



شبكة المعلومات الجامعية  
التوثيق الإلكتروني والميكرو فيلم

# بسم الله الرحمن الرحيم



**MONA MAGHRABY**



شبكة المعلومات الجامعية  
التوثيق الإلكتروني والميكروفيلم



# شبكة المعلومات الجامعية التوثيق الإلكتروني والميكروفيلم



**MONA MAGHRABY**



شبكة المعلومات الجامعية  
التوثيق الإلكتروني والميكروفيلم

# جامعة عين شمس

## التوثيق الإلكتروني والميكروفيلم

### قسم

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها  
علي هذه الأقراص المدمجة قد أعدت دون أية تغيرات



### يجب أن

تحفظ هذه الأقراص المدمجة بعيدا عن الغبار



**MONA MAGHRABY**



# USING TRUSTED CLOUD COMPUTING TO PROVIDE TRUST INTO MULTI-BLOCKCHAIN ECOSYSTEMS

By

**Fady AbdelMoneim Mohamed Ibrahim**

A Thesis Submitted to the  
Faculty of Engineering at Cairo University  
in Partial Fulfillment of the  
Requirements for the Degree of  
**DOCTOR OF PHILOSOPHY**  
in  
**Computer Engineering**

FACULTY OF ENGINEERING, CAIRO UNIVERSITY  
GIZA, EGYPT  
2021

# **USING TRUSTED CLOUD COMPUTING TO PROVIDE TRUST INTO MULTI-BLOCKCHAIN ECOSYSTEMS**

By

**Fady AbdelMoneim Mohamed Ibrahim**

A Thesis Submitted to the  
Faculty of Engineering at Cairo University  
in Partial Fulfillment of the  
Requirements for the Degree of  
**DOCTOR OF PHILOSOPHY**  
in  
**Computer Engineering**

Under the Supervision of

**Prof. Dr. Amr Wassal      Prof. Dr. Elsayed Hemayed**

Computer Engineering Department  
Faculty of Engineering, Cairo University

Computer Engineering Department  
Faculty of Engineering, Cairo University

**FACULTY OF ENGINEERING, CAIRO UNIVERSITY  
GIZA, EGYPT  
2021**

# USING TRUSTED CLOUD COMPUTING TO PROVIDE TRUST INTO MULTI-BLOCKCHAIN ECOSYSTEMS

By

**Fady AbdelMoneim Mohamed Ibrahim**

A Thesis Submitted to the  
Faculty of Engineering at Cairo University  
in Partial Fulfillment of the  
Requirements for the Degree of  
**DOCTOR OF PHILOSOPHY**  
in  
**Computer Engineering**

Approved by the Examining Committee:

---

|                              |                     |
|------------------------------|---------------------|
| <b>Prof. Dr. Amr Wassal,</b> | Thesis Main Advisor |
|------------------------------|---------------------|

---

|                                   |         |
|-----------------------------------|---------|
| <b>Prof. Dr. Elsayed Hemayed,</b> | Advisor |
|-----------------------------------|---------|

---

|                               |                   |
|-------------------------------|-------------------|
| <b>Prof. Dr. Hoda Baraka,</b> | Internal Examiner |
|-------------------------------|-------------------|

---

|                                                                  |                   |
|------------------------------------------------------------------|-------------------|
| <b>Prof. Dr. Salwa Nassar,</b><br>Electronics Research Institute | External Examiner |
|------------------------------------------------------------------|-------------------|

FACULTY OF ENGINEERING, CAIRO UNIVERSITY  
GIZA, EGYPT  
2021

**Engineer's Name:** Fady AbdelMoneim Mohamed Ibrahim  
**Date of Birth:** 15/01/1984  
**Nationality:** Egyptian  
**E-mail:** fady4comp@gmail.com  
**Phone:** 0122 11 95 631  
**Address:** Remaya Officers City, El-Haram, Giza  
**Registration Date:** 01/03/2014  
**Awarding Date:** --/~/2021  
**Degree:** Doctor of Philosophy  
**Department:** Computer Engineering



**Supervisors:**

**Prof. Dr. Amr Wassal**  
**Prof. Dr. Elsayed Hemayed**

**Examiners:**

|                                  |                       |
|----------------------------------|-----------------------|
| <b>Prof. Dr. Amr Wassal</b>      | (Thesis Main Advisor) |
| <b>Prof. Dr. Elsayed Hemayed</b> | (Advisor)             |
| <b>Prof. Dr. Hoda Baraka</b>     | (Internal Examiner)   |
| <b>Prof. Dr. Salwa Nassar</b>    | (External Examiner)   |
| Electronics Research Institute   |                       |

