UMEÅ UNIVERSITY
Department of Computing Science
Master thesis report

Examensarbete för civilingenjörsexamen i teknisk datavetenskap 30HP, 5DV143, VT19

Planning for master-thesis

Name	Carl-Johan Andersson
CAS	caan0156@umu.se
CS	c14can@cs.umu.se
Date	2019-01-31

University Supervisor
Jan-Erik Moström (jem@cs.umu.se)
Company Supervisor
Oskar Janssson (oskar.jansson@cinnober.com)

1 Introduction

Cinnober is a provider of IT solutions to the infrastructure providers of the global financial industry, including exchanges and clearing houses. Cinnober has solutions from price discovery, trading, clearing to settlement of financial securities. So it is in their interest to try and be on the forefront when it comes to new technologies in finance. While the block chain it self is a relatively new technology an even newer concept is atomic swaps. This is what will be the subject of my study.

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 Bitcoins nascence, other similar solutions have appeared. Some are modified forks of Bitcoin while some are built from scratch using the same ideas.

A recent development is the concept of atomic swaps. Trusting intermediaries always comes with a risk, the third-party in a swap could run off with the money or maliciously co-operate with the other party. An atomic swap gets around this problem by using the clever way that bitcoin and other cryptocurrencies transactions can be programmed or scripted. In 2013 a new method of doing swaps was discovered that allows two parties to swap coins across chains in a trustless way. A cross-chain transaction refers to two different transactions on two different chains. In its most basic form an atomic swap is a transaction from A to B on chain 1 and from B to A on chain 2. The atomicity means that the swap either is fully performed or nothing happens at all. The atomicity is assured with so called trap-door mathematics.

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 pos- itive balance can use it to send bitcoins to the other party. The channel is strictly bidirectional and with a constant capacity, you can only transfer coins to the owner of the address that is targeted in the payment channel. A payment channel update is only between the two parties involved in the channel, meaning transactions using the channel don't need to be registered as transactions in a block in the base layer. Once any of the parties wishes to use their coins somewhere else, they can publish a closing transaction to the base layer, closing the channel and unlocking the coins attributed to each party. Usage of payment channels is very convenient if you have two parties that frequently send bitcoin back and forth between each other. A popular example could be a trader sending bitcoin to an exchange, in that case the trader need only keep the balance required to execute their trades on the exchange, having the rest available for transfer on their side in the channel.

An exciting use of payment channels is that they can be linked together to form a network. There is an ongoing effort to build one such network, under the name The Lightning Network (LN). In the LN, nodes set up payment channels to other nodes and enable routing of payments through them. Given a well-connected network and enough capacity, it promises to provide the best support for everyday payments yet. There is still a lot of work to be done before widespread and frequent use of LN is valid, but the future of networks like LN looks bright.

Atomic swaps and lightning channels can be combined, indeed the mathematical concepts driving the atomic swap is not that different from what makes the lightning network function in the first place. Cross chain lightning network swaps has so far been demonstrated to work.

1.2 Goal

The goal of this thesis is to investigate techniques for conducting settlement of assets on different cryptocurrency chains, evaluating advantages and drawbacks in different use cases.

The main purpose of the thesis is to further my own and the worlds knowledge about the new settlement methods that has been discovered recently. The second objective is to become somewhat of an expert in the field of block-chain, lightning network, atomic swaps and settlements.

2 Objectives

The primary objectives are the following:

- Understand most or all there is to know about block-chain
- Gain a good understanding of lightning network and all the possibilities it brings.
- Perform and understanding the mathematics and underlying concepts of atomic swaps.
- Perform and understand atomic swaps on two different lightning networks. (For example Bitcoin to Litecoin)
- (If there is time) Perform and understand an alternative to atomic swaps, for example micro swaps.
- Understand the advantages and disadvantages of the different types of settlement.

3 Literature and references

This entire field is relatively new and quite complex, So a lot of extensive reading and studying has to be done. Below I have compiled the litterature and references I intend to look at primarily. This is only the start, more will probably be read as the project proceeds.

3.1 Literature

- Mastering bitcoin, second edition.[1]
- The original bitcoin whitepaper[2]
- The original lightning network white paper[3]

3.2 Source code

A lot of the work will go into studying the source code and documentation for underlying technologies and solutions.

- Bitcoin core reference node
- Lightning network node

3.3 Other

If the project gets stuck somewhere or something is unclear there is a number of places where I could get help from others who are involved in block-chain etc.

- Bitcoin talk
- Free node chat (lnd)

