Association for Information Systems
AIS Electronic Library (AISeL)

CONF-IRM 2019 Proceedings

International Conference on Information Resources Management (CONF-IRM)

5-2019

The potential effect off-chain instant payments will have on cryptocurrency scalability issues – The Lightning Network

Jagger S. Bellagarda
The University of Pretoria, U15165702@tuks.co.za

The potential effect off-chain instant payments will have on cryptocurrency scalability issues – The Lightning Network

Jagger S. Bellagarda
The University of Pretoria
U15165702@tuks.co.za

Abstract
The rapid increase in popularity regarding cryptocurrency and specifically Bitcoin has been unprecedented over the past number of years. However, scalability has become a major barrier keeping it from gaining wide spread mass adoption. The purpose of this paper will be to investigate the potential effect off-chain instant payments will have on cryptocurrency scalability issues, with a focus on the Lightning Network. This will be achieved by means of a quantitative study through the process of testing various factors associated with the Lightning Network against another potential scalability solution, increasing block size limit. This study will provide comprehensive insight into off-chain instant payments generally and the Lightning Network specifically. This research paper will, therefore, primarily add to the body of knowledge indicating whether the Lightning Network is a potential solution to scaling the Bitcoin blockchain. In addition, it will lay a foundation for future research into the scalability of cryptocurrency.

Keywords:
Lightning Network, Bitcoin, Off-Chain Instant Payments, Blockchain Technology

1. Introduction
Since the release of the Bitcoin whitepaper by Satoshi Nakamoto (Nakamoto, 2008), cryptocurrency has been rapidly grabbing mainstream attention. In addition, Blockchain has gained tremendous momentum over the past year and has achieved an understanding of global proportions. It has gone far beyond just revolutionizing existing financial frameworks but has been viewed by many to have a much wider application potential (Xavier Olleros & Zhegu, 2016).

However, even though huge inroads have been made into the mass adoption of blockchain technology, there is still several issues holding it back. The biggest of these and the main topic for this paper is scalability, and that until it has been solved, blockchain will always be limited by its ability to scale. In this paper, the proposed scalability solution of off-chain instant payments will be discussed with Bitcoins Lightning Network taking centre stage of the study. The Lightning Network is a proposed solution to dealing with the monumental adoption of Bitcoin. It acts as a "second layer" payment protocol utilizing its own smart-contract scripting language allowing for the occurrence of instant transactions between network participants (Lighning Network, 2017). Presently the speed of the Bitcoin network is dependent on block confirmation times but with the Lightning Network's intention to allow individuals to make off-chain transactions with the confidence of on-blockchain enforceability, it will allow the Bitcoin blockchain to scale in parallel to the rapid influx of participants to the network.

The aim of this research paper will therefore be to determine whether the Lightning Network is a potential viable scaling solution and whether or not another scaling alternative may be preferred.

2. Literature Review

The following literature review will systematically detail what Bitcoin is and explain why it is struggling to scale. Furthermore, it will discuss the difference between on-chain and off-chain instant payment soltions before finally elaborating on the Lightning Network – a potential off-chain payment solution to scaling Bitcoin.

2.1. Bitcoins scalability issue

Bitcoin is defined as an open-source, decentralised peer-to-peer electronic cash system (Nakamoto, 2008). Due to the rapid rise in its popularity, a simultaneous increase in the network of nodes has occurred. Based on blockchain research, the higher the number of nodes connected, the longer it takes to reach a consensus and validate a Bitcoin transaction. This results in the average speed of a transaction being confirmed decreasing as the blockchain network gets larger.

The biggest technical parameter contributing to the fact that Bitcoin cannot manage the amount of transactions comes down to its block size limit. Based on blockchain research, each block contains a finite amount of transactions. Satoshi Nakamoto set a 1 Megabyte block size for Bitcoin which was done as a security measure to prevent DoS attacks from occurring. This is where hackers could create exceptionally large blocks and broadcast it across the network with the hopes of incapacitating it. The results of block size limits being insufficient is that when the Bitcoin network reaches peak loads, it gets highly congested. This results in transactions taking hours and sometimes even days to be processed. Another vital issue is that miners are more inclined to process transactions that offer a higher transaction fee which has resulted in senders of transactions to compete with one another by paying higher and higher fees in order for their transactions to be processed faster (Marshall, 2017).

