Modeling Effective Lifespan of Payment Channels

Soheil Zibakhsh Shabgahi, Mahdi Hosseini, Behnam Bahrak, Seyed Pooya Shariatpanahi

***Abstract*—While being fully decentralized, secure, and reliable, Bitcoin and Blockchain based cryptocurrencies come with the cost of scalability. For Bitcoin to reach its full potential and wide use, overcoming this barrier is a necessity. One of the most promising approaches so far has been the Lightning Network with payment channels as the network edges. Using Hashed Timelock Contracts a payment channel is established between two nodes. Since not all nodes are connected directly to each other, nodes use a network (a.k.a. the Lightning network) to route their payments. Each node puts an initial balance payment as a warranty which is frozen in an account for the duration of the channels life span. Each node can only send as much balance as they have. We say the channel is unbalanced when there isn't sufficient balance in one direction. It is important to know how much fund is needed to get the wanted effective channel lifespan to make decisions on when to make a new channel and drop the old one.**

In this paper we developed a mathematical model to predict the expected effective lifespan of each channel based on the network's topology and payment size. We then proceed to do an analysis on how the lifespan of channels are affected if we change certain characteristics of the payment channel. We then analyse a snapshot of the lightning network to find how the effective lifespan is distributed throughout the network.

***Index Terms*—Bitcoin, Lightning Network, Payment Channel, Random Walk**

I. Introduction

BITCOIN is the first decentralized cryptocurrency, introduced in 2008 which provides security, anonymity, transparency, and democracy without any trusted third party[1]. Most of these properties are achieved by using a Blockchain as a distributed ledger; an inherent problem with using a Blockchain over a network is that it sacrifices scalability. The reason is that all nodes, potentially tens of thousands, must exchange, store, and verify each and every transaction in the system[2]. Furthermore, each block has a limited size and blocks get generated at regular intervals (approximately every 10 minutes), this means that with the current blocksize of 1 MBs the throughput of Bitcoin is about 4.6 transactions per second, which is not nearly good enough compared with centralized systems like Visa, WeChatPay, and PayPal[3]; making the use of Bitcoin in everyday transactions impractical.

Another trade-off the Blockchain consensus makes, is that it ensures security by waiting for other miners to extend the block holding the transactions; this way it makes sure that the double spending attack never happens. Currently the standard waiting time for a block to be confirmed is 6 blocks, which is roughly 1 hour [4].

Bitcoin's capacity limitations are being felt by users in the form of increased transaction fees and latency. With increasing demand for making transactions, users need to pay more transaction fees in order to make sure that their transaction is more profiting for the miners; hence has a higher chance of making it into a block. Queuing of transactions and network bandwidth will lead to longer delay time for a transaction to be decided.

There are many different proposals to solve the scalability problem. Most of the proposals fall into three categories: $layer0$, $layer1$, and $layer2$ solutions. $Layer0$ solutions try to enhance the infrastructure, like the network that connects the nodes. $Layer1$ solutions try to enhance the Blockchain's shortcomings by changing the consensus and protocols. $Layer2$ solutions propose ways to move away from the Blockchain and for this reason they are also called off-chain solutions. In this paper we discuss one of the more promising proposals in $Layer2$.

In 2016 the idea of Lightning Network was proposed to move the transactions to the second layer (off-chain)[2]. The Lightning Network consists of payment channels in a p2p fashion. Payment channels allow two parties to exchange payments with negligible time and cost, but both parties must freeze an initial fund in the channel so no one can spend more money than they own and no double spending accrues. It is important to note that the sum of funds in each channel remains constant throughout the channel's lifespan and only the channel's Balance changes. When two parties that don't have a direct channel want to exchange payments they can use other parties to route their payments. So a network of Nodes is constructed and all the connected nodes can send each other payments.

This system moves the cost of submitting a transaction off the Blockchain. Only the final states between two nodes will eventually make it into the Blockchain, which significantly increases throughput. Furthermore, no time is needed for the transaction to be confirmed and all transactions in a channel happen almost instantly.

This system works well until after a number of transactions. Channels start to get unbalanced; meaning all of the channel's fund has gone to one of the parties and the other one can't route any more payments through the channel.

Once a channel gets unbalanced, one of the major issues is that it effectively wont route half of the payments. It will be considerable to close the channel or start a new one.

II. Our Contribution

In this work, we provide a mathematical model of payment channels to predict the expected time for a channel to get unbalanced considering its position in the network and the initial balances of that channel. We call this time ”Expected Lifespan”. We then do an analysis on how Expected Lifespan is affected if we change any characteristics of the channel. We then provided simulation evidence of how channel unbalancing impacts its throughput. We then continue by doing an analysis on a recent snapshot of the Lightning Network to find the distribution of channel lifespans and its correlation with other topological parameters. Numerous payment channel protocols are given in [5], [6], [7], [8], [9], [10], [2], all presenting different methods for creating payment channels. However, our work is independent from the specifics of each method, thus applies to all such solutions.