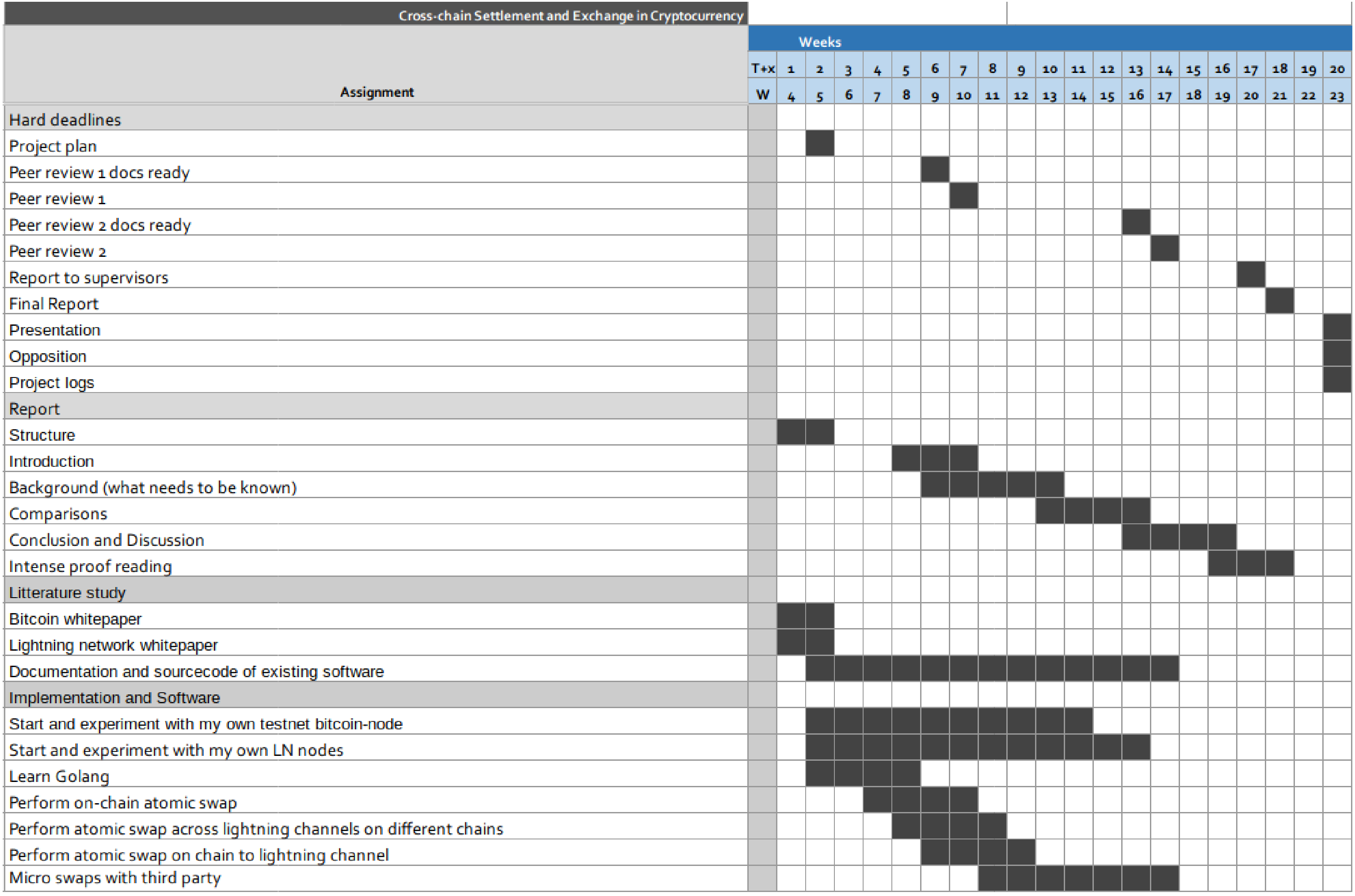
4 Documentation and communication

All the documentation and project diary will be collected into a single git-repo together with the thesis report.

Communication with supervisors will be split between Oskar and Jan-Erik. When talking with Oskar the discussion will be more about technical and implementation wise. While communication with Jan-Erik will be mostly related to the report and other deadlines in the course.

5 Timeplan

Below is a diagram that shows how I think I can best allocate my time. Note that this is only preliminary and the real schedule will probably not look like this:



Cross-chain Settlement and Exchange in Cryptocurrency																					
	Weeks																				
	T+x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Assignment	W	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Hard deadlines																					
Project plan			■																		
Peer review 1 docs ready							■														
Peer review 1								■													
Peer review 2 docs ready														■							
Peer review 2															■						
Report to supervisors																		■			
Final Report																			■		
Presentation																					■
Opposition																					■
Project logs																					■
Report																					
Structure		■	■																		
Introduction						■	■	■													
Background (what needs to be known)							■	■	■	■	■										
Comparisons											■	■	■	■							
Conclusion and Discussion														■	■	■	■				
Intense proof reading																	■	■	■		
Litterature study																					
Bitcoin whitepaper		■	■																		
Lightning network whitepaper		■	■																		
Documentation and sourcecode of existing software			■	■	■	■	■	■	■	■	■	■	■	■	■						
Implementation and Software																					
Start and experiment with my own testnet bitcoin-node			■	■	■	■	■	■	■	■	■	■									
Start and experiment with my own LN nodes			■	■	■	■	■	■	■	■	■	■	■	■							
Learn Golang			■	■	■	■															
Perform on-chain atomic swap					■	■	■	■													
Perform atomic swap across lightning channels on different chains						■	■	■	■												
Perform atomic swap on chain to lightning channel							■	■	■	■											
Micro swaps with third party									■	■	■	■	■	■	■						

References

[1] Andrea M. Antonopoulos. *Mastering Bitcoin: programming the open blockchain.* OReilly, 2 edition, 2017.

[2] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2009.

[3] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments, Jan 2016.