Distributed Atomic Swap on Cryptocurrencies

Huseyin Ergun (Corresponding author)

Department of Computer Science, Maltepe University

PO box 34220, Yildiz Technical University Technopark C1 111 Istanbul, Turkey

Tel: 90-532-724-1823 E-mail: huseyinergun@gmail.com

Mesut Razbonyali

Department of Computer Science, Maltepe University

Marmara Education Campus, Istanbul 34857, Turkey

E-mail: mesutrazbonyali@maltepe.edu.tr

Erdal Guvenoglu

Department of Computer Science, Maltepe University

Marmara Education Campus, Istanbul 34857, Turkey

E-mail: erdalg@maltepe.edu.tr

Can Razbonyali

Department of Computer Science, Maltepe University

Marmara Education Campus, Istanbul 34857, Turkey

E-mail: canrazbonyali@maltepe.edu.tr

Abstract

Anyone who wants to trade something in his possession with something else desires three things: To trade at the most appropriate rate, to trade at the least cost, not to be exposed to theft and fraud during the clearing. The cryptocurrency swap is also no different from swapping of any two entities. Crypto-currencies are getting more and more attractive day by day because their stock exchanges are open 24/7. Although all crypto-money markets in the world have similar expectations, existing market models have difficulties and risks while operating on them. The problem of this research is centralized exchange markets and risks while operating on them.

The study aims to develop a distributed exchange model on blockchain using smart contracts for atomic swap method, and payment channels technology for liquidity. With this model, users will pay less without taking risks of centralized exchange markets, like hacking, theft and fraud.

In central exchanges, users first send their cryptocurrencies to the stock exchange's account to trade. This results in collection of all cryptocurrencies of users in a single pool. With this model, users will be allowed to wait in their wallets until the cryptocurrency is exchanged, and the risk of central hacking will be eliminated. Original contribution of this study...

Keywords: Atomic Swap Between Cryptocurrencies, Block-Chain; Cryptocurrency; Distributed Cryptocurrency Market; Cryptocurrency Payment Gateway

1. Introduction

In central exchanges, users first send their crypto-money to the stock exchange's central account to trade. This resulted in the accumulation of cryptocurrencies of all users in a single pool (Raval, 2016), which has become a center of attraction for hackers. Almost all central stock exchanges have encountered hacking cases of various sizes in history (Tapscott & Tapscott, 2016). Due to the continual opening of the new stock market, it is not possible

to mention a specific rate however the biggest hacking event in history happened on stock market called MtGox, which had been hacked many times in 2014 with a total of 750.000 bitcoins (7% of all bitcoins) and the market value of $ 473 million on that period (6.75 billion dollars on June 2020). (wikipedia.org). This event ensued to the bankruptcy of the stock market. The model published on this study recommends that, users hold their currencies in their own wallets until the cryptocurrency is exchanged. Thus, there will not be a single point of failure.

In decentralized stock exchanges fraud or internal or external central theft on cryptocurrencies is not possible due to users held their cryptocurrencies on their own wallet until the moment of exchange (Goodman, 2014). However, liquidity problem exists on decentralized exchanges. The liquidity problem can be defined as the high price when you want to buy a certain amount of crypto-money and the low price when you want to sell, a "high bid ask spread" in financial terms. It is caused by the absence of excessive buyers-sellers (Houben & Snyers, 2018). All clearing transactions on decentralized exchanges are real crypto-money transfer transactions.

This results on, every time a swap is made, it is obliged to pay the commission in the blockchain, except the stock market commission. This situation demotivates high frequency traders or short-term investors, who expects to profit from short-term movements, using decentralized markets. These short-term traders provide liquidity to the markets (Greene & McDowall, 2018).

This study aims to solve the liquidity problem through payment channels technology and channel provider investors. Currently, in recent decentralized exchanges, it is observed that there is higher bid ask spread that regular exchange markets hence this shows they cannot solve the liquidity problem so far. The originality of this thesis study is; providing distributed exchange market model and combining with Payment Channels technologies to create decentralized market as liquid as central exchanges.

