Spring 5-2-2018

Bitcoin, Blockchain and Trust

Quentin Rene Marcel Rosso

Bitcoin, Blockchain and Trust

A Capstone Project Submitted in Partial Fulfillment of the
Requirements of the Renée Crown University Honors Program at
Syracuse University

Quentin Rene Marcel Rosso

Candidate for Bachelor of Science
and Renée Crown University Honors
Spring 2018

Honors Capstone Project in Finance and Political Philosophy

Capstone Project Advisor: _____
Prof. Raja Velu

Capstone Project Reader: _____
Prof. Linda D. Hartsock

Honors Director: _____
Chris Johnson, Interim Director

Abstract

In the past few months, there has been an incredible craze about Bitcoins and Blockchain. Prices skyrocketed, and trading platforms emerged very quickly. This new cryptocurrency economy has been compared to the more traditional economy which has been shaken by many crises in the past twenty years. Crises arise when trust collapses. With a mix of interpersonal and institutional trust, our financial system and its institutions are considered obsolete. We are repeating the same mistakes over and over again. Bitcoin will fix our current economy by providing three new elements of Trust: (1) Decentralized architecture and governance neutrality based on consensus protocols (2) Transparency of the algorithms (3) Unbreakable Underlying Technologies. Computational trust provides answers to questions that have been raised since 2008 and help avoid fraud and any potential breach of trust.

However, Bitcoins has its limits and is highly volatile. By proving the market inefficiency, the specific relationships between the different exchanges and showing potential arbitrage opportunities with respectively an autocorrelation analysis, a volatility spillover analysis and a co-integration analysis, one will understand how this Bitcoin's "wild west" can only reach maturity if and if only, regulations come into the Bitcoin the market.

Executive Summary

Our current financial system has a systemic trust issue. Two models of trust currently exist: interpersonal trust and institutional trust. Interpersonal trust corresponds to our daily interactions with other human beings. Trust results from habit and predictability. Institutional trust relies on organizations and protects individuals from the risks of moral hazard. In finance, it is expressed with the trust in trade: savings in transaction costs, a shift in the role of information and value creation.

Blockchain might solve the trust problems. To define Blockchain, one need to imagine a very large notebook, that everyone can read freely, on which everyone can write, impossible to erase and indestructible. Bitcoin relies on this technology. Bitcoin allows people to transfer funds between each other separate from a central authority. However, Bitcoins might also have trust related issues that might negatively influence the current financial system.

Over the last six years, we analyzed daily Bitcoin prices from five different exchanges. Utilizing Yang Zhang volatility, returns measure, autocorrelation, volatility spillovers and co-integration, we assess the efficiency of the market and the potential opportunities of arbitrage between the different Bitcoin exchanges. Arbitrage opportunities exist and some exchanges such as Coinbase have a higher level of trust from investors than other exchanges. Taking Bitcoins out of Coinbase and Bitstamp and investing in IBIT could be profitable. Thus, Blockchain might solve existing trust related issues in the current financial system but is not regulated enough to remove any potential mistrust toward the exchanges holding the coins. Current trust issues provide arbitrage opportunities that might be subjects for further research papers.

Table of Contents

Acknowledgements

Special thanks to my advisor Prof. Raja Velu, my reader Prof. Linda D. Hartsock, and Li Fu for helping on this research. Thank you for having being part of this very fast paced adventure for my final semester. Thank you for your patience. Working on this Capstone allowed me to do the thing I love the most: cross-disciplinary research between Philosophy, Economy, Finance and Engineering. Especially on the Financial side of the Capstone, Prof. Raja Velu has been incredibly helpful. I learned a tremendous amount of knowledge in such a short period of time. All the skills I learned in this Capstone will help me to write a book about Trust and its significance not only in Finance but in many fields today. Thank you for everyone who have helped me on this initial journey. This is only the beginning.

Chapter 1: The Role of Trust in the Financial System

Section 1: From Interpersonal Trust to Institutional Trust

It is widely known that trust is usually used to describe “reliance on the character, ability, strength, or truth of someone or something” (Webster, 2018). People we trust are people who are “well known” to us, people we have known for a long time, with whom we share similar experiences. We feel a connection, and attachment to them. We know, or we feel more or less vaguely what such a person is capable of, what are his or her inclinations, his or her ways of seeing and doing. No doubt this knowledge sometimes leads us to show mistrust rather than trust. Even if one term is the opposite of the other, the fundamental principle remains the same: It is a matter of deciding what this or that person will say or do, given what we see him or her saying or doing right now or in a near future. Between human beings, trust is the result of a habit and predictability. Uncertainty is avoided, and trust presents itself as an immediate assurance without questioning or doubt. It then seems trust affects positively our *ratio* (reason in Latin). However, it is impossible to assimilate trust as a potential foundation for any reasoning.

Actions of questioning, reasoning and verifications are lacking in the case of inter-personal trust. Thus, trust is not based on any fundamental facts. Trust exists only thanks to the existence of uncertainty. Does it really deserve the name of trust? The answer is not easy, because on one hand the uncertainty does exist, insofar as it is perfectly possible for the person to be trusted to do anything other than what was expected of him or her. On the other hand, this uncertainty is not at all conscious in the one who "trusts" the mere habit. Therefore, perhaps this attitude deserves the name of mere opinion or pseudo-knowledge. Defined as *doxa* in *The Republic* of Plato, opinions are opposed to science and its underlying facts. Hypothetically, trust

would be apparent to an opinion. Fascinating enough, trust is a necessary condition to the exchange and acquisition of knowledge. Knowledge is defined as “the range of one's information or understanding” (Webster, Knowledge | Definition of Knowledge, 2017). Scientific knowledge, moral knowledge and almost all knowledge in fact “depends for its acquisition on trust in the testimony of others” (McLeod, 2015). Consequently, the creation of trust only happens by the acquisition of knowledge from others through the use of our senses. Then, trust is a main medium to empower and accelerate the exchange of knowledge between individuals.

What is central to the definition of interpersonal trust might not have the same importance in the case of institutional trust. The typologies on trust fit, for the most part, in the framework defined by Zucker. It distinguishes three forms of trust: interpersonal trust, inter-organizational trust and institutional trust. According to Zucker, “the economy at its origin was shaped by mechanisms, including new organizations, designed to rebuild, to produce trust” (Zucker, 1985, p. 3). Interpersonal trust is not sufficient enough to build a solid trust framework in our economy. However, interpersonal still plays an important role in the cooperation between economic actors and the economic exchanges. For instance, the benefits of trust in trade are the following:

1. Savings in transaction costs: Transaction costs are defined as “the costs associated with the transfer, capture, and protection of rights” (Yoram, 1997). To reduce transaction costs, trust makes it easier for economic and financial actors to exchange by reducing funds allocated for negotiation purposes, monitoring and enforcement.
2. A shift in the role of information: The degree of proximity of interpersonal relations does influence the quality and quantity of information exchanged between the individuals.

3. Value creation: The cornerstone of any economic transaction increases proportionally to the amount of trust between the economic actors. The actors are committed to act for a common good.

Institutional trust is an authority in itself. Institutional trust protects individuals from the risks of moral hazard. Trust is then understood as a common factor shared between individuals through social mediums. Zucker explains the institutional side of trust by highlighting two specific characteristics: inter-subjectivity and objectivity. In the process of reconstruction of trust called institutionalization, Zucker states that “the process of redefining acts as exterior when intersubjective understanding causes them to be seen as part of the external world and objective when they are repeatable by others without changing the common understanding of the acts” (Zucker, 1985, p. 11). This independence of both people and the specific context of their action guarantees also its objectivity.

Section 2: The Role and Limits of Trust in our Current Financial System

"Trust is the lubrication that makes it possible for organizations to work", said Warren Bennis. In 2000, Wall Street faced the bursting of the Internet Bubble, the internet economy in which the whole investing community invested billions of dollars and was ready to invest billions more. The exuberant optimism disappeared, the market crashed. However, the real trust crisis and most serious one, began at the end of 2001 at the time of the revelations about the fraudulent accounting practices of Enron. The scandals that followed, from Tyco to WorldCom, led to massive sales of shares. The damage has been done and mistrust was reigning in the US and European markets. Fraud, fake accounts and corrupted financial transactions created a major trust crisis that still persist today. Asymmetry of information is part of the financial game and applies to any financial markets. The company issuing stocks has a better understanding of the yield opportunities than the money lender. Several solutions exist to limit the effects of asymmetry of information. Building trust is an inherently human behavior. In an economic perspective, the economic agent is taking the risk of seeing the trustee failing. In order to avoid a potential disappointment, the trustor might monitor the trustee in ways both the trustee and the trustor will end up losing their common trust. Following this paradox, one would understand that the trustee is always placed on a very sensitive balance swinging between trustworthiness and untrustworthiness. "Because trust is risky, the question of when it is warranted is of particular importance" (McLeod, 2015).

As explained in Section 1, trust alone is never enough and should be improved by rules. One of the most successful form of cooperation is trade, defined as "the action of buying and selling goods and services" (Oxford). Trade cannot exist without trust at its core and "it is very

difficult to trust strangers" (Harari, 2011, p. 36). In order to enable trust between strangers, "fictional entities" (Harari, 2011, p. 36) have been created (i.e. Federal Reserve Bank, dollar…). These "fictional entities" create rules to enhance mutual trust and improve the flow of transactions. These rules are often simple codifications of human behaviors and lay down the foundations of both of our political and financial institutions. Nevertheless, these rules suffer from insufficiencies and failures diminishing their scope. Rules exist because they tend to "reduce the costs involved in face-to-face personal influence" (McLeod, 2015). However, applying these rules and enforcing them tend to be very costly. Complexity comes into place when a third party needs to be brought around the table in order to certify the rule. Transgressing the rules follows a very rational behavior where the individual will "evaluate the benefit of transgression against the cost of norm compliance" (McLeod, 2015). The one with the highest expected utility will be chosen. Finally, these rules become partially obsolete as soon as significant technical progress calls into question the functioning of the system. Rules are not the perfect safeguards of trust in markets. We cannot avoid crisis.

Crises arise when trust collapses. This "time of intense difficulty or danger" (Dictionaries, n.d.) (*krisis* in Greek) marks a turning point in a society and the life of its people. According to Ramon C. Reyes, a crisis is a "moment of critique" (Reyes, 1986) in which a "man tries to gain or re-gain understanding of the fundamental assumptions underlying his community's manner of living" (Reyes, 1986). These fundamental assumptions can be understood as the natural aspects of their lives human beings can trust and believe in. They are part of our human nature and enable our natural tendency to trust our close relatives. Consequently, even in a time of crises, human beings are still looking to trust something.

However, because of the underlying nature of trust, the way people trust never fundamentally changed and crisis repeat over and over again with always the same origins. We understand that the ups and downs of the markets are as old as the existence of financial capitalism. "Fraud is the ultimate expression of unenlightened self-interest in comparison to self-interest that is enlightened by benevolence" (Whalen & Feldkamp, 2014) explain Frederick L. Feldkamp and R. Christopher Whalen in the summary of their book "Financial Stability: Fraud, Confidence, and the Wealth of Nations". Financial statements are often affected by several excesses: debt, asset valuation, executive compensation … As long as trust exists, some individuals will transgress the rules in order to enrich themselves or improve their position. However, illegal behaviors are not the only dangers to trust in the financial markets.

