Task Description - Advancing Cryptocurrencies and Blockchain Technology

Master Thesis - Conrad Burchert

September 27, 2016

1 Introduction

Electronic cash, cryptocurrencies and Blockchain technology are gaining a large amount of support in today's financial industry. A vast number of different systems is in use, however all of them have major drawbacks.

Classical electronic cash systems require trust in banks and have slow transaction speed. Blockchain based approaches suffer from bad scalability, as all transactions, which have ever been done, need to be stored on all nodes of the network. The time needed to generate new blocks also makes it unsuitable for instant transfer of funds at checkouts, without a trusted party taking the risk of a failed transaction.

Further problems include fraudulent transactions such as those leading to the bankruptcy of the Mt. Gox cryptocurrency exchange platform or the hardfork of the Ethereum Blockchain. A system to refund this kind of transactions is needed to allow long term stability.

2 Aim of the project

The aim of this project is to improve on existing currency systems or develop a new currency system with improved properties such as:

- Scalability
- Transaction speed
- Number of trusted parties
- Controllability of the amount of currency generated
- Feasability of offline transactions
- Possibility to refund fraudulent transactions
- Anonymity

3 Outline

Milestones of the project include:

1. Assess the current state of research, including:
   - Electronic cash infrastructure
   - Variants of blockchain technology
   - Possibly other systems without blockchains
2. Propose a new or improved system
3. Assess the advantages and disadvantages in comparison to the existing systems

4 Organization

Duration: 6 month
Supervisor: Prof. Roger Wattenhofer, wattenhofer@ethz.ch