On central cryptocurrency exchanges, the commission rate is, on average, 0.2% of the settlement made. Since central exchanges keep the cryptocurrencies of the users within their own system, there are many expenses regarding their transfers and safe storage of which this study defines that as problem. There had been strategies developed on cryptocurrencies, and algorithmic trading has been made on these cryptocurrency exchanges using APIs. When the difficulties encountered and risks taken during use are evaluated, all crypto-money circles in the world have similar expectations. It is observed that there is no stock market meeting both a distributed model and enough competitive liquidity.

In a private blockchain based decentralized stock exchange, the cost is only for keeping the blockchain accessible and adding new data. Thus, it is envisaged to work with commissions that are much lower, estimated one tenth of regular markets (0.02%), and therefore may attract the customers. In cryptocurrencies with a total market share of 200 billion dollars, daily exchange volume can reach 10 billion dollars. This volume increases as cryptocurrencies become more widespread.

The purpose of this study is to use, the private blockchain technology, atomic swap method, and payment channels technology as well as large central stock exchanges in the market; cryptocurrency users pay the least amount without taking risks on existing exchanges; hacking, theft and fraud are not possible; is to design a decentralized cryptocurrency exchange model where all available exchanges can take advantage of. Combining Atomic Swap as distributed exchange and Payment Channels technologies, creating a liquid decentralized stock market model as efficient as central exchanges are the original contribution of this study to the literature.

2. Literature Review

Cryptocurrency is produced by i) the cryptocurrency system, ii) when the system is created, and iii) at a time known to everyone, iv) at a defined rate, v) in bulk. In economic systems such as the Central Bank and the Federal Reserve System, company boards or governments are obliged to print or request new money to be printed. In decentralized cryptocurrencies, company boards of directors or governments cannot generate new capital and support the firms, banks, or institutions that currently have the money. The technical system based on cryptocurrencies was created by the group or individual known as Satoshi Nakamoto (The Economist, 2016).

2.1 Bitcoin

Satoshi Nakamoto in his thesis titled "Bitcoin: A Peer-to-Peer Electronic Cash System," named Bitcoin as;

It has been identified with features such as i) enabling direct transactions by eliminating the need for trusted third parties, ii) enabling irreversible transactions, iii) reducing credit costs in small comfortable transactions, iv) reducing transaction fees and v) preventing double-spending (Nakamoto, 2009).

Bitcoin, the first decentralized cryptocurrency, has gained an essential place in the media, academics, and finance industry since its foundation in 2009. Based on blockchain technology, it maintained its leadership among

cryptocurrencies and showed no signs of slowing down. Bitcoin is based on cryptographic evidence that provides many advantages over traditional payment methods (such as Visa and Mastercard), rather than relying on traditional trust, such as currency, higher liquidity, lower transaction costs and anonymity (Chan et al., 2017).

There are a lot of researches done on the most popular cryptocurrency, "Bitcoin":

Using the model Hencic and Gourieroux (2014) and Cauchy errors, a non-causal autoregressive process made Bitcoin exchange rate estimates against the US Dollar. The results reveal that the daily Bitcoin / USD exchange rate shows local trends, indicating periods of speculative behavior from online transactions.

Sapuric and Kokkinaki (2014), using data from July 2010 to April 2014, investigated Bitcoin's volatility by comparing the volatility rates of major global currencies. Their analysis shows that it has higher annual volatility than the regular exchange rate. Still, it can be considered more stable considering the transaction volume.

Briere et al. (2015) used weekly data from 2010 to 2013 to analyze various investment portfolios and see that Bitcoin is extremely volatile and exhibits huge average returns. Perhaps surprisingly, the results show that Bitcoin is very little associated with other assets, although it helps diversify investment portfolios.

