Throughput Limitation of the Off-chain Payment Networks

Shayan Hamidi Dehshali* , Seyed Mahdi Hosseini* , Soheil Zibakhsh Shabgahi* , Behnam Bahrak
College of Computer and Electrical Engineering, University of Tehran
{shayanhamidi, soheil.zibakhsh, mahdi.hosseini, bahrak}@ut.ac.ir

***Abstract*—Off-chain payment channels were introduced as one of the solutions to the blockchain scalability problem. The channels shape a network, where parties have to lock funds for their creation. A channel is expected to route a limited number of transactions before it becomes unbalanced, when all of the funds are devoted to one of the parties. Since an on-chain transaction is often necessary to establish, rebalance, or close a channel, the off-chain network is bounded to the throughput of the blockchain. In this paper, we propose a mathematical model to formulate limitation on the throughput of an off-chain payment network. As a case study, we show the limitation of the Lightning Network, in comparison with popular banking systems. Our results show that theoretically, the throughput of the Lightning Network can reach the order of 10000 transactions per second, close to the average throughput of centralized banking systems.**

***Index Terms*—Bitcoin, Blockchain, Payment Channels, Channel Rebalancing**

I. Introduction

Bitcoin, introduced in 2008, has demonstrated several superiorities to the conventional banking systems. These systems are centralized; hence, they could be easily manipulated. Also, anonymity and transparency were critical objectives of Bitcoin designers, while their banker counterparts have taken no similar measures [1]. These advantages have popularized this cryptocurrency over the past decade.

However, Bitcoin's design fails to scale the throughput of this network to respond to the skyrocketing demand. Owing to the essence of Bitcoin's consensus algorithm, Proof of Work, the throughput of this network is limited to less than 10 transactions per second [2], [3]. This shortcoming has made Bitcoin scalability a challenging problem, while a centralized system such as Visa can handle up to 24000 transactions per second [4].

A couple of studies have suggested solutions to scale blockchain-based cryptocurrencies. These solutions can be classified into on-chain or off-chain. On-chain solutions focus on modification of blockchain's structures, protocols, and consensus algorithms. On the other hand, off-chain solutions discussed in this paper, propose separate structures to reduce the traffic of the main network [5].

Off-chain payment networks enable users to route payments to other indirectly connected users through payment channels [6], [7], [8], [9]. Lightning Network is probably the most well-known solution of this type, which is designed for Bitcoin. Every two participants in a payment network can establish a channel where they have to form a financial relationship, implemented by multi-signature blockchain transactions.

Setting up or tearing down a channel can be done using one on-chain transaction; meanwhile, these channels are capable of routing thousands of off-chain payments during their lifespan. Broadcasting a payment and waiting for its confirmation is not obligatory in off-chain payment networks; hence, the throughput of the cryptocurrency's network enhances significantly.

As mentioned, both endpoints of a channel may allocate an initial fund by a shared on-chain transaction. Moreover, each party keeps track of the amount of owned coin, i.e., the balance. If a party intends to route a payment, consequently modifying balances, such that the minimum of the balances drops beneath a threshold, the channel becomes unbalanced, and routing through this channel is only possible in one direction. Since the success rate of a single unit payment decreases dramatically in an unbalanced network [10], the channels ought to be rebalanced.

A fundamental problem arising from the payment channels rebalancing is the need for two costly on-chain transactions. Some studies put forward rebalancing schemes that require on-chain transactions less often [11], [12]. Still, their schemes apply to a small portion of network topologies or are incompatible with on-chain protocols.

Based on this problem, our goal is to formulate a link between the blockchain's throughput and the off-chain payment network. We want to evaluate how well the off-chain payment networks address the scalability issue of the blockchain systems and if they can compete with centralized banking systems.

The rest of this paper is organized as follows. In Section II, we elaborate relevant terms and concepts. Section III discusses the studies relevant to this work. In Section IV, we describe our proposed mathematical model that formulates the limitation of the payment network's throughput. In Section V, using the same network specifications, we present a comparison between the throughput limit of the Lightning Network and the average throughput of popular banking systems. Finally, Section VI concludes our work.