"Risk comes from not knowing what you are doing" wrote Warrant Buffet. Beyond illegal actions, trust in financial markets can be undermined by the fact the players don't give the same meaning to the market signals. In financial markets, the selection of a security is not based on its intrinsic value and is far from the book value of the company. Intrinsic value is defined as the value of a company determined through fundamental analysis without reference to its market value. The price is not influenced by the quantity of potential buyers or the expectations of the economic actors in terms of how the company will perform in the future. In its general Theory of Employment, Interest and Money (1936), Keynes gives the "beauty contest" metaphor. In a London newspaper at the time, UK readers were selecting the most beautiful women among the hundreds published photographs. The winner was the one whose choice was the closest to the majority choice. To win this game, it is unnecessary to think about your own tastes but to think about other tastes instead. Applied to the financial markets, this means that stock selection is

based on their market value instead of being based on the actual performance of the company. Markets are inefficient. Even if agents believe the market is mistaken, they might want to stay in the game to follow the trend of exponential trust into a bubble in order later on to sell before the market reaches its momentum and the stocks pick, once trust starts to collapse. However, things go wrong when the bubble starts to burst. Market operators, knowing the rules of the game in which they participate, withdraw quickly. Better, they take advantage of the fall that, from now on, they anticipate, covering themselves with derivatives. It is not the same for small shareholders, late in the game of speculation and often react with a delay. Disappointed with not having understood the rules of the game and, especially, having suffered real losses, abandon the financial markets which contributes to their turnaround which then make the market operators suffer themselves. The existence of speculative bubbles results from the mimetic behavior of agents and the self-fulfilling power of their beliefs. These two characteristics of the financial markets explain why the price of an asset can sustainably deviate from its fundamental value.

We have explained how trust is built and why it collapses. We spoke about the rules that tend to try to limit excessive behaviors. However, we might need to understand the importance of the regulatory agencies and other governmental. Again, quoting the talented Yuval Noah Harari seems to be necessary in order to remind ourselves of the fundamentals of trust. “the most universal and most efficient system of mutual trust ever devised” (Harari, 2011, p. 157). In page 159 of “Sapiens: A Brief History of Humankind”, Harari continues his theory by stating that “total strangers could easily agree on the worth of a Roman denarius coin, because they trusted the power and integrity of the Roman emperor, whose name and picture adorned it” (Harari, 2011, p. 159). Money is a medium of trust. For its power to be trusted, people have to trust a

socially established organization codified by rules making it stable and guaranteeing safety of its members. Today, the issuance of money by central banks guaranties the adoption of this system of mutual trust. For the purpose of our research, we will call this model, the centralized trust system where a single third party guaranties the validity and the value of the transaction.

One specific case we might be interested is the role of this centralized institution. In the case of the financial markets, the public authorities play the role of trust safeguard by preventing excesses. They are set up as regulators of the market. In 1933, the Securities and Exchange Commission (SEC) was created and has been duplicated in most countries since. Every crisis had the consequence of increase the power the SEC by tightening regulations. In the 2000s, President Bush gave the SEC important budget extensions in order to strengthen its powers. The Senate also passed a bill on accounting procedures that created a supervisory commission to set standards and conduct inspections. Severe penalties (up to 20 years in prison) for business were established for leaders guilty of fraud on the accounts of their company. Yet all the precautions seemed to have been taken. In the Enron affair, and outside of the company's management, the accounting firm Andersen, which certifies the group's accounts is the main defendant. At the end of the last annual report published by Enron in the spring of 2001, Andersen makes two comments. The first attests to the quality of the internal accounting of the company “able to provide reliable documents”. The second states that the reports “honestly present, in all their material aspects, the financial situation”. A few weeks before the publication of this document, on February 5, 2001, at an internal meeting, Andersen's partners and executives had discussed Enron's suspicious accounting practices and questioned the risk of retaining a such customer.

While certifying Enron's balance sheets, the firm was contracting lucrative consulting contracts with the same company. In 2001, Andersen received $ 25 million from Enron, his second client, for checking his accounts and $ 27 million for advising it. By announcing on November 8, a revaluation down nearly 600 million dollars of its results since 1997, the energy group revealed its mistakes and those of its auditor. The latter not only showed incompetence, but perhaps also complicity. He acknowledged January 10, 2002 having destroyed in October and November 2001 accounting documents related to this case after the opening of an investigation by the SEC. Accounting records were also destroyed, this time in December 2001 and January 2002, at Enron headquarters itself by its own employees. In this case, the accountability was obvious, trust was broken, and their acts were considered morally wrong. However, according to a "Report to the Nations on Occupational Fraud and Abuse" quoted by CNBC, "auditors detected just 3 percent of the fraud cases reported last year [2013], compared to 7 percent uncovered by accident" (Cohn, 2014). Most financial crimes go unnoticed and most of the financial actors end up not being considered accountable. Accountability is considered as "the fact or condition of being accountable" (Oxford, n.d.) And having moral responsibility.

In order to resolve this problem of accountability and ultimately reduce financial frauds, the Sarbanes-Oxley SOX passed in July 2012. The Act's stated purpose is "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes" (Scott, 2004, p. 2). In order to guarantee trust in the financial markets, it requires the Presidents of companies listed in the United States to certify their accounts with the SEC. Three different principles are defined by the law: accuracy and availability of information, the direct responsibility of the leaders and auditor independence. All

of these principles have a significant impact on the development of trust between the different financial actors. First, enforcing the accuracy and availability of information aims at reducing the asymmetry of information and uncovering potential fraudulent acts. The exactness and availability of the information is highly important to guarantee trust and all of the information should be provided to the SEC. Second, enforcing a direct responsibility of the leaders of the organization brings our concept of inter-personal trust to reinforce institutional trust. Direct responsibility of the directors (CEO and CFO) is on the table. In case of irregularities the leaders risk 20 years of prison. In order to monitor the potential "material violations of the securities laws by the corporation or its agents", lawyers are required to report breaches of fiduciary duties. A fiduciary duty is defined as a "'breach of fiduciary or similar duty recognized under an applicable federal or state statute or at common law', including, but not limited to, misfeasance, non feasance, abdication of duty, abuse of trust, and approval of unlawful transactions." (Mitchell, 2003, p. 1205). Third, the legislation enforces the existence of external auditors authorized to receive information or complaints from either shareholders or employees. Similarly, to the lawyers, they play the role of agents of trust. The auditors should be also frequently changed in order to guarantee their independence.

Thanks to this new legislation aiming at restoring investors' trust into corporate governance, "it has brought corporate governance and responsibility even further into the spotlight" (Scott, 2004, p. 2). However, according to a PwC survey only "35% of company executives think the law will help restore investor confidence in capital markets" (Scott, 2004, p. 2). Other factors start emerging as factors of trust when making investing decisions. Disclosing

social and environmental information are critical to help investors and the public determine whether or not a firm is “ethical, responsible, credible and trustworthy” (Scott, 2004, p. 2).

When a massive breach of trust occurs, there is a risk of systemic mistrust spreading light-speed. A serious breach of trust in the financial markets has been with the fall of Lehman Brothers in 2008. As most of us know, the financial crisis of 2007 began after the bursting of a bubble of the real estate market full of subprime credit agreements to low-income households. Lehman Brothers got hit very hard and did not find the enough funds to refinance its colossal losses. On September 15, 2008, Lehman Brothers declared bankruptcy. Considered too big to fail, the fall of this titan aggravated an already delicate situation by promoting contagion to the entire banking system. In addition, the bankruptcy generated a problem of mistrust that has spread very quickly. The markets were wary of the banks and they stopped lending to each other overnight. This problem was highly critical because, in order for the financial system to function properly, it is necessary for the agents to put trust into the future and especially into each other. Ben Bernanke (president of the Fed) did not rescue Lehman Brothers to fight against moral hazard. Indeed, when economic agents know for a fact that they will be saved in any case, they take more risks and thus increase the probability of financial crises occurring. This situation shows how a breach of trust between two important financial actors can lead to total undermining of trust in the markets. Mistrust spread faster than trust gets built.

Both our rules and institutions face challenges in a more and more complex financial environment plagued by the existence of speculative bubbles resulting from the mimetic behavior of agents and the self-fulfilling power of their beliefs. The time of the financial markets is much shorter: The suspicion of one company weighs on all the others. This is maybe why in

2002, the SEC “approved a final rule that changed the deadlines for Form 10-K and Form 10-Q for ‘accelerated filers’” (SEC, n.d.). But the choice between the rule, heavy and slow, and trust, flexible and fast, remains unresolved. Our financial system needs a new architecture of trust.

Section 3: Trust and Technology

Asking the question about the trustworthiness of the financial system is also asking the same question about the engine of finance: technology. Technology in finance connects all the economic agents together. Whether these are direct consumers, banks or watchdogs, technology powers our current financial system. Trust is built through technological protocols and algorithms characterized by their predictability, reliability and transparency. Of course, these characteristics can change according to the technologies involved during a financial transaction. As a support to institutionalized trust, technology provide the means to fulfill the two specific characteristics defined by Zucker as inter-subjectivity and objectivity. According to the main point discussed in Chapter 1, independence of both people and the specific context of their action guarantees also its objectivity. This institutional trust protects individuals from the risks of moral hazard. The same goes with technology. Thanks to its predictability, individuals can expect actions to happen without any human interaction. Neutral automation happens only following a certain protocol known by the stakeholders involved in a transaction. In order, to make this protocol available, transparency is essential to allow people to trust the technology itself and have safe expectations about the outcome. Then, thanks to both these factors, another essential component in the trust equation is created: reliability, or in other words, the quality of being trustworthy and performing consistently well. The process and the outcomes are perfectly known. Trust is created.

Of course, most of the technologies we interact with today and especially the ones freely available on internet bring a mix of institutional, interpersonal and technological trust. For instance, an individual would like to trade on Robinhood. Being an open, free-to-use and easily accessible platform, Robinhood brings all of these three branches of trust together. First, interpersonal trust is probably the most obvious one. We have all probably heard about this application from a friend. The trust given to an online actor is proportional to the percentage of individuals using this app. This idea relates to the shift in the role of information defined earlier in the research. The degree of proximity of interpersonal relations influences the quality and quantity of information exchanged between the individuals. Second, institutionalized trust is built due to the legitimacy of Robinhood as a trading platform. Third, even if the user does not have access to full information about how the technology and algorithms work, the complexity is reduced by a user experience making the user comfortable in any actions on the software. Reducing complexity is also a way to increase trust into a system. However, as explained by Bhaskar Chakravorti, "the public may be losing trust in technology" (Chakravorti, 2018). In his mind, consumers are learning to be worried about the security of their personal information: "News about a data breach involving 57 million Uber accounts follows on top of reports of a breach of the 145.5 million consumer data records on Equifax and every Yahoo account – 3 billion in all" (Chakravorti, 2018). Companies need to invest un trust-building technology systems.

Chapter 2: A New Architecture of Trust
Section 1: The Blockchain, at the Heart of the Technology

> *"I'm reasonably confident … that the Blockchain will change a great deal of financial practice and exchange,… 40 years from now, Blockchain and all that followed from it will figure more prominently in that story than will Bitcoin."*
>
> Larry Summers, US Former Treasury Secretary (Guarda, 2016)

The Bitcoin network operates completely autonomously. Everything relies entirely on its users and their computers computing power made available to the system. The main principle of Bitcoin is to keep up to date on a very large number of computers - called nodes, distributed across the network - a set of public and tamper-proof registries of all transactions carried out since the system exists. These registers are synchronized across the network and operate according to the model of the Blockchain. The Blockchain is at the heart of the cryptocurrency model. To fully understand the Blockchain, the French mathematician Jean-Paul Delahaye synthesizes it as follows: Imagine "a very large notebook, that everyone can read freely, on which everyone can write, impossible to erase and indestructible. We immediately think of a large accounting book, with digital data, but without manual records and where exchanges are happening automatically between participants of a large peer-to-peer network on internet" (Abiteboul, 2016).

