# Building a secure and scalable cryptocurrency exchange

Florian M. Harwöck, Lukas G. Kurz

A diploma thesis submitted to the department of Computer Science of Higher Technical College Leonding

Principal Advisor: Franz Auernig

April 8, 2019

## **Declaration of Academic Honesty**

I declare in lieu of an oath that I have written the present thesis independently and without external help, that I have not used sources and aids other than those indicated, and that I have identified as such the places taken from the sources used, both literally and in terms of content.

### Eidesstattliche Erklärung

Hiermit erkläre ich an Eides statt, dass ich die vorgelegte Diplomarbeit selbstständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Gedanken, die aus fremden Quellen direkt oder indirekt übernommen wurden, sind als solche gekennzeichnet. Die Arbeit wurde bisher in gleicher oder ähnlicher Weise keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

- Florian M. Harwöck
- Lukas G. Kurz

## Gender Clause

For better readability, gender-specific wording is not included in this paper. It is expressly pointed out that the wording in the text refers to all genders in the same way.

### Gender Klausel

Zur besseren Lesbarkeit wird in der vorliegenden Arbeit auf geschlechterspezifische Formulierungen verzichtet. Es wird ausdrücklich darauf hingewiesen, dass im Text personenbezogene Formulierungen immer gleichermaßen auf alle Geschlechter bezogen sind.

## Acknowledgements

We would like to express our special thanks to our thesis supervisor *Franz Auernig*, who supported us in all phases of our work and gave us support and mentorship. A further thank you goes to our families and friends, who helped us during the work on our diploma thesis with feedback and suggestions for improvement.

### Danksagungen

Unser besonderer Dank gilt unserem Arbeitsbetreuer *Franz Auernig*, der uns in allen Phasen unserer Arbeit zur Seite stand und uns unterstützt und betreut hat. Ein weiterer Dank geht an unsere Familien und Freunde, die uns während der Arbeit an unserer Diplomarbeit mit Feedback und Verbesserungsvorschlägen geholfen haben.

## Abstract

In 2009 "Satoshi Nakamoto" published the cryptocurrency Bitcoin. Since then, around  $2100^1$  digital assets have been published. In total, these projects have a market capitalization of \$181 billion USD<sup>2</sup>. In order to be able to trade all those different currencies and assets among themselves, digital exchanges are needed, which are currently often insufficiently secure or scalable. This diploma thesis shows how a cryptocurrency exchange, that fulfills modern security requirements and has sufficient scalability, can be built.

Implemented with a reasonable mix of proven software components and cloudnative products, this project shows a prototype implementation with a solid security and scalability foundation that can be used by future digital exchange projects of all kinds. It is compatible with the largest decentralized digital asset network, Ethereum's ERC20 token standard. The primary intention and objective of this thesis is to build a prototype implementation which focuses on the fundamental issues of security and scalability.

### Zusammenfassung

Im Jahr 2009 hat "Satoshi Nakamoto" die Kryptowährung Bitcoin veröffentlicht. Seitdem wurden bereits über 2100<sup>3</sup> weitere digitale Vermögensgegenstände veröffentlicht. Insgesamt weisen diese Projekte eine Marktkapitalisierung von \$181 Mrd. USD auf<sup>4</sup>. Um all diese verschiedenen Währungen und Vermögenswerte untereinander handeln

<sup>&</sup>lt;sup>1</sup>As of https://coinmarketcap.com on the 8th of April 2019

 $<sup>^{2}</sup>$ See note 1

<sup>&</sup>lt;sup>3</sup>See note 1

 $<sup>^{4}</sup>$ See note 1

zu können, bedarf es digitaler Börsen, welche derzeit oft unzureichend sicher oder skalierbar sind. Diese Diplomarbeit zeigt, wie ein Kryptowährungs Börse aufgebaut werden kann, welche moderne Sicherheitsanforderungen erfüllt und über eine ausreichende Skalierbarkeit verfügt.

