Effectivenes simulation of a rebalancing algorithm for the Lightning Network under partial participation

Bachelor Thesis

August 1, 2020

Organization	FHNW, School of Business, Basel
Study program	Business Information Technology
Author	Tobias Koller
Supervisor	Prof. Dr. Kaspar Riesen
Project sponsor	Prof. Dr. Thomas Hanne
Expert	René Pickhardt

Abstract

Here follows my abstract Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.1-2

Keywords: Lightning, Bitcoin, path finding

Contents

Declaration of honor

Add declaration of honor. I hereby confirm that: . . .

Foreword

Some background

Glossary

Should be able to auto generate that thing

- Bitcoin
- Bitcoin Node
- Lightning Node
- Routing
- Forwarding
- Blockchain
- Base chain, second layer

Also define here what does it mean if some text is:

- **Bold**
- *Italic*
- <u>underlined</u>

1 Introduction

This section aims to give a basic understanding of the Bitcoin and Lightning technology.

> Define certain terms like, node, (block)chain, confirmation, channel, balance, capacity, source routing, forwarding

1.1 Lightning technology

The Lightning Network is a network that utilizes Bitcoin as its underlying system. It can, therefore, be described as a "second layer" protocol building upon the Bitcoin "base layer". Bitcoin is a decentralized peer-to-peer money system with no central entities. The system was designed with security and robustness being the main objectives, sacrificing other properties such as transaction throughput (speed).

The Bitcoin system consists of nodes each maintaining a ledger of historic transactions. All new transactions must be distributed to all nodes and validated by them. Transactions are therefore public information and must be stored by all nodes. To allow many people to run a node, therefore promoting a decentralized network, the hardware requirements must be as low as possible. This is why there is a limitation of new transactions that can be recorded in the network causing this low transaction throughput.

The Lightning technology offers a solution to this issue of scaling by adding a second network on top. In this network participants open payment channels with each other. Transactions within these channels are only visible to the two partners but stay invisible to the rest of the network. While opening and closing a channel each requires one transaction in the base layer (Bitcoin) unlimited transactions with almost no throughput restriction can be facilitated within a channel during its lifetime.

It is important to note the difference between a Lightning node and a Bitcoin node. While they can run on the same system, they operate in two different networks. A Bitcoin node works well individually but a Lightning node needs to have access to a Bitcoin node.

For a node to pay another node that it has no direct channel open with, he can simply route the transaction via other nodes and their channels. Since the network graph is public, the path can be chosen by the initiator of a transaction. This is called source routing.

A payment channel is always opened between two nodes. One of the participants acts as the initiator and provides funds for the channel in the form of bitcoin. This leads to the total capacity being allocated to his or her balance within the channel. As soon as he starts to make payments towards the other node, his or her balance decreases, and the partner's balance increases (total capacity remains constant). Transactions can only be executed if the amount is smaller or equal than the channel's capacity and if the sending node has enough local balance. Channels and their capacities are announced to the network but the distribution of balances remains private to the channel partners.

1.2 Previous work

René Pickhardt's and Mariusz Nowostawski's publication "Imbalance measure and proactive channel rebalancing algorithm for the Lightning Network" [1] serves as a base to formulate the question for this thesis. In their work, they present a solution for the pathfinding problem in a privacy-aware payment channel network. The proposed solution includes a rebalancing protocol which the nodes of the network should follow to achieve a higher balancedness (for itself but also

the entire network). It consists of instructions to proactively rebalance their channels within their friend of a friend's network, redistributing the relative funds owned in a channel but leaving total funds owned unchanged.

Rebalancing is an activity where one node engages in a circular payment that pays itself. This is only possible when the node has at least two channels with different peers. The payment gets routed **out** through one channel and is **received back** over another. On the way, it can use one or more hops to find back to the sender node. This procedure enables a node to change the balances of the individual channels while the total node balance stays the same. In practice, there would be a fee collected by the intermediate nodes whose channels are used. In the proposed rebalancing protocol nodes would forego the fee and only participate in the rebalancing attempt if their balancedness improves as well.

1.3 Problem statement

These payment channel networks are decentralized by nature and no protocol change can be forced upon the node operators. Therefore, the question arises on how effective this protocol change will be assuming only partial participation of nodes. What are the effects of different levels of participation on the imbalance measure [1] of the network during repeated rebalancing cycles? What is the effect of different levels of participation on the network's ability to route payments between random nodes?

2 Path finding problem

> Explain why finding a path in the lightning network can be so difficult

Nodes trying to find a path in the Lightning Network work with limited information. While they know what channels are available and what their capacities are, they do not know about the balances and therefore whether the nodes can forward their payment or not. Hence, it is likely that a payment attempt fails because a node had insufficient balance. The paying node needs to find another route and retry the payment until it succeeds. If the payment fails repeatedly it can cause delays that are bad for the user experience.

3 Methodology

> explain how to get the network information for a running node. quickly show how I extracted the data from the full node. Explain the structure of the python class **Network**

. And some more **bold text**.

To model the network, public information from the Lightning Network is used. From a Lightning node, all the channel and node information can be extracted.

For all further manipulations and calculations, the programming language Python will be used. This includes writing code that facilitates:

- The selection of nodes, participating in the protocol change.
- Implement the proposed algorithm [1, p. 3].
- Performing rebalancing in the network.
- Storing different network states for different scenarios.

---

[1]Defined as the inequality of the distribution of a nodes channel balance coefficients

- Calculate different performance measures.
- Aggregate data.
- Plot graphs to visualize the results.

4 Routing measures

5 Experimental setup

5.1 Preprocessing

explain which nodes and channels where selected

5.2 Implementing routing protocol

Describe how the proposed protocol change is impolemented in the **Network** class.

show illustrations with a dummy network

ask Rene to his dummy network

6 Results

7 Conclusion

8 Outlook

References

[1] R. Pickhardt and M. Nowostawski, *Imbalance measure and proactive channel rebalancing algorithm for the Lightning Network*. 2019.

9 Todo-Notes