In Kristoufek (2015), he researched the factors affecting Bitcoin's price and applied it to the Chinese Bitcoin market. He found short and long-term connections and said that Bitcoin shows both the characteristics of standard financial assets and speculative assets. This leads to further discussion about whether Bitcoin can be classified as a currency, asset, or investment instrument.

Chu et al. (2015) made the first statistical analysis of the Bitcoin exchange rate. It compares 15 of the most common distributions used in financing to the logarithmic returns against the US dollar according to the Bitcoin exchange rate. Using data from 2011 to 2014, they showed that the overall hyperbolic distribution gave the most appropriate.

Corlu and Corlu (2015) compared the generalized lambda distribution to other flexible distributions such as distorted t distribution, unlimited Johnson distributions, and standard inverse Gauss distribution to capture the distortions and peaks of exchange rate returns. They concluded that for Value at Risk and Expected Deficit, the generalized lambda distribution performed similarly and could be used as an alternative to fulfill the behavior of the heavy tail in financial data in general.

Chu et al. (2015) and Corlu and Corlu (2015) review the exchange rate returns study and demonstrate that the Student t distribution can perform similar to the distributions tested in Corlu and Corlu (2015).

Bruneau and Moran (2017) investigated the effect of exchange rate fluctuations in the Canadian manufacturing industries on labor market regulations.

Dai et al. (2017) examined the role of exchange rates on economic growth in East Asian countries.

Parlapiano et al. (2017) analyzed the exchange rate risk according to European companies' value.

Schroeder (2017) investigates macroeconomic performance related to exchange rates in developing countries.

Seyyedi (2017) provides an analysis of the interactive links between gold prices, oil prices, and the exchange rate in India.

Another issue investigated in the literature is the volatility of cryptocurrencies. Numerous researches have revealed many definitions and methods for calculating volatility (Chan et al., 2017).

In Sapuric and Kokkinaki (2014), volatility is defined as the annual fluctuation (or standard deviation) representing daily fluctuations in the exchange rate. This is calculated by multiplying the standard deviation of the exchange rate by the square root of the number of annual trading days.

Briere et al. (2015) uses annual returns and also calculates annual volatility in its analysis.

A blockchain is a distributed database of i) all transactions performed and shared between participating parties, ii) records of digital events, iii) public books. For each transaction in the public book, the majority of the participants in the system are reconciled, and once entered into the system, the information can never be deleted. The blockchain contains a precise and verifiable record of each transaction (Zhang et al., 2019).

2.2 Bitcoin Technologies

Bitcoin is the most popular and controversial example which is internally linked to blockchain technology. It has to deal with several regulatory issues involving national governments and financial institutions. It enables a large volume of anonymous transaction markets without government control. It can be said that Bitcoin creates new functions by combining existing technologies. i) Without any central authority, ii) Bitcoin is a suitable system to operate like a system for electronic money, iii) to prevent data from being tampered and iv) to avoid the duplication

of payments (Cermeno, 2016).

By working flawlessly for years, blockchain technology has been successfully applied to financial and non-financial world practices. Last year, Marc Andreessen, one of the leading capitalists in Silicon Valley, announced that he saw the blockchain's distributed model as the most important invention since the internet itself. Johann Palychata of BNP Paribas wrote in Quintessence magazine that bitcoin's blockchain should be considered as an invention like a steam or combustion engine that has the potential to transform the world of finance, software that allows digital money to function (Joshi et al., 2019).

The current digital economy is based on trusting a particular, trusted authority. All of our online transactions work with trust in someone who will tell us the truth. (the e-mail service provider may have notified that the e-mail has been delivered; it may be a certification authority that tells us that a particular digital certificate is reliable; or a social network such as Facebook, that our articles about events in our lives are shared only with our friends, or that our money is delivered to our loved ones in the remote country, etc.) It is possible that we live our lives precariously in the digital world by relying on a third party for the security and privacy of our digital assets and that it is quite clear these third-party resources can be are attacked, manipulated, or compromised (Nofer et al., 2017).

