An Intent-based Blockchain-agnostic Interaction Environment

Eder John Scheid

Department of Informatics

An Intent-based Blockchain-agnostic Interaction Environment

Dissertation submitted to the
Faculty of Business, Economics and Informatics
of the University of Zurich

to obtain the degree of
Doktor der Wissenschaften, Dr. sc.
(corresponds to Doctor of Science, PhD)

presented by
Eder John Scheid
from
Cerro Largo, Rio Grande do Sul, Brazil

approved in July 2022

at the request of
Prof. Dr. Burkhard Stiller
Prof. Rémi Badonnel, PhD

Berichte aus der Informatik

Eder John Scheid

An Intent-based Blockchain-agnostic Interaction Environment

Shaker Verlag
Düren 2022

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Zugl.: Zürich, Univ., Diss., 2022

Printed in Germany.

ISBN 978-3-8440-8798-7
ISSN 0945-0807

Shaker Verlag GmbH • Am Langen Graben 15a • 52353 Düren
Phone: 0049/2421/99011-0 • Telefax: 0049/2421/99011-9
Internet: www.shaker.de • e-mail: info@shaker.de

The Faculty of Business, Economics and Informatics of the University of Zurich hereby authorizes the printing of this dissertation, without indicating an opinion of the views expressed in the work.

Zürich, July 20, 2022

The chairman of the Doctoral Board: Prof. Dr. Thomas Fritz

Abstract

Blockchains (BC) are used in different fields of applications besides providing Trusted Third Party (TTP)-free financial transactions (*i.e.*, cryptocurrencies). For example, BCs are employed in supply-chain to increase transparency within the process and in the Internet-of-Things (IoT) scenario to provide an immutable and trusted database for records. However, each application field has different requirements (*e.g.*, access control or fast transaction processing) and not all BCs are able to meet such requirements. Thus, resulting in the increase of purpose-specific BCs implementations.

In this sense, selecting a BC platform that meets all the requirements of a given use-case becomes a cumbersome and non-trivial task due to the myriad of BC platforms available and their underlying technical differences (*e.g.*, consensus mechanisms, transaction costs, and block time). Further, given the small amount of of standards regarding the development of such platforms, it is hard to compare and classify them and, ultimately, integrating the selected platform with existing systems. Therefore, the following challenges revolve around such a selection and integration process: *(a)* the multitude number of BC platforms hindering the selection process, *(b)* complex technical underlying details requiring deep technical knowledge of individuals to interact with BCs, and *(c)* the shortage of BC standards leading to heterogeneous and not interoperable solutions.

Given such challenges, this PhD thesis develops an Intent-based BC-agnostic Interaction Environment, based on the concepts of Intent-based Networking (IBN) and notary scheme-based interoperability, where users are able to define requirements in the form of intents (*i.e.*, abstract high-level policies) used to select the most suitable BC platform to store data while complying with cost or performance constraints. This environment is composed of three prototyped and evaluated solutions, *(i)* an intent refinement solution, *(ii)* an policy-based BC selection framework, and *(iii)* an BC-agnostic interoperability Application Programming Interface (API). These solutions seamlessly

interact to achieve the complete refinement of user-driven intents to a complete signed transaction automatically sent to the most suitable BC platform.

Evaluations, based on a survey, of the intuitiveness of the language defined for *intent* authoring and tests on the functionality of the environment's BC selection process revealed that *(a)* the language is intuitive for non-technical and technical users, and *(b)* the selection algorithms selected correct BCs given the policy requirements. Further, performance tests of these prototyped solutions demonstrate a minimal introduced overhead to refine an *intent* to a policy ($\approx$ 5 ms), execute the BC selection algorithms ($\leq$ 22 ms), and abstract technical details from the BC interaction ($\approx$ 60 ms for an Ethereum transaction). Thus, demonstrating that the environment does not only address the posed challenges, but also provides an intuitive language, an efficient BC selection process, and a BC interoperability solution with minimal overhead.

This thesis' key contributions, proved by peer-reviewed publications, are fourfold. The first is a so far non-existent intent refinement continuum that presents five steps to refine abstract user-defined requirements that guide BC selection in the supply chain context, ultimately enforcing a transaction in the selected BC. The second is the definition of a novel intuitive Controlled Natural Language (CNL) that allows users to express such BC selection requirements without technical BC knowledge. The third is the proposal of two functional BC selection algorithms that are able to filter and efficiently select a BC platform. The fourth is a straightforward and modular BC interoperability API that allow users and applications to transparently interact with a myriad of BC platforms.