Following the previous arguments about technology and trust, one might question the trustworthiness of this technology. Blockchain relies on three different principles of trust. These different principles are also thoroughly discussed across the next sections of the research: (1)

Decentralized architecture and governance neutrality based on consensus protocols: The Blockchain relies on a very large quantity and diversity of independent contributors and is decentralized by nature. Unlike a centralized architecture where decisions can be made unilaterally, reaching a consensus will have an effect on the system. Thus, any change in governance rules must first be approved by a consensus of the majority of the contributors, who will then execute the code. (2) Transparency of the algorithms: Any transaction, any block, any rule of governance is freely accessible and readable by everyone; as such, anyone can audit the system to ensure the proper operation of the Blockchain and the legitimacy of transactions. The advantage is to allow experts from the user community to scan the code and alert if there is suspicion. Trust is built by whistleblowers. (3) Unbreakable Underlying Technologies: Cryptographic techniques and usage patterns ensure that the Blockchain cannot be tampered with, that the transactions entered are authentic even if they are issued under full anonymity, and finally that the security of the Blockchain is able to keep up with technological developments thanks to adaptive security levels.

When we want to send money through the internet, trust between the sender and the receiver is non-existent. Consequently, we rely on trusted intermediaries: PayPal, Venmo, Banks, etc… Blockchain eliminates the need for trust. We do not need to trust the intermediaries, or any stakeholder involved in the transaction. We trust the technology and replace the need for trust with the need for proof safely and transparently provided by the Blockchain. Any transaction is recorded and built upon the previous one (as blocks) and validated by other network users. Except if someone successfully captured 51% of the network, the safety of the network is guaranteed. The transaction certification normally guaranteed by the banks is now guaranteed by

the whole network. For a long time, virtual currencies have faced a core problem: we could not validate the transaction. The transaction could be duplicated. With the Blockchain, this problem has been solved. For Blockchain, the database is decentralized. Everyone owns a copy of the network which is constantly updated. Thus, it becomes very hard to cheat. This fraud would be detected by other members in the network. The transaction would not go through. More the network increases, less trust is needed.

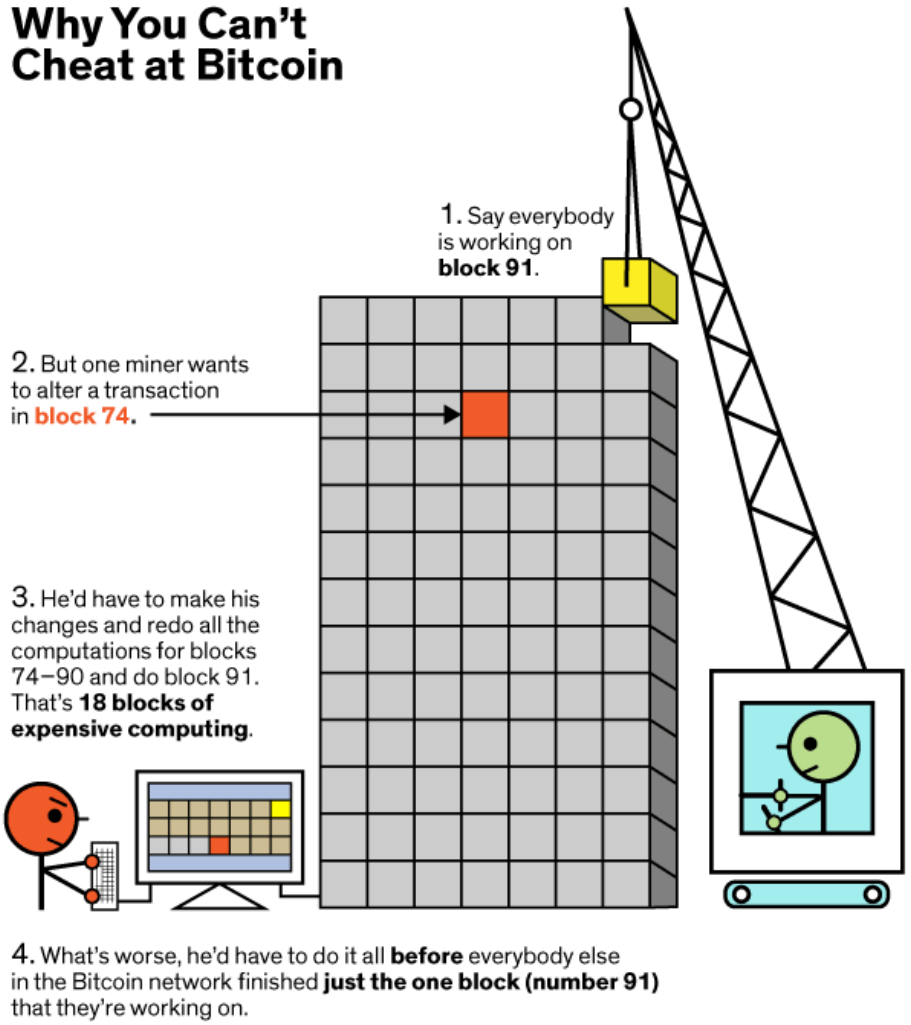
Others describe it as an information storage and transmission technology, with transaction validation mechanisms associated with value exchanges (monetary or otherwise). Unlike the Internet with TCP / IP, the digital data transport protocol, the Blockchain represents the Internet of value, with a more advanced protocol based on a distributed consensus to validate and record transactions. This is ultimately a big database that it is both transparent (everyone can see all the exchanges, present and past), decentralized (without a control body or trusted third party, it is based on peer-to-peer exchanges), unfalsifiable and secure (unlike more traditional databases, it is distributed, ie different copies exist simultaneously on different computers called nodes of the network, what to avoid that it is hacked).

After having understood the fundamental aspects of trust and its influence on human economic behaviors, it will be interesting to first see how the shift of institutional trust system to a purely computational trust paradigm influence our financial and economic behaviors. In this case, it will be interesting to focus on the utilization of the Blockchain (and potentially the Bitcoin as a cryptocurrency) and its implication in trusting financial institution. Computational trust is the creation of trusted authorities through the use of cryptography. In computer science, applications have historically moved from centralized systems to decentralized system. Our economy is at the image of this software and is rapidly shifting to a new decentralized paradigm.

Pablo R. Velasco has been of the first political philosopher to look at this shift in his "Computing Ledgers and the Political Ontology of the Block-chain". He explains that with Blockchains, "Authority is displaced from the institutional actors in the system to the instrumental control of trust by the software" (Velasco, 2017). Velasco then considers that Blockchain is not "inherently political" (Velasco, 2017) and that the software protocols have properties normally given to institutions and governments: "control, trust, and authority" (Velasco, 2017). For Velasco, an object can have political properties in two ways: inherent and non-inherent. With the inherent property, the "systems require a certain kind of political relationships that 'are strongly, perhaps unavoidably, linked to a particular institutionalized pattern of power and authority" (Velasco, 2017). The use of the system is initiated with a certain ideology in mind. It can be adopted with a certain "pattern of power or authority" (Velasco, 2017). One of his main observation is that intangible social goods (which are normally made by human beings for human beings) are being now generated by computational systems" (Velasco, 2017). Today, states and banks have control and the power to create different financial instruments. With Blockchain, this might reduce the power of these institutions. A shift in the way we trust also implies a shift in the way we exchange value. In a TED talk, Bettina Warburg starts her presentation by stating a fundamental fact about Blockchain: Tt changes how we exchange value. However, in her mind, this change is not new and is a "continuation of a very human story" (Warburg, 2016). On one hand, we always try to increase our trust, lower our uncertainty. On the other hand, we also try to completely remove the need for trust from our existing systems. She confirms what we have seen in the previous chapter: "we built up more formal institutions, institutions like banks for currency, governments, corporations" (Warburg, 2016). She then finishes her talk with a brilliant observation stating that by collapsing our institutions we try to convert "a lot of our uncertainties

into certainties" (Warburg, 2016). On this last sentence, one might see a connection with the financial markets and the constant need of transparency to avoid fraud or other harmful actions going against the general will.

***Figure 1**: Why it is Impossible to Cheat at Bitcoin (Services, n.d.)*

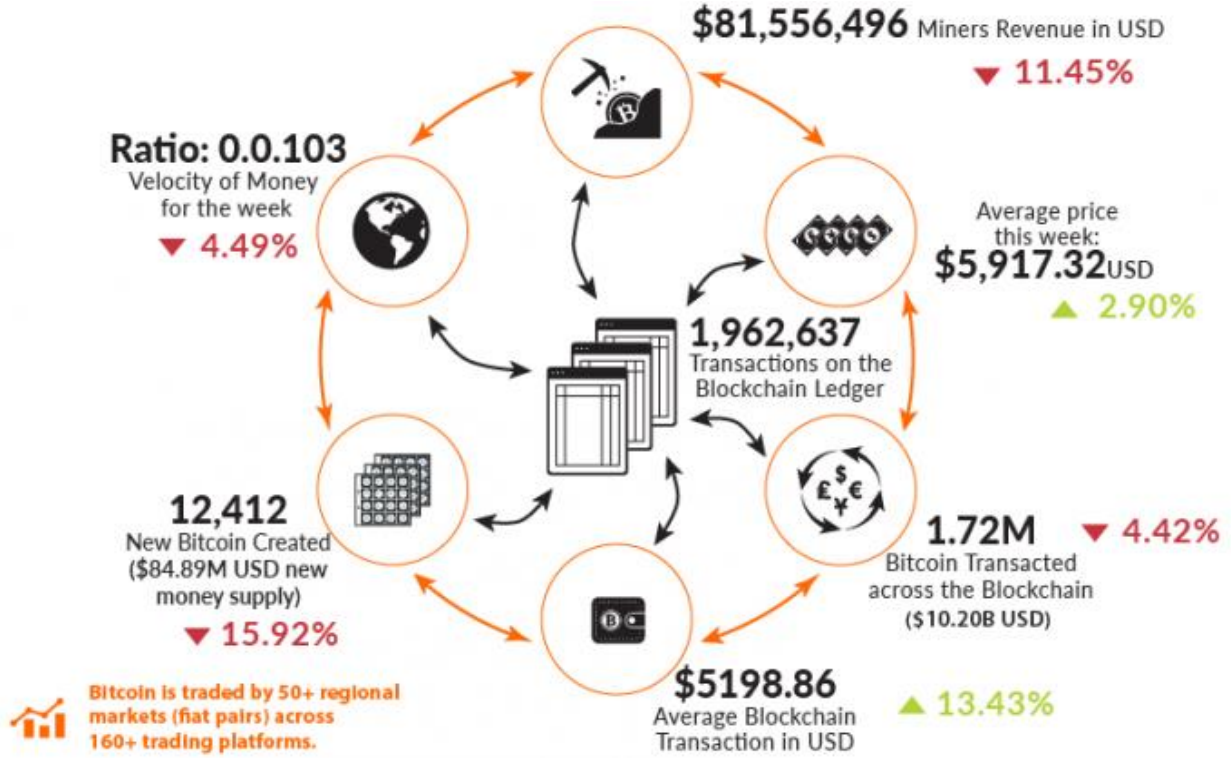


Section 2: Presentation of the Bitcoin and How It Works

From 2009 to 2015, Bitcoin has served approximately “62.5 million transactions between 109 million accounts” (Rainer Böhme, 2015). Bitcoin has been around since 2009 but did not take off before mid-2012. It then traded between $5 and $10, and the number of transactions made per day did not even reach 10,000. During the year 2013, the system was the victim of several hacks and the number of transactions has more than once been in free fall. However, at the end of 2014, the overall number of transactions per day was reaching 50,000 a day, and Bitcoin traded then for just over $1,000. While this impressive growth was happening, the very popular Chinese search engine Baidu announced that they were now accepting payments in Bitcoin, and several hearings held in the US Congress on the subject of Bitcoin were rather favorable. The Central Bank of the People's Republic of China, however, banned Chinese financial institutions from using Bitcoin in December 2013. This decision had the effect of lowering the price of Bitcoin and limiting transactions. Even today, some services offered by Baidu are not payable in Bitcoin. At the end of 2014, following the fall of one of the major trading platforms, Mt. Gox, Bitcoin traded for $383. Several states are beginning to think about various forms of regulation to try to control the exchanges and transactions within the Bitcoin system. Among other things, it is a question of considering Bitcoin as a taxable asset and of regulating exchanges made in Bitcoin. There is also a question of subjecting the exchange platforms to anti-money laundering laws and the requirements of the fight against terrorism.