The scalability issue facing Bitcoin and many other cryptocurrencies is one of the main obstacles standing in the way of mass adoption. As the user base of Bitcoin enthusiasts and users continues to grow, so does the network and if Bitcoin cannot scale accordingly then it may reach the end of its lifespan.

2.2. Off-Chain Instant Payments: The Lightning Network

2.2.1. On-chain vs. Off-chain Instant Payments

An on-chain Instant payment is a first layer payment solution. A suitable number of miners will validate a transaction and broadcast it to the whole network, thus reflecting it on the public ledger and making fundamental changes to the blockchain (Investopedia, 2018). The term “off-chain” refers to the fact that payments made between two parties are not completed on the main blockchain of a cryptocurrency and are instead processed off-chain through payment channels. Once a payment channel is closed by the participating parties, the final amount is pushed to the network and added to the respective blockchain. It is imperative to note that off-chain instant payments are finalised almost immediately with little to no fees involved, opposed to on-chain transactions that majority of the time take longer to be confirmed and involve higher fees(Investopedia, 2016).

2.2.2. Lightning Network overview

The Lightning Network was first proposed by Thaddeus Dryja and Joseph Poon in their 2015 whitepaper as a potential solution to the ongoing problem of scaling cryptocurrency and specifically the Bitcoin blockchain. It essentially involves adding a “second layer” payment protocol on top of the Bitcoin blockchain that would eventually settle onto it (Poon & Dryja, 2015). Second layer refers to secondary applications that are built and run on top of the main

blockchain and make no fundamental changes to the actual blockchain. Transactions are instead off-loaded to these secondary payment channels with the aim of allowing users to send and receive payments instantaneously with reduced transactions fees. It is important to note that the Lightning Network was made possible by the implementation of Segregated Witness, which brought with it the ability to perform instantaneous transactions and allowed for transaction malleability (SegWit Resources, 2017).

Due to the nature of a payment channel setup between the two users, the amounts transferred are not broadcast to the entire blockchain network and are therefore almost instantaneous and carry little or no transaction fees. Once the payment channel is closed, the final amount, which is a sum of all the transactions that occurred on the channel is pushed to the blockchain network. Therefore, what would essentially be multiple transactions flowing through the Bitcoin blockchain is now solidified into just one final transaction. It would be highly useful for big business who make regular payments with other parties to perform those transactions off-chain at near immediate speeds(Poon & Dryja, 2015).

The versatility of the Lightning Network is one of its most important aspects – the ability for users who don't have direct payment channels with each other to still be able to send Bitcoin using connected payments channels. This can be highlighted through the following imaginary narrative according to the *six degrees of separation* theory (The Oxford Math Center, 2018). This theory states that all people are six, or fewer, connections away from each other and that everyone can trace back to each other through six or less social relationships. This forms the basis of how users of the Lightning Network can make payments using the multi-signature channels of others. The following details an example:

Person A intends to send money to Person C, but they do not have a payment channel setup. Person A does, however, have a payment channel with Person B and Person B has a payment channel with Person C. The transaction will therefore still be able to work between Person A and Person C. Details are presented in Figure 1.

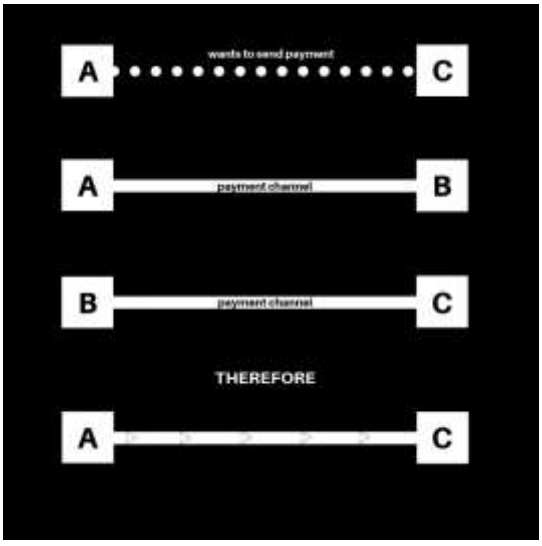


Figure 1: A graphic displaying the versatility of the Lightning Network according to the six degrees of separation theory.

