[[1]](#footnote-1)

Analysis of the Lighting Network(2021)

Joseph Lazarus, Puri Rudick, and Rick Fontenot

*Abstract*— **Bitcoin is the most established cryptocurrency in the market but is still rapidly developing in structure. The original decentralized transaction system now has added second level protocols to facilitate larger volumes of transactions with faster clearing times and lower fees. In this emerging second level transaction marketplace, there are low barriers to entry and opportunities to optimize structure and revenue as a transaction clearing house (node). Our goal is to analyze publicly available data on the market, set up our own node to process transactions, and study methods of optimizing our node structure and fee rates. Beyond the timeline of this initial project and as we collect private data on our node transactions, we aim to build models predicting total revenue as a response to our fee rates and liquidity. The models optimum setup would then be tested on our own node and iteratively updated with new data. Phase 2 of this project could potentially be evaluated as a capstone project.**

*Index Terms*— Bitcoin, Blockchain, Cryptography, Lightning Network, Network Analysis, Optimization, Payments,

# INTRODUCTION

B

itcoin is a digital cryptocurrency created in 2009. Unlike fiat currency, bitcoin is created, distributed, traded, and stored with the use of a decentralized ledger system, known as a blockchain. It has lower transaction fees than traditional online payments using centralized banks and government issued currencies.

Reference: <https://www.investopedia.com/terms/b/bitcoin.asp>

# On Chain Vs Off Chain Transactions

Bitcoin uses a blockchain as a ledger to record all transactions. All bitcoin in existence can be found somewhere on the blockchain. All Bitcoin transactions recorded on the blockchain are considered **on-chain transactions** and the ledger is available to the public. Bitcoin is locked in an address, and, using the private key corresponding to that address, you can sign a transaction sending this bitcoin to a new address. All on-chain transactions must pay a transaction fee in order to be included in a block. The higher the fee, the faster the transaction will be confirmed. On-chain transactions are highly secure and reliable, however transaction fees are rising based on demand and the time to confirm and clear a transaction can take 10 minutes to multiple hours. Bitcoin blocks can only hold a certain number of transactions so this method of transaction lacks scalability.

## Off Chain transactions

Off-chain transactions occur through a private peer-to-peer network where a channel is set up to make many transactions between merchant and/or individual pairs. When the parties have concluded a group of transactions, similar to a tab, the net transfer amount is recorded as a single on-chain transaction and becomes part of the public blockchain ledger. The benefits are lower transaction fees, faster (near instant) confirmation and clearing of transactions and improved scalability for large numbers of transactions. The tradeoffs are higher risk private transactions, capital to meet liquidity requirements, and capacity limits on channels which limit large transactions.\*

## Blocksize Dilemma

The reader at this point may wonder why not increase the blocksize. Doing so would increase the throughput of the system and eliminate the need for a second layer payment network. The answer is complicated. Bitcoin protocol is not controlled by anyone person or body. The Bitcoin miners are one body within the network that assert influence. The miners solve a hash problem to assemble a new block. This earns them six Bitcoins per block and processes transactions with the remaining space on the block. Each block has a theoretical maximum size of 4 megabytes but a more realistic maximum size of 2 megabytes. User who run an active node assert another vector of influence. Nodes validate transactions and blocks and accepts transactions from other nodes to support the network. Nodes check each transaction by verifying the rules of the Bitcoin Protocol are met. If a transactions breaks the rules the nodes want accept it as a valid transactions. This prevents miner’s from creating a Bitcoins out of thin air. Or unilaterally changing the Blocksize limit. Bitcoin Core developers are the third body within the network that exert influence. They test the protocol, debug and support miners and nodes.

Thus changing the protocol requires a large consensus of compute power on Bitcoin’s network from miner’s and nodes, that are supported by developers. Such a change was proposed in 2017. “Big Blockers” arguing in favor of increasing the artificial block limit. They argued doing so would benefit the network by increasing throughput. “Small Blockers” resisted the change. Their argument was that large blocksizes would inhibit ordinary individuals from running a nodes. This they argued would centralize the network to a few nodes that could handle such dramatic increase in compute and bandwidth requirements.

