Smart Contracts for Blockchain-based Reputation Systems

by Ahmed Saud Almasoud

Thesis submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy

under the supervision of Associate Professor Farookh Hussain

University of Technology Sydney
Faculty of Engineering and Information Technology

May 2020

Certificate of Authorship / Originality

I certify that the work in this thesis has not previously been submitted for a degree nor has it been submitted as part of requirements for a degree except as fully acknowledged within the text.

I also certify that the thesis has been written by me. Any help that I have received in my research work and the preparation of the thesis itself has been acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This research is supported by the Australian Government Research Training Program.

Production Note:
Signature removed prior to publication.
....
Signature of Candidate

12 May 2020
Date

Acknowledgement

I start by thanking Allah, lord of the world, for he has given me all the possibilities, blessings, and exceptional experience. He has given me ways to reach what I have reached so far. When a dream comes true, you should look a little backward to thank those who have had a major role in this success. Success cannot be achieved without the joint effort of different parties.

I thank the owner of the noble and essential role in this success, Professor Farookh Hussain, who tolerated my mistakes and was not only a supervisor of my thesis, but also the older brother, the supreme leader and the glorious professor; as he never hesitated to give me or extend a helping hand when I needed it. Honestly, without him being by my side, I could not pass this stage of my life. I owe him for all this success.

I would also like to thank the University of Technology Sydney (UTS) for giving me this opportunity to study in it. It was like my second home.

I would like to thank my parents, my wife, and my colleagues; without their support, this work could not have been completed.

LIST OF PUBLICATIONS

Journal publication

1- Almasoud. A. S., Hussain, F. K., and Hussain, O. K., ‘Smart Contracts for Blockchain-based Reputation Systems: A Systematic Literature Review’ 2019, *Journal of Network and Computer Applications (JNCA).* **(ERA, CORE – Q1 Journal).**

Conference publication

1- A. S. Almasoud, M. M. Eljazzar and F. Hussain, "Toward a Self-Learned Smart Contracts," *2018 IEEE 15th International Conference on e-Business Engineering (ICEBE)*, Xi'an, 2018, pp. 269-273. **(ERA, COREB*-Rank).**

بسم الله الرحمن الرحيم
١٤٢٠ م

Table of Contents

Certificate of Authorship / Originality……………………………………………..….…..... i

Acknowledgement…………………………...……………………………………… ii

List of Publications……………………………………………………………………… iii

List of Figures……………...…………………..………………………………………… x

List of Tables………………………………………………………………………… xiii

Abstract……………………………………………………………………………….. xiv

Chapter 1 : Introduction.. 1

1.1 Introduction 1

1.2 Statement of the Problem 2

1.3 Blockchain Technology.. 3

1.3.1 Blockchain Structure 3

1.3.2 Blocks... 4

1.3.3 Block Time.. 4

1.4 Smart Contracts 4

1.5 The relationship between Smart Contracts and Blockchain.................................. 5

1.6 Purpose of Using Smart Contracts in Blockchain Technology.............................. 6

1.7 Peer-to-Peer Networks 8

1.7.1 P2P Network Topology... 9

1.8 Reputation Systems 9

1.9 Challenges Faced by the current Generation of Reputation System 10

1.10 Research Contribution 12

1.10.1 Scientific Contribution... 12

1.10.2 Social Contribution 12

1.11 Thesis Plan.. 13

1.12 Conclusion 16

Chapter 2 A Systematic Literature Review 17

2.1 Introduction 17

2.2 Key requirements from a Smart Contract.. 19

2.2.1 Ability to derive overall reputation value of service providers based on the values (or ratings) present in the smart contracts (Req: 1).. 20