The difference of blockchain technology emerges at this point. Every past and present online transaction involving the digital world can revolutionize the digital world by providing it with a distributed consensus that it can be verified at any time in the future. This does not require that digital assets and interested parties compromise their privacy. Distributed consensus and anonymity are two crucial features of blockchain technology (Zubaydi et al., 2019).

2.3 Peer to Peer Communication

In a general client-server network, a server takes the task of protecting and maintaining data and a client requests data from the server and gains access. In this case, the roles of both parties are fixed. In contrast, in a P2P (peer to peer) network, all participating nodes (referring to computers for communication, also called "peers") retain data. An autonomous network is created between these nodes, where data is requested and provided on an equal basis. In a P2P network, unlike the status of a client-server network, the roles of a server or client-related nodes are not fixed (Kisembe & Jeberson, 2017).

When adopting a P2P network, it is necessary to consider search methods and data transfer methods. Search methods are tools for managing the locations of nodes and data. Representative examples include nodes that perform management with only a P2P network, set up a directory server, and manage high processing power (supernodes). Data transmission methods are tools for transmitting data between nodes. They are divided into direct transmission between nodes and transfers transferred over another node (Yan et al., 2019). In the P2P network used for Bitcoin, while P2P is adopted as a search method, it is performed by crossing nodes related to data transmission (Delgado-Segura et al., 2018).

P2P network technology has contributed to developing a foundation for a fully distributed network and eliminating the only point of failure in Bitcoin. Moreover, considering the blockchain data, this will be explained later. All nodes participating in the Bitcoin P2P network and mining must have the same data (Park et al., 2019).

3. Atomic Swap Model Design

3.1 Method

While developing the system, first of all, existing crypto money systems and infrastructure in the market are examined. The logic and map of change are drawn.

A suitable cleaning method and exchange are designed for this system, this project will be coded and tested in real life.

While designing atomic transactions, the existing database systems (acid), distributed transaction systems in asynchronous networks, and the current crypto exchange methods are examined. A general transaction structure suitable for the entire system is created.

Afterward, the system was completed by generalizing the clearing business by offering a monetary infrastructure used by the central banks, the largest clearing instrument. While designing this system, firstly, the different features and advantages of all cryptocurrencies are listed. The design was made by taking into consideration the needs of the Central Banks.

People should be able to exchange various cryptocurrencies with each other freely and securely. Today, the most practical way to do this is central cryptocurrency exchanges. In these central cryptocurrency exchanges, users send

the cryptocurrencies they want to trade to these exchanges. In this situation, users are forced to live with the risk of being hacked or stealing money from the insider in the stock market. Decentralized cryptocurrency exchanges are undertaken to eliminate these risks.

We can examine the work of decentralized cryptocurrency exchanges under 2 main headings. (1) Order matching and (2) atomic swap.

People need to agree on the price before they can trade. In a decentralized stock market, this is also achieved using blockchain technology, as in cryptocurrencies. So the stock market itself is also a cryptocurrency. In this way, there is no need for a central server for the stock exchange to work. Also, this cryptocurrency is used to provide the incentive-deterrence necessary for the parties to complete the agreement during the atomic exchange.

3.1 An Exemplary Scenario

An atomic swap is made to realize the amounts agreed during order matching without mutual trust.

A typical atomic swap is done as follows (Figure 1).

Let's say Alice and Bob have agreed for 1 bitcoin (BTC) for 100 litecoin (LTC). Alice will send 1 BTC to Bob, Bob will send 100 LTC to Alice.

In blockchains, crypto money can be sent to an address or to a script. With inputs that return the result of the scenario to the right, these cryptocurrencies can be sent to other addresses or scripts.

Alice sends 1 BTC to Bob's address with a password Alice knows or a script that can be sent to Alice's address after a long period of time.

Bob sends 100 LTC to Alice's password or a script that can be sent to his own address after a short time. Bob's short return time shall be smaller than Alice's long return back time.

