MSc Wirtschaftsinformatik

Master Thesis (MATH) FS 2018

«Label-Chain»

Konzeption & Entwicklung eines Blockchain-Prototyps im Bereich Supply-Chain-Management

Hauptreferent: Prof. Dr. Thomas Keller

Korreferent: Dr. Peter Heinrich

Eingereicht in Zürich am 25.05.2018 von

Kessler Nik, kesslnik@students.zhaw.ch, S13559844

Hochschule: Zürcher Hochschule für Angewandte Wissenschaften (ZHAW)

Vertraulichkeitserklärung der/des Studierenden

Masterarbeit: «Label-Chain»

Der Student Nik Kessler bestätigt mit seiner/ihrer Unterschrift auf dem vorliegenden Dokument, dass er die von «BIO SUISSE Vereinigung Schweizer Biolandbau-Organisation» erhaltenen Informationen ausschliesslich im Rahmen der Masterarbeit «Label-Chain» verwendet und diese Informationen ohne Zustimmung des Unternehmens «BIO SUISSE Vereinigung Schweizer Biolandbau-Organisation» zu keinem Zeitpunkt Dritten zugänglich macht.
Als Dritte gelten Personen, die nicht mit der Betreuung oder der Beurteilung der Masterarbeit befasst sind.

Zürich, 25.05.2018

N. Kessler

Wahrheitserklärung

«Ich erkläre hiermit, dass ich die vorliegende Arbeit selbständig, ohne Mithilfe Dritter und nur unter Benützung der angegebenen Quellen verfasst habe und dass ich ohne schriftliche Zustimmung der Studiengangleitung keine Kopien dieser Arbeit an Dritte aushändigen werde.»

Gleichzeitig werden sämtliche Rechte am Werk an die Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) abgetreten. Das Recht auf Nennung der Urheberschaft bleibt davon unberührt.

Name der / des Studierenden
Nik Kessler

Unterschrift (Student/in)

Ort, Datum: Zürich, 25.05.2018
Unterschrift: N. Kessler

Vertraulichkeitserklärung ZHAW

Vertraulichkeitserklärung zur Masterarbeit in den konsekutiven Masterstudiengängen an der School of Management and Law der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW)

Im Rahmen der Masterarbeit wird der Verfasser, Nik Kessler, der Projektarbeit mit dem Titel «Label-Chain» möglicherweise vertrauliche Informationen verarbeiten und in der Masterarbeit offen legen oder verwerten. Die seitens der ZHAW mit der Projektarbeit befassten Personen verpflichten sich deshalb, die in der Projektarbeit offen gelegten Informationen geheim zu halten.

Dies bedeutet,

- dass die in der Projektarbeit offen gelegten vertraulichen Informationen nicht an aussenstehende Dritte weitergegeben werden. Ausgenommen davon und ausdrücklich erlaubt ist die Überprüfung der Masterarbeit durch eine Plagiatserkennungssoftware. Die Arbeit wird auf Verlangen des Geheimnisherrn nach erfolgter Überprüfung vollständig aus der Datenbank gelöscht.
- dass die Projektarbeit mit der gebotenen Sorgfalt aufbewahrt wird, und
- dass die offen gelegten vertraulichen Informationen auch innerhalb der ZHAW nicht weiterverwendet werden.

Die Geheimhaltungspflicht entfällt, wenn die Informationen

- allgemein bekannt oder allgemein zugänglich sind oder
- schon vor der Bekanntgabe durch den Verfasser der Projektarbeit beim Empfänger vorhanden waren oder
- ohne Verletzung der Geheimhaltungsvereinbarung allgemein zugänglich sind oder werden oder
- von einem Angehörigen der ZHAW intern, ohne Benützung der dieser Vereinbarung unterstellten Informationen entwickelt oder erfunden wurden oder einem Angehörigen der ZHAW von einer dritten Partei übergeben wurden, von der die/der Angehörige der ZHAW annehmen durfte, dass sie das Recht hat, ihm diese Informationen zu übergeben oder
- aufgrund einer gesetzlichen oder vertraglichen Pflicht offengelegt werden müssen. Dies ist insbesondere dann der Fall, wenn die Bewertung der Masterarbeit angefochten wird. Der Geheimnisherr anerkennt, dass die ZHAW in einem solchen Fall zur Offenlegung der Informationen gegenüber den Rechtsmittelinstanzen verpflichtet ist.

Die Geheimhaltungspflicht entfällt ausserdem, wenn

- der/die Geheimnisherr/in an der Aufrechterhaltung der Geheimhaltung kein schutzwürdiges Interesse mehr hat, oder
- beim/bei der Geheimnisherrn/in der Wille nicht mehr besteht, die Kenntnis der geheim zu haltenden Informationen auf einen bestimmten Kreis beschränkt zu halten, oder
- der/die Geheimnisherr/in den/die Empfänger/in der Information durch ausdrückliche schriftliche Erklärung von der Geheimhaltungspflicht entbunden hat.

Das Nichtbestehen der Geheimhaltungspflicht ist von derjenigen Partei zu beweisen, die sich darauf beruft.

Winterthur, den

Unterschrift(en) Geheimnisempfänger/in der ZHAW:

_____

Management Summary

Aktuell wird die Blockchain von CEOs und weltweitem Fachpublikum als eine Technologie, die das Potenzial einer «ökonomischen Revolution» in sich birgt, bezeichnet. Auch führende amerikanische Marktforschungs- und IT-Beratungsunternehmen schätzen die Technologie als aktuellen Hype im IT-Bereich ein. Nun gilt es, diese Trend-Technologie auf deren tatsächliche Praxistauglichkeit zu untersuchen, mit der Fragestellung, wie das Anwendungspotenzial der Blockchain-Technologie für eine Schweizer Organisation einzustufen ist.

Dazu wird in einem ersten Schritt im Rahmen einer Vorstudie nach wissenschaftlichen Arbeiten über mögliche Anwendungsfelder der Blockchain gesucht. Aus den gesammelten Use Cases kann ein Anwendungsfeld definiert werden, welches anschliessend präzise untersucht wird. Im Fall der Thesis ist dies der Einsatz von Blockchain im Zusammenhang mit dem Supply-Chain-Management. Die Vorgehensweise zur Untersuchung dieser Thematik, lehnt sich an die Design Science Forschungsmethodologie an. Das Ziel dieser gewählten Methodik ist es, das Anwendungspotenzial der Blockchain an einer Schweizer Organisation über den gesamten Prozess, von der wirtschaftlichen Perspektive bis zur technischen Umsetzung, zu erforschen. Das an der Thesis partizipierende Beispielunternehmen ist ein Label, welches zertifizierte Nahrungsmittel in der Schweiz vertreibt. In Zusammenarbeit mit dieser Organisation wird eine Problemidentifikation im Bereich des Supply-Chain-Managements vorgenommen, aus welcher anschliessend mehrere Konzepte zur Lösung dieser Problemfelder basierend auf den Eigenschaften der Blockchain erstellt werden. Das Konzept mit dem grössten Potenzial trägt den Namen «Label-Chain» und bildet die Grundlage für die darauffolgende Entwicklung des Prototyps. Das Endresultat dieses Prozesses ist eine Prototyp-Applikation basierend auf den Frameworks Hyperledger Fabric und Hyperledger Composer, welche anschliessend mit 25 unterschiedlichen Testfällen evaluiert wird.

Im Rahmen der Erarbeitung der Master Thesis kann festgestellt werden, dass beim Einsatz der Blockchain im Supply Chain Management oftmals das Ziel der erhöhten Rückverfolgbarkeit genannt wird. Jedoch kann dies in diversen Fällen auch von einer vertrauenswürdigen Drittpartei übernommen werden und ist daher nicht geeignet für die Anwendung einer Blockchain. Eine weitere Problematik ist der Link zwischen der physischen und digitalen Welt, respektive ob ein Produkt authentisch ist und den digitalen Angaben der Blockchain entspricht. Aus diesen Gründen ist das Ziel der Label-Chain nicht eine blosse Rückverfolgbarkeit, sondern einen faireren und transparenteren Handel mit zertifizierten Nahrungsmittel Label-übergreifend zu ermöglichen.

Bei der technischen Umsetzung des Prototyps sind sämtliche Kernfunktionen des Konzepts erfolgreich implementiert worden. Jedoch stellte sich dabei die Frage, inwiefern die Technologien bereit für den produktiven Einsatz sind. Abschliessend gilt es zu erwähnen, dass in einigen untersuchten Fällen das Potenzial der Blockchain zu hoch eingeschätzt wird, es aber durchaus Bereiche gibt, in welchen der Einsatz der Blockchain-Technologie Potenzial hat.

Inhaltsverzeichnis

Abkürzungs-, Abbildungs- und Tabellenverzeichnis

Abkürzungsverzeichnis

- ACL Access Control List
- BFT Byzantine Fault Tolerance
- CA Certificate Authority
- CEO Chief Executive Officer
- CLI Command Line Interface
- CTO Composer Modeling Language (in Zusammenhang mit dem Composer)
- DCM Demand Chain Management
- DS Design Science
- DSRM Design Science Research Methodology
- GoO Guarentees of Origin
- ICO Initial Coin Offering
- IoT Internet of Things
- Inc. Incorporation
- IS Information System
- LTS Long Term Support
- MVP Minimum Viable Product
- PoC Proof of Concept
- PoW Proof of Work
- PoS Proof of Stake
- PBFT Practical Byzantine Fault Tolerance
- RFID Radio-frequency identification
- SaaS Software as a Service
- SCM Supply-Chain-Management

Abbildungsverzeichnis

Tabellenverzeichnis

Vorstudie

1 Einleitung

Die Blockchain wurde bereits im Jahr 2016 von Richard Branson, dem CEO der «Virgin Group», als eine Technologie, die das Potenzial einer «ökonomischen Revolution» in sich birgt, bezeichnet (Kharpal, 2016). Das amerikanische Marktforschungs- und IT-Beratungsunternehmen «Gartner» positionierte die Blockchain im Jahr 2017 im Bereich der «Peak of Inflated Expectations» ihres jährlich publizierten «Hype Cycle for Emerging Technologies» (Gartner Inc., 2017). Nun gilt es, diese Trend-Technologie auch auf deren Praxistauglichkeit zu untersuchen. Hierfür wird in dieser Vorstudie die Grundlage für die Master Thesis gebildet. Das Ziel der Vorstudie ist es, das Forschungsdesign für die Master Thesis festzulegen und erste Untersuchungen im Bereich der Anwendungsmöglichkeiten von der Blockchain durchzuführen.

Mittels einer Literaturrecherche werden Blockchain-basierte Anwendungsmöglichkeiten erforscht. Das Ziel dieser ersten Untersuchung ist es, ein möglichst breites Spektrum von potenziellen und bereits realisierten Anwendungsfällen in verschiedenen Branchen zu erläutern. Der Leser erhält somit einen Überblick an Applikationen, welche sich die Eigenschaften der Blockchain in unterschiedlicher Weise zu nutzen machen. Diese gesammelten Anwendungsfälle bilden die Grundlage für den Untersuchungsgegenstand und die Umfangsabgrenzung der Master Thesis.

Die Arbeit ist wie folgt strukturiert: In einem ersten Schritt soll der Ursprung von der Blockchain und die wichtigsten Merkmale definiert werden. Anschliessend gibt es eine Erläuterung der aktuellen Entwicklungen und Trends im Bereich der Blockchain. Danach wird das Forschungsdesign für die Master Thesis entwickelt und die detaillierte Vorgehensweise für die Literaturrecherche beschrieben, um die Reproduzierbarkeit der erhaltenen Resultate sicherzustellen. Abschliessend werden die Ergebnisse präsentiert, diskutiert und die nächsten Schritte für den Beginn der Master Thesis erläutert.

2 Ausgangslage «Blockchain»

Das Konzept der Blockchain wurde durch den Artikel «Bitcoin: A Peer-to-Peer Electronic Cash System», welcher unter dem Pseudonym Satoshi Nakamoto (2008) veröffentlicht wurde, bekannt. In diesem Artikel wird beschrieben, wie über ein Peer-to-Peer Netzwerk eine Online-Zahlung möglich ist, ohne dass eine Finanzinstitution für die Transaktion erforderlich ist (Nakamoto, 2008, S. 1). Die Transaktionen innerhalb des Netzwerks werden mit einem Zeitstempel versehen und anschliessend mittels eines hash-basierten «Proof of Work» (PoW) in die Kette eingebunden (Nakamoto, 2008, S. 2). Die Transaktionen können im Nachhinein nicht geändert werden, ohne dass der PoW wiederholt werden muss. Das längste Stück der Kette dient nicht nur als Beweis der Sequenz von Transaktionen, sondern auch als Beweis dafür, dass es vom grössten Pool an CPU-Power stammt (Nakamoto, 2008, S. 1). Daher werden Angriffe verhindert, sofern die Mehrheit der Rechenleistung bei kooperativen Parteien liegt (Nakamoto, 2008, S. 1). Des Weiteren können einzelne Parteien das Netzwerk verlassen und zu einem späteren Zeitpunkt wieder eintreten, indem sie die längste PoW Kette akzeptieren (Nakamoto, 2008, S. 1).

Mittlerweile gibt es über 1200 Kryptowährungen (CoinMarketCap, 2017) und das Thema Blockchain wird weiterhin stark diskutiert. Ein Team der Sun Yat-sen Universität in China (Zheng, Xie, Dai, Chen, & Wang, 2017) hat in Zusammenarbeit mit nationalen Instituten eine Übersicht zur technologischen Architektur, den Consensus-Algorithmen und zu den zukünftigen Trends erstellt. Gemäss Zheng et al. (2017, S. 558 f.) hat eine Blockchain folgende Hauptmerkmale: «Decentralization», «Persitency», «Anonymity» und «Auditability». Die Dezentralisierung erfolgt über verteilte Systeme, welche mithilfe des Consensus-Algorithmus die Datenkonsistenz im Netzwerk sicherstellen (Zheng et al., 2017, S. 558). Die Persistenz ist gewährleistet, weil Transaktionen validiert und von Minern bestätigt werden (Zheng et al., 2017, S. 558). Von Anonymität wird gesprochen, weil jeder Anwender mit einer generierten Adresse handeln kann, ohne dabei die wahre Identität preiszugeben (Zheng et al., 2017, S. 558). Die Überprüfbarkeit erfolgt dadurch, dass jede Transaktion von einem vorher getätigten Eintrag nachgewiesen werden kann und sich dadurch eine Kette bildet (Zheng et al., 2017, S. 559).

Des Weiteren unterscheiden Zheng et al. (2017, S. 558) zwischen drei Arten von Blockchains: «Public», «Consortium» und «Private». In öffentlichen Blockchains sind alle Einträge sichtbar und jeder beteiligt sich am Consensus-Prozess. In Konsortien kann nur eine Gruppe von vorselektierten Nodes am gemeinsamen Consensus-Prozess arbeiten (Zheng et al., 2017, S. 559). In privaten Blockchains ist es nur Angehörigen dieser Organisation erlaubt, dem Netzwerk

beizutreten und am Consensus-Prozess mitzuarbeiten (Zheng et al., 2017, S. 559). Insofern ist auch der Consensus-Algorithmus abhängig von der gewünschten Blockchain-Art. Beispielsweise eignet sich der PoW oder «Proof of Stake» (PoS) nur für öffentliche Netzwerke und der «Practical Byzantine Fault Tolerance» (PBFT) Algorithmus für Konsortien oder private Blockchains (Zheng et al., 2017, S. 560).

Eine Erscheinung, welche im Artikel der chinesischen Wissenschaftler erwähnt wird, haben zwei Forscher der Cornell University unter dem Begriff «Selfish Mining» publik gemacht (Eyal & Sirer, 2014). Selfish Mining ist die Bezeichnung für eine Gruppe von Minern mit einer Strategie, bei der sie ihre berechneten Blocks nicht direkt mit dem Netzwerk teilen und ihren Zweig (Branch) erst publizieren, wenn es für sie lukrativ ist (Eyal & Sirer, 2014, S. 5 f.). Diese Schwäche bewegt rationale Miners dazu, den Selfish Minern beizutreten (Eyal & Sirer, 2014, S. 1). Die Autoren schlagen eine Modifikation des BitCoin-Protokolls vor und eine Begrenzung des Ressourcen-Pools auf einen Viertel der gesamten Rechenleistung und nicht auf die bis anhin falsch angenommene Hälfte (Eyal & Sirer, 2014, S. 1).

Abschliessend gilt es festzuhalten, dass es mittlerweile viele Kryptowährungen und andere Arten von Blockchains mit ihren jeweils verschiedenen Konsensus Verfahren oder asymmetrischen Verschlüsselungen gibt. Zusätzlich kann zwischen mehreren Kategorien von Blockchains unterschieden werden, welche in Abhängigkeit des Anwendungsfalles verschiedene Charakteristiken aufweisen.

3 Methode

In der Wirtschaftsinformatik werden Informationssysteme und Kommunikationssysteme im Bereich der Wirtschaft und der öffentlicher Verwaltung untersucht (vgl. Mertens, 2009, S. 1). Die Forschung im Bereich «Information Systems» (IS) ist eine Forschungsdisziplin, in der oftmals Theorien und Methoden von anderen Disziplinen wie der Wirtschaft, der Informatik oder der Sozialwissenschaften angewandt werden, um Probleme im Bereich Informatik und Organisation zu untersuchen (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007, S. 46). In dieser Arbeit wird ein Informationssystem untersucht, welches sowohl eine technische wie auch eine organisatorische Komponente beinhaltet. Die in der Einleitung beschriebene «Blockchain-Technologie» wird auf deren Anwendungspotenzial und auch der damit verbundenen organisatorischen Einbettung untersucht. In diesem Kapitel werden die Problemstellung, die Abgrenzung, die Zielsetzungen, die Forschungsfrage und das Forschungsdesign erläutert.

3.1 Problemstellung & Abgrenzung der Thesis

Die Blockchain ist eine Technologie, welche aktuell als Trend (vgl. Gartner, 2017) bezeichnet wird und ein grosses ökonomisches Potenzial in sich birgt (vgl. Kharpal, 2016). Um diese Trend-Technologie auf ihr Potenzial hin zu erforschen, wurde in einem ersten Schritt mittels einer Literaturrecherche nach Blockchain-basierten Anwendungsfällen gesucht. Das Ziel der Literaturanalyse war, ein breites Spektrum an Use Cases aus unterschiedlichen Branchen zu definieren. Die Ergebnisse zeigen, dass die Thematik «Blockchain» in vielen Anwendungsbereichen diskutiert wird (Kapitel 4). In einem direkten Vergleich (Kapitel 4.8) der unterschiedlichen Anwendungsfälle konnte festgestellt werden, dass die Transparenz oder die Herkunft (Provenance) eines physischen Gutes oder von digitalen Daten ein relevantes Argument für den Einsatz von Blockchain ist. Daher wird in der Thesis ein Anwendungsfall im Bereich des «Herkunftsnachweises» behandelt. Mit dieser Eingrenzung kann ein spezifischer Anwendungsfall im Detail untersucht werden und gleichzeitig der Umfang der Master Thesis definiert werden. Des Weiteren wird in der Master Thesis ein Use Case untersucht, welcher für eine in der Schweiz ansässige Organisation von Bedeutung ist.

3.2 Relevanz «Master Thesis»

Die Master Thesis richtet sich an Forscher und Forscherinnen, welche sich mit den Anwendungsmöglichkeiten von Blockchain auseinandersetzen. Eine weitere Zielgruppe sind

professionelle IT-Spezialisten, die sich mit der Entwicklung von Blockchain-basierten Applikationen beschäftigen. Des Weiteren werden Anforderungen, Bedingungen und Auswirkungen auf eine Unternehmung festgehalten, welche Schweizer Organisationen bei der Entscheidungsfindung einer möglichen Blockchain-Anwendung unterstützen.

3.3 Zielsetzung der Thesis

Das Ziel der Master Thesis ist es, die Technologie «Blockchain» auf deren Praxistauglichkeit zu untersuchen. Um diese Zielsetzung zu erreichen, wird eine entsprechende Methodologie aus dem Bereich der «Information System Research» gewählt. In dieser Arbeit wird der Ansatz der «Design Science»(DS) verfolgt. Das Grundprinzip der DS Research ist das Wissen und Verständnis eines Designproblems und dessen Lösung mittels eines Artefakts (Hevner, March, & Ram, 2004, S. 82). Im Zusammenhang mit der Informatik wird unter einem Artefakt ein Konstrukt (Prosa), ein Modell (Abstraktion), eine Methode (Algorithmus) oder eine Instanz (Prototyp) verstanden (Hevner et al., 2004, S. 77). Eine grobe Vorgehensweise für die Masterarbeit wird in der Abbildung (1) dargestellt. Mit diesem Vorgehen wird folgende Forschungsfrage beantwortet:

Welches Potenzial hat eine Blockchain-Anwendung im Bereich des Supply-Chain-Managements für eine Schweizer Organisation?

3.4 Forschungsdesign

Das Forschungsdesign ist an die Design Science Research Methodology (DSRM) nach Peffers et. al (2007, S. 52 ff.) angelehnt. Die DSRM ist in sechs Hauptaktivitäten aufgeteilt: Die erste Aktivität ist die Identifizierung eines Problems und die Motivation zur Problemlösung. Dieser Schritt ist an die vorherrschende Meinung, dass DS Forschung ein relevantes Problem adressieren sollte angelehnt (Hevner et al., 2004). Die zweite Aktivität besagt, dass die Ziele für eine Lösung definiert werden sollten (Peffers et al., 2007, S. 55). Aus der Problemstellung werden realistische Ziele abgeleitet, welche bis dato nicht aufgegriffen wurden. Die ersten beiden Aktivitäten sind mit den ersten drei Schritten im Forschungsdesign abgedeckt (siehe Abbildung 1, «Literaturrecherche» bis «Definieren der Use Case Spezifikation»).

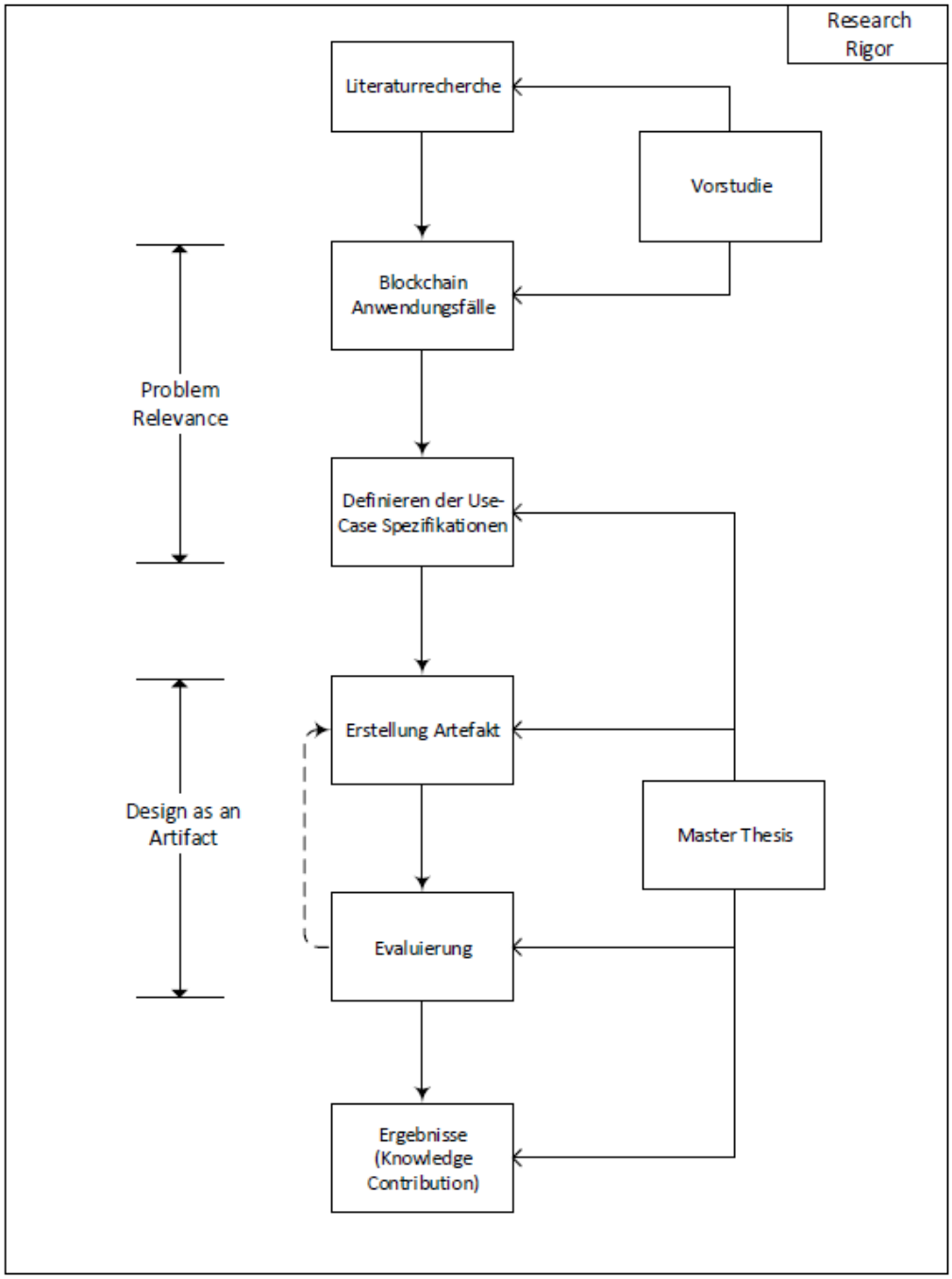

Abbildung 1: Forschungsdesign (in Anlehnung an Peffers, 2007 et. al und Hevner et. al 2004)

Die dritte Aktivität wird als «Design und Entwicklung» bezeichnet (Peffers et al., 2007, S. 55). In dieser Stufe wird ein entsprechendes Artefakt kreiert und dafür notwendige Theorien aufgegriffen. Der nächste Schritt wird als «Demonstration» bezeichnet. Es soll gezeigt werden, wie das Artefakt ein oder mehrere Instanzen eines Problems löst (Peffers et al., 2007, S. 55). Dies erfolgt durch eine Simulation, ein Experiment oder ein sonstiges passendes Vorgehen. Die fünfte Aktivität ist die Evaluation. In dieser wird gemessen, wie erfolgreich das Artefakt die Lösung unterstützt (Peffers et al., 2007, S. 55). Dies kann durch einen Vergleich zu den definierten

Zielfunktionalitäten, quantitativen Messwerten oder anderweitig passender Methode erfolgen (Peffers et al., 2007, S. 55). Typischerweise wird dieser Schritt mit einer entsprechenden empirischen Vorgehensweise oder einem logischen Beweis festgehalten (Peffers et al., 2007, S. 55). Im Falle, dass die Resultate nicht den erwarteten Leistungen entsprechen, wird bei der dritten Aktivität erneut begonnen, bis dieser iterative Prozess mit aussagekräftigen Ergebnissen verlassen werden kann (Peffers et al., 2007, S. 55). Die drei Aktivitäten (3, 4 & 5) sind im Forschungsdesign (Abbildung 1) in den Blöcken «Erstellung Artefakt» und «Evaluierung» enthalten. Die sechste und letzte Aktivität ist die Kommunikation. Im Rahmen dieses Schrittes werden die Resultate, das wissenschaftlich rigorose Vorgehen und alle Aspekte des Artefaktes der entsprechenden Peer Group mitgeteilt (Peffers et al., 2007, S. 56). Im Forschungsdesign wird dieser Schritt «Ergebnisse» oder Knowledge Contribution genannt.

Des Weiteren wurden Teile des Forschungsdesigns an das «Information Systems Research Framework» von Hevner et al (2004, S. 78 ff.) angelehnt. Ein Artefakt adressiert ein relevantes Organisations-Problem (Hevner et al., 2004, S. 82). Dies ist im Forschungsdesign (Abbildung 1) als «Design as an Artifact» vermerkt, gemäss der ersten definierten Richtlinie nach Hevner. Die «Problem Relevance» ist als Informationsbeschaffung und Verständnisprozess zu verstehen, welcher eine Entwicklung einer technischen Lösung ermöglicht (vgl. Hevner et al., 2004, S. 84). Diese Lösung muss ein ungelöstes, relevantes Business Problem beheben. Die Richtline Fünf des Frameworks wird als «Research Rigor» bezeichnet. In Design Science wird die Rigorosität durch eine effektive Anwendung von Forschungsmethoden und theoretischen Grundlagen erreicht (Hevner et al., 2004, S. 88). Das wissenschaftlich rigorose Vorgehen wird über das gesamte Forschungsdesign gestellt und für die Master Thesis sowie die Vorstudie angewandt.

3.5 Literaturrecherche «Vorstudie»

Der erste Teil der Untersuchungen basiert auf einer Literaturrecherche, durchgeführt im Zeitraum von Oktober bis November 2017. Dabei wurde hauptsächlich mit den Keywords «Blockchain» und «Blockchain Applications» nach wissenschaftlichen Arbeiten gesucht, die in folgenden Verlagen und Suchmaschinen vorhanden sind: «IEEE Xplore», «Springer», «Elsevier», «ACM» und «Google Scholar». Der Autor las jeweils das Abstract, die Introduction und die Conclusion. Die so gesammelten Artikel bildeten einen ersten Überblick der aktuell diskutierten Anwendungsfälle. Die Zielsetzung der Recherche, ein breites Spektrum an Anwendungsfällen in unterschiedlichen Branchen abzubilden, leitete die erste Filterung der Use Cases ein. Um den Umfang der Untersuchungen einzugrenzen, konnte nicht jeder Use Case erläutert werden.

Beispielsweise gibt es diverse Vorschläge von Blockchain-Anwendungsfällen im Zusammenhang mit IoT. Daher wurde nur ein Use Case beschrieben, welcher einer oder mehrere der folgenden Eigenschaften aufweist: Ein möglichst hoher Innovationsgehalt, eine adäquate Nutzung der Eigenschaften einer Blockchain, ein hohes ökonomisches Potenzial und eine fundierte wissenschaftliche Dokumentation. Anschliessend las der Autor die ausgewählten Anwendungsfälle und ergänzte diese entsprechend mit Literatur oder erweiterte sie mit Beispielen aus der Praxis. In einem letzten Schritt wurden die erhaltenen Resultate der Literaturanalyse kritisch diskutiert und verglichen.

Die Ergebnisse der Recherche bilden die Grundlage zur Definition eines relevanten Business Problems, wie es entsprechend im Forschungsdesign festgehalten ist. Mit der Zielsetzung möglichst unterschiedliche Anwendungsfälle von verschiedenen Branchen zu untersuchen, können die wichtigsten Hauptmerkmale verglichen werden. Diese Erkenntnisse sind für das spätere Vorgehen in der Master Thesis von Bedeutung.

4 Use Cases

In diesem Kapitel werden die Resultate der Literaturrecherche dokumentiert. In einem ersten Schritt werden die verschiedenen Anwendungsfälle erläutert, welche in Zusammenhang mit Blockchain diskutiert werden. Anschliessend gibt es eine Diskussion und mögliche Ergänzungen zu den Anwendungsfällen werden angebracht. In einem letzten Schritt werden die verschiedenen Use Cases verglichen und die Hauptmerkmale definiert.

4.1 Kryptowährungen

Dieser Use Case ist der erste Anwendungsfall von Blockchain, welcher durch die Kryptowährung «Bitcoin» allgemeine Bekanntheit erlangte (vgl. Nakamoto, 2008). Die Anzahl der verschiedenen Kryptowährungen ist mittlerweile auf über 1200 angestiegen (CoinMarketCap, 2017). Jedoch ist selbst dieser Typ von Use Case noch nicht komplett ausgereift, wie man am Beispiel eines Eingriffs der Singapurer Finanzmarktaufsicht erkennen kann. Dort wurden in einer offenbar abgesprochenen Aktion bei zahlreichen Firmen, welche mit sogenannten «Initial Coin Offerings» (ICO) am Markt auftauchten, die Bankkonten geschlossen. Ein ICO ist eine Form der Geldbeschaffung für neue Kryptowährungsprojekte, welche dem Crowdfunding ähnelt (Yadav, 2017). Besonders daran ist jedoch, dass diese relativ unreguliert sind (Yadav, 2017). In der Praxis eines ICOs wird Geld für ein Kryptowährungsprojekt gesammelt und die Geldgeber erhalten dafür einen «Token» (Adhami, Giudici, & Martinazzi, 2017, S. 1). Dieses Token kann in Sekundärmärkten verkauft oder dazu verwendet werden, zukünftige Produkte zu kaufen oder Dienstleistungen zu erbringen (Adhami et al., 2017, S, 1). Ein ICO kann daher eine Art Future-Kontrakt sein oder einer klassischen Obligation ähneln und in gewissen Fällen als überaus komplexes Finanzkonstrukt bezeichnet werden (Müller, 2017). Auch Rist (2017) hält fest, dass ICOs Kapital generieren und in lukrative Geschäftsbereiche von etablierten Banken eintreten, ohne Sorgfaltsplichten erfüllen zu müssen. Diese neuen Reglungen und das Einmischen der Singapurer Finanzmarktaufsicht sind insofern als wichtig zu beobachten, da Singapur grundsätzlich den Fintech Unternehmen ein attraktives Umfeld bieten möchte (Rist, 2017). Mittlerweise haben ICOs auch in der Schweiz markant zugenommen (Müller, 2017). Die Eidgenössische Finanzmarktaufsicht (FINMA) hat damit begonnen, ICOs in der Schweiz zu untersuchen (Lux, 2017). Denn gewisse ICOs fallen unter bestehendes Aufsichtsrecht, da das Schweizer Finanzmarktrecht der Technologieneutralität folgt und prinzipienbasiert ist (Lux, 2017).

4.2 IoT / Cloud

Drei Forscher am Computer Science and Engineering Department der Seoul Universität in Südkorea schlagen eine auf Blockchain-basierte Cloud-Architektur für ein IoT-Netzwerk vor (Sharma, Chen, & Park, 2017, S. 1). Dafür wird die Blockchain-verteilte Cloud-Architektur über softwaredefinierte Netzwerke und «Fog Controller» am Rande des Netzwerks ermöglicht (Sharma et al., 2017, S. 1). «Fog Computing» wird wie folgt definiert: eine geographisch verteilte Datenverarbeitungs-Architektur mit einem Ressourcen-Pool von einem oder mehreren allgegenwärtigen verbundenen heterogenen Geräten am Rande eines Netzwerks (Yi, Hao, Qin, & Li, 2015, S. 74). Diese Ressourcen können elastisch Rechenleistung, Kommunikation, Speicher oder andere Services zur Verfügung stellen (Yi et al., 2015, S. 74). Beispielsweise liegt die Verarbeitung der Daten, welche über netzwerkfähige Geräte generiert werden, näher beim Endkunden (am Rande des Netzwerks), ohne dass diese direkt in eine Cloud Umgebung übertragen werden (Yi et al., 2015, S. 74). Für Blockchain-basierte Cloud-Plattformen gibt es bereits Angebote auf dem Markt. Der Anbieter «Neboulus Inkorporation» wirbt damit, komplette Dezentralisierung und wirkliche Redundanz mit seiner Lösung zu erreichen (Herbert, 2017). Zusätzlich sei keine dritte Partei (z.B. Amazon) in kompletter Kontrolle der Dateien, sondern es werden Fragmente von verschlüsselten Kundendaten über verschiedene Instanzen gespeichert. Der Besitzer hat mit seinem privaten Schlüssel darauf Zugriff (Herbert, 2017). Aus der Kombination von softwaredefinierten Fog-Nodes für eine effiziente Datenverarbeitung und einer Blockchain-basierten Cloud-Lösung haben Sharma et. al. (2017) eine wettbewerbsfähige Lösung vorgeschlagen. Die Blockchain-basierte Cloud-Lösung wird als eine performante, kostengünstige, sichere, on-demand Architektur angepriesen (Sharma et al., 2017, S. 1). Bei der Evaluierung wurde die Architektur mit existierenden Modellen verglichen und es konnten Leistungsverbesserungen festgestellt werden (Sharma et al., 2017, S. 1). Die verkürzte Antwortzeit, die verschnellerte Datenverarbeitung und die Möglichkeit zur Erkennung von realtime-Attacken in das IoT-Netzwerk konnten beobachtet werden (Sharma et al., 2017, S. 1).