II. Technical Background

In this section, we explain relevant terms and concepts, and provide the technical background to understand the remainder of this paper.

*equal contribution

A. Payment Channels

A payment channel is a temporary off-chain trading mechanism in which users allocate funds using a 2-of-2 multi-signature address which can be spent with the cooperation of both parties. Parties create a spending transaction to devote the funds of this address to each of them. This contract acts as a financial relationship. Making a transaction consists of creating a new output balance for the contract and getting both parties to sign it. This method allows the parties to make transactions with negligible cost. A channel becomes unbalanced when almost all of the balance is allocated to one of the parties; hence, only one of the parties can make payments. We call the sum of funds inside a channel its *capacity*. The channel closes when one of the parties publishes the latest contract to the blockchain; spending the funds inside the multi-signature address.

B. Payment Networks

Since the cost of initiating and tearing down a payment channel is the fee for two transactions on the blockchain, it is unreasonable for each pair of users to be connected directly. Several connected parties (i.e. payment channels) form a payment network. A payment network can route payments between nodes that are indirectly connected by intermediary nodes. The *Lightning Network* is the payment network built for Bitcoin.

C. Channel Effective Lifespan

A channel's *effective lifespan* is the time from creating a channel until the first imbalance occurs [**?**]. Since the exact pattern of routed payments through a channel cannot be predicted, the effective lifespan of the single channel can be projected with a probability distribution. In this paper, we refer to this distribution as $f(t^*)$ where t^* is the time passed since the last rebalancing of the channel.

Limit on the blockchain's throughput

Blockchain's payment confirmation consists of several steps. First, a block should be mined. The blockchain protocol adjusts the time interval between two consecutive mined blocks in order to prevent double-spending attacks [13]. This adjustment keeps the time interval around a particular value (e.g. 10 minutes for the Bitcoin network), according to the total computational power in the network. In addition, the payment must be placed in a block. The capacity of a block is restricted, so a limited number of transactions can be fit.

Second, the blocks and transactions needed to be broadcasted through the network. With the assumption of 250 bytes transaction sizes, if Bitcoin grows so that the network has to process 40,000 transactions per second (processing level of the Visa network at its peak), the data stream of the network will be 10 megabytes per second (MBps) to receive all the transactions, excluding the traffic overhead of transactions' information. Although 10 MBps is ordinary in high-speed links, it rules out nodes that cannot meet this requirement [14]. Consequently, the decentralization prerequisite would be unfulfilled.

Therefore, the Bitcoin blockchain's current throughput ends up less than ten transactions per second [15].

III. Related Work

Khalil et al. [11] propose an algorithm in which a set of users can rebalance securely without any on-chain transactions. Yet, the existence of a cycle in the participants' channel graph is a condition that a small portion of network topologies satisfy. Similarly, this condition applies to the Lightning Network [6], a second layer off-chain payment network built on Bitcoin, whose rebalancing algorithm involves a local search of rebalancing cycles (transactions of a fixed amount that begin and end with the same user) initiated by a single user. Although Ge et al. [12] suggested a rebalancing scheme applicable to acyclic networks that often achieves refunding with only one on-chain transaction, it is not compatible with Bitcoin.

Tikhomirov et al. [16] analyzed the limit of the Hashed Timelock Contracts (HTLC), and they estimated the effect of the limit on the number of concurrent payment channels; thus, casting doubt on further scaling of the Lightning Network. Conoscenti [17] in his detailed thesis, inspected the capabilities and limitations of the payment channel networks. With a self-implemented Lightning Network simulator (CLoTH), he achieved to simulate a set of snapshots of the Lightning Network with a variety of its parameters (such as payment amount, payment rates, and channel capacities); hence, discovering the correlation between payments' success rate and given network's parameters.