**Title of Thesis:**

**Using Trusted Cloud Computing to Provide Trust into  
Multi-blockchain Ecosystems**

**Key Words:**

Blockchain; Off-chain; Trusted Computing; Cloud Computing

**Summary:**

We developed a framework, called Trusted Blockchain-Oracle Request Framework (T-BORF), to show how can we use trusted cloud computing to attest to an oracle and provide this remote attestation to a blockchain. We offered a trusted way for off-chains communications. For example, using our framework with Hyperledger Fabric, any organization participating in a business network (that plays the role of an oracle) proves the trust state of all the virtual machines where the containers of the peers exist.



# Disclaimer

I hereby declare that this thesis is my own original work and that no part of it has been submitted for a degree qualification at any other university or institute.

I further declare that I have appropriately acknowledged all sources used and have cited them in the references section.

Name: Fady AbdelMoneim Mohamed Ibrahim

Date:

Signature:



# Dedication

I want to dedicate this thesis to my lovely family for all of their support.

# Acknowledgements

I want to acknowledge my supervisors Dr Elsayed Hemayed and Dr Amr Wassal, for their efforts throughout my thesis with their patience and knowledge. One could not wish for better or kinder supervisors.

# Table of Contents

|                                                                 |              |
|-----------------------------------------------------------------|--------------|
| <b>Disclaimer</b>                                               | <b>i</b>     |
| <b>Dedication</b>                                               | <b>ii</b>    |
| <b>Acknowledgements</b>                                         | <b>iii</b>   |
| <b>Table of Contents</b>                                        | <b>iv</b>    |
| <b>List of Commands</b>                                         | <b>ix</b>    |
| <b>List of Tables</b>                                           | <b>x</b>     |
| <b>List of Figures</b>                                          | <b>xi</b>    |
| <b>List of Abbreviations</b>                                    | <b>xiii</b>  |
| <b>List of Publications</b>                                     | <b>xviii</b> |
| <b>Abstract</b>                                                 | <b>xix</b>   |
| <b>1 INTRODUCTION</b>                                           | <b>xx</b>    |
| 1.1 Problem Statement . . . . .                                 | 1            |
| 1.2 Motivation . . . . .                                        | 1            |
| 1.3 Thesis Proposal . . . . .                                   | 2            |
| 1.4 Contribution . . . . .                                      | 2            |
| 1.5 Thesis Outline . . . . .                                    | 3            |
| <b>2 BACKGROUND</b>                                             | <b>4</b>     |
| 2.1 Blockchain . . . . .                                        | 5            |
| 2.1.1 Blockchain History . . . . .                              | 5            |
| 2.1.1.1 Bitcoin History (First Generation) . . . . .            | 5            |
| 2.1.1.2 Ethereum History (Second Generation) . . . . .          | 6            |
| 2.1.1.3 Hyperledger Fabric History (Third Generation) . . . . . | 7            |
| 2.1.1.4 Blockchain Comparison . . . . .                         | 7            |