4.3 Produktion und Logistik

Wenn eine Privatperson heute Waren bei Online-Händlern einkauft, sind etliche Stakeholder an diesem Prozess beteiligt (Petersen, Hackius, & Kersten, 2016, S. 628). Das können beispielsweise Vertragspartner, Zollbehörden, Kooperationspartner, Subunternehmen oder weitere Parteien sein, welche bei der Auftragsabwicklung involviert sind (Petersen et al., 2016, S. 628). Da meistens jede beteiligte Partei eine zentrale Datenspeicherung vornimmt, ist eine durchgängige

Sendeverfolgung heute nicht mehr möglich (Petersen et al., 2016, S. 628). Mittels angebrachtem Transponder könnte die Sendung eindeutig identifiziert werden und in einer Blockchain sämtliche transaktionsbezogenen Daten gespeichert werden (Petersen et al., 2016, S. 628). Dadurch würde die Zollabwicklung erleichtert, die Zustellungszeit verkürzt und die Zahlungsabwicklung in der Kette mitintegriert werden (Petersen et al., 2016, S. 628). Auch heutige Produktionsnetzwerke sind aufgrund ihrer hohen Komplexität und geringer Pufferstände ein mögliches Anwendungsfeld für Blockchain-basierte Applikationen (Petersen et al., 2016, S. 628). Bei Störungen dieser komplexen Systeme kann es schwierig sein, einen Überblick der Lieferfähigkeit und Bestände der beteiligten Parteien zu ermitteln (Petersen et al., 2016, S. 628). Wenn in einem solchen Netzwerk alle Teilnehmer die kompletten Echtzeit-Informationen über Produktionsfortschritte oder Bestände in eine Blockchain schreiben würden, könnte eine erhöhte Robustheit, Transparenz und Effizienzsteigerung erreicht werden (Petersen et al., 2016, S. 628).

4.4 Energiemarkt

Europäische Energieproduzenten können «Guarantees of Origin» (GoO) einkaufen, welche Ihnen ermöglichen, grüne Energie an den Konsumenten weiterzuverkaufen (Castellanos, Coll-Mayor, & Notholt, 2017, S. 367). Die an den Konsumenten gelieferte Energie ist tatsächlich aber «graue» Energie, welche mit den GoOs als «grün» deklariert werden kann (Castellanos, Coll-Mayor, & Notholt, 2017, S. 367). Die «European Energy Exchange» bietet zusammen mit der «European Commodity Clearing» einen Markt an, um GoOs zu handeln (Castellanos et al., 2017, S. 368). Jedoch ist die Teilnahme an solchen Märkten mit vielen regulatorischen Barrieren und hohe Kosten verbunden (Castellanos et al., 2017, S. 368). Um diesen Prozess zu erleichtern, wird in diesem Paper vorgeschlagen, einen Energiemarkt mittels Blockchain-Tokens (ersetzt die GoOs) zu simulieren (Castellanos et al., 2017, S. 367). Dies ermöglicht Konsumenten, welche grüne Energie subventionieren möchten, direkten Kontakt mit den Produzenten herzustellen (Castellanos et al., 2017, S. 367). Eine Simulation wurde erfolgreich mit «Ethereum» realisiert und mit verschiedenen Preis Strategien getestet (Castellanos et al., 2017, S. 367).

Bereits im Jahre 2011 schlugen Nick Gogerty und Joseph Zitoli vor, eine Währung zu definieren, die nicht auf Schulden oder Gold basiert ist, sondern auf der Energieproduktion. Die Energieproduktion wird durch sogenannte «Power Purchase Agreements» festgehalten und über Zentralbanken stabilisiert (Gogerty & Zitoli, 2011, S. 8 ff.). Aus ihrem Vorschlag kreierten sie «SolarCoin». Dabei repräsentiert ein «SolarCoin» eine Megawattstunde generierte Solarenergie (The SolarCoin Foundation, 2017). Die Coins können nur als verifizierter Solarstromproduzent

generiert werden. Danach können Solarenergieproduzenten ihre Coins weiterverkaufen, um so eine Amortisierung der Solaranlange zu beschleunigen (The SolarCoin Foundation, 2017).

4.5 Personendaten im Gesundheitswesen

Eine Übersicht über die Krankengeschichte eines Patienten zu erhalten, ist heutzutage eine Herausforderung, denn die Patientendaten sind typischerweise in zentralen Datenbanken von verschiedenen Gesundheitsorganisationen abgelegt (Roehrs, da Costa, & da Rosa Righi, 2017, S. 70). Diese Datenbanken, in denen die «Elecotronic Health Records» gespeichert sind, haben meistens keinen externen Zugang und sind in unterschiedlichen, teilweise proprietären Standards entwickelt worden (Roehrs et al., 2017, S. 70). Die Autoren schlagen daher eine «OmniPHR» (Personal Health Record) vor (Roehrs et al., 2017, S. 70). Bei dieser sollten sowohl der Patient als auch die Gesundheitsbetriebe den Zugriff auf die komplette Krankengeschichte erlangen und nicht nur auf Fragmente davon (Roehrs et al., 2017, S. 70). Die Evaluation dieses Blockchain-basierten Modells hat ergeben, dass eine solche Lösung eine genügend hohe Elastizität und Skalierbarkeit aufweist (Roehrs et al., 2017, S. 80). Zukünftige Untersuchungen müssen das Modell auf die Integration mit anderen Systemen, auf die Sicherheit und die Privatsphäre der Patientendaten prüfen (Roehrs et al., 2017, S. 80).

Jedoch gestaltet sich bereits der Austausch von Daten zwischen verschiedenen Gesundheitsinstitutionen als eine Herausforderung (Peterson, Deeduvanu, Kanjamala, & Boles, 2016, S. 1). Denn um die Daten effizient auszutauschen zu können, müssen sich die Institutionen auf Syntax, Bedeutung und Sicherheitsaspekte einigen (Peterson, Deeduvanu, Kanjamala, & Boles, 2016, S. 1). Deshalb entwickelten die Forscher einen Consensus-Algorithmus, um das Problem der Interprobabilität der Daten zu reduzieren. Anstatt mit dem PoW-Algorithmus zu arbeiten, entwickelten die Forscher den «Proof of Interoperability» (Peterson, Deeduvanu, Kanjamala, & Boles, 2016, S. 5 f.). Im Unterschied zum PoW wird der Aufwand, um einen Netzwerkkonsens zu erreichen stattdessen für die Berechnung von etwas Nützlichem verwendet (Peterson, Deeduvanu, Kanjamala, & Boles, 2016, S. 5). Die Miners überprüfen im Rahmen des Consensus-Algorithmus, ob die eingehenden Nachrichten in Bezug auf die vordefinierten strukturellen und semantischen Einschränkungen interoperabel sind. Somit wird die benötigte Rechenleistung für den Konsens verwendet, um zu überprüfen, ob die Gesundheitsdaten den festgelegten Anforderungen entsprechen (Peterson et al., 2016).

4.6 Datenherkunft

Mit der beinahe exponentiellen Zunahme von Forschungsdaten wird es immer wichtiger, die Qualität sicherzustellen und Datenmanipulation zu verhindern (Ramachandran & Kantarcioglu, 2017, S. 1). Um dieser Problematik vorzubeugen, schlagen die beiden Forscher eine Blockchain-Plattform vor, um eine vertrauenswürdige Sammlung, Verifikation und Verwaltung von unterschiedlichen Daten zu ermöglichen (Ramachandran & Kantarcioglu, 2017, S. 1). Das entwickelte System nutzt «Smart-Contracts» und ein «Open Provenance Model», um unveränderbare Datenspuren festzuhalten (Ramachandran & Kantarcioglu, 2017, S. 1). Sämtliche Änderungen werden mit einem «Proof of Change», mit digitalen Signaturen und Zeitstempeln festgehalten (Ramachandran & Kantarcioglu, 2017, S. 10). Auch die Zugriffsmechanismen konnten erfolgreich implementiert werden, denn nur die Anwender mit entsprechendem Key konnten den «Proof of Change» einsehen (Ramachandran & Kantarcioglu, 2017, S. 10). Die Voraussetzung für dieses System ist, dass die Mehrheit der Teilnehmer korrekt arbeitende Nodes sind (Ramachandran & Kantarcioglu, 2017, S. 1).

Unter dem Namen «ProvChain» publizierten amerikanische Forscher eine Cloud-Architektur, um Metadaten in einer dezentralisierten Umgebung sicherzustellen (Liang et al., 2017). Metadaten sind in diesem Fall die Daten, welche bei Operationen wie beispielsweise einer Modifikation eines Datensets entstehen (Liang et al., 2017, S. 468). Dies wird von den Autoren als Clouddatenherkunft bezeichnet. Diese soll durch die Einbindung von Änderungen in Blockchain-Transaktionen erreicht werden (Liang et al., 2017, S. 468 f.). Die Forscher implementierten ihr Modell und stellten bei der Evaluierung fest, eine fälschungssichere, zuverlässige Lösung mit erhöhter Anwendersicherheit kreiert zu haben (Liang et al., 2017, S. 476). Jedoch gilt es anzumerken, dass die Lösung nur innerhalb eines Cloudanbieters getestet wurde (Liang et al., 2017, S. 476).

4.7 Diskussion der Use Cases

Das Ziel dieser Literaturanalyse ist es, einen Überblick von Blockchain-basierten Use Cases, welche in unterschiedlichen Branchen Anwendungspotenzial vorweisen, zu erstellen. Der Anfang wurde mit dem bereits bekannten Anwendungsfall der Kryptowährungen gemacht. Dieser ist insofern relevant, als mit der Umsetzung des Papers «BitCoin: A Peer to Peer Electronic Cash System» die Blockchain Technologie seine Bekanntheit erlangte. Obwohl der Artikel von Nakamoto bereits im Jahre 2008 veröffentlicht wurde, gibt es im Bereich Kryptowährungen

immer noch sehr viel Potenzial zur Weiterentwicklung. Beispielsweise wurde die breite Öffentlichkeit, durch die Berechnungen des Onlineportals «Digiconomist», über den enormen Stromverbrauch der Kryptowährung «BitCoin» informiert (Digiconomist, 2017). Durch das Mining, welches für den PoW notwendig ist, werden jährlich 30 Terrawattstunden (TWh) gebraucht, dies entspricht etwa dem Energiekonsum eins Jahres für den Oman. Eine weitere Erscheinung sind die erwähnten ICOs, welche insbesondere durch die aktuell fehlenden Regulierungen für Investoren von Interesse sind. Diese Informationen deuten darauf hin, dass vermutlich noch einige Änderungen und Entwicklungen im Bereich Kryptowährungen in Erscheinung treten werden.

Der Use Case aus dem Artikel «A Software Defined Fog Node based Distributed Blockchain Cloud Architecture for IoT» ist vermutlich der technisch innovativste, aber auch komplexeste welcher im Rahmen dieser Untersuchung erläutert wurde. Die Kombination aus einer redundanten Blochain-basierten Cloud-Architektur für ein IoT-Netzwerk könnte bestehende Herausforderungen im Bereich IoT und Cloud lösen. Zum Beispiel werden die Kosten für die IoT-User geringer, da die Fog-Nodes einen Teil der Daten bereits filtern und der kostenpflichtige Datendurchsatz bei den Cloudanbietern kleiner wird. Ein weiterer Vorteil ist, dass die Daten verschlüsselt sind und nur mit entsprechendem Key benutzt werden können. Wie sich dieses Konzept hinsichtlich der Praxistauglichkeit bewähren wird, lässt sich zum jetzigen Zeitpunkt noch nicht sagen.

Im Bereich der Produktion und Logistik könnte die Blockchain in Zukunft eine wichtige Rolle einnehmen. Die Nachvollziehbarkeit von Produktionsschritten, die grosse Anzahl an unterschiedlichen Vertragspartner oder Lieferanten und der Wunsch des Kunden nach Transparenz, könnten in Zukunft mit dem Einsatz von Blockchain gelöst werden. In diesem Bereich gibt es bereits Start-ups wie «Everledger», welche ihren Case zum Diamantenhandel bereits an der «IBM Edge» 2016 präsentierten (Everledger Ltd, 2017). Mit ihrer Lösung können wertvolle Güter über ihren gesamten Lifecycle verfolgt werden. Damit wird die Herkunft der Diamanten sichergestellt und illegalem Handel und Missbrauch vorgebeugt. Daraus lässt sich schliessen, dass in diesem Bereich zukünftig einige Blockchain-Projekte vorangetrieben werden.

Der Energiemarkt ist durch die vorhandenen regulatorischen Barrieren ein Bereich, welcher sich für die Blockchain eignet. Bereits Nakamoto hatte bei der Erstellung von «BitCoin» den Anspruch, eine Währung zu kreieren, mithilfe derer Zahlungen ohne Finanzinstitut vollzogen werden können. Im Energiemarkt ist dieselbe Problemstellung vorhanden, nur dass eine

Energiehandel- und nicht eine Finanz-Institution umgangen wird. Mittels Tokens oder «SolarCoins» können Konsumenten die Produzenten grüner Energie direkt unterstützen. Dieser Anwendungsfall lässt erahnen, dass zukünftig noch weitere Blockchain-Applikationen mit etablierten Institutionen konkurrieren könnten.

Der Austausch von Patientendaten im Gesundheitssektor ist eine Herausforderung für alle beteiligten Stakeholder. Mit dem Einsatz von Blockchain sollten die Gesundheitsorganisationen eine sichere Möglichkeit zum Austausch von Daten erhalten. Zusätzlich kann auch der Patient die Einsicht in seine Gesundheitsakte erlangen und profitiert so von dem Gesundheitsnetzwerk. Dies deutet darauf hin, dass im öffentlichen Sektor einige Anwendungsfälle existieren, bei welchen die beteiligten Stakeholder (Staatsinstitution / Bürger) vom Einsatz einer Blockchain einen Nutzen haben. Beispielsweise könne auch der Wahlprozess mittels Blockchain verbessert werden, wie das Start-Up «Followmyvote» proklamiert (Follow My Vote, Inc., 2017).

4.8 Hauptmerkmale/Vergleich der Use Cases

In der folgenden Tabelle werden die wichtigsten Faktoren, respektive die aktuellen Unterscheidungsmerkmale der Use Cases hervorgehoben.

Tabelle 1: Hauptsmerkmale (Unterscheidungsmerkmale) Use Cases

	Kryptowährungen	IoT / Cloud	Produktion und Logistik	Energiemarkt	Personendaten im Gesundheitswesen	Datenherkunft
Art	Public	Public	Konsortium	Public	Public/Konsortium	Konsortium
USP	anonyme Bezahlung, ohne dritte Instanz (z.B Zentralbank)	Sicherheit, Redundante Datensicherung mit Verschlüsselung der Daten->Nur Zugänglich mit Private Key	Transparenz, Herkunftsnachweis-> Alle beteiligten Stakeholder wissen welche Produkte wie verifiziert sind und von wo sie herkommen	Bezahlung an grüne Energieproduzenten, Energie-Institution umgehen	Austauschbarkeit der Personendaten (Gesundheitsorganisationen (Konsortium) und Patienten (Public)), Transparenz und Sicherheit für alle	Transparenz, Herkunftsnachweis, Sicherheit vor Manipulation
Transaktion	Coins	IoT-Daten	Verträge, Nachweise, Dokumente	Tokens (GoO), Coins	Patientendaten	Metadaten, «Proof of Change»

Das erste Hauptmerkmal der Use Cases ist die «Art» der Blockchain. Diese wurde gemäss den Definitionen von Zheng et al. (2017, S. 558) klassifiziert (siehe Kapitel 2). Diese Klassifizierung ist ein relevantes Merkmal zur Einteilung der Use Cases, denn es wird implizit vorgegeben, ob es sich um ein anonymes Netzwerk handelt und was für ein Consensus Algorithmus verwendet wird. In einer «Public»-Blockchain sind die Teilnehmer anonym, der Ledger ist öffentlich einsehbar

und jeder kann am Consensus-Prozess teilhaben, während bei Konsortien nur vorselektierte Nodes am Consensus-Prozess beteiligt sind und die Sichtbarkeit des Ledgers reguliert werden kann (vgl. Zheng et al., 2017 S. 589 ff.). Insofern braucht eine öffentliche Blockchain einen entsprechenden Consensus-Algorithmus wie PoW, PoS (mit Minern) während für ein Konsortium der PBFT-Algorithmus (mit vorselektierten Nodes) passender ist (Zheng et al., 2017, S. 561).

Die «Unique Selling Propositioning» (USP), ist als ein einzigartiges Verkaufsversprechen zu verstehen. In diesem Zusammenhang ist es ein wichtiges Merkmal, weshalb diese Problemstellung mit der Blockchain gelöst werden soll und nicht mit einer zentralen Datenbank oder einer «konventionellen» Methode. Unter der Rubrik «Transaktion» wird definiert was die Netzwerkteilnehmer mit der Blockchain austauschen.

Abschliessend gilt es zu sagen, dass es deutliche Unterschiede zwischen den Anwendungsfällen gibt, aber auch Merkmale, die alle teilen. Beispielsweise ist bei den öffentlichen Blockchains die Dezentralität und der Ausschluss einer mächtigen Institution ein Grundgedanke für den Einsatz von Blockchain. Bei Konsortien ist die Nachweisbarkeit, mithilfe eines private Keys und des Hash-Verfahren, ein zentrales Argument für die Anwendung von Blockchain.

4.9 Fazit Vorstudie & Ausblick auf Master Thesis

Das Ziel der Master Thesis ist die Untersuchung des Potenzials einer Blockchain-Anwendung im Bereich des «Herkunftsnachweises». Die Vorstudie beinhaltet das Vorgehen und erste Untersuchungen von Anwendungsfällen der Blockchain. Der erste Teil der Vorstudie besteht aus einem Überblick sowie aktuellen Entwicklungen im Bereich der Blockchain. Anschliessend wird das Vorgehen für die Masterarbeit definiert. Dieses Kapitel beinhaltet unter anderem die Zielsetzung, das Forschungsdesign und die Abgrenzung der Thesis. Der letzte Teil der Vorstudie besteht aus den Ergebnissen der Literaturrecherche. Die gefundenen Use Cases wurden entsprechend erläutert, verglichen und diskutiert.

Beim Beginn der Master Thesis wird ein konkreter Use Case im Bereich des «Herkunftsnachweises» ausgewählt. Dieser muss entsprechende Hauptmerkmale vorweisen und ein relevantes Business Problem adressieren. Anschliessend werden die Ziele der zu entwickelnden Lösung definiert. Diese Schritte sind notwendig, um später eine passende Applikationsarchitektur im Rahmen der Artefaktentwicklung vorweisen zu können und um das Anwendungspotenzial der Blockchain-Technologie zu erforschen.

Master Thesis

5 Methodik Master Thesis

Dies ist der zweite Teil des gesamten Master Thesis Projekts, verteilt über zwei Semester. Der erste Teil wurde im Herbstsemester in Form einer Vorstudie abgeliefert. Aufgrund der erlangten Erkenntnisse und dem vorgeschlagenen Forschungsdesign der Vorstudie werden nun die weiteren Untersuchungsschritte festgelegt. Das Ziel des gesamten Master Thesis Projekts ist es, das Potenzial der Blockchain-Technologie zu erforschen.

In diesem Kapitel wird das Vorgehen gemäss dem festgelegten Forschungsdesign in der Vorstudie weiter verfeinert, entsprechend ergänzt und beschrieben. Gewisse Details und Erläuterungen des Vorgehens sind im Fliesstext in den nachfolgenden Kapiteln festgehalten, da das Lesen und das Verständnis bei einer zu starken Trennung von Inhalt und Methodik erschwert wird. Des Weiteren werden die Zielsetzungen und entsprechenden Grenzen der Arbeit erläutert.

5.1 Zielsetzung

Das gewählte «Design Science» (DS)-Vorgehen (vgl. Vorstudie, Kapitel 3.4) gibt die Struktur für das gesamte Master Thesis Projekt vor. Das Ziel der DS-Methodik ist es, eine Lösung zu konzipieren, welche ein relevantes Organisations-Problem adressiert (vgl. Hevner et al., 2004, S. 82). Die Idee für das gewählte Vorgehen wurde aus den folgenden Überlegungen erarbeitet: Im Rahmen der Vorstudie wurden zahlreiche Cases und Problemstellungen aus unterschiedlichen Gebieten aufgezeigt, welche mit einer Blockchain-Anwendung gelöst oder verbessert werden sollten. Trotz unterschiedlichen Ausprägungen der Applikationen konnten Ähnlichkeiten zwischen den Use Cases festgestellt werden, wie beispielsweise das Bedürfnis der Nachweisbarkeit. Nach Absprache mit dem Professor wurde die «Traceability / Provenance» (Nachweisbarkeit) im Bereich des Supply-Chain-Managements (SCM) als Untersuchungsgegenstand definiert (vgl. Use Case Kapitel 4.3). Um dieses Gebiet präziser zu erforschen, wurde nach einem Schweizer Unternehmen gesucht, bei welchem die Nachweisbarkeit ein zentrales Werteversprechen an die Kundschaft ist. Mit dieser Organisation wird nun ein möglicher Blockchain Use Case definiert und exemplarisch untersucht werden. Das Ziel dieses induktiven Vorgehens ist es, dass Anwendungspotenzial der Blockchain für eine Schweizer Organisation zu untersuchen und die Implikationen auf die Organisation und deren

Ökosystem festzuhalten. Es wird erforscht, wie das tatsächliche Potenzial von Blockchain einzustufen ist und auf welche Aspekte beim Einsatz dieser Technologie geachtet werden muss.

Bei der Auswahl der zu untersuchenden Beispielorganisation wurde darauf geachtet, dass die Nachweisbarkeit der Produkte als relevante Kernkompetenz zu beurteilen ist und eine gewisse Bekanntheit, respektive Markmacht vorhanden ist. Auf diese Bedingungen passt der Verein Bio Suisse, welcher einerseits Biolebensmittel zertifiziert und andererseits kontrolliert, ob die Standards im Biolandbau eingehalten werden. Die Kunden von Bio Suisse bezahlen verglichen mit konventionell hergestellten Lebensmitteln einen höheren Preis für die zertifizierten Produkte. Die Bio Suisse zeigte auf die elektronische Anfrage des Verfassers Interesse am Master Thesis Projekt und erklärte sich bereit, sich als Beispielunternehmen für die Konzeption und die Umsetzung eines Prototyps zur Verfügung zu stellen. Dieser Ansatz hat folgende zwei Vorteile für die angewandte Wissenschaft im Bereich «Information Systems» (IS) und für das partizipierende Unternehmen: Zum einen kann damit die praktische Relevanz, welche für das Anwenden der Design Science Research Methodology relevant ist (vgl. Hevner et al., 2004, S. 82), mit der Untersuchung an einem realen Exempel erreicht werden. Zum anderen profitiert das mitarbeitende Unternehmen von den gesammelten Erfahrungen aus der Konzeptionierung und der Umsetzung des Prototyps. Somit wird in dieser Master Thesis der komplette Prozess, vom Konzept bis zur Entwicklung einer Blockchain-Applikation, im Rahmen der DS-Forschungsmethode untersucht.

5.2 Übersicht Forschungsdesign & Gliederung

In der folgenden Abbildung 2 wird das aktualisierte Forschungsdesign der Vorstudie mit entsprechenden Kapitelverweisen abgebildet. Das entwickelte Forschungsdesign, welches in Anlehnung an die Aktivitäten 1-6 der «Design Science Research Methodology» (DSRM) von Pfeffers et al. (2007) und an das «Information Systems Research Framework» nach Hevner et al. (2004) konzipiert wurde (detaillierte Beschreibung: siehe Kapitel 3.4), bildet die Struktur dieser Arbeit.

Die Master Thesis ist in zwei Hauptteile gegliedert. Der erste Teil, welcher in Kapitel 6 beschrieben wird, ist die wirtschaftliche Betrachtungsweise der Blockchain-Technologie. In diesem Kapitel werden sämtliche Schritte, von der Problemidentifikation (vgl. Peffers et al., 2007, S. 52 ff.) bis zur Erstellung des Konzeptes, beschrieben. Dieses Konzept wird anschliessend im Kapitel 7 in Form eines Prototyps umgesetzt. Die daraus gewonnenen Ergebnisse der

Lösungskonzipierungen und der Erstellung des Prototyps werden anschliessend in Kapitel 8 diskutiert und ausgewertet.

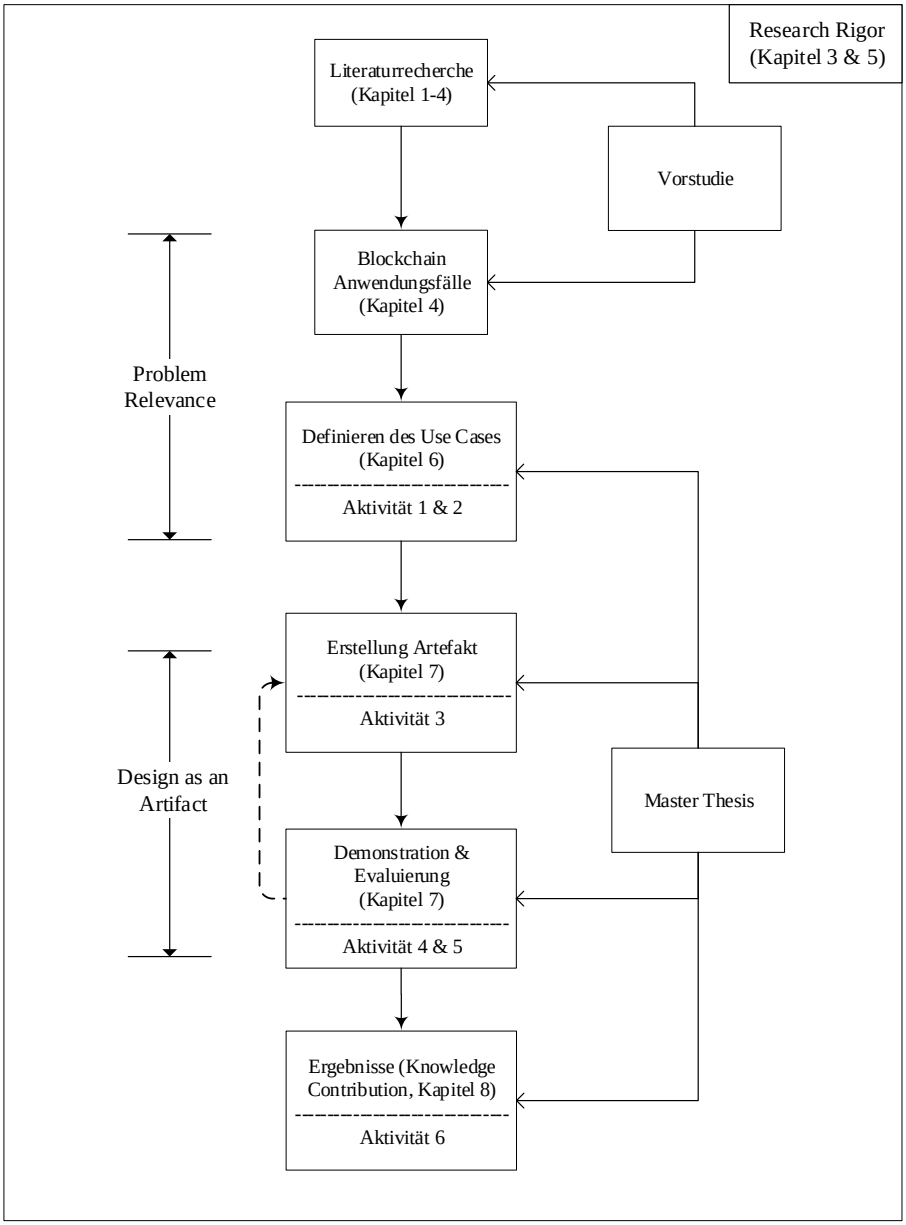

Abbildung 2: Forschungsdesign & Gliederung (anlehnend an Vorstudie, 2018)

5.3 Erarbeitung des Use Cases

In diesem Methodenkapitel wird erläutert, wie im Kapitel 6 für die «Definition des Use Cases» vorgegangen worden ist und wie es zu den Ergebnissen gekommen ist. Der erste Schritt begann mit der Sammlung von Informationen über die Bio Suisse, um einen Überblick über den Verein zu erlangen. Die Online Recherche fand im Zeitraum von Januar bis und mit Februar 2018 mithilfe der Suchmaschinen «Google» und «Qwant» statt. Dabei wurde hauptsächlich mit dem

Keyword «Bio Suisse» gesucht, wobei die Suche mit zielgerichteten Begriffen wie «Verbandsrechnung» oder «Statuten» erweitert wurde. Die gesammelten Berichte bildeten die notwendigen Informationen für die weiteren Untersuchungen und sind im ersten Unterkapitel (6.1) zusammengefasst.

Die DSRM nach Peffers et. al (2007, S. 52 ff.) schlägt sechs Hauptaktivitäten vor, welche für die Forschung im Bereich Design Science (DS) in dieser Arbeit angewandt werden. Die erste Aktivität ist die Identifizierung eines Problems und die Motivation zur Problemlösung. Dieser Schritt schliesst an die vorherrschende Meinung an, dass DS-Forschung ein relevantes Problem adressieren sollte (vgl. Hevner et al., 2004). Deshalb wurde ein Workshop mit der Bio Suisse angestrebt, bei welchem einerseits Informationen zu möglichen Problemfeldern gesammelt werden konnten. Andererseits war es möglich, zusätzliches Wissen über den Biomarkt, die Prozesse und die Supply-Chain der Bio Suisse zu aggregieren. Der Workshop fand am 14.02.2018 mit Oliver Gaede von Bio Suisse und Nik Kessler (Autor) statt. Das Treffen dauerte ca. acht Stunden und sämtliche Unterlagen, die im Zusammenhang des Workshops erarbeitet wurden, sind im Anhang A (2018) abgelegt. Es sind absichtlich keine Tonaufnahmen dieser Interaktion gemacht worden, die Analyse dieser Gespräche hätte nicht dem Umfang und der Zielsetzung dieser Arbeit entsprochen. Das im Workshop erarbeitete Wissen bildet die Grundlage zur Problemidentifikation und wird als erster Input für die Konzeption des Artefaktes verwendet. Sämtliche Ergebnisse sind im Kapitel 6.2 beschrieben und wurden mit öffentlichen Beiträgen oder Zeitschriftenartikel ergänzt.

Aufbauend auf den Resultaten der Problemidentifikation war es möglich, neue Lösungen und Konzepte für die Bio Suisse zu entwickeln. Gemäss der zweiten Aktivität der DSRM nach Peffers et al. (2007, S. 55) müssen die Ziele für das zu kreierende Artefakt definiert werden. Konkret müssen aus den identifizierten Problemen realistische Zielsetzungen definiert werden, welche bis dato nicht aufgegriffen wurden. Dieser Prozess ist in Kapitel 6.3 ersichtlich. Begonnen wurde mit zwei möglichen Entwurfskonzepten (6.3.1), die jeweils unterschiedlich identifizierte Problemfelder lösen. Weil es für eine dezentrale Anwendung relevant ist, die Interessen der verschiedenen theoretisch möglichen involvierten Parteien zu beurteilen, wurden die beiden Entwürfe präziser mit einer Stakeholderanalyse (6.3.2) untersucht. Diese Vorgehensweise wurde deshalb gewählt, weil somit alle unterschiedlichen Absichten dargestellt, hinsichtlich der Einführung einer Blockchain-Anwendung bewertet und mögliche Interessenkonflikte aufgezeigt werden können. Für diese Analyse wurden hauptsächlich Annahmen getroffen und keine Interviews oder Befragungen durchgeführt, um den vorgegebenen Umfang der Master Thesis

einzuhalten. Dies bedeutet, dass im Zusammenhang dieser Arbeit keine empirische repräsentative Untersuchung mit möglichen beteiligten Stakeholdern am Netzwerk oder anderen Unternehmen geführt wurden. Insofern wurden keine Experteninterviews oder repräsentative Umfragen mit unterschiedlichen Unternehmen zum Thema Blockchain geführt. Denn zurzeit gibt es vermutlich eine grosse Zahl an Proof-of-Concepts (POCs), Prototypen oder Applikationen auf dem Stand eines Minimum Viable Product (MVP), welche aber nicht im «produktiven» Operationsmodus sind. Deshalb würden mit solchen Umfragen vermutlich höchstens die aktuelle «Gefühlslage» zur Blockchain-Thematik, aber nicht generalisierbare Fakten erforscht werden. Die Perspektive von Bio Suisse und eine Einschätzung der restlichen Stakeholder wurde mit Oliver Gaede, dem Supply-Chain Verantwortlichen von Bio Suisse, erstellt. Diese Informationen sind in einer Videokonferenz, welche am 11.04.2018 stattgefunden hat, als Aufzeichnung gespeichert worden. Das gesamte Gespräch dauerte ungefähr eine Stunde und ist als Anhang B (2018) gekennzeichnet.

Anschliessend sind aus den entworfenen Konzepten mögliche Varianten der Konsortien (6.3.3) generiert worden, um verschiedene Use Cases mit unterschiedlicher Ausprägung vorzuschlagen. Die Idee dieses Vorgehens ist es, unterschiedliche Anwendungsfälle zu definieren und diejenige Option mit dem grössten Potenzial weiterzuverfolgen. Für die Auswahl eines möglichst realitätsnahen Blockchain-Projektes muss auch der Business Case berücksichtigt werden. Im Kapitel 6.3.4 wird eine von Gartner (Kandaswamy & Furlonger, 2017) vorgeschlagene Auflistung der zu bewertenden Aspekte dargestellt, gewissermassen eine Kosten-Nutzen-Analyse, welche bei einem Blockchain-Projekt zu berücksichtigen ist. Jedoch gilt es klar anzumerken, dass kein tatsächlicher Business Case in dieser Arbeit erarbeitet wird. Dieses Kapitel bietet lediglich mögliche Anhaltspunkte für die Aufstellung eines Business Cases und ist als Ergänzung zu betrachten. Dies bedeutet auch, dass kein detailliertes Business Modell erstellt wurde. Im Rahmen des Konzepts werden zwar Rahmenbedingungen festgelegt, jedoch wird beispielsweise nicht definiert, mit welchem exakten Preismodell die Einnahmen generiert werden können. Dies gilt es beim Zusammenstellen des Konsortiums zu definieren.

