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

Maecenas consequat risus quis auctor tincidunt. Sed ornare magna eu bibendum pretium. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Aliquam erat volutpat. Interdum et malesuada fames ac ante ipsum primis in faucibus. Cras dictum felis nibh, sit amet lacinia nisi fermentum nec. Cras quis tortor interdum, aliquam nisi ac, efficitur ipsum. Nunc mollis varius neque, a elementum erat. Integer mauris ex, vehicula in feugiat eu, hendrerit suscipit odio. Etiam tincidunt lectus lorem, nec suscipit dui porttitor nec. Aenean pulvinar non justo id tincidunt.

3   Literature and references

Mauris ultricies pretium feugiat. Phasellus a placerat dolor, vel aliquam augue. Quisque blandit orci nec nisi posuere dictum. Nulla facilisi. Sed et maximus ante. Aliquam nec consequat arcu. Sed nec felis egestas, tincidunt odio vel, mattis nisl. Quisque a orci ut lectus scelerisque sodales ac ac libero. Praesent consectetur turpis vel posuere luctus. Sed suscipit sapien sed volutpat dapibus. Sed varius ultricies ante sed facilisis. Praesent purus mauris, finibus non turpis at, sodales sollicitudin lorem.

- one

- two

- three

4   Documentation and communication

Ut nec mauris orci. Maecenas libero lectus, malesuada dictum accumsan eget, hendrerit sit amet nibh. Praesent ut sodales magna. Praesent rhoncus quis turpis vitae dictum. Sed a tristique justo, vel lobortis enim. Nunc commodo dui vel consequat pellentesque. In ut venenatis felis. Etiam in dolor congue, tempor nisi id, dignissim nunc. Ut nulla orci, tempor a diam sed, ultricies facilisis est. Proin tempus ut risus vel blandit.

5   Timeplan

Praesent fermentum elit arcu, eget feugiat sapien fermentum nec. Suspendisse fringilla, ex vel molestie imperdiet, ipsum massa blandit velit, et iaculis libero urna quis diam. Aenean eleifend ullamcorper lacinia. Sed vel libero volutpat, laoreet lorem id, varius tellus. Nunc pellentesque enim at augue bibendum faucibus. Cras sit amet mauris eu tortor placerat blandit non sed ipsum. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Proin commodo finibus enim et vestibulum. Nulla vulputate posuere ante, vitae vulputate lacus convallis a.