Chapter 1

Introduction

This thesis has been inspired by a recent paper that introduced OmniLedger[1]: a scalable, decentralized ledger. In a world where more and more uses are found for blockchain technology, the promise of such a technology that scales in performance with the amount of users is incredibly interesting. Considering that current systems might actually perform worse when the amount of users increases, it is interesting to look at OmniLedger to see whether it can help in that regard.

In particular, this thesis focusses on multi-signature algorithms that may be used to improve the performance of RandHound[2]. RandHound is used by OmniLedger to ensure that the system remains uncompromised. Since evaluation has shown that RandHound takes up more than 70% of the total runtime in the bootstrap process of OmniLedger, which happens periodically, improving the performance of RandHound should lead to an improvement in performance of OmniLedger.

Therefore the research question of this thesis is as follows: " .. ". To answer this question, some background is needed, before comparisons can be made between various multi-signature algorithms.

As such the second chapter introduces algebraic varieties, leading up to an explanation of elliptic curves and some properties that are used to great effect in cryptography. The chapter concludes with an explanation of the Weil pairing on elliptic curves, which is used in one of the multi-signature algorithms used.

The third chapter then introduces the technological background of ledgers, blockchain and multi-signatures among other terms and concepts used to

clearly show the context of the research.

In chapter four and five two different multi-signature algorithms are studied, leading up to the comparison of them in chapter six and the conclusion as to the most suitable choice for RandHound.