Kurzfassung

Blockchains (BC) werden nicht nur für Finanztransaktionen (z. B. Kryptowährungen) ohne vertrauenswürdige Dritte (Trusted Third Party, TTP) eingesetzt, sondern auch in verschiedenen anderen Bereichen. So werden BCs beispielsweise in Lieferketten Anwendung verwendet, um die Transparenz innerhalb des Prozesses zu erhöhen, und im Internet-of-Things-Szenario (IoT), um eine unveränderliche und vertrauenswürdige Datenspeicherung für Aufzeichnungen bereitzustellen. Jeder Anwendungsbereich hat jedoch andere Anforderungen (z.B. entweder die Zugangskontrolle oder die Geschwindigkeit der Transaktionsverarbeitung), und nicht alle BCs können diese Anforderungen erfüllen. Dieses führt dazu, dass immer mehr zweckspezifische BCs implementiert werden.

In diesem Sinne wird die Auswahl einer BC-Plattform, die alle Anforderungen eines bestimmten Anwendungsfalls erfüllt, zu einer zeitintensiv und nicht trivialen Aufgabe, da es eine Vielzahl von BC-Plattformen gibt, diese sich jedoch technisch klar unterscheiden (z.B. durch Konsensmechanismen, Transaktionskosten oder Blockzeiten). Da es nur wenige Standards für die Entwicklung solcher Plattformen gibt, ist es zudem schwierig, sie zu vergleichen, zu klassifizieren und schließlich die ausgewählte Plattform in bestehende Systeme zu integrieren. Die folgenden Herausforderungen spielen daher in einem solchen Auswahl- und Integrationsprozess eine wichtige Rolle: *(a)* die Vielzahl von BC-Plattformen, die den Auswahlprozess erschweren, *(b)* komplexe technische Details, die ein tiefes technisches Wissen der Personen erfordern, welche mit BCs interagieren, und *(c)* der Mangel an BC-Standards, der zu heterogenen und nicht interoperablen Lösungen führt.

Angesichts dieser Herausforderungen wird in dieser Dissertation eine Intent-basierte BC-agnostische Interaktionsumgebung entwickelt, die auf den Konzepten des Intent-based Networking (IBN) und der Interoperabilität auf der Grundlage des Notariatsschemas basiert. Die Benutzer können Anforderungen in Form von Intents (d.h. abstrakten durch Regeln bestimmten Absichten) definieren, die zur Auswahl der am besten geeigneten BC-Plattform für die Datenspeicherung unter Einhaltung von Kosten- oder Leistungsbeschränkungen verwendet werden. Diese Umgebung besteht aus drei

prototypischen und ebenfalls evaluierten Lösungen, *(i)* einer Lösung zur Verfeinerung von Intents, *(ii)* einem richtlinienbasierten Ansatz für das Auswählen von BCs und *(iii)* einer BC-agnostischen Interoperabilitätsschnittstelle (API). Diese Lösungen interagieren nahtlos miteinander, um die vollständige Spezialisierung von benutzergesteuerten Absichten zu einer vollständig signierten Transaktion zu erreichen und um automatisch die am besten geeignete BC-Plattform zu selektieren.

Auf der Grundlage einer Umfrage und Tests der Funktionalität des BC-Auswahlprozesses ergaben die folgenden Bewertungen der Intuitivität der für die Erstellung von Absichten definierten Sprache zwei entscheidende Ergebnisse: (a) die Sprache ist für nicht-technische und technische Benutzer intuitiv und (b) die Auswahlalgorithmen wählen angesichts der Richtlinienanforderungen korrekte BCs aus. Darüberhinaus zeigen Leistungstests dieser prototypischen Lösungen einen minimalen technischen Overhead für die Verfeinerung einer Absicht zu einer Richtlinie ($\approx$ 5 ms), die Ausführung des BC-Auswahlalgorithmus ($\leq$ 22 ms) und die Abstraktion technischer Details von der BC-Interaktion ($\approx$ 60 ms für eine Ethereum-Transaktion). Damit wird gezeigt, dass die BC-Umgebung nicht nur die gestellten Herausforderungen erfüllt, sondern auch eine intuitive Sprache, einen effizienten BC-Auswahlprozess und eine BC-Interoperabilitätslösung mit minimalem Overhead bietet.

Die vier wichtigsten Beiträge dieser Arbeit, die durch begutachtete Veröffentlichungen belegt sind, sind die folgenden. Der erste Beitrag ist die Definition eines bisher nicht existierendes Kontinuums zur Verfeinerung von Absichten, das fünf Schritte zur Verfeinerung abstrakter benutzerdefinierter Anforderungen vorstellt, die die Auswahl von BCs im Kontext der Lieferkette leiten und schließlich eine Transaktion in der ausgewählten BC erzwingen. Der zweite Beitrag ist die Definition einer neuartigen, intuitiven, natürlichen Sprache (Controlled Natural Language, CNL), die es den Benutzern ermöglicht, solche Anforderungen ohne technische BC-Kenntnisse an die BC-Auswahl auszudrücken. Drittens werden zwei funktionale BC-Auswahlalgorithmen vorgeschlagen, mit denen eine BC-Plattform aus einer Liste von Kandidaten gefiltert und effizient ausgewählt werden kann. Der vierte Beitrag stellt eine einfache und modulare BC-Interoperabilitäts-API bereit, die es Benutzern und Anwendungen ermöglicht, transparent mit einer Vielzahl von BC-Plattformen zu interagieren.