Implementiert mit einer sinnvollen Mischung aus bewährten Softwarekomponenten und Cloud-basierten Produkten, zeigt dieses Projekt eine Prototypen Implementierung mit einer soliden Sicherheits- und Skalierbarkeitsbasis, die von zukünftigen Projekten über digitale Börsen aller Art genutzt werden kann. Der Prototyp ist kompatibel mit dem größten dezentralen Digital Asset Network, dem ERC20-Token-Standard von Ethereum. Die primäre Absicht und Ziel dieser Arbeit ist es, einen Prototypen zu implementieren mit Fokus auf Sicherheit und Skalierbarkeit.

# Contents

D	eclar	ation o	of Academic Honesty	i
G	ende	r Clau	se	iii
A	cknov	wledge	ements	iv
A	bstra	$\mathbf{ct}$		$\mathbf{v}$
1	Intr	oducti	ion	<b>2</b>
	1.1	Motiv	ation	3
	1.2	Objec	tives	3
<b>2</b>	The	esis Re	sults	4
	2.1	The tl	nesis' final result	5
		2.1.1	Theoretical achievements	5
		2.1.2	Practical achievements	5
	2.2	Overv	iew of the developed prototype	7
3	The	oretic	al Background	12
	3.1	Block	chain	13
		3.1.1	Ledger	13
		3.1.2	Digital Signatures	14
		3.1.3	Decentralization	17
		3.1.4	Blocks	18
		3.1.5	Reaching consensus through proof-of-work	19
		3.1.6	Chaining blocks together	20

		3.1.7	Blockchain summary and conclusion	22
		3.1.8	Oversimplifications	26
	3.2	Smart	contracts	30
		3.2.1	What are smart contracts	30
		3.2.2	Ethereum $\ldots$	31
	3.3	Crypt	ocurrency exchanges	33
		3.3.1	What are cryptocurrency exchanges	33
		3.3.2	Current state of online exchanges	34
4	Tec	hnical	Challenges	35
	4.1	Match	ing different trading offers	36
		4.1.1	Adding an order	37
		4.1.2	Moving Assets	38
		4.1.3	Finishing an order	38
		4.1.4	Different operation modes	39
	4.2	Secure	e storage of sensitive data	41
		4.2.1	Password storage	42
		4.2.2	PII storage	46
	4.3	Displa	ying large amounts of data in a chart	46
		4.3.1	Provide graphs with a good user experience	47
		4.3.2	Trade off with performance and user experience $\ldots$	48
		4.3.3	Creating the data points	49
	4.4	Makin	ng the exchange scale	50
		4.4.1	What is a monolith	50
		4.4.2	Problems with traditional monoliths	53
		4.4.3	Splitting the system into microservices	56
		4.4.4	Communication between microservices	57
<b>5</b>	Imp	olemen	tation details	59
	5.1	Syster	n Architecture	60
	5.2	Fronte	end Architecture	60
		5.2.1	Advantages of a website	61
		5.2.2	Single Page App	62

		5.2.3	GRPC Web	64
	5.3	Struct	ure of the website	64
		5.3.1	Registration and login	64
		5.3.2	Dashboard	66
	5.4	Backer	nd Architecture	77
		5.4.1	Authentication Service	78
		5.4.2	User Management Service	82
		5.4.3	Mail Service	83
		5.4.4	Price Graph Service	83
		5.4.5	Token Management Service	83
		5.4.6	Trash Email Detection Service	84
		5.4.7	Matching Engine Service	84
6	Tecl	hnolog	ical Glossary	88
	6.1	Langu	ages	89
		6.1.1	Go	89
		6.1.2	Typescript	89
	6.2	Frame	works	93
		6.2.1	GRPC	93
		6.2.2	Angular	95
	6.3	Librar	ies	99
		6.3.1	Highcharts	99
		6.3.2	ZXCVBN	99
	6.4	Extern	al applications	100
		6.4.1	Hashicorp Vault	100
A	ppen	dices	1	108
$\mathbf{A}$	Plai	nning j	phase	109
	A.1	Start o	of planning	110
		A.1.1	Agile development management framework	110
		A.1.2	Agile techniques used in the planning phase	110
		A.1.3	Tools used in the planning phase	110
	A.2	Impac	t mapping	111

A.3	User s	tory mapping $\ldots \ldots 113$
	A.3.1	User Story Map - Registration
	A.3.2	User Story Map - Settings
	A.3.3	User Story Map - Trading
A.4	User s	tories $\ldots \ldots \ldots$
	A.4.1	Analytics - Count of priority
	A.4.2	Analytics - Stories per release
	A.4.3	Analytics - Value per release
	A.4.4	Analytics - Distribution of value/risk matrix

## Chapter 1

# Introduction

This chapter delivers a summary of the motivation of this thesis. The main topic of cryptocurrencies and their respective digital exchanges are introduced. Furthermore, the common problems faced in the industry are briefly addressed. In addition, the defined objectives are described, and their reasoning is explained.