|         |                                                       |    |
|---------|-------------------------------------------------------|----|
| 2.1.2   | Definitions . . . . .                                 | 7  |
| 2.1.2.1 | Ledger . . . . .                                      | 8  |
| 2.1.2.2 | Smart Contracts . . . . .                             | 8  |
| 2.1.2.3 | Decentralized Application (DApp) . . . . .            | 8  |
| 2.1.3   | Public Blockchain Components . . . . .                | 9  |
| 2.1.4   | Business Network . . . . .                            | 9  |
| 2.1.5   | Hyperledger Fabric Network Components . . . . .       | 10 |
| 2.1.5.1 | Client Node (Client App) . . . . .                    | 10 |
| 2.1.5.2 | Peer Node . . . . .                                   | 11 |
| 2.1.5.3 | Orderer Node . . . . .                                | 11 |
| 2.1.5.4 | Other components . . . . .                            | 11 |
| 2.1.6   | Hyperledger Fabric Consensus . . . . .                | 11 |
| 2.1.6.1 | Step 1 - Proposing a Transaction . . . . .            | 12 |
| 2.1.6.2 | Step 2 - Executing the Transaction Proposal . . . . . | 12 |
| 2.1.6.3 | Step 3 - Proposal Response . . . . .                  | 14 |
| 2.1.6.4 | Step 4 - Order Transaction . . . . .                  | 14 |
| 2.1.6.5 | Step 5 - Delivering the Transaction . . . . .         | 14 |
| 2.1.6.6 | Step 6 - Validating the Transaction . . . . .         | 16 |
| 2.1.6.7 | Step 7 - Notification about the Transaction . . . . . | 16 |
| 2.1.7   | Hyperledger Fabric Potential Risks . . . . .          | 16 |
| 2.2     | Trusted Computing (TC) . . . . .                      | 17 |
| 2.2.1   | TC Definition and TCG . . . . .                       | 18 |
| 2.2.2   | Trusted Platform Module (TPM) . . . . .               | 18 |
| 2.2.3   | Platform Configuration Registers (PCRs) . . . . .     | 19 |
| 2.2.4   | TPM Keys . . . . .                                    | 19 |
| 2.2.4.1 | Endorsement Key (EK) . . . . .                        | 19 |
| 2.2.4.2 | Storage Root Key (SRK) . . . . .                      | 20 |
| 2.2.4.3 | Attestation Identity Key (AIK) . . . . .              | 20 |
| 2.2.4.4 | Other Keys . . . . .                                  | 21 |
| 2.2.4.5 | Creating and Using TPM Keys . . . . .                 | 21 |
| 2.2.5   | Roots of Trust (RoTs) . . . . .                       | 21 |
| 2.2.5.1 | Root of Trust for Measurement (RTM) . . . . .         | 21 |

|          |                                                           |           |
|----------|-----------------------------------------------------------|-----------|
| 2.2.5.2  | Root of Trust for Reporting (RTR) . . . . .               | 23        |
| 2.2.5.3  | Root of Trust for Storage (RTS) . . . . .                 | 23        |
| 2.2.6    | Remote Attestation . . . . .                              | 23        |
| 2.2.6.1  | Attestation to the Platform (Certify AIK) . . . . .       | 23        |
| 2.2.6.2  | Attestation of the Platform (Quote Operation) . . . . .   | 23        |
| 2.2.6.3  | Attestation by the TPM (Certify Other TPM Keys) . . . . . | 24        |
| 2.2.7    | Other TC Key Concepts . . . . .                           | 24        |
| 2.2.7.1  | Sealed storage . . . . .                                  | 24        |
| 2.2.7.2  | Memory curtaining . . . . .                               | 25        |
| 2.3      | Trusted Cloud Computing (TCC) . . . . .                   | 25        |
| 2.3.1    | Virtualization . . . . .                                  | 25        |
| 2.3.2    | Cloud Computing . . . . .                                 | 26        |
| 2.3.3    | Integrating TC with Cloud Computing . . . . .             | 26        |
| <b>3</b> | <b>RELATED WORK</b>                                       | <b>27</b> |
| 3.1      | Inter-blockchain Communication . . . . .                  | 27        |
| 3.1.1    | Atomic Cross-chain Transactions . . . . .                 | 27        |
| 3.1.2    | Cross-network Transactions . . . . .                      | 28        |
| 3.1.3    | Sidechains . . . . .                                      | 28        |
| 3.1.4    | Ledger-of-ledgers . . . . .                               | 28        |
| 3.1.5    | Inter-blockchain Comparison . . . . .                     | 29        |
| 3.2      | vTPM . . . . .                                            | 29        |
| 3.2.1    | Software-based vTPM . . . . .                             | 29        |
| 3.2.2    | Software-based vTPM with vTPM_Creator . . . . .           | 30        |
| 3.2.3    | Hardware-based vTPM . . . . .                             | 31        |
| 3.2.4    | Paravirtualization-based vTPM . . . . .                   | 31        |
| 3.2.5    | KVM-based vTPM . . . . .                                  | 32        |
| 3.2.6    | vTPM Comparison . . . . .                                 | 32        |
| 3.3      | Remote Attestation . . . . .                              | 33        |
| 3.3.1    | Terra . . . . .                                           | 33        |
| 3.3.1.1  | Original Terra . . . . .                                  | 33        |
| 3.3.1.2  | Step after Terra . . . . .                                | 34        |
| 3.3.2    | Integrity Measurement Architecture (IMA) . . . . .        | 34        |

