# Chapter 1

# Technical Background

This chapter provides the technical background to the various terms and concepts used in this thesis. If the reader is already familiar with anything explained in a section in relation to blockchain, skipping it should not hinder in further reading. If the reader is unfamiliar, or wishes to refresh his memory, reading this chapter is advised.

A bottom-up approach is used in this chapter, which means that sections may use or require terms and concepts explained in a previous section, or previous sections. Each section aims to give an intuitive understanding via an example and offers a detailed explanation. A visual representation of how the various sections are linked can be found in appendix A.

The chapter first leads up to explaining blockchain, followed by an introduction to signature schemes. To end the chapter, RandHound and finally OmniLedger are explained.

## 1.1 Concensus protocol

By definition consensus is an opinion that everyone in a group agrees with or accepts. An agreement, in other words. A protocol, in the technical definition, is an established method for connecting computers so that they can exchange information. A consensus protocol is therefore a method to reach agreement between connected computers.

In relation to blockchain technology, a consensus protocol[1] is a protocol used to reach agreement over input to add to the ledger, and the order in which it should be added. Blockchain technology recognises various such

protocols, operating in various ways under different assumptions and requirements.

Below brief explanations will be given of the consensus protocols used by Bitcoin and Stellar. The former uses a concept known as proof-of-work, the latter introduces a notion of trust.

### 1.1.1 Bitcoin

Conversely, the consensus protocol used by Bitcoin[3] does not require any trust in other participants. Instead it relies on a mechanism known as proof-of-work. In Bitcoin a reward goes to the participant that manages to create the next agreement. This agreement is a set of transactions, called a block, that fulfills the requirements set for the block. Once a participant has found such a block, he sends it to as many others as he can, so that his result will be on the chain, which makes the reward his. Other participant can easily verify that a block meets those requirements, after which they'll accept the result and forward it to others.

The protocol functions with the help of a one-way hash function. A one-way function is a function that makes it easy to compute f(x) given x, but makes calculating x from f(x) (near) impossible. A one-way hash function has the added property of producing output of a fixed length.

What happens in the protocol used by Bitcoin is that each participant will create a block. This block then serves as input for the one-way hash function. The goal is to have a block that results in a hash with a certain amount of leading zero's. Given the block, others can easily verify that hashing the block results in a hash with a sufficient amount of leading zero's.

Producing a wrong block, therefore, is not in the best interest of the participant. Others will quickly refure the block, and all the effort put into creating the block will be wasted.

Therefore the notion of proof-of-work for the Bitcoin consensus protocol is apt. Arriving at a sufficient result requires the participant to try various input blocks, with no way to compute one from the desired result.

### 1.1.2 Stellar

To understand the Stellar Consensus Protocol[2] (SCP) some definitions are needed. SCP introduces a quorum, a set of participants that is sufficient to

reach agreement, and a quorum slice, a subset of a quorum that can convince one participant of the agreement.

The basis of SCP is that participant trust others in their quorum slice to behave honestly, hence the notion of trust in SCP. Assuming all participant behave honestly and under the same set of input and rules, each participant should arrive at the same conclusion. After a participant reaches his conclusion, he publishes it to the others in his quorum slice. In publishing his conclusion he votes for it, as do all others in his slice. The final conclusion is the one most voted for.

As long as there are sufficient reputable participants, the network can never be corrupted. Behaving dishonestly is further disincentivised by the protocol, since those participants are not trusted to be part of a quorum slice, and the influence of their opinion will then quickly be reduced. Conversely, reputable participants will be part of multiple quorum slices, which gives them a large influence over the decisions made.

To ensure that the whole network is indeed connected and reaches network wide consensus, SCP requires that there are no disjunct quorums. Since disjunct quorum can reach their opinion separate from the network, a different agreement undermines the network wide consensus. Participants wishing to join the network have to make sure that they join a quorum in such a way that no disjunct quorums are created.