#### 1.1 Motivation

In late 2017, most significant cryptocurrencies, such as Bitcoin, Ethereum, Litecoin, and Ripple, saw a drastic increase in value. Bitcoin nearly had a threefold increase in price from November to the end of December. The rise in price lead to a sort of "hype" in the community, resulting in more publicity and growth of the cryptocurrency industry. The writers of this paper, Florian Harwöck, and Lukas Kurz, also gained interest in these cryptocurrencies, but more from a technical viewpoint. They were interested in the inner workings of cryptocurrencies and cryptocurrency exchanges. There are many different exchanges, all trying to appeal to users, but upon closer inspection, many of these exchanges lack essential features. While some of them are not able to cope with massive amounts of traffic, which negatively impacts the user experience on the exchanges being hacked, using all kinds of methods, ranging from the simplest forms of server exploitation and Social Engineering to brute force attacks.

### 1.2 Objectives

Both of the writers have a background in software engineering and knowledge of software architecture. To improve the situation, the writers decided to research basic techniques for security and scalability, used in modern applications, and apply some of them to a cryptocurrency exchange. The aim was not to devise new means for scalability and security, but instead, use and implement already well known and established concepts, from other areas. The goal was to display ways of making exchanges more secure and scalable, but also to spread awareness about specific security techniques, that can be used to protect exchanges and their customers.

## Chapter 2

# Thesis Results

This chapter delivers a short overview of the final achievements for this diploma thesis, without going into technical details. Short explanations of functionalities and relevant information to understand them is given. All theoretical research, thoughts, trade-offs, comparisons, etc. and the practical implementations are discussed and shown in later chapters.

#### 2.1 The thesis' final result

This thesis reached its objectives and goals in two different areas: Firstly different concepts for improving scalability and security were designed. In conjunction with other industry proven best-practice-standards and software products, significant improvements compared to standard solutions were achieved. Secondly, most of the concepts could be directly implemented in the developed prototype and therefore validated for practicability and feasibility.

Design decisions, system architectures, security concepts, and learnings in this thesis can be used by future projects in similar directions as a solid foundation for security and scalability. The first section will introduce the reader into the more theoretical concepts behind this thesis' work. The second section will further elaborate on the prototype, and all the challenges and curiosities faced while developing a cryptocurrency exchange.

#### 2.1.1 Theoretical achievements

#### Blockchain

One of the most critical aspects of a cryptocurrency exchange is the interaction with the decentralized network powering these systems. Even though the exchange software is a standard central software solution (in the meaning of a centrally controlled backend; the system itself is built on distributed microservices), one needs a deep understanding of blockchains, smart contracts, cryptography, and a few other topics.

#### 2.1.2 Practical achievements

#### Order book and the trade matching algorithm

Processing orders as fast as possible is one of the tasks of an exchange. This task might seem rather trivial but requires at least a fast algorithm, so the exchange is not slowed down when more customers create trade offers. Creating such an algorithm also requires an understanding of the different kinds of modes in which orders can operate. Not only has the algorithm to support multiple types of trading offers, but it also needs to be able to make different kinds of order modes work with each other. Otherwise the concept of multiple modes would be useless. Our algorithm is capable of handling market orders and limit orders. It was designed with three main processes in mind, validating and enqueueing orders, matching and persisting in the order book, and processing asset transactions.

#### High performance charts

What proved to be more difficult than expected, was making charts and graphs for the prices of the currencies. These charts have to display a large amount of data, while still performing reasonably fast and also look good, as to fit in with the rest of the user interface. Finding a solution to this problem, required much research, as well as testing different frameworks and libraries for creating such charts. These libraries had to be tested for performance, but also needed to be good looking, or atleast have the option of customizing them, to fit them to our needs. Highcharts was the library that best met those needs, so it was chosen as the library to develop the charts for the prices of the currencies.