2.2.3. Lightning Network operations

The following analogy will explain in-depth, how the Lightning Network operates.

Two Individuals exist – John and Bob, who are users on the Bitcoin network. They plan to send each other money quite often and want to do it with the lowest possible transaction fees. They therefore decide to create a payment channel on the Lightning Network.

Step 1: Multisignature Wallets

John creates a payment channel (multisignature wallet) and selects Bob to share it with. John and Bob both send, in this case 0.05 BTC to the 2-of-2 multisignature wallet – this process is called the "opening transaction" and is a normal Bitcoin transaction and is therefore on-chain. After this, all transactions occur in the payment channel (off-chain) and are known as "commitment transactions". A multisignature wallet is setup for security reasons and requires multiple digital signatures (or passwords) from the various parties for it to be opened (Dedi, 2017).

Step 2: Multisignature Transactions

As a type of "smart contract", John and Bob each create a 2-of-2 multisignature transaction that pays out 0.05 BTC to each of them respectively. A multisignature transaction is where X number of public keys are put in place on the condition that at least Z of those keys are required for a transaction to take place. In layman's terms, it is a transaction that requires the private keys of all parties involved in order to for it to be authorized (Cryptoverze, 2018). Hypothetically, should John sign this transaction and send it to Bob, he would just have to add his signature to it in order to place it into effect and add it to the Bitcoin blockchain. It should be noted that a visa versa of this example would operate the exact same way. These so-called pay-out transactions also utilize HTLC (Hash Time Locked Contract) which is a technology that locks the amount paid out by the executing party for a specific period in order to avoid fraudulent transactions from occurring (Cryptoverze, 2018).

Step 3: Creating a Payment

John wants to pay 0.01 BTC to Bob. A "smart contract" is generated by John that states he receives 0.04 BTC and Bob receives 0.06 BTC. The process then moves onto each party receiving a transaction signed by the other as mentioned in step 2. It is imperative to understand that neither party can try and sign the old transaction (0.05 BTC to each person respectively) due a "anti-cheat" transaction each party can generate. Once one-party attempts to activate the now "invalid" transaction, the funds are locked for a specific period (as mentioned in step 2) and the other party has time to broadcast the "anti-cheat" transaction which sends the result amounts of the first transaction to the other. Due to the potential of earning a specific percentage of the "anti-cheat" transaction as a bounty for identifying a fraudulent transaction, all nodes on the network can now be on the lookout for these "invalid" transactions (Unocoin, 2018).

In conclusion, John and Bob can continue to send as many payments back and forth between each other through the setup payment channel almost instantaneously (depending on how quickly they communicate with each other) without broadcasting anything to the Bitcoin blockchain. Should one of them try and defraud the other by attempting to broadcast a fraudulent payment, they will be held liable by the entire network who will be watching.

3. Research Methodology

This research paper is aiming to determine the potential effect off-chain instant payments will have on cryptocurrency scalability issues. Therefore, due to the nature of this study, the most suitable way to research the potential effect of off-chain instant payments will have in comparison to an alternative is to perform a quantitative study. A collection of current and

historical data will be collected and analysed regarding each protocol that aims to scale Bitcoin. The Lightning Network, Bitcoin Cash and Bitcoin will each be evaluated solely and in some cases against each other. The evaluation will compare each protocol against a set of predetermined criteria that includes factors such as number of nodes, the transaction fees associated with each protocol and the change in the number of unconfirmed Bitcoin transactions over a specific period.

A positivist research paradigm will be undertaken. A positivist research paradigm states that only facts gained through measured observation are viewed as trustworthy. In this research paradigm, the researcher is limited to data collection and objective interpretation of that data. This coupled with the research approach describes why a positivist research paradigm is favoured regarding this study. Since this research paper will take a quantitative approach, an experiment research strategy will be employed. The cause-and-effect of several different variables will be established, and the researcher will aim to control all these variables other than the one between manipulated. The result of these experiments between the independent and dependent variables will be collected and analysed in order to draw an educated conclusion (Center for Innovation in Research and Training, 2017).

