Cryptocurrencies: Applications, Complications and Solutions

Jacob Graubæk Houlberg[1]

This version: April 29, 2018

Abstract: This article explores the possibility of improving the overall adoption and usability of cryptocurrencies in a given economy. By focusing on cryptocurrencies as a medium of exchange, the complications hindering them from gaining widespread adoption are analyzed in details. Volatility is identified as a natural adoption barrier as it gives rise to currency risk, and a solution to it, in the form of a stablecoin, is brought forward. In particular, the proposed stablecoin utilizes an arbitrage enforced price ceiling and changes in supply/demand to act as price pressure mechanisms that pressures the market price towards its intended level.

Keywords: Cryptocurrency; blockchain; price volatility; stablecoin; smart contract
JEL codes: E142, E51, G10, G21 & G23

1. Introduction

Throughout history, money has taken many different forms, and it has in recent times evolved from a purely physical object to a medium existing in cyberspace. Cryptocurrencies are among the most recent inventions within this field. They hold the potential to create new currencies that do not require the purview of centralized intermediaries in order to operate and they have been speculated to encompass the ability to be as transformational as the World Wide Web (Tapscott and Tapscott, 2016). However, the adoption rate of cryptocurrencies and their ability to make an actual impact on the global economy and especially within the field of finance have been comparatively limited (Duivestein et al., 2016). It is by

1. Jacob Graubæk Houlberg, University of Copenhagen, Jacob@Houlberg.org.

many in the world of finance not treated any differently than a speculative investment with large volatility. The aim of this article is to identify and analyse some of the sources of these adoption barriers and subsequently to devise and discuss a solution that has the potential to help overcome these fundamental issues. First, the fundamental concepts of cryptocurrencies will be introduced, how they function and what their sources of competitive advantage are. Building on this analysis, this article will subsequently explore potential real world applications and their inherent benefits and limitations. Furthermore, some of the current issues cryptocurrencies are facing will be discussed to illustrate why these key problems need to be addressed before cryptocurrencies can achieve widespread adoption. One of these fundamental issues is excessive price volatility which is the focus of the final part. A potential solution to volatility through the idea of a stablecoin will be presented as well as a framework that utilizes arbitrage and microeconomic theory to achieve its desired properties.

2. A Primer on Cryptocurrencies

The Oxford dictionary defines a cryptocurrency as »*A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating indepen- dently of a central bank*« (Oxford Dictionary, 2016). Expanding on this definition, the original use of a cryptocurrency is akin to that of any other currency since it acts as a medium of exchange, storage of value and unit of account. Currently, the most common cryptocurrencies operate in a system without centralized entities where agents share information directly with each other, this is also known as a P2P network (Buford et al., 2008). While the most well-known cryptocurrency is Bitcoin, several other exist, such as Ethereum, Dash, Litecoin etc. (CryptoCoin Charts, 2017). Regular digital financial transactions require centralized trusted intermediaries to mediate them and ensure that no fraudulent behavior occurs. Cryptocurrencies does away with the centralized entities by use of what is known as a blockchain, which can simply be thought of as a shared public ledger, chronologically containing all valid past transactions ever recorded.

The first cryptocurrency, Bitcoin, was introduced in 2009 in a paper published under the pseudonym Satoshi Nakamoto (Nakamoto, 2009). It has since grown from insignificance to a fairly known concept in the world of finance, with a current total market value of approximately 70 billion USD. Bitcoin started its rise to prominence during 2013-2014 where its price spiked from approximately 2 USD to over 1000 USD (Coin Market Cap, 2016). During this time, Bitcoin has experienced several severe bubbles and crashes making it a notoriously »*volatile and speculative investment*« (The Economist Editor, 2014). The original vision for Bitcoin was to be an alternative to existing currencies, by acting as a digital medi-

um of exchange and storage of value that did not require the support of centralized entities.

2.1. The Functionality of the Blockchain

Initially, looking at the blockchain it may seem like a convoluted way of solving a problem that does not exist. However, after a cursory glance, it becomes evident that a cryptocurrency without a blockchain, or a blockchain-like feature supporting it, is simply not viable (Keeler et al., 2016).

At their core digital currencies can be compared to the way the Rai Stones, Yapese for stone money, of the Micronesian island of Yap was used as money. The Rai Stones are large circular disks made of limestone and can weigh up to 4 metric tons. The immediate realization is that it is a problem to use an item no single person can carry as a medium of exchange. However, when the Rai Stones exchanged ownership they were usually not physically moved, and in one case where a stone sank to the floor of the sea it continued to be traded as normal because everyone agreed it still existed. The ownership of the Rai Stones was transferred by the initial owner publicly announcing that they transferred ownership of the stone to the new owner (Friedman, 1991). In effect, it is the same way cryptocurrencies work, an agent does not need a physical monetary representation in order for him to be accepted by the system as the owner of a digital asset. As long as the system has an agent registered as the owner, then everyone accepts that as fact.

The most basic and general function of the blockchain is that it acts as a ledger that stores past transactions, i.e. the blockchain is a chronological storage of all the announcements of one agent transferring ownership of a specific number of coins to another agent. That all transactions are appended to the blockchain chronologically ensures that no agent can engage in double spending, where double spending is defined as using the same money multiple times. The monetary system on Yap functions because the community is relatively small, agents are identifiable and the Rai Stones represent a scarce good, meaning no one can flood the market and destroy their value. For a cryptocurrency the first two elements are not present. It is therefore imperative that the system is designed such that malicious and adversarial agents' ability to negatively impact the system, either by trying to cause mayhem or by double spending is minimized. In the regular financial system this property is achieved through the use of centralized intermediaries that record and store the transactions to ensure their legitimacy, a cryptocurrency achieves this through the use of its blockchain.

In the following section, the Bitcoin blockchain will be used to explain and exemplify the fundamental functions of a blockchain, as it is simple and most other blockchains reuse many of its core concepts. The blockchain can be visualized as an unbroken chain of blocks filled with data linked together all the way back to

the original block, which is usually referred to as the Genesis block. Each block is made up of four elements

1. Block Size;
2. Transaction Counter;
3. Transactions;
4. Block Header.

The Block Size denotes the size of the data in the particular block. The Transaction Counter states how many transactions are included, and Transactions specifies all the transactions included. A Bitcoin transaction can be decomposed into two main parts: an input and an output value. The input value is a set of previously received transactions with a combined value equal to or greater than the amount to be transferred. The output value specifies the amount to be transferred and the address of the receiver, where an address can be thought of as akin to a regular bank account. Addresses utilize asymmetric encryption and consist of a public and private encryption key pair (Bitcoin.Org, 2017). Instead of a normal encryption scheme where agents have a single encryption key used to both encrypt and decrypt a message, with asymmetric encryption each agent has their own unique private and public key. The public key is, as the name implies, visible to the public and it is used to derive the address, which is needed when wanting to transfer funds from one wallet to another. The private key is akin to the password associated with the address. Both of these keys are usually stored as a file on a computer, but can also be written down on a piece of paper. Generally speaking asymmetric encryption has two functions as explained by Stallings (1999):

1. Anyone can encrypt a message using the public key which only the holder of the private key can decrypt;
2. Use the public key to authenticate that a given message was sent from the holder of the private key.