Um die erstellten Varianten präziser zu bewerten, wurde nach Literatur mit der folgenden Thematik gesucht: Welche Faktoren gilt es beim allfälligen Blockchain-Einsatz zu beachten und ist die Technologie tatsächlich für diesen Use Case geeignet. Dabei sind zwei Papers (Wüst & Gervais, 2017) (Peck, 2017), welche über Google Scholar gefunden worden sind und ein Präsentationsdokument (Le Hors, 2018), welches ein Technical Steering Comittee Member von Hyperledger verfasste, verwendet worden. Jedoch gilt es bei diesen Arbeiten anzumerken, dass vermutlich keine einem hohen wissenschaftlichen Standard entspricht. Zum Zeitpunkt des

Verfassens dieser Arbeit sind keine exakten quantifizierbaren Merkmale in einem Journal Paper gefunden worden. Ein weiteres Modell von Gartner (Kandaswamy & Chesini, 2017) zu dieser Thematik wurde absichtlich nicht verwendet, da bei diesem Modell der Business Case und nicht der Use Case in den Fokus gerückt wird und gewisse Aspekte des Modells weder beschrieben noch mit dem aktuellen Wissenstand erklärbar waren (siehe Kapitel 6.4) Mit den drei verwendeten Arbeiten konnte eine Übersicht darüber gewonnen werden, wie die aktuelle Lage für den möglichen Einsatz von Blockchain einzuschätzen ist. Denn bei einem Vergleich der drei Fragenkataloge wird ersichtlich, dass teilweise sehr ähnliche Hauptmerkmale für eine Beurteilung eines allfälligen Blockchain Use Case von den Autoren beschrieben werden. Diese Hauptmerkmale bildeten die Grundlage, um die unterschiedlichen Optionen der Use Cases zu evaluieren.

Die gesammelten Erkenntnisse werden anschliessend in Kapitel 6.5 in vier Varianten eingeteilt und bewertet. Dies bedeutet, dass die Entwurfskonzepte mit den unterschiedlichen Zielsetzungen und möglichen Varianten von Konsortien in diesem Unterkapitel evaluiert werden. Das Ziel ist es, einen möglichst validen und realitätsnahen Use Case für die Bio Suisse zu kreieren. Die Ausgangslage sind die Konsortiumsparteien, die unterschiedlichen Zielsetzungen und ein möglicher high-level Business Case. Die definierten Hauptmerkmale im vorherigen Kapitel «Blockchain-Fit» dienen als Bewertungsgrundlage der vier Varianten. Eine Übersicht der wichtigsten Eckpfeiler der Optionen ist in Form einer Tabelle dargestellt und wird anschliessend diskutiert. Bei der Prüfung der Varianten auf den jeweiligen Blockchain-Fit konnte festgestellt werden, dass insbesondere die Frage des Vertrauens zwischen Organisationen schwer zu beurteilen ist. Deshalb ist in Kapitel 6.6 eine Ergänzung zur Rolle des «Trust» zwischen Organisationen vorzufinden, inklusive einer möglichen Vorgehensweise für das Messen des Vertrauens. Es gilt anzumerken, dass eine empirische Untersuchung des Vertrauens nicht dem Umfang dieser Arbeit entspricht und dieses Kapitel als Erweiterung zu betrachten ist. Im Abschnitt 6.7 ist die Beschreibung des Use Cases und des kreierten Konzeptes «Label-Chain» vorzufinden. Es werden erste Anforderungen zur Umsetzung des Artefakts geliefert und die Rahmenbedingungen für das weitere Vorgehen impliziert. Der Abschluss des Kapitels der Use-Case-Erstellung bildet eine Generalisierung beziehungsweise eine Diskussion über den Einsatz von Blockchain in Zusammenhang mit dem SCM (6.8). Für dieses Kapitel wurden Arbeiten, welche sich mit dem Einsatz von Blockchain im SCM befasst haben, zitiert. Es geht in diesem Kapitel darum, das ausgewählte Anwendungsfeld kritisch zu diskutieren und den Einsatz der Blockchain zu hinterfragen. Die Diskussion über das gesamte Kapitel 6 und der erhaltenen Resultate wird im Kapitel 8.1 im Rahmen der «Knowledge Contribution» geführt.

5.4 Umsetzung des Prototyps

In diesem Methodenkapitel wird beschrieben, wie im Kapitel 7 «Umsetzung der Label-Chain» vorgegangen worden ist. In diesem Kapitel werden die Hauptaktivitäten 3, 4 & 5 gemäss der DSRM nach Peffers et al. (2007) durchgeführt.

Begonnen wurde mit Untersuchungen zur Auswahl der passenden Blockchain-Technologie in Kapitel 7.1. Dazu wurden die groben Anforderungen an die Applikation «Label-Chain» beschrieben und es wurde definiert, welche Art von Blockchain implementiert werden muss. Das erstellte Konzept entspricht einer «permissioned» oder Konsortiums-Blockchain (vgl. Kapitel 2). Insofern muss ein Framework oder eine Technologie ausgewählt werden, welche diese Art von Blockchain unterstützt. Es wurde hauptsächlich über Google Scholar nach wissenschaftlichen Arbeiten gesucht, die bekannte Blockchain Frameworks vergleichen. Denn das Ziel dieser Arbeit ist es, das Potenzial der Technologie und nicht eine spezifische Technologie zu untersuchen. Es wurde angenommen, das bekannte Frameworks ausgereifter als deren neuere Konkurrenztechnologien sind. Ein Working Paper des Blockchain Center der Frankfurt School von Valenta & Sandner (2017) vergleicht Ethereum, Corda R3 und Hyperledger Fabric hinsichtlich der Governance, «Mode of Operation» (bspw. permissionless) und weiteren Aspekten. Aufgrund der Anforderungen der Label-Chain und den Vergleichen von Valenta & Sadner (2017) hat sich Hyperledger Fabric als favorisierte Technologie herausgestellt. Ein weiterer Faktor für die Wahl des Hyperledger Fabric war, dass der Autor zum Zeitpunkt des Verfassens der Arbeit bei der IBM Schweiz angestellt ist. IBM Research sowie IBM Hursley sind massgeblich an der Entwicklung von Hyperledger Fabric beteiligt, insofern ist es dem Autor möglich bei Entwicklungsproblemen auf ein internes Netzwerk zurückzugreifen. Es gilt aber anzumerken, dass Hyperledger Fabric keine proprietäre IBM Softwarelösung ist, sondern von der Linux Foundation verwaltet wird und ein Open-Source Projekt ist, bei welchem 28 verschiedene Unternehmen aktiv Beiträge leisten. Für die Entwicklung der Logik und des Netzwerkes wurde das Framework Composer verwendet. Das Hauptziel von Composer ist es, die Entwicklung zu vereinfachen und die benötigte Zeit zum effektiven Einsatz der Applikation zu reduzieren (Hyperledger Composer, o.J.e). Dieses Framework wurde gewählt, weil der Fokus des Prototyps nicht die Untersuchung einer spezifischen Technologie ist, sondern die Entwicklung eines realistischen Use Cases und dessen Implikationen für die Organisation und deren Ökosystem. Weitere Informationen zu dieser Thematik sind in Kapitel 8.2 beschrieben.

Das gewählte Vorgehen gemäss der DSRM nach Peffers et al. (2007, S. 55 f.) sieht vor, folgende Aktivitäten zu trennen: das Design und die Entwicklung (Hauptaktivität 3), die Demonstration (Hauptaktivität 4) und die Evaluierung (Hauptaktivität 5). Dabei sollte am Ende dieser drei Aktivitäten entschieden werden, wie das Forschungsprojekt weitergeführt werden soll (Peffers et al., 2007, S. 56). Dies bedeutet, dass entweder nach der Evaluierung zur Aktivität 3 zurückgekehrt werden muss, um die Effektivität des Artefaktes zu verbessern oder dass man zur nächsten Hauptaktivität schreitet und Verbesserungen nachfolgenden Projekten überlässt (Peffers et al., 2007, S. 56). Die Art des Forschungsprojektes gibt vor, ob eine solche iterative Vorgehensweise zielführend ist und durchgeführt werden kann (Peffers et al., 2007, S. 56). Für die Master Thesis wurde diese iterative Vorgehensweise adaptiert, jedoch mit gewissen Änderungen: In Abhängigkeit des Umfangs der Master Thesis und der zur Verfügung stehenden Ressourcen sind die drei Aktivitäten, die Entwicklung, die Demonstration und die Evaluierung, in ein Kapitel zusammengelegt worden. Das heisst, es wurde iterativ gearbeitet, jedoch in viel kleineren Schritten und nur der Anfangs- und Endzustand wurde ausführlich dokumentiert. Dieses Vorgehen hat insbesondere bei neuen Technologien und Frameworks den Vorteil, dass jeder neu implementierte Schritt wieder getestet werden kann. Somit besteht keine Gefahr, dass man zuerst eine komplette Applikationsarchitektur designt und dann anschliessend bei der Implementierung feststellt, dass dieses Konzept oder Vorgehen gar nicht mit diesem Framework kompatibel ist.

Im Kapitel 8.3 werden sämtliche benötigten Softwarekomponenten und relevanten Dateien, welche für die Entwicklung mit dem Hyperledger Composer Framework benötigt werden, erläutert. Das Ziel an diesem Zeitpunkt der Arbeit war, zu verifizieren, dass die Installation fehlerfrei verlaufen ist und das Composer Framework tatsächlich unter diesen Voraussetzungen funktionsfähig ist. Anschliessend wurden die Erkenntnisse dieses Vorgehens dokumentiert und mit entsprechenden Erläuterungen ergänzt, sodass der Leser ein Grundverständnis für das Framework und den tatsächlichen Prototyp aufbauen kann. Falls dieser Test nicht erfolgreich gewesen wäre, hätte zu diesem Zeitpunkt nach einem neuen Blockchain-Framework gesucht werden müssen. Da dieser Testfall aber erfolgreich auf einem Fabric-Netzwerk durchgeführt werden konnte, wurde anschliessend mit der tatsächlichen Entwicklung der Label-Chain fortgefahren.

Im Kapitel 8.4 wird das Resultat der Umsetzung Label-Chain beschrieben. Des Weiteren werden die Grundlagen und die Gründe beschrieben, welche zu den entsprechenden Design-Entscheidungen geführt haben. Dies entspricht der Hauptaktivität «Design und Entwicklung» gemäss der DSRM nach Peffers et al. (2007, S. 55). Die Applikation wurde auf dem

standardmässigen Fabric-Netzwerk mit einer einzelnen Organisation aufgebaut. Für den Prototyp wurde es nicht als notwendig erachtet, die Applikation bereits auf einem dezentralen Netzwerk zu installieren, da in diesem Stadium des Master Thesis-Projekts der Fokus auf der Business-Logik und dem Konzept liegt. Jedoch kann die Applikation auch auf einem tatsächlich dezentralen Netzwerk mit mehreren Organisationen hochgefahren werden, was relevant wird, sobald sich ein tatsächliches Konsortium bildet und ein wirkliches dezentrales Netzwerk aufgebaut wird (vgl. Hyperledger Composer, o.J.c). Ein weiterer relevanter Aspekt, welcher an dieser Stelle erwähnt werden muss ist, dass zu diesem Zeitpunkt sämtliche Bereiche, welche mit erheblichem Integrationsaufwand verbunden sind, nicht berücksichtigt wurden. Insofern wurden weder die Transportunternehmen zur Verfolgung der tatsächlichen Ware, noch der Finanzfluss, welcher die Mitarbeit eines Finanzdienstleisters benötigt, berücksichtigt. Beide Bereiche sind in Abhängigkeit des Konzepts ein relevanter Teil der angestrebten Plattform, jedoch befindet sich die Applikation im Stadiums eines Prototyps. Denn der Integrationsbestandteil einer Blockchain-Applikation wird insbesondere dann relevant, wenn in den operativen Modus gewechselt wird. In den Unterkapitel 8.4.1 bis 8.4.5 werden die Funktionen der Label-Chain anhand der unterschiedlichen Teilnehmer der Blockchain-Applikation erläutert. Die Erklärungen sind in Textform und mit jeweiligen Code Ausschnitten (Code Snippets) ergänzt worden. Beim beschriebenen Stand des Prototyps wurden die zentralen Rollen von Teilnehmern und deren Funktionen abgebildet, weitere Teilnehmer und zusätzliche Funktionen müssen in zukünftigen Forschungsprojekten aufgebaut werden.

Die Hauptaktivität 4 wird gemäss Peffers et al. (2007, S. 55) als eine Demonstration des Artefakts bezeichnet, in welcher gezeigt wird, wie eine oder mehrere Instanzen des identifizierten Problems gelöst werden können. Dies kann in einer Simulation, einer Case Study, einem Experiment oder einer anderen angemessenen Aktivität geschehen. In der Hauptaktivität 5 nach Peffers et al. (2007, S. 56) wird eine Evaluation durchgeführt, in welcher beobachtet oder gemessen wird, wie erfolgreich das kreierte Artefakt das identifizierte Problem löst. Diese beiden Aktivitäten wurden in der Master Thesis leicht modifiziert und folgendermassen aufgeteilt: Im Kapitel 7.5.1 wird erklärt, wie die Blockchain Applikation mithilfe des REST-Servers verwendet werden oder an einem Fachpublikum präsentiert werden kann. Diese Komponente könnte auch mit der Erweiterung eines anwenderfreundlichen Front-end verwendet werden, um interessierte oder potenzielle Stakeholder für den Aufbau eins gemeinsamen Konsortiums zu überzeugen. Für die Master Thesis diente der REST-Server als Schnittstelle zum Testen des konzipierten Netzwerks. Mithilfe des Postman Tools konnten unterschiedliche HTTP-Anfragen an den REST-Server gemacht werden, um die einzelnen Funktionen zu testen. Zusätzlich konnte mithilfe der Docker-

Logs konnte anschliessend das Resultat dieser Anfragen präziser analysiert werden. Jedoch stellte sich diese Methode zur Evaluierung der Applikation aus verschiedenen Gründen als schwerfällig und unzureichend heraus. Beispielsweise war das Testen der einzelnen Funktionalitäten und der jeweiligen Rollen (Teilnehmer) umständlich, worauf auf ein erweitertes Test-Framework zurückgegriffen wurde. Das verwendete Test-Framework Mocha.js wird im Kapitel 7.5.2 erläutert. Dazu gehören auch sämtliche geschriebenen Testfälle, welche für die Evaluierung und die Entwicklung des Label-Chain Prototyps verwendet wurden. Insgesamt wurden 25 unterschiedliche Testfälle geschrieben, wobei alle kurz beschrieben werden und teilweise mit entsprechen Code Ausschnitten ergänzt werden. Die Diskussion zu den erhaltenen Resultaten der Testfälle und der Umsetzung der Label-Chain wird im Kapitel 8.2 geführt.

5.5 Diskussion & Fazit

In diesem Methodenkapitel wird beschrieben, wie der Schluss der Master Thesis aufgebaut ist. Die letzte Hauptaktivität 6 gemäss Peffers et al. (2007, S. 56) ist die Kommunikation nach der Erstellung und Evaluierung eines Artefaktes. In dieser Aktivität muss das Problem und dessen Relevanz sowie die Lösung durch den Einsatz des Artefakts kommuniziert werden. Gemäss dem Information System Research Framework nach Hevner et al. (2004, S. 80 ff.) werden die Ergebnisse der «Knowledge Base» hinzugefügt, sodass zukünftige Projekte oder Forscher von den gesammelten Erfahrungen profitieren können.

Im Kapitel 8.1 wird der gesamte Prozess und die Ergebnisse der Use Case Erarbeitung (Kapitel 6) diskutiert. Dies bedeutet, es wird eine Wiederholung der Hauptresultate auch im Hinblick zur Forschungsfrage sowie eine kritische Diskussion geführt. Des Weiteren wird auf mögliche Generalisierungen hingewiesen und Handlungsempfehlungen abgegeben. Dazu gehören Hinweise für zukünftige Forschungsarbeiten und Unternehmen, welche ein Blockchain-Projekt durchführen möchten. Anschliessend wird dieser Prozess identisch für das Kapitel «Umsetzung der Label-Chain» (7) durchgeführt.

Der Schluss der Arbeit bildet das Fazit, in welchem eine Kurzzusammenfassung über das gesamte Master Thesis Projekt gegeben wird. Zusätzlich wird auf mögliche Implikationen dieser Arbeit hingewiesen.

6 Definition Use Case

In diesem Kapitel wird der Use Case und das Konzept für die Entwicklung des Blockchain-Prototyps definiert. Das Ziel ist es einen möglichst realen Anwendungsfall zu definieren, um das Potenzial der Blockchain-Technologie zu erforschen und die Rahmenbedingungen und die Auswirkungen auf die Organisation zu ergründen.

6.1 Die Bio Suisse

Die «Bio Suisse Vereinigung» ist eine Schweizer Biolandbau-Organisation (nachfolgend Bio Suisse) und Eigentümerin der Marke «Knospe» (Bio Suisse, o.J.a). Der Dachverband wurde 1981 gegründet und die Knospe ist das Verbandslogo, mit welchem die Mitgliederbetriebe ihre Produkte kennzeichnen (Bio Suisse, o.J.a). Die Bio Suisse ist gemäss den gültigen Statuten (ab 01.01.2018) ein Verein nach Art. 60 ff. ZGB (Bio Suisse, 2017b, S. 4). Der Zweck dieses Vereins ist die Förderung des biologischen, bzw. ökologischen Landbaus, also eine umwelt-, tier- und menschengerechte Anbauweise (Bio Suisse, 2017b, S. 4). Die Bio Suisse bezweckt die Förderung von Angebot und Nachfrage von biologischer Produktion, besonders mit Fokus auf die Schweiz (Bio Suisse, 2017b, S. 4). Die eigene Kollektivmarke (Knospe) wird von Bio Suisse verwaltet, entwickelt, geschützt und auf die rechtmässige Verwendung durch Mitglieder, Produzenten, Lizenznehmer und Markennutzer überprüft (Bio Suisse, 2017b, S. 4). Des Weiteren werden die Richtlinien für die Erzeugung, die Verarbeitung, den Handel, den Import und die Vermarktung der Knospe-Produkte von Bio Suisse erarbeitet und kontrolliert (Bio Suisse, 2017b, S. 4).

Gemäss der Jahresbericht-Webseite für das Jahr 2016 sind 6144 Knospe-Landwirtschaftsbetriebe in der Schweiz und Lichtenstein registriert (Bio Suisse, 2017b). Dies entspricht einer Netto-Zunahme von 113 Biobetrieben, welche gesamtschweizerisch betrachtet auf einen Anteil von 13,2 % kommen (Bio Suisse, 2017b). Alle Bio Suisse-Betriebe müssen streng nach den Richtlinien arbeiten, welche dieses Jahr weiter verschärft wurden (Bio Suisse, 2017b). Beispielsweise hat die Delegiertenversammlung beschlossen, dass die Reservenantibiotika nur noch im Ausnahmefall eingesetzt werden dürfen (Bio Suisse, 2017b).

Bei der Bio Suisse sind insgesamt 885 Lizenznehmer registriert (Stand: Jahresende 2016) (Bio Suisse, 2017b). Lizenznehmer sind typischerweise verarbeitende Betriebe, Händler oder Importeure von Nahrungsmittel, die nach Bio Suisse-Richtlinien innerhalb und ausserhalb der Schweiz herstellen (Bio Suisse, 2017c). Diese Lizenznehmer müssen zusätzliche Aufwände für

die Bioproduktion erbringen, wie beispielsweise der Verzicht auf unnötige Verarbeitungsschritte oder die Beachtung einer möglichst schonenden Herstellung der Lebensmittel. Konkret ist der Gebrauch von zusätzlichen Vitaminen, Aroma- oder Farbstoffen für Knospe-Produkte nicht zugelassen (Bio Suisse, 2017b). Insgesamt sind bei Bio Suisse-Produkten nur 40 Zusatzstoffe erlaubt. Dies ist verglichen mit konventionellen Produkten, bei welchen über 400 zugelassen sind, eine beschränktere Auswahl an Zusatzstoffen (Bio Suisse, 2017b). Des Weiteren dürfen für die Knospe-Produkte keine chemische Verarbeitung, keine Bestrahlung, keine Mikrowellenbehandlung und keine gentechnisch hergestellten Zusatzstoffe verwendet werden (Bio Suisse, 2017b).

Die Bio Suisse hat im Jahre 2016 Einnahmen von insgesamt 14‘425'125 Schweizer Franken erzielt (CHF) (Bio Suisse, 2017c). Über neun Millionen stammen von den Lizenz- und Markennutzungsgebühren, somit werden 62,7 % der Gesamteinnahmen der Bio Suisse von den Lizenznehmern für die Verwendung der Marke «Knospe» erbracht (Bio Suisse, 2017c). Die Lizenznehmer bezahlen umsatzabhängige Gebühren an Bio Suisse. Auch Markennutzungsgebühren müssen bezahlt werden, diese sind als Ausgaben von Unternehmen zu verstehen, welche Knospe-Produkte einsetzen oder diese zu Kommunikationszwecken verwenden (Bio Suisse, 2017c). 3,58 Millionen Schweizer Franken (24.8 % der Gesamteinnahmen) werden durch die Produzentenbeiträge eingenommen (Bio Suisse, 2017c). Diese bestehen aus jährlichen Mitgliederbeiträgen von 100 Franken und variablen Abgaben pro Anbauflächen oder Grossvieheinheiten (Bio Suisse, 2017c). Des Weiteren erhält die Bio Suisse Gelder vom Verband für Schweizer Milchproduzenten, welche von den Biobauern einbezahlt werden (Bio Suisse, 2017c). Vom Bund erhält die Bio Suisse weitere 1,17 Millionen CHF (8,1 % der Gesamteinnahmen) für die Unterstützung von Kampagnen und Kommunikationsmassnahmen für die Schweizer Landwirtschaft (Bio Suisse, 2017c). Diese Gelder werden verwendet für die Absatzförderung, das Aufbauen des Images der Marke und die Entwicklung des Schweizer Biomarktes (Bio Suisse, 2017c). Die restlichen 600'000 CHF der Gesamteinnahmen setzten sich aus Anzeigen und Abonnementsverkäufen des Magazins «Bioaktuell» zusammen oder von Fonds für Nachhaltigkeit der Coop Genossenschaft (Bio Suisse, 2017c).

Gewisse Prozesse und Funktionsweisen der Systeme von Bio Suisse sind öffentlich zugänglich, wie beispielsweise der Bio Suisse «Supply-Chain-Monitor» (siehe Abbildung 3). Diese Grafik zeigt auf einem abstrahierten Level, wie ein Exporteur (letzter finanzieller Eigentümer ausserhalb der Schweiz) Güter in die Schweiz liefern kann, respektive diese einem Schweizer Importeur übergeben kann (Bio Suisse, o.J.b). Zusätzliche und detailliertere Informationen zu den Prozessen

und Handelspartner konnten in einem gemeinsamen Workshop erarbeitet werden (vgl. Anhang A, 2018). Beispielsweise wurden im Workshop sämtliche Parteien in der Supply-Chain von Bio Suisse beschrieben und deren konkrete Aufgabe diskutiert (vgl. Anhang A, S. 1 ff., 2018). Eine detaillierte Analyse dieser Unterlagen wird in der konkreten Erstellung des Artefakts vorgenommen.

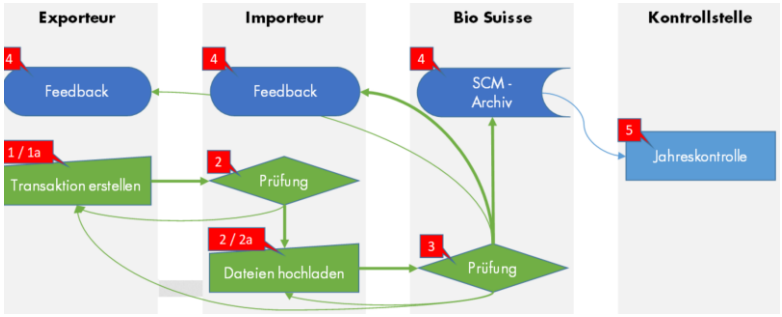

Abbildung 3: Dokumentfluss mit dem Bio Supply Chain Monitor (Bio Suisse, o.J.b)

6.2 Problemidentifikation

In diesem Kapitel werden die gesammelten Daten (Anhang A, 2018) hinsichtlich der relevanten Probleme der Organisation untersucht. Dieses Kapitel bildet somit die Grundlage zur Zielsetzung und Konzeption des Artefakts. In Zusammenarbeit mit dem Verantwortlichen der Supply-Chain für Bio Suisse wurden im Rahmen des Workshops folgende Problembereiche identifiziert (Anhang A, 2018, S. 9): *Die physische Rückverfolgbarkeit* der Güter, welche von Bio Suisse zertifiziert werden. Aktuell wird bei Bio Suisse nur der finanzielle Fluss der Güter, über den bereits erwähnten «Bio Suisse Supply-Chain-Monitor» (vgl. Abbildung 3) verfolgt, nicht aber die physische tatsächliche Lokation des Transportgutes (Bio Suisse, o.J.b). Insofern können Güter in finanziellem Besitz einer Unternehmung sein, diese können aber die Bearbeitung oder den Transport an unterschiedlichen Subunternehmern oder Vertragspartnern überlassen und es ist nicht transparent, wo sich die Güter befinden. Die Untersuchungen in der Vorstudie haben gezeigt, dass eine durchgängige Sendeverfolgung im Bereich von Produktion und Logistik nicht immer möglich ist (Petersen et al., 2016, S.628). Aufgrund der verschiedenen involvierten Paketdienstleister, Kooperationspartner, Subunternehmer und Zollbehörden, welche bei einem Warenaustausch beteiligt sind, ist die Rückverfolgbarkeit nicht gegeben (Petersen et al., 2016, S.628). Diese Situation trifft aktuell auch bei der Bio Suisse zu. Eine weitere damit verbundene Schwierigkeit ist *die Trennung vom physischen und finanziellen Warenfluss* (Anhang A, 2018, S. 8 f.). In einer anzustrebenden Lösung sollte ein Artefakt kreiert werden, bei welchem die beiden Informationsflüsse (physisch & finanziell) abgebildet werden können. Zusätzlich werden aktuell nur Güter, welche in die Schweiz importiert werden über den Bio Suisse Supply-Chain-Monitor

verfolgt. Die anzustrebende Lösung sollte unabhängig vom Ursprungsland sein und auch den Güterfluss in der Schweiz abbilden.

Ein weiterer Risikobereich ist *die erste Meile und der systematische Betrug* (Anhang A, 2018, S. 9). Der Verantwortliche der Bio Suisse Supply-Chain sieht die Gefahr beim Betrug bei der Erfassung einer Charge, respektive bei der ersten Transaktion. Die erfasste Transaktion muss grundsätzlich bei der Kontrollstelle angemeldet werden und es werden Stichproben der Produkte geführt. Jedoch können kleine Mengen von nicht zertifizierten Produzenten, welche mit Knospe-zertifizierter Ware gemischt werden, kaum erkannt werden. Die wirtschaftlich grösste Gefahr für Bio Suisse geht aber von grossen Mengen einer Importware aus. Der Schaden von grossen Mengen fälschlicher zertifizierte Ware könnte für das Label zu einem starken Imageschaden führen. Beispielsweise gab es im Jahr 2011 einen Skandal, welchen auch den Schweizer Biomarkt betroffen hat (Schürer & Kressbach, 2012). Im Zentrum des Skandals war das Unternehmen «Sunny Land», welches in Italien einen mutmasslichen systematischen Grossbetrug begangen hat, indem konventionelle Ware fälschlicherweise als «Bio» deklariert wurde (Schürer & Kressbach, 2012). Dieser Skandal führte auch ehemalige jahrelange Mitglieder wie der Biobauer Markus Lanfranchi dazu, den Verein zu kritisieren, wie aus der Berichterstattung der NZZ ersichtlich ist (Bracher, 2013). Der Biobauer bemängelt, dass durch die geführte Wachstumspolitik und den wachsenden Import-Anteil die ursprüngliche Idee des biologischen Landbaus vergessen geht (Bracher, 2013). Auch der Biobauer Armin Capul, welcher sich für Kühe und Ziegen mit Hörnern einsetzt, hat sich aus dem Bio Suisse Verein zurückgezogen (Bracher, 2013). Er kritisiert das Importgeschäft und es wurde ihm von einem Delegierten von Bio Suisse gesagt, dass keine exakte Zahl eruiert werden kann, als er diesen auf den Anteil ausländischer Biowaren angesprochen habe (Bracher, 2013). Tatsächlich gibt es auch heute keine präzisen Zahlen zum Verkauf von Biowaren in der Schweiz, was im Workshop unter der Thematik Datenverfügbarkeit diskutiert wurde (Anhang A, 2018, S. 9). Ein weiterer Kritikpunkt an Bio Suisse stammt vom Biobauer Markus Ritter: er bemängelt unter anderem die Kontrollen und die Anerkennung der verschiedenen Standards zwischen der Schweiz und anderen Länder (Bracher, 2013). Denn die unterschiedlichen Standards der verschiedenen Länder würden gemäss dem Äquivalenzprinzip anerkannt, auch wenn diese nicht vergleichbar seien und die Kontrollen zu nachlässig durchgeführt werden, argumentiert Ritter (Bracher, 2013). Auch Daniel Imhof, ein Kantonschemiker, welcher Proben von Lebensmitteln vornimmt, geht davon aus, dass die Kontrollen im Inland gut funktionieren, zweifelt aber an Kontrollsystemen im Ausland (Breitinger, 2012, S. 8). Je weiter weg die Biowaren produziert werden, desto weniger sei das Gut kontrollierbar (Breitinger, 2012, S. 8). Im internationalen Biohandel genügten Papierkontrollen

nicht, es brauche mehr unangekündigte Kontrollen vor Ort, artikuliert der Kantonschemiker Imhof (Breitinger, 2012, S. 9). Deshalb rät die Betrugsexpertin Beate Huber beim Biobauern in der Nähe einzukaufen oder bei Produzenten, welche die volle Rückverfolgbarkeit anbieten, bspw. über «bio-inspecta.ch» oder über «bio-mit-gesicht.de» (Breitinger, 2012, S. 9).

Die angesprochene Problematik der teilweise *fehlenden internationalen Transparenz* und dem *Kontrollverlust* wurde auch im Workshop diskutiert (Anhang A, 2018, S. 9). Eine Manipulation für den unrechtmässigen Verkauf von grossen Mengen ist am ehesten möglich, wenn ein komplettes Netzwerk von Bauer und Kontrollstellen sich am Betrug beteiligen. Dass dies eine reale Gefahr ist, zeigt das erwähnte Beispiel der italienischen Firma Sunny Land. Die Bio Suisse macht darauf aufmerksam, dass ausländische Betriebe regelmässig kontrolliert würden und dies den ebenso strengen Vorschriften wie der Schweiz entspricht (Bracher, 2013). Des Weiteren komme es immer wieder zur Aberkennung der Knospe: Im Jahr 2011 waren es 55, im Jahre 2012 wurden 61 ausländischen Betrieben das Gütesiegel entzogen (Bracher, 2013). Bio Suisse habe auch die Risikobeurteilung von Lieferanten verfeinert und systematisiert, hält die Bio Suisse Sprecherin Sabine Lubow fest (Bracher, 2013). Anhand des Vorfalls mit dem involvierten italienischen Unternehmen «Sunny Land» kann festgestellt werden, wie zentral das Vertrauen in die Knospe für Bio Suisse ist. Bei Unregelmässigkeiten, ungenügenden Kontrollmechanismen und intransparenter Supply-Chain kann in kurzer Zeit ein grosser Image-Schaden für die Marke entstehen. Das Vertrauen in die Marke, die Zulieferer, die Partner und die Zertifizierungsstellen scheint für die Bio Suisse eine hochrelevante Thematik zu sein.

6.3 Ziel und Konzeptionsbildung

Aus den behandelten Problemfeldern im vorherigen Kapitel werden nun Konzepte erstellt, welche die geschilderte Situation verbessern könnten. Eine weitere Grundlage sind die erhaltenen Angaben zu den beteiligten Stakeholdern, welche in der Supply-Chain der Bio Suisse involviert sind (Anhang A, 2018, S. 1). Die behandelten Herausforderungen wurden in Zielsetzungen und mögliche Konzepte unterteilt.

6.3.1 Entwurf von Blockchain-Applikationen

Der erste Entwurf (Label-Blockchain, Abbildung 4) wurde von den folgenden identifizierten Problemen abgeleitet: *Die physische Rückverfolgbarkeit, die Trennung vom physischen und finanziellen Warenfluss, die fehlende internationale Transparenz und die Datenverfügbarkei*t. Das Ziel dieses vorgeschlagenen Konzepts ist eine Supply-Chain-Applikation, mit welcher die

drei genannten Probleme behoben werden sollte. Es wird ein Konzept vorgeschlagen, bei den sämtlichen Parteien der Supply-Chain ihre Transaktionen in die Blockchain schreiben. Der Vorteil dieser Lösung wäre, dass ein dezentrales System über die ganze Supply-Chain von verschiedenen Label / Organisationen läuft und alle Supply-Chain-Prozessschritte komplett Rückverfolgbar sind (Zertifizierung, Kontrolle, Produktion, Verarbeitung, Transportwege). Keine Organisation wäre in kompletter Kontrolle der Daten und abhängig von der Konsortiumsbildung könnten die Teilnehmer nach Belieben ein- und austreten. Des Weiteren könnte mit diesem Konzept auch ein Teil einer Handelsplattform angestrebt werden, indem Händler die produzierte Ware der Bauern über die Blockchain-Applikation kaufen könnten. Das Ziel der Label-Blockchain ist, die Umsatzzahlen der Labels zu erhöhen, das gesamte Supply-Chain-System zu optimieren und das Vertrauen in die Labels zu stärken.

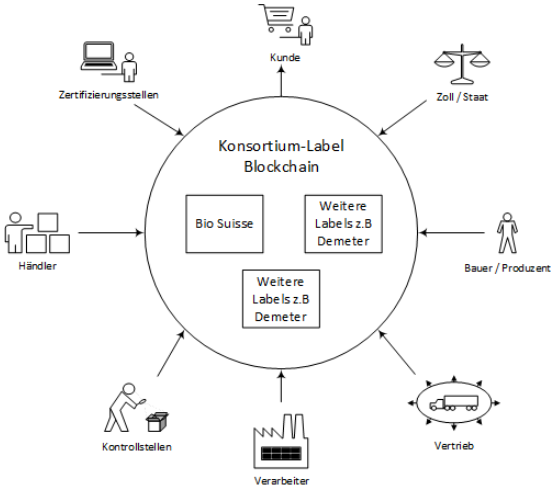

Abbildung 4: Entwurf Label-Blockchain (Eigene Darstellung, 2018)

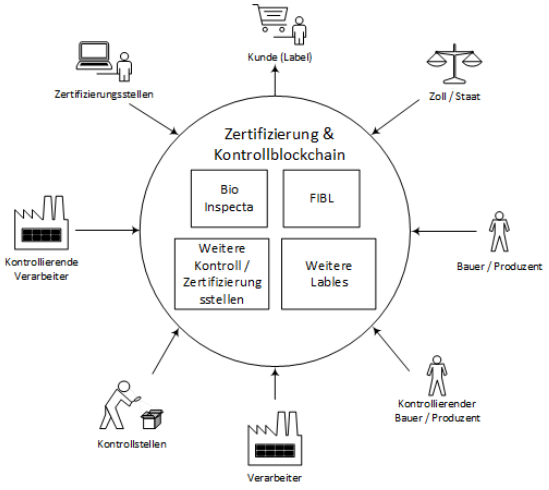

Abbildung 5: Entwurf Zertifizierungs- & Kontroll-Blockchain (Eigene Darstellung, 2018)

Der zweite Entwurf (Zertifizierungs- und Kontroll-Blockchain, Abbildung 5) wurde aus den folgenden identifizierten Problemen abgeleitet: *die erste Meile, der systematische Betrug und dem Kontrollverlust.* Das Ziel des vorgeschlagenen Konzepts ist es, die Zertifikate und Kontrolle über eine Blockchain-Applikation zu erweitern und zeitgleich eine Optimierung anzustreben. Das Konsortium könnte aus Zertifizierungsdienstleister (bspw. Inspecta) und Labels gebildet werden. Die Idee ist es, neben den herkömmlichen Kontroll- und Zertifizierungssystemen eine weitere Kontrollinstanz einzubinden. Möglich wäre, dass ein Bauer aus einer anderen geographischen Lokation einen anderen Biobauern überprüft. Analog würden die Lizenznehmer die Konkurrenz kontrollieren, respektive von dieser überprüft werden. Das Ziel dabei ist, das Risiko von systematischem Betrug von Netzwerken aus Bauern, Lizenznehmer und Kontrollsystemen zu minimieren. Denn durch eine eingebaute Kontrolle, von zufällig ausgewählten Parteien aus geographisch fernen Regionen, könnten sich betrügende Netzwerke aus Bauern und

Lizenznehmer nur erschwert durchsetzen. Des Weiteren hätten alle beteiligten Parteien Einsicht in die Ablage der Zertifikate in einer dezentralen Applikation, bei welcher keine Institution die gesamte Kontrolle über das System besitzt. Mit diesem Konzept soll zukünftigem Betrug vorgebeugt werden und das Vertrauen in die Labels und Zertifizierungsstellen gesteigert werden.