August of 2017 a contingent of big blockers hard-forked the protocol and started Bitcoin Cash. This created a non-backwards compatible implementation protocol that would enable bitcoin’s use as a medium for daily exchange. Less than a year later Bitcoin Cash underwent a hard-fork that saw the creation of Bitcoin SV. Both of these new protocols lacked the general support from developers, miners and nodes.

During the same period work on the lightning network continued. Second layer payment network gained wider adoption. The market for Bitcoin has increased and Bitcoin hard forks and trading at less than 1% of Bitcoin’s value. Seemingly the small blockers won that skirmish. Consensus for achieving scalability through a second layer payment network has won out, for now.

# What is the Lightning Network

Bitcoin Lightning Network is a second-layer protocol designed to enable off-chain Bitcoin transactions. It aims at breaking the trade-off between block size and centralisation by processing most of the transactions off-chain: it is a 'layer 2' protocol that can operate on top of Blockchain-based cryptocurrencies such as Bitcoin.  Because they are not recorded on the blockchain, and thus require no mining, Lightning payments are extremely fast and cheap. Unlike the Bitcoin network, Lightning transactions are not publicly broadcast and instead, individual Lightning nodes transact with one another privately.

For example a transaction from party A to party D is not direct and channel is opened Party A 🡪 Node B 🡪 Node C 🡪 Party D. Each node comprising the channel earn a fee for each transaction run through the channel in each direction. When all transactions are complete a single net on-chain transaction is made to the public ledger. The combination of small node transaction fees and the final larger on-chain fee result in a lower fee per transaction and transactions clear much faster.

I In a payment channel, cryptographic protections are used to ensure that channel updates in both directions are executed atomically, i.e., either both or neither of them are performed. In addition, incentive-based protections are also implemented to prevent users from stealing funds in a channel, e.g., by committing a revoked state. Similar techniques allow payment routing for longer paths.

Furthermore, payment router intermediaries are financially motivated to relay payments as they are entitled to claim transaction fees after each successfully routed payment. LN as a PCN consists of nodes representing users and undirected, weighted edges representing payment channels. Users can open and close bidirectional payment channels between each other and route payments through these connections.

# The goal

Network participation is incentivized through the reward of routing payments. Payment routing is a passive means of earning Bitcoin. We sought to analyze the lightning network to come up with a strategy for maximizing profits for our Bitcoin node.

# Collecting and analyzing data

Throughout our work we tried several methods of collecting Data. BTCPayServer is an open source project that allows online vendors to easily accept and generate invoices. MyNode is a private company that offers licensed software compatible with market available hardware to run a Bitcoin Node. Simulated data from Ferenc Beres Lightning Network Simulation. Once collected the collection plan called for storing the data in MongoDB.

## Issues with Collecting Data From our Node

BTCPay Server an open source stack that allows users to run a Bitcoin Node using virtual private clouds (VPCs). Their solution provides an attractive advantage of not having to maintain any hardware. The software stack is easy to run and operate a node but our team found it difficult to off load this data. Advantages of BTCPay are that users are aple to run an the open source software stack on a Virtualized Machine. We built two BTC-Pay server nodes. One implementing a solution on AWS EC2 instance. Memory one of our Docker Images filled to its max capacity during the synchronization of the state of the Bitcoin’s Blockchain.

Synchronization is a major step in any implementation of a Bitcoin Node. For node to participate in the network it must first download a copy of the entire Blockchain. Referring to the discussion on the blocksize dilemma the lightning network implementation is seeking to solve an issue for the small block size. Even with the small blocksizes the synchronization is no small step. With larger blocksizes this project may not have been attainable for the resources available to our shoestring budget.

With the EC2 instance it was on day 3 of the synch when the docker image filled up crashing our node. Unfortunately, once a docker image is filled to maximum compacity there is nothing a user can do.

