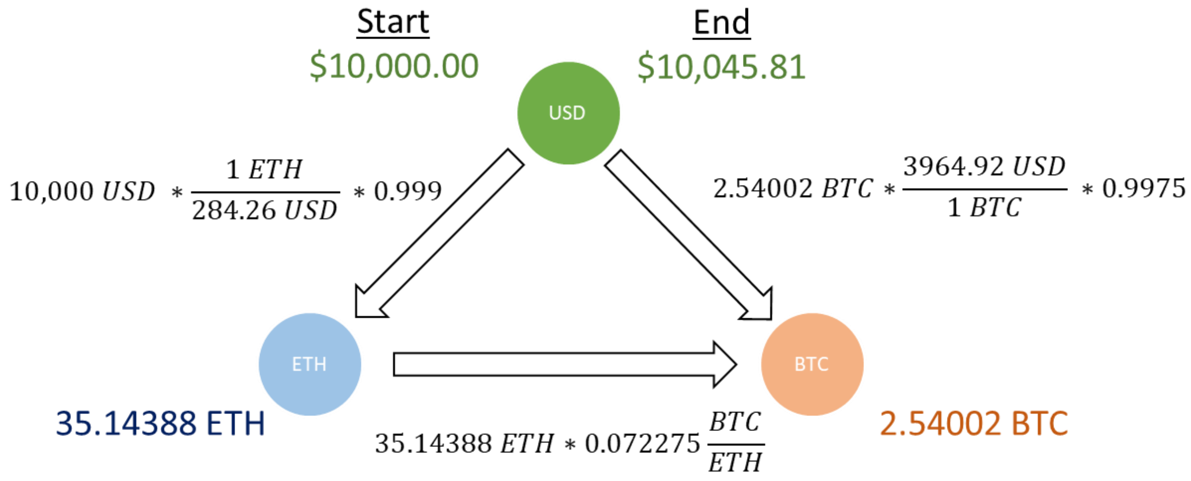

Start
$10,000.00
End
$10,045.81
USD
$10{,}000\ USD * \frac{1\ ETH}{284.26\ USD} * 0.999$
$2.54002\ BTC * \frac{3964.92\ USD}{1\ BTC} * 0.9975$
ETH
BTC
35.14388 ETH
$35.14388\ ETH * 0.072275 \frac{BTC}{ETH}$
2.54002 BTC

Fig. 9 - Triangular Arbitrage Example using Historical Data

It should be noted that, in order for Jane to earn this profit, she must commit to three transfers simultaneously and immediately. It should be noted that cryptocurrency prices can have relatively large fluctuations even within the span of just an hour which would also affect the feasibility of the arbitrage effort if all exchanges were not undertaken simultaneously. Furthermore, Jane must already have had in her possession an amount greater than or equal to each currency that she was exchanging prior to beginning these transactions. Given this limitation, arbitrage conducted in this manner may only be reasonably accomplished by established traders or firms rather than individuals. However, the example shows that arbitrage via direct cryptocurrency exchanges is theoretically possible and increases the appeal for further research on cross-chain cryptocurrency interoperability and exchange schemes.

While the situation above is a hypothetical scenario, there are tens of thousands of hourly data points available on many of the top cryptocurrency schemes which offers a unique opportunity for us to determine how often triangular arbitrage is viable in the real world. The aim of our work in this section is to continue this analysis on many data points in an effort to draw conclusions about the prevalence of arbitrage opportunities.

In order to accomplish this, we will design a program in Java that will read the data available in the .CSV files available on several exchanges located on CryptoDataDownload.com. The data is organized based on Unix Epoch Time (Unix time), so we will compare data whenever it is available for at least two coins at the same Unix time. Our simulation will also account for arbitrage that is available through trading between an arbitrary number of exchanges greater than three. This experiment will evaluate the prevalence of arbitrage opportunities given markets that exist currently, though we will discuss the implications of our results given the possibility of interoperability schemes becoming popular in the future.

6.3.1 Experiment Design

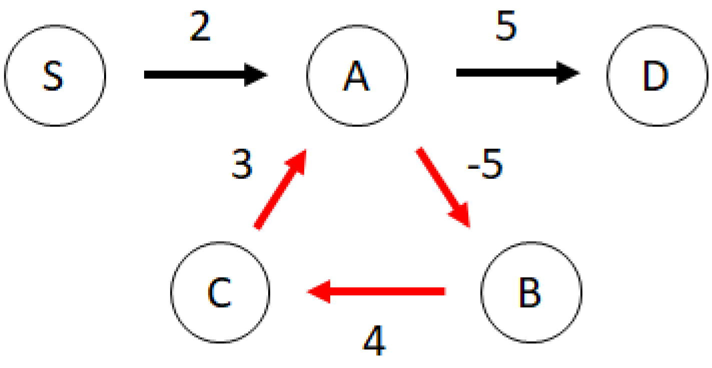
In order to create a model of cryptocurrency exchanges that will allow us to test for the presence of arbitrage, we will envision each coin being exchanged on a market as a node within a directed graph. The weight between each exchange will be based upon the exchange rate of a particular pair of coins as well as any fees that would be associated with that exchange. We can detect arbitrage in this situation by searching for a cycle within this graph with a weight production greater than zero. If we then take the logarithm of these weights, we can instead find a cycle where the *summation* of its weight is larger than zero to detect arbitrage rather than its production. Such a cycle with the sum its weights being greater than zero is known as a positive weight cycle. If we negate these weights in the positive weight cycle, however, we can search for a cycle where the weights in the cycle have a sum less than zero (a negative weight cycle). The Bellman-Ford algorithm is a shortest-path algorithm that is compatible with negative weights on the paths within a graph and can be used to detect negative weight cycles. Therefore, we can also use the Bellman-Ford algorithm to detect instances where arbitrage is possible.

To summarize, our experiment will involve creating numerous graphs using exchange rates that existed at particular moments in time as weights. We will then take the negative logarithm of those weights and apply the Bellman-Ford algorithm to determine whether we can detect negative weight cycles. If we do detect a negative weight cycle, then we can confirm that arbitrage was possible in that moment. We are interested in determining how often we can detect such an arbitrage opportunity, and with what factors influenced the existence of that opportunity.

6.3.1.1 Design Description

In this subsection, we will attempt to explain in simpler terms why we can detect arbitrage in the fashion described above. A set of paths through nodes in a graph can exist as a cycle in which a trail exists where the only repeated vertices are the first and last vertex (i.e., a loop). If the weights of the paths in the cycles are such that they sum to a number larger than zero, then you can travel through the cycle multiple times in order to continually increase the total weight of the path traveled. This is known as a positive weight cycle.[5]

The weights of graphs in a currency exchange market can be represented as the exchange rates between the currencies in that market. If a positive weight cycle exists in such a graph, then that cycle is indicative of arbitrage. For example, one could imagine Jane completing her arbitrage scenario above five times instead of once, which would be represented in the graph by traveling through the cycle five times. Figures 10, 11 and 12 below demonstrate this idea visually. Notice in Figure 10 that while a direct path from node S to node D has a weight of 7 directly, the cycle indicated by red arrows has a weight of 2. This means that moving along the path from S and going through the cycle indicated by red arrows once before arriving at node D will increase the total weight of the path from 7 to 9. A path can travel through the cycle unlimited times to increase the total weight of the path toward infinity. This is an example of a *positive* weight cycle.

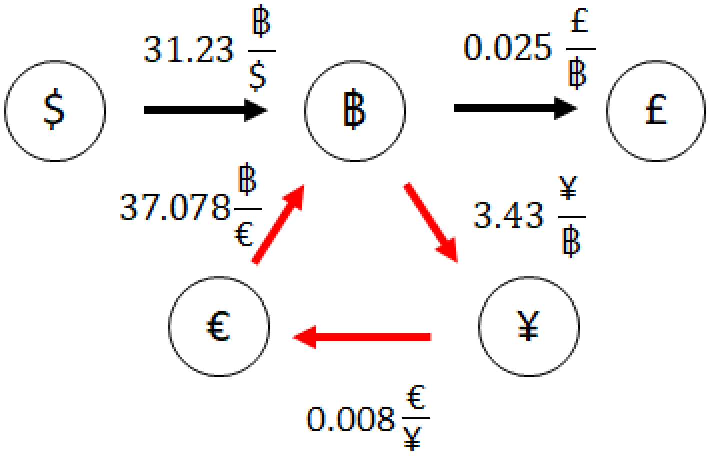


$$d(S,A) = d(S,B) = d(S,C) = d(s,D) = \infty$$

[5] While for demonstration purposes we will visualize positive weight cycles, it is important to note that positive weight cycles are difficult to detect. For this reason, in our experiment, we will be negating the weights in the graphs and using the Bellman-Ford algorithm to detect negative weight cycles. This will allow us to locate the same paths in the cycle that would otherwise have been a positive weight cycle.

