CloudCoin
A decentralized service negotiation, payment, and rating platform based on distributed consensus, distributed hash tables, and distributed trust

Author:
Tobias BOEHM

Primary Supervisor:
Prof. Dr. Debora WEBER-WULFF

Secondary Supervisor:
Prof. Dr.-Ing. Kai Uwe BARTHHEL

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in
Internationale Medieninformatik
Fachbereich 4 - Informatik. Kommunikation und Wirtschaft

March 10, 2015
Contents

Declaration of Authorship i

Abstract ii

Acknowledgements iii

Contents iv

List of Figures vii

List of Tables viii

Abbreviations ix

1 Introduction 1
   1.1 Preface 1
   1.2 General Political Situation of Cyberspace 2
   1.3 Introduction to CloudCoin 2
   1.4 The Structure of this Thesis 3

2 CloudCoin Objective 4
   2.1 CloudCoin - a Decentralized Marketplace 4
      2.1.1 Services 5
      2.1.2 Decentralized Identity and Authentication 5
      2.1.3 Decentralized Service Provider Reference 7
      2.1.4 Contracts 7
      2.1.5 Payments via it's Own Cryptocurrency 8
      2.1.6 Decentralized Ratings and Trust 9
      2.1.7 Decentralized ServiceStore 10
      2.1.8 Distribution of CloudCoin Updates 11
   2.2 Competitors 11
      2.2.1 Storj 11
      2.2.2 OpenBazaar 12

3 Technical Concept of Bitcoin 13
   3.1 Introduction 13
   3.2 Bitcoin Address 14
3.3 Coins and Transactions 14
  3.3.1 Transaction Output 15
  3.3.2 Transaction Input 16
  3.3.3 Coinbase Transaction 16
  3.3.4 Bitcoin Script 17
3.4 Blocks 17
3.5 Mining and Proof-of-Work 19
3.6 Weaknesses of Bitcoin's PoW 20
3.7 Block Chain 20
3.8 Impede Double-Spending 21
3.9 Other Notable Block Chain Related Projects 22
  3.9.1 Naniecoin - A Decentralized Key/Value Store 22
  3.9.2 Peercoin - The First Implementation of Proof-Of-Stake 23
  3.9.3 Counterparty - Piggybacking the Bitcoin Protocol 24

4 Technical Concept of CloudCoin 26
4.1 Introduction 26
4.2 CloudCoin's Decentralized Infrastructure 26
  4.2.1 Kadenilia based DHT 27
  4.2.2 File Distribution via BitTorrent 30
  4.2.3 CloudCoin Blockchain 30
4.3 CloudCoin ServiceNetwork 32
  4.3.1 Securing ServiceNetwork Storage Areas 33
  4.3.2 Extended Contact Information 35
  4.3.3 Service Announcements 36
  4.3.4 Detailed Service Descriptions 37
  4.3.5 Service Offer Announcements 38
4.4 Trust Management in CloudCoin 38
  4.4.1 Member Roles and Potential Malicious Actions 39
  4.4.2 PACE - A Trust-Incorporating Application Framework 44
  4.4.3 4C - A Reputation-Based Trust Model Framework 48
  4.4.4 EigenTrust - A Trust Computation Algorithm 52
4.5 CloudCoin Currency Generation and Distribution 57
  4.5.1 Formal Characteristics of CloudCoin currency 57
  4.5.2 Currency Initialization Phase 58
  4.5.3 Dynamically Generated Hash Chains for PoW ASIC Hardening 58
4.6 CloudCoin Contract Negotiation Guideline 60
4.7 Raising the Anonymity Level 61
  4.7.1 Cash Flow Obfuscation via ZeroCash 61
  4.7.2 Anonvinizing Network Communication via TOR 63
4.8 Language-independent Communication via Protocol Buffers 65
4.9 Decoupling Software Components using OSGi 65

5 CloudCoin Implementation 67
5.1 Introduction 67
5.2 Choosing a Foundation 67
  5.2.1 Bitcoin Core 68