We started the process again. This time using LunaNode. BTCPay server and LunaNode collaborated to create a seamless integration allowing users to leverage advantages built in. For example, LunaNode provides a feature for users to temporarily increase compute capacity just for the synchronization process of the node. Useful to decrease the length of time needed for a node to synch with the state of the current blockchain. Dynamic memory capacity solved the docker image problem faced in the EC2 instance.

Once up and running we found that the implementation of BTCPay server a useful for anyone to easily create a Bticoin node. Yet we found the open source software lacking in a few key areas of interest. It seems the BTCPay server is highly optimized for the use of online vendors. The software stack can autmotically generate invoices. Easily add the ability to conduct transactions on the Onion Network. Even the possibility for users to accept alternative cryptocurrencies. Yet, we were unable to gather data about the state of the lightning network.

MyNode is a promising application that allowed the team to take physical control of the node and data storage. This implementation of a Bitcoin node is an on premises solution. Raspberry Pi 4 provided the compute and requires a 1TB 2.5’’ SSD drive for memory. This implementation is limited to the compute power of the Raspberry Pi and its write to memory speed. Already a slower process, the Blockchain synch with MyNode was slowed further by hardware issues. Raspiberry Pi 3.2 USB connection proved fickle. It had trouble writing to the first SATA connection 3.2 connection. MyNode Troubleshooting steps provided Raspberry Pi preferred 3.2 USB SATA connection. Even with the preferred equipment used the synchronization took more 3 weeks to complete. The delay in gathering data through this method meant moving on to analysis phase without our own nodes data.

## Open Source Data

GitHub user “FiatJaf” created an open source Postgres data base of the Lightning Network. The data is collected by a python script that uses the following c-lightning, a compliant lightning implementation in C. Bitcoin-Knots a desktop application to run a Bitcoin Wallet. Esplora, an open source Blockchain explorer. FiaJjaf’s script runs once a data and creates snap shots of the network.

Ferenc Beres Lightning Node Simulator providing the team with a simulated lightning network traffic data. It used snapshots of the network collected from a period of from 2018 through 2019. Using the Lightning network simulator we accepted a few strong assumptions. First, that data from that time period is still relevant today. Fixed payments amounts is another strong assumption. However, various distributions such as Poisson on Pareto greatly increases the complexity of the experimentation. At the onset of each simulation randomized capacity between channel and endpoints was used.

Regardless of the source of the data, our node, FiaJaf, Ferenc Beres’s LNSimulator, we expected the size to be great. A method for storing the data in order to create a data science pipeline required database integration.

# database Integration

## Postgress integration

Puri Can you talk about what you did with FiatJaf’s database? Did you download the data and store it in Postrgres Or did you run your own instance of the database?

## MongoDB integration

Ferenc Beres’s LNSimuulator gave our team useful insights into the lightning network. The simulator allows users to tweak the internal state of the simulation prior to running. Output files from the simulation came in the form of four csv files and one json file. MongoDB provided a great resource for the team to store, lablel, and create a data science pipline from.

The flexibility of json like documents made capturing the output from the csv files possible and a desirable feature. MongoDB collections made tracking the internal state of the simulation that produced a particular output easy as well. By giving a collection a snap shot ID the team could track what simulation conditions produced a particular output.

Database integration also provided the team with an increase in availability. One person could run a simulation and through a predetermined naming convention could share the results. Allowing any of the team participants to access this data. The sheer size of the lightning network data necessitated using databases for analysis. Which could not have otherwise been performed on an ordinary computer importing a csv file.

# Results

## Analysis of Base Fee rate on the Lightning Network

With the objective finding the optimal base fee rate for our node we analyzed the open source data on the lightning network collected by FiatJaf. In the following diagram you can see the distribution of fees that are being used for channels on the lightning network. The fees are announced in the gossip protocol. What we observed are the most used fees are zero, 1000 MilliSatoshi’s. The Y scale is logarithmic. That indicates that these most common base fee rates are extremely common.