Fig. 10 - Positive Weight Cycle

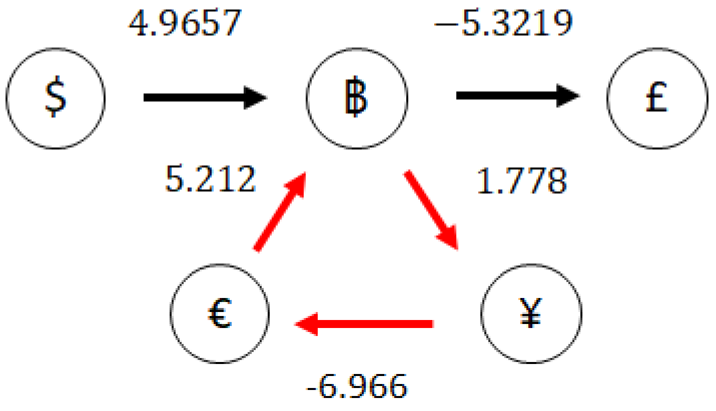
Now, we consider how the example of positive weight cycles can affect exchange markets. For simplicity, lets first consider fiat currency exchanges. In Figure 11, it is clear that one can exchange U.S. Dollars for Thai Baht, and Thai Baht for pounds sterling to receive an exchange of about 0.78 Pounds/Dollar. However, once again we find a positive weight cycle in the form of exchange rates. This cycle creates an opportunity for triangular arbitrage similar to the example listed above for Jane. For each 1 baht that we pass through the positive weight cycle, we increase the total weight by 1.038 Baht. This, in turn, will allow us to receive a higher exchange rate in pounds per dollar each time we move through the cycle. Or, if we were able to exchange baht back into dollars for an equivalent exchange rate, we would see a guaranteed profit that would increase every time through the cycle. In the real world, market forces will eventually eliminate this opportunity as the exchange rates fluctuate due to supply and demand forces. This is why the currency exchanges in our model must occur simultaneously to be viable.



$$1\text{฿} * 3.43\frac{\text{¥}}{\text{฿}} * .008 * \frac{\text{€}}{\text{¥}} * 37.82\frac{\text{฿}}{\text{€}} = 1.038\text{฿}$$

Fig. 11 - Fiat Currency Arbitrage Example

Figure 12 below represents the same graph as Figure 11 above but uses the logarithm of each weight instead of the exchange rate itself. As you can see from the graph, the exchange of Baht for Yen, Yen for Euros, and Euros sums to an amount greater than zero, so we are able to locate the exact same path. If the exchange rates did not adjust, you can trade through this weight cycle infinite times to receive a guaranteed profit after each loop. Our experiment will be designed to detect such cycles and to measure how often they exist using historical data points.



$$1.778 - 6.966 + 5.212 = 0.024$$

Fig. 12 - Arbitrage with Logarithmic Weights

6.3.2 Simulation

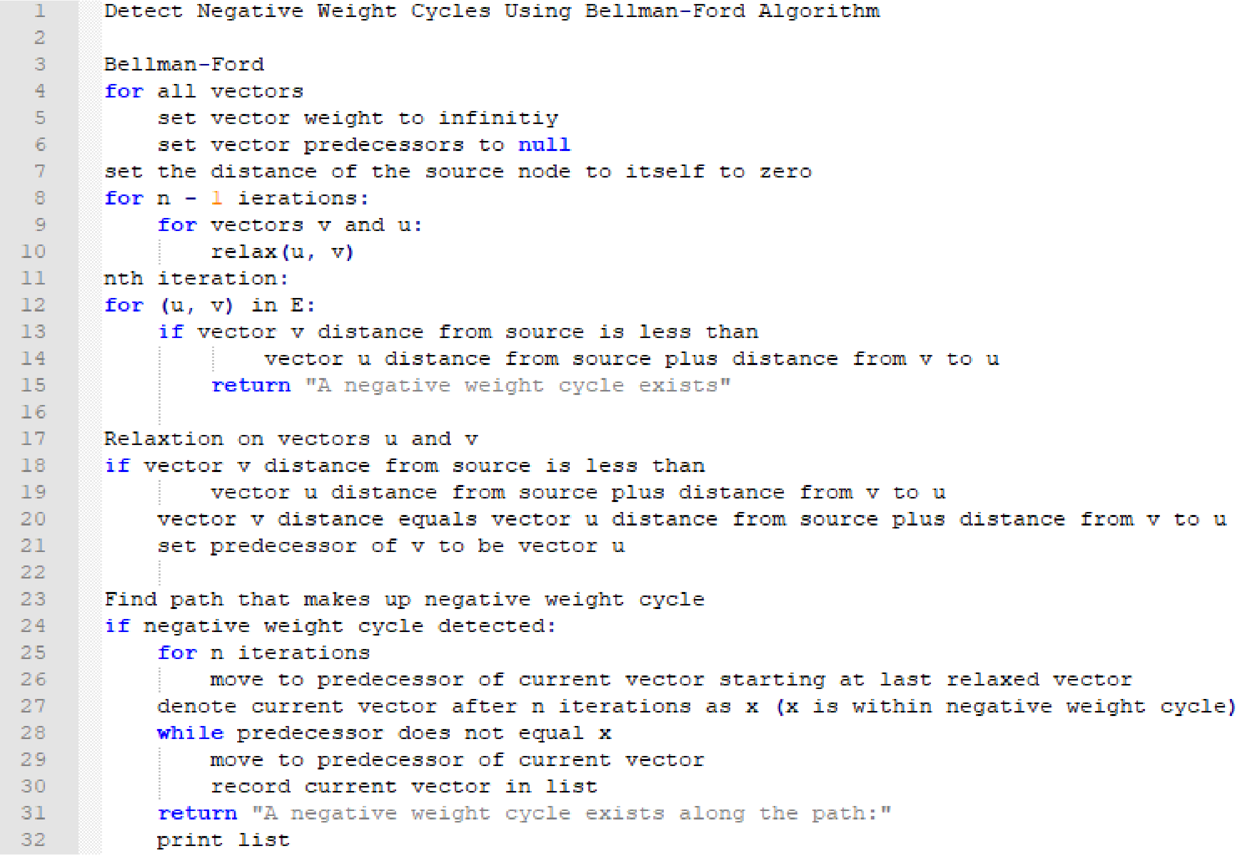
Because a negative weight cycle within a graph can be used to check for a potential arbitrage opportunity, our simulation will attempt to model the market at a given time as a graph. Each market will exist as a node on the graph, and the weight of each edge will be the exchange rate combined with the fee for that exchange. In order to locate negative weight cycles in these graphs, we will need to create a program that implements the

Bellman-Ford algorithm to detect negative weight cycles in graphs that we create using publicly available data.

The Bellman-Ford algorithm calculates the shortest path by relaxing the edges of all vertices that have been encountered in each iteration. Relaxing an edge can be understood as the operation where we update the weight of an edge between two vertices when we find a shorter path. For example, consider an instance where the weight of the edge after one iteration from Vertex A to Vertex B is found to be equal to 4. After subsequent iterations, however, we find that the path from Vertex A to Vertex C has weight 1 while the path from Vertex C to Vertex B has weight 2. We can now see that a path from Vertex A to Vertex B through Vertex C only has a total weight of 3. Relaxation, in this case, would be updating the weight of the Path from A to B to equal 3, since that is the shortest distance between the two vertices.

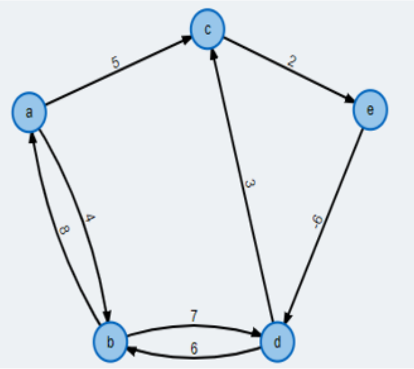
With |V| (which we will denote as *n*) vertices and |E| (which we will denote as *m*) edges, the Bellman-Ford algorithm has a time complexity of O(*n*•*m*) and all edges should be completely relaxed after *n*-1 iterations of the algorithm if there are no negative weight cycles. Relaxing of any edges, therefore, on then^{th}iteration indicates the presence of a negative weight cycle somewhere within the graph.

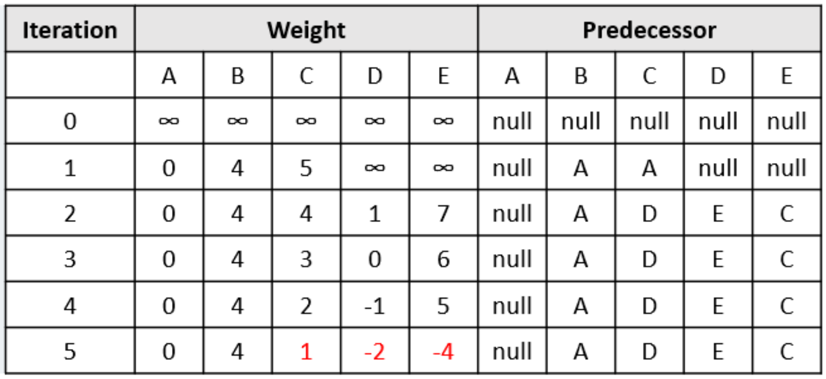
We can find the negative weight cycle by beginning at the vertex whose connected edge was relaxed on iteration *n*, which we will call vertex *r*. Because *r* relaxed, it follows that *r* either lies within, or else must be reachable from, the negative weight cycle. Thus, if we pass through the predecessor of each vertex, starting at *r, n* times, we will eventually come to a vertex, *x*, that is guaranteed to be within the path of the negative weight cycle ("Finding a Negative Cycle in the Graph"). At this point, if we continue moving through the predecessors, beginning at *x* until we arrive back at *x*, then we will have discovered the nodes that make up the negative weight cycle. The nodes within this cycle constitute the coins on a specific market and the weights refers to exchange rates between those markets that makes arbitrage possible in this scenario.



```
Detect Negative Weight Cycles Using Bellman-Ford Algorithm

Bellman-Ford
for all vectors
    set vector weight to infinitiy
    set vector predecessors to null
set the distance of the source node to itself to zero
for n - 1 ierations:
    for vectors v and u:
        relax(u, v)
nth iteration:
for (u, v) in E:
    if vector v distance from source is less than
            vector u distance from source plus distance from v to u
        return "A negative weight cycle exists"

Relaxtion on vectors u and v
if vector v distance from source is less than
        vector u distance from source plus distance from v to u
    vector v distance equals vector u distance from source plus distance from v to u
    set predecessor of v to be vector u

Find path that makes up negative weight cycle
if negative weight cycle detected:
    for n iterations
        move to predecessor of current vector starting at last relaxed vector
    denote current vector after n iterations as x (x is within negative weight cycle)
    while predecessor does not equal x
        move to predecessor of current vector
        record current vector in list
    return "A negative weight cycle exists along the path:"
    print list
```

Fig. 13 - Bellman-Ford Algorithm for Finding Negative Weight Cycles Pseudo-Code





Iteration	Weight					Predecessor				
	A	B	C	D	E	A	B	C	D	E
0	∞	∞	∞	∞	∞	null	null	null	null	null
1	0	4	5	∞	∞	null	A	A	null	null
2	0	4	4	1	7	null	A	D	E	C
3	0	4	3	0	6	null	A	D	E	C
4	0	4	2	-1	5	null	A	D	E	C
5	0	4	1	-2	-4	null	A	D	E	C

Caption: In this example, there are 5 nodes (meaning that *n* = 5 in this example). According to the algorithm, if there was no negative weight cycle, then we would stop seeing any relaxation happening after 4, or (*n* - 1), iterations. Because the distance from the source to nodes, C, D, and E occurred in iteration 5, we are guaranteed to have a negative weight cycle in our graph.