III. Related Work

While the LN white paper [2] doesn't discuss channel re-balancing, there is already research on re-balancing the channels [11]. There are researches on the re-balancing of the network to improve its performance [12]. Also, there have been other research on the security and the probability to uncover the channel balances [13]. As far as we have looked, no other research tries to estimate the expected lifespans of channels in the payment networks.

IV. Background

We first provide some background on Bitcoin transactions and multi-signature contracts. We proceed by talking about payment channels and their role in lightning networks.

Basic Transactions

A Bitcoin address is equivalent to a traditional account in a banking system. An account is the hash of a public key (This is how privacy is preserved in Bitcoins) and the private key is like the password. Imagine that Alice had previously got some Coins from Eve through a transaction that transferred Eve's Coin to Alice's address. When Alice wants to send the coin to Bob she needs to sign a transaction (using her private key) that takes the transaction, with the coin Alice wants to spend (In this case the transaction between Eve and Alice), and the signature as its input and confirms the Coin at Bob's address as its output.

Contracts

Coins are transferred via transactions, sometimes called contracts, which are essentially small blocks of code(a.k.a. script) that can have multiple inputs and multiple outputs. Transaction scripts return a boolean value that every miner can evaluate. Only transactions returning a true value are evaluated and included in the Blockchain by the miners. A transaction is only evaluated true if the unlocking script can successfully unlock a previous transaction's locking script. The locking script freezes Coins in such a way that only users with the corresponding unlocking script can spend the Coin. The unlocking script is used to spend the Coin from a previous transaction's locking script inside the Blockchain.

Complex Contracts

More complex locking scripts use "Pay to Script Hash" (P2SH) that can allow multi-signature locking scripts where N out of M possible signatures are sufficient to unlock the script (and effectively spend the Coin). Another type of script is the Hashed TimeLock Contract(HTLC). A HTLC allows a user to make a transaction that can't be spent before some time has passed(either in absolute time or by the number of blocks passed). P2SH and HTLC are the main types of contracts used in making a payment channel.

Payment Channels

Payment channels help two parties to send funds back and forward as many times as they want with a negligible overhead. This is considered an off-chain payment because the transaction isn't broadcasted to the Blockchain.

There are two main proposals for payment channels, Duplex Micropayment Channels[7] and Lightning Channels[14]. In both proposals both parties must put in an initial fund that is locked for the duration of the channel's lifespan. We call these funds balances. Parties can send each other payments but they can't spend more than their deposit. We say a channel is unbalanced if all of the funds in the channel are in one side's hands; therefore, the other side can't send more payments. HTLC contracts are used to lock the funds of both parties in the payment channel for a specific amount of time, which can be unlimited. In case of unlimited time, any of the nodes can decide to close the channel and cash out. There are many implementations of payment channels [5], [6], [7], [8], [9], [10], [2], but this work is independent of the channel construction specifics.

The Network

Nodes who don't have a direct channel between them can use other nodes to route their payments. So a network of payment channels is created to route each payment a.k.a. the Lightning Network. Each node gets a routing fee per each payment. The Routing Fee could depend on the payment amount. Some routing challenges arise to find the path to the destination with minimum routing fees [15]. It is important where the node is connected inside the network. Well connected nodes can profit a lot by routing the payment of other nodes [3]. This has led the network to transform to an internet-like network; with few highly connected nodes and many low connection nodes [16].

After a number of payments, some channels will get unbalanced. The unbalanced channels can't route any payments in the unbalanced direction. It is considerable for nodes to re-balance or terminate an unbalanced channel.

V. Modeling

To determine the expected time it takes for a channel to get unbalanced (The Expected Lifespan); we introduce a mathematical model. We model the dynamics of a payment channel with the movement of a random walker. Each payment passing through the channel will represent a step the random walker takes. In the next subsection we discuss our assumptions and describe the model in detail. We then discuss how to find the model parameters. We then proceed by doing an analysis on how the expected lifespan is affected by changing channel's characteristics.

A. Random Walker Model

Take a payment channel between two nodes A and B, take the initial channel balance to be F_A and F_B respectively. The goal is to determine the expected time it will take for this payment channel to become unbalanced for the first time. for simplicity, we make the following assumptions:

- All the payments have the same amount denoted with ω.
- The payments from each node come with a Poisson distribution.
- The rate of the Poisson distribution is constant.

We model the dynamics of a Payment Channel with movement of a random walker. Let the random walker start at the origin of the number line. For each step we flip a coin with probability p for landing Heads and probability q for Tails $(p + q = 1)$. If the coin lands on Heads we take a step in the positive direction of the number line and if the coin lands on Tails we take a step in the negative direction of the number line. Points $+a$ and $-b$ are end points for our random walker. We can imagine that there is a cliff in $+a$ and $-b$; so the random walker stops the first time it reaches these points.