#### Cryptocurrency wallets

One challenging part during the development of a digital asset exchange is the storage solution for the digital assets itself. A bank has big physical vaults to safeguard assets, whereas in the digital world this isn't possible. To solve this issue as efficient and most importantly as secure as possible, a specialized service was developed. This service is the single authority for all assets stored and is also the only entity, that is allowed to make changes in the balance records of a user. This system together with the extensive use of cryptography lets the service store digital assets securely.

#### Microservice design

One of the goals for designing this exchange was creating a backend that would be capable of scaling to fit the varying demands due to traffic. To achieve this, a microservice architecture for the backend was used. Microservices have benefits regarding the scaling issue, but also bring their own unique set of problems with them. A solution for letting the microservices communicate with each other had been chosen. To make development easier and communication more uniform across the microservices, we chose GRPC for our API.

Debugging the whole system is always a difficult task since the code and work are split up into different services. To handle this, we used a modular approach, making what looks like a monolith, but its inner workings function like different modules communicating with each other, just like microservices. This way the whole microservice system can be split up in the production environment but also put back together into a monolith, when the system needs debugging.

#### Secure storage systems

Financial platforms, like exchanges, have a lot of interesting and valuable data. This data ranges from exact personal identifiable information (PII) and passwords to metrics about financial credibility and liquidity. To keep these data points as secure as possible content encryption is performed in transit and storage. Furthermore, pseudonyms are used throughout the system to remove links between the assetbalances, trading offers, and the end user identities.

### 2.2 Overview of the developed prototype

As with most services nowadays the user journey starts with a registration process of a new user account. In the case of this prototype, the user is obligated to enter a valid email address and password that fulfills the minimum expected requirements. During typing in the password, the user gets a dynamic overview with red and green dots for each condition. (see figure 2.1 on page 8)

I ALREADY HAVE AN ACCOUNT - L	OGIN	
Registration	Process	
Signing up for a Coinalm Accou will grant you access to all trad	int and verifying your identity through our KYC procedure ing pairs listed on the Coinalm Exchange.	_
Email		
jon.doe@gmail.com		
Password		
Your password must fulfill follow	ing properties:	
<ul> <li>10 or more characterse</li> <li>Strength: very guessable - 10</li> </ul>	<ul> <li>Not a common password seconds</li> </ul>	
The distributed ledger technology ( site are currently unregulated form are not currently perceived as repre Buying, selling and trading coins ar Please click here to read our terms	DLT) coins & tokens that are referenced and can be traded on this of value exchange under European financial services laws and senting 'transfeable securities' or other' financial instruments'. Id tokens represent a number of significant risks to participants. and conditions and here to review our risk warnings.	
By proceeding you agree to have re	ead the text above, our terms of service, and our risk warning.	
CANCEL	PROCEED WITH REGISTRATION	

Figure 2.1: The prototype's registration page

After finishing the necessary registration process, the user is required to enter his details. That is done to comply with KYC (Know-Your-Customer) regulations from the European Union. The information entered includes name, gender, date of birth, phone number, residential address, passport number, employment status, self annual income, and expected investment. (see figure 2.2 on page 8) [1] [2]

_	**
	2
Thank you for cre	ating your account.
Please now enter	your personal data.
We need your personal data to comply w Union. This is a mandatory step and you	ith regulatory legislation from the European 're obligated to enter correct information.
Identity details	
Firstname	Lastname
Jon	Doe
Gender	Date of birth
Male / Female / etc.	2018-09-20
Contact Information	Primary oboneoumber
Email florian@harwoerk.at	+43.680.23210.75
in a more than the second	
Residential Address	
Country/Region of Residence	State/Province
Austria	Upper Austria
City	Postcode
Wels	4600
Street Address/Building Name	Building/Apartment Number

Figure 2.2: The personal data collection part of the registration process

After finishing the registration process, users are redirected to the dashboard. In this main application view, the user can see his estimated account balance (only if the user already deposited digital assets) and other information. Furthermore, the user can log out of the application. (see figure 2.3 on page 9)

