*Computing Science and Mathematics*
*University of Stirling*

# Smart contracts on Hyperledger Fabric

**Yordan Gospodinov**

**Supervised by Dr. Andrea Bracciali**

*Submitted in partial fulfilment of the requirements for the degree of*
**B. Sc. in Computer Science**

*April 2019*

# Abstract

Summarise the dissertation within one page. Introductory headings like this are entered using the *intro* paragraph style. It is suggested that the abstract be structured as follows:

**Problem:** what you tackled, and why this needed a solution

**Objectives:** what you set out to achieve, and how this addressed the problem

**Methodology:** how you went about solving the problem

**Achievements:** what you managed to achieve, and how far it meets your objectives.

# Attestation

I understand the nature of plagiarism, and am aware of the University's policy on this. I certify that this dissertation reports original work by me during my University project except for the following (adjust according to the circumstances):

- The technology review in section 3.2 was largely adapted *www.software-review.org/article9815.html*.
- The code discussed in section 3.1 was created by Acme Corporation (*www.acme-corp.com/JavaExpert*) and was used in accordance with the licence supplied.
- The code discussed in section 3.1.1 was written by my supervisor.
- The code discussed in section 3.1.1 was developed by me during a vacation placement with the collaborating company. In addition, this used ideas I had already developed in my own time.

**Signature:** **Date:**

# Acknowledgements

First and foremost I would like to thank to Dr. Andrea Bracciali for introducing me to blockchain. What's more I am grateful for his patience, guidance and support, without which I would not have been able to grow into what I am today. Thank you.

I am grateful to my parents for giving me the opportunity to study in University of Stirling.

I am grateful to my classmates for helping me out, when I could not understand something, and just for being around, it was fun.

I would like to thank the library for having the nice, quiet, fourth floor, and for always buying the books I requested.

# Contents

**Abstract** **i**

**Attestation** **ii**

**Acknowledgements** **iii**

**1 Introduction** **1**

1.1 Background and Context . . . . . 1

1.2 Scope and Objectives . . . . . 2

1.3 Achievements . . . . . 3

1.4 Overview of Dissertation . . . . . 3

**2 State-of-The-Art** **4**

2.1 Successful projects made with Hyperledger Fabric . . . . . 4

2.1.1 Altoros . . . . . 4

2.1.2 Verify.Me . . . . . 4

2.1.3 TradeLens . . . . . 5

2.1.4 BitNation . . . . . 6

2.1.5 E-Residency . . . . . 6

**3 Technical Chapters** **7**

3.1 First Section . . . . . 7

3.1.1 First Subsection . . . . . 7

3.1.2 Second Subsection . . . . . 7

3.2 Second Section . . . . . 8

**4 Conclusion** **9**

4.1 Evaluation . . . . . 9

4.2 Future Work . . . . . 9

**A User Guide** **11**

# List of Figures

1 Highly Technical Diagram . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8

# Chapter 1

# Introduction

Recently a new technology emerged into the world that is called blockchain. The idea is that it is a distributed decentralized database of blocks of transactions. The reason why I find it so interesting is that it has the potential to change many aspects of life, by changing the way of accessibility and security of a data. Hyperledger Fabric is a blockchain framework designed especially to make the system easily adoptable for different business use cases. The main two objectives of this project are: to research how the smart contracts in Hyperledger Fabric works; to make a prototype of self-sovereign system with the gathered knowledge.

## 1.1 Background and Context

Information has always been one of the most valuable assets a person could have. Through times information was traded in many different ways, from barter to monetization. Recently the information about an individual has become a great selling point, because it can be used in variety of fields, from science to business. However, the collection of this data is becoming a problem.

As individuals, our identities are, to some extend, not ours anymore. If we cannot certify who we are, we became no one in the eyes of business and government. Needless to say that have we lost all of the documents that certify our place in the city, company, country, Earth, we would be in a big trouble. [2]

Another approach to critical and private information is how it is being used live. Whenever we want to identify ourselves somewhere, the usual document for identification would be either an ID or a passport. Here is the problem concerning all information on this document. It turns out that whenever a person wants to prove his or her existence, the party that requires this identification, can take and keep a record of all sensitive data on that document. In some countries this may be illegal. This data then could be used for not a rightful purpose. [1]

Furthermore whenever a person is signing in to receive some kind of certificate, whether that would be a school or an academy, he or she is leaving sensitive data with this company. In most countries, whenever a person starts living in a city, he or she has to identify himself/herself to the council. In the end, there is a lot of institutions that keep sensitive data for an individual. This is a problem, because some of those institutions or businesses have different levels of security. So, an attacker only needs to pick the easiest target, and he will get a great deal of sensitive data.

I believe all of these problems are just a subproblems of a bigger challenges - what is an identity today and how to be able to give private access to our data. The solution could provide us awareness for a better control of our own data, as well as to be able to share only whats exactly needed to provide to those companies and institutions.

## 1.2 Scope and Objectives

The scope will involve Blockchain technology and what is digital identity. This project will focus on Hyperledger Fabric. This is a permissionless blockchain modular framework, especially developed for businesses.