Every time a payment goes through the channel we flip a coin. Because the maximum number of payments we can send from A to B is initially $[\frac{F_A}{\omega}]$; we have $a = [\frac{F_A}{\omega}]$. Likewise, $b = -[\frac{F_B}{\omega}]$.

Because we know that the payments from each side are made with a Poisson distribution, we can say that payments come to the channel with a Poisson distribution having:

$$\lambda_{payment} = \lambda_{A,B} + \lambda_{B,A} \tag{1}$$

so the relation between expected time and expected number of coin flips is:

$$E_{time} = \frac{E_{steps}}{\lambda_{payment}} \tag{2}$$

We model node $S's$ channel balance to be the distance of the random walker from point $+a$ multiplied by PaymentSize (ω), and the balance of node $T's$ to be the distance of the random walker from point $-b$ multiplied by PaymentSize.

Our objective is to determine the time it takes for the channel to become unbalanced. We first solve "What is the expected number of steps needed for the random walker to reach $+a$ or $-b$ for the first time", then knowing the rate of the coin flip we can determine the expected time it will take the random walker to reach $+a$ or $-b$. In the next section we will determine the model parameters p and λ.

According to Lemma 1 the expected number of steps a random walker takes to reach $+a$ or $-b$, considering the probability p for the positive direction and $q = 1 - p$ for the negative direction, is:

$$E_{steps} = \begin{cases} \frac{ap^a(p^b - q^b) + bq^b(q^a - p^a)}{(p-q)(p^{a+b} - q^{a+b})} & p \neq 1/2 \\ ab & p = 1/2 \end{cases} \tag{3}$$

We ran a simulation of a Random Walker who starts from point zero with the same probability of going to each side ($p = \frac{1}{2}$). The simulation ran 10000 times to find the distribution of the number of steps needed to reach +a or -b. Figure (1) shows the result of the simulation. Figure (1) illustrates that most of the times the Random Walker reaches the bounds in less than 400 steps, but there aren't many situations where the Random Walker reaches the bounds in a huge number of steps. However, the average number of steps needed to reach the bounds is 400.5, which confirms (3).

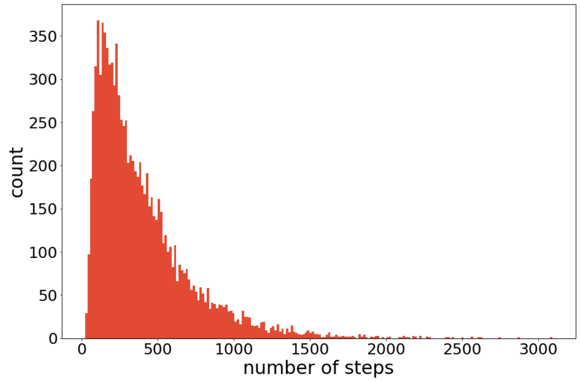

Fig. 1. Distribution of expected lifespan with 10000 random walker simulations with $p = \frac{1}{2}$ and $a = b = 1.2\,Msat$.

B. Finding P

In the previous section we modeled the payment channel dynamics with a Random Walker and a parameter-based formula was constructed according to Lemma 1. In this section we will discuss a methodology to find the parameters based on some assumptions.
Our assumptions are:

- The amount of all the payments in the network are the same and this amount is denoted with ω.
- Each node sends its payments to other nodes with a Poisson distribution.
- The payment rate between each pair of nodes is a given constant.

A payment network can be formally expressed by an unweighted directed graph consisting of a set of nodes, represented by V, and a set of edges denoted by E. Each channel is represented using two edges from E.

$MRates$ represents the matrix of payment rates between each two nodes. For example the rate of payments (number of payments per day) from node i to node j is denoted by $MRates_{ij}$.

$\lambda_{A,B}$ represents the rate of payments, which are transmitted over the $edge(A, B)$. $\lambda_{A,B}$ consists of the sum of portions of the payment rate between each pair of nodes that pass through $edge(A, B)$. So we have:

$$\lambda_{A,B} = \sum_{\substack{S,T \in V \\ S \neq T}} \frac{\sigma(S, T|edge(A, B))}{\sigma(S, T)} MRates_{ST} \tag{4}$$

Where $\sigma(S, T)$ is the number of shortest paths from node S to node T and $\sigma(S, T|edge(A, B))$ is the number of shortest paths from node S to node T passing through $edge(A, B)$ in the directed graph G.

Lemma 2. $\frac{p}{q} = \frac{\lambda(A,B)}{\lambda(B,A)}$.

According to Lemma 2:

$$p = \frac{\lambda_{A,B}}{\lambda_{A,B} + \lambda_{B,A}} \tag{5}$$

Therefore we can find p based on the network topology.

Lemma 3. *If* $\forall S,T \in V : MRates_{ST} = MRates_{TS}$ *then* $p = 0.5$.

If we assume that $MRates$ is a symmetric matrix, according to Lemma 3 we can find p without knowing $MRates$ and the topology.