6.3.2 Stakeholderanalyse

Um die vorgeschlagenen Konzepte präziser zu untersuchen, wird in diesem Kapitel eine Stakeholderanalyse durchgeführt. Bei einer dezentralen Anwendung ist es bedeutend, die Interessen der verschiedenen möglichen involvierten Parteien zu beurteilen. Deshalb wurde eine Vorgehensweise ausgewählt, bei welcher die unterschiedlichen Absichten untersucht werden können. Das Konzept der Stakeholder wurde in Verbindung mit dem strategischen Management von Freeman erstmals im Jahre 1984 wie folgt definiert: Das Konzept der Stakeholder setzt sich zusammen aus einer Gruppe von Personen oder Individuen, welche eine Zielerreichung einer Organisation beeinflussen oder von deren beeinflusst werden können (Freeman, 2010, S. 52). Für die Master Thesis wurde nach Literatur gesucht, welche für die Analyse von Stakeholdern bei Projekten angewandt wird. Der Hauptzweck einer Stakeholderanalyse im Projektumfeld ist derjenige, die Projektmanager zu einem zeitgemässen handeln zu befähigen, welches im Sinne der Projektstakeholder und deren Interessen ist (Jepsen & Eskerod, 2009, S. 341). Eine weitere zentrale Prämisse des Projektstakeholder-Managements ist, dass Projetmanager über limitierte Ressourcen verfügen und diese Ressourcen so nutzen sollten, um die bestmöglichen Ergebnisse zu erzielen (Jepsen & Eskerod, 2009, S. 336). Dieser Leitsatz trifft auch auf die Master Thesis zu, da der Prozess des zu kreierenden Prototyps die Basis für die zu gewinnenden Erkenntnisse dieser Arbeit bilden. Die Stakeholder Analyse wird gemäss Jepsen & Eskerod (2009, S. 336) in folgenden drei Schritten durchgeführt:

1. Identifikation der (relevanten) Stakeholder (Jepsen & Eskerod, 2009, S. 336).
2. Charakterisierung der Stakeholder hinsichtlich deren (a) notwendigen Beitragsleistungen, (b) der erwarteten Vorteile, wegen ihren geleisteten Bemühungen und (c) deren Macht in Bezug auf das Projekt (Jepsen & Eskerod, 2009, S. 336).
3. Entscheidung welche Strategie anzuwenden ist, um die jeweiligen Stakeholder zu beeinflussen (Jepsen & Eskerod, 2009, S. 336).

Die Resultate der Analyse werden anschliessend in einer Tabelle anlehnend an Andersen, Grude, & Haug, (2009, S. 45) aufgezeigt (siehe Abbildung 6).

Stakeholder	Area of interest	Contri-butions	Expecta-tions	Power	Strategy	Respon-sible

Abbildung 6: Beispieltabelle für Stakeholderanalyse (Andersen et al., 2009, S.45)

Um die beiden Konzepte hinsichtlich der Interessen der Stakeholder zu untersuchen, wurden Annahmen getroffen und keine Interviews oder Befragungen durchgeführt, um dem vorgegeben Umfang der Master Thesis gerecht zu werden. Nur die Perspektive von Bio Suisse wurde mit dem Supply-Chain-Verantwortlichen im Rahmen einer Videokonferenz festgelegt (Anhang B, 2018). Des Weiteren gab Bio Suisse Angaben zur Einschätzung der restlichen Stakeholder (Anhang B, 2018). Der erste Schritt, die Identifikation der beteiligten Stakeholder, erfolgte über die gesammelten Unterlagen während des Workshops (Anhang A, 2018, S. 1 f.). Eine Trennung zwischen Exporteur und Importeur, respektive internationalem und Schweizer Handel wurde nicht gemacht. Denn grundsätzlich sollten die Stakeholder möglichst identisch behandelt werden, unabhängig von der geographischen Lokation (ausgenommen von der Zollkontrolle). Des Weiteren wurden die Interessengebiete der Stakeholder hinsichtlich des Projektes hinzugefügt (Andersen et al., 2009, S. 44). Die Spalte für die zuständige Person wurden in dieser konzeptionellen Phase noch nicht berücksichtigt. Das Ergebnis dieses Prozesses ist in den folgenden Tabellen ersichtlich (siehe Tabelle 2 & 3)

Für die Planung der anzuwendenden Strategie auf die verschiedenen Stakeholder wurde die «Macht / Interessen Matrix» verwendet (siehe Abbildung 7). Dies ist ein Instrument zur Klassifikation der Stakeholder in Relation zu deren Macht und Interesse bezüglich des Projekts (Newcombe, 2003, S. 844). Die Art der Interaktion der Projektleiter mit den Stakeholdern ist abhängig von deren Einfluss und Interesse am Projekt (Newcombe, 2003, S. 844). Deshalb werden die Stakeholder in die vier unterschiedlichen Zonen eingeteilt. Somit können passende Strategien für jeden einzelnen entworfen werden. Die Stakeholder sollten auch während des Projektes aktiv überwacht werden, da beispielsweise die Projektziele oder der Projektumfang laufend ändern können, wodurch eine Repositionierung der Stakeholder zu beobachten ist (vgl. Newcombe, 2003, S. 845).

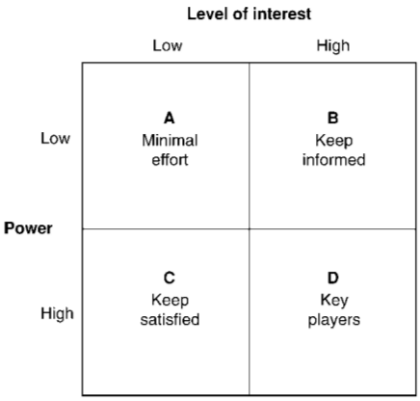

Abbildung 7: Macht / Interessen Matrix (Newcombe, 2003, S. 844)

Tabelle 2: Stakeholderanalyse «Label-Blockchain»

Stakeholder	Interessenbereiche	Beiträge	Erwartungen	Macht	Strategie
Bio Suisse (oder andere Labels)	Rückverfolgbarkeit der Güter, Finanzen sowie der Zertifikate, höhere Sicherheit, Transparenz und grösseres Vertrauen in Label	Entwicklungs- & Betriebskosten der Applikation, Marketingkosten & Aufwände für Blockchain-Projekt	Ein System für die gesamte Supply-Chain, Finanz- sowie Warenfluss;	Grosse Machtausübung, Key-Player	Zusammenarbeit mit allen Labels anstreben
Bauern (Produzenten)	faire (Schweizer) Bio Produkte, positives Bio-Image; neue mögliche Abnehmer über Handelsplattform, grössere Absatzmarkt, wenig Administrationsaufwand	Einarbeitungskosten und evtl. zusätzliche Arbeitsschritte für das neue System	Verkauf an neue Händler / Lizenznehmer, mehr Transparenz und Vertrauen in Label	Macht über Verein (bei Bio Suisse), Keep-satisfied	Praxistaugliches System in enger Zusammenarbeit entwerfen
Lizenznehmer (bspw. Händler / Verarbeiter)	neue potenzielle Lieferanten, Vertrauen in Label, Reduktion Administrationskosten, Prozesseffizienzsteigerung	Beitragskosten Handelsnetzwerk, Einarbeitungskosten und evtl. zusätzliche Arbeitsschritte für das neue System	Neue potentielle Lieferanten, mehr Vertrauen in Label,	Mittel -starke Machtposition, keep-satisfied	Praxistaugliches System, möglichst simple Integration mit bestehenden Systemen anstreben
Kontrollen- / Zertifizierungsstellen	erhöhte Kontrollfunktion, mehr Sicherheit gegen Betrug, möglicher Konflikt (Kontrollschritte, respektive Teilaufgaben könnten entfallen)	Einarbeitungskosten und evtl. zusätzliche Arbeitsschritte für das neue System	Effizienzsteigerung und trotzdem keinen Umsatzverlust, mehr Transparenz,	Mittel-geringe Machtposition, keep-informed	möglichst simple Integration mit bestehenden Systemen anstreben
Verteilzentren, Grosshändler & Einzelhändler	Umsatzsteigerung, Vertrauen in Labels, korrekte Informationen über Produkte	evtl. marginaler Aufpreis & Integration des neuen Systems	erhöhtes Vertrauen & Transparenz in Produkte des Labels, Effizienzsteigerung	Zentrale Absatzfunktion für ein Label, mittlere Machtposition, keep-informed	Kommunikationsstrategie & Marketingkampagne gemeinsam definieren

Zoll (Staat)	Verlässlichkeit der Daten, korrekte Deklarierung der Importe und kürzere Prozessabwicklungszeit	Einarbeitungskosten und evtl. zusätzliche Arbeitsschritte für das neue System	Effizienzsteigerung, hohe Datenqualität, verringerung Kontrollintensität	Mittlere Machtposition, keep-informed	Früh beim Projektstart Kontakt aufnehmen, rechtliche Normen / Gesetzte einhalten
Endkunde / Verbraucher	Vertrauen in Produkt und Label, der tatsächliche Inhalt entspricht der deklarierten Ware	evtl. marginaler Aufpreis	erhöhtes Vertrauen & Transparenz in Produkte des Labels	Geringe Machtposition, minimal effort	Kommunikation dann aufnehmen, wenn Projektfortschritt vielversprechend ist
Vertrieb / Logistik	Rückverfolgung der Ware, Nachweisbarkeit bei Disputen, keine zusätzlichen ungedeckten Kosten	Integration in bestehende operative Systeme, einarbeitungskosten Mitarbeiter	Risikominimierung, Effizienzsteigerung	Geringe Machtposition, minimal effort	Kommunikation dann aufnehmen, wenn Projektfortschritt vielversprechend ist

Tabelle 3:Stakeholderanalyse «Kontroll- und Zertifizierungs-Blockchain»

Stakeholder	Interessenbereiche	Beiträge	Erwartungen	Macht	Strategie
Bio Suisse (oder andere Labels)	Rückverfolgbarkeit der Zertifizierung; höhere Sicherheit, und grösseres Vertrauen in Label	Entwicklungs- & Betriebskosten der Applikation, Marketingkosten & Aufwände für Blockchain-Projekt	Ein System mit zusätzlichen Kontrollmechanismen zur Vorbeugung gegen Betrug	Grosse Machtausübung, Key-Player	Zusammenarbeit mit ähnlichen Labels anstreben
Bio.inspecta (andere Zertifizierungs- und Kontrollstellen)	Betrugsfälle der eigens zertifizierten und kontrollierten Bauern reduzieren, keine Umsatzeinbussen durch neues Zertifizierungskonzept-> daher mögliche gemeinsame Erarbeitung eines neuen Business Modells, Mehr Aufträge durch Wachstum des Labelmarkts	Einarbeitungskosten und evtl. zusätzliche Arbeitsschritte für das neue System	Aufbau eines effektiven Systems und Betrugsfälle minimieren, Effizienzsteigerung, mehr Transparenz	Mittlere -grosse Machtausübung, Key-Player	Zusammenarbeit mit vielen Zertifizierungsstellen anstreben, simple Integration in bestehende operative Systeme

Bauern (Produzent & Kontrolleur)	Faire (Schweizer) Bio Produkte, positives Bio-Image, mehr Vertrauen in Bio Suisse, Entschädigung für Kontrollfunktion	Arbeitsstunden für Kontrollfunktion, Einarbeitungskosten und evtl. zusätzliche Arbeitsschritte für das neue System	Mehr Transparenz und Vertrauen in Label, mehr Wertschätzung für die Produkte	Macht über Verein (bei Bio Suisse), Keep-satisfied	Praxistaugliches System in enger Zusammenarbeit entwerfen, enge Kooperation für Kontrollkonzept
Lizenznehmer Händler / Verarbeiter (Produzent & Kontrolleur)	Mehr Sicherheit / Vertrauen für die geleisteten Beiträge an Label,	Beitragskosten Handelsnetzwerk, Einarbeitungskosten und evtl. zusätzliche Arbeitsschritte für das neue System	Neue potentielle Lieferanten, mehr Vertrauen in Label und mögliche Umsatzerhöhung	Mittel -geringe Machtposition, keep-informed	Praxistaugliches System, möglichst simple Integration mit bestehenden operativen Systemen anstreben
Endkunde / Verbraucher	Erhöhtes Vertrauen in Produkt und Label	Evtl. marginaler Aufpreis	Erhöhtes Vertrauen & Transparenz in Produkte des Labels	Geringe Machtposition, minimal-effort	Kommunikation dann aufnehmen, wenn Projektfortschritt vielversprechend ist
Evtl. (Staat)	Verlässlichkeit der Daten, höher Sicherheit und Weiterentwicklung der Schweizer Labels,	Einarbeitungskosten und evtl. zusätzliche Arbeitsschritte für das neue System	Effizienzsteigerung, hohe Datenqualität, Verringerung Kontrollintensität	Mittlere Machtposition, keep-informed	Früh beim Projektstart Kontakt aufnehmen, rechtliche Normen / Gesetzte einhalten

6.3.3 Konsortium Varianten

Um die vorgeschlagenen Konzepte präziser zu untersuchen werden nun die verschiedenen Möglichkeiten der Konsortiumsbildung untersucht. Der Begriff «Konsortium» steht für eine meist vorübergehende Vereinigung von Unternehmen, zur Durchführung von gemeinsamen Handels- oder Finanzoperationen (Wirtschaftslexikon24, 2017). Für diese Master Thesis wird unter Konsortium die Vereinigung von unterschiedlichen Organisationen verstanden, welche zusammen eine Blockchain-Applikation entwerfen und anschliessend auch betreiben. Daher wird zwischen Teilnehmern und aktiven Konsortiumsparteien unterschieden. Die Konsortiumsparteien sind für die Entwicklung, Governance und für sämtliche operative Aufgaben zuständig. Zu diesen Aufgaben gehört das zur Verfügung stellen von Rechenleistung, respektive das Betreiben von Nodes, welche für das Netzwerk benötigt werden. Die Teilnehmer ohne Konsortiumsfunktion sind die restlichen Stakeholder, welche die Blockchain-Applikation nutzen können.

In den ausgearbeiteten Varianten des Konsortiums wird die Bio Suisse oder andere Label-Vertreter zwingend miteinbezogen, da die Bio Suisse die exemplarische Schweizer Organisation für die Master Thesis repräsentiert. Des Weiteren werden nur die Stakeholder berücksichtigt, deren Machtposition für ein solches Netzwerk aktuell auf mindestens mittel-gross eingeschätzt wurde. Die restlichen Stakeholder können als Teilnehmer in der Blockchain-Applikation agieren, werden aber für die Gestaltung der Anwendung nur begrenzt miteinbezogen. Die dargestellten Varianten (siehe Tabelle 4) sind eine Kombination aus den beiden Entwurfskonzepten aus den vorherigen Kapiteln.

Tabelle 4: Varianten Konsortium

	Varianten			
Stakeholder	I	II	III	IV
Bio Suisse (oder andere Labels)	x	x	x	x
Bio.inspecta (andere Zertifizierungs- und Kontrollstellen		x		x
Händler / Verarbeiter & Bauern (Produzent & Kontrolleur)			x	x

6.3.4 Business Case

Bei einem Blockchain Use Case, ähnlich wie bei anderen Anwendungsfällen, sollte eine Abwägung für den Business Case durchgeführt werden, wobei Gartner den CIOs Unterstützung bei diesem Vorhaben geben möchte (Kasey Panetta, 2017). Während viele Unternehmen Interesse an der Blockchain-Technologie haben und ihre PoCs vorantreiben, geht es oftmals nicht weiter mit dem Projekt (vgl. Kandaswamy & Furlonger, 2017, S. 2). Gartner schlägt daher in einem Research Note vor, wie Unternehmen ihren Business Case aufstellen können und welche Kosten und Nutzen sie vergleichen sollten (siehe Abbildung 8) (vgl. Kandaswamy & Furlonger, 2017, S. 2 ff.). Neben der Kosten/Nutzen-Analyse sollten auch die Projektrisiken betrachtet werden, wie beispielsweise die Unreife der Blockchain-Technologie oder die aktuell noch fehlenden Standards im rechtlichen Bereich (Kandaswamy & Furlonger, 2017, S. 5 ff.). Des Weiteren wird von Gartner geraten, den Einsatz von Blockchain mit alternativen Technologien zu überprüfen und insbesondere auch das Ökosystem zu betrachten (Kandaswamy & Chesini, 2017). Insofern sollte ein Unternehmen verifizieren, ob es bereits ein mögliches Konsortium existiert, welchem man beitreten könnte oder ob eine Marktführungsposition vorhanden ist, die man entsprechend mit anderen Unternehmen ausnutzen kann (Kandaswamy & Chesini, 2017, S. 2 ff.).

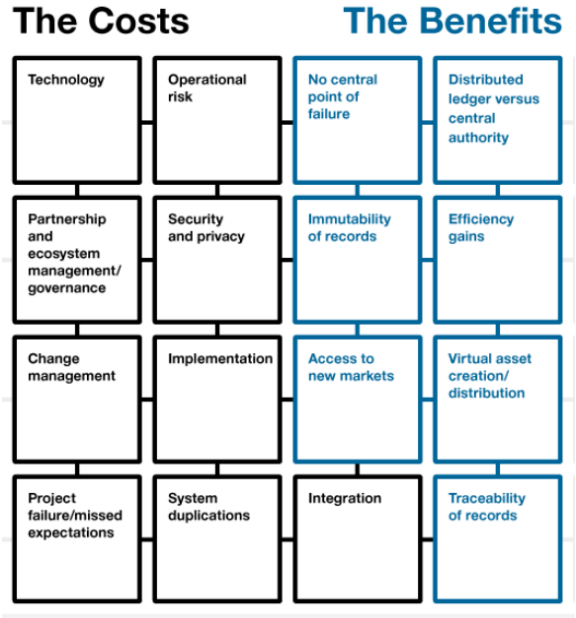

Abbildung 8:See how benefits and costs stack up (Kasey Panetta, 2017)

6.4 Blockchain-Fit

Um die dargestellten Varianten der Konsortiumsbildung auszuwerten, können anhand verschiedener Fragestellungen die einzelnen Optionen geprüft und verifiziert werden. Damit wird überprüft, ob es sich bei den vorgeschlagenen Use Cases um passende Anwendungen der Blockchain Technologie handelt. Diese Merkmale sind generell gültig und nicht für einen spezifischen Typ von Industrie oder Use Case. Gemäss Arnaud Le Hors, einem Mitglied des «Technical Steering Comittee» von Hyperledger (2017), muss für einen Blockchain Use Case in erster Instanz geprüft werden, ob ein Business Problem vorhanden ist, welches nicht mit einer

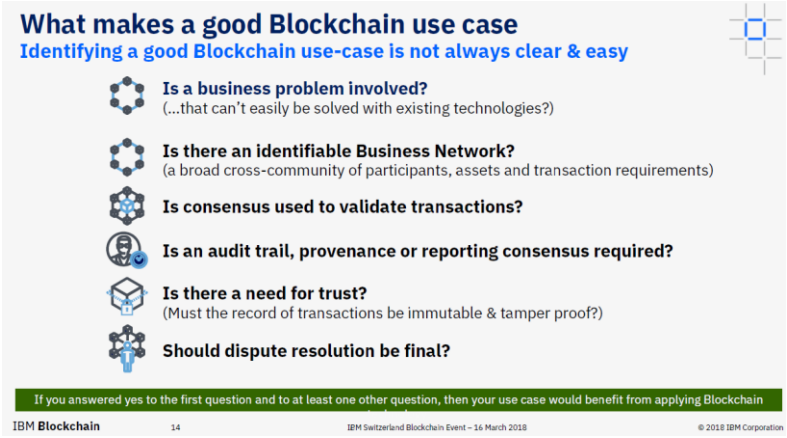

Abbildung 9:What makes a good Blockchain use case (Le Hors, 2018, S. 14)

existierenden Technologie gelöst werden kann (Le Hors, 2018, S. 14) (siehe Abbildung 9). Wenn diese Bedingung zutrifft, müssen weitere Untersuchungen durchgeführt werden. Beispielsweise die Untersuchung, ob ein identifizierbares Business Netzwerk vorhanden ist oder ob das Transaktionsprotokoll unveränderbar und manipulationssicher sein muss (Le Hors, 2018, S. 14). Falls eine dieser Überprüfungen positiv ausfällt, kann von einem möglichen Blockchain-Use Case gesprochen werden (Le Hors, 2018, S. 14).

Auch ein Paper aus dem IEEE Spectrum widmet sich der Thematik, ob die Blockchain als Technologie für den Use Case geeignet ist (Peck, 2017). In einem ersten Schritt wird in diesem Artikel gefragt, ob eine konventionelle Datenbank-Technologie für den Anwendungsfall geeignet ist (Peck, 2017, S. 39) (siehe Abbildung 10). Anschliessend werden gemäss dem Diagramm weitere Fragen gestellt, wie beispielsweise, ob mehrere Teilnehmer Zugriff auf die Daten haben müssen und sich diese Parteien grundsätzlich trauen (Peck, 2017, S. 39). Anhand der Antworten wird eine Empfehlung abgegeben, welche Art von Blockchain für den Use Case eine valide Option ist. Insofern kann der Use Case für eine

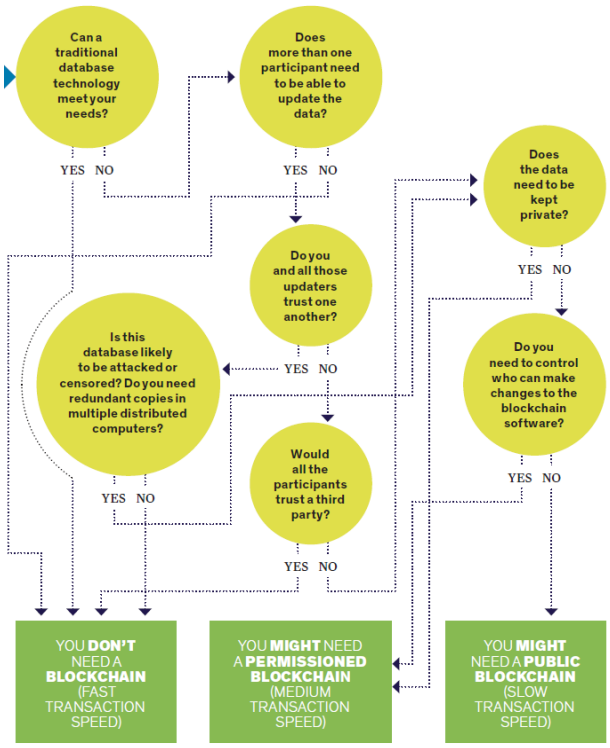

Abbildung 10: Do you really need a Blockchain? (Peck, 2017, S. 39)

«permissioned / public Blockchain» geeignet sein oder aber es wird von der Anwendung einer Blockchain abgeraten (Peck, 2017, S. 38 f.).

Zwei Forscher an der ETH Zürich des Departments für Informatik haben sich in einem Paper ebenfalls der Thematik der sinnvollen Einsatzmöglichkeiten der Blockchain-Technologie gewidmet (Wüst & Gervais, 2017). In diesem Artikel wird ein Diagramm für die Unterstützung des Entscheidungsprozesses über den Einsatz von Blockchain vorgestellt (siehe Abbildung 11). Das Ziel dieses Prozesses ist festzustellen, ob die Blockchain eine angemessene Technologie zur Lösung eines Problems ist (Wüst & Gervais, 2017, S. 2 f.). In einem ersten Schritt wird nach der Notwendigkeit einer Datenspeicherung gefragt und überprüft, ob mehr als ein Teilnehmer in die Blockchain schreiben muss (Wüst & Gervais, 2017, S. 2 f.). Denn für eine Partei ist eine konventionelle Datenbank viel effizienter als eine Blockchain, da eine Datenbank eine viel höhere Performanz in Bezug auf Datendurchsatz und Latenz aufweist (Wüst & Gervais, 2017, S. 2). Anschliessend muss der Einsatz einer online verfügbaren TTP (Trusted Third Party) geprüft werden (Wüst & Gervais, 2017, S. 2 f.). Des Weiteren muss evaluiert werden, ob sich die schreibberechtigten Parteien kennen und Vertrauen zwischen diesen vorhanden ist (Wüst & Gervais, 2017, S. 2). Falls sich die Parteien vertrauen oder eine vertrauenswürdige Drittpartei eingesetzt werden kann, ist der Einsatz einer Datenbank mit gemeinsamem Schreibzugriff einer Blockchain-Lösung vorzuziehen (Wüst & Gervais, 2017, S. 2). Anhand des eben erwähnten Vorgehens kann gemäss dem folgenden Diagramm (siehe Abbildung 11) eine Ausprägung der Blockchain oder eine Verwendung einer anderen Technologie empfohlen werden.

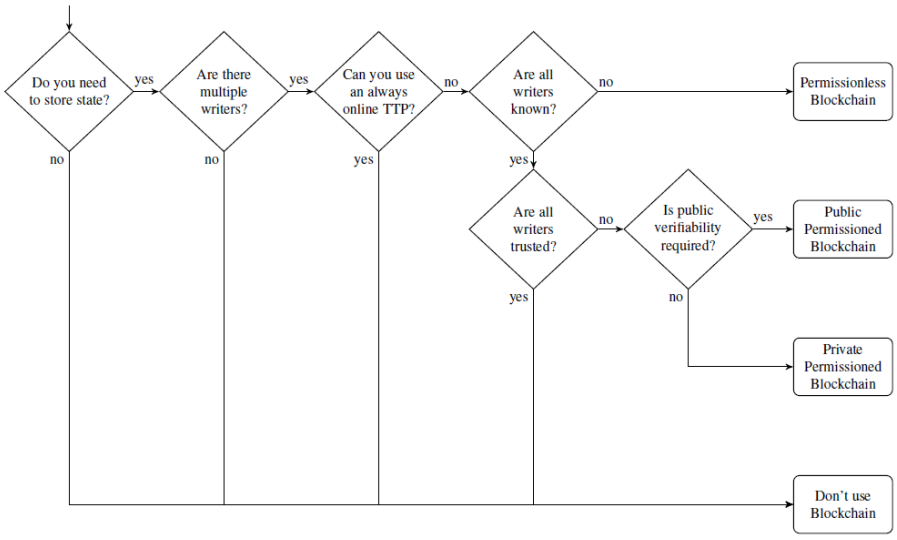

Abbildung 11: Is Blockchain an appropriate technical Solution? (Wüst & Gervais, 2017, S. 3)

Gartner hat im Zusammenhang mit ihrer publizierten Research Note, zur Unterstützung der CIOs für einen Blockchain Business Case, das «Blockchain Decision Framework» entworfen(Kandaswamy & Chesini, 2017). Das zugrundeliegende Prinzip dieses Frameworks ist

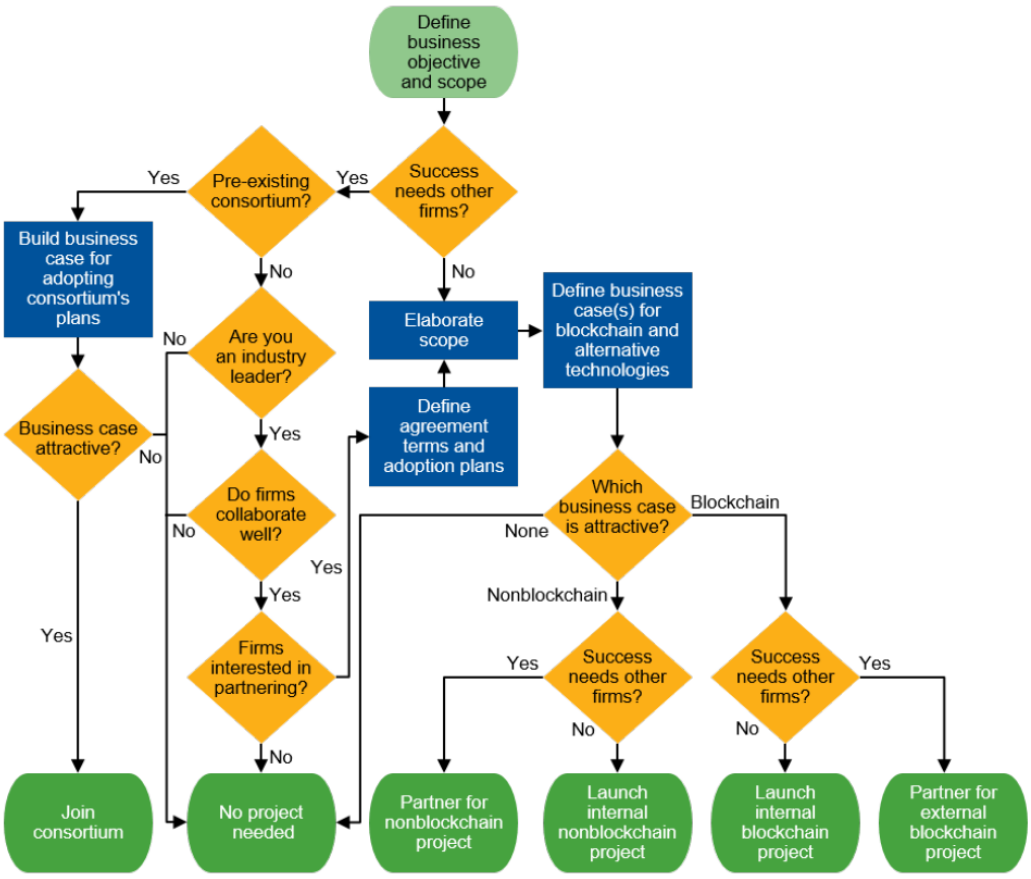

Abbildung 12: Blockchain Decision Framework (Gartner, 2017)

die Rolle der anderen Firmen im Ökosystem zu evaluieren und andere Technologien zu untersuchen, bevor in ein Blockchain-Projekt investiert wird (Kandaswamy & Chesini, 2017, S 3). Abhängig von den Auswertungen wird daher empfohlen, entweder in ein bestehendes Konsortium, in ein internes Blockchain-Projekt oder gar kein Projekt zu investieren oder aber Partner für ein externes Blockchain-Projekt zu suchen (Kandaswamy & Chesini, 2017, S 4). Im Vergleich zu den anderen Fragekatalogen wird hier der Business Case und nicht der Use Case als Entscheidungspunkt verwendet. Jedoch ist durch die Research Note nicht ersichtlich, weshalb ein Blockchain-Projekt gestartet werden sollte, wenn für das Projekt kein «Success needs other firms?» notwendig ist (siehe Abbildung 12) (Kandaswamy & Chesini, 2017, S 3 ff.). Wenn ein Blockchain-Projekt nur firmenintern geführt wird, stellt sich die Frage weshalb kein zentrales System zur Anwendung kommen kann. Dies würde implizieren, dass kein Vertrauen innerhalb der eigenen Organisation vorhanden ist und dies ist kein technologisches, sondern ein strukturelles Problem.

In einem nächsten Schritt wurden die Hauptmerkmale zur Definition eines Blockchain Use Cases definiert. Das Modell von Gartner wurde für diese Aufgabe nicht berücksichtigt, da dort im Vergleich zu den anderen nicht der Anwendungsfall im Zentrum steht, sondern der Business Case. Des Weiteren sind gewisse Teilfragen nicht explizit beschrieben oder das Modell ist möglicherweise noch nicht auf dem gewünschten Reifegrad. Die erwähnte Betrachtung des Business Cases und der Ökosysteme ist bei einer Entscheidung über den Start eines Blockchain Projektes bedeutungsvoll, jedoch nicht für die Definition des Use Cases oder für die Untersuchung des Potenzials der Technologie.

Bei einem Vergleich der drei Fragenkataloge (Wüst & Gervais, 2017) (Le Hors, 2018) (Peck, 2017) wird ersichtlich, dass die Frage der Notwendigkeit eines Einsatzes der Blockchain-Technologie zwingend evaluiert werden muss. Denn möglicherweise gibt es bereits eine alternative Technologie oder eine Datenbank mit gemeinsamer Zugriffsberechtigung, welche angemessener für den diskutierten Use Case ist. Die folgenden abstrahierten Hauptmerkmale gilt es daher für den eventuellen Einsatz einer Blockchain-Applikation zu diskutieren:

- A: Notwendigkeit einer Speicherung der Daten und Aufzeichnungen und ob diese unveränderlich und manipulationssicher sein müssen (vgl. Wüst & Gervais, 2017) (vgl. Le Hors, 2018).
- B: Es müssen mehrere schreibberechtigte Parteien vorhanden sein, welche das Business-Netzwerk bilden (vgl. Le Hors, 2018) und mit der Blockchain-Applikation arbeiten (vgl. Wüst & Gervais, 2017) (vgl. Peck, 2017).
- C: Das Vertrauen zwischen allen beteiligten Parteien ist gering oder nicht vorhanden und es existiert keine vertrauenswürdige dritte Partei (vgl. Le Hors, 2018) (vgl. Wüst & Gervais, 2017) (vgl. Peck, 2017).

Diese Kriterien sollten bei einem allfälligen Blockchain-Einsatz bei jedem potentiellen Use Case untersucht werden. Falls eine dieser Kriterien nicht zutrifft, handelt es sich vermutlich um keinen Blockchain Use Case und es kann eine alternative Technologie eingesetzt werden. Des Weiteren muss erwähnt werden, dass auch bei einem Zutreffen all dieser Kriterien keine zwingende Notwendigkeit zum Einsatz einer Blockchain impliziert wird. Es sind lediglich Indikatoren, die auf einen möglichen Use Case hinweisen. Es ist möglich, dass eine andere bereits ausgereiftere Technologie situationsabhängig bevorzugt werden muss. Denn bei der Blockchain handelt es sich zurzeit nicht um eine ausgereifte Technologie, deshalb sind auch noch keine exakten quantifizierbaren Merkmale für die Umsetzung eines Projektes in diesem Bereich bekannt.