Fig. 14 - Illustration of Bellman-Ford Algorithm

The graph and table in Figure 14 provide a simple example of how the above algorithm will work. Consider Vertex A to be the source node when we run the Bellman-Ford algorithm (note that which node we designate as the source is arbitrary). Each iteration in the table represents one iteration (*i*) of the Bellman-Ford algorithm. The weight at each iteration represents the smallest weight of any path of at most *i* edges given the current weights of each vertex.

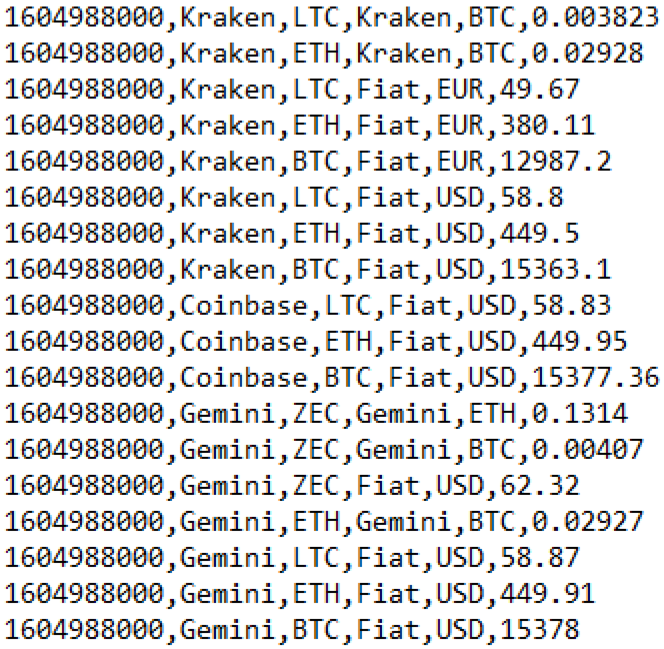
Because there are five vertices, we should have found the shortest distances between Vertex A and any other node by the fourth iteration. However, notice the red numbers on the fifth iteration, indicating that at least one Vertex was relaxed (C, D, and E). This is our indication that a negative weight path exists.

Our algorithm would then choose one of the vertices whose weight changed. We will then move to the predecessor of the selected vertex *n* times. In our case, we get C → D (1) → E (2) → C (3) → D (4) → E (5). Now, we know that E exists within the negative weight cycle. If we continue to move through each vertex's predecessor until we reach Vertex E again and record each vertex that we travel through, we will have a list that details vertices and the order of the negative weight path. In the case of our simulation, these vertices and paths will tell us which exchange and which specific transfers would allow us to reach arbitrage.

We will run our simulation over every hour beginning at Unix time 1498906800, July 1, 2017 at 11am UTC until the present. We will focus on three cryptocurrency exchanges markets: Gemini, Coinbase, and Kraken. We will choose a fee structure that is based on the amount that charged for the largest available transfers given the taker price. In the case of Coinbase, which has different fees based on location, we chose the fee for the U.S. as these exchanges are all based in either San Francisco or New York. The fee structures that our experiment is based on is as follows:

- Gemini exchanges will incur a 1.99% fee (“Web Exchange Fee Schedule”)
- Coinbase Exchanges will incur a 1.49% fee (“Coinbase Pricing and Fees Disclosures”)
- Exchanges on Kraken will incur a 0.1% fee (“Fee Schedules”)

The nodes that represent these cryptocurrency markets will store data that will be valuable to us as we examine our results. For example, the nodes will tell us which markets allow for arbitrage, and which coins were used as part of the arbitrage. We will collect and aggregate this data in order to make observations about the market as a whole over time. Our intention is that the output of the simulation will show how often since July 1, 2017 triangular arbitrage was available as a proportion of every graph constructed. An example of the raw data used for a single hour (at Unix time 1604988000) is shown below in Figure 15.



```
1604988000,Kraken,LTC,Kraken,BTC,0.003823
1604988000,Kraken,ETH,Kraken,BTC,0.02928
1604988000,Kraken,LTC,Fiat,EUR,49.67
1604988000,Kraken,ETH,Fiat,EUR,380.11
1604988000,Kraken,BTC,Fiat,EUR,12987.2
1604988000,Kraken,LTC,Fiat,USD,58.8
1604988000,Kraken,ETH,Fiat,USD,449.5
1604988000,Kraken,BTC,Fiat,USD,15363.1
1604988000,Coinbase,LTC,Fiat,USD,58.83
1604988000,Coinbase,ETH,Fiat,USD,449.95
1604988000,Coinbase,BTC,Fiat,USD,15377.36
1604988000,Gemini,ZEC,Gemini,ETH,0.1314
1604988000,Gemini,ZEC,Gemini,BTC,0.00407
1604988000,Gemini,ZEC,Fiat,USD,62.32
1604988000,Gemini,ETH,Gemini,BTC,0.02927
1604988000,Gemini,LTC,Fiat,USD,58.87
1604988000,Gemini,ETH,Fiat,USD,449.91
1604988000,Gemini,BTC,Fiat,USD,15378
```

Fig. 15 - Raw Sample Data for Unix time 1604988000 (November 10, 2020 at 6am GMT)

CSV files are simple text files, with character arrays being delimited by commas. The data can be understood as each row representing the exchange between two individual currencies on a single exchange at that Unix time. The five commas separate each row into six attributes that the program stores and analyzes. The attributes, from left to right, are as follows:

1. Unix time
2. Cryptocurrency exchange that offers the coin at the given exchange rate
3. The first currency
4. Exchange offering the exchange or a designation of ‘fiat’ for non-cryptocurrencies
5. The second currency
6. The opening price of the exchange at that Unix time

Each row with the same Unix time will be included in a single graph (all the lines of data in Figure 15 being an example of a single graph), which we will run our Bellman-Ford algorithm on the graph to analyze it for arbitrage opportunities. Our program reads in 29,709 individual graphs. In total, 499997 lines were read in by the program.

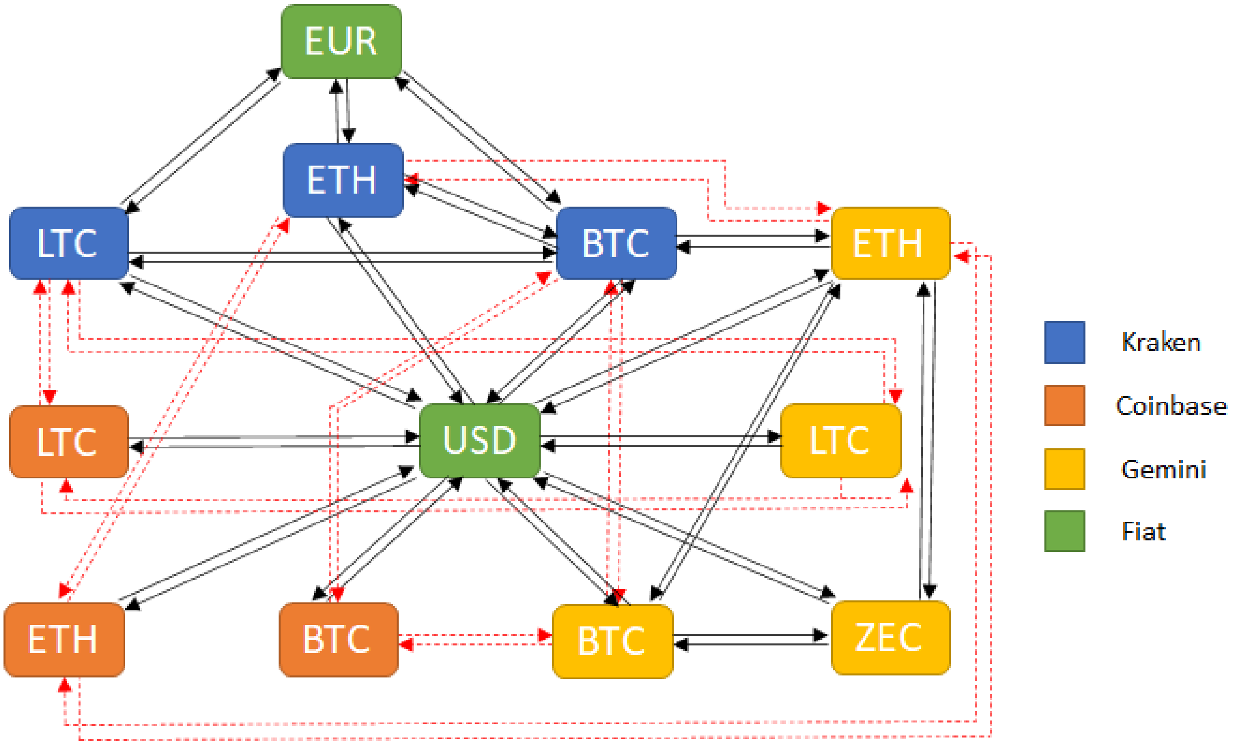


Fig. 16 - Illustration of Graph with paths created for Unix time 1604988000

Figure 16 illustrates the paths of the graph that would be created for the exchange rates available at 1604988000. It should be noted that path weights were intentionally left out of the graphic to avoid cluttering. The weight of the path in each direction will be the negated weight of the path in the opposite direction.

6.3.3 Simulation Caveats

It is worth noting that this method for detecting negative weight cycles will also detect two distinct, unwanted results. First, rounding errors may occur when inversing the exchange rates between two currencies. For example, imagine Currency A is trading for

Currency B at 1.00000 A/B, but currency B is trading to Currency A for 1.00001 B/A, you could earn a profit of 0.00001 by trading A for B, and then B back to A. Our program will detect this and flag it as arbitrage. Second, in order to simulate trading a single currency on multiple exchange markets (for example, trading Bitcoin simultaneously on both the Kraken and Gemini markets), we add an edge between "like" coins within our simulation with a 1 to 1 exchange rate. In Figure 16, these paths are represented by red, dashed arrows. When the logarithm of this exchange is accounted for, we end with a weight of 0 for these edges in both directions. However, this causes our program to detect arbitrage in any instance where the prices of that single coin are not identical in two different exchanges.