C. Model Analysis

In this section we analyse the effect of different channel parameters on the channel's expected lifespan. For more realistic parameter values we used a recent snapshot of the Lightning Network taken on $Feb2019$ as a reference point. The average payment amount is considered to be $60000\,sat$ [17] and the average channel capacity is considered 2.4 Msat according to the snapshot. Because the rates of payments are only estimations and depend on the network topology, we put the expected number of payments until the channel is unbalanced as our y-axis rather than expected lifespan. Furthermore, the expected number of payments until unbalancing occurs, is a more robust variable in comparison with the expected time until unbalancing; when multiplied by fee base, it gives the expected routing income, and when divided by λ it gives the expected lifespan. For simplicity we use ”lifespan” and ”expected number of payments until channel is unbalanced” interchangeably.

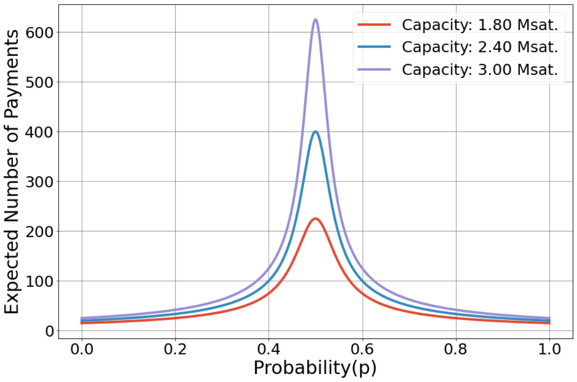

Fig. 2. Effect of payment direction probability, according to different channel capacities with equal initial balances.

The first question that comes to mind is: How sensitive is a channel's lifespan to the changes in p. As demonstrated in fig. 2; if the channel is initially balanced, the maximum lifespan happens when $p = \frac{1}{2}$. Also, lifespan is more sensitive to changes in p when the capacity is higher. From this result we can infer that it is an important consideration for a node to make sure the channel is placed in a way that p is close to $\frac{1}{2}$, otherwise the channel's lifespan is affected dramatically. Our proposal for nodes who want to keep their channels active as long as possible is to charge routing fees in a way that encourages other nodes to route their payments through the network in a $p = 50\%$ fashion. Figure (3) illustrates that if the channel is initially unbalanced, the maximum possible lifespan takes a hit. Although the maximum lifespan does not occur at $p = \frac{1}{2}$, the maximum lifespan still happens close to $p = 50\%$. So even if a channel is somewhat unbalanced the nodes must still try to keep p as close as possible to 50%.

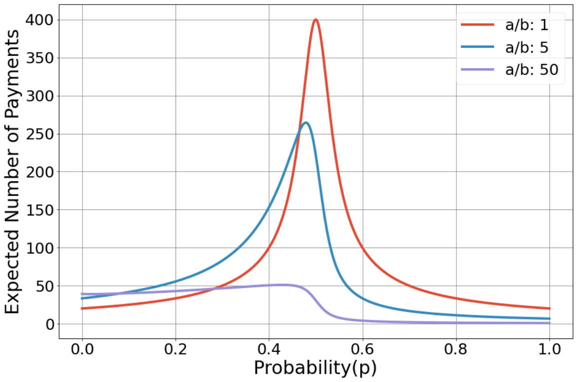

Fig. 3. The effect of payment direction probability on expected number of payments, according to different initial balance ratios. The channel capacity is considered 2.4 Msat.

The next important question is: How is the lifespan affected by channel capacity. As the figure (4) shows, the channel lifespan increases with capacity. It is noteworthy that the slope of this graph is increasing. So if a node doubles its channel capacity, the channel's lifespan will be more than doubled. Moreover, Figure (4) shows the toll of initial channel imbalance on the channel's lifespan.

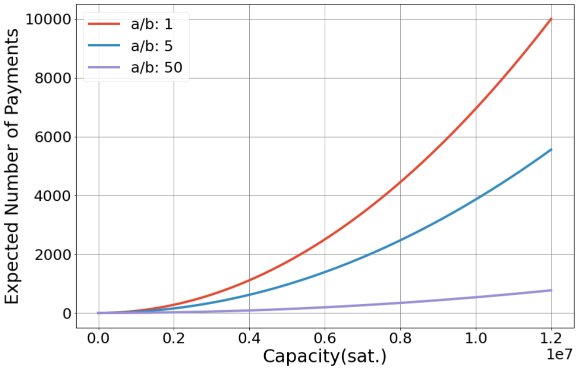

Fig. 4. Effect of channel capacity on the expected number of payments, according to initial balance ratios

Usually when a node wants to create a new channel with another node in the network, the only parameter it has control over is the amount of funds it wants to put towards the channel; not the other way around. This brings up the question: How will the channel's lifespan be affected with the amount the other node wants to put in the channel if our fund stays at a fixed value. Figures (5) and (6) illustrate this effect. Fig. 5 shows the maximum achievable lifespan considering any p