In this work, we propose a correlation between the throughput of the off-chain payment networks and off-chain and on-chain network parameters, based on the rebalancing method of the off-chain payment network. Since alternative rebalancing schemes can not always guarantee less on-chain transactions, our proposed limit on the throughput stays firm.

IV. Model

In this section, we provide a detailed description of our model. We want to find a link between the inherent throughput limitation of a blockchain network and the payment network built on top of it. This tie lies at the interaction point of the two systems, which is when a channel needs to be created, terminated, or rebalanced. We assume that rebalancing requires two consecutive termination and creation transactions on the blockchain.

For the purpose of finding a theoretical limit of the payment network, we assume that the blockchain's throughput is only dedicated to payment network transactions. Thus, all blockchain transactions are assumed to be rebalancing transactions. We consider a *steady state* for the payment network, meaning the topology is fixed, unbalanced channels request a rebalancing transaction from the blockchain, and are immediately rebalanced.

We define L as the blockchain's transaction rate. In addition, we define β as the rate of requested rebalancing transactions.

In order to have a bounded queue of requested rebalancing transactions, condition

$$\beta < L \tag{1}$$

should be fulfilled. Fig. 1 visualizes our model.

Fig. 1. The interaction of the payment network and blockchain system

A. Single Channel Analysis

We found a correlation between the probability of the first unbalancing event at time t^*, from the last rebalancing, and the probability of unbalancing at time t, from the creation of a channel. We define $f(t^*)$ and $g(t)$ to formulate this correlation.

Consider $f(t^*)$ to be the probability density function of random variable t^*, also mentioned in Section II-C. We define $g(t)$ so that $g(t)\delta t$ is the probability of channel unbalancing between times t to $t+\delta t$, where δt is small enough that at most one unbalancing event occurs in this interval.

We need to discover the behavior of $g(t)$ at distant times or $t \to \infty$, where we show the unbalancing requests converge to a Poisson process. At distant times, the probabilities of unbalancing are equal during each period. This behavior brings steadiness to the network; therefore, we included this distant time behavior in the aforementioned *steady state* definition.

According to Lemma A-A, the correlation between f and g can be formulated as:

$$g(t) = f(t) + \int_0^t g(\tau) f(t-\tau)\, d\tau \tag{2}$$

It is difficult to solve this equation; still, finding the limit of $g(t)$ at $+\infty$ is possible using Laplace transform. Consequently, after taking Laplace transform equation 2 turns to:

$$G(s) = \frac{F(s)}{1-F(s)}. \tag{3}$$

Based on equation 3 and Lemma A-B, the value for $g(t)$ at the steady state is:

$$\lim_{t\to+\infty} g(t) = \frac{1}{E\left[f(t)\right]}, \tag{4}$$

where $E\left[f(t)\right]$ is the expected value of the probability density function $f(t)$.

B. Expected Lifespan of a Channel

Zibakhsh et al. [**?**] show the expected time for a channel to become unbalanced is:

$$E\left[f(t)\right] = \frac{C^2}{8 \times EBC_G(a,b) \times r \times \omega^2}, \tag{5}$$

where C is the channel capacity, ω is the payment sizes, r is the rate at which every two nodes send payments to each other, and $EBC_G(a,b)$ is the edge betweenness centrality in the payment network G between nodes a and b.

When applying this equation, we assume that all payments have the same size, ω, and each pair of nodes send payments to each other with a Poisson process with the fixed rate of r.

C. Network Analysis

As shown in Section IV-A, after a long time from the creation of a channel, the probability of an imbalance at an interval of size δt is the constant $\frac{1}{E[f(t)]} \times \delta t$. Thus, the rebalancing requests from a single channel to the blockchain have a Poisson distribution with $\lambda = \frac{1}{E[f(t)]}$.

Since channels are considered to be rebalanced instantly, and the network is not dynamic, the unbalancing of channels are independent. Accumulation of k independent Poisson processes with rates λ_i, for i from 1 to k, is a Poisson process with rate $\sum_{i=1}^{k} \lambda_i$. It can be inferred that the network's overall rebalancing transaction requests to the blockchain is a Poisson process. To remind, each rebalancing request requires two on-chain transactions.