In crypto-space, the second function is especially important as it gives the public a way to verify that a given message was sent by the holder of a specific private key. Thus, when someone sends Bitcoin from their address to another address he/she essentially broadcasts that he/she gives the holder of the private key linked with that address the right to spend the number of coins he/she sent. This message is signed with that person's private key and other agents can then use his/her public key to confirm it. As such, the public key is analogous to a bank account number, where everyone can deposit money and the private key is the password to access said bank account enabling the owner to make transfers.

The Block Header differs from the rest of the elements as it encompasses multiple pieces of different information and serves as the element that links block n to the previous block $n-1$, see figure 1 for an overview.

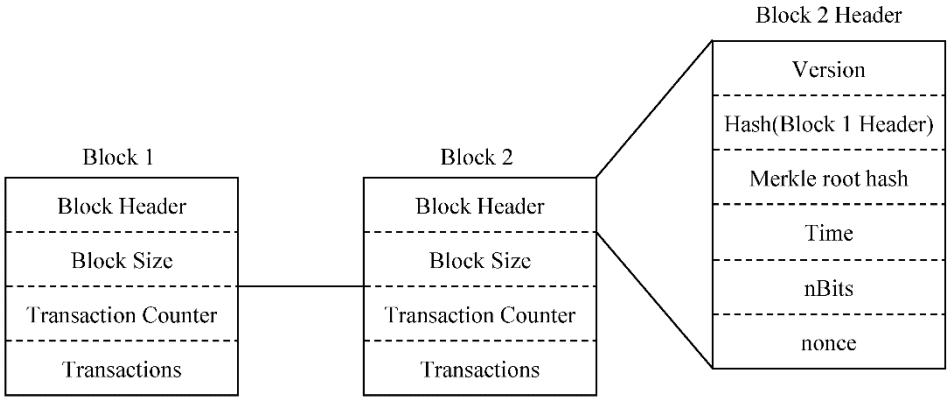

Figure 1: Breakdown of a block in the blockchain

The first part of a block's header is a version number that states what rules the block should follow. The second element is a hash of the previous block's header. A hash is an output or digest of a hashing function, which maps an input of text or numbers to an output of a predefined length. The output of a hash function is deterministic, however, due to the structure of the hash function the output is seemingly random. This means that the digest of an input acts as its digital fingerprint, where it is easy to verify if a given input corresponds to a given output, but practically impossible to determine the input from a given output (Gilbert and Handschuh, 2016).

The hashed header effectively links each block on the blockchain to one another. The header of block n includes the hashed header of block $n-1$, also called the parent block, which in turn includes the hashed header of block $n-2$ and so forth back to the genesis block. This system ensures traceability and that every block only has one parent block (Bitcoin.org, 2016). While a block can only have one parent, it is possible for it to have multiple blocks originating from it; these blocks are called children. In case one block has more than one child what happens is known as a fork, the consequence of which will be explained later. The Time variable is simply the time that has elapsed since January 1, 1970, 24:00 GMT/UTC in seconds until the block was created. The Merkle root hash is the top value of a binary tree storing the double-hashed values of all the transactions in a block, this binary tree is known as a Merkle or hash tree. The idea behind such a tree is to create a tool that can easily verify that a specific transaction is in a block, without needing the entire contents of the block.

The last two variables, nBit and Nonce, are both instrumental in what is known as the proof-of- work required to create a block. A proof-of-work is a problem which is computationally difficult to solve, but easy for others to verify that a given solution is valid. An example of a proof-of-work problem is finding a hash input that is part of a specific set of hash outputs, e.g. finding the hash input that yields a hash output with at least a predefined number of zeros. The nBit variable determines the difficulty of the proof-of-work problem needed to create a new block. The nBit is adjusted every two weeks to ensure that on average each block will take 10 minutes to create. The proof-of- work on the Bitcoin blockchain has the following structure. Agents send their transactions to miners in the P2P network. A miner then fills their block with the transactions he/she wants to include and then hashes the block's header. If the produced hash is lower than the difficulty represented by the nBit variable, then the proof-of-work problem is considered solved, a new block is created and the miner is awarded a given number of Bitcoin for the work. In case the hash or message digest is not below the difficulty level, the miner changes the Nonce variable and tries again. This process is repeated until a Nonce value is found that makes the hashed block header smaller than the difficulty represented by the nBit value. It can take many hash calculations to find a correct Nonce, but once it is found it only takes one calculation to verify that it is correct. Once a miner has found a Nonce that solves the proof-of-work problem he/she propagates the block throughout the P2P network where other miners can verify the solution and begin working on the next block. Thus, the creation of new blocks essentially constitutes a competition of computing power, where the winner's block becomes part of the dominant blockchain and he/she is rewarded with some Bitcoin.

When a block has been distributed throughout the P2P network, the receivers of the block locate its parent block and append the received block to it. Agents then check the validity of the block, e.g. that all the transactions in the block are valid, that the time stamp is within two hours of the correct time, etc. If part of the information contained within the block is invalid the block is discarded by the network and the miner will then have lost all the time and electricity spent on creating the block. As such, miners are incentivized to fill each block with non-corrupted data and verify that the transactions within the block are legitimate as they otherwise risk losing the effort put into finding the solution for their proof-of-work problem. It is important to note that a miner cannot just change one small piece of input in case something is wrong as this changes the hash of the block header entirely and he/she would have to start the mining process all over again.

In the event that two miners solve the proof-of-work problem almost simultaneously and propagate their newly founded block throughout the network a fork is created. This happens because people will receive two child blocks with a different hashed block header to one parent block. All agents who receive the two

blocks will fork their stored blockchain and usually start working on whatever block they received first. The fork that has the highest computing power will on average find the solution to the child block the fastest and distribute that solution to the rest of the network. The result is that one fork will prevail and miners working on the failing fork will switch over and continue working on the prevailing one. When a fork prevails and is used by the rest of the network then even the miner who found the solution for the child block in the non-dominant fork will switch. The reason being that all the Bitcoin he/she mines and transactions he/she includes on the non-dominant fork will be considered invalid by the dominant fork and by implication invalid by the rest of the P2P network, making him/her unable to spend any obtained Bitcoin. The network of Bitcoin nodes will always accept the longest valid blockchain as the true one, due to it being the blockchain that has the most computing power backing its transactions, and therefore the largest chance of being legitimate. Hence, the idea that the network votes for which fork they support with their computing power is a central idea behind the security of the blockchain.