If Alice sends 100 LTC from the script sent by Bob to his own address, he will show his password to the world and to Bob.

Thus, Bob can withdraw 1 BTC from the script that Alice locks 1 BTC, using the same password to her address.

If Alice does not withdraw 100 LTC to her address at the end of the time Bob enters the script, Bob sends 100 LTC to her address because it is up and not settled.

Alice, too, can wait until her longer expire time and send 1 BTC to her address.
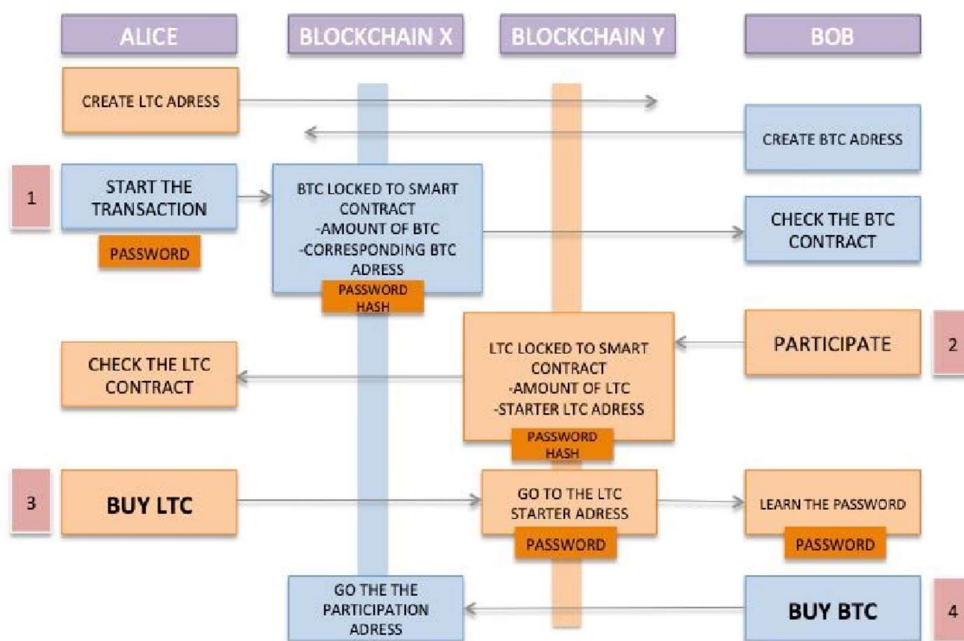

Figure 1. Exemplary Scenario

In summary, both of the transactions occur one after the other, or none of them executes and rolls back.

There are other difficulties in the decentralized cryptocurrency exchange. During these waiting periods, as a result of the price progressing negatively, one of the parties may stop trading.

To prevent this, it is necessary to take deterrent measures. In general, a certain proportion of the traded value is left pledge in the cryptocurrency before the transaction begins, and only returned to the party that carries its responsibility.

3.3 Achievements

Risks of Persons- Decommissioning of 3rd Persons in the Finance Industry

The financial industry relies heavily on trusted 3rd Persons. Assets such as clearing houses, central counterparties, stocks, and futures exchanges exist to reduce the risk between financial institutions that do not fully trust each other but need to work together. Adding such third parties to the process creates new problems (Radivojak & Grujic, 2019). The model reduces the need for trusted third parties and is an achievement to eliminate those parties.

Technical Failure

In some cases, the third party may become a single potential point of failure. Technical malfunctions may occur, or central effects may occur. For example, in October 2014, when the "Real-Time Gross Settlement" payment system, which was responsible for cleaning hundreds of thousands of payments worth £ 275 billion a day, did not work for ten hours, significant payments were delayed. This led to the need for an independent review. Similar problems may arise in exchanges, which are central assets where buyers and sellers meet. This process leaves customers at risk, they may be temporarily unsure about the status of the transactions. Another example of this is that the New York Stock Exchange did not operate for more than three hours in July 2015 due to a software error (Popper, 2015). On distributed models, the system may on multiple servers and it can be verified, run or followed on those instances. It has no risk of having central downtime or failure.