Because we are limiting the scope of our experiment to the detection of triangular arbitrage, we only accept the findings of arbitrage if the program reports that at least three distinct currencies are used to achieve arbitrage. If our first attempt to detect arbitrage locates a negative weight cycle with less than three distinct currencies, we reject this detection and continue searching for triangular arbitrage by changing the source node from which we begin the execution of the Bellman-Ford algorithm.[6] If we do not detect triangular arbitrage with this brute-force method after running the algorithm over every starting node, then we will record that graph as not having any detectable arbitrage opportunities (by which we mean specifically triangular arbitrage between three or more currencies).

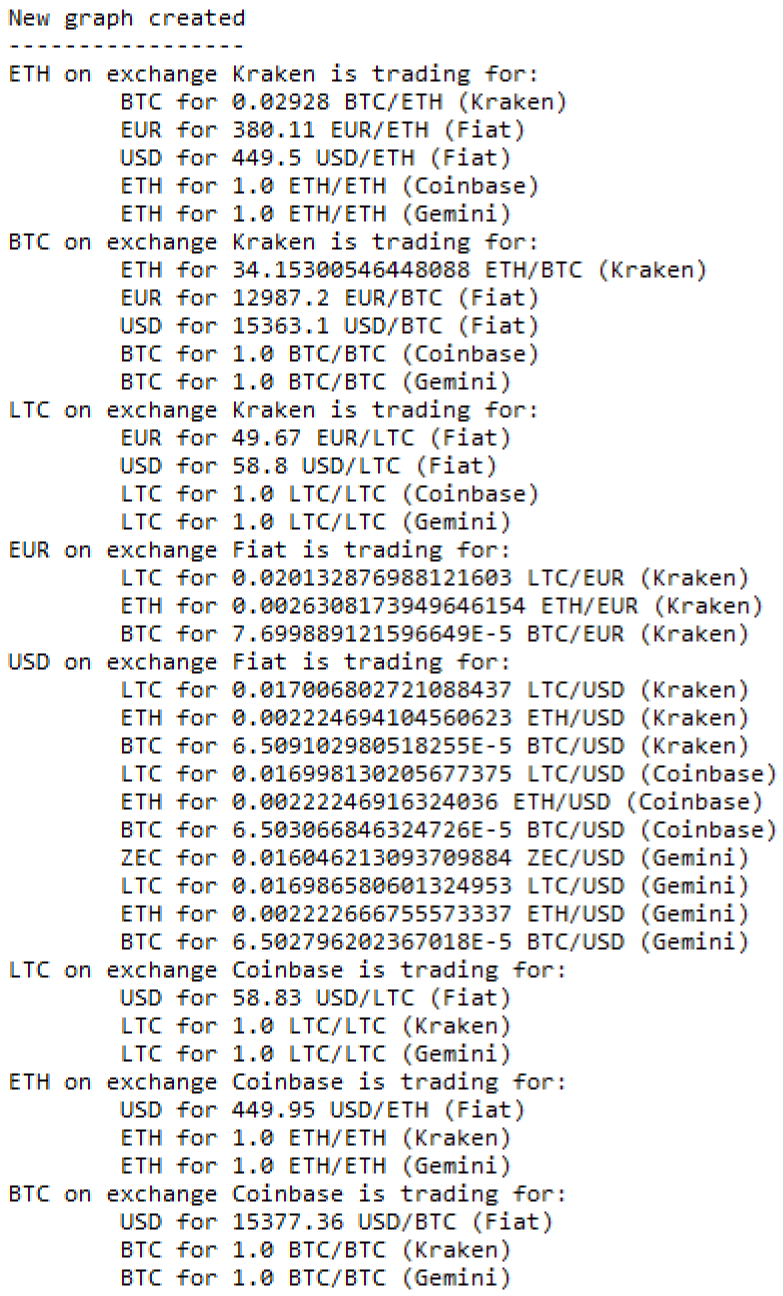
Another note to make about our simulation is that detecting negative weight cycles using the Bellman-Ford algorithm does not allow us to determine how many negative

[6] We will only test other source nodes when *some* type of arbitrage (read: non-triangular) is detected in the first case. The Bellman-Ford algorithm will always detect arbitrage when it exists, so if we do not detect arbitrage from the first source node, we will not continue searching for arbitrage.

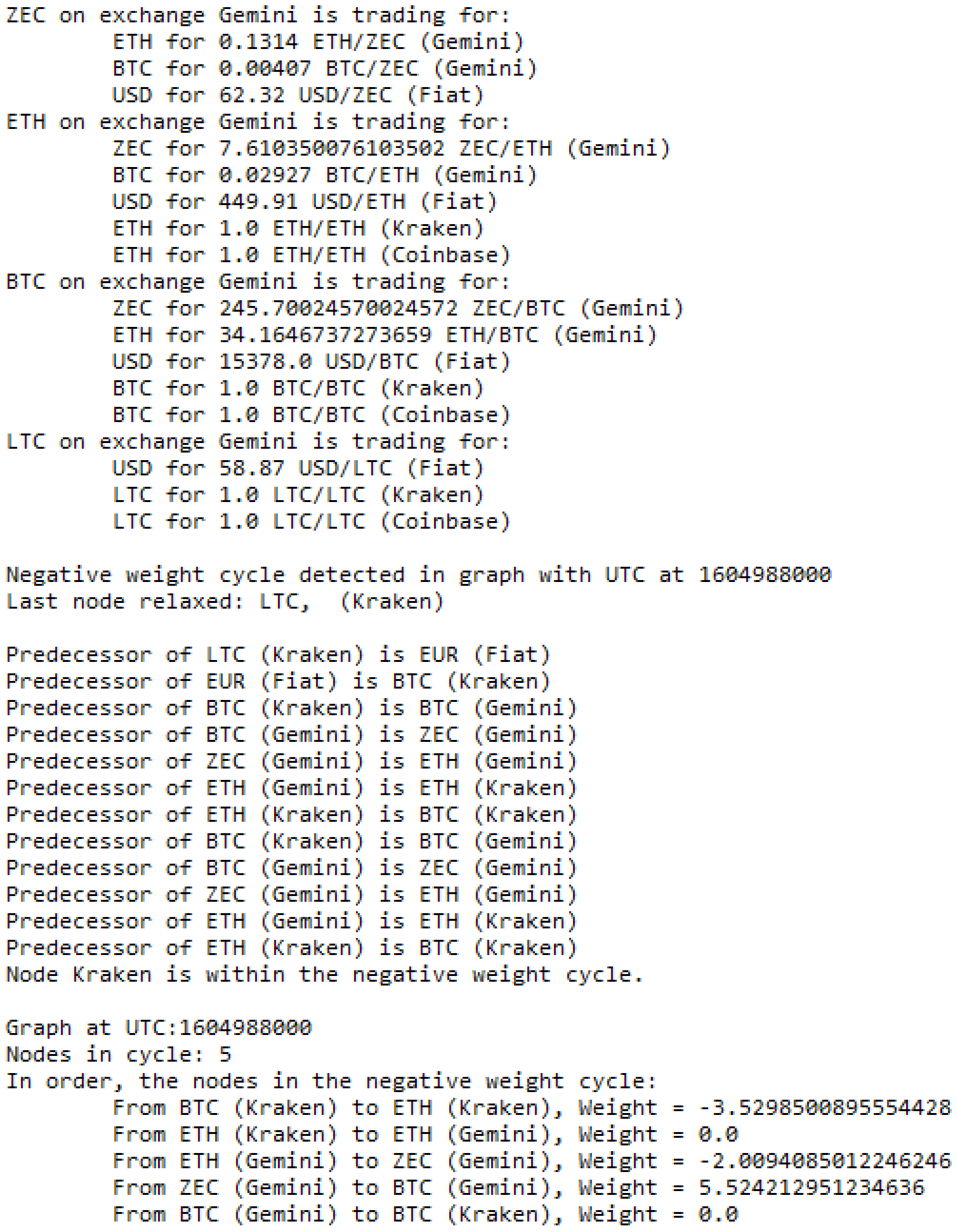
weight cycles exist within a graph. Even the brute-force method in the previous paragraph may not reveal every negative weight cycle if multiple exist in a graph. For this reason, our analysis is somewhat limited to a binary result: whether or not an arbitrage opportunity exists.