The difficulty of the proof-of-work problem that is solved is re-evaluated every 1,209,600 seconds or approximately two weeks. The algorithm dictating the difficulty calculates how many blocks were created in this time span and subsequently calculates the average time spent creating each block. It then adjusts the difficulty so that the following two weeks blocks should be created approximately every 10 minutes. This ensures that even if the aggregate Bitcoin computing power grows, either due to an increase in miners or better hardware, blocks will always on average be created every 10 minutes. This serves two main purposes: firstly, if the expected time between block creation decreases to for example a few seconds, then forks would happen constantly, additionally many of the forks would become moderately long before a prevailing fork would be found. This creates inefficiencies as all the work done on a non-prevailing fork will be discarded by the network in favor of the prevailing fork. As the security of the blockchain depends on the efficiency of the computing power supporting the longest chain, this has detrimental implications for the security of the blockchain as well as being economically wasteful. It should however be noted that this is a balance as a longer time between blocks also means longer time between when a transaction is initiated to when it is included in a block. The second purpose of the readjustment is that it ensures that mining will neither create abnormal positive or negative profit, and it does so without affecting the price of Bitcoin. This happens by virtue of there being only one block mined approximately every 10 minutes, meaning that a fixed amount of Bitcoin derived from the block creation and transaction fees is available, which has to be shared by all the miners in the ecosystem. Thus, if profits derived from mining were abnormally high outside agents would acquire hardware and start mining, putting a downward pressure on the expected return per amount of electricity spent, as more people would be

competing for the same amount of Bitcoin. However, if profits within mining were abnormally low, then miners would leave the market, reducing the aggregate computing power, leading to a lower difficulty post the readjustment and fewer miners to compete for the same amount of Bitcoin with. This, in turn, increases the expected return per amount of electricity spent. The result is that the readjustment acts as a mechanism to keep the mining markets in equilibrium without affecting the price of Bitcoin.

2.2. The Process of Minting New Cryptocurrency

Bitcoin will once again be used as an example of how cryptocurrencies are minted. Whenever a block is successfully created on the Bitcoin blockchain, the miner who created it is rewarded with a prespecified amount of Bitcoin. The first 210,000 blocks were worth 50 Bitcoin each, from then the Bitcoin minted per block decreases geometrically with 50% per 210,000 blocks (CoinDesk, 2016). Thereby making the final supply of Bitcoin finite and capped at 21 million,

$$Maximum\ supply = \sum_{i=0}^{\infty} \frac{210,000 \cdot 50}{2^i} = \frac{210,000 \cdot 50 \cdot 2}{2^0} = 21,000,000 \quad (1)$$

In addition to the newly minted coins, miners are rewarded with transaction fees, i.e. the cost of sending Bitcoin from one account to another goes directly to the miners as payment for their work. Technically, transaction fees are voluntary, the sender determines the size of the transaction fee, but miners are not obligated to include a specific transaction in their block. The result of this system is that a higher transaction fee increases the probability that the transaction is quickly included in a block. Transaction fees are important for the long-term viability of Bitcoin, as once the 21 million Bitcoin is minted, mining would no longer be profitable, if not for the transaction fees. Because miners are not required to fill blocks up with transactions even given a low transaction volume new Bitcoin can still be minted due to the formation of new blocks.

2.3. Smart Contracts

A recent invention within cryptocurrencies is smart contract functionality incorporated on the blockchain and as discussed by Popper (2016), Ethereum is currently the largest and most well- developed cryptocurrency supporting the smart contract functionality. Smart contract functionality gives users the ability to create contracts which utilize the blockchain for input, execution and output. This can, for example, be used to create a smart contract that behaves like a call option on a stock. This smart contract call option would function just like a regular call option, with a buyer, seller, settle date, strike price etc. and at settlement it would pay out the proceeds accordingly. However, because the output is stored on the blockchain and due to the trustless nature of the blockchain there would be no need for a centralized entity to act as a mediator. The result of removing this in-

termediary is a potential minimization of spread, transaction costs, and friction, thereby increasing the efficiency of the financial markets. In addition to financial contracts and other uses, smart contracts also give users the ability to create their own cryptocurrency that operates within the Ethereum ecosystem and is backed by the Ethereum blockchain.

A simple use is the direct contracts between agents exemplified earlier, but smart contracts can also be used to create autonomous entities which operate solely through the code of its underlying smart contracts. Users would be able to interact with this autonomous entity through interacting with its contracts. All of the rules associated with these autonomous entities would be located on the blockchain and all of its transactions and interactions would be solely governed by those rules and regulations. As everyone would be able to inspect the underlying code and regulations, the actions of the autonomous entity would be predictable with certainty given a known set of input factors. It is however important to note that this immutability means a sacrifice in flexibility because it might not be effectively possible to change the entity's rules and there is only one possible interpretation of them. Creating an entity with transparent rules and guidelines entirely functioning on the blockchain still encompasses certain possibilities which will be further discussed and utilized later in this article. The idea that every user and participant must follow the rules and regulations set forth by any smart contract they choose to interact with is also known as the concept of »*Code is Law*« (Arvicco, 2016).

3. Potential Applications of Cryptocurrencies

Cryptocurrencies do in theory, have the ability to replace the world's current financial system, thereby initiating an era where central banks are unable to effectively regulate the money supply. However, as shown by D'Alfonso et al. (2016) there is little to no research that indicates this to be a probable outcome. Therefore, cryptocurrencies such as Bitcoin and Ethereum should derive their value through their potential as innovative technologies within the regular world of finance and commerce. A simple, yet powerful, way cryptocurrencies have the potential to disrupt global financial institutions is through their ability to transfer funds between accounts and act as a digital medium of exchange, without the need for centralized intermediaries. Money transfers and medium of exchange is also one of the original uses described in the Bitcoin white paper by Satoshi, and is widely regarded as one of the simplest ways cryptocurrencies can impact the world's economy (Mager and Huls, 2017) (Nakamoto, 2009).

Disregarding cash transfers, currently whenever one agent wants to transfer funds to another, he/she has to go through at least one trusted intermediary, often a financial institution. This implies that people need access to the financial

grid either via a bank account or at least a physical operating branch of a financial services company. Furthermore, in the majority of cases the financial institution requires compensation for the service it provides, i.e. it often charges a flat or a percentage based fee of the money being transferred. While access to the financial grid is abundant in the western world, it is much less prevalent in the developing world. According to the World Bank approximately 62% of the world's adult population is currently unbanked. While this naturally restricts their access to services offered by financial institutions, such as loans, savings plans etc., it also means any non-cash monetary transfer is complicated and necessitates interactions with entities that often charge significant fees (The World Bank, 2014). In the case of crossborder transfers, through the use of financial service companies such as Western Union, the fees can be upwards of 7% of the entire amount for smaller transfers in the range of 200 USD (The World Bank, 2017). Sending the same value using the Ethereum blockchain would cost approximately 0.011% of the amount (ETH Gas Station, 2017).