Acknowledgments

There is a quote that says "*Happiness is only real when shared*"; that could not be more true in the context of this thesis. During the four and half years that led to this thesis being finished, I had the privilege of having a wonderful family, excellent supervisors, and amazing friends to support me. That is why I would like to *share* the *happiness* of successfully arriving at this point and acknowledge that all of you contributed to this thesis and were vital for it.

This thesis is dedicated to family. Hence, I want to thank them, especially my father Ademar, my mother Neusa, and my brother Amir, in the first moment, as they are the solid foundation and my "porto seguro" ("safe port" in English). Without them, I would never be able to achieve this, as they always pushed me to be the best version of myself, encouraged me to seek what made me happy, and always reminded me that they would always be there, no matter what happened. I have a strong admiration, and I am very proud of both my parents; Ademar, an example of father and man, his detail-oriented and caring nature passed on to me, and I am very thankful for that; and Neusa, a strong, hardworking, and dedicated woman showed to me that, although life is full of surprises, there is no battle we cannot win, we just need to put our mind and heart and believe it. Amir, the best and most intelligent brother one can have, your focus and determination are examples for everyone. Eu amo muito vocês! Obrigado!

I would like to thank Prof. Dr. Burkhard Stiller for his priceless supervision. Thank you, Burkhard, for providing an excellent environment for a PhD candidate to grow, both professionally and personally. Thank you for trusting me with teaching activities and student supervisions, giving me the freedom to research and propose ideas, and being an example of professor. All the discussions and interactions that we had served to refine my work (by definition, this thesis) and taught me several valuable lessons that I will take for my entire life. Vielen Dank! I hope that our friendship continues beyond the PhD. I would also like to thank Rémi Badonnel for all the meetings and crucial feedback that helped improve this thesis's quality and for accepting being part of the defense committee.

Still in the context of supervisors, I want to express my deepest gratitude to my previous supervisors, Prof. Dr. Lisandro Z. Granville and Prof. Dra. Andrea Charão; the years under your supervision at the Federal University of Rio Grande do Sul (UFRGS) and Federal University of Santa Maria (UFSM) and the teachings were essential to allowing me to make the best from the PhD at the UZH and provided me the essential tools to make the PhD journey as smooth possible. Thank you for your trust, lessons and for being excellent mentors.

Several friends have accompanied me during this long path. I am grateful for all the colleagues, present and past, in the Communications Systems Group (CSG) that I shared the day-to-day, discussions, coffees, and beers, especially Muriel F. Franco (ever since the master's degree at UFRGS), Christian Killer, Jan von der Assen, Dr. Bruno Rodrigues, and Dr. Alberto Huertas; you were crucial for this thesis. Thank you, if it depends on me, our friendship and collaborations continues past the CSG. Further, I would like to say that I consider all the students that I supervised during these years as friends. So thank you very much, Alexander Hofmann, Andreas Knecht, Calvin Falter, Carlos Schweizer, Daniel Demeter, Daniel Lakic, David Diener, Dominik Bünzli, Dominik Sommer, Fabian Küffer, Jesús Fernández-Benito, Jonas Brunner, Lawand Muhamad, Luciana Cristea, Manuel Keller, Marc Iseli, Matteo Gamba, Michael Bucher, Niels Kübler, Noah Berni, Pascal Kiechl, Patrick Widmer, Raphael Imfeld, Ratanak Hy, Sandro Padovan, Sebastian Küng, Severin Wullschleger, Tim Strasser, and Timo Hegnauer, for trusting in me to guide you during your Bachelor, Masters, and related studies, for the contributions to this thesis, and for teaching me a lot.

Living in another country means leaving your birth country, which means seeing your long-time friends once or twice a year, so thank you very much, my dearest friends from Santo Ângelo (*i.e.*, Taiada), Santa Maria (*i.e.*, Cautela), and spread across Brazil (*i.e.*, Blá) for keeping the same strong friendship and support no matter the distance. Our friendship will last forever. Last but not least, in this context, I want to say a big thank you to the so-called "*Papers Machine*": Arthur S. Jacobs, Muriel F. Franco, Dr. Ricardo J. Pfitscher, and Dr. Ricardo L. dos Santos. Your friendship, collaborations, and discussions since the 210 office at UFRGS is one-of-a-kind!