2.2.2 Ability to determine the trust value of a service provider in a context (Req: 2)…………………………………………………………………………………...21
2.2.3 Reputation system as a digital asset and moving across platforms (Req: 3) . 21
2.2.4 Detection of non-compliant behavior (Req: 4) 22
2.2.5 Mathematical models and algorithms (Req: 5) 22
2.3 Process adopted for shortlisting the papers for SLR 23
2.3.1 Step 1: Criteria for searching the literature 23
2.3.2 Step 2: Inclusion and Exclusion Criteria... 25
2.3.3 Step 3: Quality Evaluation 27
2.3.4 Step 4: Shortlisted papers for SLR and categorizing them into broad areas.. 28
2.4 Summary of papers shortlisted in the SLR.. 28
2.4.1 Trust and reputation systems... 28
2.4.3 Blockchain-based Reputation Systems 36
2.4.4 Smart Contracts for Reputation Systems 41
2.4.5 Research gaps in the existing studies from the requirement perspective of a smart contract 50
2.5 Smart contracts-based reputation system service framework 52
2.5.1 Modelling and deducing the overall reputation value of service providers (Req: 1).. 55
2.5.2 Modelling and deducing the trust value of service providers within a context (Req: 2).. 55
2.5.3 Transferring reputation among service providers and across platforms (Req: 3)…………………………………………………………………………………...56
2.5.4 Detection of non-compliant behavior and manipulation of reputation ratings (Req: 4).. 57
2.5.5 Mathematical models and algorithms for reputation computation post-reputation trading (Req: 5) 57
2.6 Conclusion 57
Chapter 3 : Research Questions and Objectives 59
3.1 Introduction 59
3.2 Gaps in the Literature 59
3.3 Key Definitions 59
3.4 Research Questions 61
3.5 Research Objectives 62

3.6 Conclusion 63

Chapter 4 : Research Methodology and Solution Overview 64

4.1 Introduction 64

4.2 Keys Definitions 64

4.3 Selected Research Methodology 65

4.4 Solution Overview 66

4.4.1 Architecture of the FarMed 67

4.5 Overview of solution for RQ2 70

4.6 Overview of solution for RQ3 71

4.7 Overview of solution for RQ4 72

4.8 Overview of solution for RQ5 74

4.8.1 Testing and Verification of the Solution 74

4.9 Conclusion 74

Chapter 5 : Smart Contract-Based Reputation Framework and Determination of the Current Reputation of Service Providers 75

5.1 Introduction 75

5.2 Phases in the Smart-Contracts based Reputation Framework 76

5.2.1 Working of the Marketplace Phase 76

5.2.2 Smart Contract Execution Phase 78

5.2.3 Blockchain-Based Trust Values and Computations Phase 79

5.3 Modelling and Determination of the Current Reputation Values of Service Providers 82

5.3.1 Workflow for Solution 82

5.3.2 Computing the updated Trust Value of a Service Provider 84

5.4 Prototype Implantation 86

5.4.1 Aims of Engineering the Prototype System 86

5.5 Datasets Used for Validation 86

5.6 Steps in the working of the prototype system for reputation computation 88

5.6.1 Steps in local reputation computation 89

5.6.2 Steps in Blockchain-based reputation computation 90

5.7 Prototype Evaluation and Discussion 92

5.8 Conclusion 94

Chapter 6 : Context-driven inferencing of Trust Value for Service Providers 95

6.1 Introduction 95
6.2 Service Ontology 95
6.2.1 Service Metadata 96
6.2.2 Transport Service Ontology 97
6.2.3 Service Knowledge Base 99
6.3 Algorithm for Semantic Distance Computation 100
6.3.1 AKTIVERANK 100
6.3.2 Algorithm for Context-Based Inference 106
6.4 Validation 107
6.5 Conclusion 111
Chapter 7 : RAS for Transferring of Reputation among Service Providers 112
7.1 Introduction 112
7.2 Reputation Auction Service 112
7.3 Algorithm for Reputation Computation 113
7.3.1 Submission of New Reputation Request 115
7.3.2 Dividing and Storing the Score Installments in Smart Contracts 117
7.4 Testing and Validation of the Solution 121
7.4.1 Steps in the prototype system 121
7.5 Evaluation Results and Discussion 125
7.6 Conclusion 128
Chapter 8 : Prototype Working and Demonstration 129
8.1 Introduction 129
8.2 Prototype Setup 129
8.2.1 Description of the Local machine Setup 130
8.2.2 Description of the Blockchain Setup 134
8.3 Prototype Working for Reputation Computation 146
8.4 Prototype Working for Reputation Transfer 152
8.5 Conclusion 156
Chapter 9 : Conclusion and Future Work 157
9.1 Introduction 157
9.2 Problems Addressed in this Thesis 157
9.3 Contributions to the Existing Literature 158