⊖ COINALM ₽	1 Bitemur,~15513 HB00ein,~15032 Bitemir_155339 Text,~15125
MENU Mame E Assets	Hello, Florian 🐵. Here's your account summary and all available quick actions.
▲ Trade □ History	Your last login was 14 days ago on the 14th of March, 2018
은 Profile ④ Settings	EUR 23, I/Y3.12 Estimated total balance +9.25 % + USD 4,578.02 since last login since last login
session [→ Logout	

Figure 2.3: The dashboard of the implemented prototype

The user can display his details, entered previously in the KYC part of the registration, by visiting the profile page. In an arranged overview the user can verify the accurateness of his information. (see figure 2.4 on page 9)

	Residential Address	
	Country/Region of Residence: Austria State/Province: Vienna City: Vienna Potcode: 1200 Street Address/Building Name: Samplestreet Building Ajartment Number: 41 Prod of Residence/ Address Certification: Some made up document	
Personal information	Identification Document Identification Type: Passport Identification Number: 5324143323AD35164 Document Issing Country/Region: Vienna Expiration Day: Sun Apr 05 2020	
Lashame: Doe Gender: Male Dete of birth: Fri Mar 10 1967 Email: johndoegamaiprovider.com Primary phonenumber: +65464.335256	Source of Funds Employment Status: Employed Investment Source of Funds: Inheritence Self Annual Income: 200.000 € Expected Investment: 40.000 €	

Figure 2.4: The overview of a user's entered details

To get to the core feature of the prototype, the trading page, the user first needs to select the trading pair he wants to trade. All available trading pairs are displayed in a list. (see figure 2.5 on page 10)

Icon	Name	Price	
ЕТН	Ethereum	1012.125	
EOS	EOS	5.466	
TRX	TRON	0.02	
BNB	Binance Coin	9.601	
VEN	VeChain	0.014	
WTC	Walton	27.002	
OMG	OmiseGO	3.469	
ZRX	Ox	0.545	
ZIL	Zilliqa	0.034	
MKR	Maker	353.342	
ICX	ICON	0.638	
AE	Aeternity	0.917	

Figure 2.5: The list of all trading pairs available

After the user has selected one of the trading pairs, he will be redirected to the trading details page. In this view, a history price graph, information resources, and the buy- and sell-offer form is found. The resources contain a small introduction text to the digital asset and links to their white-paper and websites. Users can use this information to educate them further about specific assets. To create a trading offer the user needs to enter the price at which he wants to buy or sell and the amount of the assets in question. (see figure 2.6 on page 10)



Figure 2.6: The trading page of a specific asset

After a trading offer was created and submitted, it is shown in the trading history list. A user can see all previously happened trades and their respective conditions. (see figure 2.7 on page 11)

Icon	Name	Туре	Amount	Date
OMG	OmiseGO	Sell	0.08340182386969985	Sat, 30 Mar 2019 11:54:23 GMT
VEN	VeChain	Deposit	8.174312777082719	Thu, 07 Mar 2019 08:50:35 GMT
EOS	EOS	Withdrawal	6.729310293677808	Sun, 13 Jan 2019 00:02:27 GMT
EOS	EOS	Sell	9.694505980162162	Wed, 12 Dec 2018 12:41:40 GMT
ZIL	Zilliqa	Buy	6.357213447752881	Sun, 18 Nov 2018 18:20:17 GMT
VEN	VeChain	Withdrawal	8.915125494044393	Sat, 25 Aug 2018 20:16:07 GMT
AE	Aeternity	Buy	1.070960099174485	Thu, 02 Aug 2018 01:54:23 GMT
TRX	TRON	Buy	3.6348023841100097	Sat, 02 Jun 2018 03:36:30 GMT
BNB	Binance Coin	Sell	3.540588928469919	Thu, 24 May 2018 09:07:42 GMT
ETH	Ethereum	Deposit	7.7766793553463165	Thu, 05 Apr 2018 05:55:18 GMT
ETH	Ethereum	Buy	7.213321359362352	Sun, 25 Mar 2018 07:26:40 GMT
ETH	Ethereum	Deposit	3.2205853507515814	Sat, 10 Feb 2018 07:47:55 GMT

Figure 2.7: The history list of all trading offers happened for this user account