6.5 Evaluierung der Use Case Varianten

Im folgenden Kapitel werden nun die gesammelten Informationen über die möglichen Zielsetzungen und unterschiedlichen Varianten von Konsortien untersucht. Die vier Varianten werden gemäss den drei definierten «Blockchain-Fit»-Merkmalen geprüft, um einen möglichst validen Use Case festzulegen. Zusätzlich wird kurz angeschnitten, wie die Kosten gedeckt oder wie sich ein möglicher High-level Business Case zusammensetzen könnte. Daher werden in der folgenden Tabelle (5) verschiedene Ausprägungen der vorgeschlagenen Konzepte verglichen. In diesem Kapitel gilt es zwingend anzumerken, dass keine Interviews oder Befragungen durchgeführt wurden, sondern mit öffentlich verfügbaren Informationen gearbeitet und Annahmen getroffen wurden.

Tabelle 5: Use Case Auswertung

Varianten	Zielsetzung	Möglicher Business Case	Blockchain-Fit		
I: • Bio Suisse • Weitere Labels	Rückverfolgbarkeit physischer & finanzieller Transaktionsfluss	Labels tragen den grössten Teil der Kosten für mehr Transparenz und Sicherheit, daher mehr Kostenstelle als neues Business Modell.	A: Durch die angestrebte Rückverfolgbarkeit ist dies eine Notwendigkeit.->JA	B: Es sind verschiedene Labels beteiligt, die in die Blockchain schreiben, aber nicht zwingend ein gesamtes Business Netzwerk-> Tendenz NEIN	C: Es herrscht grundsätzlich kein Mistrauen zwischen den Labels ->NEIN
II: • Labels • Kontrollstellen	Vorbeugung gegen systematischen Betrug, erweiterte Kontrolle und Rückverfolgbarkeit der Zertifikate	Label und Kontrollstellen tragen den grössten Teil der Kosten für mehr Transparenz und Sicherheit, die Bauern / Verarbeiter zahlen Aufwand für Kontrolle	A: Durch die angestrebte Rückverfolgbarkeit der Zertifikate ist dies eine Notwendigkeit.->JA	B: Es sind verschiedene Parteien beteiligt, die in die Blockchain schreiben und es kann von einem Business Netzwerk gesprochen werden->JA	C: Es herrscht grundsätzlich kein Mistrauen zwischen den Labels und ihren Kontrollstellen, diese werden nämlich von den Labels beauftragt->NEIN
III: • Labels • Lizenznehmer (Händler, Verarbeiter und evtl. Bauern)	Rückverfolgbarkeit physischer & finanzieller Transaktionsfluss, Handelsplattform	Labels, Händler & Verarbeiter / Bauern tragen den grössten Teil der Kosten für mehr Sicherheit, neue Handelsmöglichkeiten und Transparenz	A: Durch die angestrebte Rückverfolgbarkeit der Transaktionen ist dies eine Notwendigkeit. ->JA	B: Es sind verschiedene Parteien beteiligt, die in die Blockchain schreiben und es ist ein Business Netzwerk vorhanden ->JA	C: Es sind viele verschiedene Parteien involviert, die sich vermutlich nicht alle vertrauen. Bspw. Müssen sich unbekannte Lizenznehmer, die miteinander handeln möchten, nicht zwingend trauen. -> JA

IV: • Labels • Kontrollstellen • Lizenznehmer (Händler Verarbeiter / evtl. Bauern)	Rückverfolgbarkeit physischer & finanzieller Transaktionsfluss, inklusive Zertifikate und Kontrollen, Handelsplattform	Labels, Händler & Kontrollstellen, Verarbeiter / Bauern tragen den grössten Teil der Kosten für mehr Sicherheit, neue Handelsmöglichkeiten und Transparenz	A: Durch die angestrebte Rückverfolgbarkeit der Transaktionen & Zertifikate ist dies eine Notwendigkeit.->JA	B: Es sind verschiedene Parteien beteiligt, die in die Blockchain schreiben und es ist ein Business Netzwerk vorhanden ->JA	C: Es sind viele verschiedene Parteien involviert, die sich vermutlich nicht alle vertrauen. Bspw. Müssen sich unbekannte Lizenznehmer, die miteinander handeln möchten, nicht zwingend trauen. -> JA

Bei der **Variante «I»** setzt sich das Konsortium aus der Bio Suisse und mindestens einem anderen Label zusammen. Die Idee wäre eine Rückverfolgbarkeit der zu handelnden Güter, der Zertifikate und der verschiedenen Kontrollinstanzen zu erreichen. Die physischen und finanziellen Transaktionen könnten in der Blockchain abgebildet werden und es würde eine Stufe der Transparenz in der Supply-Chain der Labels erreicht werden. Bei diesem Vorschlag stellt sich jedoch die Frage, weshalb kein zentrales System verwendet werden kann oder was die Labels zusammen für ein Business-Netzwerk bilden, bei dem das gegenseitige Vertrauen fehlt. Denn wenn nur die Labels Teil des Konsortiums sind, entsteht nicht ein Business-Netzwerk, sondern mehr eine Kooperation von zwei Parteien mit getrennten Business-Netzwerken, welche sich die Kosten teilen. Daher könnte vermutlich auch eine vertrauenswürdige dritte Partei gebildet werden und es besteht keine Notwendigkeit für den Einsatz eines verteilten Systems. Zusätzlich ist der Business Case für diese Variante relativ limitiert, da die Labels für die erhöhte Transparenz praktisch nur weitere Kosten ohne zusätzliche Vorteile mit dieser Option erreichen.

Bei der **Variante «II»** wird ein Konsortium aus Bio Suisse und anderen Labels sowie den Zertifizierungs- / Kontrollstellen vorgeschlagen. Das Ziel dieser Applikation ist es, dem systematischen Betrug vorzubeugen und die Kontrollen zu verbessern. Der Kostenaufwand für sämtliche Aspekte in Bezug auf die Applikation würde von den Labels und Kontrollstellen getragen. Die zusätzliche Kontrolle würde von den Verarbeitern und Bauern übernommen werden, welche durch ein Anreizsystem (bspw. Reduktion der Mitgliederbeiträgen) entlohnt werden könnten. Bezüglich des Blockchain-Fits wird diese Variante folgendermassen beurteilt: Es ist notwendig, die Transaktionen fälschungssicher zu speichern und es gibt verschiedene schreibberechtigte Parteien, welche zusammen ein Business-Netzwerk bilden. Jedoch herrscht zwischen einem Label und dessen Kontrollstellen ein starkes Vertrauen, da ein Label den Kontrollstellen die Überprüfung des fachgerechten Biolandbaus anvertraut. Insofern könnte auch eine zentrale Lösung von einer der beteiligten Parteien oder eine Drittorganisation diese Aufgabe übernehmen. Ein weiterer zu berücksichtigender Aspekt dieser Lösung, sind die Interessen der Zertifizierungsstellen. Wie bereits in der Stakeholderanalyse (siehe Kaptiel 6.3.2) vermerkt wurde, sind insbesondere die Kontrollstellen bei der Digitalisierung und Automatisierung der Kontrollprozesse durch mögliche Umsatzeinbussen betroffen (vgl. Anhang B, 2018). Insofern müsste gemeinsam an neuen Business Modellen oder Services gearbeitet werden, bei welchem alle Beteiligten profitieren. Daher ist nicht klar zu beurteilen, wie die aktuelle Haltung der Unternehmen mit den Kontroll- und Zertifizierungsaufträgen gegenüber einer neuen Blockchain-Applikation ist.

Bei der **Variante «III»** bilden mindestens zwei oder gar mehrere Labels, die Lizenznehmer und ein möglicher Verbund von Bauern das Konsortium. Zusammen entsteht ein Netzwerk, um die Rückverfolgbarkeit / Transparenz zu erhöhen und gleichzeitig eine gemeinsame Handelsplattform um das Label-Ökosystem weiter auszubauen. Dabei könnte ein Bauer mithilfe der Handelsplattform eine neue Charge «Bio Gala Äpfel» einreichen, welche dann von einem entsprechenden Händler oder anderem Lizenznehmer eingekauft werden kann. Denn aktuell gibt es keine Übersicht der Produzenten und der Abnehmer, sodass nur über das bereits etablierte persönliche Netzwerk gehandelt wird (vgl. Anhang A, 2018). Dieses System würde gleichzeitig die Rückverfolgbarkeit sicherstellen und über prozentuale Einnahmen oder Mitgliedsbeiträge der Handelsplattform finanziert werden. In Bezug auf den Blockchain-Fit ist die Situation folgendermassen zu beurteilen: Es ist ein Business-Netzwerk vorhanden, bei dem die Transaktion von den verschiedenen Parteien in die Blockchain geschrieben werden. Es sind unterschiedliche Parteien am Netzwerk beteiligt, die sich nicht zwingend alle kennen und vertrauen müssen. Die Bauern / Lizenznehmer vertrauen in das Image der Knospe und bezahlen Mitgliederbeiträge, trotzdem werden sie entsprechend von einer Zertifizierungsstelle, welche im Auftrag der Labels arbeitet, kontrolliert. Daher ist das Label in diesem Fall die vertrauenswürdige Drittpartei. Jedoch vertrauen die Lizenznehmer nicht zwingend anderen Labels oder ihren Konkurrenten oder unbekannten Produzenten (Bauern). Daher könnte die Blockchain eine passende Technologie für diesen Use Case sein. Es wird daher ein Netzwerk angestrebt, bei welchem verschiedene Labels mit ihren Produzenten, Händlern und Verarbeitern von zertifizierten Gütern die allgemeine Transparenz erhöhen und den Handel Label-übergreifend vereinfachen soll. Zusätzlich wird eine Machtkonzentration verhindert und die Daten der Handelsplattform sind auf einem verteilten System. Daher ist grundsätzlich ein fairer Wettbewerb unter den Abnehmer und Produzenten möglich.

Bei der **Variante «IV»** wird ein Konsortium vorgeschlagen, bei dem die Labels, die Kontrollstellen, die Lizenznehmer und mögliche Gemeinschaften von Bauern teilnehmen. Diese Variante ist ähnlich wie Variante III aufgebaut, jedoch werden die Kontrollstellen miteinbezogen. Es wird der Aufbau einer Handelsplattform mit einer Rückverfolgbarkeit des Güterflusses inklusive einer Erweiterung des Zertifizierungssystems angestrebt. Die Kontrolltätigkeiten der Bauern und Lizenznehmer sollen analog der Anreizsysteme der Variante «II» aufgebaut werden. Diese Variante ist daher ein komplettes Label-Ökosystem mit Handelsplattform und zusätzlicher Kontrolle zum Schutz der Marke basierend auf einer Blockchain-Applikation. Die Nachweisbarkeit der Zertifikate und Transaktionen erfüllen das erste Blockchain-Fit Merkmal. Ebenso schreiben viele unterschiedliche Parteien in die Blockchain, welche ein komplettes

Business-Netzwerk miteinander bilden. Vermutlich ist zwischen diesen vielen unterschiedlichen Parteien ähnlich wie bei der Variante «III» nicht vollumfängliches Vertrauen vorhanden, daher könnte die Blockchain eine passende Technologie sein. Jedoch bleibt das Verhalten und Interesse der Kontrollstellen schwer abzuschätzen, möglicherweise sehen diese Unternehmen ihre Aufgabe und Einnahmequelle in Gefahr. Deshalb müsste für die Realisation eines Konzepts, bei welchem die Kontrollstellen miteinbezogen sind, vorgängig zusätzliche Erhebungen durchgeführt oder zusätzliche Informationen gewonnen werden.

Abschliessend kann durch diese Evaluierung der Varianten festgestellt werden, dass die Frage des Vertrauens ein relevanter zu untersuchender Aspekt für den Einsatz von Blokchain ist. In den drei Papers ist auch keine exakte Definition oder Methode zur Bestimmung des Vertrauens erwähnt worden. Deshalb wird diese Thematik im nächsten Kapitel diskutiert. Aufgrund der Variantenevaluation muss mindestens die Use Case Variante «III» angestrebt werden. Dieser Anwendungsfall weist beim aktuellen Untersuchungstand und den getroffenen Annahmen das grösste Potenzial der vier Varianten auf. Des Weiteren sollte das Konzept und die Applikation so aufgebaut werden, dass mit kalkulierbarem Aufwand eine Erweiterung gemäss der Variante «IV» implementiert werden kann.

6.6 Vertrauen

Aus der Diskussion der Evaluierung der unterschiedlichen Varianten von Konsortien ist oftmals die Frage des Vertrauens zwischen den Parteien ein relevantes Entscheidungskriterium für den Einsatz von Blockchain. Daher wird empfohlen, den «Trust» zwischen den Teilnehmern mit einem Modell oder einer passenden Methode zu untersuchen. Die Rolle des Trusts wurde bereits in vielen kulturellen, soziologischen oder wirtschaftlichen Bereichen in den letzten 50 Jahren diskutiert. Beispielsweise gesamtgesellschaftlich betrachtet im oftmals zitierten Buch «Trust: The social virtues and the creation of prosperity» von Fukuyuma (1995) oder als Grundlage für zwischenmenschliche Zusammenarbeit in Organisationen (McAllister, 1995). In der Publikation von McAllister (1995) wird zwischen Affekt- und Kognitionsbasiertem Vertrauen unterschieden. Zwischenmenschliches kognitionsbasiertes Vertrauen beruht auf Gedankengängen unter gegebenen Voraussetzungen und der Menge an vorhandenem Wissen über die andere Person (vgl. McAllister, 1995, S. 25 f.) Das affektbasierte Vertrauen wird definiert als eine emotionale Bindung zwischen Individuen (vgl. McAllister, 1995, S. 26). Im Zusammenhang mit der Untersuchung des Blockchain-Fits geht es nicht primär um zwischenmenschliches Vertrauen, sondern um das Vertrauen zwischen unterschiedlichen Organisationen. Die Autoren Mayer,

Davis, & Schoorman (1995) schlagen in einer vielzitierten Arbeit ein integratives Modell für Organisationsvertrauen vor. Den «Trust» definieren die drei Autoren (Mayer et al., 1995, S. 712) folgendermassen: *"the willingness of a party to be vulnerable to the actions of another party*

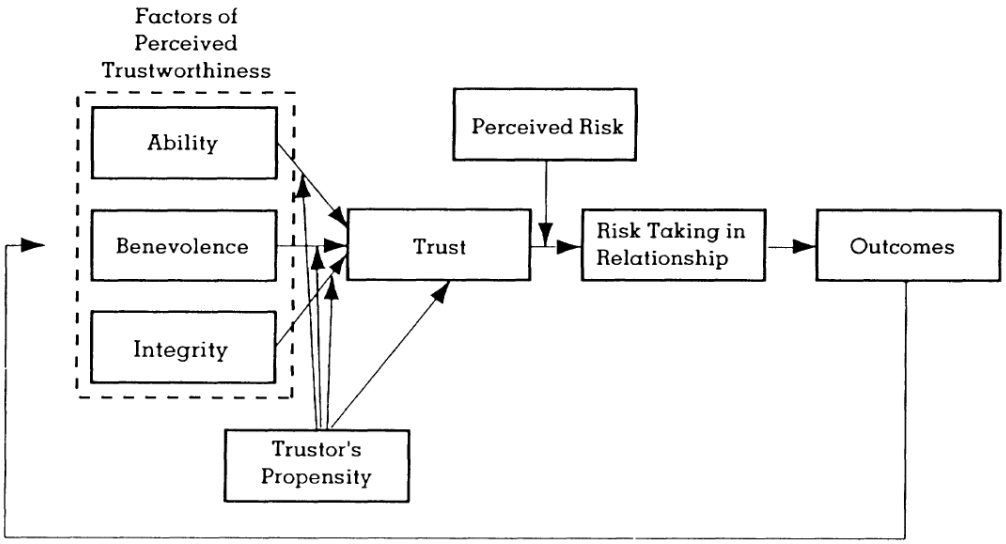

Abbildung 13: Model of Trust (Mayer et al., 1995, S. 715)

based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other part". Diese Definition ist valide für eine Beziehung zwischen der eigenen und einer anderen identifizierbaren Partei, bei welcher ein Wille zum Handeln wahrgenommen wird (Mayer et al., 1995, S. 712). Diese Bedingungen sind vergleichbar mit einem Anwendungsfall einer «permissoned / consortium» Blockchain, bei welcher sich die Parteien kennen um zu handeln, aber sich nicht ohne Regeln vertrauen. Um den «Trust» exakter zu untersuchen, kann das Modell von Mayer et al. (1995) verwendet werden (siehe Abbildung 13). Dieses Modell ist folgendermassen zu verstehen: Der erste Teil des Modells behandelt die Faktoren, welche den «Treuegeber / Trustor» betreffen und welche anschliessend bei einem «Treuenehmer / Trustee» zu Vertrauen führen (Mayer et al., 1995, S. 714). Dies bedeutet, dass die Faktoren, welche zum Vertrauen führen und das Vertrauen an sich zu unterscheiden sind, respektive separat gemessen werden müssen (Mayer et al., 1995, S. 729). Beispielsweise muss die Fähigkeit, das Wohlwollen und die Integrität beim Trustee separat untersucht werden, wobei die Neigung als moderierende Variable wirkt (Mayer et al., 1995, S. 720 ff.). Dieses Modell ist dazu gedacht, Vertrauen als unidirektionale Beziehung zu validieren, also von einer Organisation zur anderen und nicht wechselseitig (Mayer et al., 1995, S. 730). Für diese Arbeit wurde das empirische Befragen der verschiedenen Stakeholder hinsichtlich deren Vertrauen untereinander bewusst nicht durchgeführt, weil ansonsten der Umfang der Thesis nicht eingehalten werden kann. Daher kann die Frage des Vertrauens nicht endgültig geklärt werden, dies sollte aber bei zukünftigen Projekten untersucht werden.

6.7 Konzept Label-Chain

Aus den bisherigen Kapiteln wird nun ein Konzept, respektive die high-level Anforderungen an eine Blockchain-Applikation definiert. Dieses Konzept trägt den Namen «Label-Chain» und wurde gemäss der Evaluation im Kapitel 6.5 definiert. Bei dieser hat sich herausgestellt, dass mindestens folgendes Netzwerk angestrebt werden muss, dass der Einsatz von Blockchain gerechtfertigt, respektive passend ist:

- Konsortium-> Bio Suisse und im Minimum ein weiteres oder mehrere Labels, Lizenznehmer (Händler, Verarbeiter) und möglicherweise Produzentenverbände
- Zielsetzung-> Erhöhung der Transparenz, Sicherheit und Image der Labels, Möglichkeit zum Handeln über eine unabhängige dezentrale Plattform
- Teilnehmer-> Bauern, Kontrollen- / Zertifizierungsstellen, Abnehmer (Verteilzentren, Grosshändler & Einzelhändler)
- Weitere mögliche Teilnehmer-> Staat (bspw. Zoll), Vertrieb / Logistik, Endkunden / Verbraucher
- Business Case-> Kosten hauptsächlich durch Labels und Lizenznehmer abgedeckt, Einnahmen durch die Handelsplattform, mögliche Anreizsysteme für Handel und Erweiterungen der Kontrollsysteme

Diese Rahmenbedingungen müssen vorhanden sein, sodass die «Label-Chain» aus IT-Perspektive und auch aus wirtschaftlicher Sichtweise eine sinnvolle Lösung darstellt. Von diesem high-level-Konzept können nun erste Requirements für die Blockchain-Applikation festgelegt werden. Die Diskussion zum Prozess, den erhaltenen Resultaten und dem tatsächlichen erstellten Konzept wird in Kapitel 8.1 durchgeführt.

6.8 Generalisierung & Diskussion Blockchain für SCM

Abschliessend zur Use Case-Entwicklung gilt es erneut zu erwähnen, dass die Blockchain Technologie eine neue Erscheinung ist und es deshalb keine etablierten quantifizierbaren Merkmale zur Garantie eines Use-Cases gibt. Der Einsatz einer möglichen Blockchain Anwendung muss zwingend überprüft werden. Es kann auch eine philosophische Diskussion geführt werden, nämlich ob jeder Beteiligte bereit ist, einer möglicherweise mächtigen Institution aus Performanz und Kostengründen seine Daten anzuvertrauen oder ob der Wille da ist, ein verteiltes System gemeinsam zu betreuen.

Im Artikel von Wüst & Gervais (2017) wird der Einsatz von Blockchain im Zusammenhang mit einer Supply-Chain diskutiert. Neben Optimierungen des klassischen SCM könnte mittels Blockchain ein sogenanntes Demand Chain Management (DCM) realisiert werden (Wüst & Gervais, 2017, S. 3 f.). DCM wird als Vorgehensweise, bei der die Supply-Chain von den Endkunden rückwärts bis zum Lieferanten gemanagt wird, definiert (Frohlich & Westbrook, 2002, S. 729). Dies bedeutet, dass mittels eines «Pull-Prinzips» und nicht eines «Push-Prinzips» wie im konventionellen SCM gearbeitet wird. (Frohlich & Westbrook, 2002, S. 729). Um das zu erreichen, wird eine extensive Up- und Downstream Integration mit allen beteiligten Business Partnern benötigt (Frohlich & Westbrook, 2002, S. 729). Die Blockchain-Technologie sollte nun helfen, das DCM zu optimieren, jedoch stellt sich weiterhin die Frage, ob dies nicht mit einer vertrauenswürdigen dritten Partei erreicht werden kann (Wüst & Gervais, 2017, S. 4). Bei einer Anfrage eines Anbieters (Skuchain, o.J.), welcher mit "*enterprise supply chains with blockchain*" wirbt, erhalten Wüst & Gervais (2017, S. 4) folgende Informationen: *"Skuchain acknowledged (upon request in private correspondance) that for most supply chain management features a single source of truth would be sufficient — as such a single trusted database at Skuchain should be sufficient to satisfy most business needs."*

Eine weitere grosse Problematik für den Einsatz von Blockchain im Bereich des SCM ist der Link zwischen der digitalen und physischen Welt (Wüst & Gervais, 2017, S. 4). Meistens wird ein Gut von einem Mitarbeiter einer Logistikfirma beim Empfang entsprechend registriert und beispielsweise auf die Qualität geprüft (Wüst & Gervais, 2017, S. 4). Falls diesem Mitarbeiter nicht bei dieser Aufgabe getraut wird, kann die ganze Kette durch seine inkorrekte Eingabe kompromittiert werden (Wüst & Gervais, 2017, S. 4). Somit ist die gesamte Abbildung in der Blockchain zwar digital korrekt, wurde aber durch die Eingabe verfälscht und entspricht nicht dem Zustand in der realen Welt. Wird dem Mitarbeiter hingegen vertraut, könnte auch eine zentrale Datenbank mit gemeinsamem Zugriff verwendet werden (Wüst & Gervais, 2017, S. 4). Die Verlinkung zwischen der realen Welt und dem digitalen Ledger könnte beispielsweise über «Radio Frequency Identification» (RFID) geschehen. Ein Forscher der Universität Wien schlägt in einem IEEE Konferenz Artikel eine Kombination von Blockchain und RFID für den Agrikulturmarkt in China vor (Tian, 2016). Bisherige RFID-basierte Systeme zur Rückverfolgbarkeit der Lieferkette beruhen auf der Idee, ein zentralisiertes System eines Ministerium oder einer Drittorganisation zu verwenden (Tian, 2016, S. 4). Jedoch mangelt es bei diesen Systemen an der Transparenz und die einzelnen Teilnehmer werden nicht in der Lage sein, die Details einer Transaktion zu kennen (Tian, 2016, S. 4). Der Einsatz von RFID im SCM wurde

bereits vor über zehn Jahren diskutiert und erforscht (vgl. Michael & McCathie, 2005) (vgl. Kärkkäinen, 2003). Trotzdem sind die Kosten für die Tags im Verhältnis zu den Gütern im Nahrungsmittelmarkt noch relativ hoch und des Weiteren werden für den Aufbau eines solchen Systems grosse finanzielle Investitionen benötigt (Tian, 2016, S. 5). IBM Research versucht bereits mit sogenannten «Crypto Anchors» im Bereich der Verlinkung einer digitalen Aufzeichnung zu einem tatsächlich existierenden physischen Objekt einen Schritt weiter zu gehen. Der Forscher Andreas Kind, welcher im IBM Lab in Rüschlikon im Bereich Blockchain forscht, präsentierte an der diesjährigen «Think» die Crypto Anchors (IBM Research, 2018). Crypto Anchors werden als fälschungssichere digitale Fingerabdrücke in Produkte integriert (IBM Research, 2018). Beispielsweise können Crypto Anchors in einem Malaria-Medikament als essbaren Farbton in Form von magnetischer Tinte integriert werden (IBM Research, 2018). Durch den Kontakt von Wasser würde sichtbar werden, dass es sich um ein authentisches Produkt handelt und es der Konsument einnehmen könnte (IBM Research, 2018). Die Crypto Anchors, welche zur Authentisierung von physikalischen Gütern designt wurden, soll es zukünftig auch in Form eines Mikrochips geben. Dabei soll der Chip die Grösse eines Sandkorns haben und mit weiteren Funktionen ausgestattet sein, wirbt IBM Research (2018). Diese Crpyto Anchors werden als hochsicher angepriesen, da sie aus kryptographischen Mechanismen bestehen, welche aus einer nichtklonbaren Identifikation bestehen (IBM Research, 2018). IBM erhofft sich mit der Kombination von Blockchain und Crypto Anchors eine neue Methode zur Bekämpfung von systematischem Betrug entworfen zu haben. Die ersten Modelle dieser «Anchors» sollten in den nächsten 18 Monaten für die ersten Kunden verfügbar werden und in den nächsten fünf Jahren weiterentwickelt werden, beispielsweise in Mikroflüssigkeiten (IBM Research, 2018).

Diese Diskussionspunkte zeigen klar, dass die Forschung für den Blockchain-Einsatz im Bereich des SCM noch nicht abgeschlossen ist und in Zukunft sicherlich noch weitergeführt wird.

7 Umsetzung der Label-Chain

In diesem Kapitel wird die theoretische Business-Logik des Use Cases mit einem Prototyp validiert. Das Ziel ist es zu erforschen, ob die Blockchain-Technologie geeignet ist für einen solchen Use Case. Mit anderen Worten wird überprüft, ob die Vorgaben erreicht werden können und wie das Potenzial, respektive die Reife der Technologie für Anwendungen bei Schweizer Organisationen einzuschätzen ist. Dazu wurde in einem ersten Schritt die passende Technologie ausgewählt. Anschliessend wird das verwendete Framework erläutert und mit der Entwicklung des tatsächlichen Prototyps begonnen. Der letzte Teil dieses Kapitels besteht aus der Evaluierung der Lable-Chain-Applikation.

7.1 Blockchain-Technologiewahl

Wie bereits bei der Vorstudie angesprochen (Kapitel 2) kann bei der Blockchain zwischen verschiedenen Arten unterschieden werden. Dies bedeutet, es wird zwischen sogenannten «permissioned», «private» oder «permissionless» Blockchain-Arten unterschieden (vgl. Wüst & Gervais, 2017, S. 3 f.). Diese Charakteristiken der Blockchain haben entsprechend unterschiedliche Eigenschaften hinsichtlich der Sichtbarkeit der Einträge, der Pseudoanonymität (Adresse) der Teilnehmer und dem Konsensus-Algorithmus (vgl. Zheng et al., 2017, S. 558 f.). Es muss daher eine Art von Blockchain ausgewählt werden, welche für den jeweiligen Use Case geeignet ist. Des Weiteren hat die Technologiewahl Auswirkungen auf die Anzahl der verwendbaren Nodes und die Performanz. Beispielsweise kann mit den PoW-Konsensus-Algorithmen (bspw. Bitcoin) eine hohe Skalierbarkeit der Nodes erreicht werden, jedoch mit relativer tiefer Performanz (Transaktionen pro Sekunde) (Vukolić, 2016, S. 113 f.). Gemäss Vukolic (2016, S. 113) ist noch nicht geklärt, in welchem Bereich das Optimum von der

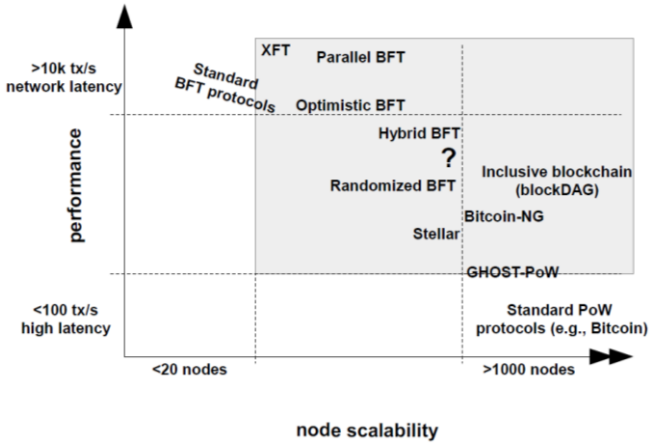

Abbildung 14: Performance / Scalability of diffrent families of PoW and BFT (Vukolić, 2016, S. 113)

Skalierbarkeit der Nodes und der zu erreichenden Performanz für die jeweiligen Use Cases am zutreffendsten ist (siehe Abbildung 14).

Bei dem definierten Use Case der Label-Chain sind sämtliche schreibberechtigten Parteien bekannt und unidentifizierte Drittparteien dürfen nicht in die Kette schreiben. Des Weiteren handelt es sich vermutlich um eine kleinere Anzahl an Nodes verglichen mit dem Bitcoin-Netzwerk. Es kann auch nicht von einer privaten Blockchain gesprochen werden, da sich verschiedene Unternehmen und Organisationen am vorgeschlagenen Netzwerk beteiligen (vgl. Zheng et al., 2017, S. 559). Deshalb kann der definierte Use Case als ein **Konsortium**, respektive eine **«permissioned» Blockchain** bezeichnet werden. Insofern muss eine Technologie gewählt werden, welche für eine Art der «permissoned» Blockchain konzipiert wurde.

Ein Working Paper des Blockchain Center der Frankfurt School unterstützt Entscheidungsträger bei der Wahl der passenden Blockchain-Technologie in Abhängigkeit des Use Cases (Valenta & Sandner, 2017). In diesem Paper wurden die drei bekannten Frameworks Hyperledger Fabric, R3

Characteristic	Ethereum	Hyperledger Fabric	R3 Corda
Description of platform	– Generic blockchain platform	– Modular blockchain platform	– Specialized distributed ledger platform for financial industry
Governance	– Ethereum developers	– Linux Foundation	– R3
Mode of operation	– Permissionless, public or private[4]	– Permissioned, private	– Permissioned, private
Consensus	– Mining based on proof-of-work (PoW) – Ledger level	– Broad understanding of consensus that allows multiple approaches – Transaction level	– Specific understanding of consensus (i.e., notary nodes) – Transaction level
Smart contracts	– Smart contract code (e.g., Solidity)	– Smart contract code (e.g., Go, Java)	– Smart contract code (e.g., Kotlin, Java) – Smart legal contract (legal prose)
Currency	– Ether – Tokens via smart contract	– None – Currency and tokens via chaincode	– None

Abbildung 15: Comparison of Ethereum, Hyperledger Fabric and Corda (Valenta & Sandner, 2017, S. 2)

Corda und Ethereum verglichen (siehe Abbildung 15) (Valenta & Sandner, 2017, S. 1). Ethereum und Hyperledger Fabric werden als Use Case-unabhängige Plattformen angepriesen, während R3 Corda hauptsächlich für Anwendungen im Finanzbereich konzipiert wurde (Valenta & Sandner, 2017, S. 1). Valenta & Sandner (2017, S. 7 f.) bezeichnen Hyperledger Fabric und Ethereum beide als hochflexible Frameworks, jedoch in unterschiedlichen Aspekten. Ethereum zeichnet sich

durch die leistungsstarke «smart contract engine», welche sehr generisch designt wurde und viele Möglichkeiten zur Anwendung offenlässt, aus (Valenta & Sandner, 2017, S. 7). Dafür wird durch die «permissionless» Blockchain und der angestrebten Transparenz keine hohe Performanz erreicht (Valenta & Sandner, 2017, S. 7). Hyperledger Fabric ist durch den Einsatz eines BFT-Algorithmus stärker in der Performanz und ist mit den exakt definierbaren Zugriffsberechtigungen für Applikationen im «permissioned» Blockchain-Umfeld ausgelegt (Valenta & Sandner, 2017, S. 7). Des Weiteren ist die Fabric-Architektur sehr modular aufgebaut, wodurch es für Variationen von unterschiedlichen Use Cases geeignet ist (Valenta & Sandner, 2017, S. 7). Der Fokus von Corda R3 sind Funktionen im Bereich der finanziellen Transaktionen, wodurch die Architektur simpler aufgebaut ist als beim Fabric (Valenta & Sandner, 2017, S. 8). Daher vermuten Valenta & Sandner (2017, S. 8), dass Corda mehr eine "*out-of-the-box experience"* bietet.

Für den definierten Use Case der Label-Chain-Applikation wird, wie bereits erwähnt, eine Technologie benötigt, welche eine Art der «permissioned»-Blockchain zulässt. Gemäss dem Vergleich der drei Technologien nach Valenta & Sandner (2017) würde daher Hyperledger Fabric oder Corda geeignet sein. Jedoch liegt der Fokus von Corda auf Finanz-Applikationen, daher ist Hyperledger Fabric für die Label-Chain von diesen dreien zu bevorzugen. Durch die vielen neuen Entwicklungen und Fortschritte im Blockchain-Umfeld gibt es eine grosse Anzahl an zur Verfügung stehenden Frameworks. Jedoch ist das Ziel dieser Arbeit nicht neue Blockchain-Technologien zu untersuchen, sondern das allgemeine Potenzial zu erforschen. Deshalb wurden für die Auswahl nur Frameworks betrachtet, welche vermutlich ausgereifter sind als neuere Konkurrenztechnologien. Ein weiterer Faktor für die Wahl des Hyperledger Fabric ist, dass der Autor zum Zeitpunkt des Verfassens der Arbeit bei der IBM Schweiz angestellt ist. IBM Research sowie IBM Hursley sind massgeblich an der Entwicklung von Hyperledger Fabric beteiligt, insofern ist es dem Autor möglich bei allfälligen Schwierigkeiten im Entwicklungsprozess auf ein internes Netzwerk zurückzugreifen. Hyperledger Fabric ist aber keine proprietäre IBM Softwarelösung, sondern wie in Abbildung 15 ersichtlich, wird Fabric von der Linux Foundation verwaltet und ist ein Open-Source Projekt, bei welchem 28 verschiedene Unternehmen aktiv Beiträge leisten.

Ein Paper, das hauptsächlich von IBM Research verfasst wurde, erklärt die aktuelle Architektur und das Kernkonzept von Hyperledger Fabric (Androulaki et al., 2018). Hyperledger Fabric ist ein modulares und erweiterbares Open-Source-System für den Einsatz und Betrieb von «permissioned»-Blockchain-Applikationen (Androulaki et al., 2018, S. 1). Es wird als erstes

tatsächlich erweiterbares Blockchain-System für verteilte Applikationen beschrieben, mit der Möglichkeit zur Wahl des Konsensus-Protokolls, wodurch Fabric auf den Use Case und das Trust-Modell massgeschneidert werden kann (Androulaki et al., 2018, S. 1). Gemäss Androulaki et al. (2018, S. 1) unterscheidet sich Fabric von anderen Technologien dadurch, dass eine verteilte Applikation in universalen Programmiersprachen, ohne eine systematische Abhängigkeit von einer Art von Kryptowährungen, entwickelt werden kann. Dies bedeutet, dass keine domänenspezifische Programmiersprache für Smart-Contracts oder eine spezifische Kryptowährung für die Transaktion verwendet werden musss (Androulaki et al., 2018, S. 1). Des Weiteren zeigen die Forscher wie mit einer gängigen Konfiguration (Softlayer Datacenter, dedicated VMs connected with 1Gbps, Config-VM: 2.0 GHz 16-vCPU, Ubuntu 8GB RAM and SSD as Disks) und einer Blockgrösse von 2MB über 3000 Transaktionen pro Sekunde erreicht werden können (Androulaki et al., 2018, S. 12 f.)