Therefore

$$\beta = 2 \times \sum_{i=1}^{n} \frac{1}{E[f_i(t)]}, \tag{6}$$

where n is the number of channels in the payment network and $E[f_i(t)]$ is the expected lifespan of payment channel i.

From equations 5 and 6 we have:

$$\beta = 16 r \omega^2 \times \sum_{i=1}^{n} \frac{EBC_G(i)}{C_i^2}, \tag{7}$$

where C_i is the capacity of channel i and $EBC_G(i)$ is the edge betweenness centrality of channel i in the network G.

V. Case Study

In this section, we compare Lightning Network's throughput with centralized banking systems.

We assume all channels' capacities is a constant C, where C is the average channel capacity of the real-world Lightning Network. We also assume that the network topology is a star graph [18]. Lemma A-C shows:

$$\sum_{i=1}^{n} EBC_{stargraph}(i) = n^2, \tag{8}$$

where n is the number of channels in the star graph. Considering these assumptions, we rewrite equation 7 as:

$$\beta = \frac{16 r n^2 \omega^2}{C^2} \tag{9}$$

According to [**?**], the payment network throughput T can be calculated by summing all entries in the $Mrates$ matrix, the matrix of payment rates between each pair of nodes. Since we assumed that all nodes send payments to all other nodes with rate r, and the number of nodes is $n+1$, the payment network throughput is:

$$T = n(n+1)r, \tag{10}$$

where n is the number of channels in a star graph payment network, and r is the payment rate between each two nodes.

We take b to be $\frac{C}{2}$, representing the initial fund each node allocates to the channel.

Taking equations 9, 10, and condition 1, we have the following inequality:

$$T < \frac{b^2 L}{4\omega^2}(1 + \frac{1}{n}), \tag{11}$$

where L is the blockchain throughput and ω is the average payment size. In a real-world scenario, n is in the order of millions, so the 11 inequality can be simplified to:

$$T < \frac{b^2 L}{4\omega^2} \tag{12}$$

In table I, we presented operational statistics of some popular banking systems in 2020 and compared their throughput to the upper bound of the Lightning Network. Total payment volume (TPV) is the total amount of money transacted in US dollars ($). Payment transactions (PT) is the number of transactions during 2020. The average payment size (ω) is calculated as TPV divided by PT. Total volume (TV) is the total amount of deposited funds in US dollars ($); when divided by the number of users (NU), it gives the average deposit (b).

Using b, ω, equation 12, and taking Bitcoin blockchain throughput as 7_{tps}, we calculate T_{sup}, the supremum of the Lightning Network throughput if it had the same specifications as the corresponding banking system. Also, AT is the average throughput (per second) of the banking system; derived from PT.

VI. Conclusion and Future Work

In this study, we proposed a model to link the inherent blockchain throughput limitation to the limitation of off-chain payment networks.

First, we presented an inequality that links the network's unbalancing rate to the blockchain's throughput. Then, we reached a formula for the unbalancing rate of a single channel. We proceeded by generalizing the formula to the payment network. As a case study, we compare centralized banking systems' average throughput to the Lightning Network's throughput limit with the same specifications. Our results show the theoretical limit of the Lightning Network has the same order of magnitude as the average throughput of centralized banking systems.

As a future direction for this research, deep-learning and generative adversarial networks can be utilized to predict how the network scales. This prediction will improve the estimation significantly; because we can estimate with a more accurate network topology.

References

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

[2] E. Georgiadis, "How many transactions per second can bitcoin really handle? theoretically." *Cryptology ePrint Archive*, 2019.

[3] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. Gün Sirer, *et al.*, "On scaling decentralized blockchains," in *International conference on financial cryptography and data security*. Springer, 2016, pp. 106–125.