6.4 Results

By way of demonstration, Figure 16 displays the results that the program will display for the graph data from Figure 15 (Unix time 1604988000) that is read in by the program.



```
New graph created
-----------------
ETH on exchange Kraken is trading for:
        BTC for 0.02928 BTC/ETH (Kraken)
        EUR for 380.11 EUR/ETH (Fiat)
        USD for 449.5 USD/ETH (Fiat)
        ETH for 1.0 ETH/ETH (Coinbase)
        ETH for 1.0 ETH/ETH (Gemini)
BTC on exchange Kraken is trading for:
        ETH for 34.15300546448088 ETH/BTC (Kraken)
        EUR for 12987.2 EUR/BTC (Fiat)
        USD for 15363.1 USD/BTC (Fiat)
        BTC for 1.0 BTC/BTC (Coinbase)
        BTC for 1.0 BTC/BTC (Gemini)
LTC on exchange Kraken is trading for:
        EUR for 49.67 EUR/LTC (Fiat)
        USD for 58.8 USD/LTC (Fiat)
        LTC for 1.0 LTC/LTC (Coinbase)
        LTC for 1.0 LTC/LTC (Gemini)
EUR on exchange Fiat is trading for:
        LTC for 0.020132876988121603 LTC/EUR (Kraken)
        ETH for 0.0026308173949646154 ETH/EUR (Kraken)
        BTC for 7.699889121596649E-5 BTC/EUR (Kraken)
USD on exchange Fiat is trading for:
        LTC for 0.017006802721088437 LTC/USD (Kraken)
        ETH for 0.002224694104560623 ETH/USD (Kraken)
        BTC for 6.509102980518255E-5 BTC/USD (Kraken)
        LTC for 0.016998130205677375 LTC/USD (Coinbase)
        ETH for 0.0022224691632403 6 ETH/USD (Coinbase)
        BTC for 6.503066846324726E-5 BTC/USD (Coinbase)
        ZEC for 0.016046213093709884 ZEC/USD (Gemini)
        LTC for 0.016986580601324953 LTC/USD (Gemini)
        ETH for 0.002222666755573337 ETH/USD (Gemini)
        BTC for 6.502796202367018E-5 BTC/USD (Gemini)
LTC on exchange Coinbase is trading for:
        USD for 58.83 USD/LTC (Fiat)
        LTC for 1.0 LTC/LTC (Kraken)
        LTC for 1.0 LTC/LTC (Gemini)
ETH on exchange Coinbase is trading for:
        USD for 449.95 USD/ETH (Fiat)
        ETH for 1.0 ETH/ETH (Kraken)
        ETH for 1.0 ETH/ETH (Gemini)
BTC on exchange Coinbase is trading for:
        USD for 15377.36 USD/BTC (Fiat)
        BTC for 1.0 BTC/BTC (Kraken)
        BTC for 1.0 BTC/BTC (Gemini)
```



```
ZEC on exchange Gemini is trading for:
        ETH for 0.1314 ETH/ZEC (Gemini)
        BTC for 0.00407 BTC/ZEC (Gemini)
        USD for 62.32 USD/ZEC (Fiat)
ETH on exchange Gemini is trading for:
        ZEC for 7.610350076103502 ZEC/ETH (Gemini)
        BTC for 0.02927 BTC/ETH (Gemini)
        USD for 449.91 USD/ETH (Fiat)
        ETH for 1.0 ETH/ETH (Kraken)
        ETH for 1.0 ETH/ETH (Coinbase)
BTC on exchange Gemini is trading for:
        ZEC for 245.70024570024572 ZEC/BTC (Gemini)
        ETH for 34.1646737273659 ETH/BTC (Gemini)
        USD for 15378.0 USD/BTC (Fiat)
        BTC for 1.0 BTC/BTC (Kraken)
        BTC for 1.0 BTC/BTC (Coinbase)
LTC on exchange Gemini is trading for:
        USD for 58.87 USD/LTC (Fiat)
        LTC for 1.0 LTC/LTC (Kraken)
        LTC for 1.0 LTC/LTC (Coinbase)

Negative weight cycle detected in graph with UTC at 1604988000
Last node relaxed: LTC,  (Kraken)

Predecessor of LTC (Kraken) is EUR (Fiat)
Predecessor of EUR (Fiat) is BTC (Kraken)
Predecessor of BTC (Kraken) is BTC (Gemini)
Predecessor of BTC (Gemini) is ZEC (Gemini)
Predecessor of ZEC (Gemini) is ETH (Gemini)
Predecessor of ETH (Gemini) is ETH (Kraken)
Predecessor of ETH (Kraken) is BTC (Kraken)
Predecessor of BTC (Kraken) is BTC (Gemini)
Predecessor of BTC (Gemini) is ZEC (Gemini)
Predecessor of ZEC (Gemini) is ETH (Gemini)
Predecessor of ETH (Gemini) is ETH (Kraken)
Predecessor of ETH (Kraken) is BTC (Kraken)
Node Kraken is within the negative weight cycle.

Graph at UTC:1604988000
Nodes in cycle: 5
In order, the nodes in the negative weight cycle:
        From BTC (Kraken) to ETH (Kraken), Weight = -3.5298500895554428
        From ETH (Kraken) to ETH (Gemini), Weight = 0.0
        From ETH (Gemini) to ZEC (Gemini), Weight = -2.0094085012246246
        From ZEC (Gemini) to BTC (Gemini), Weight = 5.524212951234636
        From BTC (Gemini) to BTC (Kraken), Weight = 0.0
```

Fig. 17 - Results from a Single Graph

As evidenced, our program has detected an arbitrage opportunity involving Bitcoin, Ether, and ZCash (an altcoin similar in design to Bitcoin but with added privacy features). Two separate exchanges (Kraken and Gemini) are required in this example for the arbitrage opportunity that was detected.

6.5 Analysis

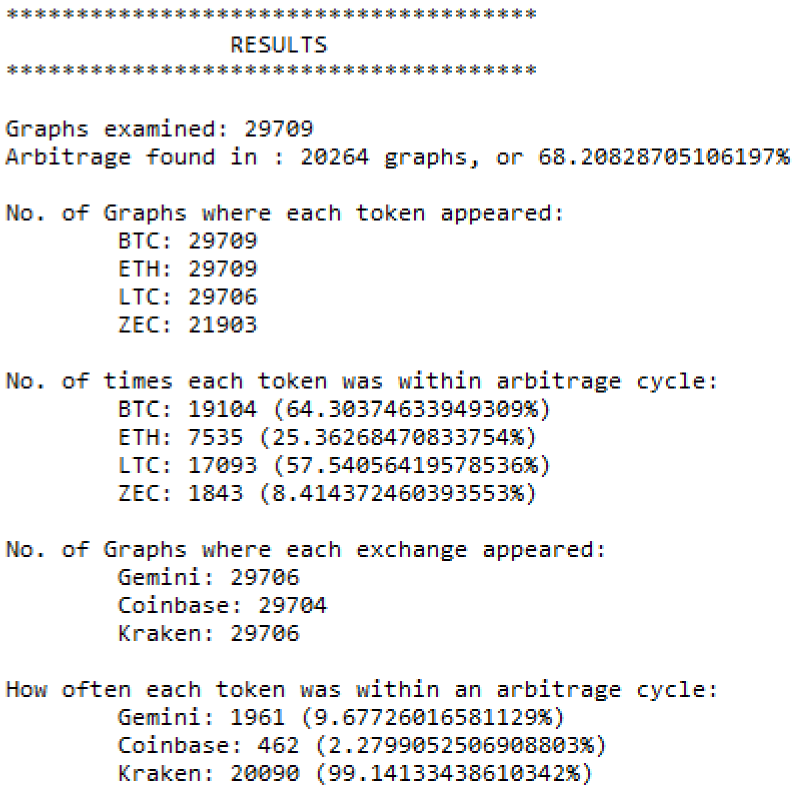
We can see the exchange rates between the currencies listed in the column on the left, so we can test the negative weight cycle to confirm whether an arbitrage opportunity was found. For the purposes of this example, we will start with 1 Bitcoin (BTC) being traded on the Kraken market. It is also important to remember, that each transaction on Gemini must occur simultaneously and will incur the fee for every transfer. After incorporating the exchange fees for both Kraken and Gemini, we can apply the exchange rates from Figure 15 to determine that for every Bitcoin that originally is traded on the Kraken market, an arbitrator can guarantee themselves a 0.01515940 Bitcoin profit.

$$1\,BTC\ (K) * \frac{1\,ETH\ (K)}{0.02928\,BTC\ (K)} * (1 - 0.001) * \frac{ETH\ (G)}{ETH\ (K)} * \frac{ZEC\ (G)}{0.1314\,ETH(G)} * (1 - 0.0199) * \frac{0.00407\,BTC\ (G)}{ZEC\ (G)} * (1 - 0.0199)$$

$$= 1.01515940\,BTC$$

It is important to reiterate that in order for this to work, the arbitrageur must have Bitcoin available on the Kraken marketplace, as well as ZCash and Ethereum available on the Gemini Marketplace. Additionally, these results assume that a buyer was able to be found immediately when initiating these trades, which will affect the possibility of this arbitrage opportunity being possible.

Figure 18 displays the results displayed by the simulation when it attempts to detect arbitrage over all the graphs entered into the dataset. Out of the 29,709 graphs analyzed, our simulation was able to detect a potential arbitrage opportunity in 20,264 graphs. This indicates that we were able to detect arbitrage in about 68.21% of all the graphs analyzed. The results also indicate how many graphs each token appeared in, the occurrence of different coins within the detected arbitrage cycles, how many graphs each exchange appeared in, and the proportion of total arbitrage cycles detected in which token appeared.

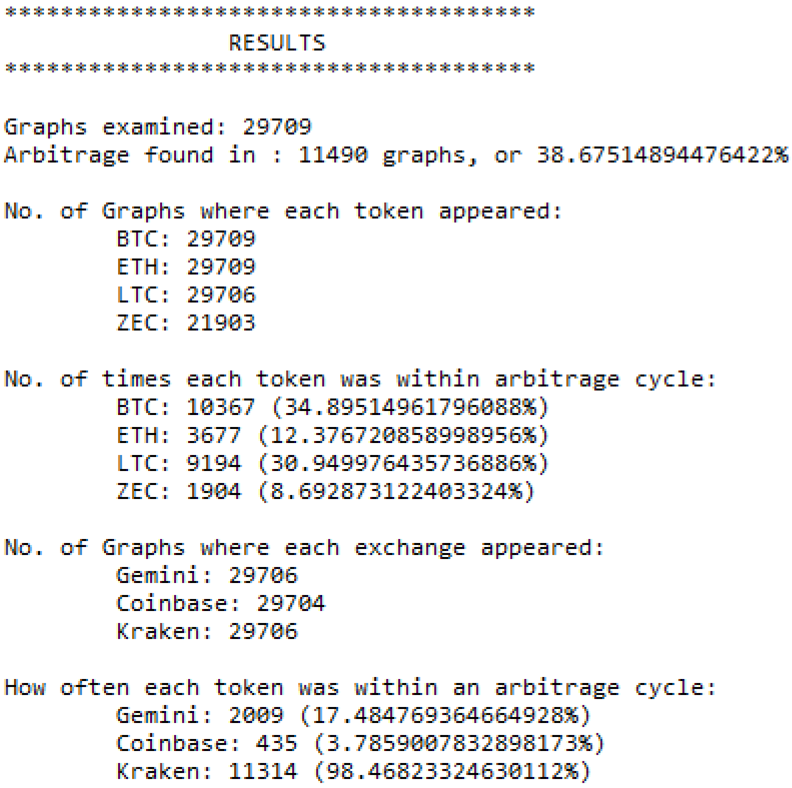


```
**************************************
                RESULTS
**************************************

Graphs examined: 29709
Arbitrage found in : 20264 graphs, or 68.20828705106197%

No. of Graphs where each token appeared:
        BTC: 29709
        ETH: 29709
        LTC: 29706
        ZEC: 21903

No. of times each token was within arbitrage cycle:
        BTC: 19104 (64.30374633949309%)
        ETH: 7535 (25.36268470833754%)
        LTC: 17093 (57.54056419578536%)
        ZEC: 1843 (8.414372460393553%)

No. of Graphs where each exchange appeared:
        Gemini: 29706
        Coinbase: 29704
        Kraken: 29706

How often each token was within an arbitrage cycle:
        Gemini: 1961 (9.67726016581129%)
        Coinbase: 462 (2.2799052506908803%)
        Kraken: 20090 (99.14133438610342%)
```

Fig. 18 - Simulation Results

There is a crucial note to understand about these results. Because our model is incapable of detecting multiple negative weight cycles within a graph, we cannot be certain of the exact number of tokens or exchanges that appear within the total possible number of negative weight cycles. Further, not every coin was tracked for every Unix time period. ZCash was not recorded as often as Bitcoin, so we do not attempt to say that arbitrage is more probable using Bitcoin, even though at a glance the statistics above may suggest that this is true. However, by making a slight alteration in our calculations, the difference in the outcome has significant implications that we may begin to draw some conclusions from.

