UMEÅ UNIVERSITY
Department of Computing Science
Master thesis report

Master thesis presentation document
30HP, 5DV143, VT19

Evaluating Cross-chain Settlement and Exchange in Cryptocurrency

Chapter 1

Abstract

Chapter 2

Introduction & Background

Alright, so the thing that is on everybody's mind is probably: what is an atomic swap? An atomic swap is where two parties exchange assets atomically, which means that either the transaction takes place fully, or the state is reset to the pre- exchange state. This is made possible by clever use of cryptography and programmable contracts on the bitcoin network and blockchain.

So, most people, especially in computer science, have heard of Bitcoin, but I could almost count on one hand the number of people I have met that have more than a basic understanding of how it works. I could talk for hours about this subject, but sadly there is no time for that. So I will try to give you the shortest possible version where you can at least understand the rest of my thesis.

The simplest description of Bitcoin is a shared public ledger, that relies on proof-of-work to build network-wide consensus. First of proof-of-work is a way to prove mathematically that work was put into doing something. The most common way of doing this is via hashing of some datatype. The hash has to meet certain criteria to be accepted. There is no known way of producing a wanted hash, so the only way is to try different combinations until a good result is found. So if you have data that produces a certain hash that hash serves as proof that you put work into creating it.

Another thing you have probably heard about before is the blockchain, but just as with Bitcoin overall, people know little about what it actually is. A blockchain is basically a shared datatype. It is very reminiscent of a linked list, but allows for branching, meaning that two elements can link to the same parent. We will come back to this in a moment, but first, let's take a closer look at the blocks.

A block is a data structure that has a header and data. The header contains metadata about the block itself as well as a reference to the previous block in the chain. In Bitcoins case, the data in the block is just a list of transactions, but you could put anything you want into this field. The reference to the previous block is what forms the chain. You can from any block follow the references all the way back to the original block. Anyone can add a block to the chain. But it has to meet the proof-of-work criteria. The Bitcoin network independently calculates something called mining-difficulty. This is represented by a large 256-bit number. For your new block to be accepted the header of the block has to produce a hash that is strictly smaller than the difficulty number. You produce unique hashes by changing a field in the header called nonce, this process is what is referred to as mining.

The mining-difficulty is set so that the sum of all participant's hash-calculating power, or hashrate, will produce new block on average every 10 minutes. The difficulty is adjusted

every 2016th block.

So how does proof-of-work ensure that the shared ledger stays consistent? This is where concepts like longest chain comes in. The Bitcoin network only accepts the longest chain as truth, in other words the chain with most accumulated proof-of-work. This works as long as the majority of participants is honest. However due to the probabilistic manner of how new valid blocks are found there is still a chance for contention even if all participants are honest. For example what will the network do in the case where two different blocks