Creating and using a cryptocurrency wallet only requires Internet access and can be set up within approximately one hour. The implication of which is that any person, even someone with only periodic Internet access will have the opportunity to enter and utilize the financial grid through cryptocurrencies. There are virtually no fixed costs associated with having a cryptocurrency account, as the information needed to operate it can be written down on a piece of paper, and it can be accessed all over the world. Moreover, cryptocurrencies should hypothetically be able to provide the same money transfer services for a fraction of the price, due to the removal of a need for trusted intermediaries (Nigam, 2016).

While cryptocurrencies are especially relevant for financial service areas with large fees, it can also have an impact on customers using regular financial services like credit and debit cards for day-to-day purchases. In June 2015 the European Commission enacted the »*Antitrust: Regulation on Interchange Fees*« resulting in several regulatory changes including effectively capping the interchange fee within the EU to 0.2% and 0.3% of the value of the transaction for consumer debit and credit cards respectively (European Commission, 2016). There are several reasons for why these regulations were passed, but first and foremost according to the European Commission it was due to the problematic incentive structure within interchange fees leading to a distorted type competition. In a usual setting, competition results in lower prices for the end customers, however, with interchange fees the opposite is true. This is because the issuing bank benefits from high interchange fees as it increases the bank's revenue. The result is that credit card companies compete by offering higher fees to banks, which in turn is being passed on to the retailers who passes it on to the end customers. This creates a situation where competition does not put downward pressure on prices but instead increases them. Additionally, it is important to note that this legislation is only in effect within the EU, meaning that other countries around the world are

still susceptible to this type of competition with negative consequences for the final consumers. With cryptocurrencies these skewed incentive structures are not present, as miners compete in a decentralized market with low barriers of entry serving to drive down the transfer fees to their minimum level. Moreover, the majority of the intermediaries are eliminated which lessens financial friction, as fewer agents need to earn an economic return.

4. Current Complications of Cryptocurrencies

While cryptocurrencies exhibit multiple complications, there are especially two issues which this paper identifies as inhibiting widespread adoption, namely price volatility and scalability. These issues have been identified because they both have a very limiting effect on cryptocurrencies' ability to be used as a medium of exchange as exemplified in the following sections.

Most cryptocurrencies have throughout their life experienced extreme volatility, table 1 gives an overview of various standard ways to measure volatility applied on a select few fiat currencies, cryptocurrencies and precious metals. All measures are for the relative changes of inter-day closing prices denominated in USD from 1/1/2016 to 1/3/2017.

Table 1: Volatility overview of fiat currencies, cryptocurrencies and precious metals

	Fiat currencies		
	EUR	GBP	JPY
Min	-2.01%	-2.54%	-2.33%
Max	2.31%	8.27%	3.44%
Std	0.51%	0.83%	0.77%
95% obs. interval	(-0.80% , 0.70%)	(-1.00% , 1.10%)	(-1.20% , 1.10%)
	Cryptocurrencies		
	Ether	Litecoin	Bitcoin
Min	-43.29%	-37.79%	-41.50%
Max	47.61%	80.16%	81.84%
Std	7.35%	5.98%	6.12%
95% obs. interval	(-10.10% , 12.00%)	(-4.70% , 4.10%)	(-5.20% , 5.40%)
	Precious metals		
	Gold	Silver	Platinum
Min	-4.48%	-6.49%	-4.04%
Max	3.14%	8.00%	4.92%
Std	0.93%	1.55%	1.40%
95% obs. interval	(-1.40% , 1.60%)	(-2.70% , 2.30%)	(-2.50% , 2.20%)

Source: (Bloomberg, 2017) (Poloniex, 2017)

As seen from table 1, cryptocurrencies are more volatile on virtually all metrics compared to precious metals and fiat currencies as well as being especially sus-

ceptible to extreme outcomes (The Bitcoin Volatility Index, 2016). A study conducted by Kasper (2017) comparing the volatility of Bitcoin and currencies of the 39 least developed countries in the world, found Bitcoin's volatility to be higher than all examined currencies for the majority of the time. This is further corroborated by Bakar and Rosbi (2017) who found the price of Bitcoin to follow a non-normal distribution with a high degree of volatility. The actual source of the volatility found within cryptocurrencies is outside the scope of this article, but it will simply be taken as a fact, as suggested by the data. Because cryptocurrencies are not only a speculative investment, but also act as a currency and medium of exchange, large volatility is an inherent adoption barrier. The reason being that it exposes the users to currency risk, which Levi (2005) defines as »... *the variability of domestic- currency values of assets or liabilities due to unanticipated changes in exchange rates*«. Currently, no economies in the world use cryptocurrencies as their dominant currency (Scott, 2016). Thus, whenever a business accepts cryptocurrency as payment the business will be directly exposed to cryptocurrency's volatility. The effect is amplified by the fact that it is difficult to create a natural hedge with cryptocurrencies by matching income and expenses because the majority of the world's commercial ecosystem does not accept cryptocurrencies. Therefore, a company that accepts cryptocurrencies generally has three options:

1. Keep the cryptocurrency and receivables on its balance sheet, either to potentially pay some expenses or because it believes the price will rise;
2. Exchange the cryptocurrency for local currency when it is received and keep the cryptocurrency denominated liabilities on the balance sheet unhedged;
3. Exchange the cryptocurrency for local currency when it is received and hedge the cryptocurrency denominated liabilities on the balance sheet through a series of financial instruments.

Smith et al. (1993) provide empirical evidence which supports the hypothesis that hedging currency exposures increases firm value by reducing expected costs associated with financial distress, taxes and certain types of agency costs. Therefore, if companies want to minimize volatility and maximize firm value then all positions denominated in any cryptocurrency must be sold or hedged as much as possible, leading to three key implications.

Firstly, it increases the costs associated with accepting cryptocurrencies for any given company because the cryptocurrency has to be resold when it is received, and in the case of a receivable the company needs to hedge the exposure though financial instruments. Financial instruments on Bitcoin such as futures contracts are currently offered on the Chicago Mercantile Exchange (CME), making hedging an actual, but expensive, possibility (CME, 2018). In theory, the fee for transferring cryptocurrency from one account to another should be low. However, because the sale of cryptocurrency for fiat currency has to go through an exchange

means an added layer of fees. Therefore, companies that accept cryptocurrency will need to pay extra fees to continuously sell off any cryptocurrency they receive. Furthermore, in the case a perfect hedge does not exist, the company has to bear the remaining risk on its balance sheet. The ensuing result is a situation where it may very well not be economically feasible for companies to accept cryptocurrencies.

The second implication is that these necessary actions increase the complexity related to accepting cryptocurrency. Moreover, many smaller companies do not have access to sufficient hedging tools and instruments. A likely outcome of this is that the expected return does not outweigh the complexities associated with accepting cryptocurrencies. This can especially be the case for smaller companies who may not have specialized staff on hand that has the required financial knowledge to perform the needed set of actions.