7.2 Hyperledger Composer

Die gesamte Architektur und das Konzept von Hyperledger Fabric können im erwähnten Paper (Androulaki et al., 2018) oder über hyperledger-fabric.redthedocs.io nachgelesen werden. Für diese Arbeit wird jedoch nicht nur Fabric verwendet, sondern das Framework «Hyperledger Composer». Hyperledger Composer ist ein umfangreiches Entwicklungstoolset und Framework für den Aufbau von Geschäftsnetzwerken (The Linux Foundation, 2017). Das Framework ermöglicht sowohl den Business-Verantwortlichen und den Entwicklern das Konzipieren von Smart-Contracts und Blockchain-Applikationen, welche zur Lösung von Geschäftsproblemen dienen (The Linux Foundation, 2017). Composer bietet geschäftsorientierte Abstraktionen und Beispielapplikationen mit Entwicklungsprozessen, um robuste Blockchain-Lösungen zu erstellen (The Linux Foundation, 2017). Das Hauptziel von Composer ist es, die Entwicklung zu vereinfachen und die benötigte Zeit zum effektiven Einsatz zu reduzieren (Hyperledger Composer, o.J.e). Die Zielsetzung dieser Arbeit, das Anwendungspotenzial der Blockchain für eine Schweizer Organisation zu untersuchen, war ausschlaggebend für die Entscheidung zusätzlich den Composer und nicht nur Fabric zu verwenden. Der Fokus des Prototyps liegt nicht die Untersuchung einer spezifischen Technologie, sondern darauf, ob ein realistischer Use Case entwickelt werden kann und was dies für Implikationen für die Organisation und deren Ökosystem hat. Es muss erforscht werden, wie das tatsächliche Potenzial von Blockchain einzustufen ist und auf welche Aspekte beim Einsatz dieser Technologie geachtet werden muss. Eine weitere Entwicklung, welche zu beachten ist, sind die Fortschritte und Änderungen der Blockchain-Technologien. Beispielsweise ist der vorletzte «stable release» von Fabric am 31.

Oktober 2017 mit der Version 1.0.4 veröffentlich worden und am 15. März 2018 wurde die nächste stabile Version 1.1.0 veröffentlicht (vgl. Hyperledger, 2018). Diese Situation ist auch bei anderen Blockchain-Technologien zu beobachten, beispielsweise wurde Corda V 2.0 Ende November 2017 veröffentlicht und am 12. März 2018 wurde die Version 3.0 publiziert, wie auf GitHub ersichtlich ist (vgl. GitHub Repository, Baker, 2018). Diese Entwicklungen in einem relativen kurzen Zeitraum lassen vermuten, dass weiterhin intensiv an den unterschiedlichen Blockchain-Technologien gearbeitet wird. Aus diesen Gründen wurde der Composer einer nativen Fabric-Entwicklung vorgezogen, wodurch auf einem höheren Abstraktionslevel gearbeitet werden kann. Falls gewisse Funktionen nicht mit dem Composer abgedeckt werden können, kann in einem späteren Zeitpunkt überprüft werden, ob diese mit einer nativen «Fabric-Entwicklung» oder einer anderen Technologie eher möglich gewesen wären.

7.3 Entwicklung des Prototyps

In diesem Kapitel wird erläutert, wie für das Entwickeln der Applikation vorgegangen worden ist. In einem ersten Schritt wird erläutert, wie die Entwicklungsumgebung aufgebaut ist und welche Versionen der Softwarekomponenten verwendet worden sind. Anschliessend werden die benötigten Composer-Komponenten anhand der ersten Version des lauffähigen Label-Chain-Netzwerks beschrieben.

7.3.1 Entwicklungsumgebung

Für die Entwicklung von Hyperledger Fabric 1.1.0 gibt es Tutorials für Windows, MacOS oder Ubuntu (Hyperlegder, 2017). Das erste Tutorial-Beispiel mit dem Namen «Building your First Network», bei welchem vier Peers (zwei Organisationen) und ein «Orderer Node» hochgefahren werden, konnte erfolgreich mit Windows 10 und 7 sowie Ubuntu 16.04 durchgeführt werden. Jedoch läuft der Hyperledger Composer nur auf Ubuntu 14.04 / 16.04 oder mindestens auf einem Mac OS 10.12 (Hyperledger Composer, o.J.d). Deshalb wurde für die Entwicklung der Label-Chain-Applikation Ubuntu verwendet. Ein Vorteil dabei ist, dass für Ubuntu ein Bash-Skript zur Verfügung gestellt wird, mit welchem alle benötigten Komponenten überprüft und gegebenenfalls installiert werden (Hyperledger Composer, o.J.d). In der folgenden Auflistung werden die aktuell notwendigen Softwarekomponenten (Hyperledger Composer, o.J.d) für die Entwicklung mit dem Hyperledger Composer Framework sowie diejenigen, welche tatsächlich für die Arbeit verwendet wurden, angegeben:

General software components:

- Software Component: Required version -> Version used
- Operating System: Ubuntu Linux 16.04 LTS (both 64-bit)->16.06.4 LTS
- Docker Engine: Version 17.03 or higher->18.03.0-ce
- Docker-Compose: Version 1.8 or higher->1.13.0
- Node: Version 8.9 or higher (node version 9 is not supported)->8.11.1 LTS
- npm: Version 5.x ->5.8.0
- git: Version 2.9.x or higher->2.17.0
- Python: Version 2.7.x->2.7.12

Hyperledger Fabric & Composer components:

- Software Component: Version used
- Hyperledger Fabric (HLF): 1.1.0:
    - HLF Certificate authority (CA): Docker image version 1.1.0
    - HLF Peer node: Docker image version 1.1.0
    - HLF Orderer node: Docker Image version 1.1.0
    - HLF Couch-DB: Docker image version 0.4.6
    - HLF Baseimage: Docker image version 0.4.6
- Composer-CLI (Command Line Interface): Version 0.19.1
- Composer Generator: Version 0.19.1
- Composer-Rest-Server: Version 0.19.1

Diese Software-Komponenten wurden installiert und für die Entwicklung des «Label-Chain-Prototyps verwendet. Der erste Schritt nach der Installation der Software-Komponenten war es, ein Composer-Netzwerk auf einem Fabric-Netzwerk (Orderer, CA & Peer Node + Couch DB) zu deployen, mit welchem eine Transaktion eines Assets zwischen zwei Teilnehmern möglich ist. Dies wurde gemacht, um zu verifizieren, ob die Installation fehlerfrei verlaufen ist und dass das Framework tatsächlich funktionsbereit ist. Die dazu benötigten Dateien und Definitionen werden nun in den folgenden Kapiteln kurz erläutert.

7.3.2 Model File

Der Hyperledger Composer bietet eine objektorientierte Modellierungssprache um das Domänenmodell des Business-Netzwerks zu definieren (Hyperledger Composer, o.J.f). Mit einer Datei können neue Klassen von Konzepten, Transaktionen, Assets, Teilnehmern definiert werden.

Diese Klassen beruhen auf abstrakten Definitionen, welche in der Basisdatei festgelegt sind (Hyperledger Composer, o.J.f). Des Weiteren können zusätzliche abstrakte Klassen, Enumerationen oder unidirektionale Beziehungen definiert werden (Hyperledger Composer, o.J.f). Im folgenden «Code Snippet 1» aus dem Label-Chain GitHub Repository (Anhang C, 2018) kann ein Beispiel eines Business Netzwerks angesehen werden. Diese Definition wurde für die erste Iteration eines lauffähigen Netzwerks verwendet. Es wurde ein Typ eines Teilnehmers (Produktionsbetrieb), ein Asset (GalaApfel), ein Event (ApfelTransEvent) und eine Transaktion (ApfelTransaction) definiert.

```
namespace org.labelchain

participant Produktionsbetrieb identified by eorinr {
 o String eorinr
 o String firstName
 o String lastName
}

asset GalaApfel identified by artikelNr {
 o String artikelNr
 o Integer amount
 --> Produktionsbetrieb owner
}

transaction ApfelTransaction {
  --> GalaApfel apfel
  --> Produktionsbetrieb newOwner
}

event ApfelTransEvent {
 --> GalaApfel apfel
}
```

Code Snippet 1: Business Model Defintion, File: org.acme.labelchain.cto, slightly modified Git Commit: "lauffähiges Netzwerk", (Anhang C, 2018)

7.3.3 Transaction Processor Functions

Die als «Transaction Processor Function» bezeichnete JavaScript Logik wird automatisch aufgerufen, sobald Transaktionen über die Business-Netzwerk-API gesendet werden (Hyperledger Composer, o.J.g). Die Struktur einer Transaktionsprozessorfunktion ist unterteilt in Dekoratoren, in Metadaten und in eine JavaScript-Funktion, in welcher die Transaktionslogik definiert ist (Hyperledger Composer, o.J.g). Die Metadaten, welche der JavaScript-Funktion übergeben werden, sind in der CTO-Datei festgelegt. Sämtliche existierende Beziehungen zwischen Teilnehmern oder Assets, werden automatisch vor der Ausführung der Transaktion aufgelöst, sodass die zu transferierenden Objekte bearbeitet werden können (Hyperledger Composer, o.J.g). Eine weitere Eigenschaft dieser Transaktionsfunktionen ist, dass die Änderungen als «atomar» bezeichnet werden (Hyperledger Composer, o.J.g). Dies bedeutet, dass

entweder alle Änderungen gemäss der Funktion übernommen werden oder dass die Transaktion fehlschlägt und sämtliche Änderungen verworfen werden (Hyperledger Composer, o.J.g).

```
/** * Track the trade of an Apple from one Producer to another
 * @param {org.labelchain.ApfelTransaction} trade - the trade to be processed
 * @transaction
 */
 async function tradeCommodity(trade) {

   // The relationships are fully or recursively resolved, so you can also
   // access nested relationships. This means that you can also access the
   // owner of the asset. With this example below, you can set the new owner.
   trade.apfel.owner = trade.newOwner;

   // Get the asset registry that stores the assets. Note that
   // getAssetRegistry() returns a promise, so we have to await for it.
   let assetRegistry = await getAssetRegistry('org.acme.labelchain.GalaApfel');

   // emit a notification that a trade has occurred
   let tradeNotification = getFactory().newEvent('org.acme.labelchain','ApfelTransEvent');
   tradeNotification.apfel = trade.apfel;
   emit(tradeNotification);

   // Update the asset in the asset registry. Again, note
   // that update() returns a promise, this means have to return
   // the promise so that Composer waits for it to be resolved.
   await assetRegistry.update(trade.apfel);
}
```

Code Snippet 2: Transaction Processor Function, File: logic.js, slightly modified Git Commit "lauffähiges Netzwerk", (Anhang C, 2018)

Im Code Snippet 2 ist eine solche Transaktionsprozessorfunktion mit Kommentaren zu den einzelnen Abschnitten dargestellt. In der Funktion «tadeCommodity» wird das definierte «trade»-Objekt bearbeitet und eine Instanz des GalaApfel-Assets einem neuen Besitzer übergeben. Nach der Übergabe wird der Asset-Register aktualisiert und ein Event kreiert, sodass mögliche Interessenten über die Transaktion informiert werden können.

7.3.4 Access Control List (ACL)

Hyperledger Composer enthält eine Zugriffskontrollsprache (ACL), welche es ermöglicht, die Zugriffskontrolle über Elemente des Domänenmodells festzulegen (Hyperledger Composer, o.J.a). Somit ermöglichen die ACL-Regeln eine Definition, welche den Benutzer/Rollen ermöglicht, Instanzen des Domänenmodells im Business-Netzwerk anzulegen, zu lesen, zu aktualisieren oder zu löschen (Hyperledger Composer, o.J.a). Des Weiteren wird beim Hyperledger Composer zwischen dem Zugriff auf das Business Netzwerk (Business Access Control) und der Zugriffskontrolle für die Administration des Netzwerks unterschieden (Network Access Control), welche beide über die ACL-Datei definiert werden. Zusätzlich kann mit der

Erstellung von unterschiedlichen «namespaces» (siehe CTO-Datei) eine spezifischere Unterscheidung von unterschiedlichen Zugriffsrechten ermöglicht werden (Hyperledger Composer, o.J.a). Das Prinzip zur Überprüfung der erstellten Regeln ist so festgelegt, dass die Regeln der Reihenfolge nach evaluiert werden und sobald eine Kondition zutrifft, wird entsprechend Zugriff erteilt oder verweigert (Hyperledger Composer, o.J.a). Falls keine Kondition zutrifft, wird der Zugriff automatisch verweigert (Hyperledger Composer, o.J.a).

```
rule Default {
    description: "Allow all participants access to all resources"
    participant: "ANY"
    operation: ALL
    resource: "org.acme.labelchain.*"
    action: ALLOW
}
rule SystemACL {
  description:  "System ACL to permit all access"
  participant: "org.hyperledger.composer.system.Participant"
  operation: ALL
  resource: "org.hyperledger.composer.system.**"
  action: ALLOW
}
rule NetworkAdminUser {
    description: "Grant business network administrators full access to user resources"
    participant: "org.hyperledger.composer.system.NetworkAdmin"
    operation: ALL
    resource: "**"
    action: ALLOW
}
rule NetworkAdminSystem {
    description: "Grant business network administrators full access to system resources"
    participant: "org.hyperledger.composer.system.NetworkAdmin"
    operation: ALL
    resource: "org.hyperledger.composer.system.**"
    action: ALLOW
}
```

Code Snippet 3: Access Control List, File: permissions.acl, slightly modified Git Commit: "lauffähiges Netzwerk", (Anhang C, 2018)

Für das Erstellen des ersten Business Netzwerks wurden noch keine spezifischen Regeln festgelegt, sondern sämtlichen Teilnehmern (Rule Default) alle Rechte zugesprochen (siehe Code Snippet 3).

7.3.5 Query Language

Mithilfe der Query Language können Abfragen an den «World State» der Blockchain gesendet werden (Hyperledger Composer, o.J.h). Der World State ist der aktuelle Wert einer Variable in der Blockchain, welcher bei jeder neuen Transaktion aktualisiert wird (Hyperledger, 2017a). Der World State wurde deshalb kreiert, um bei einer Abfrage nicht die gesamte Blockchain durchsuchen zu müssen, sondern dass die einzelnen Werte in einer Datenbank gespeichert sind und effizient Einträge gefunden werden können (Hyperledger, 2017a). Die Blockchain ist bei Hyperledger Fabric bestehend aus den Transaktions-Logs, in welchen sämtliche Änderungen aufgezeichnet werden und der World State vorgeben wird (Hyperledger, 2017a). Mithilfe der Query Language können dynamische oder fixe Abfragen an den World State der Blockchain gesendet werden (Hyperledger Composer, o.J.h). Fixe Abfragen sind spezifiziert über die Business Netzwerk Definitionen, während dynamische beispielsweise von der Transaktionsprozessorfunktion oder einem einzelnen Node aufgerufen werden können (Hyperledger Composer, o.J.h). Für das erste lauffähige Business Netzwerk werden noch keine Abfragen benötigt, jedoch werden im folgenden Code Snippet zwei Beispiele aufgezeigt, wie mögliche Queries aufgebaut sein können.

```
query selectGalaApfelByOwner {
 description: "Select all commodities based on their owner"
 statement:
     SELECT org.acme.labelchain.GalaApfel
         WHERE (owner == _$owner)
}

query selectApfelWithHighAmount {
 description: "Select commodities based on quantity"
 statement:
     SELECT org.acme.labelchain.GalaApfel
         WHERE (amount > 60)
}
```

Code Snippet 4 Query Example, File: queries.qry, slightly modified Git Commit: "lauffähiges Netzwerk", (Anhang C, 2018)

7.3.6 Composer CLI & REST Server

Die vier beschriebenen Dateien in diesem Kapitel bilden die Grundlage zur Erstellung eines lauffähigen Business-Netzwerks. Um das Netzwerk zu deployen, müssen zuerst die vier Dateitypen (.cto, .js, .acl & .qry) mithilfe der zuvor installierten Composer CLI in ein «Business Network Archive» (.bna) gebündelt werden (Hyperledger Composer, o.J.b). Nachdem das Packet generiert wurde, kann es mithilfe der Composer CLI auf einem Fabric-Netzwerk installiert werden (Hyperledger Composer, o.J.b). Für die Installation des Chaincodes auf verschiedenen Fabric-Peers gilt es zu beachten, dass seit dem Fabric v. 1.1.0 zwischen Mitgliedern und

Administratoren auf den Peer Nodes unterschieden wird (Hyperledger Composer, o.J.b). Die Administratoren haben die Berechtigung, den Chaincode auf den Hyperledger Fabric Peers zu installieren, während die Mitglieder keine Berechtigung für solche Operationen haben (Hyperledger Composer, o.J.b). Insofern muss zuerst eine entsprechende Peer-Admin-Card erstellt werden, um den Chaincode auf den Nodes zu installieren. Sobald dies geschehen ist, kann das kreierte «Business Network Archive» auf dem Fabric-Netzwerk installiert werden.

Mit der Verwendung des «Composer REST Servers» werden REST-Schnittstellen zur Verfügung gestellt, über welche die Anwender mit der Blockchain-Applikation interagieren können (Smith, 2018). Der REST-Server verwendet das «Loopback»-Framework, um dynamisch REST-APIs für die Clients zur Verfügung zu stellen (Smith, 2018). Sämtliche Composer-CLI-Befehle und notwendige Skripts vom Start des Fabric-Netzwerks bis hin zur Definition des REST-Servers sind im folgenden Bash-Skript dargestellt (siehe Code Snippet 5).

```
#!/bin/bash

echo please specify label-chain network version
read version
echo Creating Archive 0.0.$version and start REST Server

   #start new Fabric
   cd ~/fabric-tools
   ./startFabric.sh
   ./createPeerAdminCard.sh
   cd label-chain

   #Create Archive & import Card
   composer archive create --sourceType dir --sourceName . -a label-chain@0.0.$version.bna
   composer network install --card PeerAdmin@hlfv1 --archiveFile label-chain@0.0.$version.bna
   composer network start --networkName label-chain --networkVersion 0.0.$version --networkAdmin admin
   --networkAdminEnrollSecret adminpw --card PeerAdmin@hlfv1 --file networkadmin.card

   #Start REST Server
   composer-rest-server -c admin@label-chain -n never -w true
```

Code Snippet 5: CLI Commands & Skripts, File: createArchive.sh, slightly modified Git Commit: "BashSkripts for DEV", (Anhang C, 2018)

Nach dem Start dieses Skripts ist das definierte Business-Netzwerk auf dem Fabric installiert und es kann über den REST-Server oder die CLI darauf zugegriffen werden. Für den ersten Test wurden über den REST-Servers zwei Teilnehmer und ein Asset erstellt. Nach erfolgreicherer Erstellung konnte die Transaktionsprozessorfunktion getestet werden. Das erstellte «GalaApfel»-Asset mit der Identifikationsnummer «33» konnte erfolgreich dem «Produktionsbetrieb» mit dem Identifikator «2» übergeben werden (siehe Abbildung 16).

Abbildung 16: Screenshot HTTP Response 200 (Eigene Darstellung, 2018)

Dies ist eine kurze Übersicht darüber, wie ein Hyperledger Composer Netzwerk erstellt werden kann. Sämtliche weitere Infos und detailliertere Beschreibungen sind in den Dokumentationen gemäss den angegebenen Referenzen einsehbar. Es wurde bewusst keine vollumfängliche Dokumentation über sämtliche Spezifikationen des Hyperledger Composer gegeben, sondern eine Übersicht der wichtigsten Schritte und Dateien, um dem Leser eine Einführung zu geben und gleichzeitig den erfolgreichen Test des ersten lauffähigen Netzwerks zu präsentieren.

7.4 Der Prototyp «Label-Chain»

In diesem Kapitel wird beschrieben, wie die einzelnen Komponenten der Label-Chain aufgebaut sind. Zudem werden die Gründe aufgezählt, die zu den jeweiligen Design-Entscheidungen führten. Die folgenden Punkte sind vor der detaillierten Dokumentation zu erwähnen: Die Applikation wurde auf dem standardmässigen Composer Netzwerk, das heisst mit einem «Orderer», einem «Peer», einer «Certificate Authority» und einer Datenbank «Couch-DB», entwickelt. Es ist daher auf einem Fabric-Netzwerk mit einer einzelnen Organisation und nicht mit einem dezentralen Netzwerk über eine Vielzahl von Organisationen installiert worden. Jedoch kann die Applikation auch auf einem tatsächlich dezentralen Netzwerk mit mehreren Organisationen hochgefahren werden (vgl. Hyperledger Composer, o.J.c). Beispielsweise wird erklärt, wie ein «Multiorganisations-Blockchain-Netzwerk» aufgebaut wird, inklusive der notwendigen Sicherheitsartefakte, um anschliessend ein Composer-basiertes sicheres Netzwerk zur Verfügung zu stellen. Für den Prototyp wurde es nicht als notwendig erachtet, die Applikation bereits auf einem dezentralen Netzwerk zu installieren, da in diesem Stadium des Master Thesis-Projekts der Fokus auf der Business-Logik und dem Konzept liegt. Daher werden sämtliche Teilnehmer des Netzwerks über das Konsortium kreiert, respektive über die Administrationskarte des Konsortiums. Dies impliziert, dass beispielsweise ein Label keine neuen Teilnehmer (bspw. Bauern) erstellen kann und jeder neue Teilnehmer vom Konsortium angelegt wird. Falls der

Prototyp weiterentwickelt und in eine produktive Umgebung gewechselt wird, müssen diese technischen Komponenten erneut untersucht werden. Jedoch empfiehlt sich die Möglichkeit zur Anmeldung der verschiedenen Teilnehmer über das Konsortium zu ermöglichen, sodass kein Teilnehmer konstant an ein Gateway eines Labels gebunden ist und ein offener und unabhängiger Handel garantiert werden kann. Ein weiterer relevanter Aspekt, welcher an dieser Stelle erwähnt werden muss ist, dass zu diesem Zeitpunkt sämtliche integrationsaufwendige Bereiche nicht berücksichtigt wurden. Insofern konnten zu diesem Zeitpunkt weder die Transportunternehmen zur Verfolgung der tatsächlichen Ware, noch der Finanzfluss berücksichtigt werden. Besonders die Integration des Geldflusses hätte grosse Vorteile für eine Handelsplattform. Denn sobald beispielsweise eine Bezahlung im System eingeht, könnte automatisch der Transport und der Transfer der Ware eingeleitet werden. In den folgenden Kapiteln wird mit der Verwendung von Code-Ausschnitten erläutert, wie die einzelnen Komponenten aufgebaut sind und wie diese untereinander interagieren.

7.4.1 Labels & Mandate

```
concept Address {
  o String street
  o String city default ="Zuerich"
  o String country default = "CH"
}
abstract participant Business identified by eorinr {
  o String eorinr
  o String businessName
  o Address address optional
}
participant Label extends Business {
}
participant Control_Authority extends Business {
}
participant Trader extends Business {
}
```

Code Snippet 6: Abstract Business Class & Label, File: org.acme.labelchain.cto, slightly modified Git Commit: “update control access list and logic”, (Anhang C, 2018)

In einem ersten Schritt wurden die Labels und weitere mögliche Teilnehmer der Label-Chain in der objektorientierten Composer-Modellierungssprache definiert. Im folgenden Code Snippet 6 ist dargestellt, wie der grösste Teil der «Participants» aufgebaut wurde. Ausgehend von der abstrakten Klasse mit den Namen «Business» wurden die entsprechenden weiteren Teilnehmer definiert. Des Weiteren ist das Konzept «Adress» mit optionalen festgelegten Werten in der Business-Klasse enthalten. Theoretisch könnten auch Teilnehmer ohne hierarchisch gegliederte oder abstrakte Klassen erstellt werden, jedoch muss danach ein Konzept entworfen werden, in welchem die Referenzen auf andere Objekte (bspw. Assets) klassenübergreifend trotzdem möglich sind (vgl. Code Snippet 7).

Mit der programmierten Definition der Teilnehmer (vgl. Code Snippet 6) kann beispielsweise innerhalb des Assets «Mandate», eine Referenz (-->Business owner, siehe Code Snippet 7) auf die hierarchisch höher gestellten Klassen gemacht werden. Dieses Design ermöglicht es, dass ein Asset beliebig zwischen allen unterschiedlichen Unterklassen ausgetauscht werden kann. Identifiziert wird eine Instanz der Klasse «Label» durch den definierten String «eorinr», welcher als eine einzigartige Betriebsnummer zu verstehen ist und aus den mit Bio Suisse gemeinsam erarbeiteten Workshopunterlagen entnommen worden ist (Anhang A, S. 1 2018). EORI steht für «Economic Operators Registration and Identification number» und jedes Geschäft oder jede Person, welche in der EU Handel betreiben möchte, benötigt diese Nummer bei allen Zollverfahren zur eindeutigen Identifikation (European Comission, o.J.). Auch Wirtschaftsteilnehmer aus Nicht-EU-Staaten benötigen diese Nummer in verschiedenen Situationen, beispielsweise bei der Beantragung zur Vereinfachung bei wirtschaftlichen Verfahren in der EU (European Comission, o.J.). Es gibt auch die Möglichkeit, die EORI-Nr. über eine Datenbank der europäischen Kommission überprüfen zu lassen (European Comission, o.J.). Jedoch wurde bei dieser Arbeit nicht die Einhaltung der exakten europäischen Standards berücksichtigt, sondern es wurden lediglich Möglichkeiten aufgezeigt, wie eine solche Anwendung aufgebaut werden könnte. Wie die Standards bei einer tatsächlichen Implementierung definiert werden, liegt bei der Entscheidungskompetenz des Konsortiums.

```
asset Mandate identified by mandateId{
  o String mandateId
  o DateTime validsince
  o DateTime validuntil
  --> Business issuer
  --> Business owner
}
transaction MandateTransaction {
  --> Business newOwner
  --> Mandate mandate
}
```

Code Snippet 7: Mandate Asset, File: org.acme.labelchain.cto, slightly modified Git Commit: "update control access list and logic", (Anhang C, 2018)

Ausgehend von den Workshopunterlagen (Anhang A, 2018) wurde ein Konzept definiert, wie die Bio Suisse und andere Labels ihre Funktionen im Blockchain-Netzwerk ausüben können. Es gilt anzumerken, dass die Bio Suisse das exemplarische Unternehmen für diese Arbeit ist, jedoch müssen zwingend auch andere Labels mit der Applikation arbeiten können. Insofern muss der Aufbau des Konzepts flexibel genug sein, um auch anderen Unternehmen mit ähnlichen, aber nicht identischen Funktionsweisen die Verwendung dieser Applikation zu ermöglichen. Aus diesem Grund wurde ein Asset mit dem Namen «Mandate» entworfen (siehe Code Snippet 7).

Dieses Mandat wird von den Labels ausgestellt und gibt Kontroll- oder Zertifizierungsstellen, in einem festgelegten Zeitrahmen, das Recht zur Erstellung von Zertifikaten im Auftrag der Labels (siehe Code Snippet 7). Die Labels haben das Recht, die Mandate (siehe Code Snippet 9) über eine Transaktion einer Kontrollstelle zu übergeben. Dazu müssen sie eine «MandateTransaction» initialisieren und den neuen Besitzer sowie das zu transferierende Mandat angeben (siehe Code Snippet 7). Dies triggert die folgende Transaktionsprozessorfunktion (siehe Code Snippet 8), welche entsprechend der «@param»-Bezeichnung zu identifizieren ist (Hyperledger Composer, o.J.g). Die mitgegebenen referenzierten Ressourcen werden anschliessend der JavaScript-Funktion als Argument übergeben (Hyperledger Composer, o.J.g).

```
/** * Track the trade of a Mandate from a label to a control authority
 * @param {org.labelchain.MandateTransaction} trade - the trade to be processed
 * @transaction
 */
async function tradeMandate(trade) {
   //check if issuer matches the creator of the transaction
   if(trade.mandate.issuer==trade.mandate.owner){
   // set the new owner of the mandate
   trade.mandate.owner = trade.newOwner;
   //get the mandate registry
   let assetRegistry = await getAssetRegistry('org.labelchain.Mandate');
   // persist the state of the mandate
   await assetRegistry.update(trade.mandate);
   } else {
       //throw error if issuer or label does not match
       throw new Error('LabelId does not match with the issuerId');
   }
}
```

Code Snippet 8: Mandate Transaction Function, File: logic.js, slightly modified Git Commit "cleanup and adding some comments", (Anhang C, 2018)

Es gilt anzumerken, dass sämtliche geschriebene Funktionen einige Definitionen von JavaScript ES2017 enthalten können. Beispielsweise kann in einer «async»-Funktion der Ausdruck «await» verwendet werden, mit welchem die Ausführung der Funktion angehalten wird, bis das «Promise» (Art eines strukturierteren Callbacks) aufgelöst wird (Mozilla Developer Network, 2018).

In der Funktion «tradeMandate» wird überprüft, ob das Mandat für das korrekte Label erstellt wurde, um zu verhindern, dass ein Label fälschlicherweise ein Mandat für ein anderes Label ausstellt. Denn grundsätzlich ist die Applikation so konzipiert, dass jeder Teilnehmer, welcher die entsprechenden Rechte besitzt (vgl. Code Snippet 9), ein syntaktisch korrektes Asset erstellen kann, welches aber semantische Fehler enthält. Diese werden erst in der dazugehörigen Transaktionsprozessorfunktion, also bei der Übergabe eines Assets, überprüft.

```
rule LabelCanReadotherLables {
   description: "Allow labels to read other labels"
   participant: "org.labelchain.Label"
   operation: READ
   resource: "org.labelchain.Label"
   action: ALLOW
}
rule LabelCanCreateAndAlterOwnMandates {
   description: "Enable lables to create and update mandates"
   participant(p): "org.labelchain.Label"
   operation: CREATE,UPDATE,DELETE
   resource(r): "org.labelchain.Mandate"
   condition:(p.getIdentifier()==r.issuer.getIdentifier())
   action: ALLOW
}
rule LabelCanTransferMandate {
   description: "Enable lables to trade mandates"
   participant(p): "org.labelchain.Label"
   operation: CREATE,READ
   resource(r): "org.labelchain.MandateTransaction"
   condition:(r.mandate.owner.getIdentifier() == p.getIdentifier())
   action: ALLOW
}
```

Code Snippet 9: Label Access Control List, File: permissions.acl, slightly modified Git Commit: "simplify access rights", (Anhang C, 2018)

Die Labels sind berechtigt, sämtliche Mandate zu lesen und eigene Mandate zu kreieren, anzupassen, zu transferieren oder zu löschen (siehe Code Snippet 9). Relevant dabei ist, dass die Labels in der Lage sind nach der Übergabe der Mandate, auch wenn sie nicht mehr der Besitzer sind, die eigens ausgestellten Mandate (issuer, vgl Code Snippet 7) zu löschen. Denn möglicherweise wurde ein Leistungsauftrag einer Zertifizierungsstelle nicht erwartungsgemäss erfüllt und das Label muss dieser Organisation das Mandat entziehen. Ohne ein gültiges Mandat ist die Zertifizierungsstelle nicht mehr handlungsfähig, beziehungsweise verliert sie ihre Berechtigung stellvertretend für das Label zu handeln.

7.4.2 Kontrollstellen

Bei Bio Suisse gibt es zwei Möglichkeiten: Entweder werden die Zertifizierung und die Kontrolle von unterschiedlichen Organisation durchgeführt oder sie werden durch dieselbe Organisation übernommen (Anhang A, S. 6, 2018). Für den Prototyp sind die beiden als Teilnehmer «Control_Authority» definiert, weil sie zusammen die Funktion der «Kontrolle» übernehmen und daher eine ähnliche Rolle im gleichen Aufgabenfeld wahrnehmen. Im folgenden Code Snippet 10 sind sämtliche Modeldefinitionen dargestellt, welche hauptsächlich mit den Kontrollstellen in Verbindung gebracht werden. Die Zertifikate sind wie die Mandate mit einem Gültigkeitsdatum versehen und referenzieren einen Aussteller, ein Label sowie einen Besitzer, welcher anschliessend berechtigt ist, die zertifizierten Aktivitäten durchzuführen. Der Aussteller und das Label werden referenziert, weil dadurch direkt ersichtlich ist von wem und für welches Label das

Zertifikat gültig ist. Des Weiteren können die Zertifikate analog zu den Mandaten beim Verstossen gegen die Richtlinien von den Kontrollstellen entzogen werden.

```
participant Control_Authority extends Business {
}
asset Certificate identified by certificateId {
  o String certificateId
  o DateTime validsince
  o DateTime validuntil
  o LicensedActivity activity
  o ProductTypes [] productTypes
  --> Business owner
  --> Control_Authority issuer
  --> Label validForLabel
}
enum LicensedActivity {
  o Processing
  o Producing
  o Importing
  o Trading
}
transaction CertificateTransaction {
  --> Certificate cert
  --> Business newOwner
}
enum ProductTypes {
o Cherries
o Apples
o Broccoli
o ……
}
```

Code Snippet 10: Control Authority Model Definitions, File: org.acme.labelchain.cto, slightly modified Git Commit: "update control access list and logic", (Anhang C, 2018)

Um einen Überblick darüber zu erlangen, wie Zertifikate aufgebaut sind, wurde auf ProCert und Bio Inspecta nach unterschiedlichen Zertifikaten gesucht. Anhand dieser Beispielzertifikate (Anhang D, 2018) wurden die Aktivitäten und die Produkttypen definiert. Es konnte festgestellt werden, dass die Definitionen der Produkte auf unterschiedlicher Granularitätsstufe vorhanden sind (Anhang D, 2018). Beispielsweise ist in dem Zertifikat mit ID 505373 definiert, dass das Unternehmen die Anforderungen für die Produktgruppe «Früchte» erfüllt, inklusive einer Produktliste, in welcher exakt aufgelistet ist, welche Produkte dies konkret betrifft (bspw. Beerenkirschen) (vgl. Anhang D, 2018). In anderen Zertifikaten (Nr. BL-78115) ist lediglich die Gruppe «Pflanzliche Erzeugnisse» festgehalten (Anhang D, 2018). Möglicherweise ist dies der Fall, weil der letztgenannte Betrieb sich in «Bio-Umstellung» befindet. Jedenfalls ist davon auszugehen, dass bei jedem Label andere Definitionen und Bestimmungen in diesem Bereich vorzufinden sind, deshalb müsste sich das Konsortium auf einen Standard einigen oder aber jedes Label müsste ihre eigene Enumeration von Produkttypen definieren. Bei dieser Determination ist lediglich relevant, dass die festgelegten Werte im Array «productTypes» des Zertifikats (Code Snippet 10) mit einem Wert der tatsächlichen Produktcharge verglichen werden können, um sicherzustellen, dass ein Zertifikat einem spezifischen Produkttyp entspricht.

```
rule ControllauthCanWorkTheirCertificates {
   description: "Enable control authorities to creat,read & updates their certificates"
   participant(p): "org.labelchain.Control_Authority"
   operation: ALL
   resource(r): "org.labelchain.Certificate"
   condition:(r.issuer.getIdentifier() == p.getIdentifier())
   action: ALLOW
}
rule ControllAuthCanReadMandates {
   description: "Enable control authorities to read mandates"
   participant(p): "org.labelchain.Control_Authority"
   operation: READ
   resource(r): "org.labelchain.Mandate"
   condition: (r.owner.getIdentifier() == p.getIdentifier())
   action: ALLOW
}
rule ControllAuthCanTransferCertificate {
   description: "Enable control authorities to trade their certificates"
   participant(p): "org.labelchain.Control_Authority"
   operation: CREATE,READ
   resource(r): "org.labelchain.CertificateTransaction"
   condition:(r.cert.issuer.getIdentifier() == p.getIdentifier())
   action: ALLOW
}
rule EverybodyCanReadCertificates {
   description: "Enable everybody to read certificates"
   participant: "org.labelchain.*"
   operation: READ
   resource: "org.labelchain.Certificate"
   action: ALLOW
}
```

Code Snippet 11:Control Authority Access, File: permissions.acl, slightly modified Git Commit: “simplify access rights”, (Anhang C, 2018)

```
/** * Track the trade of a certificate from a control authority to a business
 * @param {org.labelchain.CertificateTransaction} trade - the trade to be processed
 * @transaction
 */
async function tradeCertificate(trade) {
  //get the certificate registry and initiate date variable
  let assetRegistry = await getAssetRegistry('org.labelchain.Certificate');
  let d1 = new Date();
  //create query and look for mandate of trading control authority
  let querytxt = "resource:org.labelchain.Control_Authority#"+trade.cert.owner.eorinr;
  let results = await query('selectMandateByOwner', {owner:querytxt});
  //loop through mandate array and check for matching mandate for the certificate
  let mandate = results.find(function(element){
      if(element.issuer.$identifier == trade.cert.validForLabel.$identifier){
        return element;}}
  ); //if there is no matching mandate, throw error
  if (mandate==undefined) {
      throw new Error('No matching mandate could be found');
  }else{ //check if the mandate is valid at the point of transaction
        if (mandate.validsince< d1< mandate.validuntil){
              //set new owner
              trade.cert.owner = trade.newOwner;
        }else{ //throw error if mandate is not valid
              throw new Error('Mandate not valid');}
  // persist the state of the certificate
  await assetRegistry.update(trade.cert);}
}
```

Code Snippet 12: Certificate Transaction Function, File: logic.js, slightly modified Git Commit “update tradeCertificate”, (Anhang C, 2018)

Alle Unternehmen mit einer Kontrollfunktion sind berechtigt, sämtliche Operationen auf den von ihnen ausgestellten Zertifikaten durchzuführen. Dazu gehört auch, die eigenen Zertifikate mittels einer Transaktion zu übergeben und alle Mandate, welche sie besitzen, zu lesen (siehe Code Snippet 11). Die Mandate müssen die Kontrollstellen zwingend lesen können, dies nicht nur aus informationstechnischen Gründen, sondern weil die Query in der Transaktionsprozessorfunktion ansonsten keine gültigen Einträge zurücksendet (vgl. Code Snippet 12). Des Weiteren gilt es hier anzumerken, dass jeder Teilnehmer des Netzwerks das Recht besitzt, sämtliche Zertifikate zu lesen, wie dies bereits heute beispielsweise über ProCert möglich ist.