An experiment was used whereby data was collected regarding current proposed scaling solutions of Bitcoin. The following proposed scaling solutions were studied:

- The Lightning Network
- Increasing block size limit (Bitcoin Cash)

A criterion of factors was used to analyse one and/or both solutions against Bitcoin. The following is a list of these factors:

- Number of nodes
- Growth in the number of nodes
- Transaction fees (measured per byte)

Finally, in order to gain the potential effect off-chain instant payments will have on cryptocurrency scalability issues (the main research question) an in-depth analysis of the Bitcoin mempool was conducted. This would indicate the level of congestion on the Bitcoin blockchain both pre-and post the Implementation of the Lightning Network.

The following research questions were asked when viewing the pre-existing data:

1. What is the current number of nodes for both Bitcoin Cash and the Lightning Network (as documented in May 2018)?
2. What is the growth in terms of number of nodes for both Bitcoin Cash and the Lightning Network since its launch?
3. What is the current transaction fee (per byte) between Bitcoin, Bitcoin Cash and the Lightning Network?
4. How has the mempool size of Bitcoin changed pre- and post the implementation of the Lightning Network?

Each of these questions will be asked using a quantitative research approach and an experiment-based research strategy based on a document and record review data gathering technique.

4. Findings & Discussion

4.1. Number of nodes

A node can be described in layman's terms as a point of connection (any device) to a blockchain network. It is an imperative aspect to the popularity and ultimate survival of a specific protocol because it details the volume of users that want to participate in that network. In order to compare the number of nodes currently operating within Bitcoin (as a standard), Bitcoin Cash and the Lightning Network respectively, external tracking agents were utilized. Details are presented in Table 1 (figures were documented in May 2018).

Protocol	No. of Nodes	Source
Bitcoin (Standard)	9502	https://coin.dance/nodes
Bitcoin Cash	2015	https://cash.coin.dance/nodes
Lightning Network	3454	https://1ml.com/statistics

Table 1: The number of nodes between Bitcoin, Bitcoin Cash and The Lightning Network

It can be concluded that based on the data recorded, the Lightning Network is gaining traction in terms of number of nodes in its network. It has a 1439 more nodes than Bitcoin Cash (3454 – 2015) which indicates the popularity and use of the network is on an upward trajectory.

4.2. Growth of nodes

A further study was conducted into both Bitcoin Cash and the Lightning Network in order to gain a deeper understanding around the growth of nodes each protocol since their inception. It must be noted that in terms of the Lightning Network, only nodes with channels were recorded. Bitcoin statstic engines *Bitcoin Visuals* and *Coin Dance* were used as sources for the Lightning Network & Bitcoin Cash respectively. The data gathered was recorded monthly for both Bitcoin Cash and the Lightning Network. Details are presented in Table 2.

Date (Data was recorded on the 19th day of each month)	Number of nodes (Bitcoin Cash)	Number of nodes (Lightning Network)
June 2017	0	-
July 2017	92	-
August 2017	1180	-
September 2017	1080	-
October 2017	1040	-
November 2017	1500	-
December 2017	1450	-
January 2018	1410	54
February 2018	1420	557
March 2018	1930	672
April 2018	1950	1054
May 2018	2180	1322
June 2018	2110	1446
July 2018	2130	1502
August 2018	2230	1519
September 2018	1860	1571

Table 2: The number of nodes gathered monthly between Bitcoin Cash and The Lightning Network

Furthermore, in order to display the growth of each protocol over the time period, a line graph was generated. Details are presented in Figure 2.