9.3.1 Systematic Literature Review 158

9.3.2 Creation of a Novel Solution: The FarMed Framework 158

9.3.3 Evaluation, Validation, and Implementation of the proposed solutions 160

9.4 Future Work 160

References 162

List of Figures

Figure 1. 1. Relationship between smart contract and blockchain technology 6

Figure 1. 2. The thesis structure 15

Figure 2.1. Relationship between Smart Contract and Blockchain Technology 19

Figure 2.2. The three phases of a smart contract.. 20

Figure 2.3. The study selection process 27

Figure 2.4: Details of the FarMed Service. 52

Figure 2.5. Sequence of FarMed framework's working 54

Figure 2.6. Sequence of working of the Smart contract execution phase of FarMed framework…………………………………………………………………………………55

Figure 2.7. Example of reputation scores before and after the auction............................... 56

Figure 4.1. Design science research approach (Ken et. al., 2009) 65

Figure 4.2. Architecture of FarMed Service 67

Figure 4.3. Overview of the Smart contract-based reputation system service framework .. 69

Figure 4.4. Intelligent Method for Reputation Computation 70

Figure 4.5. Intelligent Method for Context-driven inferencing of trust value 72

Figure 4.6. Intelligent Method for service provider reputation transfer on auction............ 73

Figure 5.1. Smart Contract-based Reputation Framework.. 77

Figure 5.2. Smart Contract Execution Logic for Reputation Systems 79

Figure 5.3. Trust Values and Computations Phase 81

Figure 5.4. Intelligent Method for Reputation Computation 83

Figure 5.5. Overview of steps in Computing Trust Values of Service Provider 85

Figure 5.6. Flow chart of local marketplace reputation computation process 89

Figure 5.7. Flow chart of Blockchain reputation computation process 91

Figure 5.8. Latency experienced by *FarMed* 94

Figure 6.1. Transport service metadata format (Dong *et al.,* 2008b)................................. 97

Figure 6.2. The structure of the service ontology 98

Figure 6.3 The transport service ontology (sourced from Dong et al (2008b)) 99

Figure 6.4. Service Knowledge base (sourced from Dong et al (2008b))......................... 100

Figure 6.5. AKTiveRank Architecture (Alani and Brewster, 2006) 101

Figure 6.6. Overview of steps in computing the trust value of a service provider in a given context………………………………………………………………………………109

Figure 6.7. Screenshot of the listed products before rating 109

Figure 6.8. Screenshot of the listed products after rating *iPhone X* product 110

Figure 6.9. Screenshot of the listed products after rating *iPhone 11* product 110

Figure 6.10. Screenshot of the listed products after inferring the reputation score for *iPhone 12* product………………………………………………………………………110

Figure 7.1. Example of reputation scores before and after the auction 113

Figure 7.2. Overview of Reputation Auction Service 114

Figure 7.3. Overview of the submission process for submitting new lending request 116

Figure 7.4. Verification of Payback Score and Score Instalments 118

Figure 7.5. Execution of due installments 120

Figure 7.6. Flow chart of reputation trading process in local marketplace 122

Figure 7.7. Flow chart of reputation trading process in blockchain 124

Figure 7.8. Results obtained from implementing the Reputation Auction Service 125

Figure 7.9. Latency for the Reputation Auction Service 127

Figure 7.10 (See description below) 127

Figure 7.11. (See description below) 127

Figures 7.10 and Figure 7.11 are showing the dashboard of Reputation Auction Service 127