This following figure makes it possible to better understand the reality of this digital currency:

***Figure 2**: Bitcoin statistics for the week ending November 1st, 2017. (Sedgwick, 2017)*



Bitcoin has been described by its users as the very first implementation of the cryptocurrency concept. Cryptocurrencies are currencies that use the cryptography system to validate transactions and generate the currency. They are therefore digital and decentralized currencies. In the spirit of cryptology, cryptography makes it possible to send messages by protecting them with keys, generated using mathematical algorithms. Only people with the keys specific to the message sent can decode it and have access to it. In fact, each user of Bitcoin has a digital wallet called "wallet", which assigns an address to the user in the form of public key which has the role of being shared to other users wishing to trade with this user. A private key is also assigned and is kept secret. These two keys are used during transactions to encode and decode the messages, thus guaranteeing the confidentiality of the information exchanged. When

sending a message, the sender uses the public key of the recipient to encode the message. Only the recipient, using the corresponding private key, can then decode it. In a similar fashion, the sender can also use his private key to encode the message, and the recipient will then use the corresponding public key to decode it. This digital signature system thus makes it possible to authenticate the author of the message and its recipient, as well as to protect its confidentiality. All Bitcoin operations are based on this public and private key cryptography system.

An example makes it easy to understand this operation. Imagine a user A who wants to send 5 BTC to a user B. The transaction then takes the form of a file, created by the wallet of the user A, and is published on the network. This file contains several elements. First, the two keys needed to identify the users A and B involved in the transaction, depending on whether the message will be signed or encrypted; the content of the transaction itself, namely the 5 BTCs; and finally, the references of the previous transactions of the user A, which thus make it possible to ensure that he actually owns these 5 BTCs. Finally, the entire file is signed or encrypted thanks to the selected key of the user A. In this way the authenticity of the message as well as the identities of users are preserved.

Bitcoin is definitely a potential alternative to a centralized trust system especially when it comes to financial and monetary transactions. It actually removes the need for trust. How does it achieve this goal? It does it with the help of the Blockchain technology.

Section 3: Mining, an activity essential for the proper functioning of the entire network

Mining, for its part, is an activity that requires a strong use of computer hardware to run a cryptographic algorithm to confirm the transaction blocks and ensure the security of the network. The execution of these algorithms is very expensive in hardware and also in energy. This is why it happens that the miners are grouped together, they then form a pool, to divide the work and thus the material and energy costs especially of this activity. A miner can, however, undermine alone. "Mining" therefore means running a certain algorithm - the SHA-256 - many times until it finds a result that proves that it has found a block, according to some criteria specific to the Bitcoin system. Most often the miner must run this algorithm several billion times per second for several minutes before finding a block. When executed, the SHA-256 produces a more or less random string of characters that is called a hash.

An example of hash could be:

6b1f6fde5ae60b2fe1bfe50677434c88.

Finding a block is like finding the hash that starts with a number of zeros. To do this, the miners execute the algorithm by adding an increment, which they increase each cycle, until they find the right hash. An example allows to better understand this operation: First let's take a random string of characters, for example "Bitcoin is amazing!".

By applying the SHA-256 algorithm to this character string, we obtain as a result the following hash: 66925f1da83c54354da73d81e013974d. But this hash does not start with zero. So we reapply the algorithm to the string, adding this time an increment: " Bitcoin is amazing!-1", " Bitcoin is amazing!-2", etc., until finding a hash that begins with a zero. The first hash starting

with zero is obtained with the seventh increment, " Bitcoin is amazing!-7", which actually gives as 0fe46518541f4739613b9ce29ecea6b6.

In this example, seven attempts were needed to find a hash that starts with a zero. In reality, billions of tests are needed for miners to find a hash that starts with the correct number of zeros. Once the good hash has been found, the miner sends it to all nodes in the network that check this result and adds it to their block chain. The mining activity requires equipment allowing a very high computing power which makes it a very competitive activity. The miners therefore have every interest to equip themselves as well as possible to mine as quickly as possible before the others. Then, because the SHA-256 algorithm requires a lot of computing resources. It is today for example impossible to undermine with a simple PC. For comparison, the tools miners work today can average around 400,000 MH / s (four hundred thousand million hash per second), and can soon reach 1,500,000 MH / s , while a regular computer has an average power of 100 MH / s.

A high computing power is necessary for the security of the Bitcoin network. Indeed, to be able to insert fraudulent transactions in the block chain, a fraudulent miner should be able to collect more than half of the total power of the network. This fact is known as the 51% rule. It would have to have 51% of the power of the network, which is virtually impossible. Since mining is an activity that requires time and, above all, a lot of energy and investment, the miners receive remuneration from the network. For this they must provide proof of their work and resources used. This point is very important in the Bitcoin system, because if the miners were not remunerated they would have no incentive to invest so much in such computing powers, to

ensure the proper functioning and security of the network. The miners' pay is done in fractions of newly created Bitcoins, and is the only way to create new Bitcoins. This creation of money is transparent, since everyone can know how many new Bitcoins have been created based on validated blocks, and ensures the proper functioning of the network. Thanks to this system, the Bitcoin network can function without an entity that plays the role of a central bank.

An essential point to note is that the reward, or remuneration, of miners is not fixed. As the number of validated blocks increases, the remuneration of the mining activities decreases. It is halved every 210,000 blocks found, and this for one simple reason: the total sum of Bitcoins is limited. The system is indeed programmed so that its total money supply does not exceed 21 million units in the long run. When it was created in 2009, the pace of creation of new Bitcoins was 1 Bitcoin every 25 minutes. This rate has been roughly halved since 2013. At the end of 2014, already 12 million Bitcoins had already been put in circulation. When the creation of Bitcoins ceases, the miners will be rewarded with a commission taken on the transactions they verify. They will always have an incentive to work for the proper functioning and security of the network.

Section 4: Bitcoins as a Currency to Trade and to Process Payments

Bitcoins seems to be ideal as a future means of official payments. Years after years, payments made online are getting higher and higher. Thanks to new systems such as Bitcoin, exchanges are better facilitated. Cryptocurrencies have a real impact on e-commerce. They seem to be an easy solution as they are simple to use compared to official monetary currencies. In the case of buying goods or services online, there are a couple of advantages the Bitcoin provides. It is well known that buying online by credit card always presents a certain risk of fraud or identity theft. It is necessary to enter the number of the credit card and its cryptogram, as well as the owner personal details. With Bitcoin, payments are anonymous, no need to enter your details, and only secure lines of code are sent to pay for your purchases. Another major advantage of Bitcoins is the removal of transaction fees. There are no banking intermediaries, the transaction is made directly between the consumer and the merchant. Therefore, the merchant does not incur charges related to the handling of Bitcoin unlike payment by debit/credit card. This lack of fees often pushes merchants to offer advantageous discounts to customers paying in Bitcoins which lead to an increase of the customer purchasing power.

Credit and debit card networks are also affected, “Bitcoin could offer an alternative that might pressure card networks to lower their prices to merchants” (Rainer Böhme, 2015). Finally, any payment in Bitcoins is final. Thus, it is impossible to return to a transaction in Bitcoins. Therefore, merchants, businesses and self-employed who offer to pay for their products and / or services in Bitcoins have a real guarantee of payment.

Bitcoin is also a major speculative asset traded on dozens of different platforms. Two types of platform exist to enable users to both sell/buy and store Bitcoins: the exchanges and the wallets. The currency exchanges enable their users to trade Bitcoins for other currencies. This solution is still today one of the easiest way to acquire the first Bitcoin in a wallet. Most of these platforms operate double auctions with bids and asks much and "charge a commission ranging from 0.2 to 2 percent" (Rainer Böhme, 2015). Of course, these trades are heavy in term of conversions including with a conversion with an intermediary currency and a final conversion with the traditional currency. The wallets are also important elements of the Bitcoin supply chain. These wallets record the transactions. Other users will potentially want to manage their own wallet and look at the price every single day. These wallets offer great simplicity of use, never encumber the hard disk and allow the saving as well as the automatic encrypted sending of the private keys, making them very attractive for the average user.

On the other hand, it is of course possible that the selected online portfolio is compromised or may be offline for technical reasons. Their ease of use as well as their flexibility therefore has as drawback a low level of security. Frauds, money laundering and trafficking are all a certain threat upon the trust we have on Bitcoins as a mean of exchange. How can it be possible to accurately define the trust individuals have into the Bitcoin and how does this trust evolve across time?

Chapter 3: Analysis of Bitcoin Trading Behaviors and the Trust Implications

"Virtually every commercial transaction has within itself an element of trust."
(Arrow, 1972)

Section 1: Hacking, Fraudulent Acts and Limits of the Technology

The preservation of crypto-assets is subject to significant cyber-risks and offers no protection in terms of assets' security. There are proven risks of hacking electronic wallets that allow the storage of crypto-assets. In this context, the holders have no recourse in case of theft of their assets by hackers. Repeated episodes of major fraud illustrate the vulnerability of the crypto ecosystem. And the high level of associated risks, in the absence of guarantee mechanisms. No central entity is present to coordinate or monitor the proper functioning of the system, nothing is planned and cannot be activated in case of loss of Bitcoins. It suffices for a user to lose his electronic keys for example to no longer have access to the wallet containing his Bitcoins. No remedy is possible in this case, and Bitcoins are simply lost for both the user and the entire network. It is the same in case of unfortunate removal of Bitcoins. No remedy is possible after a transaction. Any transaction is indeed irreversible, whatever the circumstances of its execution, and the system is in no way guaranteeing the reliability of the sellers, even more difficult to find in case of fraud due to the anonymity of Bitcoin addresses.

Finally, there are real risks of theft of Bitcoins or denial of service, against which nothing is planned to ensure users. The market is not regulated. The most obvious example is Mt. Gox, which was the largest Bitcoin exchange platform in volume. It collapsed sharply in February 2014, supposedly because of hacking that would have costed nearly 750,000 Bitcoins - which then amounted to $ 350 million. The site had suspended transactions in early February and

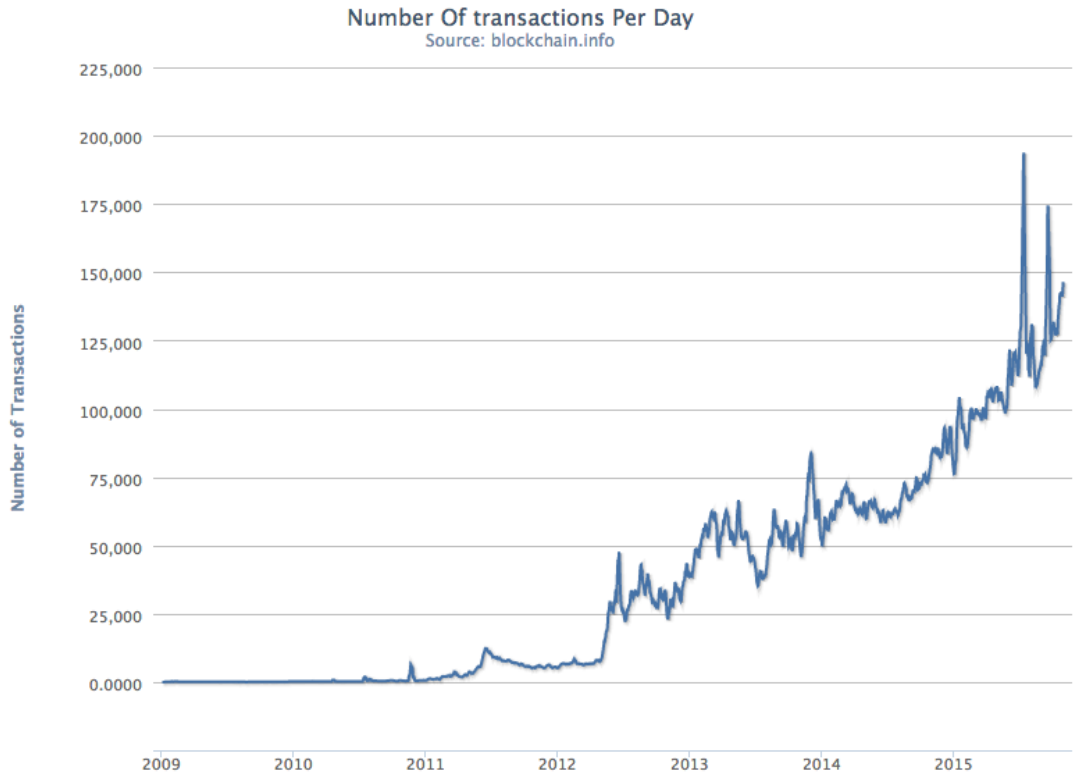
stopped any possibility of withdrawal for users, evoking a computer bug. Subsequently, the content of the site has simply disappeared, simply leaving users with more or less significant losses. All these risks are proven and are true limits to= the Bitcoin system. All of these weaknesses constantly affect the way people trust the cryptocurrencies and trade Bitcoins. The price is highly volatile.