Chart, histogram

Description automatically generated

Figure 1. Distribution Base Fees in MilliSatoshis. Note that the Y scale is logarithmic. The most common base fee is zero.

Another way to absorb this data is to look at the culminative distribution function. Chart

Description automatically generated

Figure 2 Cumulative distribution function of Base Fee Rate. What this shows is for every base fee rate, what is the number of nodes that have a lower base fee.

The cumulative distribution function graph shows us that almost all nodes have a lower base fee rate of 1500 MilliSatoshis. Is this a good base fee rate? Data will never include transaction amounts, sources, and targets in any form, and it is very unlikely that it will give information on the capacity distribution over the channels, since that would leak information on the actual transactions. Thus, in order to explore this idea we turned to the LNSimulator.

## Analysis of Simulated Lightning Network Transactions.

The network in the simulator has a fixed number of nodes *N* – corresponding to all Bitcoin users that may decide to switch to the LN – and is *sparse*, i.e. the number *M* of edges is *M* ≪ *N*2. If we consider node *i* and *j* having fitness *xi* and *xj* respectively, a LN channel, i.e. an edge between them, is added with probability

Text

Description automatically generated Furthermore, payment router intermediaries are financially motivated to relay payments as they are entitled to claim transaction fees after each successfully routed payment. LN as a PCN consists of nodes representing users and undirected, weighted edges representing payment channels. Users can open and close bidirectional payment channels between each other and route payments through these connections. Therefore, LN can be modeled as an undirected, weighted multigraph since nodes can have multiple channels between each other. The weights on the edges correspond to the capacity of the payment channels. By simulating transactions at different traffic volumes and transaction amounts, we shed light on the fee pricing policies.

Keeping in mind the assumptions of LNSimulator, fixed payment amounts and 2019 snapshots of the Lightning Network we found the following distribution of router fees, i.e. the fee charged by a node to route a payment.

Chart, histogram

Description automatically generated

Figure Histogram of Router Fees in MilliSatoshis. Note, a fee of zero is the most common fee. Also supported by our open source Lightning Network Data.

Taking a look at the income distribution

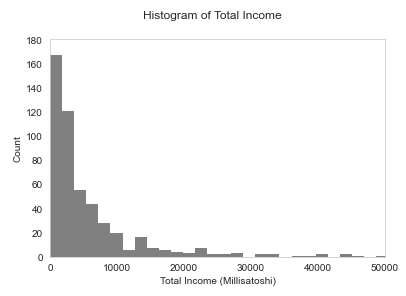


Figure Income Distribution in MilliSatoshi's: Right Tailed distribution. Because most nodes have a fee of zero they are not earning income

The LNSimulator provides optimal fee output which is itself a simulation run in parallel to the first simulation. The transactions take the map of the network based on path lengths and fees simulate where on the network the sender would be routed for lowest cost. The optimal fee then loops through the possible sources, increases their fees and determines if their income increases or not. If it produces an increase in income the simulation calculates a fee difference and outputs the optimal.

Chart

Description automatically generated with medium confidence

Figure Optimal Fee Distribution. Note, another right tailed distribution. Most optimal increases are between 0 and 4000 MilliSatoshi's.

What does this mean for our optimizing our node? Leaving the routing fee at zero produces no income. Exactly what fee we should start will depend on several factors. Where our node fits into the Lightning Network will play a part in routing algorithm. Establishing channels with active nodes will help improve our nodes position to charge a higher fee. Maintaining an active node will help decrease failed transaction rate. Keeping liquidity a node also improves performance. Nodes that are not adequently funded cannot forward payments behind their own channel liquidity.

References

*Basic format for books:*

1. J. K. Author, “Title of chapter in the book,” in *Title of His Published Book, x*th ed. City of Publisher, Country if not
2. USA: Abbrev. of Publisher, year, ch. *x*, sec. *x*, pp. *xxx–xxx.*

*Examples:*

1. G. O. Young, “Synthetic structure of industrial plastics,” in *Plastics,* 2nd ed., vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.
2. W.-K. Chen, *Linear Networks and Systems.* Belmont, CA: Wadsworth, 1993, pp. 123–135.

*Basic format for periodicals:*

1. J. K. Author, “Name of paper,” *Abbrev. Title of Periodical*, vol. *x,* no. *x,* pp*. xxx-xxx,* Abbrev. Month, year.

*Examples:*

1. J. U. Duncombe, “Infrared navigation—Part I: An assessment   
   of feasibility,” *IEEE Trans. Electron Devices*, vol. ED-11, no. 1, pp. 34–39, Jan. 1959.
2. E. P. Wigner, “Theory of traveling-wave optical laser,” *Phys. Rev*.,   
   vol. 134, pp. A635–A646, Dec. 1965.
3. E. H. Miller, “A note on reflector arrays,” *IEEE Trans. Antennas Propagat*., to be published.

*Basic format for reports:*

1. J. K. Author, “Title of report,” Abbrev. Name of Co., City of Co., Abbrev. State, Rep. *xxx*, year.

*Examples:*

1. E. E. Reber, R. L. Michell, and C. J. Carter, “Oxygen absorption in the earth’s atmosphere,” Aerospace Corp., Los Angeles, CA, Tech. Rep. TR-0200 (4230-46)-3, Nov. 1988.
2. J. H. Davis and J. R. Cogdell, “Calibration program for the 16-foot antenna,” Elect. Eng. Res. Lab., Univ. Texas, Austin, Tech. Memo. NGL-006-69-3, Nov. 15, 1987.

*Basic format for handbooks:*

1. *Name of Manual/Handbook*, *x* ed., Abbrev. Name of Co., City of Co., Abbrev. State, year, pp. *xxx-xxx.*

*Examples:*

1. *Transmission Systems for Communications*, 3rd ed., Western Electric Co., Winston-Salem, NC, 1985, pp. 44–60.
2. *Motorola Semiconductor Data Manual*, Motorola Semiconductor Products Inc., Phoenix, AZ, 1989.

*Basic format for books (when available online):*

1. Author. (year, month day). *Title.* (edition) [Type of medium]. *volume (issue).* Available: site/path/file

*Example:*

1. J. Jones. (1991, May 10). *Networks.* (2nd ed.) [Online]. Available: [http://www.atm.com](http://www.atm.com/)

*Basic format for journals (when available online):*

1. Author. (year, month). Title. *Journal.* [Type of medium]. *volume (issue),* pages. Available: site/path/file

*Example:*

1. R. J. Vidmar. (1992, Aug.). On the use of atmospheric plasmas as electromagnetic reflectors. *IEEE Trans. Plasma Sci.* [Online]. *21(3),* pp. 876–880. Available:<http://www.halcyon.com/pub/journals/21ps03-vidmar>

*Basic format for papers presented at conferences (when available online):*

1. Author. (year, month). Title. Presented at Conference title. [Type of Medium]. Available: site/path/file

*Example:*

1. PROCESS Corp., MA. Intranets: Internet technologies deployed behind the firewall for corporate productivity. Presented at   
   INET96 Annual Meeting. [Online]. Available: <http://home.process.com/Intranets/wp2.htp>

*Basic format for reports and handbooks (when available online):*

1. Author. (year, month). Title. Comp an y . C ity, State or Country. [Type of Medium]. Available: site/path/file

*Example:*

1. S. L. Tall een. (1996 , Apr . ). The In t r an et Archi -tecture: M a nagi ng i n f o rm at i on i n t h e ne w paradigm. Amdahl Corp., CA. [Online]. Available:<http://www.amdahl.com/doc/products/bsg/intra/infra/html>

*Basic format for computer programs and electronic documents (when available online):* ISO recommends that capitalization follow the accepted practice for the language or script in which the information is given.

*Example:*

1. A. Harriman. (1993, June). Compendium of genealogical software. *Humanist.* [Online]. Available e-mail: [HUMANIST@NYVM.ORG](mailto:HUMANIST@NYVM.ORG) Message: get GENEALOGY REPORT

*Basic format for patents (when available online):*

1. Name of the invention, by inventor’s name. (year, month day). *Patent Number* [Type of medium]. Available: site/path/file

*Example:*

1. Musical toothbrush with adjustable neck and mirror, by L.M.R. Brooks. (1992, May 19). *Patent D 326 189*

[Online]. Available: NEXIS Library: LEXPAT File: DESIGN

*Basic format for conference proceedings (published):*

1. J. K. Author, “Title of paper,” in *Abbreviated Name of Conf.*, City of Conf., Abbrev. State (if given), year, pp. *xxxxxx.*

*Example:*

1. D. B. Payne and J. R. Stern, “Wavelength-switched pas- sively coupled single-mode optical network,” in *Proc. IOOC-ECOC,* 1985,   
   pp. 585–590.

*Example for papers presented at conferences (unpublished):*

1. D. Ebehard and E. Voges, “Digital single sideband detection for interferometric sensors,” presented at the 2nd Int. Conf. Optical Fiber Sensors, Stuttgart, Germany, Jan. 2-5, 1984.

*Basic format for patents:*

1. J. K. Author, “Title of patent,” U.S. Patent *x xxx xxx*, Abbrev. Month, day, year.

*Example:*

1. G. Brandli and M. Dick, “Alternating current fed power supply,”   
   U.S. Patent 4 084 217, Nov. 4, 1978.

*Basic format**for theses (M.S.) and dissertations (Ph.D.):*

1. J. K. Author, “Title of thesis,” M.S. thesis, Abbrev. Dept., Abbrev. Univ., City of Univ., Abbrev. State, year.
2. J. K. Author, “Title of dissertation,” Ph.D. dissertation, Abbrev. Dept., Abbrev. Univ., City of Univ., Abbrev. State, year.

*Examples:*

1. J. O. Williams, “Narrow-band analyzer,” Ph.D. dissertation, Dept. Elect. Eng., Harvard Univ., Cambridge, MA, 1993.
2. N. Kawasaki, “Parametric study of thermal and chemical nonequilibrium nozzle flow,” M.S. thesis, Dept. Electron. Eng., Osaka Univ., Osaka, Japan, 1993.

*Basic format for the most common types of unpublished references:*

1. J. K. Author, private communication, Abbrev. Month, year.
2. J. K. Author, “Title of paper,” unpublished.
3. J. K. Author, “Title of paper,” to be published.

*Examples:*

1. A. Harrison, private communication, May 1995.
2. B. Smith, “An approach to graphs of linear forms,” unpublished.
3. A. Brahms, “Representation error for real numbers in binary computer arithmetic,” IEEE Computer Group Repository, Paper R-67-85.

*Basic format for standards:*

1. *Title of Standard*, Standard number, date.

*Examples:*

1. IEEE Criteria for Class IE Electric Systems, IEEE Standard 308, 1969.
2. Letter Symbols for Quantities, ANSI Standard Y10.5-1968.

1. “Bitcoin summary is supported by the Investopedia website. Reference: <https://www.investopedia.com/terms/b/bitcoin.asp>

   . “On Chain Vs off chain transactions information is supported by the following Reference: <https://river.com/learn/on-chain-vs-off-chain-bitcoin-transactions/>

   The Authors of this paper are have no affiliation with the following references.

   S. B. Author, Jr., was with Rice University, Houston, TX 77005 USA. He is now with the Department of Physics, Colorado State University, Fort Collins, CO 80523 USA (e-mail: author@lamar.colostate.edu).

   T. C. Author is with the Electrical Engineering Department, University of Colorado, Boulder, CO 80309 USA, on leave from the National Research Institute for Metals, Tsukuba, Japan (e-mail: author@nrim.go.jp). [↑](#footnote-ref-1)