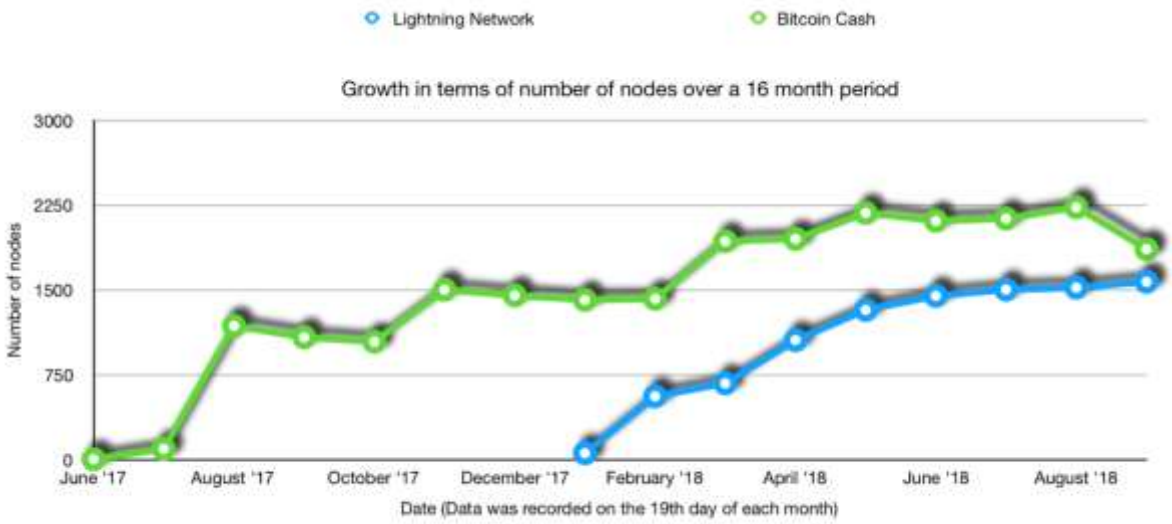


Figure 2: The growth in number of nodes between Bitcoin Cash and the Lightning Network since their inception

A few conclusions can be drawn:

1. Bitcoin Cash and the Lightning Network have both experienced a linear increase in the growth of number of nodes.
2. The Lightning Network, however, has seen a continuous upward trajectory while Bitcoin Cash has experienced several drops in its growth.
3. The Lightning Network has also reached near the same number of nodes as Bitcoin Cash in around half the time. This is further validated since only nodes in the Lightning Network with channels were measured.

4.3. Transaction fees

Transaction fees in my opinion, are regarded as the corner stone to the ultimate success of a cryptocurrency achieving wide-spread mass adoption. The amount it will cost an individual when they make use of Bitcoin needs to be low enough to compete with current banking models but at the same time keep intact key aspects, such as decentralisation and anonymity.
In order to gain the transaction fees of each protocol, a measurement of the number of Satoshi's per byte (sats/byte) was conducted for Bitcoin, Bitcoin Cash and the Lightning Network simultaneously in order to gain the most accurate result. The transaction data for Bitcoin and Bitcoin Cash was gathered from *BTC*, a reliable search and analysis engine. However, the transaction data for the Lightning Network was a more strenuous process since transactions occur in a payment channel and are therefore off-chain. The measurement of transaction fees can only be recorded when the payment channel is opened and closed.

Therefore, in order to track the fees incurred from using The Lightning Network, an experiment was executed which utilized a testnet wallet on a test site. The test site used is Starblocks where "virtual" drinks can be purchased using Bitcoin. The testnet wallet being used is Eclair Testnet Wallet.

The following process was executed:
Step 1: Create a new wallet
A new wallet was generated via the Eclair Testnet Lightning Wallet. This is an Android based wallet and is solely intended for Lightning Network testing.

Step 2: Load Bitcoin
A total of 0.14751261 BTC was loaded via a testnet faucet. This is a web-based program and provides "testing Bitcoin" to be used solely for testing purposes and holds no real-world value.

Step 3: Open a lightning channel and add funds
A lightning channel was created and funded with 0.00500705 BTC (31.7974 USD). The fee to open this channel was 705 Satoshi's (0.0448 USD) and was 149 bytes in size.

Step 4: Make a purchase
A purchase of 53 "Blockaccino's" was made on the Starblocks test site in order to create the equivalent worth of a normal $5 Coffee. This payment was made via the lightning channel opened and was repeated four times in order to display the purchase of each item in the store (see Appendix A).

The following details the costs of each item:
53 x Blockaccino = 0.000795 BTC (5.17 USD)
53 x Espresso Coin Panna = 0.000901 (5.85 USD)
53 x Scala Chip Frappuccino = 0.001007 (6.54 USD)
53 x Satoccinamon Dolce Latte = 0.000636 (4.13 USD)
Total = 21.69 USD

It must be noted that the purchase of these items is off-chain and therefore, confirmed near instantaneously (less than one second).

Step 5: Closing the lightning channel
The lightning payment channel is closed and pushed to the Bitcoin blockchain. The fee incurred to close this channel is 510 Satoshi's (0.033 USD) and was 115 bytes in size.