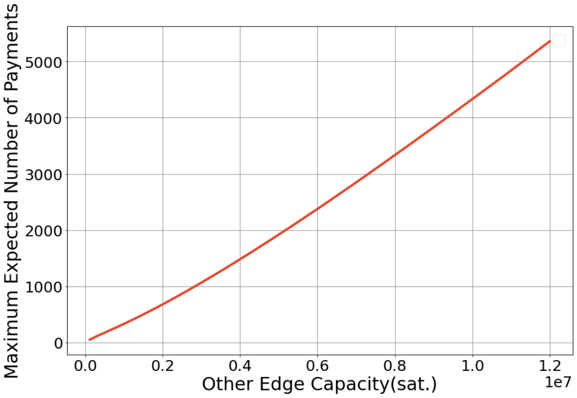

Fig. 5. For fixed channel capacity a = 1.2 Msat, the effect of channel b's capacity on the maximum possible lifespan in any p.

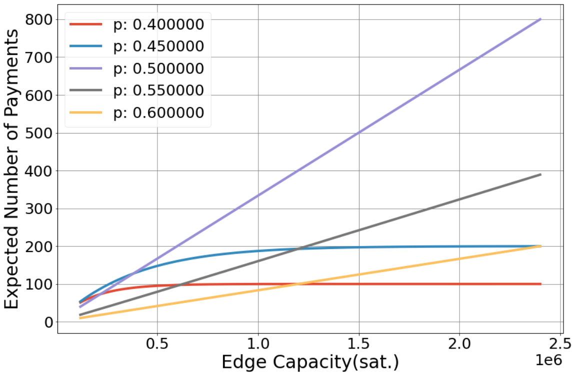

Fig. 6. Having a fixed initial balance from peer node (b) analysing the effect of our initial balance fund (a), according to different payment direction probabilities (p).

value and how it is affected by the capacity that the other node puts towards the channel. The maximum lifespan grows with the capacity of the other edge in a linear fashion. Fig. 6 illustrates the effect of our edge capacity if the peer node's capacity is fixed. Figure (6) shows that if p is in favor of most payments in the direction of our edge ($p \geq \frac{1}{2}$), the capacity increases almost linearly; if p is in favor of the other edge ($p < \frac{1}{2}$), the other edge becomes the bottleneck and the fund we put towards the channel will have little to no effect on the expected lifespan of the channel. We can say that if the funds we put towards the channel do not have an effect on the channel's lifespan, we have wasted cost opportunities.

VI. Unbalancing Impact

In this section we analyse the impact of becoming unbalanced on a channel's effective throughput. In the previous section we introduced a model to predict the time it takes for a channel to become unbalanced for the first time (the first time routing a payment fails). The question is how many payments will fail because of being imbalanced in the future.

We ran a simulation on a payment channel to see how much the failure rate increased after the first time that the channel became unbalanced. Table. VI shows the failure rate after the first time a channel becomes unbalanced. The simulation routes 5000 payments through an initially balanced channel and calculates the failure rate after the first time the channel becomes unbalanced. As table. VI suggests, the probability of payment direction is the key factor in determining how much the efficiency degrades after the first imbalance occurs(aka channels lifespan). Channels capacity has little to no impact on how well the channel can route payments.

		Probability(p)				
		0.3	0.35	0.40	0.45	0.5
Cap (Msat.)	1.2	40.13	30.03	20.03	10.37	4.84
	1.8	40.16	29.88	19.99	10.01	3.29
	2.4	39.98	30.00	19.94	10.09	2.51
	3.0	40.13	30.09	20.05	10.06	2.19
	3.6	40.18	30.04	20.06	10.13	1.98

TABLE I
FAILURE RATE AFTER UNBALANCING IN DIFFERENT CAPACITIES AND PROBABILITIES.

These results show that the probability of payment direction (p), which depends on the network topology and the network's transaction flow, is one of the most important parameters to determine the channel's lifespan; more importantly the level the channel's throughput degrades after the channel becomes unbalanced.

VII. Network Analysis

In this section we will provide an analysis on channel lifespans of a recent snapshot of the Lightning Network. The simulation is constituted by nodes and channels taken from a snapshot of the Lightning Network Mainnet [18] on $Feb2019$.

In section $5.A$ we modeled a payment channel with a Random Walker and we found a formula that shows what is the expected number of steps needed to reach $+a$ or $-b$. Moreover, the expected lifespan of a payment channel can be found if the rate of payments and Random Walker's expected number of steps are known by using (2). Lemma 3 shows that if we have the same rate for every pair of nodes, the probability of going to each side is equal to 0.5.

Because payment rates and channel balances are not public in the Lightning Network, we have to make assumptions on the distribution, the amount of payments, and channel balances. We assume that all payment rates have the same value r, which means that the rates matrix($MRate$) is symmetric. Thus according to Lemma 3, $p = 50\%$ for every channel in the network. According to (3) the expected number of payments is equal to ab, where $a = [\frac{F_A}{\omega}]$ and $b = [\frac{F_B}{\omega}]$ for a bidirectional channel between A and B. We assume that all channels are initially balanced, meaning $a = b = \frac{C}{2\omega}$, where C is the channel's capacity.