|          |                                                       |           |
|----------|-------------------------------------------------------|-----------|
| 3.3.2.1  | Original IMA . . . . .                                | 34        |
| 3.3.2.2  | PRIMA . . . . .                                       | 34        |
| 3.3.2.3  | myTrustedCloud . . . . .                              | 35        |
| 3.3.2.4  | OB-IMA . . . . .                                      | 35        |
| 3.3.3    | Trusted Cloud Computing Platform (TCCP) . . . . .     | 36        |
| 3.3.3.1  | Original TCCP . . . . .                               | 36        |
| 3.3.3.2  | Improved TCCP . . . . .                               | 36        |
| 3.3.3.3  | TCCI . . . . .                                        | 37        |
| 3.3.3.4  | DTCCP . . . . .                                       | 37        |
| 3.3.4    | Remote Attestation Comparison . . . . .               | 38        |
| 3.4      | Our Framework . . . . .                               | 39        |
| <b>4</b> | <b>METHODOLOGY</b>                                    | <b>40</b> |
| 4.1      | Oracles . . . . .                                     | 41        |
| 4.2      | Trusted Blockchain-Oracle Request Framework . . . . . | 42        |
| 4.2.1    | Preparation Step . . . . .                            | 44        |
| 4.2.2    | Step 1 - Session Key Agreement . . . . .              | 45        |
| 4.2.3    | Step 2 - Quote Request . . . . .                      | 47        |
| 4.2.4    | Step 3 - Verify Quote Reply . . . . .                 | 48        |
| 4.2.5    | Step 4 - Off-chain Data Request . . . . .             | 48        |
| <b>5</b> | <b>IMPLEMENTATION</b>                                 | <b>50</b> |
| 5.1      | Oracle on GCP . . . . .                               | 52        |
| 5.2      | Blockchain on IBP . . . . .                           | 54        |
| 5.3      | Auctions Blockchain and Bank Oracle . . . . .         | 57        |
| <b>6</b> | <b>EXPERIMENTAL RESULTS</b>                           | <b>60</b> |
| 6.1      | Continuous Calls . . . . .                            | 62        |
| 6.1.1    | Usage of CPU and Memory . . . . .                     | 62        |
| 6.1.2    | Total Network Traffic . . . . .                       | 68        |
| 6.1.3    | Average Time . . . . .                                | 69        |
| 6.2      | Separated Calls . . . . .                             | 69        |
| 6.2.1    | Usage of CPU and Memory . . . . .                     | 69        |
| 6.2.2    | Total Network Traffic . . . . .                       | 75        |

|          |                                                               |           |
|----------|---------------------------------------------------------------|-----------|
| 6.2.3    | Average Time . . . . .                                        | 75        |
| 6.3      | Discussion . . . . .                                          | 76        |
| 6.3.1    | CPU Usage Peak . . . . .                                      | 76        |
| 6.3.2    | Memory Usage Peak . . . . .                                   | 77        |
| 6.3.3    | Total Network Traffic . . . . .                               | 77        |
| 6.3.4    | Average Time . . . . .                                        | 77        |
| 6.3.5    | Performance Impact Factors . . . . .                          | 78        |
| 6.3.6    | Generalization . . . . .                                      | 78        |
| 6.3.7    | Analysing Hyperledger Fabric Risks . . . . .                  | 78        |
| 6.4      | Comparing T-BORF and Oraclize . . . . .                       | 79        |
| 6.5      | Security Analysis . . . . .                                   | 80        |
| 6.5.1    | Security Against MITM Attacks . . . . .                       | 80        |
| 6.5.1.1  | Preparation Step . . . . .                                    | 80        |
| 6.5.1.2  | First Step . . . . .                                          | 80        |
| 6.5.1.3  | Second and Fourth Steps . . . . .                             | 81        |
| 6.5.2    | Security Against DoS Attacks . . . . .                        | 81        |
| 6.5.3    | Security Against DNS Attacks . . . . .                        | 81        |
| 6.5.4    | Security Against Attacks on Oracle's Nodes . . . . .          | 81        |
| 6.5.5    | Security Against Goldfinger Attack . . . . .                  | 82        |
| 6.5.6    | Security Against TLS and Private Keys Issues . . . . .        | 82        |
| 6.5.7    | Security Against False Inputs from External Sources . . . . . | 83        |
| <b>7</b> | <b>CONCLUSION AND FUTURE WORK</b>                             | <b>84</b> |
| 7.1      | Conclusion . . . . .                                          | 85        |
| 7.2      | Future Work . . . . .                                         | 86        |
|          | <b>References</b>                                             | <b>87</b> |