In der Transaktionslogik werden die erhaltenen Resultate der Query (ähnlich aufgebaut wie bei Code Snippet 4) anschliessend auf das Zertifikat-passende Mandat gefiltert (siehe Code Snippet 12). Danach wird überprüft, ob das Mandat noch gültig ist und die Transaktion wird in Abhängigkeit zu dieser Operation dementsprechend durchgeführt oder verworfen. An diesem Punkt gilt es anzumerken, dass auch ohne Query gearbeitet werden könnte, wenn die Zertifizierungsstelle das gültige Mandat selbst angeben würden und nicht über das System nach dem passenden gesucht werden müsste. Es wird daher empfohlen, eine Evaluation darüber durchzuführen, inwiefern eine grosse Anzahl solcher Queries die Performanz des Systems beeinflusst oder inwiefern die Usability für die Anwender durch solche Entscheidungen beeinträchtigt wird. Jedoch werden diese Problemfelder erst im Hinblick auf ein operatives System relevant.

7.4.3 Landwirtschaftsbetriebe

Die Landwirtschaftsbetriebe, Bauern oder Produktionsbetriebe sind zurzeit die einzigen Betriebe, welche in der Lage sind, neue Chargen von Produkten zu erstellen. Im Workshop wurde die hierarchische Gliederung, respektive die Unterscheidung zwischen Produkten, Artikeln und Chargen festgehalten (Anhang A, S. 8, 2018). Jedoch ist anzunehmen, dass bei anderen Labels oder Betrieben unterschiedliche Standards anzutreffen sind. Es muss lediglich beachtet werden, dass der kleinste einheitliche Nenner gemeinsam zu definieren ist. Denn sämtliche weitere hierarchisch höher gestufte Objekte können in abstrakten Klassen oder Konzepten abgebildet werden. Für die Label-Chain wurde die kleinste Einheit gemäss Anhang A (S. 8, 2018) als Charge definiert (siehe Code Snippet 13). Diese Definition muss schlussendlich vom Konsortium festgelegt werden. Relevant ist nur, dass ein einheitlicher Produkttyp zum Vergleich mit den Zertifikaten vorhanden ist sowie eine Mengenangabe und für den Prototyp ein Array mit der «History» der Charge. Bei dieser Anwendung könnte selbstverständlich auch die Historie in der Blockchain nachgesehen werden, jedoch müssten so jedem Besitzer erweiterte Rechte auf den

«HistorianRecord» gewährt werden und dabei könnten möglicherweise Einträge sichtbar werden, welche nicht öffentlich sein sollten. Deshalb wurde zum aktuellen Zeitpunkt die Historie an der Assetklasse angehängt, respektive wurden die Einträge in der Transaktionsprozessorfunktion bei jedem Besitzerwechselt generiert und angehängt (siehe Code Snippet 14), was jedoch für ein MVP überarbeitet werden müsste.

```
participant Farmer extends Business {
}
asset Charge identified by chargeNr {
  o String chargeNr
  o ProductTypes productType
  o HS_code hscode
  o Integer amount
  o TradeHistoryEntry [] tradehistory optional
  --> Business owner
  --> Certificate chargeCert
}
transaction ChargeTransactionFarmer {
  --> Charge charge
  --> Business newOwner
}
event ChargeEventFarmer{
  --> Charge charge
}
```

Code Snippet 13: Control Authority Model Definitions, File: org.acme.labelchain.cto, slightly modified Git Commit: "update control access list and logic", (Anhang C, 2018)

Die Funktion in Code Snippet 14 überprüft in einem ersten Schritt, ob der «Farmer» ein Zertifikat in seinem Besitz referenziert hat. Anschliessend wird evaluiert, ob dieses gültig und der Landwirt zum Herstellen dieses Produkttyps berechtigt ist. Falls die Prüfung erfolgreich verläuft, wird wie bereits erwähnt, ein Eintrag in die Chargen-Handelsgeschichte hinzugefügt und das Asset übertragen.

Des Weiteren wird nach erfolgreichem Aktualisieren des Asset Registers ein Event kreiert, welches die Kontrollstelle abonnieren kann (siehe Code Snippet 14). Dies ermöglicht den Zertifizierungsstellen direkt informiert zu werden, sobald ein Produzent mit einer Charge handelt, welche mit einem ihrer Zertifikate versehen ist. Zusätzlich haben die Kontrollstellen das Recht, sämtliche Transaktionen im Nachhinein zu betrachten (siehe Code Snippet 17), wodurch eine erhöhte Kontrollfunktion möglich ist. Beispielsweise kann eine Zertifizierungsstelle unmittelbar feststellen, wenn eine grössere Menge, als es von diesem Betrieb zu erwarten ist, erstellt wurde. Mit diesen Mechanismen kann ermöglicht werden, Missbrauchsversuche schon beim ersten Handelseintrag eines Produkts festzustellen und nicht erst nachträglich bei einer Jahresprüfung (vgl. Anhang B, 2018)

```
/** * Track the trade of a charge from a farmer to a business
  * @param {org.labelchain.ChargeTransactionFarmer} trade - the trade to be processed
  * @transaction
  */
 async function tradeCharge(trade) {
   //get the charge registry and initiate variables
   let assetRegistry = await getAssetRegistry('org.labelchain.Charge');
   let ccert = trade.charge.chargeCert
   let d1 = new Date();
   //check if charge owner references the correct certificate
   if (trade.charge.owner.$identifier!==ccert.owner.$identifier){
       throw new Error('Certificate do not match');
   }else{
       //check if the certificate is valid at the point of transaction
       if (ccert.validsince< d1 && d1< +ccert.validuntil){
            //check if activity is "producing" for the farmer
            if(ccert.activity=="Producing"){
                //check if product type of the certificate matches the product type of the charge
                let found = ccert.productTypes.find(function(element) {
                  return element ==trade.charge.productType;});
                    //if not, throw error
                    if (found==null){
                        throw new Error ("No matching product type found");
                     }else{
                         // if the trade is valid, set new owner and create "TradeHistoryEntry"
                         trade.charge.owner = trade.newOwner;
                         let history = getFactory().newConcept('org.labelchain','TradeHistoryEntry');
                          history.cert= ccert;
                          history.recieved = d1;
                          tradeHisto = new Array();
                          tradeHisto.push(history);
                          trade.charge.tradehistory=tradeHisto;}
            }else{
                //throw new error if the activity on the certificate is not matching with producing
                throw new Error('Activity not correct');}
       }else{
         //throw new error if the referenced certification is not valid
         throw new Error('Certification not valid');}
   }// persist the state of the charge
   await assetRegistry.update(trade.charge);
   //create & emit event for control authority,
   so they get notified if a farmer creates a new charge with their certificate
   let tradeNotification = getFactory().newEvent('org.labelchain', 'ChargeEventFarmer');
   tradeNotification.charge = trade.charge;
   emit(tradeNotification);
}
```

Code Snippet 14: Charge Transaction Function, File: logic.js, slightly modified Git Commit "update tradeCertificate", (Anhang C, 2018)

```
rule FarmerCanTransferCharge {
    description: "Enable farmers to trade charges"
    participant(p): "org.labelchain.Farmer"
    operation: CREATE, READ
    resource(r): "org.labelchain.ChargeTransactionFarmer"
    condition:(r.charge.owner.getIdentifier() == p.getIdentifier())
    action: ALLOW
}
rule FarmerCanTransferOffer {
    description: "Enable farmer to put offering in marketplace"
    participant(p): "org.labelchain.Farmer"
    operation: CREATE
    resource(r): "org.labelchain.PlaceOffer"
    condition:(r.offer.owner.getIdentifier() == p.getIdentifier())
    action: ALLOW
}
rule EverybodyCanSeeTheirChargetheyOwn {
    description: "Enable everybody to see the charge they own"
    participant(p): "org.labelchain.*"
    operation: READ
    resource(r): "org.labelchain.Charge"
    condition:(r.owner.getIdentifier() == p.getIdentifier())
    action: ALLOW
}
rule ControllAuthCanSeeChargeTradesWithTheirCertificate {
    description: "Enable control authorities to see the charges issued with their certificates"
    participant(p): "org.labelchain.Control_Authority"
    operation: READ
    resource(r): "org.labelchain.ChargeTransactionFarmer"
    condition:(r.charge.chargeCert.issuer.getIdentifier() == p.getIdentifier())
    action: ALLOW
}
```

Code Snippet 15: Farmer and Charge-related Access, File: permissions.acl, slightly modified Git Commit: “ACL simplify”, (Anhang C, 2018)

Die «Farmer» besitzen sämtliche Rechte auf ihre erstellten Chargen, bis zur Übergabe (siehe Code Snippet 15). Anschliessend können die Chargen nur noch vom Besitzer selbst eingesehen und nicht mehr geändert werden. Dies bedeutet, dass sobald sich ein Bauer und ein Händler über den Austausch einer Charge geeinigt haben, der Händler nicht mehr im Stande ist, diese nachträglich zu vergrössern und die Restmenge mit konventioneller Ware aufzustocken.

7.4.4 Lizenznehmer

```
participant Licensee extends Business {
}
transaction ChargeTransactionLicensee {
  o Integer amount
  --> Charge charge
  --> Business newOwner
  --> Certificate cert
}
```

Code Snippet 16: Control Authority Model Definitions, File: org.acme.labelchain.cto, slightly modified Git Commit: “rephrasing trader”, (Anhang C, 2018)

Die Lizenznehmer sind gemäss der Businessklasse erweitert worden und können eine eigene Art von Chargentransaktionen ausführen. Dies wurde so definiert, weil die Händler die Möglichkeit haben müssen, Chargen aufzusplitten und an unterschiedliche Parteien weiterzuverkaufen. Des

Weiteren gilt es anzumerken, dass beim aktuellen Stand des Prototyps nur die Händler berücksichtigt worden sind. Insofern wurden die Funktionen der Importeure oder Verarbeiter im aktuellen Prototyp ausgegrenzt, um den Umfang der Thesis einzuhalten. Die Importeure wurden noch nicht berücksichtigt, weil in einem ersten Schritt die Zollbehörden noch nicht im Projekt miteinbezogen sind. Denn zuerst muss eine Grundsatzentscheidung gefällt werden, ob die Label-Chain hauptsächlich für den Schweizer Markt gedacht ist oder auch in einem späteren Zeitpunkt für den europäischen Markt verwendbar sein sollte. Die technische Implementierung einer Importfunktion wäre möglich, ohne die rechtlichen Aspekte zu betrachten, indem bei jeder Transaktion das Herkunftsland der beiden am Handel beteiligten Parteien verglichen wird. Falls die Charge eine Landesgrenze überschreitet, müssten der entgegennehmende Händler im Besitz eines gültigen Zertifikats mit der Aktivität (vgl. Code Snippet 10.) «Import» sein. Bei den Verarbeitern sieht die technische und betriebliche Ausgangslage komplexer aus. Denn sobald ein Verarbeiter grosse Mengen in Silos lagert und neue Produkte aus Anteilen von unterschiedlichen Chargen herstellt, wird die Nachweisbarkeit schwieriger (Anhang A, 2018). Beispielsweise können grosse Mengen an Getreide in einem Silo gelagert und in gestaffelten Zeitabschnitten neue Chargen hinzugefügt werden. Ab diesem Zeitpunkt sind die Chargen vermischt und nicht mehr exakt identifizierbar. Deshalb müssen die Funktionen der Importeure sowie diese der Verarbeiter in zukünftigen Arbeiten untersucht werden.

Bei jeder Transaktion einer Charge, welche die Lizenznehmer mit einer Händlerfunktion initialisieren können, muss die ausgewählte Charge sowie das korrekte Zertifikat referenziert und der neue Besitzer sowie die zu handelnde Menge angegeben werden (siehe Code Snippet 16). Dieser Handel wird anschliessend bei der Transaktionsprozessorfunktion in einem ersten Schritt in der «validateTrade»-Funktion überprüft (siehe Code Snippet 17). Falls das Zertifikat gültig ist, die korrekte Aktivität vorhanden ist und die Menge nicht grösser ist, als diejenige der ursprünglichen Charge, kann die Transaktion fortgesetzt werden (siehe Code Snippet 17). Falls die Menge unverändert bleibt, wird der Handel durchgeführt und im Asset-Register gespeichert. Wenn der Händler aber nur eine Teilmenge der Charge handeln möchte, wird eine zweite Charge mit der gleichen Historie erstellt, welche im Besitz des Händlers bleibt. Dies verstösst gegen die Policy, dass sämtliche Chargen ihren Ursprung bei einem Landwirt haben. Jedoch kann über die Access Control List eine Regel definiert werden, dass nur während einer Transaktion gewisse Operationen für einen Teilnehmer zur Verfügung stehen (siehe Code Snippet 18). Mit dieser Regel sind die Lizenznehmer berechtigt, eine neue Charge zu erstellen, dies aber nur während einer aktiven Transaktionsprozessorfunktion.

```
* @param {org.labelchain.ChargeTransactionLicensee} trade - the trade to be processed
* @transaction
async function tradeChargeLicensee(trade) {
   let assetRegistry = await getAssetRegistry('org.labelchain.Charge');
   let d1 = new Date();
   //function to check for product types, see validateTrade
   let find = trade.cert.productTypes.find(function(element){
       return element == trade.charge.productType });
   //validate trade function, to prohibit to much nested if else statements,
   //check on correct identifieres, valid dates, activities of the certificate and the amount of the charge
   validateTrade= trade =>
   trade.cert.owner.$identifier !==trade.charge.owner.$identifier ? new Error('Certification does not match charge owner')
   :trade.cert.validsince >d1 || d1> trade.cert.validuntil ?new Error ("Certification not valid")
   :trade.cert.activity !== "Trading" ? new Error ("Activity of certification not matching")
   :find==undefined? new Error ("Not certified for trading this kind of product type")
   :trade.amount > trade.charge.amount ? new Error ("Amount is not matching the received charge")
   :true
   //if trade is valid, proceed with trade
   let isTradeValid= validateTrade(trade);
       if(isTradeValid==true){
           //check if there is a need for a splitting up the charge and create another charge with the amount left
           if(trade.amount!==trade.charge.amount){
               //create new charge with the amount left, with the same trade history
               let chargeleft = getFactory().newResource('org.labelchain', 'Charge', trade.charge.$identifier+1);
               chargeleft.owner = trade.charge.owner
               chargeleft.productType = trade.charge.productType
               chargeleft.hscode = trade.charge.hscode
               chargeleft.amount = trade.charge.amount-trade.amount;
               chargeleft.chargeCert = trade.charge.chargeCert;
               chargeleft.tradehistory = trade.charge.tradehistory;
               // add the new charge to the registry
               await assetRegistry.add(chargeleft);
           }//set new owner & store the certificate of the last owner
           trade.charge.owner = trade.newOwner;
           trade.charge.chargeCert = trade.cert;
           //create new trade history entry
           let history = getFactory().newConcept('org.labelchain', 'TradeHistoryEntry');
           history.cert= trade.cert;
           history.recieved = d1;
           trade.charge.tradehistory.push(history);
           // persist the state of the charge
           await assetRegistry.update(trade.charge);
       }else{//throw validation error with corresponding message generated in the function
           throw new Error(isTradeValid);}
}
```

Code Snippet 17: Licensee Charge Transaction Function, File: logic.js, slightly modified Git Commit "rephrasing trader", (Anhang C, 2018)

```
rule LicenseesCanTransferOwnCharge {
    description: "Enable licensees to transfer their own charge"
    participant(p): "org.labelchain.Licensee"
    operation: CREATE
    resource(r): "org.labelchain.ChargeTransactionLicensee"
    condition:(r.charge.owner.getIdentifier() == p.getIdentifier())
    action: ALLOW
}
rule LicenseesCanUpdateAndCreateChargesDuringTransaction {
    description: "Enable licensees to create new charges during the transaction an existing one"
    participant(p): "org.labelchain.Licensee"
    operation: UPDATE,CREATE
    resource (r): "org.labelchain.Charge"
    transaction(tx): "org.labelchain.ChargeTransactionLicensee"
    condition:(r.owner.getIdentifier() == p.getIdentifier())
    action: ALLOW
}
```

Code Snippet 18: Licensee Access, File: permissions.acl, slightly modified Git Commit: “rephrasing trader”, (Anhang C, 2018)

7.4.5 Der Marktplatz

Der Markplatz ist das Objekt, über welches der Handel stattfinden kann. Es gilt anzumerken, dass für das Konzept des Marktplatzes der Business Case einen zentralen Einfluss auf sämtliche Elemente des Prototyps hat. Beispielsweise könnte eine Gebühr erhoben werden, welche den Teilnehmern die Nutzung des Marktplatztes ermöglicht. Dadurch hätten nur diejenigen Zugriff zur Plattform, welche ein entsprechendes Leistungspaket eingekauft haben. Eine andere Variante wäre, dass ein Teil des Werts, der gehandelten Chargen auf dem Marktplatz an das Konsortium geht, was eine zwingende Integration mit einem Finanzdienstleister bedeuten würde. Eine weitere Möglichkeit wäre es, allen Teilnehmern die Handelsfunktion ohne Gebühren zur Verfügung zu stellen und eine Finanzierung über zusätzliche Services wie Transport oder Versicherungsangebote anzustreben. Diese Aspekte müssen zwingend im Business Case oder bei der Konsortiumsbildung diskutiert werden. Die aktuelle Konzeption betrachtet aber nur die Möglichkeit des Handelns über die Blockchain-Applikation und nicht die damit verbundenen finanziellen Aspekte in einem Geschäftsnetzwerk.

Über den Marktplatz können Angebote (Offer) und Anfragen (Requests) von den Teilnehmern platziert werden (siehe Code Snippet 19). Für die Master Thesis wurden nur die Angebote komplett ausgearbeitet. Die Anfragen können aber nach demselben Prinzip aufgebaut werden. Die Angebote werden von Bauern initialisiert, welche eine Charge eines Produktes verkaufen möchten. Die Anfragen aber können nur von Lizenznehmern mit Handelsberechtigung eingereicht werden. Dies bedeutet, ein Bauer platziert ein Angebot mit den entsprechenden

Angaben und einem Datum sowie einem minimalen Preis für diese Charge auf der Handelsplattform (siehe Code Snippet 19). Die Idee dahinter ist, dass ein verbindliches Angebot mit gewissen Mindestauflagen auf dem Marktplatz positioniert werden kann und sobald ein Händler daran interessiert ist, kann er eine Bestätigung senden und die beiden Parteien verpflichten sich zu den minimalen Anforderungen dieses Deals.

```
participant Marketplace extends Business {
}
asset Offer identified by offerId {
 o String offerId
 --> Business issuer
 --> Business owner
 --> Certificate cert
 o ProductTypes productType
 o Integer amount
 o DateTime offerAvailableAt
 o Integer minimalCommitmentPrice
}
asset OfferConfirmation identified by confirmationId {
 o String confirmationId
 --> Business issuer
 --> Business owner
 --> Certificate cert
 --> Offer offer
 o String comments optional
}
transaction PlaceOffer {
 --> Offer offer
 --> Marketplace market
}
event NewOffer{
 --> Offer offer
}
transaction OfferConfTransaction {
 --> OfferConfirmation offConf
}
```

Code Snippet 19: Marketplace Model Definitions, File: org.acme.labelchain.cto, slightly modified Git Commit: “rephrasing trader”, (Anhang C, 2018)

Die Transaktionsprozessorfunktion ist so aufgebaut, dass in einem ersten Schritt ein Landwirt ein Angebot erstellt und dieses anschliessend an den Markplatz transferiert. Sobald es auf dem Markplatz ist, wird das Angebot für alle Lizenznehmer sichtbar. Dieses Konzept wird mithilfe einer Regel implementiert (siehe Code Snippet 20), bei welcher alle Teilnehmer berechtigt sind die Angebote zu sehen, sobald diese im Besitz einer Instant der Klasse «Marketplace» sind. Die Transaktion des Angebots ist analog zur Chargentransaktionsfunktion aufgebaut (vgl. Code Snippet 17). Das heisst, es wird überprüft, ob der Bauer ein gültiges Zertifikat für dieses Angebot hat und berechtigt ist, dieses Produkt herzustellen. Wenn die Transaktion erfolgreich ist, wird ein Event publiziert, welchen interessierte Händler abonnieren können, um über das neue Angebot direkt informiert zu werden.

Falls ein Lizenznehmer interessiert an einem Angebot ist, kann dieser eine «Offerconfirmation» (Code Snippet 19) erstellen, welche direkt auf das entsprechende Angebot verlinkt ist. Sobald der Lizenznehmer eine Transaktion der «Offerconfirmation» auslöst, wird in der «offerConfirmation»-Funktion überprüft, ob der Händler berechtigt ist, diese Charge zu handeln (siehe Code Snippet 21). Falls die Überprüfung erfolgreich verläuft, wird die Bestätigung direkt dem Angebotserstellenden und das Angebot dem Bestätigungserstellenden übergeben. Das Recht zur Transaktion eines Angebots hat der Lizenznehmer nur während einer entsprechenden Transaktionsprozessorfunktion (siehe Code Snippet 20). Nun sind beide interagierenden Parteien im Besitz eins Zugeständnisses und die verhandelte Charge kann übergeben werden. Ob dieses Konzept aus rechtlicher Perspektive sämtliche Rahmenbedingungen erfüllt, muss bei der Ausarbeitung des Konsortiums mit Rechtsexperten festgelegt werden

```
rule LicenseeCanReadOffersOnMarketplace {
   description: "Enable licensees to look for offers on the marketplace"
   participant: "org.labelchain.Licensee"
   operation: READ
   resource(r): "org.labelchain.Offer"
   condition:(r.owner.instanceOf("org.acme.labelchain.Marketplace")==true)
   action: ALLOW
}
rule LicenseeCanCreateandUpdateOfferConfirmation {
   description: "Enable licensees to create and update their offer confirmations"
   participant(p): "org.labelchain.Licensee"
   operation: CREATE,UPDATE,READ
   resource(r): "org.labelchain.OfferConfirmation"
   condition:(r.owner.getIdentifier() == p.getIdentifier())
   action: ALLOW
}
rule LicenseeCanPLaceOfferConfirmation {
   description: "Enable licensees to place an offer confirmation"
   participant(p): "org.labelchain.Licensee"
   operation: CREATE,UPDATE,READ
   resource(r): "org.labelchain.OfferConfTransaction"
   condition:(r.offConf.owner.getIdentifier() == p.getIdentifier())
   action: ALLOW
}
rule LicenseeCanUpdateOfferDurringTransaction {
   description: "Enable licensees to transfer an offer to them during transaction"
   participant(p): "org.labelchain.Licensee"
   operation: UPDATE
   resource (r): "org.labelchain.Offer"
   transaction(tx): "org.labelchain.OfferConfTransaction"
   condition:(tx.offConf.issuer.getIdentifier() == p.getIdentifier())
   action: ALLOW
}
```

Code Snippet 20: Access Marketplace, File: permissions.acl, slightly modified Git Commit “rephrasing trader”, (Anhang C, 2018)

```
/** * Track the trade of a confirmation from a licensee to a farmer
* @param {org.labelchain.OfferConfTransaction} trade - the trade to be processed
* @transaction
*/
async function offerConfirmation(trade) {
   //get the offer and the confirmation registry and initiate variables
   let offerConf = await getAssetRegistry('org.labelchain.OfferConfirmation');
   let offerRegistry = await getAssetRegistry('org.labelchain.Offer');
   let d1 = new Date();
    //function to check for product types, see validateConfirmation
   let find = trade.offConf.cert.productTypes.find(function(element){
       return element == trade.offConf.offer.productType
   });
   //validate confirmation function check on correct identifiers, valid dates and
   //activities of the certificate for the confirmation
   validateConfirmation= conf =>
   conf.cert.owner.$identifier !==conf.owner.$identifier ?  new Error('Certification does not match
   offer confirmation issuer')
   :conf.cert.validsince >d1 || d1> conf.cert.validuntil ? new Error ("Certification not valid")
   :conf.cert.activity !== "Trading" ? new Error ("Activity of certification not correct")
   :find==undefined? new Error ("Not certified for that offering")
   :true
   //if confirmation is valid, proceed
   let isConfirmationValid= validateConfirmation(trade.offConf);
       if(isConfirmationValid==true){
           // set the new owner of the offer and the new one of the confirmation
           // the confirmer receives the offer and the confirmation goes to the issuer of the offer
           // the licensee can only move the offer during the transaction, see access control
           trade.offConf.owner = trade.offConf.offer.issuer;
           trade.offConf.offer.owner = trade.offConf.issuer;
           await offerConf.update(trade.offConf);
           await offerRegistry.update(trade.offConf.offer);
       }else{//throw validation Error with corresponding message generated in the function
           throw new Error(isConfirmationValid);
       }
}
```

Code Snippet 21: Offer Confirmation Transaction Function, File: logic.js, slightly modified Git Commit "rephrasing trader", (Anhang C, 2018)

7.5 Demonstration & Evaluierung

In diesem Kapitel wird erläutert, wie der Prototyp «Label-Chain» verwendet werden kann. Des Weiteren wird erklärt, wie die Funktionalitäten der entwickelten Prototyp-Applikation getestet wurden. In einem ersten Teil wird daher beschrieben, wie mithilfe des erwähnten REST-Servers (siehe Kapitel 7.3.6) die Interaktion mit der konzipierten Blockchain-Applikation möglich ist. Anschliessend wird die Testumgebung erläutert, welche zur Entwicklung der Applikation und Programmierung von erweiterten Testfällen verwendet wurde.

7.5.1 REST-Server

Um mit der Blockchain-Applikation zu arbeiten, muss nach dem Entwickeln des objektorientierten Modells, der Transaktionslogik usw., ein Geschäftsnetzwerkarchiv (.bna) erstellt werden. Dieses kann anschliessend auf einem Cloud-Service (bspw. IBM Blockchain Starter Plan (vgl. Harrison, 2018)) installiert und mit einem REST-Server und einem Front-end (z.B. mit Composer Angular Generator) verbunden werden. Für die Master Thesis wurde jedoch eine lokale Testumgebung bevorzugt, weil die Cloud-Services oftmals neu auf dem Markt und noch in der Beta-Phase sind (vgl. Harrison, 2018). Zusätzlich konnte zum aktuellen Standpunkt des Projekts, noch kein Mehrwert für einen Cloud-basierten Prototyp erkennt werden. Deshalb wurde der Prototyp auf einer der lokalen Installation (siehe Kapitel 7.3.1) getestet. Das heisst, es wurde ein Geschäftsnetzwerkarchiv auf einer Organisation (Peer, Orderer, CA, Couch-DB) installiert und mithilfe des REST-Servers Anfragen an das Netzwerk gesendet, um die Funktionalitäten der Applikation zu testen. Falls zusätzliche Debugging-Informationen von Bedarf sind, können die Log-Files der Container analysiert werden (hauptsächlich die Log-Files des Peer Nodes, da dort der Chaincode installiert ist).

Mit Hilfstools wie Postman können ganze Kollektionen an HTTP-Anfragen gesendet werden (siehe Abbildung 17). Diese automatisierten HTTP-Anfragen sind im GitHub-Repository im Ordner «postmanreqs» gespeichert. Grundsätzlich sind es zehn Anfragen, mit welchen von der Label-Erstellung bis zur Transaktion einer Charge sämtliche Funktionen durchgeführt werden. Jedoch müsste für jeden Request eine andere Identität verwendet werden, um die Testfälle korrekt mit den unterschiedlichen Rechten der Teilnehmer zu testen. Das impliziert, dass zuerst ein Bash-Skript geschrieben werden müsste, mit welchem sämtliche Teilnehmer mit ihren zugehörigen Identitätskarten erstellt werden könnten. Nur wenn die Requests so durchgeführt werden, kann das erstellte Geschäftsnetzwerk mit sämtlichen Gegebenheiten vollumfänglich getestet werden.

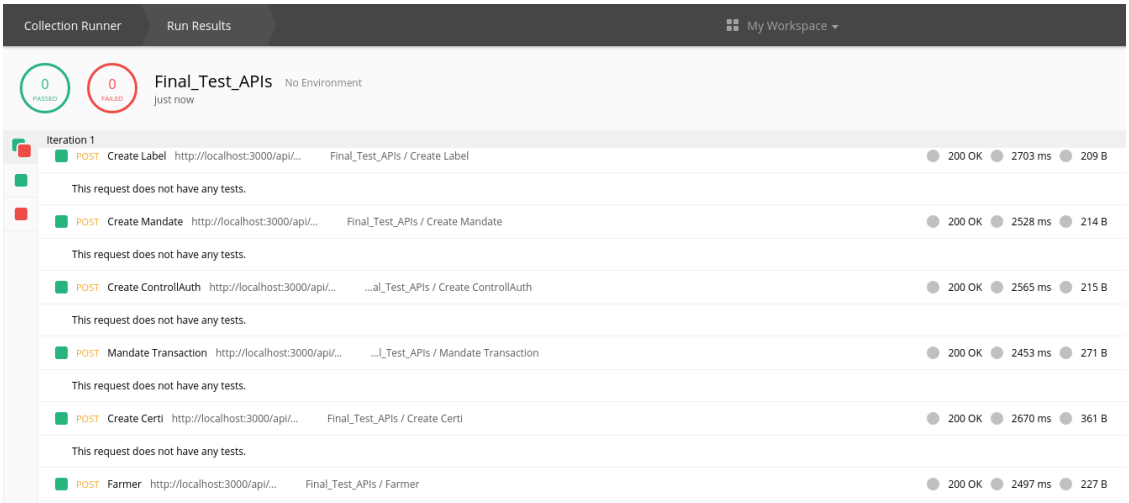

Abbildung 17: Postman Collection Runner (Eigene Darstellung, 2018)

Falls gewisse Anfragen ungültig waren oder Transaktionen nicht durchgeführt werden konnten, sind korrespondierende Fehlermeldungen in den HTTP-Antworten zurückgesendet worden. Die durchgeführten Transaktionen und Assets können anschliessend mit GET-Requests mithilfe des REST-Servers überprüft werden (siehe Abbildung 18). In der Abbildung 18 ist einerseits ersichtlich, dass ein Lizenznehmer im Besitz einer Charge «Broccoli» ist und andererseits, welches Zertifikat zuletzt bei einer Aktivität dieser Charge verwendet wurde. Zusätzlich ist die Historie erkennbar, wobei der Eintrag in diesem Fall identisch mit dem ursprünglichen Zertifikat des Landwirts ist.

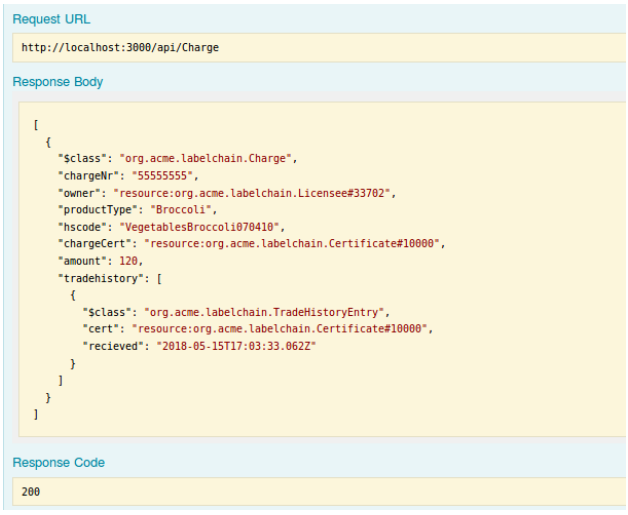

Abbildung 18 Charge GET Request, REST-Server (Eigene Darstellung, 2018)

Um die Applikation umfänglich zu testen, ist die Analyse der Docker-Logs und das stetige neue Erstellen des Geschäftsnetzwerksarchivs nicht effizient, da bei jeder Änderung das gesamte Archiv neu erstellt wird und jede Transaktion erneut durchgeführt werden muss. Des Weiteren muss vor jedem Request, welcher von einem spezifischen Anwender ausgeführt wird (beispielsweise die Erstellung einer Charge), die Composerkarte zur Identifikation eines Teilnehmers (bsp Bio Insepcta) gewechselt werden. Aus diesen Gründen wurde eine Testlogik mithilfe des Mocha-Frameworks geschrieben.

7.5.2 Mocha-Tests

Das Mocha-Framework ist ein JavaScript-Framework, welches im Browser oder auf Node.JS läuft, womit ein asynchroner Quellcode getestet werden kann (mochajs.org, 2018). Mithilfe des Mocha-Frameworks konnten 25 Testfälle geschrieben werden, um die unterschiedlichen Funktionen des Netzwerks zu testen. Mithilfe des verwendeten Editors «Visual Studio Code» kann eine Debug-Konfiguration erstellt werden und anschliessend können die Mocha-Tests über das Tool gestartet werden. Jedoch muss vor dem Start kontrolliert werden, ob die abhängigen Node-Module über «npm» installiert worden sind, ansonsten können die Tests nicht durchgeführt werden.