Third parties are at risk from both external hackers and internal employees. The intensity of valuable data has made third parties an attractive target for both reselling data and damaging systems. Internal employees have privileged access to data and systems. This lack of security increases the risk (Musonera & Vincent, 2008). On Decentralized exchange models the users keep their money on their wallets hence eliminates the risk of theft and hacking.

Often the third parties of the industry are a monopoly and industry participants, and usually they have no alternative. Therefore, deep-rooted industrial organizations have no real reason to offer competitive prices and produce superior customer experience. No efforts for innovation are made. For example, SWIFT, an interbank messaging network and standardization scheme used to send messages related to payments, is proof that there is no real competition in the banking industry. Similarly, CLS (a specialist US financial institution) is the de facto swap mechanism in FX transactions. Many countries use swap banks for stock transactions. Each of such trusted third parties acts as a semi-monopoly for their functions (Destais, 2014). On decentralized exchange model, the system runs on competitive, transparent and published model. It is easy to understand and fork the system when the existing market becomes inefficient by any external reason.

Since international third parties have jurisdiction that may differ from the jurisdiction where each party has a transaction, this is a new legal risk factor. There are many reasons why trust, power, and control are not desired to be given to third parties. The potential for the reconciliation of distributed books (distributed ledger) allows third parties to be removed from the system. However, even when third parties are removed from the system, it is seen that the participants have achieved real results (Locher et al., 2018).

Filling Trust Gaps

Blockchains are ideal solutions for objective entities that do not fully trust each other and need a data source protected from manipulation or need to agree on a specific transaction (Gervais et al., 2016).

Paper System

Paper documents have historically been used to replace trust. Instead of relying on the trader's speech, the certificate of authenticity is relied. However, over time, digitally signed documents have become widespread against the risk of duplication or copying of paper documents. Blockchains can guarantee authenticity and create privacy records that protect privacy (Lemieux, 2017).

Technology Trust Trump

In cases where digital records are kept centrally by a single party, if the asset's trust is low or the business has to show that the data cannot be intervened, blockchains can be used as a solution. If data is on a blockchain, this is an indication that previous chain is accepted and confirmed with a mathematical trust (Meijer, 2017).

4. Conclusion

Central platforms or trusted third-party systems may contain human error. Due to its decentralized nature, the model on this paper is a blockchain based distributed peer to peer transfer where security risks arising from human error will be prevented. Also, when the need for intermediary systems are eliminated, security risks, hacking and digital attacks on central system will be eliminated. Only the people at both ends and their own personal wallets will be affected on any security issue on their personal systems where it is not related with usage of this system. If any of the peers on both sides do not verify the transfer, the transfer will be cancelled at all and their money will be returned to their own wallets. This was a transaction model is formed, therefore, there are not any problem of loss on system breakdown.

Central platforms require operational processes for clearing transactions and to act as intermediaries. This makes users dependent on a platform and requires a period of time to execute. With this model, the exchange process will take place in between spouses only regardless of system load. Since the investment on central platform and work load required to act as intermediary will be diminished high commission fees deducted on transactions will be eliminated. With the new model, usage and spread of blockchain technologies will increase. On the second part of the model, It is aimed to solve the liquidity problem through payment channels technology and channel provider investors.

The weak parts of this model are, the time required for distributed handshake is longer than regular CPU time on a single machine. Like TCP model on network packets, it requires a handshake on both parties where a response waiting time is required. This handshake time is longer than the regular transaction times on single machine. Another weak part is, the system has a distributed model and a chain which requires some parties to maintain the ladder and running the chain for handshake. It is cost efficient but requires at least one party to initiate the system. This part can be solved using private chain on existing blockchain platforms and models. Also, a market maker is required to lower the initial bid ask spread since at the beginning till enough people begin to use the system, there will not be much buyer and sellers. System requires lower rates to attract more people. It is like torrent based distributed download systems, where it requires some initial people for seeding the torrent files so that more and more people will begin to download and distribute and after a period of time it will become a very efficient platform.