I want to acknowledge the support of the whole administrative team of the Department of Informatics at the UZH and the Komission für Technologie und Innovation (KTI), Switzerland (CTI-No. 26996.L PFES-ED) project named Blockchain Based Temperature Monitoring for Cold Chains in Medical Drug Distribution (BC4CC) and the European Union's Horizon 2020 Research and Innovation Program project under grant agreement No. 830927 entitled Cyber Security Competence for Research and Innovation (CONCORDIA).

Contents

1 Introduction **1**

1.1 Blockchain Interoperability . . . 3
1.2 Problem Statement . . . 4
1.3 Research Questions . . . 5
1.4 Thesis Contributions . . . 6
1.5 Thesis Organization . . . 7

2 Thesis Fundamentals **8**

2.1 Policy- and Intent-based Management . . . 8
2.1.1 Policy-based Network Management . . . 9
2.1.2 Policy Continuum and Refinement . . . 12
2.1.3 Evolution to Intent-based Networking . . . 14
2.2 Blockchain Foundations . . . 18
2.2.1 Data Structure . . . 19
2.2.2 Transaction . . . 20
2.2.3 Address Generation and Transaction Signing . . . 21
2.2.4 Deployment Types . . . 23
2.2.5 Consensus Mechanisms . . . 25
2.2.6 Technical Differences . . . 32
2.2.7 Blockchain Platforms Examples . . . 41
2.3 Blockchain Standards and Interoperability . . . 48
2.3.1 Standardization Efforts . . . 49
2.3.2 Interoperability . . . 52
2.4 Thesis Fundamentals in a Nutshell . . . 57

3 Literature Review 59
3.1 Intent-based Management . . . 60
3.1.1 Approaches . . . 60
3.1.2 Summary . . . 62
3.2 Blockchain Selection . . . 63
3.2.1 Approaches . . . 64
3.2.2 Summary . . . 66
3.3 Blockchain Interoperability . . . 67
3.3.1 Approaches . . . 67
3.3.2 Summary . . . 70
3.4 Key Findings and Takeaway . . . 72

4 An Intent-based Blockchain-agnostic Interaction Environment 75
4.1 Blockchain Intent Continuum . . . 76
4.2 Environment Architecture . . . 77
4.3 Blockchain-driven Intent Refinement . . . 79
4.3.1 Blockchain Selection Intent Language . . . 80
4.3.2 Intent Parameters . . . 81
4.3.3 Refinement Process . . . 84
4.3.4 Implementation . . . 87
4.4 Policy-based Blockchain Selection . . . 92
4.4.1 Framework Architecture . . . 92
4.4.2 Workflow, Policy Parameters, and Conflicts . . . 93
4.4.3 Cost-aware Blockchain Selection Algorithm . . . 99
4.4.4 Implementation . . . 100
4.5 Modular Blockchain Interoperability . . . 103
4.5.1 Overview and Characteristics . . . 104
4.5.2 Components, Blockchain Adapters, and Features . . . 105
4.5.3 Interaction Standardization . . . 110
4.5.4 Implementation . . . 113
4.6 From an Intent to a Blockchain Transaction . . . 118

5 Evaluations and Discussion 120
5.1 Evaluations . . . 121
5.1.1 Quantitative Experiments . . . 121

5.1.2 Qualitative Assessments . . . 130
5.2 Discussion . . . 142
5.2.1 Use Case . . . 142
5.2.2 Machine Learning Employment . . . 144
5.2.3 Management Considerations . . . 147
5.3 Lessons Learned from the Evaluations and Discussion . . . 149

6 Summary, Contributions, and Further Research **153**
6.1 Summary . . . 154
6.2 Review of Research Questions and Contributions . . . 156
6.3 Further Research Outlook . . . 159

References **179**

A Publications **180**
A.1 Contribution of Own Publications Within Chapters . . . 180
A.1.1 Chapter 1. Introduction . . . 180
A.1.2 Chapter 2. Thesis Fundamentals . . . 181
A.1.3 Chapter 3. Literature Review . . . 181
A.1.4 Chapter 4. An Intent-based Blockchain-agnostic Interaction Environment . 181
A.1.5 Chapter 5. Evaluations and Discussion . . . 182
A.2 List of First Authorship Publications . . . 182
A.3 List of Co-authorship Publications . . . 183

B Controlled Natural Language Refinement State Machine **188**

C Bifröst JSON Format **192**

D Blockchain Usage Questionnaire **194**
D.1 Survey Invitation . . . 194
D.2 Questionnaire . . . 196

E Risk Evaluation **200**

F Machine Learning Employment in the Blockchain Selection Process **209**

Acronyms **214**

Glossary 220

List of Algorithms 223

List of Figures 224

List of Listings 226

List of Tables 227

Curriculum Vitae 229

To my family.