[4] Visa. small-business-tools. [Online]. Available: https://usa.visa.com/run-your-business/small-business-tools/retail.html

[5] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of blockchain: A survey," *Ieee Access*, vol. 8, pp. 16 440–16 455, 2020.

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

[7] P. Prihodko, S. Zhigulin, M. Sahno, A. Ostrovskiy, and O. Osuntokun, "Flare: An approach to routing in lightning network," *White Paper*, p. 144, 2016.

[8] R. network. Fast, cheap, scalable token transfers for ethereum. [Online]. Available: https://raiden.network/

[9] 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.

[10] 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.

[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] Z. Ge, Y. Zhang, Y. Long, and D. Gu, "Shaduf++: Non-cycle and privacy-preserving payment channel rebalancing," *Cryptology ePrint Archive*, 2022.

[13] M. Rosenfeld, "Analysis of hashrate-based double spending," *arXiv preprint arXiv:1402.2009*, 2014.

[14] A. M. Antonopoulos, O. Osuntokun, and R. Pickhardt, *Mastering the Lightning Network*. " O'Reilly Media, Inc.", 2021.

[15] B. Explorer. Transaction rate per second. [Online]. Available: https://www.blockchain.com/charts/transactions-per-second

[16] S. Tikhomirov, P. Moreno-Sanchez, and M. Maffei, "A quantitative analysis of security, anonymity and scalability for the lightning network," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2020, pp. 387–396.

[17] M. Conoscenti, "Capabilities and limitations of payment channel networks for blockchain scalability," *Turin: Politecnicno di Torino*, 2019.

[18] 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.

[19] Visa. Visa inc. q1 2021 operational performance data. [Online]. Available: https://s1.q4cdn.com/050606653/files/doc_financials/2021/q1/Visa-Inc.-Q1-2021-Operational-Performance-Data.pdf

[20] Paypal. 2021 notice of annual meeting of stockholders and proxy statement, 2020 annual report. [Online]. Available: https://s201.q4cdn.com/983461986/files/doc_financials/2021/ar/PYPL002_AR_2020_Bookmarked.pdf

[21] Logica. What's in our wallets? [Online]. Available: https://logicaresearch.com/americans-keep-more-money-in-paypal-than-cash-in-wallet/

[22] M. Card. Supplemental operational performance data q1-21. [Online]. Available: https://s25.q4cdn.com/479285134/files/doc_financials/2021/q1/1Q21-Supplemental-Operational-Performance-Data.pdf

[23] Discover. 2021 annual report. [Online]. Available: https://www.annualreports.com/HostedData/AnnualReports/PDF/NYSE_DFS_2021.pdf

Appendix A
Proofs

A. *Lemma 1.*

$$G(s) = \frac{F(s)}{1 - F(s)}, \tag{13}$$

where $f(t)$ and $g(t)$ are the functions discussed in Section IV. Also, $G(s)$ and $F(s)$ are the Laplace transforms of $f(t)$ and $g(t)$, respectively.

As a reminder, we define $g(t)$ so that $g(t)\delta t$ is the probability of channel unbalancing between times t to $t+\delta t$, where δt is small enough that at most one unbalancing event occurs.

Banking System	TPV(B$)	PT(Billions)	TV(B$)	NU(Millions)	ω($)	b($)	T_{sup}**(tps)**	AT(tps)	Refs
Visa	4508	122.09	6788	2364	36.92	2871.4	**10585**	3871	[19]
PayPal	936.06	15.42	-	377	60.7	485	**112**	489	[20], [21]
Master	2002	64.76	3434	1374	30.9	2499.3	**11449**	2054	[22]
Discover	417	7.58	153.9	59.8	55	2573.6	**3832**	240	[23]

TABLE I
POPULAR CENTRALIZED BANKING SYSTEMS IN 2020, COMPARED WITH LIGHTNING NETWORK LIMITATION

$$P\{U\} = P\{U \cap S\} + P\{U \cap \bar{S}\}, \tag{14}$$

where U is the event of unbalancing between times t to $t + \delta t$, and S is the event of no unbalancing until time t. We know from definition that $P\{U \cap S\}$ equals $f(t)\delta t$.

$$P\{U \cap \bar{S}\} = \int_0^t g(\tau) f(t-\tau)\, d\tau\, \delta t, \tag{15}$$

where τ is the last time the channel was unbalanced (based on our assumptions, rebalancing occurs immediately after unbalancing).