According to previous results in section 5 ((1) and (4)) we have:

$$\lambda_{payment} = (\sum_{\substack{S,T\in V\\ S\neq T}} \frac{\sigma(S,T|edge(A,B))}{\sigma(S,T)} + \frac{\sigma(S,T|edge(B,A))}{\sigma(S,T)})r \quad (6)$$

We also know that $\sum_{\substack{S,T\in V\\ S\neq T}} \frac{\sigma(S,T|edge(A,B))}{\sigma(S,T)}$ is equal to the

	All Channels	Central Channels
average	1833.2	172.3
STD	7086.9	587.2
median	27.0	1.6

TABLE II
LIFESPAN STATISTICS OF THE SNAPSHOT.

edge betweenness centrality of $edge(A,B)$ (EBC(A,B)) in directed graph G [19].

Because all channels are bidirectional $\forall edge(J,I) \rightarrow \exists edge(I,J)$, so $\forall S,T \in V$:

$$\frac{\sigma(S,T|edge(A,B))}{\sigma(S,T)} = \frac{\sigma(T,S|edge(B,A))}{\sigma(T,S)} \tag{7}$$

assuming $G^{'}$ as an undirected graph that derived from G we have:

$$EBC_G(A,B) = EBC_{G'}(A,B) \tag{8}$$

Thus:

$$\lambda_{payment} = 2 \times EBC_{G'}(A,B) \times r \tag{9}$$

If we replace all result in (2) we have:

$$E_{time} = \frac{(\frac{C}{\omega})^2}{4 \times 2 \times EBC_{G'}(A,B) \times r} \tag{10}$$

In this section we first calculate all payment channel lifespans in the LN snapshot by using equation (10). Then we will focus on the relation between edge betweenness and lifespan of the channels.

A. Channel Effective Life Distribution

Expression (10) shows that the lifespan of each channel can be calculated based on its edge betweenness centrality and initial fund. We assume that $r = 0.0022\, transactionsperday$ [20] and $\omega = 60000\, Msat$[17]. The distribution of channel lifespans in our snapshot is shown in figure 7. Much like the distribution of channel capacities that resemble the Power Law distribution; fig. 7 shows that there are a lot of channels with a low lifespan(in fact, most channels are) and very few channels with a very high lifespans.

According to [16] the most effective channels are the channels with the most betweenness centrality. This paper suggests that the top 14% of the channels have the most significant effect on the networks performance.

Table (II) gives some of the data, like average, standard deviation, and median, for all channels in the network and the top 14% central channels. The noticeable difference between median and average supports the idea that there are a lot of channels with short lifespan and a few channels with a very high lifespan.

B. Betweenness-Lifespan Correlation

As [16] suggests, the most central channels have the most impact on the network. And as fig. 10 shows, more central channels will have lower lifespans because they route more payments per unit of time. In figure 8 we took batches of the most central edges and calculated the average centrality and the average lifespan per batch. The result shows that in general the more central a channel is, the sooner it will get unbalanced. We see an exception to this statement somewhere in the middle of the graph, where increasing Betweenness has a positive correlation with the average lifespan. This is due to the fact that some very central edges have a large capacity so they can route more payment considering that capacity increases lifespan with a power of two.

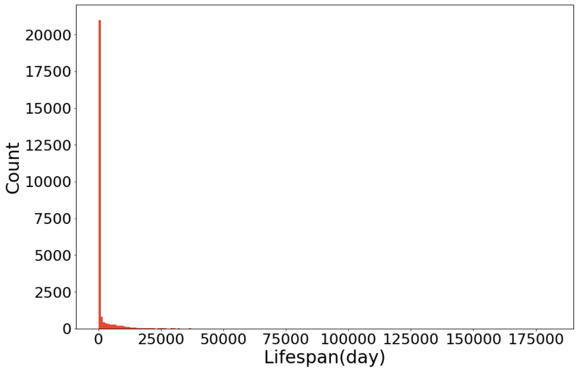

Fig. 7. Simulation histograms of expected number of steps to reach $+a$ or $-b$ with fixed step size and variable step size.

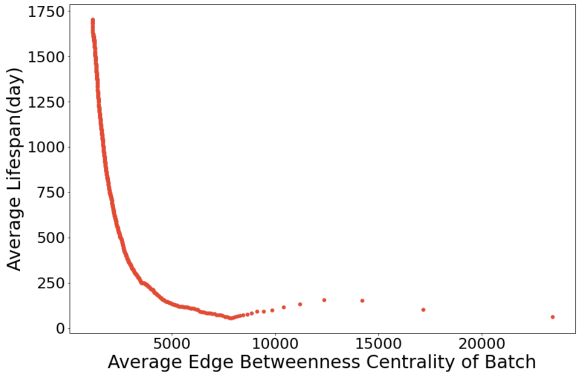

Fig. 8. Simulation histograms of expected number of steps to reach $+a$ or $-b$ with fixed step size and variable step size.