Consider Figure 18. Of all the arbitrage opportunities that were detected by our simulation, over 99% of those involved the Kraken exchange at some point in the negative weight cycle. It makes sense that this may be the result of Kraken having a much lower exchange fee than either Gemini or Coinbase.[7] This can be compared to Figure 19, which runs the exact same set of data but with a Kraken exchange rate of 0.2% instead of 0.1%. The results are striking.



```
**************************************
                RESULTS
**************************************

Graphs examined: 29709
Arbitrage found in : 11490 graphs, or 38.67514894476422%

No. of Graphs where each token appeared:
        BTC: 29709
        ETH: 29709
        LTC: 29706
        ZEC: 21903

No. of times each token was within arbitrage cycle:
        BTC: 10367 (34.89514961796088%)
        ETH: 3677 (12.376720858998956%)
        LTC: 9194 (30.949976435736886%)
        ZEC: 1904 (8.692873122403324%)

No. of Graphs where each exchange appeared:
        Gemini: 29706
        Coinbase: 29704
        Kraken: 29706

How often each token was within an arbitrage cycle:
        Gemini: 2009 (17.484769364664928%)
        Coinbase: 435 (3.7859007832898173%)
        Kraken: 11314 (98.4682324630112%)
```

Fig. 19 - Simulation results with larger Kraken Fee

Even when the exchange fees for the Kraken market doubles, it is still involved in over 98% of all the arbitrage opportunities detected. However, only 11,490 total graphs contained some arbitrage opportunity. This is a reduction from about 68.2% to 38.7%, which is a drastic reduction. So drastic, in fact, that we believe that we can say with reasonable certainty that Kraken's small exchange fees allowed for more total arbitrage

[7] It should be mentioned that a Kraken exchange rate of 0.1% is only available for the taker price when at least $10 million is posted for the trade. This rate would likely only be available to established firms with enormous assets.

opportunities. It would then follow that in order to facilitate the potential for arbitrage opportunities, low exchange fees are an important factor to consider.

Investigating further, we tested the effect of Kraken’s fee structure on the occurrence of arbitrage using a range of fees from 0 % (no fee) to 1.5%. The results seem to conform to our suspicion above and can be seen graphically represented in Figure 20.

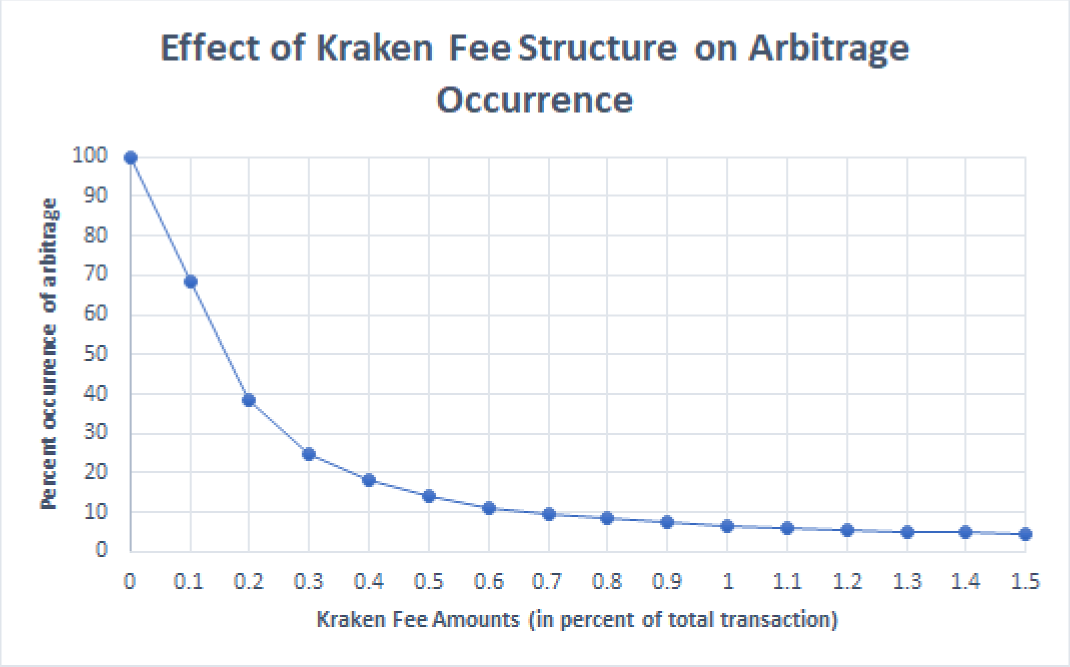


Fig. 20 - Effect of Kraken’s fee structure on the total occurrence of arbitrage in our simulation

When no fee for Kraken was taken into consideration, our program detected an arbitrage opportunity in 99.919% of all graphs tested. This indicates that there is rarely ever a situation where there is a 100% efficient market between the cryptocurrency exchanges. Meanwhile, a fee of 1.5% of the transaction total (chosen so as to be comparable to Coinbase), reduces the amount of graphs in which our program detected arbitrage down to 4.679%. The percent of graphs where arbitrage is available appears to decrease exponentially as the exchange fee increases.[8] With this new information in mind, we are confident of our assessment--arbitrage within the cryptocurrency market is possible very often when the price of exchanging one currency for another is very low. This may be indicative that market forces are slower to take effect on the cryptocurrency market than they would be on fiat currencies, but that is beyond the scope of this research.

7. Conclusions

This paper began with a discussion of the history, technical details, and basic economic analysis of different cryptocurrencies. In addition, we discussed the difficulty of exchanging data and assets effectively across different blockchains and efforts that are being made to facilitate these exchanges. Finally, we contributed to the field by exploring the prevalence of triangular arbitrage over three large cryptocurrency exchanges located in the United States. We determined that low exchange fees are a crucial determining factor when discussing the potential of arbitrage in similar scenarios.

We will conclude this paper by noting that the exchanges that we analyzed are not decentralized in any meaningful way. This goes against the founding principles that Satoshi Nakamoto was operating by when he created Bitcoin. We believe that it is likely that cross-chain interoperability schemes may have a drastic influence on these centralized exchange markets when they become available. In particular, if a decentralized exchange scheme does gain popularity and charges either an insignificant, or non-existent, exchange fee for the exchange of two cryptocurrencies, two likely scenarios may occur. (1) The lower exchange fees will facilitate arbitrage in the short run as price variations on different

[8] If the data for Kraken is removed altogether, and we only test for Arbitrage between Gemini and Coinbase, the amount of graphs with detectable arbitrage drops to 3.517%.

markets will be more likely to enable arbitrage. (2) Investors will take advantage of these arbitrage opportunities and the values of different cryptocurrencies on multiple exchanges will converge due to the increased market forces. We do not try to argue whether these outcomes are positive or negative, but that they are worth consideration.

References

Agrawal, Harsh. “What Is a BIP (Bitcoin Improvement Proposal)? Why Do You Need to Know about It?” *CoinSutra*, 6 Sept. 2019, https://coinsutra.com/bip-bitcoin-improvement-proposa/.

Average Transactions Per Block. 11 Sept. 2020, https://www.blockchain.com/charts/n-transactions-per-block.

Bernard, Zoë. “Everything You Need to Know about Bitcoin, Its Mysterious Origins, and the Many Alleged Identities of Its Creator.” *Business Insider*, Nov. 2020, https://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12.

“Bitcoin Price Index.” *CoinDesk*, 20 Nov. 2020, https://www.coindesk.com/price/bitcoin.

“Bitcoin-XT News.” *Cointelegraph*, https://cointelegraph.com/tags/bitcoin-xt. Accessed 12 Sept. 2020.

Blenkinsop, Connor. “Stablecoins, Explained.” *Cointelegraph*, 30 Apr. 2019, https://cointelegraph.com/explained/stablecoins-explained.

BTC Parachain at a Glance. https://interlay.gitlab.io/polkabtc-spec/intro/at-a-glance.html?highlight=xclaim. Accessed 18 Oct. 2020.

Bünz, Benedikt, et al. “Bulletproofs: Short Proofs for Confidential Transactions and More.” *2018 IEEE Symposium on Security and Privacy (SP)*, IEEE, 2018, pp. 315–34. *DOI.org (Crossref)*, doi:10.1109/SP.2018.00020.

Buterin, Vitalik. *A Next-Generation Smart Contract and Decentralized Application Platform*. 2015, https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf.

---. “Chain Interoperability.” *R3 Research Paper*, 9 Sept. 2016, https://www.r3.com/reports/chain-interoperability/.

Chakravarty, Abhishek. *Why Ethereum, When We Already Have Bitcoin’s Blockchain? | Hacker Noon*. 2 June 2017, https://hackernoon.com/why-ethereum-when-we-already-have-bitcoins-blockchain-3359eb7e087e.

Chaum, David. “Blind Signatures for Untraceable Payments.” *Advances in Cryptology*, 1983, pp. 199–203.

Chen, James. “Triangular Arbitrage Definition.” *Investopedia*, 20 Apr. 2019, https://www.investopedia.com/terms/t/triangulararbitrage.asp.

Chohan, Usman. *The Double Spending Problem and Cryptocurrencies*. 19 Dec. 2017.

“Coinbase Pricing and Fees Disclosures.” *Coinbase*, https://help.coinbase.com/en/coinbase/trading-and-funding/pricing-and-fees/fees. Accessed 12 Nov. 2020.

“Confirmation.” *Bitcoin Wiki*, https://en.bitcoin.it/wiki/Confirmation. Accessed 13 Oct. 2020.

“Contract.” *Bitcoin Wiki*, https://en.bitcoin.it/wiki/Contract. Accessed 26 Sept. 2020.

“Cryptographic Hash Function.” *Wikipedia*, 10 Dec. 2020. *Wikipedia*, https://en.wikipedia.org/w/index.php?title=Cryptographic_hash_function&oldid=993402727.