Being a modular framework, a lot of the scope will involve around resolving how customizable Fabric can be. To be personalized is of an essence for the creation of a good system. The other main features to be examined are the scalability and usability of this blockchain framework.

The knowledge build up from the research will be implemented in a prototype program as a final part of the project. The prototype of the self-sovereign program will focus on the decentralized nature. This work will aim to present advantages of the decentralizing element that can save resources and protect the personal data of the end-user. Last but not least, I am going to talk about how the ledger is making the whole system trustful, thus no one of the parties needs to worry about being cheated.

The objectives of the project include the following :

- Understanding how Hyperledger Fabric work;
  - Installing all prerequisites;
  - Installing Hyperledger Fabric;
  - Running a simple network with 2 organizations;
  - Learning how to add more parties into an already running system;
  - Trying out how the chaincode (smart contracts) work;
  - Trying to install and control newly added chaincode on a running system.
- Building a fully functional Fabric blockchain with several different parties;
- What an ID is and identity and how it is defined in the digital world;
- Deeper understanding of self-sovereign identity, what it is and how it should/could be best defined in a blockchain platform in order to be used genuinely and without misappropriation;
  - Trying out different configurations on Fabric;
  - Trying out different chaincode functions, to find out the best for the use case.
- Building a prototype of self-sovereign identity system ;
- Complete final report .

## 1.3 Achievements

Summarise what you have achieved.

## 1.4 Overview of Dissertation

Briefly overview the contents of what follows in the dissertation.

# Chapter 2

# State-of-The-Art

## 2.1 Successful projects made with Hyperledger Fabric

### 2.1.1 Altoros

Altoros is a software company that delivers different solutions. One of the problems their customers have is issuing bonds. The customer, Russia's National Settlement Depository (NSD), wanted a system that allows automate bond placement and accounting with blockchain, while minimizing risks of reconciliation and ensuring transparency. The reason they chose Fabric is for its support of confidential transactions and resilience in the production environment. [3]

What they did was to customize Fabric as needed for the different roles and actions. They set up four different channels so the communication,data transferring, between the peers and the NSD could be safe and secure. Every channel has its own chaincode ( smart contract) that is basically the logistics behind the given channel.

One of the challenges they had was that the REST API was still in development. Fortunately, this is not the case anymore. Another challenge is that Fabric does not support cross-channel transactions. [4]

The benefits of choosing Fabric are:

- Faster transactions compared to the traditional solution, where a lot of data exchanging has to be done through a middleman. Thus, not only making it faster but also cheaper.
- Minimizing fraud in a secure trusted network. The permissioned feature does not allow for anyone that does not meet the requirements to monitor whats happening into the world ledger. Whats more because of the non cross-channel transactions, a peer could observe only the channels he is using. And even when he or she is inspecting another peers transaction, because of the encryption, he or she would not get any valuable information.
- Reduces expenses of the bond issuer by making the process faster and simplified

### 2.1.2 Verify.Me

SecureKey is a company providing identity and authentication provider for simplified access to online services and applications. They are using trusted providers such as banks, telcos and governments to make their clients assert identity information and connect to critical online services with digital credentials.

After the government of Canada recognized their problem sending private data to a citizen, they asked for a solution. SecureKey responded to this call in collaboration with IBM with a blockchain based solution. It is a mobile app, that allows the user to connect different types of services providing only specific data. So what happens is the user connects to the blockchain through the phone. Then, it connects with the service actors. It is important to note that in the phone there are only pointers to the data and not the data itself. Whenever a person is sharing his or her identity with the new service he or she can see exactly what information is asked to be provided. [7]

The SIM card is used as an anchor of trust. Since the system is private and permissioned blockchain, only trusted actors like banks and government can write on it. Upon losing or breaking the phone, the creators reassure that is easy to recover whats lost. Again, here one of the main reasons to choose Fabric for the development of this service is mainly - the adaptability of the platform and the zero-knowledge proof supported concept. [6]

The benefits of using Fabric are :

- Data integrity
- Security and resiliency
- No central database or honeypots
- No central point of failure
- Cannot track user across relying parties; privacy of the data
- Cost efficient due to simplifying the process

Cons:

- New - open standards needed

### 2.1.3 TradeLens

TradeLens is a company founded by collaborative work of Maersk and IBM. Maersk is an integrated container logistics company working on improving the supply chain area. The idea is to make the shipping process cost-efficient, faster and in respect to accessing the needed documents - simpler.

For this task, the collaboration is combining their technical and specialized knowledge to build a system on top of Hyperledger Fabric. What they created is a network, that tracks the supply chain - the documents needed for starting a shipping process, the deal that is made, the location of the containers.

To participate, a user has to pay a price to enter the network. Still it is not confirmed what the requirements are. However, once a user decides to enter he will experience something way different from the usual way of things. Due to the blockchain technology, a user can check a block on the blockchain to track the location of the container or any other process involved. The usual way for this simple task would be to request this information from a middleman. TradeLens are saying they can reduce the paperwork and the need of a mediators, saving lots of time and money in the process. [5]

It is important to be mentioned that TradeLens is not fighting the frauds. If a user input false data at start,that seems to be correct to the endorsement parties, the system wont be able to catch it. So the network helps to have less fraud, but it is more of a side effect rather than main function.