The innovative part of this model is providing a smart contract based transaction model on blockchain where it will be possible for peers to agree on the price and exchange values without requiring a trusted third party. If any failure occurs or any part renounce during transaction it will return back to beginning state where each party will receive their money back.

In the future a payment channel and liquidity provider can be added to this transaction model in order to decrease the time required for payments, thus, it will be possible for high frequency traders to adapt to the system, which will increase the liquidity, system use and lower the bid ask spread.

Acknowledgements

References

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Čapkun, S. (2016). On the security and performance of Proof of Work blockchains. In *CCS 2016 - Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (Vol. 24-28-October-2016, pp. 3-16). Association for Computing Machinery. https://doi.org/10.1145/2976749.2978341

Hencic, A. & Gouriéroux, C. (2015). Noncausal Autoregressive Model in Application to Bitcoin/USD Exchange Rates.. In V.-N. Huynh, V. Kreinovich, S. Sriboonchitta & K. Suriya (ed.), Econometrics of Risk , Vol. 583 (pp. 17-40) . Springer . ISBN: 978-3-319-13448-2.

Dai, Bo & Forsythe, Sandra & Kwon, Wi-Suk. (2013). The impact of online shopping experience on risk perceptions and online purchase intentions: Does product category matter?. Journal of Electronic Commerce Research. 15. 13-24.

Christophe Destais (2016) Central Bank Currency Swaps and the International Monetary System, *Emerging Markets Finance and Trade,* 52:10, 2253-2266, DOI: 10.1080/1540496X.2016.1185710

Gunes Corlu, Canan & Corlu, Alper. (2014). Modelling exchange rate returns: which flexible distribution to use?.

Quantitative Finance. 15. 1-14. 10.1080/14697688.2014.942231.

Meijer, D.B. (2017). Blockchain Technology: Trust and/or Control?, TU Delft University Final Paper.

Tapscott, D., Tapscott, A. (2016). The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, *Business, and the World*, ISBN 978-0-670-06997-2.

Musonera, E. & Vincent, S. (2008). Establishing a Stock Exchange in Emerging Economies: Challenge and Opportunities.

Parlapiano, F. & Alexeev, V., Dungey, M. (2015). Exchange rate risk exposure and the value of European firms. *The European Journal of Finance*. 23, 1-19. 10.1080/1351847X.2015.1072570.

Bruneau, G. & Moran, K. (2017). Exchange rate fluctuations and labour market adjustments in Canadian manufacturing industries. *Canadian Journal of Economics/Revue canadienne d'économique*, 50, 72-93. doi:10.1111/caje.12251

Radivojak, G. Grujic, M. (2019). Future Of Cryptocurrencies and Blockchain Technology in Financial Markets. 1. 56-75. 10.7251/JOCE1901056R.

Zubaydi, H. D., Chong, Y.-W., Ko, K., Hanshi, S. M., & Karuppayah, S. (2019). A Review on the Role of Blockchain Technology in the Healthcare Domain. *Electronics*, 8(6), 679. doi:10.3390/electronics8060679

https://en.wikipedia.org/wiki/Mt._Gox Acces Date: 10 May 2020.

https://www.nytimes.com/2015/07/09/business/dealbook/new-york-stock-exchange-suspends-trading.html

Chu, J. Nadarajah, S. & Chan, S. (2015). Statistical Analysis of the Exchange Rate of Bitcoin. *PLoS ONE,* 10(7): e0133678. https://doi.org/10.1371/journal.pone.0133678

Joshi, J., Nepal, S. & Zhang, Q. (2019). Blockchain – ICBC 2019: Second International Conference, Held as Part of the Services Conference Federation, SCF 2019, San Diego, CA, USA, June 25–30, 2019, Proceedings.