Dai, Wei. *B-Money*. Consulted, Nov. 1998, http://www.weidai.com/bmoney.txt.

del Castillo, Michael. “Alibaba, Tencent, Five Others To Receive First Chinese Government Cryptocurrency.” *Forbes*, Aug. 2019, https://www.forbes.com/sites/michaeldelcastillo/2019/08/27/alibaba-tencent-five-others-to-recieve-first-chinese-government-cryptocurrency/.

Elliot-Ennis, Paul, and Rose O'Leary. "The Hidden History of Bitcoin Unlimited." *CoinDesk*, 8 Apr. 2017, https://www.coindesk.com/hidden-history-bitcoin-unlimited.

"Ethereum Average Gas Price." *YCharts*, https://ycharts.com/indicators/ethereum_average_gas_price. Accessed 30 Sept. 2020.

Evangelos, Georgiadis. "How Many Transactions per Second Can Bitcoin Really Handle? Theoretically." *IACR Cryptology EPrint Archive*, Apr. 2019, https://eprint.iacr.org/2019/416.

"FAQ — BTC Relay 1.0 Documentation." *BTC Relay*, https://btc-relay.readthedocs.io/en/latest/frequently-asked-questions.html. Accessed 11 Oct. 2020.

"FAQ: How Divisible Are Bitcoins?" *Bitcoin Wiki*, https://en.bitcoin.it/wiki/Help:FAQ#How_divisible_are_bitcoins.3F. Accessed 11 Sept. 2020.

"FAQ: Why Do Bitcoins Have Value?" *Bitcoin*, https://bitcoin.org/en/faq#why-do-bitcoins-have-value. Accessed 11 Sept. 2020.

"Fee Schedules." *Kraken*, https://www.kraken.com/features/fee-schedule. Accessed 15 Dec. 2020.

Fernando, Jason. “Bitcoin vs. Litecoin: What’s the Difference?” *Investopedia*, 21 June 2020, https://www.investopedia.com/articles/investing/042015/bitcoin-vs-litecoin-whats-difference.asp.

“Finding a Negative Cycle in the Graph.” *CP-Algorithms*, https://cp-algorithms.com/graph/bellman_ford.html#toc-tgt-6. Accessed 10 Nov. 2020.

Fitzpatrick, Luke. “A Complete Beginner’s Guide To Atomic Swaps.” *Forbes*, 2 Sept. 2019, https://www.forbes.com/sites/lukefitzpatrick/2019/09/02/a-complete-beginners-guide-to-atomic-swaps/.

Frankenfield, Jake. “Bitcoin Cash Defintion.” *Investopedia*, 20 June 2018, https://www.investopedia.com/terms/b/bitcoin-cash.asp.

---. “Bitcoin Classic.” *Investopedia*, 2 Sept. 2019, https://www.investopedia.com/terms/b/bitcoin-classic.asp.

---. “Interledger Protocol.” *Investopedia*, 23 Sept. 2020, https://www.investopedia.com/terms/i/interledger-protocol.asp.

---. “Public Key.” *Investopedia*, 30 June 2018, https://www.investopedia.com/terms/p/public-key.asp.

“Global Charts.” *CoinMarketCap*, https://coinmarketcap.com/charts/. Accessed 20 Nov. 2020.

Greenberg, Andy. “Monero, the Drug Dealer’s Cryptocurrency of Choice, Is on Fire.” *Wired*, Jan. 2017, https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/.

“Hardforks.” *Bitcoin Wiki*, 12 Sept. 2020, https://en.bitcoin.it/wiki/Hardfork.

"Hashrate Distribution Over Time." *Blockchain.Com*, https://www.blockchain.com/charts/pools-timeseries. Accessed 20 Nov. 2020.

Hayes, Adam. "Is Ethereum More Important Than Bitcoin?" *Investopedia*, 24 Jan. 2020, https://www.investopedia.com/articles/investing/032216/ethereum-more-important-bitcoin.asp.

---. *The Decision to Produce Altcoins: Miners' Arbitrage in Cryptocurrency Markets*. SSRN Scholarly Paper, ID 2579448, Social Science Research Network, 17 Mar. 2015. *papers.ssrn.com*, doi:10.2139/ssrn.2579448.

Herlihy, Maurice. "Atomic Cross-Chain Swaps." *Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing*, Association for Computing Machinery, 2018, pp. 245–254. *ACM Digital Library*, doi:10.1145/3212734.3212736.

Hertig, Alyssa. "Ethereum 101 - How Ethereum Mining Works." *CoinDesk*, 2017, https://www.coindesk.com/learn/ethereum-101/ethereum-mining-works.

"Historical Data for Bitcoin Cash." *CoinMarketCap*, https://coinmarketcap.com/currencies/bitcoin-cash/historical-data/?start=20130428&end=20200801. Accessed 12 Sept. 2020.

Hollander, Luit. "The Ethereum Virtual Machine — How Does It Work?" *Medium*, 2 Feb. 2019, https://medium.com/mycrypto/the-ethereum-virtual-machine-how-does-it-work-9abac2b7c9e.

Ip, Greg. "Facebook's Libra Could Give Dollar, Banks Some Welcome Competition." *Wall Street Journal*, 26 June 2019. *www.wsj.com*, https://www.wsj.com/articles/facebooks-libra-could-give-dollar-banks-some-welcome-competition-11561552511.

Jeffries, Adrianne. “The One True Bitcoin.” *The Verge*, 12 Apr. 2018, https://www.theverge.com/2018/4/12/17229796/bitcoin-cash-conflict-transactions-fight.

Kelleher, John P. “Why Do Bitcoins Have Value?” *Investopedia*, 30 June 2020, https://www.investopedia.com/ask/answers/100314/why-do-bitcoins-have-value.asp.

Kereiakes, Evan, et al. *Terra Money: Stability and Adoption*. Apr. 2019, https://terra.money/Terra_White_paper.pdf.

Kharif, Olga. “Tether Says Stablecoin Is Only Backed 74% by Cash, Securities.” *Bloomberg*, Apr. 2019, https://www.bloomberg.com/news/articles/2019-04-30/tether-says-stablecoin-is-only-backed-74-by-cash-securities.

---. “The World’s Most-Used Cryptocurrency Isn’t Bitcoin.” *Bloomberg.Com*, 30 Oct. 2019, https://www.bloomberg.com/news/articles/2019-10-01/tether-not-bitcoin-likely-the-world-s-most-used-cryptocurrency.

Koens, T., and E. Poll. “Assessing Interoperability Solutions for Distributed Ledgers.” *Pervasive and Mobile Computing*, vol. 59, Oct. 2019, p. 101079. *DOI.org (Crossref)*, doi:10.1016/j.pmcj.2019.101079.

Kurt Magnus, Alonso. *Monero - Privacy in the Blockchain*. Universitat Oberta de Catalunya, Dec. 2017, http://hdl.handle.net/10609/75205.

Kwon, Jae. “Tendermint: Consensus without Mining.” *Draft v. 0.6, Fall*, vol. 1, Nov. 2014, p. 11.

Kwon, Jae, and Ethan Buchman. “Cosmos Network.” *Cosmos Network*, https://cosmos.network/resources/whitepaper. Accessed 17 Oct. 2020.

Lamport, Leslie, et al. “The Byzantine Generals Problem.” *Concurrency: The Works of Leslie Lamport*, Association for Computing Machinery, 2019, pp. 203–226. *ACM Digital Library*, https://doi.org/10.1145/3335772.3335936.

Larsen, Aleks. “A Primer on Blockchain Interoperability.” *Medium*, 23 Dec. 2018, https://medium.com/blockchain-capital-blog/a-primer-on-blockchain-interoperability-e132bab805b.

Lee, Charlie. “Did a Cross-Chain Atomic Swap with LTC/BTC! 10 LTC for 0.1137 BTC with @JStefanop1. Https://T.Co/VXwTNirk0J Https://T.Co/3NTplBOoW9 Https://T.Co/DRKaHg4Wc7.” *Twitter*, 22 Sept. 2017, https://twitter.com/satoshilite/status/911328252928643072.

Libra Whitepaper. LIbra Association, 2020, https://libra.org/en-US/white-paper/.

Lielacher, Alex. “Crypto’s Fungibility Problem.” *Brave New Coin*, 28 Aug. 2019, https://bravenewcoin.com/insights/cryptos-fungibility-problem.

“Live Ethereum (ETH) Gas History.” *Live Ethereum (ETH) Gas History*, https://gitcoin.co/gas/history?breakdown=weekly. Accessed 30 Sept. 2020.

“Main Page.” *Bitcoin Wiki*, https://en.bitcoin.it/wiki/Main_Page. Accessed 11 Sept. 2020.

Makarov, Igor, and Antoinette Schoar. “Trading and Arbitrage in Cryptocurrency Markets.” *Journal of Financial Economics*, vol. 135, no. 2, Feb. 2020, pp. 293–319. *ScienceDirect*, doi:10.1016/j.jfineco.2019.07.001.

Mou, Vallery. “Blockchain Oracles Explained.” *Binance Academy*, https://academy.binance.com/en/articles/blockchain-oracles-explained. Accessed 1 Oct. 2020.

Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008, https://bitcoin.org/bitcoin.pdf.

Neutrino Research Team. “WannaShift to Monero.” *Neutrino SRL*, 1 Sept. 2017, https://www.neutrino.nu/Research_WannaShift_to_Monero.html.

Nguyen, Cong T., et al. “Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities.” *IEEE Access*, vol. 7, 2019, pp. 85727–45, doi:10.1109/ACCESS.2019.2925010.

Nick, Jonas, et al. *Liquid: A Bitcoin Sidechain*. Blockstream, 22 May 2020, https://blockstream.com/assets/downloads/pdf/liquid-whitepaper.pdf.

Nuzzi, Lucas. “Monero Becomes Bulletproof.” *Medium*, 18 Oct. 2018, https://medium.com/digitalassetresearch/monero-becomes-bulletproof-f98c6408babf.

Orcutt, Mike. “Criminals Thought Bitcoin Was the Perfect Hiding Place, but They Thought Wrong.” *MIT Technology Review*, Sept. 2017, https://www.technologyreview.com/2017/09/11/149211/criminals-thought-bitcoin-was-the-perfect-hiding-place-they-thought-wrong/.