Die Testdatei «testlogic.js» ist insgesamt über 700 Zeilen lang, deshalb werden in diesem Kapitel nur Ausschnitte davon erklärt. Für exaktere Informationen kann die gesamte Datei im GitHub Repository angesehen werden (Anhang C, 2018). Die Datei ist in zwei unterschiedliche Abschnitte gegliedert. Im ersten Abschnitt werden die notwendigen Module geladen und alle Hilfsvariablen initialisiert. Des Weiteren werden vor (before-hook) dem Start der Testfälle alle Beispielteilnehmerklassen (Participants) inklusive ihrer dazugehörigen Identität kreiert (siehe Code Snippet 22). Das bedeutet, dass ein Beispielteilnehmer pro Teilnehmerklasse (bspw. Label, Retailer, Lizenznehmer usw.) erstellt wurde, um die verschiedenen Funktionalitäten der

```
// Create a label, i.e Bio Suisse
const participantRegistry = await businessNetworkConnection.getParticipantRegistry(labelTypeNS);
const biosuisse = factory.newResource(namespace, labelType, '1');
const addr = factory.newConcept(namespace, addressType, '1');
addr.street = "Peter Marian Strasse 34";
addr.city = "4052 Basel";
biosuisse.businessName = 'Bio Suisse';
biosuisse.address = addr;
participantRegistry.addAll([biosuisse, hochstamm]);
// Create a control authority, i.e Bio Inspecta
const controllAuthRegistry = await
businessNetworkConnection.getParticipantRegistry(controllAuthTypeNS);
const controllAuth = factory.newResource(namespace, controllAuthType, '501');
const addr3 = factory.newConcept(namespace, addressType, '3');
controllAuth.businessName = 'Bio Inspecta';
addr3.street = "Ackerstrasse";
addr3.city = "5070 Frick";
controllAuth.address = addr3;
controllAuthRegistry.addAll([controllAuth]);
// Issue the identities to the participants
let identity = await businessNetworkConnection.issueIdentity(labelTypeNS + '#1', 'biosuisse1');
await importCardForIdentity(BioSuisseCard, identity);
identity = await businessNetworkConnection.issueIdentity(controllAuthTypeNS+ '#501', 'bioinspecta1');
await importCardForIdentity(BioInspecta, identity);
```

Code Snippet 22: Creating Participants File: testLogic.js, slightly modified Git Commit: "updated trade logic" (Anhang C, 2018)

entwickelten Applikation zu testen. Die Erstellung dieser Identitäten wird in einem produktiven Umfeld vom Konsortium übernommen oder es wird eine Identität über eine vertrauenswürdige Fabric-Organisation ausgestellt.

```
it('1.  The label can create and read the mandate', async () => {
 // Use the identity for Bio Suisse
 await useIdentity(BioSuisseCard);
 // Create the mandate
 let mandateRegistry = await businessNetworkConnection.getAssetRegistry(mandateNS);
 let asset1 = factory.newResource(namespace, mandatetype, '101');
 asset1.owner = factory.newRelationship(namespace, labelType, '1');
 asset1.validuntil = new Date(2020,0o4,22,15,57,48,132);
 asset1.validsince = new Date(2018,0o4,22,15,57,48,132);
 asset1.issuer = factory.newRelationship(namespace, labelType, '1');;
 await mandateRegistry.addAll([asset1]);
 //Validate the mandate.
 let assetTest = await mandateRegistry.get('101');
 assetTest.owner.getFullyQualifiedIdentifier().should.equal(labelTypeNS + '#1');
 assetTest.issuer.getFullyQualifiedIdentifier().should.equal(labelTypeNS + '#1');
});
```

Code Snippet 23: Test case 1, testLogic.js, slightly modified Git Commit: "updated trade logic" (Anhang C, 2018)

Nach dem erfolgreichen Initialisieren des ersten Teils der «testLogic.js» können die einzelnen Testfälle gestartet werden. Beim Beginn von jedem Testfall wird definiert, welche Identität, respektive welcher exemplarische Teilnehmer, verwendet wird (siehe Code Snippet 23). Dies geschieht mit der Funktion «useIdentity», womit diejenige Identität angegeben wird, welche für den gesamten Testfall gültig ist. Insgesamt wurden folgende 25 unterschiedliche Testfälle mit der Unterstützung des Mocha-Frameworks kreiert, welche in diesem Kapitel exemplarisch erläutert werden:

1. The label can create and read the mandate
2. The label can transfer the mandate to a control authority
3. The control authority can NOT transfer their mandate to another organization
4. The control authority can create certificates for a farmer and a licensee
5. The control authority can transfer the certificate to the Farmer & the licensee
6. The farmer can NOT transfer the certificate
7. The farmer can NOT update or alter the certificate
8. The farmer can create a charge
9. The farmer can transfer the charge to a licensee
10. The farmer can create another charge without a correct certificate
11. The farmer can NOT trade a charge without a correct certificate
12. The licensee can NOT transfer a higher amount then he owns to a retailer
13. The licensee can NOT transfer with another certificate or an incorrect one
14. The licensee can NOT create a new charge only during transaction

15. The licensee can NOT update or alter the charge
16. The licensee can transfer a part of a charge to a retailer while simultaneously creating a new one with the amount left
17. The retailer can see his asset and the history of the asset
18. The farmer can create an offer
19. The licensee can NOT read offers which not have been shared
20. The farmer can place the offer on the marketplace
21. The licensee is able to read the offers on the marketplace
22. The licensee can create an offer confirmation
23. The licensee can place the offer confirmation on the marketplace and receives the offer if the confirmation is valid
24. The farmer gets his offer confirmation and can see it
25. The control authority can remove one of their certificates

Die Testfälle sind als logische Reihenfolge aufgebaut, so gesehen muss beispielsweise zuerst ein Label ein Mandat erstellen und übergeben, bevor eine Kontrollstelle ein Zertifikat ausstellen kann. In den ersten zwei Testfällen (siehe Code Snippet 23) wurden die Hauptfunktionen der Labels, also das Erstellen und Transferieren von Mandaten, getestet. Im Testfall 3 wird überprüft, ob die Kontrollstellen die Mandate lesen können, aber nicht weiter transferieren, auch wenn sie die Besitzer dieses Assets sind (siehe Code Snippet 24). Demnach wird in diesem Testfall versucht eine Transaktion, welche aber mit einer entsprechenden Fehlermeldung (der Anwender besitzt nicht die entsprechenden Rechte) verworfen wird, durchzuführen. In den Testfällen vier und fünf wird überprüft, ob die Kontrollstellen die Zertifikate ausstellen und diese anschliessend transferieren können.

```
it('3.  The control authority can NOT transfer their mandate tho another organization', async () => {
 // Use the identity for Bio Inspecta
 await useIdentity(BioInspecta);
 // Create a valid transaction.
 let transaction = factory.newTransaction(namespace, 'MandateTransaction');
 transaction.newOwner = factory.newRelationship(namespace, labelType, '1');
 transaction.mandate = factory.newRelationship(namespace, mandatetype, '101');
 //The transaction should be rejected because the control authority does not have the appropriate access
 businessNetworkConnection.submitTransaction(transaction).should.be.rejectedWith(/does not have .* access to
 resource/);
});
```

Code Snippet 24: Test case 3, testLogic.js, slightly modified Git Commit: "updated trade logic" (Anhang C, 2018)

In den Testfällen 6-11 wird kontrolliert, ob ein Landwirt sämtliche erlaubten Operationen der Rolle «Farmer» durchführen kann. Beispielsweise wird im Testfall 8 kontrolliert, ob der Landwirt

eine Charge erstellen kann und diese anschliessend für ihn lesbar ist (siehe Code Snippet 25). Des Weiteren wird verifiziert, dass der Landwirt zwar eine syntaktisch korrekte Charge kreieren kann, diese aber mit einem inkorrekten Zertifikat versehen ist. Durch die erwähnte Konzeption der Applikation wird dieser Fehler oder möglicher Betrugsversuch erst bei der Transaktion ersichtlich. Der Landwirt ist daher berechtigt, diese Charge zu erstellen und die Transaktion zu initialisieren, welche jedoch mit einem Fehler verworfen wird (siehe Testfall 11, Code Snippet 26). Diese Fehlermeldung wird gemäss der Transaktionsprozessorfunktion generiert, wie es in der «validateTrade»-Funktion im Code Snippet 14 definiert ist.

```
it('8.  The farmer can create a charge', async () => {
 // Use the identity for the farmer Meier
 await useIdentity(FarmerMeier);
 //create the charge
 let assetRegistry = await businessNetworkConnection.getAssetRegistry(chargeNS);
 let charge = factory.newResource(namespace, chargeType, '55555555');
 charge.owner = factory.newRelationship(namespace, farmerType, '12576');
 charge.productType = "Broccoli";
 charge.hscode = "VegetablesBroccoli070410"
 charge.amount = 120;
 charge.chargeCert = factory.newRelationship(namespace, certificateType, '100000');
 await assetRegistry.add(charge);
 // Get the charge & validate it
 let assetRegistry1 = await businessNetworkConnection.getAssetRegistry(chargeNS);
 let asset1 = await assetRegistry1.get('55555555');
 asset1.owner.getFullyQualifiedIdentifier().should.equal(farmerTypeNS+ '#12576');
 asset1.amount = 120;
 charge.productType.should.equal("Broccoli");
});
```

Code Snippet 26: Test case 8, testLogic.js, slightly modified Git Commit: “updated trade logic” (Anhang C, 2018)

```
it('11. The farmer can NOT trade a charge without a correct certificate', async () => {
 // Use the identity for the farmer Meier
 await useIdentity(FarmerMeier);
 //create and submit valid transaction
 let transaction = factory.newTransaction(namespace, 'ChargeTransactionFarmer');
 transaction.newOwner = factory.newRelationship(namespace, licenseeType, '33702');
 transaction.charge = factory.newRelationship(namespace, chargeType, '6666666');
 //should throw error that that the certificate is not valid for this product type
 businessNetworkConnection.submitTransaction(transaction).should.be.rejectedWith(Error,
 'No matching product type found');
 });
```

Code Snippet 25: Test case 11, testLogic.js, slightly modified Git Commit: “updated trade logic” (Anhang C, 2018)

In den Testfällen 12-16 wird kontrolliert, ob die Lizenznehmer ihre Funktion als Händler wahrnehmen können. Der Testfall 12 simuliert eine Transaktion mit einer grösseren Menge als die ursprünglich erstellte Charge des Landwirts, wobei diese mit einem Fehler analog der Transaktionsprozessorfunktion im Code Snippet 18 verworfen wird. Die Fälle 13 und 15 verifizieren, dass ein korrektes Zertifikat angegeben wird sowie dass der Händler die Charge nicht ändern kann, nachdem ihm der Bauer diese übergeben hat. Der Testfall 14 ist insofern relevant,

als die Händler eigentlich nicht in der Lage sind neue Chargen zu erstellen. Jedoch muss er dazu in der Lage sein, wenn der Lizenznehmer nur eine Teilmenge der Charge weiterverkaufen möchte. Deshalb wird unter Punkt 14 überprüft, dass der Lizenznehmer grundsätzlich keine Berechtigung zur Erstellung von neuen Chargen hat, jedoch während der Transaktion einer Teilmenge einer Charge diese Operation für den Händler möglich ist (Testfall 16, siehe Code Snippet 27). Der Lizenznehmer überträgt den Integer 70, bei einer Chargengrösse von 120, worauf über die Transaktionsprozessorfunktion eine neue Charge mit der Menge 50 für den Händler erstellt wird. Anschliessend wird verifiziert, dass der Lizenznehmer tatsächlich im Besitz einer neuen Charge mit dem Wert 50 ist (Testfall 16, siehe Code Snippet 27). Darauffolgend wird im Testfall 17 überprüft, ob der angegebene Detailhändler (Retailer) die Charge mit der angegebenen Menge (70) erhalten hat und ob dieser tatsächlich die Historie der Charge sehen kann.

```
it('16. The licensee can transfer the a part of a charge to a retailer while
simultaneously creating a new one with the amount left', async () => {
 // Use the identity for the licensee Alberto
 await useIdentity(LicenseeAlberto);
 // create a valid transaction and submit it
 let transaction = factory.newTransaction(namespace, 'ChargeTransactionLicensee');
 transaction.newOwner = factory.newRelationship(namespace, retailerType, '92007');
 //smaller amount than the actual charge
 transaction.amount = 70;
 transaction.cert = factory.newRelationship(namespace, certificateType, '200000');
 transaction.charge = factory.newRelationship(namespace, chargeType, '55555555');
 await businessNetworkConnection.submitTransaction(transaction);
 //get the available assets for the licensee
 let assetRegistry1 = await businessNetworkConnection.getAssetRegistry(chargeNS);
 let asset = await assetRegistry1.getAll();
 let asset1 = asset[0];
 // check the owner of the newly created charge durring the transaction
 asset1.owner.getFullyQualifiedIdentifier().should.equal(licenseeNS+ '#33702');
 // the amount left should be the size of the new charge->50
 asset1.amount = 50;
 asset1.productType.should.equal("Broccoli");
});
```

Code Snippet 27: Test case 16, testLogic.js, slightly modified Git Commit: "updated trade logic" (Anhang C, 2018)

In den Testfällen 18-24 werden die Funktionen des Markplatzes getestet. Im Mocha-Test mit der Nummer 18 wird überprüft, ob der Landwirt ein Angebot erstellen kann. In Nummer 19 wird getestet, ob ein Händler das Angebot im Besitz des Ausstellers noch nicht lesen kann. Dies darf erst möglich sein, wenn der Bauer dies dem Marktplatz übergeben hat, was in den Testfällen 20 und 21 verifiziert und durch die «Access Rules» im Code Snippet 20 ermöglicht wird. Darauffolgend kann der Lizenznehmer eine Bestätigung erstellen (22) und diese anschliessend direkt übergeben (Testfall 23, siehe Code Snippet 28). Wenn die Bestätigung gültig ist, wird diese gemäss der Transaktionsprozessorfunktion im Code Snippet 21 direkt an den Antragssteller weitergeleitet und der Lizenznehmer erhält das entsprechende Angebot als Beweis für den

erfolgreich erstellten «Handelsvertrag». Die tatsächliche Übergabe der Charge wird zu diesem Stand des Prototyps noch nicht initialisiert, da vorerst auf eine erfolgreiche Geldüberweisung gewartet werden muss. Der finanzielle Aspekt wurde bei der Erstellung dieses Prototyps noch nicht miteinbezogen und muss in zukünftigen Arbeiten untersucht werden.

```
it('23. The licensee can place the offer confirmation on the marketplace and receives the
offer if the confirmation is valid', async () => {
 // Use the identity for the licensee Alberto
 await useIdentity(LicenseeAlberto);
 // create a confirmation for the offer and submit it
 let transaction = factory.newTransaction(namespace, 'OfferConfTransaction');
 transaction.offConf = factory.newRelationship(namespace, offerConfirmationType,
 '65735142');
 await businessNetworkConnection.submitTransaction(transaction);
 //the offer confirmation goes directly to the issuer of the offer and the licensee gets
 the offer as a form of confirmation from the marketplace
 let assetRegistry1 = await businessNetworkConnection.getAssetRegistry(offerNS);
 let asset1 = await assetRegistry1.get('2687687');
 // Check the owner of the offer, the issuer and the content
 asset1.owner.getFullyQualifiedIdentifier().should.equal(licenseeNS+ '#33702');
 asset1.issuer.getFullyQualifiedIdentifier().should.equal(farmerTypeNS+ '#12576');
 asset1.productType.should.equal("Broccoli");
 asset1.amount = 300;
});
```

Code Snippet 28: Test case 23, testLogic.js, slightly modified Git Commit: "updated trade logic" (Anhang C, 2018)

Bei den letzten zwei Testfällen (24 & 25) wird lediglich verifiziert, ob der Landwirt seine Angebotsbestätigung erhält und ob eine Kontrollstelle ein Zertifikat löschen kann, welches nicht mehr in ihrem Besitz ist, aber von dieser Kontrollstelle ausgestellt wurde. Bei der Erstellung dieser Testfälle wurde darauf geachtet, dass ein möglichst breites Feld an Funktionen nach einem logischen Geschäftsablauf überprüft wird. In der folgenden Abbildung 20 können die Resultate der erfolgreichen Überprüfung sämtlicher Mocha-Testfälle angesehen werden. Die Bedeutung und Diskussion dieser Resultate wird im Kapitel 8.2 erläutert

```
PROBLEMS   OUTPUT   DEBUG CONSOLE   TERMINAL
/home/nik/.nvm/versions/node/v8.11.1/bin/node --inspect-brk=31576 node_modules/mocha/bin/_mocha -u tdd --timeout 999999 --colors /home/nik/fabric-tools/label-chain/
Debugger listening on ws://127.0.0.1:31576/95107a3b-fbe0-4515-a01b-84353683d088
Debugger attached.

  Sample                                                                                                                                                    spec.js:46
    ✓ 1. The label can create and read the mandate (169ms)                                                                                                  spec.js:46
    ✓ 2. The label can transfer the mandate to a control authority (127ms)                                                                                  spec.js:73
    ✓ 3. The control authority can NOT transfer their mandate tho another organization (76ms)                                                               spec.js:73
    ✓ 4. The control authority can create certificates for a farmer and a licensee (165ms)                                                                  spec.js:73
    ✓ 5. The control authority can transfer the certificate to the Farmer & the licensee (187ms)                                                            spec.js:73
    ✓ 6. The farmer can NOT transfer the certificate (64ms)                                                                                                 spec.js:73
    ✓ 7. The farmer can NOT update or alter the certificate (62ms)                                                                                          spec.js:73
    ✓ 8. The farmer can create a charge (112ms)                                                                                                             spec.js:73
    ✓ 9. The farmer can transfer the charge to a licensee (78ms)                                                                                            spec.js:73
    ✓ 10. The farmer can create another charge without a correct certificate (127ms)                                                                        spec.js:73
    ✓ 11. The farmer can NOT trade a charge without a correct certificate (103ms)                                                                           spec.js:73
    ✓ 12. The licensee can NOT transfer a higher amount then he owns to a retailer (108ms)                                                                  spec.js:73
    ✓ 13. The licensee can NOT transfer with another certificate or an incorrect one (74ms)                                                                 spec.js:73
    ✓ 14. The licensee can NOT create a new charge only during transaction (78ms)                                                                           spec.js:73
    ✓ 15. The licensee can NOT update or alter the charge (75ms)                                                                                            spec.js:73
    ✓ 16. The licensee can transfer the a part of a charge to a retailer while simultaneously creating a new one with the amount left (116ms)               spec.js:73
    ✓ 17. The retailer can see his asset and the history of the asset (82ms)                                                                                spec.js:73
    ✓ 18. The farmer can create an offer (85ms)                                                                                                             spec.js:73
    ✓ 19. The licensee can NOT read offers which not have been shared (55ms)                                                                                spec.js:73
    ✓ 20. The farmer can place the offer on the marketplace (76ms)                                                                                          spec.js:73
    ✓ 21. The licensee is able to read the offers on the marketplace (54ms)                                                                                 spec.js:73
    ✓ 22. The licensee can create an offer confirmation (91ms)                                                                                              spec.js:73
    ✓ 23. The licensee can place the offer confirmation on the marketplace and receives the offer if the confirmation is valid (125ms)                      spec.js:73
    ✓ 24. The farmer gets his offer confirmation and can see it (155ms)                                                                                     spec.js:73
    ✓ 25. The control authority can remove one of their certificates (109ms)                                                                                spec.js:73
  25 passing (4s)                                                                                                                                           base.js:354
```

Abbildung 19: Output der Mocha-Tests, (Eigene Darstellung, 2018)

8 Diskussion & Handlungsempfehlungen

In diesem Kapitel wird der gesamte Prozess von der Konzeptionierung bis hin zur Umsetzung der «Label-Chain» diskutiert. Die Diskussion der Blockchain-Technologie muss auf unterschiedlichen Ebenen geschehen. Denn bereits beim ursprünglichen Entwurf von Nakamoto, (2008) war es das Ziel, eine Währung ohne Institution (Nationalbank) zu entwerfen. Des Weiteren wurde im Konzept von Nakamoto auch Überlegung zur Incentivierung der beteiligten Minern gemacht. Diese ökonomischen Aspekte verschaffen zusammen mit den technischen Komponenten wie der asymmetrischen Kryptographie oder den verteilten Systemen den tatsächlichen Nutzen, respektive einen Vorteil gegenüber herkömmlichen Lösungen. Deshalb ist es notwendig, alle involvierten Bereiche zu untersuchen, um aussagekräftige Forschung im Bereich der Blockchain zu betreiben. Aus diesem Grund wurde auch eine Design Science Vorgehensweise gewählt, weil dadurch von der wirtschaftlichen Betrachtung bis zur Umsetzung, also der gesamte Prozess enthalten sein kann. Im folgenden Kapitel 8.1 wird der gesamte Prozess und die Ergebnisse der Use Case Erarbeitung (Kapitel 6) diskutiert, die Hauptresultate wiederholt und auf mögliche Generalisierungen hingewiesen sowie Handlungsempfehlungen abgegeben Anschliessend wird dieser Prozess identisch für das Kapitel der «Umsetzung der Label-Chain» (7) durchgeführt.

8.1 Use Case Erarbeitung

Bei den Untersuchungen an der exemplarischen Organisation «Bio Suisse» konnten anlehnend an die DSRM einige unterschiedliche Problemfelder im Bereich des SCMs identifiziert werden, welche vorstellbare Lösungskonzepte in Zusammenhang mit der Blockchain ermöglichten. Um gleichzeitig die angesprochenen verschiedenen Ebenen der Blockchain-Technologie zu untersuchen und den angestrebten Umfang der Thesis einzuhalten, wurden die Konzepte mit passenden Methoden, wie beispielsweise der Stakeholderanalyse, präziser untersucht. Jedoch gilt es anzumerken, dass die Anspruchsgruppen (Stakeholder) nicht direkt befragt wurden, sondern nur mit möglichen Szenarien und Annahmen gearbeitet wurde. Dieser Bereich der Arbeit muss in weitergehenden Projekten untersucht werden. Trotzdem konnten mögliche Bedingungen und Merkmale eruiert werden, welche zutreffen müssen, um den Einsatz von Blockchain zu rechtfertigen. Beispielsweise schien anfänglich das Ziel der «Provenance» oder der Rückverfolgbarkeit im Zusammenhang mit der Supply-Chain und den verschiedenen beteiligten Parteien als vielversprechendes Anwendungsfeld für die Blockchain. Jedoch stellt sich bei genauer Betrachtung die Frage, weshalb diese Aufgabe nicht von einer vertrauenswürdigen

Drittpartei übernommen werden kann. Für eine globale Supply-Chain mit einer sehr hohen Anzahl an unterschiedlichen Parteien ist die Situation möglicherweise anders zu beurteilen. Aber im ausgewählten Anwendungsfall der Labels ist die blosse Rückverfolgbarkeit effizienter mit konventionellen Technologien zu erreichen. Da die Labels als vertrauenswürdige Intermediäre zwischen Kunden und Produzenten agieren, können sie de facto als vertrauenswürdige Drittpartei bezeichnet werden. Des Weiteren wurde bei der erweiterten Recherche festgestellt, dass es bereits in Deutschland solche Lösungen gibt, wie besipielsweise die Website «Bio mit Gesicht», über welche die Konsumenten nachvollziehen können, von welcher Person ihre Bioprodukte hergestellt worden sind. Aus diesen Gründen wurde ersichtlich, dass eine Applikation, die einzig zum Ziel hat, die Rückerverfolgbarkeit der Supply-Chain mithilfe der Blockchain sicherzustellen, in diesem Kontext nicht zielführend ist. Auch im Rahmen der allgemeinen Diskussion über den Einsatz von Blockchain im SCM-Umfeld konnte diese Problematik festgestellt werden. Dies sind Indikatoren dafür, dass vermutlich in einigen dokumentierten Anwendungsfällen tendenziell das Potenzial der Blockchain eher zu hoch eingestuft wird. Auch in einem Artikel von (Peck, 2017, S. 39) wird dieses Phänomen beobachtet. Ein Forscher von Microsoft wird von Peck mit der folgenden Aussage zitiert (Peck, 2017, S. 39): "*I find myself debunking a blockchain voting effort about every few weeks. It feels like a very good fit for voting, until you dig a couple millimeters below the surface*." Anschliessend wird erklärt, dass auch wenn ein Blockchain-Wahlsystem zur Verfügung steht, trotzdem eine zentrale Behörde benötigt wird für die Erstellung von Wahlzettel und der Authentisierung der Wähler. Wenn dieser Institution diese Aufgabe anvertraut wird, gibt es keinen Grund, dass sie nicht auch Stimmen zählen und speichern kann.

Die «Label-Chain» ist das vorgeschlagene Konzept, welches zum aktuellen Untersuchungsstand und den getroffenen Annahmen das grösste Potenzial versprach. Das Kernstück bilden die Konsortiumsparteien, also die verschiedenen Labels und die Lizenznehmer (Händler & Verarbeiter), welche in Zusammenarbeit eine Handelsplattform bilden und gleichzeitig die Rückverfolgbarkeit der Produkte, respektive die Transparenz der gehandelten Produkte, erhöhen. Die möglichen weiteren Teilnehmer wie die Bauern, profitieren bei einer Partizipation von neuen potenziellen Abnehmern. Die Endkunden und Grosseinkäufer haben einen erhöhten Vertrauenslevel in die Labels und können sicher zertifizierte Ware von unterschiedlichen Labels über die Plattform beziehen. Jedoch stellt sich an diesem Punkt die Frage, ob tatsächlich alle an einer erhöhten Transparenz und neuen Handelsmöglichkeiten Interesse haben. Möglicherweise gibt es Parteien, für welche die Intransparenz von Vorteil ist oder solche die befürchten, dass mit der Handelsplattform die Preise und Margen tiefer werden. Weitere Opposition könnte von den Zertifizierungsstellen ausgehen, welche befürchten, dass ihr Leistungsauftrag weiter reduziert

wird und Umsatzeinbussen durch eine solche Plattform für sie entstehen könnten. Eine weitere Gefahr sind Gesetze oder Normen, welche möglicherweise nicht mit der Plattform erfüllt werden können. Ein weiterer wichtiger Aspekt für eine Blockchain-Applikation, welcher in dieser Arbeit aus umfangstechnischen Gründen praktisch ausgegrenzt wurde, ist der Business Case und die Diskussion um das konkrete Geschäftsmodell. Obwohl festgehalten wurde, dass eine zentrale Einnahmequelle über die Handelsplattform generiert werden sollte, sind keine exakten Parameter für diese Plattform definiert worden. Beispielsweise könnte eine Einnahmequelle über ein Service Modell geschehen, indem zusätzliche Angebote wie Versicherung, Transport oder andere Services über die Plattform von Partnern angeboten wird. Ein weiteres Risiko bei einem denkbaren Blockchain-Einsatz ist, dass der Business Case nicht den Erwartungen der Teilnehmer entspricht und eine kostengünstigere Lösung von den Teilnehmern bevorzugt wird. Alle diese Aspekte sollten sowohl bei einer Weiterführung der «Label-Chain», wie auch bei zukünftiger Forschung im Bereich der Blockchain und dessen Anwendungsfelder berücksichtigt werden.

Eine weitere zu untersuchende Kernthematik, welche zu diesem Zeitpunkt noch nicht vollständig abgeschlossen werden kann, ist der «Blockchain-Fit» oder anders formuliert, ob die Blockchain-Technologie für einen spezifischen Anwendungsfall sinnvoll ist. Auch wenn im Rahmen der Arbeit drei Hauptmerkmale abstrahiert werden konnten, gibt es in diesem Bereich zu geringe Anzahl an empirisch erforschten Indikatoren, welche einen möglichen Blockchain-Use Case validieren könnten. Während dem Verfassen dieser Arbeit sind weitere Arbeiten von Organisationen publiziert worden. Beispielsweise das White Paper «*Blockchain Beyond the Hype - A Practical Framework for Business Leaders*», welches vom World Economic Forum Ende April 2018 veröffentlich wurde (Mulligan, Zhu Scott, Warren, & Rangaswami, 2018). Dieser Artikel konnte für die Arbeit nicht detailliert berücksichtigt werden, jedoch wurden auch dort Charakteristiken von Use Cases mit hohem Potenzial beschrieben (Mulligan et al., 2018). Diese fünf wurden im White Paper des WEFs gemäss Mulligan et al. (S. 8 2018) definiert:

- «Shared Repository (Informationen, die mehrere Parteien benötigen)»
- «Multiple Writers» (Mehr als eine Entität generiert Transaktionen und muss in die Blockchain schreiben)
- «Minimal Trust» (Ein Level von minimalem Vertrauen herrscht zwischen den Entitäten)
- «Intermediaries» (Einer oder mehrere Vermittler sind notwendig, um das Vertrauen zu stärken)
- «Transaction Dependencies» (Interaktion oder Abhängigkeit zwischen Transaktionen wird von verschiedenen Entitäten erzeugt)

Wenn nun diese fünf Charakteristiken verglichen werden mit den drei Hauptmerkmalen (siehe Kapitel 6.4), welche in der Master Thesis erarbeitet wurden, dann lässt sich feststellen, dass die Kerninhalte der Hauptmerkmale ebenfalls in diesen Charakteristiken vorhanden sind. Jedoch ist immer noch unklar, welche Use Cases tatsächlich in den produktiven Operations-Modus gehen und welche neue Business Modelle sich tatsächlich etablieren werden. Deshalb wird geraten, in diesem Bereich weitere Forschung zu betreiben und auf neue Entwicklungen im Blockchain-Umfeld zu achten, um eine faktenbasierte Grundlage zur Bewertung des Potenzials der Blockchain-Technologie zu erhalten. Eine weitere Problematik, welche bei der Evaluierung des Blockchain-Fits festgestellt wurde, ist die Bewertung des Trusts. Das Bewerten des Vertrauens zwischen Organisationen kann aufwendig sein und ist auch kein finaler Wert, sondern etwas, dass sich mit der Zeit verändert. Diese Frage konnte in Verbindung zur «Label-Chain» auch nicht abschliessend beantwortet werden. Zusätzlich wird die Auswertung des Vertrauens komplexer mit einer hohen Anzahl an Teilnehmern im Blockchain-Konsortium. Ein weiterer Faktor sind die kulturellen Komponenten, falls internationaler Handel betrieben wird. Wie bereits in der Problemidentifikation festgestellt wurde (siehe Kapitel 6.2), vertrauen nicht alle Experten den Kontrollen ausserhalb der Schweiz. In diesem Sinne könnte die «Label-Chain» tatsächlich das Vertrauen zwischen internationalen Handelspartnern fördern, insbesondere wenn eine Erweiterung der Applikation analog der Variante «IV» vollzogen würde (siehe Kapitel 6.5). Abschliessend gilt es zu sagen, dass bei diesem entwickelten Konzept zum aktuellen Wissensstand, der «Blockchain-Fit» erfüllt ist. Aber eine definitive Bestätigung dieser These lässt sich nur mithilfe von weiteren Untersuchungen und in Zusammenarbeit mit den Konsortiumsparteien erarbeiten.

8.2 Umsetzung der Label-Chain

Die Umsetzung des Prototyps wurde initialisiert mit der Untersuchung von unterschiedlichen Blockchain-Frameworks. Ausgehend von den Anforderungen des entworfenen Konzepts, konnten mögliche Frameworks verglichen und für eine allfällige Umsetzung im Hinblick auf die Label-Chain bewertet werden. Bei der Auswahl des zu verwendenden Blockchain-Frameworks wurden nur die drei bekannten Technologien, Ethereum, Hyperledger Fabric und Corda R3 verglichen. Dies wurde gemacht, weil die bekannteren Frameworks vermutlich ausgereifter sind als neuere Konkurrenztechnologien. Diese Entscheidung hat sich nachträglich nicht als falsch erwiesen, da sämtliche Anforderungen mithilfe des Hyperledger Composers abgebildet werden konnten. Bei der Auswahl der Technologie konnte festgestellt werden, dass beispielsweise bei Corda R3 und Hyperledger Fabric relativ viele Neuerungen in den letzten Monaten

dazugekommen sind. Dies lässt darauf schliessen, dass im Gebiet der Blockchain-Technologien in den nächsten Jahren noch einige Entwicklungen stattfinden werden. Einerseits ist dies eine positive Nachricht für das Blockchain-Umfeld, da klar erkennbar ist, dass aktiv an Verbesserungen der Technologien gearbeitet wird. Andererseits kann argumentiert werden, dass auch die bekannten Frameworks noch nicht vollständig ausgereift sind und nicht von einem Produktreifen «release» gesprochen werden kann. Beim hauptsächlich verwendeten Framework in dieser Arbeit, dem Hyperledger Composer, ist dieser Effekt sogar noch stärker festzustellen. Beim Beginn der Installation der definitiv verwendeten Entwicklungsumgebung wurde die Version 0.19.0 des Composers installiert. Beim Abgabedatum der Master Thesis war die letzte veröffentlichte Version bereits bei 0.19.5. Auch wenn der Hyperledger Composer als Prototyp, Pilot und Entwicklungsframework angepriesen wird und nicht mit «GA» (general availabiliy) vermerkt ist, sind dies Faktoren, welche Indizien zum Reifegrad der Technologie liefern. Für zukünftige Blockchain-Projekte sollte dies bei der Auswahl des zu verwendenden Frameworks beachtet werden. Des Weiteren sollte nach branchenspezifischen Frameworks Ausschau gehalten werden. Es ist anzunehmen, dass zukünftig noch weitere Blockchain-Technologien entworfen werden, welche beispielsweise für Anwendungen im Bereich des SCM zugeschnitten sind wie dies bei Corda R3 für Finanzdienstleistungen der Fall ist. Eine weitere Entwicklung, welche aktuell zu beobachten ist, sind branchenspezifische Blockchain-Services. Beispielsweise hat IBM vor kurzem das «Food Trust» Offering bekanntgegeben (IBM Blockchain, 2018). Mit dieser Cloud-basierten (SaaS) Blockchain- Lösung soll die «Traceability» erhöht und das «Certificate Management» vereinfacht werden (IBM Blockchain, 2018). Dies lässt vermuten, dass zukünftig noch etliche weitere ähnliche Angebote von IT-Dienstleistern in Zukunft auf dem Markt erhältlich sein werden und das Potenzial der Technologie von den IT-Unternehmen weiter als sehr hoch eingestuft wird. Diese neuen Blockchain Angebote sollten im Business Case berücksichtigt werden, denn die Verwendung eines Blockchain-Services ist vermutlich kostengünstiger, als die Entwicklung einer eigenen Lösung.

Nach der Entscheidung der Technologiewahl wurde mit der Installation der Entwicklungsumgebung und dem Aufsetzen des Composer-Frameworks begonnen. Anschliessend wurde mit der Entwicklung einer ersten Version eines lauffähigen Label-Chain-Netzwerkes gestartet. Das Ziel war zu überprüfen, ob die Installation fehlerfrei verlaufen ist und ob die angegeben Grundfunktionen des Composers ordnungsgemäss ausführbar sind. Nachdem das Geschäftsnetzwerkarchiv (.bna) erfolgreich auf einem Fabric-Netzwerk installiert werden konnte und das Durchführen einer Transaktion zwischen zwei Teilnehmern erfolgreich war, konnte mit der tatsächlichen Entwicklung der Label-Chain begonnen werden. