How to Charge Lightning: The Economics of Bitcoin Transaction Channels

Simina Brânzei
Purdue University, USA
simina.branzei@gmail.com

Erel Segal-Halevi
Ariel University, Israel
erelsgl@gmail.com

Aviv Zohar
Hebrew University of Jerusalem, Israel
avivz@cs.huji.ac.il

Abstract—Off-chain transaction channels represent one of the leading techniques to scale the transaction throughput in cryptocurrencies. However, the economic effect of transaction channels on the system has not been explored much until now.

We study the economics of Bitcoin transaction channels, and present a framework for an economic analysis of the lightning network and its effect on transaction fees on the blockchain. Our framework allows us to reason about different patterns of demand for transactions and different topologies of the lightning network, and to derive the resulting fees for transacting both on and off the blockchain.

Our initial results indicate that while the lightning network does allow for a substantially higher number of transactions to pass through the system, it does not necessarily provide higher fees to miners, and as a result may in fact lead to lower participation in mining within the system.

Index Terms—blockchain, lightning network, transaction channels

I. INTRODUCTION

A main approach to solve the scalability problem in Bitcoin is to use off-chain transaction channels that allow parties to transfer funds while communicating directly, and only occasionally to settle on the blockchain. The deployment of SegWit, a solution to transaction malleability (among other benefits) opens the path for better constructions of off-chain transaction channels. While transaction channels themselves are limited to exchanges between pairs of individuals, further developments like the lightning network [PD16] allow to route payments over longer paths and thus can allow the construction of a well connected network of payment channels that can be used to transfer money quickly and with relatively little interaction with the blockchain. For discussion of micropayment channels and scalability, see, e.g., [HS], [DW15], [CDE+16].

One of the key unknowns regarding fast payment networks is the economic effect that they will have on the Bitcoin fee market. If the blockchain is used less often, fees to miners are paid less frequently and competition for space in blocks declines. Bitcoin’s security depends heavily on having a large amount of computational power invested in solving proof-of-work puzzles, making it hard for attackers to double spend or censor transactions in the currency. As the block reward in Bitcoin declines (halving every four years), the reliance on fees increases and these must suffice to pay for enough mining by honest participants.

In this work we explore the economics of Bitcoin transaction channels, and in particular the economic equilibrium that results from the introduction of fast-payment networks to the Bitcoin ecosystem. Our main contribution is a theoretical framework in which one can reason about the usage of payment channels and the cost of committing records to the blockchain. We explore different topologies of payment channels and find the market equilibrium that dictates (among other things) the fees that will be collected by miners, the transactions that pass through the lightning network or directly through the blockchain, and the transactions that do not take place (e.g., micro transactions for which the fees are too high on both alternatives).

Summary of our findings. While our findings strongly depend on the assumptions we have made regarding the distribution of payment sizes and willingness to pay fees, we generally find that the revenue obtained by miners can sometimes be lower when lightning networks are deployed compared to when they are not, unless extremely large numbers of participants take part in transacting (there too, results depend on the distributional assumptions). Naturally, the addition of payment channels does indeed result in very high transaction throughputs in the system overall.

The implications for Bitcoin are that the revenue from fee payments alone might be insufficient to support the security of the system. Still, our results should be taken with a grain of salt: we account for very simple topologies but hope our initial exploration will inspire further exploration of such models.

A. An overview of our approach

The first step taken when modeling the effects of different transaction methods is to select a model for the demand for transactions — a model specifying which participants want to send money, to whom, what amount is transferred, and how much fee the sender is willing to pay to complete the transfer.

A second aspect that needs to be determined is the topology of payment channels that is set in the system: which pairs of participants choose to establish channels between them, and how much funding is dedicated to each such channel. This is crucial in determining the lifetime of the channel given different use patterns.

Finally, with this information at hand, we set out to compute the demand for blockchain records. Such demand stems from two main sources: the establishment and settlement of existing lightning channels, and direct transfers that occur on the blockchain. Given that the block size is limited, the daily
supply of new transaction records is fixed, and we are thus able to compute the market equilibrium fee for records.

**The mechanics of transaction channels.** Transaction channels are typically established by locking funds using a single blockchain transaction. The channel state is then updated by the two participants by exchanging transactions that update the division of funds from the locked amount. These transactions are not typically transmitted to the blockchain. Each update represents a new division of funds and usually only the last transaction is committed to finalize the transfer. The transactions exchanged by the two participants on each channel are set up so that if one of the participants (say Alice) disappears or tries to take funds that are not hers (e.g., by placing a transaction that represents an old state on the blockchain), the other participant (say Bob) can recover his funds or even punish Alice by taking all the funds in the channel. For the purpose of this work, we assume all channels are established and settled cooperatively, as we aim to consider the expected behavior of the market under “normal” circumstances.

We additionally assume that channels can be settled and reopened with a single transaction, which may be of larger size in the network. We assume the parties that transfer money back and forth do so according to a random process, and that they therefore occasionally end up in a state where all funds in the channel are directed to one of the users. In this case, the channel can only be used to transfer money in one direction and the channel must be reset or re-funded to allow flow in the other direction. Clearly, if the amount of liquidity in the channel is high, then this event will occur rarely. It is therefore of paramount importance to establish the typical amount of funding in each channel. Since liquidity that is locked within the channel represents money that is not invested elsewhere, we consider the cost of holding liquidity in the channel as the lost income from interest payments on this sum. Stated differently: we allow participants to borrow as much money as they want to fund their transaction channels, and the cost for such payments is simply the interest rate in the economy. This cost is the de facto limiting factor for the lightning network.

**Models for the demand for transactions.** We explore two primary models for the demand for transactions. The first is a model in which participants are paired and only transact with their direct partner. While this is not a realistic depiction of the flow of money in an economy, it is in some sense a best-case setting for transaction channels, as no routing of payments is required by the system. The topology of channels in this case is also simple: just create channels between transacting pairs if it is profitable to do so. In this setting we note there are several variants: one in which transactions occur with equal probability in each direction, and one in which transfers are asymmetrically biased in one direction. In this work we focus on the symmetric variant. Another axis along which we vary our analysis is regarding the size of payments. We assume in one case that payments come from a uniform distribution, and in another case that they are derived from a power-law distribution (as it often is in real life data).

Our second model assumes that all participants may pay each other, and that payments occur between participants that are chosen uniformly at random. Here we focus on an analysis of a payment network that includes a single payment hub. The hub needs to maintain additional liquidity, but allows participants that are connected to it to route payments to everyone else. We find surprisingly that the results bear great similarity to the pairs model (except for extra payments for the additional liquidity).

**Implementation.** The simulation code is: https://github.com/erels/g/bitcoin-simulations.

### B. Related Work

Following the circulation of our paper, there have been follow-up works investigating the lightning network. [WZS22] analyze the structure of the lightning network and compare it with the Barabasi–Albert model for generating random scale-free graphs via preferential attachment, finding that the lightning network has a different structure (such as different assortativity and diameter). [ZFDS22] conduct an empirical analysis of the lightning network, focusing on the betweenness centrality distribution of the routing system.

[BCV20] studies the lightning network as a percolation process and aims to understand how the distribution of volume and size of transactions impacts the feasibility of the system. [BSB21] design a publicly available traffic simulator to empirically study the transaction fees and privacy provisions on the lightning network. [GHS21] analyze payments on lightning channels that are unidirectional or symmetric bidirectional. Their work identifies conditions for two parties to optimally establish a channel, find explicit formulas for channel costs and obtain the optimal collaterals and savings entailed, deriving the implied reduction in the congestion on the blockchain.

Lightning channels may be subject to adversarial attacks, which may allow an adversary to discover channel balances, thus threatening the privacy of the users. [NFSD20] observe that the lightning network allows users to use gossip and probing mechanisms to learn about possible paths for routing their transactions, which may in turn be exploited by an adversary to learn information about the transactions. [NFSD20] analyze two types of attacks: a probing attack, where an adversary wants to detect the maximum amount transferable in a given direction on a channel by probing it, and a timing attack, where the adversary discovers how close the destination of a routed payment is. [BNT22] analyze probing attacks in the presence of multiple channels between the same pair of users on the lightning network. [KYP21] consider multiple types of attacks that an adversary may perform on lightning.

## II. Model

We analyze the market for *records* on the blockchain. A record is a part of a block, in which a single transaction is recorded. Each record has a market-price \( \phi \) [bitcoins-per-record], which is the mining-fee for a blockchain transaction. The market-price \( \phi \) is determined as a price in which the supply of records equals the demand for records.
The supply in our market is quite simple: the bitcoin protocol ensures that the supply of records per day is fixed. We denote this parameter by \( \tau \). The total revenue of the miners, which is an important factor in the security of bitcoin, will be \( \tau \cdot \phi \) [bitcoins-per-day]. The demand is driven by the need of users to transfer money to other users. Demand is determined by the next parameters:

- The number of times that user \( i \) wants to transfer money to user \( j \) per day is a Poisson random variable with mean value \( \lambda_{i,j} \) [transfers-per-day].

- The size of transfers from user \( i \) to user \( j \) is \( z_{i,j} \) [bitcoins-per-transfer]. This models the fact that some users do micro-transfers while others do bulk transfers. We will sometimes assume that \( z_{i,j} \) is drawn from a probability distribution such as uniform or power-law. We assume that the transfer-size \( z_{i,j} \) is constant for each pair, i.e., it is drawn randomly once for each pair and then remains fixed.

- The utility that user \( i \) gains from each transfer to user \( j \) is \( v_{i,j} \) [bitcoins-per-transfer]. We will often assume that the utility is proportional to the transfer size, i.e., \( v_{i,j} = \beta z_{i,j} \), where \( \beta \) is a constant in \((0, 1)\).

Each time user \( i \) considers transferring money to user \( j \), it compares three options: blockchain transfer, lightning transfer, or no transfer at all. The user selects the option with the highest net gain. In the case of a blockchain transfer, the net gain is \( v_{i,j} \) minus the blockchain fee \( \phi \). In the case of a lightning transfer, the net gain is \( v_{i,j} \) minus the lightning fee, which is derived from the cost of maintaining the lightning channel. In case of no transfer, the net gain is zero.

The lightning fee is derived from several parameters which determine the cost of using lightning:

- The number of blockchain records required for a channel-reset transaction, denoted by \( a \). Note a reset transaction is slightly larger than a standard transaction, so \( a \) is a number between 1 and 2 [records]. Therefore the cost of resetting a lightning channel is \( a \cdot \phi \) [bitcoins].

- The (fixed) interest rate \( r \) [per day]. A user who wants to use lightning has to lock money in channels, and thus it has to pay an economic cost determined by \( r \). Thus, in general, a user will not want to lock all its money in lightning channels, but instead look for the optimal amount to lock such that the total cost (economic cost plus channel-reset cost) is minimized.

We study several special cases for the transfer matrix \( \lambda_{i,j} \):

- **Pairs**: the users are divided in pairs (e.g., \((1, 2), (3, 4), \ldots\)) All transfers are only inside each pair, i.e., for every \( i \), only \( \lambda_{2i, 2i-1} \) and \( \lambda_{2i-1, 2i} \) are non-zero. This is in some sense the best case for lightning, since we only need an \( i-j \) channel.

- **Symmetric uniform**: \( \lambda_{i,j} = \lambda \) for all \( i \) and \( j \).

- **Asymmetric uniform**: for each pair \( i, j \), \( \lambda_{i,j} + \lambda_{j,i} = \ell \) and \( |\lambda_{i,j} - \lambda_{j,i}| = \Delta \). I.e., the pairs are asymmetric, either user \( i \) transfers more money to user \( j \) or vice-versa.

In general, it is possible that some agents accumulate money endlessly while other agents spend money endlessly; this can be explained by assuming that they do some transfers outside bitcoin. Alternatively, one can assume a special topology in which all nodes have an even degree and have positive net transfer in exactly half their edges.

We also consider several possible lightning topologies:

- **Pairs**: each user \( 2i \) has a channel only with user \( 2i - 1 \).
- **Star**: there is a single node (“bank”) which is connected to all users; all transfers go through the bank.

### III. Analysis of a Single Channel

The basic building-block for our analyses is the analysis of a single channel between two users, Alice and Bob. We first analyze the expected channel lifetime for a given channel capacity and distribution of transfers, and then find the optimal channel capacity.

We checked two cases related to the transfer rates: in the symmetric case the transfer-rate from Alice to Bob equals the transfer-rate from Bob to Alice; in the asymmetric case the transfer-rates are different. For brevity, this paper presents only the results for the symmetric case; we found the results for the asymmetric case to be qualitatively similar. Thus from now on we assume the channels are symmetric.

#### A. Channel Lifetime

**Theorem III.1** (Lifetime of Symmetric Channel). Let Alice and Bob have a channel with \( w \) bitcoins, which they use to transfer single bitcoins to each other at a time. Each transfer consists of one coin sent by Alice with probability \( 1/2 \) and by Bob with probability \( 1/2 \). Then the expected lifetime of the channel from the state where Alice has \( m \) bitcoins and Bob has \( w-m \) bitcoins is \( X_m = mw - m^2 \).

**Proof.** Let \( X_m \) denote the expected channel lifetime from the state where Alice has \( m \) bitcoins and Bob has \( w - m \). The channel lasts until one of the players reaches a balance of zero bitcoins. Then \( X_m = 1 + 1/2 \cdot X_{m-1} + 1/2 \cdot X_{m+1} \), which gives the recurrence \( X_{m+1} = 2 \cdot X_m - X_{m-1} - 2 \) (see, e.g., [LR06]). We have \( X_0 = 0 \), since if Alice has zero in her account and wants to make a transfer, then the channel is reset. Similarly, \( X_w = 0 \) corresponds to the case where Bob has zero in his account.

Then the associated homogeneous recurrence relation is \( X_{m+1} = 2 \cdot X_m - X_{m-1} \), with characteristic equation \( x^2 - 2x + 1 = 0 \). The roots of the associated characteristic equation are \( x_1 = x_2 = 1 \), and so the general solution has the following form, where \( a, b \) are constants:

\[
X_m^h = a + bm.
\] (1)

In general, if \( s \) is a root with multiplicity \( q \) of the characteristic equation, there exists a general solution to the recurrence such that for some constants \( p_0 \ldots p_t \):

\[
X_m^p = m^q \left( \sum_{k=0}^t p_k \cdot m^k \right) s^m.
\] (2)
The particular solution, given by Equation 2, has $q = 2$, $s = 1$, and $t = 0$, so $X^p_m = v m^2$ for some constant $v$. Then
$$v \cdot (m + 1)^2 = 2v \cdot m^2 - v \cdot (m - 1)^2 \iff v = -1.$$ The particular solution is $X^p_m = -m^2$. Adding the homogeneous part (1) and the non-homogeneous part (2), we obtain:
$$X_m = X^h_m + X^p_m = a + bm - m^2.$$ The boundary condition $X_0 = 0$ gives $a = 0$, while $X_w = 0$ gives $b = w$. Then for all $n = 0, \ldots, w$, the expected number of transfers made on the channel is $X_m = w m - m^2$.

**Corollary III.2.** Let Alice and Bob have a channel with $w$ bitcoins, which they use to transfer single bitcoins to each other at a time. Suppose both users transfer to each other using a Poisson process with mean $\lambda_A = \lambda_B = \lambda$. Then the expected number of days for the channel started from the state where Alice has $m$ bitcoins and Bob has $w - m$ bitcoins is:
$$X_m = w m - m^2 / (2\lambda) \text{ days}.$$ 

**Proof.** When the players send to each other with equal means, Alice sends to Bob a single unit with probability 1/2 and Bob sends to Alice with probability 1/2. From Theorem III.1, the expected lifetime from the state where Alice has $m$ bitcoins is $X_m = w m - m^2$. To obtain a solution in days, we divide this by the mean number of transfers per day, which is $2\lambda$.

**B. Channel Optimal Initialization**

Given the expressions for the channel lifetime, Alice and Bob can calculate the optimal way to initialize a channel with a fixed capacity $w$, i.e. the initial balance $(a, b)$ that maximizes the expected lifetime of the channel.

**Lemma III.3.** The optimal initialization of a symmetric channel with capacity $w$ is for each of Alice and Bob to start with $w/2$ bitcoins.

**Proof.** The expected channel lifetime from the state where Alice has $m$ bitcoins is $w m - m^2 / (2\lambda)$; the lifetime is maximized when $m = w/2$. An optimally initialized symmetric channel is expected to last for:
$$T(w) = w^2 / (8\lambda).$$

So far, we assumed that each transfer between Alice and Bob consists of a single coin. However, we can generalize the results to a situation in which each transfer between Alice and Bob consists of $z$ bitcoins, for some constant $z$. In this case, the channel funding $w$ is given in transfers, i.e. the channel lifetime is $T(w)$ when the channel is funded with $w \cdot z$ bitcoins.

**C. Channel Optimal Capacity**

Alice and Bob have two options for performing a sequence of transactions, namely sending money to each other on the blockchain or through a channel in the lightning network. In the case of blockchain transactions, there will be a fixed fee $\phi$ paid for each transaction, where $\phi$ is equal to the price (in bitcoins) of a blockchain record. If on the other hand Alice and Bob decide to use a lightning channel, they will incur an interest $r$ on the money that is locked into the channel, in addition to the fee $a \cdot \phi$ paid when the channel is reset and recorded on the blockchain.

We assume that this cost is covered by charging a fixed fee per lightning-transaction. The fee is calculated such that the expected fee charged during the entire channel lifetime equals the total cost of maintaining the channel.

**Lemma III.4.** Let $\phi$ be the blockchain mining fee and $r$ the daily interest rate for locking money in a lightning channel. Suppose the transfers between Alice and Bob are Poisson processes with means $\lambda_A, \lambda_B$ transfers-per-day, respectively, with $\ell := \lambda_A + \lambda_B$. Each transfer is of $z$ bitcoins, and Alice and Bob use a lightning channel with capacity $w \cdot z$ bitcoins.

Then, to cover the maintenance costs of the channel, the fee per transaction should be:
$$F(w) = wz \cdot (1 + r)T(w) + a\phi - wz \over T(w) \cdot \ell \text{ bitcoins / transaction}$$

where $T(w)$ is the expected channel lifetime (in days).

**Proof.** The players pay interest on the quantity $wz$ locked in the channel until the channel closes, i.e. for $T(w)$ days in expectation.

Since the interest is paid each day (rather than for each transaction), the cost due to the interest is: $((1 + r)T(w) - 1) \cdot wz$. The users incur an additional cost of $a\phi$ at the end for recording the channel balance on the blockchain.

The expected number of transactions during the channel lifetime is $T(w) \cdot \ell$, so the expected fee charged during the channel lifetime is $F(w) \cdot T(w) \cdot \ell$. This fee should cover the costs, thus:
$$(1 + r)T(w)^{-1} \cdot wz + a \cdot w = F(w) \cdot T(w) \cdot \ell,$$
from which the claim follows.

**Lemma III.5 (First-order approximation).** Consider the function that gives the expected fee per transaction:
$$F(w) = \frac{((1 + r)T(w) - 1) \cdot wz + a\phi}{T(w) \cdot \ell}.$$ The first-order approximation of $F$ taken around $r = 0$ is $\tilde{F}(w) = wzr / \ell + a\phi / (T(w) \cdot \ell)$, where $T(w)$ is the expected channel lifetime and is independent of the interest rate $r$.

**Proof.** Let $g(r) = (1 + r)T(w)$, where $r \in \mathbb{R}^+$. Then $F(w) = ((g(r) - 1) \cdot wz + a\phi) / (T(w) \cdot \ell)$. Since $T(w)$ is independent of $r$, we have $g'(r) = T(w) \cdot (1 + r)T(w)^{-1}$. The first order approximation of $g(r)$ around $r_0 = 0$ is:
$$\tilde{g}(r) = g(0) + g'(0) \cdot (r - r_0) = 1 + r \cdot T(w).$$ After substituting $\tilde{g}(r)$ for $g(r)$ in $F(w)$, we obtain that $\tilde{F}(w) = (wzrT(w) + a\phi) / (T(w) \cdot \ell)$.

The error term for the estimation of $g(r)$ is given by a function $h(r)$ with the property that $|h(r)| \leq Mr^2/2$, where $M$ is the maximum value of $|g''(r)|$ on the interval $[0, c]$.

We get $g''(r) = T(w) \cdot (T(w) - 1) \cdot (1 + c)T(w)^{-2}$. There are a few cases:

- $x \geq 2\sqrt{2}M: M_1 = \max_{x \in [0, c]} |g''(r)|$ is attained for $r = 1$, so we have $M_1 = |T(w) \cdot (T(w) - 1)\cdot (1 + c)T(w)^{-2} |$.
- $x < 2\sqrt{2}M$: the maximum is $M_2 = |T(w) \cdot (T(w) - 1)|$, attained for $r = 0$. 


Take $M = \max\{M_1, M_2\}$. Let $R(w) = F(w) - \hat{F}(w)$ be the error term in the approximation of $F(w)$. Then

$$|R(w)| = \left| \frac{wz \cdot (g(r) - \check{g}(r))}{T(w) \cdot \ell} \right| = \frac{wz \cdot |h(r)|}{T(w) \cdot \ell} \leq \frac{2Mz^2}{x}.$$ 

The cost of a transaction on the blockchain is $\phi$, thus performing transactions on the lightning network is profitable for Alice and Bob as long as $F \leq \phi$.

**Lemma III.6 (First order approximation of symmetric channel capacity).** Let $\phi$ be the blockchain mining fee and $r$ the daily interest rate for locking money in a lightning channel. Suppose the transfers between Alice and Bob are Poisson processes with means $\lambda_A = \lambda_B = \lambda$ transfers-per-day, with $\ell := |\lambda_A - \lambda_B| = 2\lambda$. Each transfer is of $z$ bitcoins, and Alice and Bob use a lightning channel with capacity $w \cdot z$ bitcoins.

Then the first order approximation of the expected cost per transaction on the channel is $zrw/\ell + 4a\phi/w^2$. The optimal channel capacity based on this approximation is $w_{opt} = (8a\phi/\ell)z^{1/3}$.

**Proof.** From Lemma III.5, the first-order approximation of the lightning-fee $F$ is: $F(w) = w\tau r/\ell + a\phi/(T(w) \cdot \ell)$.

For a symmetric channel, $T(w) = w^2/4k$ [days], thus $\hat{F}(w) = zrw/\ell + 4a\phi/w^2$, as claimed. The error term is:

$$|R(w)| = \left| \frac{wz}{T(w) \cdot \ell} \cdot |h(r)| \right| = \frac{wz}{w} |h(r)| \leq \frac{2Mz^2}{x}.$$

Minimizing the fee given the interest rate $r$, blockchain fee $\phi$, and mean number $\ell$ of daily transfers, is equivalent to minimizing $f(x) = 2zw \sqrt{1 + x} + 4a\phi/\sqrt{x^2}$, where $x \in [1, \infty)$ is the channel capacity [in transfers].

To find the optimal channel funding for a given $r$, $\phi$, $\ell$, we must find the minimum of $f(x)$ on the interval $[1, \infty)$. As explained before, the first-order approximation of $f$ is given by:

$$\check{f}(x) = zrw/\ell + 4a\phi/\sqrt{x^2}.$$ 

The optimal channel funding based on this approximation can be determined by taking the minimum of the function $\check{f}(x)$ on the range $(0, \infty)$. Note that $\check{f}'(x) = zr/\ell - 8a\phi/\sqrt{x}^3$ and $\check{f}''(x) = 24a\phi/\sqrt{x^4} > 0$. Thus $f$ is convex and the minimum is attained for $x_{\min}$ with the property that $\check{f}'(x_{\min}) = 0$, that is, $x_{\min} = (8a\phi/\sqrt{zr})^{1/3}$.

Then the lightning fee given the optimal funding is: $F_{\text{opt}} = F(x_{\min}) = 3(a\phi z^2 r/\ell^2)^{1/3}$. This completes the proof.

### IV. Pairs Topology

In this section we assume that the network of transfers has a very simple topology: the users are divided to pairs who only trade with each other.

Our goal is to calculate the market-equilibrium blockchain fee $\phi$. To this end, we have to calculate the demand for each value of $\phi$ and find the value of $\phi$ in which the demand equals the supply (which we assume is constant, $\tau$ records per day).

A. Symbolic computations

We start by analyzing the demand of a single pair.

**Lemma IV.1 (Choice of a single pair).** Let $\phi$ be the blockchain mining fee. Suppose the transfers between Alice and Bob are Poisson processes with means $\lambda_A, \lambda_B$ transfers-per-day respectively, where $\ell := |\lambda_A - \lambda_B|$, and each transfer is of $z$ bitcoins. Then there exist thresholds $\theta_{NL}, \theta_{NB}, \theta_{LB}$ such that Alice and Bob:

- do not transfer to each other when $z < \min\{\theta_{NL}, \theta_{NB}\}$,
- transfer only via lightning when $\theta_{NL} < z < \theta_{LB}$,
- transfer only via blockchain when $z > \max\{\theta_{NL}, \theta_{LB}\}$.

The thresholds depend on the transfer rates. With symmetric transfer rates, they are:

$$\theta_{NL} = \frac{27a^2 r^2}{\ell^2 \beta^3} \cdot \phi; \quad \theta_{NB} = \frac{\phi}{\beta}; \quad \theta_{LB} = \frac{\ell}{\sqrt{27a^2 r^2}} \cdot \phi.$$

**Proof.** The users consider three options: (1) do not transfer at all, (2) transfer through the lightning channel between them, or (3) use direct blockchain transfers. They will choose the option with the lowest net utility. We assume that the users have quasi-linear utilities, so the utility of each user is the value of the transfer minus the fee paid.

The net utility of doing no transfer is clearly 0. If the value of a transfer from Alice to Bob is $v = \beta - z$, then the net utility of doing a blockchain transfer is: $u_B = v - \phi = \beta z - \phi$. The net utility of a lightning transfer is $v$ minus the lightning fee calculated in the previous subsection, assuming optimal channel funding: $u_L = \beta z - F_{\text{opt}} = \beta z - 3(a\phi z^2 r/\ell^2)^{1/3}$.

The possible relations between the three net utilities are:

- $u_L > 0 \iff z > \left(\frac{27a^2 r^2}{\ell^2 \beta^3}\right) \cdot \phi = \theta_{NL}$.
- $u_B > 0 \iff z > \frac{1}{\beta} \cdot \phi = \theta_{NB}$.
- $u_B > u_L \iff z > \left(\frac{\ell}{\sqrt{27a^2 r^2}}\right) \cdot \phi = \theta_{LB}$.

The choice of the users depends on these parameters as follows. If $0 > \max(u_L, u_B)$, then the users choose no-transfer. If $u_B > \max(0, u_L)$, then the users transfer via the blockchain. If $u_L > \max(0, u_B)$, then the users transfer via their lightning channel. The claim follows from the above by straightforward calculations.

Observe that all three thresholds are linear functions of the blockchain-fee $\phi$, even though the channel-lifetime is a non-linear function of $\phi$.

We ignore the case in which two of the three utilities are exactly equal (e.g., $u_L = 0$ or $u_B = 0$ or $u_L = u_B$), since the transfer size $z$ is drawn from a continuous distribution, so the probability of an exact equality is zero.

The previous lemma assumed that the transfer-size $z$ is fixed. Now, we let $z$ be a random variable, and calculate the expected demand per pair. We calculate the demand function both with and without lightning.

**Lemma IV.2 (Demand of a single pair).** Let $\phi$ be the blockchain mining fee. Suppose the transfers between Alice
and Bob are Poisson processes with means $\lambda_A, \lambda_B$ transfers-per-day respectively, with $\ell := \lambda_A + \lambda_B$ and $\Delta := |\lambda_A - \lambda_B|$, and the transfer-size $z$ is a random variable with probability-distribution function $f$.

Let $\theta_{NL}, \theta_{NB}, \theta_{LB}$ be as described in Lemma IV.1. Then the expected demand of the two users, measured in records-per-day, is:

- **Without lightning:** $D^{\theta}(\phi) = \ell \int_0^{\theta_{LB}} f(z) dz$.
- **With lightning:**
  
  $$D^\phi(\theta) = \ell \int_0^{\theta_{LB}} \left( \frac{\ell \phi^2 z^2}{\phi^2} \right) \frac{1}{\phi^2} f(z) dz + \ell \left( \int_0^{\max(\theta_{LB}, \theta_{NL})} f(z) dz \right)$$

The transactions count and volume are as follows:

| Transactions count | Lightning | Blockchain |
|--------------------|-----------|------------|
| $\ell \int_0^{\theta_{LB}} f(z) dz$ | $\ell \int_0^{\theta_{LB}} f(z) dz$ | $\ell \int_0^{\max(\theta_{LB}, \theta_{NL})} f(z) dz$ |
| Transactions volume | $\ell \int_0^{\theta_{LB}} z f(z) dz$ | $\ell \int_0^{\max(\theta_{LB}, \theta_{NL})} z f(z) dz$ |

**Proof.** By Lemma IV.1, when $z > \max(\theta_{NB}, \theta_{LB})$, the users use blockchain transfers. They do $\ell$ transfers per day, each of which uses a single record, so their demand is $\ell$ records-per-day. This explains the rightmost terms in all expressions (i.e. for $D^{\theta}(\phi)$ and $D^{\phi}(\phi)$). When $\theta_{NL} < z < \theta_{LB}$, the users transact via their lightning channel, so their demand is $\alpha$ records each $T$ days, where $T$ is the channel-lifetime (in days) when it is funded optimally. So their daily demand is $(\ell \phi^2 z^2 / \phi^2)^{1/3}$. This explains the leftmost term in the expression for $D^{\phi}(\phi)$, completing the proof.

We also analyze examples with realistic numbers in the full version of the paper and observe that usually the thresholds are ordered such that $\theta_{NL} < \theta_{NB} < \theta_{LB}$.

Now we can calculate the equilibrium blockchain-fee.

**Theorem IV.3 (Equilibrium blockchain-fee).** Suppose there are $n$ users who only interact in pairs (i.e. there are $n/2$ pairs of users). In every pair, all parameters ($\lambda_A, \lambda_B, \ell$) are the same, except for the transfer-size $z$, which is drawn randomly for each pair from probability-distribution $f$. Then, the market-price $\phi_{eq}$ is a solution to the equation: $\frac{\ell}{2} \cdot D(\phi) = \tau$, where $D(\phi)$ is given by the expression in Lemma IV.2 for each case.

**Proof.** Assuming all pairs have the same parameters, the expected aggregate demand is $\frac{\ell}{2} \cdot D(\phi)$ records-per-day. The supply is $\tau$ records-per-day. The market-equilibrium price is the price in which the demand equals the supply.

**B. Power-law distribution**

We now present a special case of Lemma IV.2 for the case in which the transfer-size $z$ is distributed according to the following power-law:

$$f(z) = \begin{cases} 0 & \text{if } z < z_{\min} \\ \frac{z_{\min}}{z^2} & \text{if } z \geq z_{\min} \end{cases}$$

For simplicity we assume that $\theta_{NB} < \theta_{LB}$.

**Corollary IV.4.** When the transfer-size has power-law distribution and $\theta_{NB} < \theta_{LB}$, the expected demand of the pair (measured in records-per-day) is as follows in each case:

- **Without lightning:**
  
  $$D^{\theta}(\phi) = \begin{cases} \ell & \text{if } \theta_{NB} < z_{\min} \\ \ell \cdot \frac{z_{\min}}{\phi_{NB}} & \text{if } \theta_{NB} \geq z_{\min} \end{cases}$$

- **With lightning:**

  $$D^{\phi}(\phi) = \begin{cases} \ell, & \text{if } \theta_{LB} < z_{\min} \\ 3z_{\min} \left( \frac{\ell \phi^2}{\phi^2} + \frac{1}{\sqrt{\phi_{NL}}} - \frac{1}{\sqrt{\phi_{LB}}} \right) + \ell \cdot \frac{z_{\min}}{\phi_{LB}}, & \text{if } \theta_{NL} < z_{\min} \leq \theta_{LB} \\ 3z_{\min} \left( \frac{\ell \phi^2}{\phi^2} + \frac{1}{\sqrt{\phi_{NL}}} - \frac{1}{\sqrt{\phi_{LB}}} \right) + \ell \cdot \frac{z_{\min}}{\phi_{LB}}, & \text{if } \theta_{NL} \geq z_{\min}. \end{cases}$$

The transaction counts on lightning and blockchain, respectively, are as follows:

| Transaction counts | Lightning | Blockchain |
|--------------------|-----------|------------|
| $\theta_{LB} < z_{\min}$ | 0 | $\ell$ |
| $\theta_{NL} < z_{\min} \leq \theta_{LB}$ | $\ell \left( 1 - \frac{z_{\min}}{\phi_{LB}} \right)$ | $\ell \left( \frac{z_{\min}}{\phi_{LB}} \right)$ |
| $\theta_{NL} \geq z_{\min}$ | $\ell \left( \frac{z_{\min}}{\phi_{NL}} - \frac{z_{\min}}{\phi_{LB}} \right)$ | $\ell \left( \frac{z_{\min}}{\phi_{LB}} \right)$ |

The expected transaction volumes are as follows:

| Transaction volumes | Lightning | Blockchain |
|--------------------|-----------|------------|
| $\theta_{LB} < z_{\min}$ | 0 | $\ell$ |
| $\theta_{NL} < z_{\min} \leq \theta_{LB}$ | $\ell \phi_{min} \left( \ln \theta_{LB} - \ln z_{\min} \right)$ | $\ell \phi_{min}$ |
| $\theta_{NL} \geq z_{\min}$ | $\ell \phi_{min} \left( \ln \theta_{LB} - \ln \theta_{NL} \right)$ | $\ell \phi_{min}$ |

**V. Simulations**

In the theoretical analysis we assumed that the transfer-size $z$ is randomized once per pair of agents. We found that the case in which the transfer-size is randomized in each transfer is much more difficult to analyze theoretically. Therefore we study this case using simulations. The details of the experimental analysis can be found in the full version of the paper [BSZ17].

We consider a channel with a total capacity $w$. Since the transfer-rate from Alice to Bob is the same as from Bob to Alice, we assume that the channel is initialized symmetrically - each agent contributes $w/2$. The "channel state" is the balance for Alice in the channel; therefore the initial state is $w/2$. 

Whenever a transfer has to be made, we determine its size $z$ by randomly drawing from the power-law distribution defined by $f(z) = \frac{z_{\text{min}}}{z^2} \ [z > z_{\text{min}}]$. Then, we check whether the transfer can be done in the current channel state (i.e., whether the agent making the transfer has a sufficiently high balance). If the transfer can be done on the channel, then it is done and the channel state is updated. Otherwise, we check whether it is worthwhile to do the transfer on the blockchain: if the transfer value $\beta z$ is larger than the current $\phi$, then the transfer is done on the blockchain; otherwise, it is not done at all.

In the initial state ($w/2$), the chances of channel failure are relatively small; as the channel drifts away from this initial state towards one of its endpoints, the chances of channel failure increase. Therefore, at some states it may be worth doing a channel reset and returning the channel to its initial state. We assume there is a constant $R$ such that, whenever the state after a channel transfer is smaller than $R$ or larger than $w - R$, it is reset to $w/2$. We call $R$ the reset radius.

Then we find the optimal reset radius, the optimal channel capacity, the curve of demand for blockchain records assuming optimal channel capacity and reset radius, and the price-curves (describing the equilibrium blockchain fee as a function of the number of users); see full version [BSZ17].

Given the number of users $n$, we assume they are matched in $n/2$ pairs, such that each pair has a transaction channel. Due to space constraints, we only show here the overall network performance as a function of the number of users. We simulated random transfers over 100,000 days, and 1000 values of $n$ between $10^5$ and $10^8$ (logarithmically spaced). For each value, we calculated the equilibrium fee with and without lightning, the number and the volume of transfers done in blockchain vs. lightning. We did this experiment once for a block size of 288000 records per day and another time for a block size twice as large (of 576000 records per day). The results are shown in Figure 1.

The results are qualitatively similar with single or double block size. As the number of users grows, the equilibrium fee grows super-linearly (first line) and with it, the miners’ revenue (fifth line). However, the utility per user decreases (sixth line). All the supply of records is used (second line). Almost all transfers are done via lightning (third line), but the volume of transfers is split approximately equally between lightning and blockchain (fourth line), since the largest transfers are done on the blockchain. Doubling the block size (with lightning) has some minor quantitative differences: the blockchain fee is smaller by a factor of about 3, the miners’ revenue is smaller by a factor of about 1.5, and the utility per user is higher by a factor of 1.5 (see Figure 2).

VI. Star Topology

We now show how to solve networks where there is a central bank that each user is connected to. For each pair of users $i, j$, let $\lambda_{i,j}$ denote the flow of user $i$ towards user $j$. Then we can define $\lambda_+^i = \sum_{j \in N} \lambda_{i,j}$ and $\lambda_-^i = \sum_{j \in N} \lambda_{j,i}$. Set $p_i = \frac{\lambda_+^i}{\lambda_+^i + \lambda_-^i}$ and $q_i = \frac{\lambda_-^i}{\lambda_+^i + \lambda_-^i}$. Then $p_i + q_i = 1$, so the expected lifetime of the channel between user $i$ and the bank can be obtained as a corollary from the single channel analysis.

**Corollary VI.1** (Lifetime of Channel between User and Bank). Suppose there is a lightning star network, where the transfers from each user $i$ to any other user $j$ are given by a Poisson process with mean $\lambda_{i,j}$ transfers per day, and the channel between user $i$ and the bank has capacity $w$. Let $\lambda^+ = \sum_{j \in N} \lambda_{i,j}$ and $\lambda^- = \sum_{j \in N} \lambda_{j,i}$. Then, the expected lifetime of the channel between user $i$ and the bank from the
state where user $i$ has $m$ bitcoins and the bank has $w - m$ bitcoins on the channel with user $i$ is:

(a) when $\lambda_i^+ \neq \lambda_i^-:$

$$\tilde{X}_m^i = \frac{m}{\lambda_i^+ - \lambda_i^-} - \frac{w}{\lambda_i^+ - \lambda_i^-} \left(1 - \frac{(\lambda_i^+)^m}{(\lambda_i^-)^m}\right) \frac{(\lambda_i^+)^m}{(\lambda_i^-)^m} \text{ [days]}$$

(b) when $\lambda_i^+ = \lambda_i^-:$

$$\tilde{X}_m^i = \frac{w(m - m^2)}{2\lambda_i^+} \text{ [days]}$$

**Corollary VI.2.** The optimal initialization of a star network with channels of capacity $w$ is such that for each user $i$

- If $\lambda_i^+ = \lambda_i^-$, both the bank and user $i$ start with $w/2$ bitcoins. The expected lifetime of user $i$’s channel with the bank when initialized this way is $T_i(w) = \frac{w}{\lambda_i^+ - \lambda_i^-}$.

- If $\lambda_i^+ > \lambda_i^-$, user $i$ starts with $w$ bitcoins and the bank with $0$ bitcoins, while if $\lambda_i^+ < \lambda_i^-$ user $i$ starts with $0$ bitcoins and the bank with $w$ bitcoins. The approximate expected lifetime of user $i$’s channel is $T_i(w) = \frac{w}{\lambda_i^+ - \lambda_i^-}$.

Next we calculate the optimal channel funding for the star topology, finding that the fee per transaction for any user in the star network is twice as high compared to the pairs topology.

**Theorem VI.3.** Consider a star network with users $1 \ldots n$ connected through a bank, such that the transfer from any user $i$ to another user $j$ is a Poisson process with mean $\lambda_{i,j}$, with $\ell_i = \sum_{k \in N} \lambda_{i,k} + \lambda_{k,i}$. Let $\phi$ be the blockchain mining fee and $r$ the daily interest rate for locking money in a lightning channel. Each transfer between any pair of users is of $z$ bitcoins, and each user $i$ has a channel with the bank of $w_i \cdot z$ bitcoins. Then the expected cost of any transfer that a user $i$ is involved in is:

$$F(w_i) = \frac{w_i z \cdot (1 + r) T(w_i)}{T(w_i) \cdot \ell_i} + a \phi - w_i z \cdot \frac{r}{\ell_i} \text{ [bitcoins/transfer]}$$

where $T(w)$ is the expected lifetime (in days) of a channel of capacity $w_i$. The expected fee paid by each user $i$ is twice as high in the star network compared with the model where user $i$ transacts only with a fixed user $j$ without a bank.

**Proof.** This follows from the single channel analysis (Lemma III.4), by noting that the expected (total) cost of a transaction that passes through user $i$’s channel with the bank is given by $w_i z \cdot (1 + r) T(w_i) + a \phi - w_i z / (T(w_i) \cdot \ell_i)$. The bank does not support any cost that user $i$ incurs, so the fee for user $i$ is twice as high compared to the case where $i$ has transactions with only one other user $j$ (with no intermediary).

The analysis from the pairs topology applies here too, except that the cost of using the lightning network for each user is multiplied by a factor of two.

**VII. DISCUSSION**

Instead of Poisson transfers, we can assume that there is a fixed sequence of transfers: $(i_1, j_1), (i_2, j_2), \ldots$, where transfer number $k$ is from user $i_k$ to user $j_k$. Each user $i$ has a fixed initial budget $K_i$. The sequence is feasible, i.e., at time $k$, user $i_k$ always has a sufficient amount of money for transferring to user $j_k$. We assume that at time $k$, user $i$ considers only two options: blockchain transfer or bitcoin transfer, and selects the cheaper option. There is an interesting algorithmic question: given a fixed sequence of transfers, what is the optimal configuration of lightning channels?

**VIII. ACKNOWLEDGMENTS**

The symbolic calculations were done with Sympy [sym], the plots with Desmos [des] and Matplotlib [Hun07]. Authors are listed in alphabetical order. Part of this work was done while S. B. was visiting the Simons Institute for the Theory of Computing.

**REFERENCES**

[BCV20] S. Bartolucci, F. Caccioli, and P. Vivo. A percolation model for the emergence of the bitcoin lightning network. Nature Scientific Reports, 10, 2020.

[BNT22] A. Biryukov, G. Naumenko, and S. Tikhomirov. Analysis and probing of parallel channels in the lightning network. In Financial Cryptography, 2022.

[Bre73] R.P. Brent. Algorithms for Minimization without Derivatives. Prentice-Hall, Englewood Cliffs, NJ. 1973. Ch. 4.

[BSB21] F. Béres, I. A. Seres, and A. Bençzúr. A Cryptoeconomic Traffic Analysis of Bitcoin’s Lightning Network. Cryptoeconomic Systems, 0(1), apr 5 2021.

[BSZ17] Simina Brânzei, Eeel Segal-Halevi, and Aviv Zohar. How to charge lightning. Corr, abs/1712.10222, 2017.

[CDE+16] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. Gun Sirer, D. Song, and R. Wattenhofer. On scaling decentralized blockchains. In Financial Cryptography and Data Security, pages 106–125. Springer Berlin Heidelberg, 2016.

[des] Desmos. http://www.desmos.com.

[DW15] C. Decker and R. Wattenhofer. A fast and scalable payment network with bitcoin duplex micropayment channels. In 17th International Symposium on Stabilization, Safety, and Security of Distributed Systems, volume 9212, pages 3–18, 2015.

[GHS21] P. Guasoni, G. Huberman, and C. Shikhelman. Lightning network economics: Channels. Michael J. Brennan Irish Finance Working Paper Series Research Paper No. 21-17, Columbus Business School, 2021.

[HS] M. Hearm and J. Spillman. Bitcoin contracts. https://en.bitcoin.it/wiki/Contracts.

[Hun07] J. D. Hunter. Matplotlib: A 2d graphics environment. Computing In Science & Engineering, 9(3):90–95, 2007.

[KYP+21] G. Kappos, H. Yousaf, A. Piotrowska, S. Kanjalkar, S. Delgado-Segura, A. Miller, and S. Meiklejohn. An empirical analysis of privacy in the lightning network. In Financial Cryptography and Data Security, pages 167–186. Springer Berlin Heidelberg, 2021.

[LR06] Tom Leighton and Ronitt Rubinfeld. Random walks. https://web.mit.edu/neboat/Public/6.042/randomwalks.pdf, 2006.

[NFS20] U. Nisslmueller, K. Koerster, S. Schmid, and C. Decker. Toward active and passive confidentiality attacks on cryptocurrency off-chain networks. In 6th International Conference on Information Systems Security and Privacy (ICISSP), 2020.

[PD16] J. Poon and T. Dryja. The bitcoin lightning network: Scalable off-chain instant payments, 2016. Technical report. Sympy. https://www.sympy.org/en/index.html.

[sym] W. Zhang, R. Zhang, Y. Sun, H. Ding, and Q. Lv. Can lightning network’s autopilot function use ba model as the underlying network? Frontiers in Physics, 9:794160, 2022.

[ZFDS22] P. Zabka, K-T. Foerster, C. Decker, and S. Schmid. Short paper: A centrality analysis of the lightning network. In Financial Cryptography, 2022.