In the second chapter, it has been argued about the ability of Bitcoin and especially Blockchain to fix trust issues in our economy system by removing the need for trust and creating a fully decentralized and transparent network. In the previous section, limits have been described and might affect the trust individuals have into the Bitcoin network. Without enough trust into the main incentive for the use of the Blockchain, the system becomes counter-productive and create new trust issues. In this last section for this research, a thorough analysis will be made by analyzing both the Bitcoin stock price on different exchanges and by compiling and analyzing the different hacks that have occurred since 2010. The main goal will be to show the limits of the Bitcoin as a way to build trust based on the assumption that the stock price reflects the trust people have in the currency. Bitcoin is one of the "most speculative assets in the history of finance" (Detzel, Liu, Strauss, Zhou, & Zhu, 2018, p. 2).

In "Bitcoin: Predictability and Profitability via Technical Analysis," the authors analyze the profitability of trading Bitcoin via technical analysis. Their first two main uncertainties about the cryptocurrency are related to whether or not the Bitcoin have an intrinsic value and "whether or not Bitcoin will eventually be able to generate cash flows" (Detzel, Liu, Strauss, Zhou, & Zhu, 2018, p. 2). One highlighted statistic used in the research is the following: "Over the roughly

seven-year sample, $1 investment in the S&P500 increased to about $2.65. Over the same period, $1 invested in Bitcoin grew to more than $103,453" (Detzel, Liu, Strauss, Zhou, & Zhu, 2018, p. 8). This quote alone shows the incredible growth of the Bitcoin and trust given by its investors to continue to grow. As shown in the figure above, the number of transactions per day has been multiplied by six from 25,000 to 150,000 from the end of 2012 to the end of 2015.

***Figure 3**: Number of Bitcoin transactions per Day*



Past research has been very efficient at showing the volatility of Bitcoin prices and explaining the market bubble. This third and last chapter aims at supporting the main thesis of this research about the influence of Blockchain on trust building between financial actors. Bitcoin holders actively trading in the market put their financial gains expectations into potential

Bitcoin price shifts without any fundamental basis. Even if entirely speculative, this approach still demonstrates the existence of a certain trust associated to the Bitcoins. Bitcoins trading patterns happen in the same fashion than any security trading patterns. The goal of this research is to show how Bitcoins price shifts on one exchange are affected by Bitcoins prices on other exchanges. What are the most trustworthy exchanges? Is the market efficient and fully transparent?

Section 2: Bitcoin Prices and Market Efficiency

2.1 Methodology of creation of the dataset

In order to analyze Bitcoin prices for the last six years, data from five different exchanges have been used to provide an overall and more accurate view of the Bitcoin markets. Quandl Python API was used to retrieve the different exchange prices. They were combined and merged by utilizing the Pandas python library. The five exchanges that have been targeted are: Coinbase, Bitstamp, Itbit, Mt Gox and Kraken. The data available range from 2012-01-01 to 2018-01-01 with Open, High, Low, Close, Volume in BTC and $ and Weighted Prices. The data has then been analyzed by using Minitab Statistical software. Certain statistical measures such as Returns, and Yang Zhang Volatility based on price bars were applied to the individual and merged datasets. The Returns measure formula is the following:

$$\ln(Weighted\ Price) - lag(\ln(Weighted\ Price))$$

Returns measure

The Yang Zhang model used in this research is the following:

$$\frac{1}{2}(\ln(P_{High}) - \ln(P_{Low}))^2 - 0.386 \times (\ln(P_{Close}) - \ln(P_{Open}))^2$$

Yang Zhang Volatility

***Figure 4**: Sample Raw Data of the Kraken Exchange Bitcoin Prices from Quandl API*

Date	Open	High	Low	Close	Volume (BTC)	Volume (Currency)	Weighted Price
2014-01-07	874.67040	892.06753	810.00000	810.00000	15.622378	13151.472844	841.835522
2014-01-08	810.00000	899.84281	788.00000	824.98287	19.182756	16097.329584	839.156269
2014-01-09	825.56345	870.00000	807.42084	841.86934	8.158335	6784.249982	831.572913
2014-01-10	839.99000	857.34056	817.00000	857.33056	8.024510	6780.220188	844.936794
2014-01-11	858.20000	918.05471	857.16554	899.84105	18.748285	16698.566929	890.671709

The following method was used to create the final data frame. The 5 exchanges prices were all pulled from the Quandl API with a similar data library than the Kraken table above. The BTC Weighted prices, Volume (BTC), Open, High, Low, Close values were merged into a single data frame. After cleaning the null values, a revised data frame was created. These null values were due to the removal of the exchanges either for a short period of time or indefinitely. For instance, on December 22, 2017, the Bitcoin price plummeted. For at least two hours, “trading on the prominent cryptocurrency exchange Coinbase was stopped” (Kamhi, 2017). Another famous example would be Mt. Gox that went bankrupt and consequently terminated its trading platform. One can see the different trends of the Bitcoin prices since 2011 on the following graph with the average weighted price:

***Figure 5**: Bitcoin Price (USD) By Exchange*

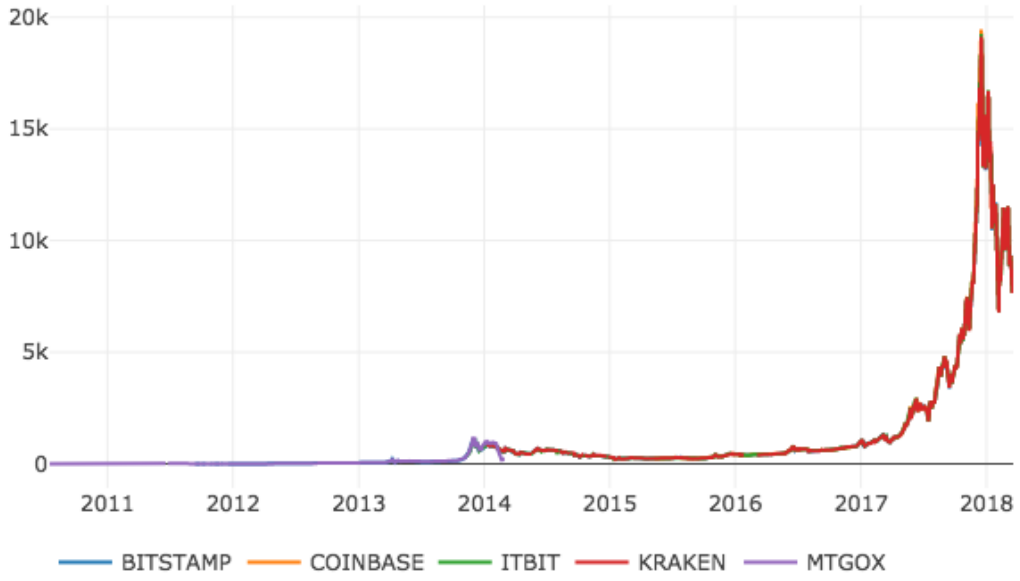
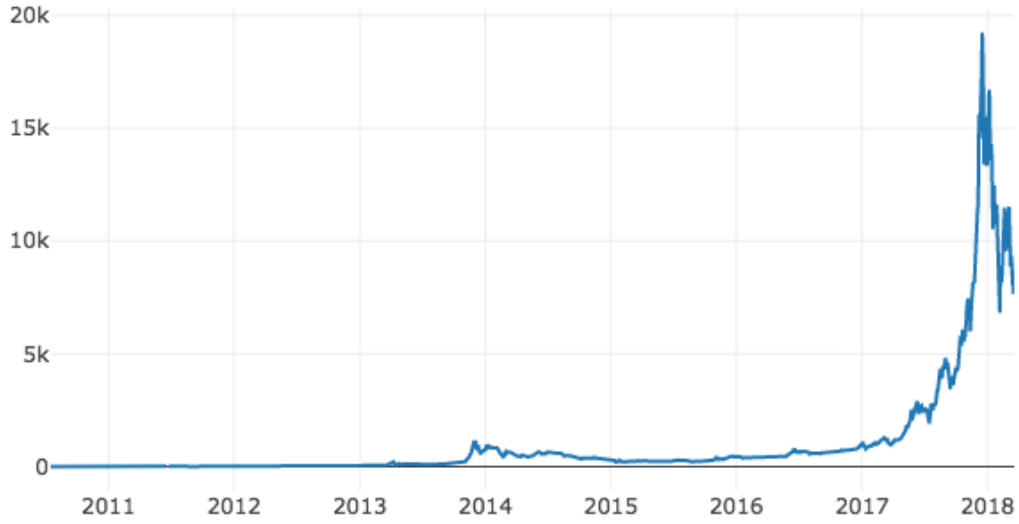


***Figure 6**: Total Average Bitcoin Price (USD)*



2.2 Market efficiency

Financial actors are characterized as the individuals running the companies and the actors in charge of monitoring them. In order to fully trust these actors, the information needed to make informed investment decisions should be complete and accurate. In order to increase confidence of the different actors, any disclosures of meaningful financial information have to be fair. Insiders should not have more data than other participants and trade on this asymmetry of information opportunity. It is only when all these components of trust are in place that we can count on healthy and efficient markets that benefit everyone. Also associated to the Law of One Price, the market efficiency theory "refers to the degree to which stock prices and other securities prices reflect all available, relevant information" (Investopedia, n.d.). Trust into the market is influenced by this level of efficiency (or inefficiency).

The Efficient Market Hypothesis (EMH) has been studied in any possible ways in Finance. Many Bitcoin academic research papers have focused on the speculative trend of the Bitcoin market. In this current research, we aim at testing the efficiency hypothesis and show the inefficiency of this market. This part of the research offers to discuss the hypothesis of efficiency of the overall Bitcoin market, including the five exchanges. This model has been advanced by Milton Friedman in 1953 and formalized in the more general framework of the financial markets by Fama (1965). Several types of efficiency can thus be defined according to whether one refers to fundamental efficiency in the sense of Fama, Friedman's macroeconomic efficiency or speculative efficiency which implies that it is not possible to make systematic profits on the foreign exchange market for a given level of risk.

Several conditions are needed to test the market efficiency assumption. First, the efficiency assumption implies that investors form rational expectations. Other conditions are necessary to validate the assumption of market efficiency: perfect market liquidity ensured by both the atomicity of agents and the absence of transaction costs; perfect information which assumes that agents have free and cost-free access to all available information. The efficient market theory relies on the fact that stock prices follow a random walk, which means that price changes are independent of one another.