The third implication is that these elements keep cryptocurrencies in a cycle of perpetual downward price pressure. This happens because commercial agents are unwilling to hold any cryptocurrency for a longer period leading to a constant sell off. The only agents that can stem this downward price pressure are investors and private individuals who utilize cryptocurrencies to purchase day to day items. This notion leads to yet another problem, while currency risk poses a significant threat to the financial stability of companies, it also poses a risk to private individuals who hold them to purchase regular goods and services. Thaler et al. (1997) find empirical evidence suggesting that individuals tend to have myopic loss aversion. The result is that they are short sighted and the potential for often negative feedback in general leads to a larger degree of risk aversion. This suggests that people might be averse to keep cryptocurrencies to use for day to day spending because they would constantly be reminded whenever they lost money due to the changing exchange rates. This scenario is bound to happen often due to cryptocurrencies' volatile nature. Moreover, individuals will be exposed to a similar exchange rate risk as companies, albeit on a lesser scale. For many individuals, it would not be feasible to have part of the net worth they need to function on a daily basis in a currency that could lose 50% of its value overnight. The importance of keeping volatility to a minimum is neither new nor exclusive to cryptocurrency, Hayek (1990) proposed in »*Denationalization of Money: The Argument Refined*« that in an environment with multiple currencies, the stability of value would be among the most crucial adoption factors.

The issue of scalability is fundamentally different from volatility as it mainly pertains to the underlying technology of the individual cryptocurrencies, but it has however proven equally difficult to adequately solve. The following section uses Bitcoin as an example, however as most cryptocurrencies are built on the same principles and technology as Bitcoin the issue of scalability is applicable to cryptocurrencies in general. The Bitcoin block size is limited to 1MB, and the size of the average block is currently at that ceiling. This means that there are a maxi-

mum amount of transactions that can be included in a block (Blockchain Info, 2017a). The result of which have negative consequences on Bitcoin's scalability, as only one block and by implication a semi-fixed amount of transactions can be processed every 10 minutes. Currently, the average amount of transactions per block is approximately 1,800 (Blockchain Info, 2017b), meaning that circa three transactions can be approved every second. Nasdaq estimates that there were roughly 49 billion debit card transactions in 2015 from Visa and MasterCard in the United States alone. This works out to approximately 1,540 transactions per second, for only those two providers in the United States (Nasdaq, 2015). Considering that those transactions are only a part of all the digital transactions and transfers the global economy currently handles, it is obvious that cryptocurrencies and especially Bitcoin have an issue with scalability. This is assuming that Bitcoin wants to be able to compete with the current services as it can handle well below 0.2% of the required transaction load. An intuitive solution to the problem of scalability is to merely increase the block size or remove the limit entirely. Setting aside the fact that this would most likely cause the Bitcoin blockchain to be split either permanently or temporarily, it is not a long-term solution because it would require agents to upload and share blocks of increasingly larger size within the P2P network. To illustrate, assume that Bitcoin acquires 10% of the transaction load that Visa and Mastercard has in the US. This would mean that the block size would have to be increased to approximately 50 MB, and the blockchain would grow with 7,200 MB per day. This would make Bitcoin infeasible for users in areas without a high-speed internet connection, and the constant size increase means that it would not be possible for regular users to store the entire blockchain on their computer.

Even disregarding the issue of block propagation and the increased storage space, simply infinitely increasing the block size is not a viable solution. The reason for this is that the marginal cost of including a transaction in a block would effectively be zero, thereby creating a race to the bottom scenario for miners. The ensuing result is a situation where miners only charge negligible transaction fees, and due to the geometrical decrease in the reward for creating a block, mining will largely become unprofitable. This leads to miners leaving the network, thereby decreasing the aggregate computing power backing the blockchain, which has severe detrimental implications for its underlying security.

Creating a solution to scalability is outside the scope of this article as the solutions will most likely be found within computer science, and not within economics and finance. However, the issue of volatility is inherently financial in nature; as such it has been chosen as the problem this article will propose and discuss a potential solution for in the following section.

5. A Proposed Solution to the Problem of Volatility

As discussed by Hsieh and Miller (1990), it is difficult to remove or drastically reduce the volatility of freely traded financial assets, such as cryptocurrencies, even with interference from a centralized authority. Therefore, this article will instead explore the possibility of creating a new type of cryptocurrency that is autonomously pegged to a real world asset or fiat currency such as the USD. This type of cryptocurrency is also known as a stablecoin. The stablecoin solution is explored by first defining and comparing the concept of a stablecoin with the fixed exchange rate systems currently in place between fiat currencies. Thereafter, different stablecoin approaches will be examined and a stablecoin solution that includes all of the necessary elements, while minimizing overall risk, will be proposed. Subsequently, the stablecoin's viability as a currency and way of solving or reducing the problem of volatility will be concluded on.

According to White (2017) a stablecoin can at its core be compared to the fixed exchange rate systems that exist between some currencies. As explained by Mankiw, normally a fixed exchange rate is obtained through the central bank promising and standing ready to buy and sell the pegged currency at a specific rate. This entails arbitrage opportunities for investors in the case the exchange rate deviates from the intended level. To carry out these actions, the central bank needs two types of reserves: domestic currency reserves which it can usually mint, and foreign currency reserves which it must have bought previously (Mankiw, 2012). It is not possible to replicate this type of system when fixing the exchange rate between a decentralized stablecoin and a fiat currency. The main reason for this is the fact that an autonomous entity functioning solely on the blockchain would be unable to possess any of the required fiat currency reserves. Therefore, a stablecoin needs a different stabilizing mechanism.

Additionally, fiat currencies are usually minted by a central bank, however as cryptocurrencies derive one of their main competitive advantages from the removal of centralized trusted entities the minting process of a stablecoin needs to created such that it retains the trustless and autonomous nature. As shown by Buterin (2014) a stablecoin solution therefore requires two fundamental features, the ability to autonomously mint new currency issues and the ability to adequately keep the exchange rate fixed within a predetermined band.

5.1. Minting New Issues of Stablecoins

In order to have a functioning stablecoin there needs to be a way to mint new stablecoins, as a currency without any actual issues and owners cannot be used as a medium of exchange. This can be incorporated through a smart contract that acts as a type of autonomous central bank (ACB), which operates solely based on the rules stipulated in its code. A simple way of minting new stablecoins is to allow users to collateralize cryptocurrencies with the ACB in exchange for newly mint-

ed stablecoins, which they can return at a later point to obtain the underlying collateral. This is effectively the same as creating a collateralized loan with liquid collateral.