Parkhouse, Diana. “Bitcoin Mining May Be Pumping out as Much CO2 per Year as Kansas City.” *MIT Technology Review*, https://www.technologyreview.com/2019/06/12/873/bitcoin-mining-may-be-pumping-out-as-much-cosub2-sub-per-year-as-kansas-city/. Accessed 1 Oct. 2020.

Patel, Ranjeet. “Byzantine Fault Tolerance (BFT) and Its Significance in Blockchain World.” *HCL*, 24 Jan. 2020, https://www.hcltech.com/blogs/byzantine-fault-tolerance-bft-and-its-significance-blockchain-world.

Platias, Nicholas. “Introducing the New Terra Protocol.” *Medium*, 21 Feb. 2019, https://medium.com/terra-money/introducing-the-new-terra-protocol-ed4a8fbefe4c.

Poon, Joseph, and Thaddeus Dryja. *The Bitcoin Lightning Network:* 2015, https://lightning.network/lightning-network-paper.pdf.

Popper, Nathaniel. “Some Bitcoin Backers Are Defecting to Create a Rival Currency.” *New York Times*, 26 July 2017, p. 1.

Posner, Eric. “The Trouble Starts If Facebook’s New Currency Succeeds.” *The Atlantic*, 25 June 2019, https://www.theatlantic.com/ideas/archive/2019/06/dont-trust-libra-facebooks-new-cryptocurrency/592450/.

Redman, Jamie. “5 Mining Operations Command More Than 50% of BTC’s Network Hashrate.” *Bitcoin.Com*, 3 Feb. 2020, https://news.bitcoin.com/5-mining-50-btc-hashrate/.

---. “A Deep Dive Into Polkadot and How DOT Became a Top Ten Crypto Contender).” *Bitcoin News*, 24 Sept. 2020, https://news.bitcoin.com/a-deep-dive-into-polkadot-and-how-dot-became-a-top-ten-crypto-contender/.

---. “What Are Altcoins and Why Are There Over 5,000 of Them?” *Bitcoin.Com*, 10 Feb. 2020, https://news.bitcoin.com/altcoins-why-over-5000/.

"Regulations for LBCOIN and Its Issue Date Approved." *Lietuvos Bankas*, 19 June 2020, https://www.lb.lt/en/news/regulations-for-lbcoin-and-its-issue-date-approved.

Reiff, Nathan. "A History of Bitcoin Hard Forks." *Investopedia*, 25 June 2019, https://www.investopedia.com/tech/history-bitcoin-hard-forks/.

"Ripple Vs. Bitcoin: Key Differences." *Cointelegraph*, https://cointelegraph.com/ripple-101/ripple-vs-bitcoin-key-differences. Accessed 11 Sept. 2020.

Rooney, Kate. "$1.1 Billion in Cryptocurrency Has Been Stolen This Year, and It Was Apparently Easy to Do." *CNBC*, 7 June 2018, https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html.

Rosic, Ameer. "What Is Ethereum Gas? [The Most Comprehensive Step-By-Step Guide Ever!]." *Blockgeeks*, 25 Mar. 2018, https://blockgeeks.com/guides/ethereum-gas/.

Rudden, Jennifer. "Bitcoin Price Index from July 2012 to August 2020." *Statista*, 8 Sept. 2020, https://www.statista.com/statistics/326707/bitcoin-price-index/.

Saurel, Sylvain. "6 Reasons Why Monero Remains A Great Investment For The Future." *Medium*, 13 Nov. 2019, https://medium.com/the-capital/6-reasons-why-monero-remains-a-great-investment-for-the-future-f32e272b6724.

Schwartz, Evan, and Vanessa Pestritto. "Interledger: How to Interconnect All Blockchains and Value Networks." *Medium*, 3 Oct. 2018, https://medium.com/xpring/interledger-how-to-interconnect-all-blockchains-and-value-networks-74f432e64543.

"Sidechain." *Bitcoin Wiki*, https://en.bitcoin.it/wiki/Sidechain. Accessed 10 Oct. 2020.

"Softfork." *Bitcoin Wiki*, https://en.bitcoin.it/wiki/Softfork. Accessed 12 Sept. 2020.

Spencer, Bogart. “Bitcoin Is a Demographic Mega-Trend: Data Analysis.” *Blockchain Capital*, 30 Apr. 2019, https://blockchain.capital/bitcoin-is-a-demographic-mega-trend-data-analysis/.

“Stablecoin Cryptocurrencies Based On Golden Standards.” *U.S. Gold Bureau*, 15 Oct. 2018, https://www.usgoldbureau.com/news/stablecoin-cryptocurrencies-based-on-gold-standards.

Steadman, Ian. “Wary of Bitcoin? A Guide to Some Other Cryptocurrencies.” *Ars Technica*, 11 May 2013, https://arstechnica.com/information-technology/2013/05/wary-of-bitcoin-a-guide-to-some-other-cryptocurrencies/.

Szabo, Nick. *The Idea of Smart Contracts*. 1997, https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html.

Tardi, Carla. “Genesis Block.” *Investopedia*, 11 Sept. 2019, https://www.investopedia.com/terms/g/genesis-block.asp.

---. “Gwei Definition.” *Investopedia*, https://www.investopedia.com/terms/g/gwei-ethereum.asp. Accessed 14 Dec. 2020.

Tassev, Lubomir. “Bank of Japan Turns Back on State-Issued Cryptocurrency.” *Bitcoin.Com*, 18 Apr. 2018, https://news.bitcoin.com/bank-of-japan-turns-back-on-state-issued-cryptocurrency/.

“Technical Overview.” *Blockstream*, https://docs.blockstream.com/liquid/technical_overview.html. Accessed 17 Oct. 2020.

"Technology Overview." *Komodo Platform*, https://komodoplatform.com/technology/. Accessed 18 Oct. 2020.

Tether: Fiat Currencies on the Bitcoin Blockchain. Tether Limited, 2016, https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf.

Thomas, Stefan, and Evan Schwartz. *A Protocol for Interledger Payments*. 2015, URL https://interledger. org/interledger. pdf.

TierNolan. "Alt Chains and Atomic Transfers." *Bitcoin Talk*, 2 May 2013, https://bitcointalk.org/index.php?topic=193281.msg2003765#msg2003765.

"Token Tracker." *Ethereum (ETH) Blockchain Explorer*, 14 Dec. 2020, http://etherscan.io/tokens.

"Top 100 Cryptocurrencies by Market Capitalization." *CoinMarketCap*, 4 Sept. 2020, https://coinmarketcap.com.

Vigna, Paul. "The Great Digital-Currency Debate: 'New' Ethereum Vs. Ethereum 'Classic.'" *WSJ*, 1 Aug. 2016, https://blogs.wsj.com/moneybeat/2016/08/01/the-great-digital-currency-debate-new-ethereum-vs-ethereum-classic/.

"Visa Acceptance for Retailers." *Visa*, https://usa.visa.com/run-your-business/small-business-tools/retail.html. Accessed 12 Sept. 2020.

Walsh, Ben. "Facebook's Libra Currency Will Be Tied, in Part, to the U.S. Dollar." *Barron's*, Sept. 2019, https://www.barrons.com/articles/facebook-libra-currency-will-be-tied-to-the-us-dollar-51569265722.

Wang, Gang, et al. "SoK: Sharding on Blockchain." *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, Association for Computing

Machinery, 2019, pp. 41–61. *ACM Digital Library*, doi:10.1145/3318041.3355457.

"Web Exchange Fee Schedule." *Gemini*, 7 May 2019, https://gemini.com/legal/web-fee-schedule.

"What Are Atomic Swaps?" *Corporate Finance Institute*, https://corporatefinanceinstitute.com/resources/knowledge/other/atomic-swaps/. Accessed 12 Oct. 2020.

"What Is Lightning Network And How It Works." *Cointelegraph*, https://cointelegraph.com/lightning-network-101/what-is-lightning-network-and-how-it-works. Accessed 13 Oct. 2020.

"What Is Tendermint." *Tendermint Core*, https://docs.tendermint.com/master/introduction/what-is-tendermint.html. Accessed 10 Oct. 2020.

Whitepaper: SmART OF GIVING (AOG) – "Coin with a Purpose, Team with a Heart." AEG Signatum LLP, 18 Jan. 2018, https://www.smartofgiving.com/assets/documents/AOG-WhitePaper.pdf.

Willet, J. R., et al. "Omni Protocol Specification." *OmniLayer GitHub*, 18 July 2020, https://github.com/OmniLayer/spec/blob/master/OmniSpecification.adoc.

William, Maxwell. "ERC-20 Tokens, Explained." *Cointelegraph*, 12 May 2018, https://cointelegraph.com/explained/erc-20-tokens-explained.

Won, Daniel. "Bitcoin Forks: Definition, History, Upcoming Forks, How to Claim." *Exodus*, 18 Mar. 2020, https://www.exodus.io/blog/bitcoin-fork/.

Wood, Gavin. *Ethereum: A Secure Decentralized Generalised Transaction Ledger*. Ethereum Foundation, 5 Sept. 2020. *Zotero*, https://ethereum.github.io/yellowpaper/paper.pdf.

---. "Polkadot, Substrate and Ethereum." *Medium*, 30 Oct. 2019, https://medium.com/polkadot-network/polkadot-substrate-and-ethereum-f0bf1ccbfd13.

---. *Polkdadot: Vision for a Heterogenous Multi-Chain Framework*. Polkadot, https://polkadot.network/PolkaDotPaper.pdf. Accessed 18 Oct. 2020.

Young, Joseph. "Crypto Traders Explain What Caused the Bitcoin Price Plunge to the $3K Range." *Cointelegraph*, 13 Mar. 2020, https://cointelegraph.com/news/crypto-traders-explain-what-caused-the-bitcoin-price-plunge-to-3-000.

Zamyatin, Alexei, Mustafa Al-Bassam, et al. *SoK: Communication across Distributed Ledgers*. Working Paper, Cryptology ePrint Archive, 8 Dec. 2019. *spiral.imperial.ac.uk*, http://spiral.imperial.ac.uk/handle/10044/1/75810.

Zamyatin, Alexei, Dominik Harz, et al. *XCLAIM: Trustless, Interoperable Cryptocurrency-Backed Assets*. 643, 2018. *ePrint IACR*, http://eprint.iacr.org/2018/643.