Another great use of this system is that, according to the World Trade Organization, simplifying the supply chain will not only reduce costs, but also help developing countries to increase their export by more than 30% . [16]

### 2.1.4 BitNation

### 2.1.5 E-Residency

# Chapter 3

# Technical Chapters

The body of the dissertation consists of a number of chapters named appropriately (*not* ‘Technical Chapter’). Follow a logical progression in how you present your work. This might be a time sequence of development activities, the phases of the software development cycle, the modules of your system, etc.

Appropriate chapters might be called Requirements, Design, Implementation and Evaluation. The emphasis should be on requirements, design and evaluation, with implementation details being of lesser importance. The requirements should be clearly stated, following from the client needs and weaknesses identified in the state-of-the-art review. The design should include discussion of the choices that were available and why particular decisions were made. The evaluation should relate back to the requirements, and demonstrate the extent to which these were met. Low-level material should appear in appendixes.

## 3.1 First Section

Subdivide your text into sections with the \*section* command.

### 3.1.1 First Subsection

If necessary, also use subsections. Subsections are entered using the \*subsection* command.

#### First Subsubsection

If you really need subsubsections, enter these using the \*subsubsection* command.

#### Second Subsubsection

And yet more subsubsections if need be.

### 3.1.2 Second Subsection

And, as required, more subsections.

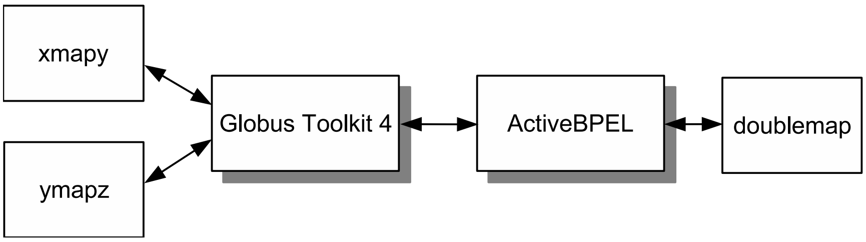

Figure 1: Highly Technical Diagram

## 3.2 Second Section

Figures are created with the *figure* environment, while tables are created with the *table* environment. They are identified by the \*label* command, and are referenced by the \*ref* command. Graphics are inserted with the \*graphic* command. Captions are entered using the \*caption* command. As an example of a figure, consider figure 1.

The native format for LaTeX graphics is EPS (Encapsulated PostScript). Graphical editors are usually capable of producing EPS. When outputting to PDF (Portable Document Format), the native graphics format is also PDF. Conversion of EPS to PDF is supported by a number of TeX toolsets.

# Chapter 4

# Conclusion

## 4.1 Evaluation

If you do not have a separate chapter on testing, explain here in detail how you went about systematically testing your system. If appropriate, also include end users in your testing. Summarise your main results, and explain how you have advanced the state-of-the-art. Stand back and evaluate what you have achieved and how well you have met the objectives. Evaluate your achievements against the objectives stated in section 1.2. Demonstrate that you have tackled the project in a professional manner.

## 4.2 Future Work

Explain any limitations in your results and how things might be improved. Discuss how your work might be developed further. Reflect on your results in isolation and in relation to what others have achieved in the same field. This self-analysis is particularly important. You should give a critical evaluation of what went well, and what might be improved.

# References

[1] S. Alboaie and D. Cosovan. Private data system enabling self-sovereign storage managed by executable choreographies. In *IFIP International Conference on Distributed Applications and Interoperable Systems*, pages 83–98. Springer, 2017.

[2] C. Allen. The path to self-sovereign identity. *LIFE WITH ALACRITY BLOG (Apr. 25, 2016), http://www. lifewithalacrity. com/2016/04/the-path-to-self-soverereignidentity. html*, 18, 2016.

[3] Altoros staff. A Blockchain-Based Platform for Automating Bond Issuing Worth 10M. [Online]. Available: *https://www.altoros.com/portfolio/blockchain-based-platform-automating-bond-issuing-worth-10m*.

[4] Altoros staff. Technical demo of NSD application with Hyperledger . [Online]. Available: *https://www.youtube.com/watch?v=NfNOT6WmRR4*.

[5] IBM staff. Maersk and IBM Introduce TradeLens Blockchain Shipping Solution. [Online]. Available: *https://newsroom.ibm.com/2018-08-09-Maersk-and-IBM-Introduce-TradeLens-Blockchain-Shipping-Solution*.

[6] SecureKey CIO Andre Boysen. How blockchain is changing digital identity. [Online]. Available: *https://www.youtube.com/watch?v=EQ5PGPIjrtI*.

[7] Verify.Me staff. Website of the company. [Online]. Available: *https://verified.me/*.

# Appendix A

# User Guide

The appendixes should contain reference material or detailed material that would detract from the flow in the body of the dissertation. Appendixes might include a user guide, a list of abbreviations, detailed program descriptions, etc. Appendixes are introduced with the *appendix* command. Appendix headings otherwise use *chapter*, *section*, etc. as usual.