Cermeño, J. S. (2016). Blockchain in financial services: Regulatory landscape and future challenges for its commercial application.

Kristoufek, L. (2013). BitCoin meets Google Trends and Wikipedia: Quantifying the relationship between phenomena of the Internet era. *Scientific reports*. 3., 3415. 10.1038/srep03415.

Goodman, L. M. (2014). The Face Behind Bitcoin, *Newsweek*, 14 March 2014.

Locher, Thomas & Obermeier, Sebastian & Pignolet, Yvonne-Anne. (2018). When Can a Distributed Ledger Replace a Trusted Third Party?.

Brière, M. & Oosterlinck, K. & Szafarz, A. (2013). Virtual Currency, Tangible Return: Portfolio Diversification with Bitcoin. *SSRN Electronic Journal*. 16. 10.2139/ssrn.2324780.

Nofer, M. & Gomber, P. & Hinz, O. & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering.* 59. 10.1007/s12599-017-0467-3.

Schröder, M. (2017). The equilibrium real exchange rate and macroeconomic performance in developing countries, *Applied Economics Letters*, 24:7, 506-509, 10.1080/13504851.2016.1205718

Popper, N. (2015). The Stock Market Bell Rings, Computers Fail, Wall Street Cringes

Kisembe, P. & Jeberson, W. (2017). Future of Peer-To-Peer Technology with the Rise of Cloud Computing. *International Journal of Peer to Peer Networks*. 8. 45-54. 10.5121/ijp2p.2017.8304.

Greene, R. & and McDowall, B. (2018). Liquidity or Leakage. Plumbing Problems with Cryptocurrencies". *Distributed Futures*, Z/Yen Group.

Houben, R. & Snyers, A. (2018). Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion', PE 619.024, 15.

Zhang, R., Xue, R. and Liu, L. (2019). Security and Privacy on Blockchain. *ACM Comput. Surv*. 1, 1, https://doi.org/10.1145/3316481

Chan, S., Chu, J., Nadarajah, S. & Osterrieder, J. (2017). A Statistical Analysis of Cryptocurrencies. *Journal of Risk and Financial Management*, 10. 12, 2017. 10.3390/jrfm10020012.

Delgado Segura, Sergi & Pérez-Solà, Cristina & Herrera-Joancomartí, Jordi & Navarro-Arribas, Guillermo & Borrell, Joan. (2018). Cryptocurrency Networks: A New P2P Paradigm. *Mobile Information Systems*. 2018. 1-16. 10.1155/2018/2159082.

Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing list at https://metzdowd.com.

Park, S., Im, S., Seol, Y., Paek, J. (2019). Nodes in the Bitcoin Network: Comparative Measurement Study and Survey. *IEEE Access*, 7, 57009–57022.

Raval, S. (2016). "What Is a Decentralized Application?". *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology.* O'Reilly Media, Inc. pp. 1–2. ISBN 978-1-4919-2452- 5. OCLC 968277125.

Sapuric, S. & Kokkinaki, A. (2014). Bitcoin Is Volatile! Isn't that Right?. *Lecture Notes in Business Information Processing*. 183. 255-265. 10.1007/978-3-319-11460-6_22.

Seyyedi, S. (2017). Analysis of the Interactive Linkages Between Gold Prices, Oil Prices, and Exchange Rate in India. *Global Economic Review*. 46, 1-15. 10.1080/1226508X.2017.1278712.

Lemieux, V. (2017). *A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation,* 2271-2278. 10.1109/BigData.2017.8258180.

Yan, Y., Wang, L., Liu, K., Wu, Y., Wu, J. (2019). Effective Data Transmission Strategy Based on Node Socialization in Opportunistic Social Networks. *IEEE Access*. PP. 10.1109/ACCESS.2019.2898895.