UMEÅ UNIVERSITY
Department of Computing Science

January 28, 2019

Routing Fee Estimation in the Lightning Network

Project Plan

preliminary 1.0

Name	John-John Markstedt
Cinnober Supervisor	Oskar Janson
University Supervisor	Jerry Eriksson
Examinator	Henrik Björklund

Contents

1 Introduction

This is the project plan for the master thesis of Routing Fee Estimation in the Lightning Network. Some parts are directly taken from the project specification to make it a self contained document.

1.1 Background

Although still very much in its early stages, blockchain and distributed ledger solutions are said to be able to transform the current financial infrastructure, especially the post-trade side. Most notable of all applications of blockchain technology is Bitcoin, which is an open decentralized network with an effectively immutable database of transactions, shared by all full nodes in the network. The internal currency, bitcoins, is provided to miners who help secure the network by participating in the Proof of Work consensus algorithm. Since Bitcoin's nascence, other similar solutions have appeared. Some are modified forks of Bitcoin while some are built from scratch using the same ideas. One of the challenges that all public decentralized blockchain networks faces is how it should handle an increased number of transactions. Increasing throughput is important in order to make the network capable of supporting e.g. regular payments. There are various ways to increase throughput, but roughly they sort into two categories:

- Increase throughput on the base layer, with consequences of increased requirements for participation in the base layer as a full node.
- Create layers on top of the base layer where most updates happen, only resolving the sum of updates to the layer below.

In 2017, the Bitcoin scaling debate raged on, in the end resulting in a split of both community and coin. In the aftermath a fork of Bitcoin was created, called Bitcoin Cash. Bitcoin Cash had the approach that throughput should increase in the base layer, in the way of increasing block size. Bitcoin itself had a more restrained strategy for the base layer, favoring the additional layers approach. Specifically, payment channels and the Lightning Network would provide an outlet for smaller transactions in the network. In a payment channel, a set amount of bitcoin is committed for use by the senders and the channel is created by an opening transaction. Once the transaction has been registered, parties in the channel that have a positive

1.2 Problem Description

In order to get compensation for providing channels for routing, the routing node can decide to take a fee for the use of its channels. One of the problems a node operator faces is what the fair price of routing through its channels is. A too high fee would result in the channel being ignored and payments would be routed through other nodes with competitive fees. It does not want to be too cheap either, since running a routing node carries risk (nodes are always online and are a target for attacks) and has requirements in terms of hardware and time spent. The task then comes to finding a competitive fee that is fair but profitable. Examples on factors that can be considered:

- Competing fees for routing towards the same segment of the network.
- The cost for the operator in rebalancing their channels.
- Operating costs for running the node.

The main problem to solve in this thesis project is that of finding the optimal fee for a routing node. Further, the optimal strategy for operating a routing node should be investigated. Sample questions to answer are:

- What is the fair discount for a transaction that balances the channel, as opposed to an unbalancing one?
- When should a new channel be opened, and what node should the new channel connect to in order to incentivize routing through the node?
- When should a manual rebalancing of the channels occur, as opposed to incentivized rebalancing using discounts?

1.3 Goal

The goal of the thesis is to investigate and implement models for the estimation of routing fees for a routing node on the lightning network.

2 Objectives

These are the main objectives with the project:

- A study of payment channels, the current Lightning Network and proposed future improvements.
- A study of routing node operation, what are the actions, costs and risks that need to be considered when operating a node?
- A study of techniques useful for estimating the routing fee.
- A model for estimating the routing fee should be produced.

3 Literature and references

The literature and references listed below will make up the base of the thesis. More literature and references will be added as the project progresses.

Andreas Antonopoulos book Mastering Bitcoin[10] is the book on bitcoin and will provide a sound basis for the on-chain necessities.

The original bitcoin[13] and lightning[14] papers and all proposed protocol improvements[1] are great primary sources.

The bitcoin reference implementation[2], along with other node implementations[4][3] as well as lightning specification[8] and implementations[6][5][7] will be studied and used during the project.

It is still unclear if Game Theory is applicable to this problem, however a couple of books on the topic are borrowed from the Jerry Eriksson. Namely Noncooperative Game Theory[11] and [12].

4 Communication

In this section the various aspects of communication during the project is discussed.

4.1 Weekly report

A report in the form of a markdown document will be written each week and be available in the thesis repository[9]. Each document will roughly follow the same structure with three major categories, namely, What I've been doing during the week, Problems I'm faced with going forward and what I should be doing the following week.

4.2 Documents and thesis report

All the project's resources will be available through a git repository[9]. There the project's progression can be observed. Git is a version control system, this will provide an extensive history over the project. Every type of resource will be made available through git including text, images and source code.

4.3 Meetings

As the thesis will be written from the Cinnober office, meetings with the Cinnober supervisor Oskar Janson can easily be had when needed.

Meetings with the University supervisor will not be had on a time schedule but on an 'as needed' basis.

5 Time plan

An external timeplan for the project should most likely be attached alongside this document. Otherwise it shall always be available in the thesis repository[9]. The timeline contains deadlines set be the university as well as a rough estimation on the project tasks.

6 Risk

As with any thesis there is some inherit risk that no proper result is even possible. Regarding this thesis there is some major question marks. How is an estimation deemed better than another one when much of the network happens off-chain and with Onion Routing? Does the whole network be simulated to get proper benchmarks and is a simulation a satisfactory replacement for real network?

I believe these problems can be dealt with and if they're to become insurmountable I have no doubt that a slight shift of focus still could deliver a proper master level thesis.

It is of course important to force these issues early in the project so if major problems arise a modification of the thesis can be done early.

References

[1] Bitcoin improvement proposals. https://github.com/bitcoin/bips.

[2] Bitcoin reference implementation. https://github.com/bitcoin/bitcoin.

[3] btcd: a full node bitcoin implementation. https://github.com/btcsuite/btcd.

[4] Light weight bitcoin node implementation. https://github.com/lightninglabs/neutrino.

[5] Lightning node c-lightning developed by blockstream. https://github.com/ElementsProject/lightning.

[6] Lightning node daemon. https://github.com/lightningnetwork/lnd.

[7] Lightning node eclair developed by acinq. https://github.com/ACINQ/eclair.

[8] Lightning specification, request for comments. https://github.com/lightningnetwork/lightning-rfc.

[9] Thesis source repository. https://github.com/Johnstedt/master-thesis-ln-fee-estimation.

[10] Andreas Antonopoulos. *Mastering Bitcoin*. O'Reilly Media, first edition, July 2014.

[11] João P. Hespanha. *Noncooperative Game Theory*. Princeton University Press, 41 William Street, Princton, New Jersey, first edition, 2017.

[12] Hamidou Lasaulce, Samson; Tembine. *Game Theory and Learning for Wireless Networks*. Academic Press, The boulivard, Langford Lane, Kidlington, Oxford, OX5 1GB, first edition, 2011.

[13] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system.

[14] Thaddeus Poon, Joseph; Dryja. The bitcoin lightning network: Scalable off-chain instant payments. https://lightning.network/lightning-network-paper.pdf.