Calculation of fees:

1. Opening Channel
   705 Satoshi/ 149 bytes = 4.73 Satoshi's per byte

2. The 4 x purchases on the test site = No Fees (*as it was made off-chain in the lightning channel)

3. Closing Channel
   510 Satoshi/115 bytes = 4.43 Satoshi's per byte

Total: (calculating the average Satoshi per byte)
(4.73 + 4.43) / 2 = **4.58 Satoshi's per byte**

Figure 3: Transaction fee calculation

It can therefore be stated that the average Satoshi per byte it cost for this Lightning Network transaction was 4.58 Satoshi's per byte.

The search and analysis engine BTC was utilized to gain the current transaction fees in Satoshi's per byte for both Bitcoin and Bitcoin Cash respectively. The recordings were taking simultaneously to the Lightning Network experiment carried out in order to receive the most accurate results possible. Bitcoin recorded 20 Satoshi's per byte as the most common transaction fee while most Bitcoin Cash transactions paid a 2 Satoshi per byte fee. Details are presented in Table 3.

Protocol	Transaction Fee (Satoshi's per byte)	Source
Bitcoin (Standard)	20	http://www.btc.com/
Bitcoin Cash	2	http://www.btc.com/
Lightning Network	4.58	StarBlocks Experiment

Table 3: The difference in transaction fees between Bitcoin, Bitcoin Cash and The Lightning Network

Based on the data recorded, it can be deduced that both The Lightning Network and Bitcoin Cash offer solutions to lower transaction fees when opposed to the current standard of Bitcoin. It is also important to highlight that the transaction fees of Bitcoin Cash (2 sats/byte) was ten times smaller than that of Bitcoin while the transaction fee of the Lightning Network experiment recorded was around a quarter of the size.

4.4. Mempool size

The mempool is defined as a network holding area for unconfirmed transactions that have not entered a block yet. Every node stores these unconfirmed transactions in RAM and removes them once they have been confirmed (Hearn, 2015). This section will analyse the size of Bitcoin's mempool over a twelve-month time period, with a focus on how the launch of the Lightning Network has affected it. The source of this data is assembled and synthesised from Blockchain, a Bitcoin blockchain-oriented search and analysis engine.

It is imperative to point out that the first mainnet Lightning Network beta (lnd 0.4-beta) was launched on 15 March 2018, according to a blog post made by the Lightning Labs team. This will act as a foundation and as a generous assumption for analysing how it changed the Bitcoin mempool size("Announcing our first Lightning mainnet release, lnd 0.4-beta!," 2018). Appendix I displays the Bitcoin mempool over a twelve-month period (November 15th, 2017 to October 15th, 2018). An analysis of the lowest and highest number of unconfirmed transactions was conducted for each month before and after the launch of the Lightning Network. Details are presented in Table 4.

Month	Lowest level (bytes)	Highest level (bytes)
November 2017	33 425 330	115 578 828
December 2017	60 057 338	128 213 319
January 2018	10 516 329	139 487 969
February 2018	274 434	91 719 602
Lightning Network Launched		
April 2018	17 113	38 191 799
May 2018	36 627	16 565 346

June 2018	47 121	47 786 066
July 2018	34 951	49 425 791
August 2018	22 990	19 370 242
September 2018	56 127	24 763 564
October 2018	69 694	12 249 159

Table 4: The difference in the Bitcoin mempool size pre- and post-implementation of the Lightning Network

Note: The month of March was excluded from this study in order to gauge the full effect of the Lightning Network in the months before and after its launch.

The following deductions were made from this analysis:

1. The average number of transactions (in bytes) pre-Lightning Network release

Lowest level
(33 425 330 + 60 057 338 + 10 516 329 + 274 434) / 4
= 26 068 357.8 bytes

Highest level
(115 578 828 + 128 213 319 + 139 487 969 + 91 719 602) / 4
= 118 749 930 bytes

2. The average number of transactions (in bytes) post-Lightning Network release

Lowest level
(17 113 + 36 627 + 47 121 + 34 951 + 22 990 + 56 127 + 69 694) / 7
= 40 660.4 bytes

Highest level
(38 191 799 + 16 565 346 + 47 786 066 + 49 425 791 + 19 370 242 + 24 763 564 + 12 249 159) / 7
= 29 764 566.7 bytes

Figure 4: Mempool calculation

Based on Appendix B and the data recorded and analysed, it can be concluded that the number of unconfirmed transactions in the Bitcoin mempool has decreased drastically since the launch of the Lightning Network. The lowest level (in bytes) decreased 64102% and the highest level (in bytes) decreased over 298%. This therefore indicates that more users are opting to utilize the Lightning Network to create payment channels off-chain than submit each transaction to the blockchain. The use of the Lightning Network has therefore reduced the potential for congestion of transaction confirmation occurring.