VIII. Conclusion

In this paper we modeled Payment Channel balances to estimate how long it takes for a channel to become unbalanced and what effect on the routing success does being unbalanced have. We demonstrated a method on determining a good placement in the network by network topology and payment rates. This work shows that just putting more funds towards a channel does not lead to having a more successful channel. The results show the channel's success in the network depends greatly on the network topology, transaction flow, and the amount of funds the other node, who we make a channel with, invests in the channel. Because investing in a payment channel means that the fund is locked for the duration of the channel's lifespan, we need to make sure the opportunity cost is less than the return we get from routing fees. The results showed how much a node should invest in a channel and for how long; to maximize the value their investment returns.

The results show that a misplaced channel can have a very short life span until unbalancing and lose up to 40% of its efficiency, so nodes could potentially create a market based on these criteria to sell each other good connections in the network.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[2] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," 2016.

[3] Z. Avarikioti, L. Heimbach, Y. Wang, and R. Wattenhofer, "Ride the lightning: The game theory of payment channels," in *International Conference on Financial Cryptography and Data Security*. Springer, 2020, pp. 264–283.

[4] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," in *Proceedings of the 2012 ACM conference on Computer and communications security*, 2012, pp. 906–917.

[5] G. Avarikioti, E. K. Kogias, R. Wattenhofer, and D. Zindros, "Brick: Asynchronous payment channels," *arXiv preprint arXiv:1905.11360*, 2019.

[6] Z. Avarikioti, O. S. T. Litos, and R. Wattenhofer, "Cerberus channels: Incentivizing watchtowers for bitcoin," in *International Conference on Financial Cryptography and Data Security*. Springer, 2020, pp. 346–366.

[7] C. Decker and R. Wattenhofer, "A fast and scalable payment network with bitcoin duplex micropayment channels," in *Symposium on Self-Stabilizing Systems*. Springer, 2015, pp. 3–18.

[8] M. Green and I. Miers, "Bolt: Anonymous payment channels for decentralized currencies," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 473–489.

[9] J. Lind, O. Naor, I. Eyal, F. Kelbert, E. G. Sirer, and P. Pietzuch, "Teechain: a secure payment network with asynchronous blockchain access," in *Proceedings of the 27th ACM Symposium on Operating Systems Principles*, 2019, pp. 63–79.

[10] A. Miller, I. Bentov, S. Bakshi, R. Kumaresan, and P. McCorry, "Sprites and state channels: Payment networks that go faster than lightning," in *International Conference on Financial Cryptography and Data Security*. Springer, 2019, pp. 508–526.

[11] R. Khalil and A. Gervais, "Revive: Rebalancing off-blockchain payment networks," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 439–453.

[12] R. Pickhardt and M. Nowostawski, "Imbalance measure and proactive channel rebalancing algorithm for the lightning network," in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2020, pp. 1–5.

[13] S. Tikhomirov, R. Pickhardt, A. Biryukov, and M. Nowostawski, "Probing channel balances in the lightning network," *arXiv preprint arXiv:2004.00333*, 2020.

[14] J. Poon and T. Dryja, "The bitcoin lightning network: scalable off-chain instant payments (2016)," *URl: https://lightning. network/lightningnetwork-paper. pdf (visited on 2016-04-19)*, 2016.

[15] F. Engelmann, H. Kopp, F. Kargl, F. Glaser, and C. Weinhardt, "Towards an economic analysis of routing in payment channel networks," in *Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers*, 2017, pp. 1–6.

[16] I. A. Seres, L. Gulyás, D. A. Nagy, and P. Burcsi, "Topological analysis of bitcoin's lightning network," in *Mathematical Research for Blockchain Economy*. Springer, 2020, pp. 1–12.

[17] F. Béres, I. A. Seres, and A. A. Benczúr, "A cryptoeconomic traffic analysis of bitcoin's lightning network," *arXiv preprint arXiv:1911.09432*, 2019.

[18] E. Rohrer, J. Malliaris, and F. Tschorsch, "Discharged payment channels: Quantifying the lightning network's resilience to topology-based attacks," in *SandB '19: Proceedings of IEEE Security Privacy on the Blockchain*, jun 2019.

[19] U. Brandes, "On variants of shortest-path betweenness centrality and their generic computation," *Social Networks*, vol. 30, no. 2, pp. 136–145, 2008.

[20] A. Research, "The growth of the Lightning Network," https://www.research.arcane.no/blog/the-growth-of-the-lightning-network, 2021, [Online; accessed 11-Nov-2021].