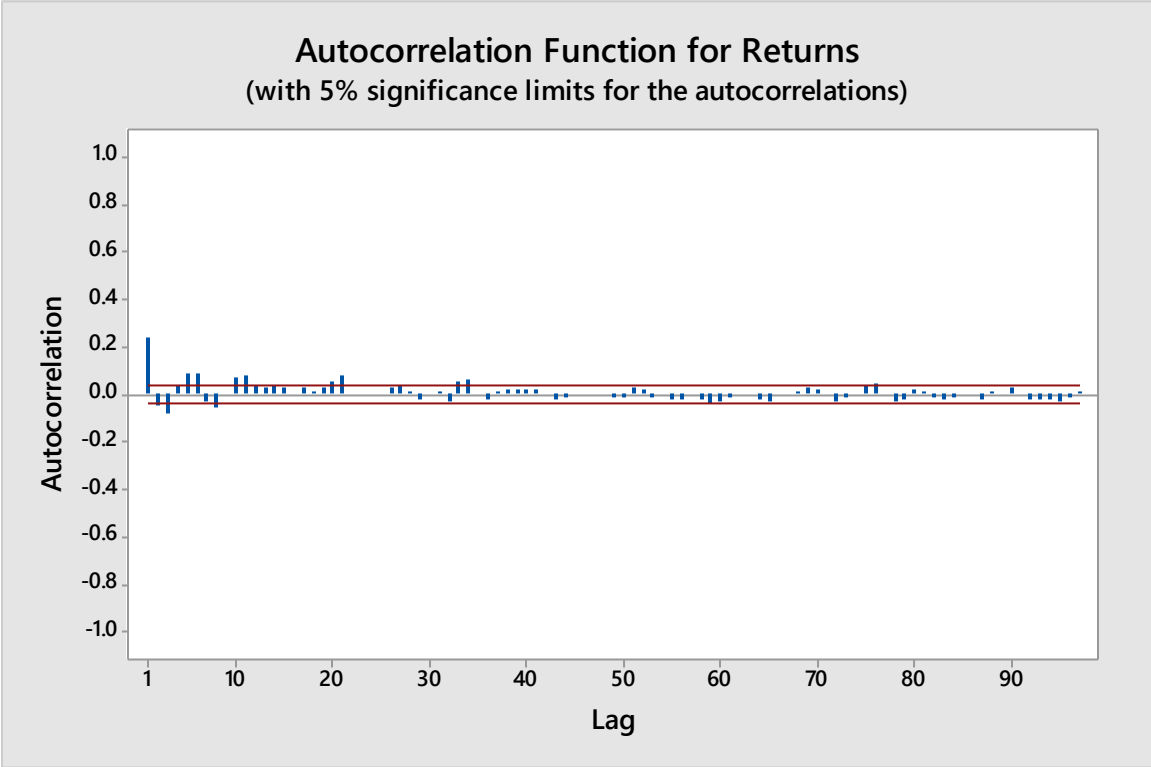
It is always very difficult to know in advance which types of assets will be good investment. An investment is "an asset or item that is purchased with the hope that it will generate income or appreciate in the future" (Investopedia, Investopedia, n.d.). The original Bitcoin manifesto does not regard Bitcoin as an investment or as a protection against the devaluation of traditional currencies by central banks. Bitcoin has been designed as a payment system that would not depend on any third-party organization. Similarly, the argument that this asset must be retained as a real store of value because of the limited supply is not working. In this research, we are interested to know whether or not the Bitcoin market tends toward market efficiency. In the case of the Bitcoin market, extensive research has been made on its bubble characteristics.

Methods we have used to test the market efficiency of the Bitcoin market has been an autocorrelation function test (ACF). It measures the "correlation between the current and lagged observations of the time series of stock returns" (Islam, Watanapalachaikul, & Clark, 2005). The equation is defined as the following:

$$\hat{r}_k = \frac{\sum_{t=k+1}^{n-k} (x_{t-k} - \bar{x})(x_t - \bar{x})}{\sum_{t=1}^{n} (x_t - \bar{x})^2}$$

where k is the lag number, xt is the value of the return at row t date, … is the mean of the returns and n is the number of returns. The data sample we analyze is the Returns of the average of the Bitcoin Weighted prices from 5 different exchanges. In the following two figures, the autocorrelation and correlation functions are used on returns from 7/17/2010 to 3/20/2018.

***Figure 7**: Autocorrelation Function for Returns*



If the Bitcoin market is efficient, then there should be no autocorrelation. Lags 1, 3, 5, 6, 8, 10, 11, 20, 33 and 34 all have corresponding autocorrellations values above 5% significance limit. This autocorrelation is important at low and medium lags. Autocorrelation is under 5% at

high lags. There are two major negative autocorrelations at lags 3 and 8. The results depicts an average level of positive autocorrelation of the daily returns on the Bitcoin prices in the 2010-2018 time period. In order to assess the significance of the autocorrelation for longer lags, Ljung-Box Q statistic (LBQ) can be used to "determine whether all the autocorrelations up to and including a specific lag are equal to 0" (Inc., Minitab, 2017). If after the the test, LBQ is higher than the corresponding critical value, then you can conclude that the autocorrelation is not equal to 0.

$$Q(k) = n(n+2)\sum_{m=1}^{k}\left(\hat{r}_m^2/(n-m)\right),\ k = 1,\ 2,\ \ldots$$

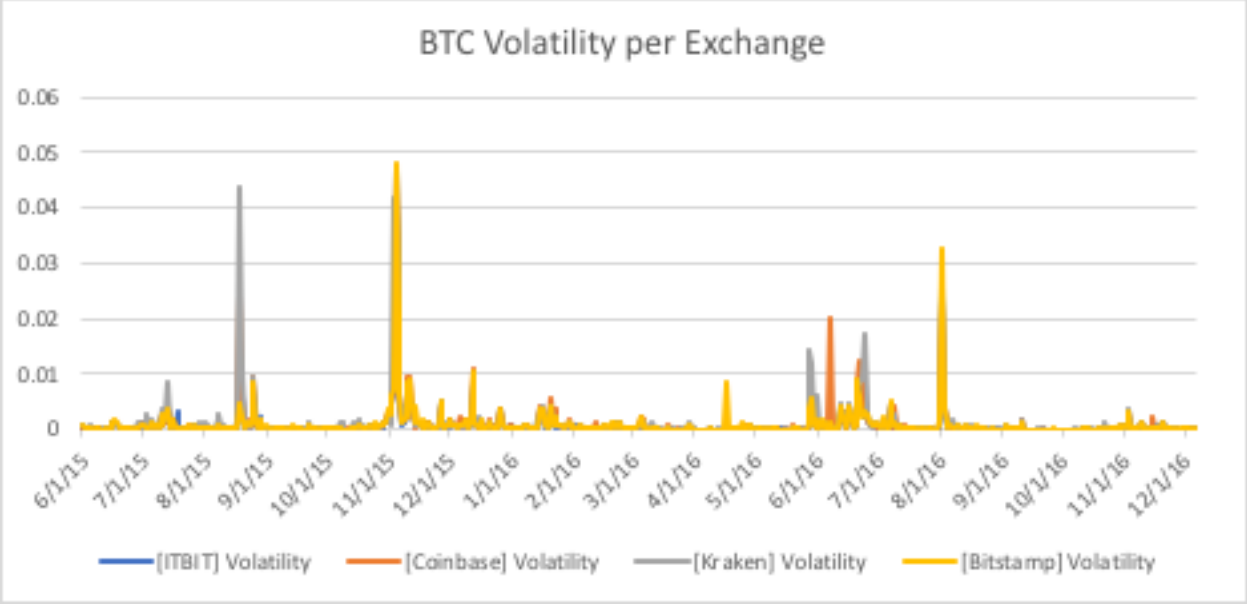
k correponds to the lag number, *n* ius the number of observations in the serie. To determine the significance of ACF and test our autocorrelation hypothesis, we determine the critical value for this chi-square distribution with *v* degrees of freedom equals the number of lags (*v = 97)*. At five per cent of significance, the *Q* statistic at 97 lags should be 120.990. Following the LBQ calculations, lag 97 yields 421.6461 > 120.990. Thus, the null hypothesis is accepted and there is existence of autocorrelation at 5% level of significance. Following the auto-correlation tests, it can be concluded that the Bitcoin market is not efficient during the 8 years of study period.

Section 3: Volatility Spillover

3.1 Data Analysis

Some academic papers have been published on the cryptocurrency and traditional stock market linkages, influences and spillovers of one crypto market on another traditional market, and vice-versa. Cryptocurrency finance literature lacks studies on cryptocurrencies volatility co-movement and volatility spillovers. In the focus on this research, we aim at analyzing the Bitcoin volatility spillovers between four major different Bitcoin exchanges. We are asking ourselves whether or not Bitcoin price volatility on one exchange affects the Bitcoin price volatility on another exchange. Are they interdependent? In the context of our research, we try to understand how fast trust in the Bitcoin market can be affected if a hack, crisis or any type of market changing events happen. Which exchange affects the other one and which one entirely relies on the other ones? We propose a test to measure the interdependence between the Bitcoin price volatility in the four different exchanges such as represented on the following graph:

***Figure 8**: BTC Volatilities, Bitcoin Exchanges, 6/1/2015 – 12/6/2016*



Volatility spillovers are “manifestations of the impact of global shocks on any given market” (Premaratne & Bala, 2018, p. 10). We base our measurement of spillover on the following function:

$$Vol_{1t} = f(Vol_{1,t-1}, Vol_{2,t-1})$$

$$= f(Vol_{1,t-1}, Vol_{2,t-1}, Vol_{3,t-1}, Vol_{4,t-1})$$

Figure 9*: Spillover Table, Bitcoin Exchanges Volatility, 6/1/2015 – 12/6/2016*

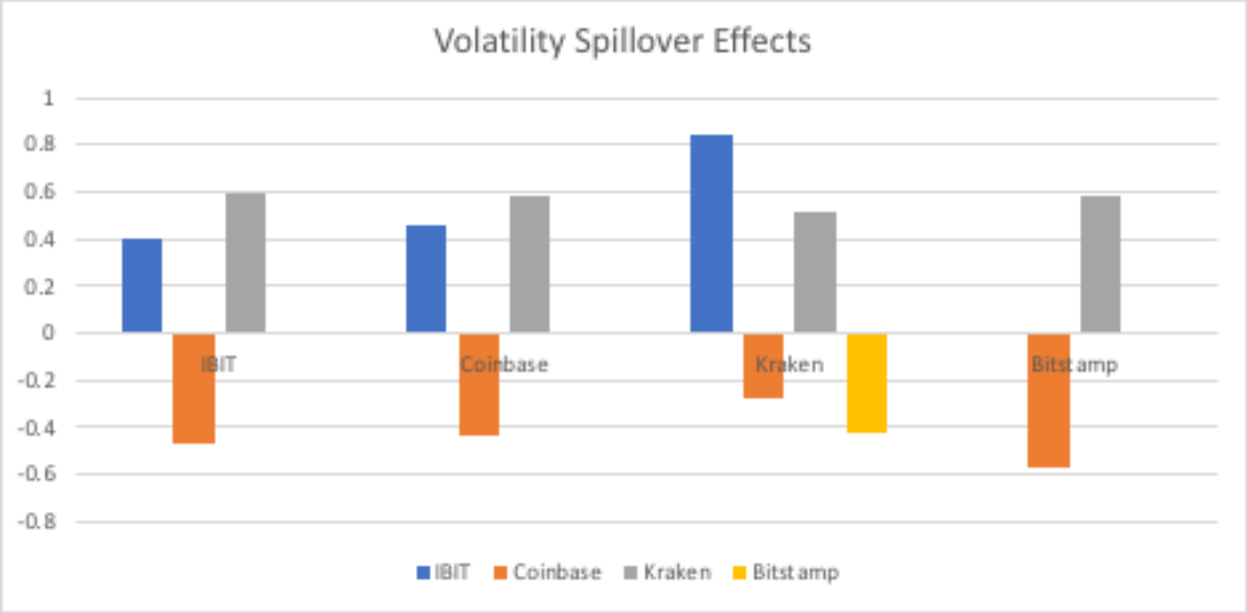
To / From	IBIT	Coinbase	Kraken	Bitstamp
IBIT	0.402*	0.46*	0.846*	0.292
Coinbase	-0.4673*	-0.4326*	-0.273*	-0.5653*
Kraken	0.5977*	0.5806*	0.5112*	0.5809*
Bitstamp	-0.145	-0.158	-0.424*	0.107
Constant	0.000333	0.000483	0.000548	0.000465
R²	0.4284	0.343	0.2951	0.3532