5. Conclusion

Since the Lightning Network is still in its infancy and under development, the extent to its effect on the scalability of Bitcoin is limited yet optimistic. Since its mainnet beta launch in March 2018, a reduction in network congestion has occurred through an offering of reduced fees and near-instantaneous transaction times, the latter being the most imperative factor. The long-term effect off-chain instant payments have on cryptocurrency scalability issues is still unknown as it is yet to scale within the wider Bitcoin and cryptocurrency community. However, based on

its design, what it has been capable of thus far (according to the findings section of this paper) and after comparing it to the alternative scaling solution of increasing block size limits, it does offer a potential viable solution to scaling cryptocurrency generally and Bitcoin specifically.

References

Center For Innovation In Research And Training,. (2018). *Quantitative Approaches*. Retrieved from cirt.gcu.edu: https://cirt.gcu.edu/research/developmentresources/research_ready/quantresearch/approaches

Cryptoverze. (2018, April 2). *What is Bitcoin Lightning Network? And How Does It Work?* Retrieved from Cryptoverze: https://medium.com/cryptoverze/what-is-bitcoin-lightning-network-and-how-does-it-work-cd80ba9c0bda

Dedi, D. (2017, December 29). *Offchain Solutions: The Lightning Network*. Retrieved from Cryptoslate: https://cryptoslate.com/offchain-solutions-lightning-network/

Hearn, M. (2015, September 9). *Mempool size limiting*. Retrieved from Medium: https://medium.com/@octskyward/mempool-size-limiting-a3f604b72a4a

Investopedia. (2018, April 10). *Off-Chain Transactions (Cryptocurrency)*. Retrieved from Investopedia: https://www.investopedia.com/terms/o/offchain-transactions-cryptocurrency.asp

Investopedia. (2018, April 5). *On-Chain Transactions (Cryptocurrency)*. Retrieved from Investopedia: https://www.investopedia.com/terms/c/chain-transactions-cryptocurrency.asp

Lightning Labs. (2018, March 15). *Lightning*. Retrieved from Announcing our first Lightning mainnet release, lnd 0.4-beta!: https://blog.lightning.engineering/announcement/2018/03/15/lndbeta.%20html

Lightning Network. (2017). *Lightning Network Scalable, Instant Bitcoin/Blockchain Transactions*. Retrieved from Lightning Network: https://lightning.network/

Marshall, A. (2017). *Bitcoin Scaling Problem, Explained*. Retrieved from Cointelegraph: https://cointelegraph.com/explained/bitcoin-scaling-problem-explained

Poon, J., & Dryja, T. (2015). *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments (Draft Version 0.5.9.1)*. Retrieved from Lightning Network: https://lightning.network/lightning-network-paper.pdf

SegWit Resources. (2017). *Is segregated witness necessary to implement the Lightning Network?* Retrieved from SegWit Resources: https://segwit.org/is-segregated-witness-necessary-to-implement-the-lightning-network-6c4545a9f9f1

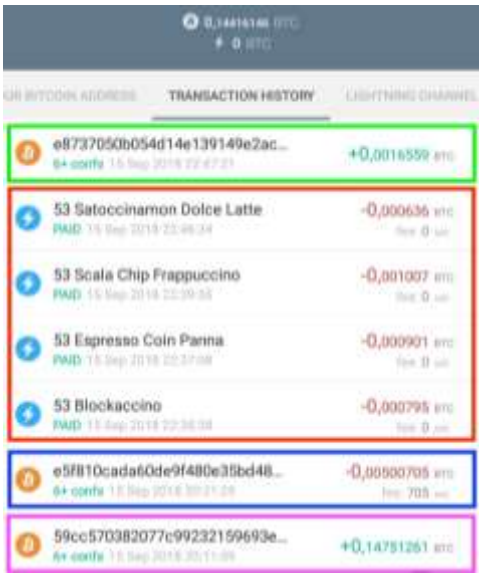
The Oxford Math Center. (2018). *Six Degrees of Separation*. Retrieved from The Oxford Math Center: http://www.oxfordmathcenter.com/drupal7/node/655