Appendix A
Proofs

A. *Lemma 1. The expected number of steps to reach $+a$ or $-b$ for the first time starting from zero.*

Consider S_x as the expected number of steps to reach $+a$ or $-b$ for the first time starting from x. Let p be the probability of going to the positive direction and q the probability of going in the negative direction ($p + q = 1$). Then we can say that if the Random Walker starts from x, he will go to $x + 1$ with probability of p and $x - 1$ with probability of q. so we can infer this recurrence equation: $s_x = 1 + qs_{x-1} + ps_{x+1}$ and for the boundary conditions we have: $s_a = s_{-b} = 0$ implying that the expected number of steps needed to reach $+a$ or $-b$ starting from $+a$ or $-b$ is zero.

so:

$$s_x = \frac{1}{p}s_{x-1} - \frac{q}{p}s_{x-2} - \frac{1}{p} \tag{11}$$

The characteristic equation of (11) is:

$$(z^2 - \frac{1}{p}z + \frac{q}{p})(z-1) = 0 \tag{12}$$

if $p = q = 1/2$ we have $\Delta = 0$ therefore $z_1 = z_2 = z_3 = 1$ so the expected number of steps needed to reach $+a$ or $-b$ starting from x is:

$$s_x = (a-x)(b-x) \tag{13}$$

if $p \neq 1/2$ we have $\sqrt{\Delta} = |\frac{1-2p}{p}|$ therefore $z_1 = z_2 = 1, z_3 = \frac{q}{p}$ and for the number of steps we have:

$$s_x = \frac{ap^{a+b} + bq^{a+b}}{(2p-1)(p^{a+b} - q^{a+b})} + \frac{1}{1-2p}x + \frac{(a+b)p^a q^b}{(2p-1)(q^{a+b} - p^{a+b})}(\frac{q}{p})^x \tag{14}$$

we take $x = 0$ as this gives the expected number of steps to reach $+a$ or $-b$ starting from zero. so we have:

$$S_0 = \begin{cases} \frac{ap^a(p^b-q^b)+bq^b(q^a-p^a)}{(p-q)(p^{a+b}-q^{a+b})} & p \neq 1/2 \\ ab & p = 1/2 \end{cases} \tag{15}$$

B. *Lemma 2.* $\frac{p}{q} = \frac{\lambda(A,B)}{\lambda(B,A)}$

In assumptions of section $5.B$ it is assumed that each node sends its payments to other nodes with a Poisson distribution. The parameter of the distribution for $edge(A, B)$ is $\lambda(A, B)$, which is the payment rate between nodes A and B. Assume the random variable of payments from A to B as X and the random variable of payments from B to A as Y.Thus we have:

$$P(X = n) = \frac{e^{-\lambda(A,B)}(\lambda(A,B))^n}{n!} \tag{16}$$

The total payment rate in each channel is the sum of rates of its two edges. It is known that the distribution of a random variable which is the sum of two random variables that have Poisson distribution is a Poisson distribution; the rate of this distribution equals the sum of rates.

When we have a payment from two Poisson distributions sending payments to the same channel; The probability for the payment to be a payment from node A to node B (p) is:

$$p = P(X = 1|X + Y = 1) = \frac{\frac{e^{-\lambda_x}(\lambda_x)^1}{1!} \times \frac{e^{-\lambda_y}(\lambda_y)^0}{1!}}{\frac{e^{-(\lambda_x+\lambda_y)}(\lambda_x+\lambda_y)^1}{1!}} \quad (17)$$

Thus:

$$p = \frac{\lambda_x}{\lambda_x + \lambda_y} = \frac{\lambda(A, B)}{\lambda(A, B) + \lambda(B, A)} \quad (18)$$

C. ***Lemma 3.*** *If* $\forall S, T \in V : MRates_{ST} = MRates_{TS}$ *then* $p = 0.5$.

We know from lemma 2 that: $\frac{p}{q} = \frac{\lambda(A,B)}{\lambda(B,A)}$ so we have:

$$\frac{p}{q} = \frac{\sum \frac{\sigma(S,T|edge(A,B))}{\sigma(S,T)} MRates_{ST}}{\sum \frac{\sigma(S,T|edge(B,A))}{\sigma(S,T)} MRates_{ST}} \quad (19)$$

Because all channels are bidirectional($\forall edge(A, B) : \exists edge(B, A)$) we have $\forall S, T \in V$:

$$\frac{\sigma(S, T|edge(A, B))}{\sigma(S, T)} = \frac{\sigma(T, S|edge(B, A))}{\sigma(T, S)} \quad (20)$$

In the other hand if we have $\forall S, T \in V : MRates_{ST} = MRates_{TS}$, we can say:

$$\frac{\sigma(S, T|edge(A, B))}{\sigma(S, T)} \times MRates_{ST} = \frac{\sigma(T, S|edge(B, A))}{\sigma(T, S)} \times MRates_{TS} \quad (21)$$

then finally we have:

$$\lambda(A, B) = \lambda(B, A) \quad (22)$$

so

$$p = \frac{1}{2} \quad (23)$$