**Correlation coefficients with a p-value lower than 5%*

In order to do the spillovers analysis, daily trading data has been captured in order to get more information than weekly and monthly data. The data of these prices consist of 24h/7d trading data points. The markets are synchronous and there are no missing data points. We analyzed on the following time period: 6/1/2015 to 12/1/2016. This period was selected due to the nonexistence of missing data points on all of the four exchanges. According to the correlation model and looking at the p-value of these correlations, out of the 16 different correlation coefficients, 12 are statistically significant at 5%. These significant spillover coefficients “imply that significant volatility shocks are imported from market B into market A through the

variances" (Premaratne & Bala, 2018, p. 12). Coefficients close to 1 mean that the series are strongly correlated. Coefficients close to -1 mean that the series are inversely correlated. Coefficients close to zero mean that the values are not correlated and fluctuate independently from each other. For instance, we learn that the volatility of Bitcoins on Kraken contributes for 0.846 of the volatility of the same currency on IBIT exchange. Volatility spillovers from Kraken to ITBIT are larger than for Kraken to Coinbase where the Kraken Bitcoin volatility contributes for -.273 of the volatility of the same currency on Coinbase. Of course, it is important to understand that spillover does not mean causation. Instead, it will reflect the correlations and co-movements between the different markets. Among all the different currencies, the strongest negative volatility spillover happens from Bitstamp to Coinbase. An increase in Bitcoin volatility on Bitstamp contributes to the decrease of .5653 of the Bitcoin volatility on Coinbase. This is the strongest negative correlation available in our dataset. Finally, the least correlated relationship of Bitcoin volatilities is from Kraken to Coinbase. The following graph provides a visual representation of the different spillovers. The exchange indicates on the graph represents the original exchange (x-axis) contributing to the volatilities of the other exchanges (y-axis). The first surprising conclusion that can be drawn is the constant negative correlation between other exchanges and Coinbase. The most important negative contribution to Coinbase is from Bitstamp (-.5653). It is also difficult to assess the real impact of the contributions from the other exchanges to Bitstamp due to inadaptability of the model to this exchange Bitcoin volatility data.

***Figure 10**: Spillover Graph, Bitcoin Exchanges Volatility, 6/1/2015 – 12/6/2016*



This graph only includes significant coefficients.

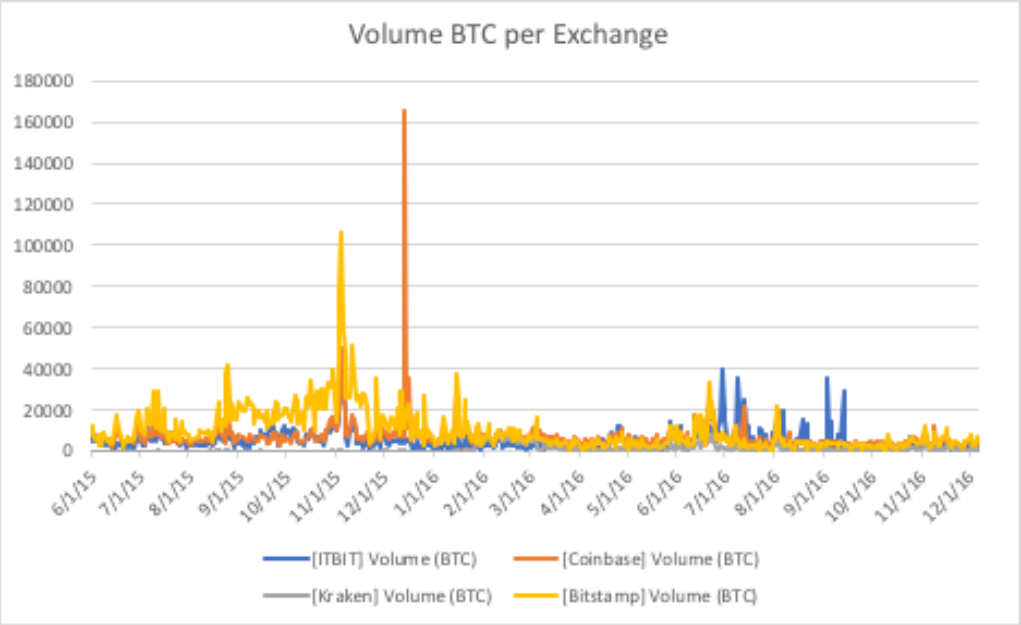
3.2 Trading and Trust Implications

From the initial analysis of the spillovers, two different cases can be analyzed:

Case 1: We can see a "significant volatility spillover effects and volatility co-movement" (Premaratne & Bala, 2018, p. 20) between Kraken and ITBIT. This correlation happens in both directions and is positive. Due to an important significance, we can conclude that the Bitcoin volatility spillovers between ITBIT and Kraken are constant. This strong linkage can be explained by geographic reasons. Both of the companies are headquartered in the United States, IBIT is in New York and Kraken is in San Francisco. Both target US customers. We can make the assumption that the target demographic of both of these exchanges are similar. Bitcoin volatility on Kraken has a higher contribution to the Bitcoin volatility on ITBIT than the contrary. The main reason can be the largest market effect where a larger market will affect a smaller market. There is a significant volatility co-movement between the two exchanges.

Case 2: Bitcoin volatility on Coinbase is negatively affected by positive volatility movements on all the other exchanges. One of the main assumption behind this trend is the use of Coinbase in a very specific way to trade Bitcoins. Compared to the four other exchanges, Coinbase has very different features. Coinbase is primarily a wallet to store Bitcoins. It does not hold dollars and requires a bank account transaction for each Bitcoin transaction. "This mechanism of payment makes it unfit as a day trading exchange. It is designed for newcomers who are learning about Bitcoin trading or those who trade with a longer view. Currently, Coinbase does not cater to advanced trading tools like bids, asks, limit orders, margin trading, or short sale orders" (Bajpai, n.d.). Thus, Coinbase is often use as a secondary platform to store initial Bitcoins. Once an economic agent desires to practice day trading, he or she will transfer its Coinbase Bitcoins to another platform and trade on the other platform. This is why an increase in volatility on the other platform means a decrease in volatility on Coinbase. Coinbase can be utilized to safely store Bitcoins and avoid volatile movements on other trading platforms.

Figure 11*: BTC Trading Volumes, Bitcoin Exchanges, 6/1/2015 – 12/6/2016*



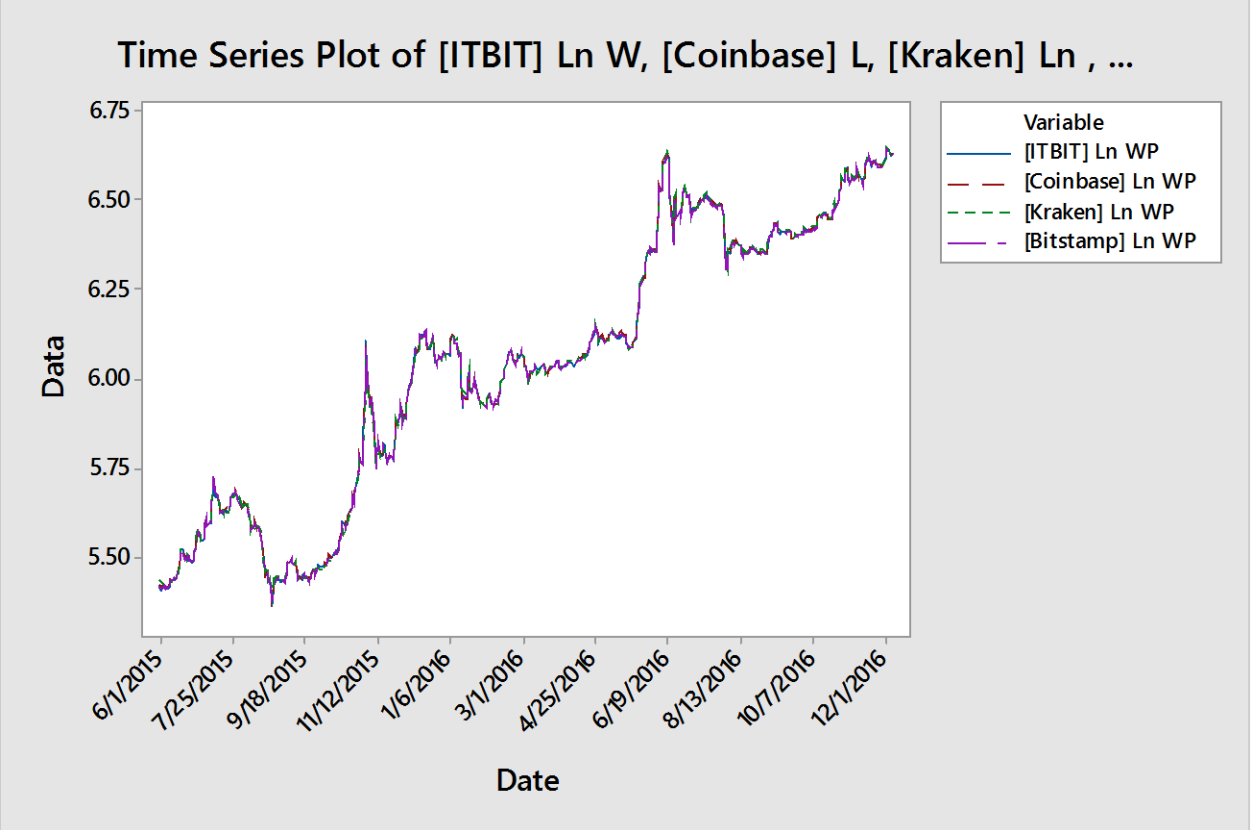
In terms of influence and dominance, both Coinbase and Kraken are the most influential exchanges in the Bitcoin market. Kraken is much more influential than IBIT in the Bitcoin market. Coinbase is much safer than other exchanges due to its specific payment method and wallet usage. We can then conclude there is a difference in term of trust between the different exchanges. Trust is also fluid and adapts to market changes. Trust into Bitcoin can be shared from one exchange to another in the case of ITBIT and Kraken. Trust can also be directed toward another exchange in a case of a negative event happening in the Bitcoin speculative market. It might affect certain exchanges but not all. Being more than an exchange by providing other services makes Coinbase the most trustworthy exchange in the market.

Section 4: Co-Integration

4.1 Data Analysis

We want to test the co-integration between Bitcoin Weighted Prices between four different exchanges. The idea behind the co-integration is that "although multivariate time series is integrated, certain linear transformations of the time series may be stationary" (Pesaran, Shin, & Smith, 2001). The test is the following: If two or more statistical series are non-stationary, but a linear combination of them is stationary, then the series are said to be co-integrated. The Time Series plot above represents the Log Weighted Bitcoin Price on 4 exchanges from 6/1/2015 to 12/1/2016:

***Figure 12**: BTC Log Weighted Prices, Bitcoin Exchanges, 6/1/2015 – 12/6/2016*



In order to test the presence of co-integration, we use Johannsen Test.