The first implication of this system is that the initial value of the collateral must always be larger than the value of the newly issued stablecoins associated with it. Essentially posting collateral with a value of σ need to yield an amount of stablecoins with a value of $\sigma \cdot \alpha$, where $\alpha < 1$ and describes the fraction of value (FOV) an agent receives in stablecoin for his/her underlying collateral. The reason for the constraint $\alpha < 1$ is that the issuance of stablecoin effectively constitutes an infinite sum which is only convergent if $\alpha < 1$. The equation for the total value of stablecoins a given initial value of collateral can create is shown in equation 2.

$$\gamma = \sum_{i=1}^{\infty} \sigma \cdot \alpha^i \tag{2}$$

where γ denotes the total value of stablecoins a given initial value of collateral can create, σ is the value of the initial collateral posting and α denotes the fraction of value of stablecoins an agent receives for their collateral. Solving this infinite sum yields equation 3.

$$\gamma = (\sigma \cdot \alpha + \sigma \cdot \alpha^{n+1}) \cdot \frac{1}{1-\alpha} \tag{3}$$

As analyzed in equation 3, as n approaches infinity this is only a convergent sum as long as $\alpha < 1$, in which case equation 3 simplifies to equation 4.

$$\gamma = \sigma \cdot \frac{\alpha}{1-\alpha} \tag{4}$$

Locking collateral against stablecoins therefore generates two distinct results: firstly, it produces stablecoins, and secondly it creates a leveraged exposure to the collateralized asset. The exposure is the total value of all the underlying collateral, as shown in equation 5.

$$\epsilon = \sum_{i=0}^{\infty} \sigma \cdot \alpha^i \tag{5}$$

where γ denotes the total value of all collateral, σ and α are the same variables as above. Solving this infinite sum with the constraint that $\alpha < 1$ yields equation 6.

$$\epsilon = \sigma \cdot \frac{1}{1-\alpha} \tag{6}$$

Thus, with an initial equity value of σ an agent is able to create a leveraged exposure to the underlying asset of $\sigma \cdot \frac{1}{1-\alpha}$. The payoff, assuming the value of the sta-

blecoin does not change, at time T + 1 from the leveraged position is shown in equation 7, where π_{T+1} denotes the profit/loss at time T + 1.

$$\pi_{T+1} = \epsilon_{T+1} - \epsilon_{T+1} = (\sigma_{T+1} - \sigma_T) \cdot \frac{1}{1-\alpha} \tag{7}$$

Demand for creating leveraged positions will therefore be the main driver for the creation of stablecoins utilizing the above stated system.

A main issue with the above-stated issuance solution is the risk of under-collateralized sta- blecoins. Under-collateralization happens in case the market value of the collateral drops below the market value of the stablecoins it was used to issue. In this case, the agent possessing the stablecoins will have no incentive to redeem them because the value of the stablecoins needed to redeem the underlying collateral is higher than the collateral.

A way of minimizing this problem is to create a minimum or maintenance collateral that needs to be fulfilled at all times, and in case it is not the position becomes open for other agents to close at a profit. This would be similar to the maintenance collateral requirements found in regular financial contracts, where agents can be margin called. Thereby, pressuring the issuer to consistently keep the value of collateral above a certain level, to minimize the possibility that the position gets under-collateralized and other agents buy their collateral at a discount. A maintenance margin should be set such that the collateral required to keep the maintenance is lower than the initial collateral and higher than the value of the stablecoins it was used to issue. Otherwise, the maintenance collateral would be below the point where the position is under- collateralized, which effectively makes it useless. Equation 8 describes the minimum required level og maintenance collateral.

$$\sigma_M = \sigma_I \cdot \beta \tag{8}$$

where σ_M is the value of the maintenance collateral, σ_I being the value of the initial collateral and β denotes the required maintenance level, subject to equation 9 as per the reasons described earlier.

$$\alpha < \beta < 1 \tag{9}$$

Thus, a position would be considered to be below the maintenance collateral requirements and open for other agents to close when equation 10 is true.

$$\sigma_M > \sigma_t \tag{10}$$

where σ_M is the same variable as described above and σ_t is market value of the collateral at time t. The maintenance margin should ensure that in the majority of the cases positions do not become undercollateralized, however if the value of the underlying asset drops virtually instantly positions can still experience undercollateralization. A potential solution to this issueis to create a con-

tinuously compounded insurance fee the issuers of stablecoins or arbitrageurs would have to pay. These fees would be added to a reserve pool of the ACB that will utilize them to bail-out the undercollateralized positions. This insurance scheme can be created by making the issuers of stablecoins receive less of the underlying collateral when they close out their positions, the difference would then quasi-continuously be added to the reserves of the ACB. Equation 11 calculates the amount of collateral the issuers receive for closing their position.

$$\mu_t = \mu_I \cdot e^{-r \cdot t} \tag{11}$$

where μ_I denotes the initial amount collateral in coins, μ_t is the amount of collateral the issuer would receive at time t, r is the insurance rate described above and t is the time. Equation 12 below describes the flow of collateral to the reserves of the ACB.

$$\xi = \mu_I \cdot e^{-r \cdot t} - \mu_I \cdot e^{-r \cdot (t+k)} \tag{12}$$

where k is strictly positive number and ξ is the added reserves from time t to time $t + k$.

If at any point a position would become undercollateralized the ACB would sell enough reserves to buy stablecoins to bailout the position at a loss. Assuming the money received through the insurance rate is higher than or equal to the money spent on bailouts this should ensure that the system has no undercollateralized positions and by implication that all stablecoins are adequately backed, thereby increasing price stability.

It is however important to note that large unanticipated drops in the value of the underlying collateral shortly after such a stablecoin has been implemented is likely to cause a complete collapse of the stablecoin. This happens as the ACB will not have built adequate reserves to bailout undercollateralized positions. This problem is naturally exacerbated by the extreme volatility that characterizes most cryptocurrencies.

5.2. Keeping the Exchange Rate Fixed

In order to ensure a stable value and that the peg is kept intact, there need to be mechanisms that put a downward pressure on the price if the stablecoin is overvalued and an upward pressure on the price if it is undervalued.

There is an inherent price ceiling for a stablecoin above which point arbitrage opportunities exist. These arbitrage opportunities exist because the ACB makes an implicit assumption of the exchange rate for the stablecoin when it issues them, as shown by equation 13.

$$\kappa = \mu \cdot M_C \cdot \frac{1}{I_P} \cdot \alpha \tag{13}$$

where κ denotes the number of stablecoins received per collateral, μ denotes the number of cryptocurrency coins kept in collateral, M_C is the market exchange rate of the cryptocurrency defines as $\frac{Pegged\ currency}{Cryptocurrency}$, I_P is the issuance rate of the stablecoin defined as $\frac{Pegged\ currency}{Stablecoin}$ and α is the FOV described in the previous equations.

A simple version would be the ACB issuing stablecoins under the assumption that the stablecoinmarket rate is equal to the intended pegged rate, i.e. $I_P = P$ where P is the exchange rate between the stablecoin and the pegged currency defined as $\frac{Pegged\ currency}{Stablecoin}$. To illustrate, assume the intended peg is 1-to-1 with the USD, i.e. $P = 1$, the market value of Bitcoin is 10 and α = 0.75. In this example agent A collateralizes 10 Bitcoins, the ACB then issues $10 \cdot 10 \cdot \frac{1}{1} 0{,}75 = 75$ stanblecoins.