Figure 8.1. XAMPP Control Panel interface 130

Figure 8.2. Apache and MySQL services activated 130

Figure 8.3. Machine is running localhost successfully 131

Figure 8.4. phpMyAdmin interface 131

Figure 8.5. Review table in database 132

Figure 8.6. Product_for_sale table in database 132

Figure 8.7. Marketplace files 133

Figure 8.8. Remix – Ethereum IDE in browser interface 134

Figure 8.9. Remix IDE compiler 135

Figure 8.10. Etherscan - EVM public web interface - Etherscan 135

Figure 8.11. MetaMask plugin installation 136

Figure 8.12. Linking Ethereum account with Ropsten Test Network connection 137

Figure 8.13: Index file in editor 138

Figure 8.14. The simulated marketplace interface 139

Figure 8.15. Adding new service provider 140

Figure 8.16. New service provider account created 141
Figure 8.17. Ether deposit option 142
Figure 8.18. MetaMask Ether Faucet 143
Figure 8.19 Ether request confirmation 144
Figure 8.20. Ether is deposited 145
Figure 8.21. Service provider's product listed in prototype 146
Figure 8.22. Confirmation Process 147
Figure 8.23. Contract Interaction pending 148
Figure 8.24. Review the order 149
Figure 8.25. Place a review 150
Figure 8.26. HP-5520 product rating 151
Figure 8.27. New values in marketplace 151
Figure 8.28. Changing the user account from MetaMask 152
Figure 8.29. Request rating interface 153
Figure 8.30. Pending waiting for approval 153
Figure 8.31. Request was approved by lender 154
Figure 8.32. Request was approved by borrower 154
Figure 8.33. New reputation score after trading for lender 154
Figure 8.34. New reputation score after trading for borrower 155
Figure 8.35. Instalments to be made 155
Figure 8.36. After first payback instalment – Borrower 155
Figure 8.37. After first payback instalment – Lender 156

List of Tables

Table 2.1. Journals and Conference Proceedings.. 24

Table 2.2. Summary of stages of evaluating and selecting relevant papers for SLR........... 26

Table 2.3. Listing of papers identified after the shortlisting in the SLR process................. 32

Table 2.4. Descriptions, issues and limitations of existing studies on trust and reputation systems………………………………………………………………………………..34

Table 2.5. Descriptions and limitations of studies on blockchain-based reputation systems………………………………………………………………………………..38

Table 2.6. Descriptions, issues and limitations of existing studies on smart contracts 44

Table 5.1 (See description below)... 87

Table 5.2 (See description below)... 88

Tables 5.1 and 5.2 are showing the dataset used for the implementation of the solutions. . 88

Table 5.3 (See description below)... 92

Tables 5.3 and Table 5.4 showing results obtained from using our Blockchain-based platform for Reputation Computation.. 92

Table 5.4 (See description below)... 92

Table 5.5. Latency values in seconds.. 93

Table 8.1: Local database connection variables.. 138

Table 8.2: Products details inserted in prototype... 146

Abstract

Smart contracts are computer protocols that are meant to oversee, enforce, or verify performances or negotiations of contracts. These protocols ensure that no third parties are involved as a part of the transaction and ensure the security and credibility of the contracts. Reputation systems have been widely implemented in e-commerce applications and websites. Reputation systems provide a platform through which users can measure the trustworthiness or reliability of people offering online services or products. Previous researchers have already proposed the use of Blockchain technology for Reputation Systems.

A Blockchain is generally built on a peer-to-peer (P2P) network and adheres to a certain protocol for the communication amongst the blocks and for the validation of new blocks. However, through a systematic literature review, we have identified that the existing literature has not proposed the use of smart contracts for blockchain-based reputation systems. Using smart contracts in reputation systems can play a vital role by adding an additional layer of openness and security.

The contracts are secured using hash signature, which makes the smart contract "immutable" to alteration. The decentralized application (Dapp) used in the system offers large file storage, protection of the user personal data, low costs of transactions as well as easy bug fixing. Smart contracts can be used to implement the proof of reputation (POR) consensus algorithm which aims at providing quantification for the various systems that are built using the blockchain technology.

POR aims at using the reputation of the participants in the system to secure the network. In the event that a participant attempts to cheat on the smart contracts, they stand to face serious consequences both financially as well as brand wise. The consensus ensures that reputation is paramount in the blockchain system. The primary objective of this study is to propose and develop an intelligent framework termed (FarMed) that is centered on smart contracts-based reputation system.

The intelligence built into Farmed provides automated and reliable mechanisms for the following: (i) determining the current reputation value of a service provider; (ii) intelligent mechanisms for trust-based inferencing in different contexts; (iii) intelligently preventing people from manipulating reviews in the reputation system; and (iv) providing a platform for transferring the reputation value of a service provider to other service providers. Finally, in order to validate the performance and accuracy of the proposed framework in this thesis, software prototyping will be chosen as the model of choice.