We first want to test the non-stationarity of the data and generate the following output:

Johansen-Procedure First Output in R

```
######################
# Johansen-Procedure #
######################

Test type: maximal eigenvalue statistic (lambda max) , with linear trend

Eigenvalues (lambda):
[1] 0.271910261 0.164747593 0.154507510 0.001910626

Values of teststatistic and critical values of test:

          test 10pct  5pct  1pct
r <= 3 |   1.06  6.50  8.18 11.65
r <= 2 |  92.81 12.91 14.90 19.19
r <= 1 |  99.55 18.90 21.07 25.75
r = 0  | 175.48 24.78 27.14 32.14
```

According to the output above, there are three linear combinations that are stationarity and one non-stationary. There are given below:

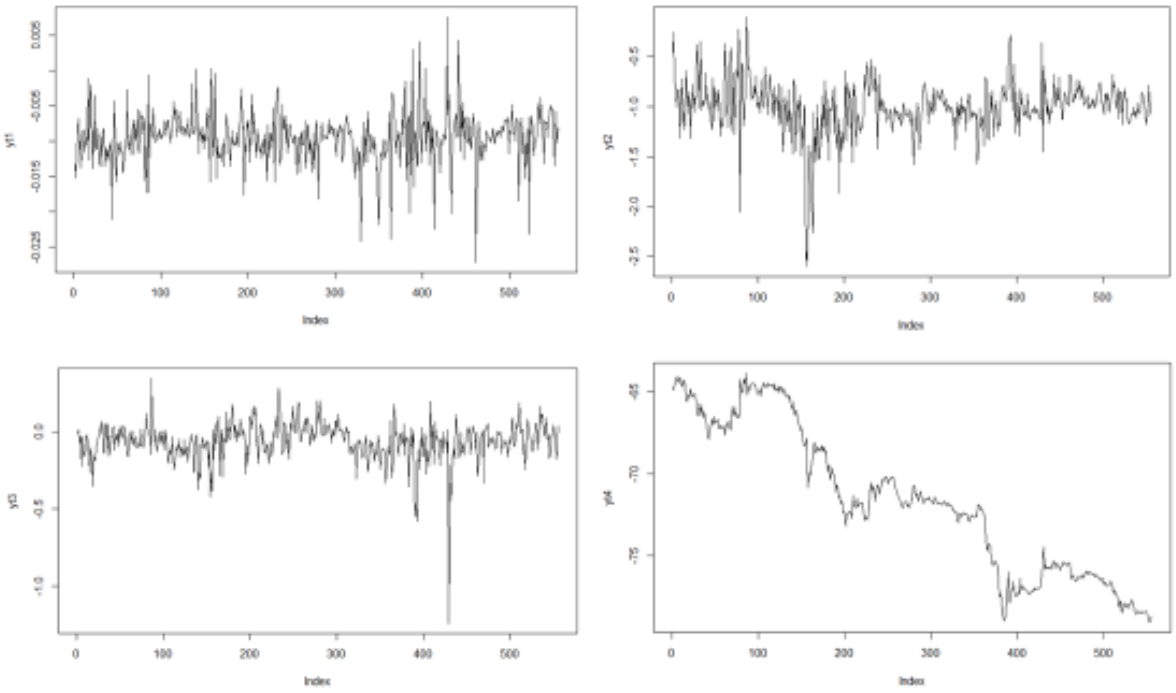
```
Eigenvectors, normalised to first column:
(These are the cointegration relations)

              ITBIT.l2  CoinBase.l2  Kraken.l2  Bitstamp.l2
ITBIT.l2         1.000      1.000       1.000       1.000
CoinBase.l2     -0.406      0.392     -29.667      -0.889
Kraken.l2        0.006     37.608       6.879     -38.575
Bitstamp.l2     -0.602    -39.177      21.791      26.604
```

We highlight the first stationary co-integrated series:

*yt1 = IBIT[,1] - 0.406 *Coinbase[,2] + 0.006*Kraken [,3] - 0.602* Bitstamp[,4]*

***Figure 13**: Co-integration Test Series Outputs*



4.2 Trading and Trust Implications

The stationarity combination can be used for trading purposes; taking Bitcoins out of Coinbase and Bitstamp and investing in IBIT could be profitable based on true deviation of the data continued. More realistic implementation can include testing this out on a moving-window basis and taking into account the transaction costs. Taking advantage of arbitrage opportunities between Bitcoin exchanges has some potential technical issues. Many exchanges require background checks and impose delays for each transaction. Transferring any fiat currency will take hours or even days. Finally, exchanges also have fees. The different fees are: “Fiat deposit fees, Fiat withdrawal fees, Bitcoin deposit fees, Bitcoin withdrawal fees, Transaction fees” (Beigel, 2018).

However, even if technical challenges arise, arbitrage opportunities still exist. Without any current regulations and specific geo-political factors affecting exchanges in different countries, there are a couple of potential arbitrage opportunities. Among the four exchanges studied in this research, the arbitrage opportunities might exist but might be low compared to ones related to trades between major exchanges and low-volume exchanges. Since the exchanges strongly rely on communities with purely speculative beliefs, arbitrage opportunities might occur once an exchange loses the trust of its traders. With an important opacity on the way these exchanges manage the customers' assets, all the ingredients are here to decrease the trust into these platforms. Less trust will lead to less buyers which will naturally lower the exchange rate. Important arbitrage opportunities occurred in the last few days of Mt Gox where the price decreased continuously due to a complete loss of trust in the exchange's ability to pay back the liquidity stolen by hackers.

Conclusion

Bitcoin and Blockchain are here to last. Blockchain is today becoming more prominent than the currency based on it. Based on the same Blockchain, many cryptocurrencies are being launched to compete with the Bitcoin and solve trust issues in different industries such as supply chain or finance. Between institutional and inter-personal trust, Blockchain applications are trying to fix potential trust issues by lowering the uncertainty and the human involvement in validating financial transactions. Even if they have not yet been detected or exploited, flaws in the Blockchain protocol are theoretically possible. No doubt many hackers are now trying to discover them. The attraction of hackers for cryptocurrencies is more and more concrete. After reading this research, one might have understood that Bitcoin is still not a miracle solution for trust. The main problem is associated with exchanges that enable miners, buyers and sellers of Bitcoins to connect between each other. Thanks to the financial analysis of the four different exchanges, weaknesses in the differences exchanges have been uncovered. Being highly volatile, Bitcoin in itself is not trustworthy enough to be used as a valuable system to increase trust in our financial system. By not having any existing regulations, arbitrage opportunities are here to take advantage of the lack of trust in one exchange or another. The volatility spillovers have shown the way people react when the price collapses and how the stakeholders move their bitcoins around different exchanges. Taking advantage of these movements of Bitcoins between the different exchanges would be a good trading strategy. However, an investor might not forget that the inefficiency in the Bitcoin market is strong and that the asymmetry of information between the different stakeholders is permanent. There are no current laws against Bitcoin insider-trading. For subsequent research, one might want to create an arbitrage trading strategy that takes into account the trust people have in both the currency and the exchanges.

Works Cited

Abiteboul, S. (2016, July 20). *Des startups Blockchain bien de chez nous…* . Retrieved from Le Monde: http://binaire.blog.lemonde.fr/2016/07/20/des-startups-Blockchain-bien-de-chez-nous/

Arrow, K. J. (1972). Gifts and Exchanges. *Philosophy and Public Affairs 1*, 357.

Cohn, S. (2014, 05 20). *Study: External audits a poor tool for fighting fraud* . Retrieved from CNBC: auditors detected just 3 percent of the fraud cases reported last year [2013], compared to 7 percent uncovered by accident

Detzel, A. L., Liu, H., Strauss, J., Zhou, G., & Zhu, Y. (2018). *Bitcoin: Predictability and Profitability via Technical Analysis.* SSRN.

Dictionaries, O. (n.d.). *Crisis*. Retrieved from Oxford Dictionaries: https://en.oxforddictionaries.com/definition/crisis

Dictionaries, O. (n.d.). *Utilitarianism*. Retrieved from Oxford Dictionaries: https://en.oxforddictionaries.com/definition/utilitarianism

Guarda, D. (2016, 05 14). *12 Bitcoin and Blockchain Thoughts and Quotes You Need to Read*. Retrieved from IntelligentHQ: https://www.intelligenthq.com/finance/12-Bitcoin-and-Blockchain-thoughts-and-quotes-you-need-to-read/

Harari, Y. N. (2011). *Sapiens: A Brief History of Humankind.* Tel Aviv: Harper.

Hidalgo, C. A. (2015). *Why Information Grows: The Evolution of Order, from Atoms to Economies.* Hachette.

Hobbes, T. (1909). Of Man, Being the First Part of Leviathan. In Harvard, *The Harvard Classics* (p. 1). London: Harvard University.

Inc., Minitab. (2017). *LBQ for Autocorrelation*. Retrieved from Minitab 18 Support: https://support.minitab.com/en-us/minitab/18/help-and-how-to/modeling-statistics/time-series/how-to/autocorrelation/interpret-the-results/lbq/

Investopedia. (n.d.). *Investopedia*. Retrieved from Investment: https://www.investopedia.com/terms/i/investment.asp

Investopedia. (n.d.). *Market Efficiency*. Retrieved from Investopedia: https://www.investopedia.com/terms/m/marketefficiency.asp

Islam, S. M., Watanapalachaikul, S., & Clark, C. (2005, May). *Are Emerging Financial Markets Efficient?* Victoria: Victoria University.

McLeod, C. (2015, 08 3). *Trust.* Retrieved from Stanford Encyclopedia of Philosophy: https://plato.stanford.edu/entries/trust/

Mitchell, L. E. (2003). The Sarbanes-Oxley Act and the Reinvention ofCorporate Governance. *Vill. L. Rev. 1189*.

Oxford. (n.d.). *Accountability*. Retrieved from Oxford Dictionaries: https://en.oxforddictionaries.com/definition/accountability

Rainer Böhme, N. C. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*, 213.

Reyes, R. C. (1986). *Philosophy in a Crisis Situation.* Retrieved from Philippine Studies: http://philippinestudies.net/ojs/index.php/ps/article/download/1230/3882

Scott, F. (2004, January). *Issue Brief #5*. Retrieved from Kenan-Flagler Business School: http://public.kenan-flagler.unc.edu/faculty/segarsa/sustain/sarbanes.pdf

SEC. (n.d.). *SEC.gov | Home*. Retrieved from SEC: https://www.sec.gov/

Sedgwick, K. (2017, November 11). *Bitcoin by Numbers: 21 Statistics That Reveal Growing Demand for the Cryptocurrency*. Retrieved from Bitcoin.com: https://news.Bitcoin.com/Bitcoin-numbers-21-statistics-reveal-growing-demand-cryptocurrency/

Services, H. (n.d.). *Questions*. Retrieved from WeUseCoins: https://www.weusecoins.com/en/questions/

Shafer-Landau, R. (2009). *The Fundamentals of Ethics.* Oxford: Oxford.

Velasco, P. R. (2017, October 10). *Computing Ledgers and the Political Ontology of the Blockchain.* Retrieved from Wiley: http://onlinelibrary.wiley.com/doi/10.1111/meta.12274/full

Warburg, B. (2016, June). *How the Blockchain will radically transform the economy* . Retrieved from TED: https://www.ted.com/talks/bettina_warburg_how_the_Blockchain_will_radically_transform_the_economy

Webster, M. (2017, 12 23). *Knowledge | Definition of Knowledge.* Retrieved from Merriam Webster: https://www.merriam-webster.com/dictionary/knowledge

Webster, M. (2018, 01 16). *Trust | Definition of Trust.* Retrieved from Merriam Webster: https://www.merriam-webster.com/dictionary/trust

Whalen, C. R., & Feldkamp, F. L. (2014). *Financial Stability: Fraud, Confidence, and the Wealth of Nations.* Wiley Finance.

Yoram, B. (1997). *Economic Analysis of Property Rights.* Cambridge: Cambridge University Press.

Zucker, L. G. (1985). *Production of Trust: Institutional Sources of Economic Structure, 1840 to 1920.* Los Angeles: University of California.