Based on equations 14 and 15, the generalized equation is:

$$g(t) = f(t) + \int_0^t g(\tau) f(t-\tau)\, d\tau \tag{16}$$

Taking the Laplace transform of equation 16 we have:

$$G(s) = \frac{F(s)}{1 - F(s)}. \tag{17}$$

B. *Lemma 2.*

$$\lim_{t \to +\infty} g(t) = \frac{1}{E\left[f(t)\right]}, \tag{18}$$

where $f(t)$ and $g(t)$ are the functions discussed in Section IV. Also, $E\left[f(t)\right]$ is the expected value of the probability density function $f(t)$.

According to the Final Value Theorem, the limit of function $g(t)$ at $+\infty$ can be calculated as below:

$$\lim_{t \to +\infty} g(t) = \lim_{s \to 0} sG(s), \tag{19}$$

where $G(s)$ is the Laplace transform of $g(t)$. We suppose that g is continuous in its domain. From equations 13 and 19, we can infer:

$$\lim_{t \to +\infty} g(t) = \lim_{s \to 0} \frac{sF(s)}{1 - F(s)}, \tag{20}$$

where $F(s)$ is the Laplace transform of $f(t)$, the probability density function mentioned in Section IV-A. Owing to the property of probability density functions, the integration of this function from 0 to ∞ equals 1. Therefore, we can imply that $F(0) = 1$.

Since the limit of both numerator and denominator in the right-hand side of equation 20 are 0, Hopital's rule can be applied. Thus, both numerator and denominator should be differentiated from s around point $s = 0$:

$$\lim_{s \to 0} \frac{sF(s)}{1 - F(s)} = \lim_{s \to 0} \frac{F(s) + sF'(s)}{-F'(s)}. \tag{21}$$

From another property of Laplace transform:

$$\lim_{s \to 0} -F'(s) = \int_0^\infty t f(t)\, dt = E[f(t)], \tag{22}$$

where $E\left[f(t)\right]$ is the expected value of distribution $f(t)$. With $E\left[f(t)\right] \neq 0$, $E\left[f(t)\right] \neq \pm\infty$, equation 21 and equation 22, We have:

$$\lim_{s \to 0} \frac{F(s) + sF'(s)}{-F'(s)} = \frac{1}{E\left[f(t)\right]} \tag{23}$$

Finally, from equations 20, 21 and 23, we can infer:

$$\lim_{t \to +\infty} g(t) = \frac{1}{E\left[f(t)\right]}. \tag{24}$$

C. *Lemma 3.*

$$\sum_{i=1}^{n} EBC_{stargraph}(i) = n^2, \tag{25}$$

where $EBC(i)$ is the edge betweenness centrality of channel i. Also, n is the number of channels in the star graph topology.

We know that the edge betweenness centrality of channel i is:

$$EBC(i) = \sum_{\substack{s,t \in V \\ s \neq t}} \frac{\sigma(s,t|i)}{\sigma(s,t)}, \tag{26}$$

where $\sigma(s,t)$ is the number of shortest paths from node s to node t and $\sigma(s,t|i)$ is the number of shortest paths from node s to node t passing through channel (edge) i.

Since star graph is a tree, exactly one path exists between each pair of nodes, that means $\forall\, s,t \in V : \sigma(s,t) = 1$. Also, for channel i, $\sigma(s,t|i) = n$. According to the symmetry of the star graph topology, channel i calculations can be applied to each of n channels. Thus:

$$\sum_{i=1}^{n} EBC(i) = n^2 \tag{27}$$