Unocoin. (2018). *What is Bitcoin's Lightning Network?* Retrieved from Unocoin: https://blog.unocoin.com/what-is-bitcoins-lightning-network-37d43f488759

Xavier Olleros, F., & Zhegu, M. (2016). Research Handbook on Digital Transformations. In F. Xavier Olleros, & M. Zhegu, *Research Handbook on Digital Transformations.* Northampton: Edward Elgar Publishing Limited.

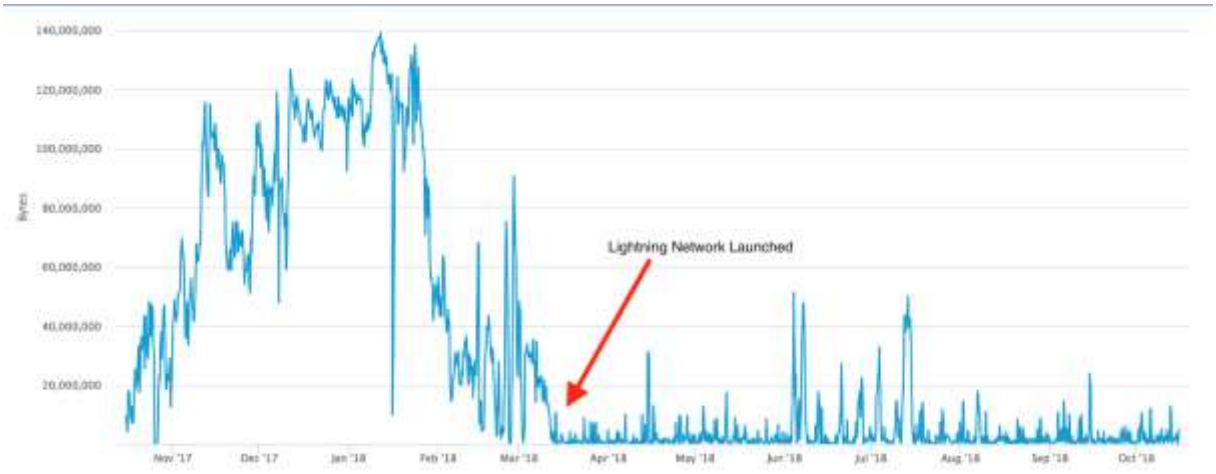
Appendix A

Éclair Wallet that displays the opening & closing of the lightning channel as well as the four purchases made within the channel.



Pink – Deposit of Bitcoin acquired from the testing faucet.
Blue – A lightning channel was opened
Red – Four purchases made in the lightning channel from the StarBlocks “virtual” store.
Green – Closing of the lightning channel.

Appendix B



Appendix C

Definition of terms

Bitcoin The first and biggest digital currency created for use in peer-to peer online transactions.

Blockchain A digital general ledger containing information that can be simultaneously used and shared within a large decentralized, publicly accessible network.

Cryptocurrency Any form of currency that only exists digitally, that usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent

	transactions. Cryptocurrency and digital currency will be used interchangeably throughout this research paper.
Mining	The generation of Bitcoin through the solving of cryptographic puzzles. It can also be viewed as the processing of users' transactions.
BTC	An abbreviation for the term *Bitcoin*.
Hash	A shorter version, fixed-length output of a larger set of data.
Node	A device connected to a *blockchain* network. It supports the network by maintaining a copy of the *blockchain* and in some situations, processes transactions.
Testnet	Alternative to the main *blockchain* of a cryptocurrency. The coins or tokens used in a Testnet hold no value and are intended for testing purposes only.
Mainnet	It is a *blockchain* that performs the actual function of sending and receiving cryptocurrency between users.
Fiat	This is legal tender whose value is backed by the government who issued it. An example would be the U.S. dollar.
DoS	Denial-of-service is a cyber attack where network resources are made unavailable to its intended users by temporarily disrupting services of a host connected to the Internet.