Assume the market value of stablecoins is 2 USD per stablecoin then the stablecoins the ACB issued has a market value of $75 \cdot 2 = 150$ USD. This stablecoin issuance scenario leads to arbitrage opportunities, because the value of the stablecoins is higher than the value of the collateral. Agent A spent 100 USD on collateral and obtained 150 USD worth of stablecoins, he/she can use the 150 USD to purchase additional cryptocurrencies to use as collateral and issue new stablecoins and so forth. Agent A would therefore be able to increase his/her personal net-worth with every issuance cycle. Moreover, as long as the arbitrage opportunity exists he/she will be able to constantly increase the supply of stablecoins which should put a downwards pressure on the price.

If the value of the received stablecoins is equal to the value of the collateral, it is effectively the same as when $\alpha = 1$ in equation 2, i.e. any agent can generate new stablecoins ad libitum and create an infinite exposure to the collateral with a minimal investment which also effectively constitutes arbitrage. Therefore, under the assumption that markets are rational and that arbitrage should not exist, equation 14 must hold at all times.

$$Value(Stablecoins\ received) < Value(Collateral\ backing\ stablecoins) \tag{14}$$

Rewriting equation 14 and inserting the known variables yields equation 15.

$$\underbrace{\kappa \cdot M_S}_{Market\ value\ of\ stablecoins} < \underbrace{\mu \cdot M_C}_{Market\ value\ of\ collateral} \tag{15}$$

Inserting equation 13, yields equation 16.

$$\mu \cdot M_C \cdot \frac{1}{I_P} \cdot \alpha \cdot M_S < \mu \cdot M_C \tag{16}$$

where κ, μ, M_C, α and I_P are the same as described above and M_S is the market exchange rate of the stablecoin defined as $\frac{Pegged\ currency}{Stablecoin}$

Using the simple issuance function of $I_P = P$ this simplifies to equation 17.

$$M_S < \frac{P}{\alpha} \tag{17}$$

As such, any market rate above the one described in equation 17, would lead to arbitrage opportunities. Under the assumption that arbitrage should not be found in the market this constitutes a price ceiling for the market rate of the stablecoin.

While this creates a price ceiling for the stablecoin it does not prohibit it from trading above its intended level, but below the price ceiling. A possible solution to this is to make the issuance price of the ACB a function of the ratio between the intended exchange rate and the market rate as well as the time the price of the stablecoin has been above or below its intended level. The derivative of this issuance rate should therefore be negative with respect to time in case the market value is above the pegged rate, and positive in case the market value is below. Equation 18 is a bounded issuance function that encompasses these characteristics.

$$I_P(M_S) = \frac{1}{e^{\Gamma \cdot (M_S - P) \cdot t}} \cdot P \tag{18}$$

where M_S and P are the same variables as described above. Γ is a constant that determines the speed of change, and t is the time since the price was either at its intended price or opposite of what its now. For example, if it is overvalued it would be the time since it was either at its intended level or undervalued. Figure 2 is a graphical representation of this with an illustrative market price development for the stablecoin.

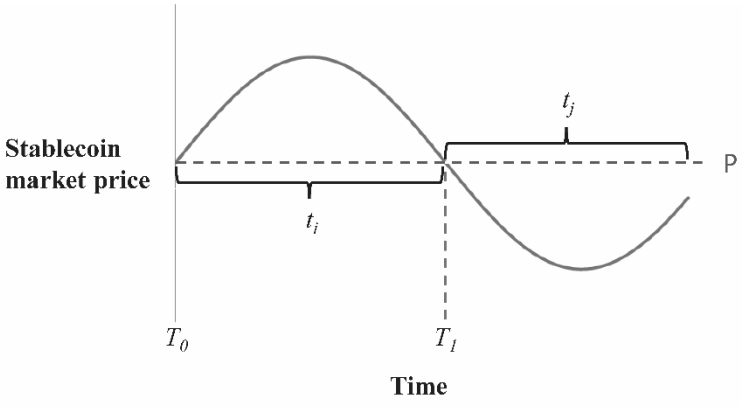

Figure 2: Example of how the value of t changes

Thus, between time T_0 and T_1 the stablecoin is overvalued, which means the ACB issues stablecoins with t_i as input in its issuance function. At time T_1 the price falls to and subsequently below its intended level, resetting t to 0. After T_1 the ACB issues stablecoins with t_j as input till the value of the stablecoin increases to and/or above the intended level at which point t will be reset to 0 once again.

The actual unit of t can be chosen at will as Γ can be adjusted to reflect it. To find the new price ceiling with this issuance function, the I_P function from equation 18 is inserted in equation 16, which yields equation 19.

$$\mu \cdot M_C \cdot \frac{1}{I_P(M_S, t)} \cdot \alpha \cdot M_S < \mu \cdot M_C \tag{19}$$

Reducing this to find the new arbitrage price ceiling yields equation 20.

$$M_S < \frac{1}{\Gamma \cdot t} \cdot W\left(\Gamma \cdot t \cdot \frac{1}{e^{ln(\frac{\alpha}{P}) - \Gamma \cdot t \cdot P}}\right) \tag{20}$$

where M_S, t, α, Γ and P are the same as described above and W is the Lambert W-function.

As analyzed in equation 20, the price ceiling now depends on time, which means that at any given time T the expectation at time $T+1$ is that the value of either the price ceiling or the stablecoin must be lower.

Creating a mechanism that pressures the price upwards is difficult, as there is no direct way to utilize arbitrage to move the market price towards its intended level. However, another type of price pressure mechanism can be created by utilizing a dynamic maintenance margin that changes with respect to time. If the stablecoin was undervalued the price pressure mechanism would increase the maintenance margin or β, meaning that owners would have to post additional collateral to ensure the position does not become open for other agents to close.

This article hypothesizes that this would lead to two distinct results: Firstly, collateral owners would be more inclined to redeem the underlying collateral for stablecoins because it will effectively become more expensive to sustain their leveraged positions. Secondly, some owners might not post the additional collateral in time resulting in positions becoming closed at a profit by arbitrageurs in the market. Both of these results lead to a decrease in the supply of the stablecoins in circulation while simultaneously artificially increasing demand, because agents have to buy stablecoins in order to redeem their underlying collateral. This puts an upwards pressure on the price for two reasons: firstly, the law of supply and demand would suggest that a lower supply and higher demand should lead to an increase in price, everything else equal. Secondly, every other agent knows that the maintenance margin will continue to increase as time progresses, meaning there is an expectation of an increase in price at some point in the future. This should lead to agents in the market buying stablecoins now to sell at a later date. The function that determines the β as a function of time needs to be

bounded between an original value β_0 and 1 and have a positive derivative with respect to time, equation 21 is an example of such a function.

$$\beta_t = 1 + \frac{\beta_0 - 1}{1 + t \cdot \lambda}, \quad t > 0 \tag{21}$$

where β_t is the maintenance value at time t, β_0 is the initial maintenance value, t is the time since the stablecoin was equal to or above its intended price and λ is a positive constant. The result of making the maintenance collateral dependent on time therefore creates an upwards price pressure mechanism.

6. Conclusion

Cryptocurrencies allow for the possibility to heavily impact the global economy but are currently stalled by internal issues ranging from scalability to volatility that prohibit widespread adoption. The issue of volatility is especially problematic as it exposes users to constant currency risk, which acts as a natural adoption barrier.

The introduction of a stablecoin is seen as a promising solution to the problem of volatility. The price stability is achieved through the introduction of an arbitrage enforced price ceiling and supply/demand mechanisms that always seek to pressure the price towards its intended level. However, creating, introducing and implementing a stablecoin is neither trivial or risk-free. This is especially true considering the overall lack of robustness of the stablecoin, arising from the fact that the cryptocurrencies used as collateral for the issued stablecoins are prone to extreme price swings. The result is that there will always remain a significant risk that the stablecoin will collapse and default at some given point in the future due to unforeseen exogenous events. This possible outcome is naturally detrimental to the reputation of a stablecoin, and by implication its probability of achieving widespread adoption.

While these risks are noteworthy and mean that there is no guarantee that the stablecoin can survive in the short- or long-term, there is theoretical evidence that suggests a stablecoin can solve or minimize the problem of volatility. The result is a potential improvement to the adoption of cryptocurrencies as a medium of exchange.

References

Arvicco (2016). Code is law and the quest for justice. https://ethereumclassic.github.io/blog/2016-09-09-code-is-law/. Accessed: 2017-02-17.

Bakar, N. A. and Rosbi, S. (2017). High volatility detection method using statistical process control for cryptocurrency exchange rate: A case study of bitcoin. *The International Journal of Engineering and Science*, pages 39–48.

Bitcoin.org (2016). Block headers. Accessed: 2016-09-6.

Bitcoin.Org (2017). Frequently asked questions. Accessed: 2017-04-12.

Blockchain Info (2017a). Average block size. https://blockchain.info/charts/avg-block-size. Accessed: 2017-04-13.

Blockchain Info (2017b). Average number of transactions per block. https://blockchain.info/charts/n-transactions-per-block. Accessed: 2017-02-6.

Bloomberg (2017). Fiat currency, cryptocurrency and precious metal prices. Bloomberg. Accessed: 2017-03-8.

Buford, J. F., Yu, H., and Lua, E. K. (2008). *P2P Networking and Applications*. Elsevier. Buterin, V. (2014). The search for a stable cryptocurrency. Accessed: 2017-08-10.

CME (2018). Bitcoin futures. http://www.cmegroup.com/trading/bitcoin-futures.html/. Ac-cessed: 2018-04-17.

Coin Market Cap (2016). Cryptocurrency market capitalization. Accessed: 2016-08-1. CoinDesk (2016). How bitcoin mining work. Accessed: 2016-09-13.

CryptoCoin Charts (2017). Crypto coins list. https://www.cryptocoincharts.info/coins/info. Accessed: 2017-04-12.

D'Alfonso, A., Langer, P., and Vandelis, Z. (2016). The future of cryptocurrency. http://www. economist.com/sites/default/files/the_future_of_cryptocurrency.pdf. Accessed: 2017-04-13.

Duivestein, S., Doorn, M., Manen, T., Bloem, J., and Ommeren, E. (2016). Design to disrupt. ETH Gas Station (2017). Gas prices. http://ethgasstation.info/. Accessed: 2017-03-30.

European Commission (2016). Antitrust: Regulation on interchange fees. Friedman, M. (1991). The island of stone money. *Hoover Institution*.

Gilbert, H. and Handschuh, H. (2016). Security analysis of sha-256 and sisters. *Selected Areas in Cryptography*, pages 175–193.

Hayek, F. (1990). *Denationalization of Money: The Argument Refined*. The Institute of Economic Affairs.

Hsieh, D. A. and Miller, M. H. (1990). Margin regulation and stock market volatility. *The Journal of Finance*, pages 3–29.

Kasper, D. J. (2017). Evolution of bitcoin - volatility comparisons with least developed countries' currencies. Available at SSRN: https://ssrn.com/abstract=3052207.

Keeler, P., Gobel, J., Krzesinski, A., and Taylor, P. (2016). Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. *Performance Evaluation*, pages 23–41.

Levi, M. D. (2005). *International Finance*. Routledge.

Mager, C. and Huls, C. (2017). Four blockchain use cases for banks. *FinTech Network*, pages 1–8. Mankiw, N. G. (2012). *Macroeconomics*. Worth Publishers.

Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system. *Bitcoin.org*.

Nasdaq (2015). Debit card tatistics. http://www.nasdaq.com/article/ debit-card-statistics-cm543408. Accessed: 2017-02-6.

Nigam, A. (2016). Emerging challenges and issues peer to peer cryptocurrency payment system with special focus on bitcoin. *International Journal of Languages, Education and Social Sciences*.

Oxford Dictionary (2016). Definition of a cryptocurrency. Accessed: 2016-09-13. Poloniex (2017). Cryptocurrency prices. https://poloniex.com/. Accessed: 2017-03-8.

Popper, N. (2016). A venture fund with plenty of virtual capital, but no capitalist. Accessed: 2017-04-07.

Scott, A. (2016). These are the world's top 10 bitcoin-friendly countries. https://news.bitcoin. com/worlds-top-10-bitcoin-friendly-countries/. Accessed: 2017-04-20.

Smith, C. J. W., Nance, D. R., and Smithson, C. R. (1993). On the determinants of corporate hedging. *The Journal of Finance*, pages 267–283.

Stallings, W. (1999). *Cryptography and Network Security: Principles and Practice*. Prentice Hall.

Tapscott, D. and Tapscott, A. (2016). Here's why blockchains will change the world. http://fortune.com/2016/05/08/why-blockchains-will-change-the-world/. Accessed: 2017-04-12.

Thaler, R. H., Tversky, A., Kahneman, D., and Schwartz, A. (1997). The effect of myopia and loss aversion on risk taking: An experimental test. *Q J Econ*, pages 647–661.

The Bitcoin Volatility Index (2016). The bitcoin volatility index. https://btcvol.info/. Accessed: 2016-09-1.

The Economist Editor (2014). The great hiccup. *The Economist*.

The World Bank (2014). Global findex (global financial inclusion database). http://databank. worldbank.org/data/reports.aspx?source=1228\#. Accessed: 2016-02-1.

The World Bank (2017). Remittance prices worldwide. https://remittanceprices. worldbank.org/ en/corridor/United-States/Pakistan. Accessed: 2016-08-30.

White, L. (2017). Dollar-denominated cryptocurrencies: Flops and tethered success. Accessed: 2017-08-10.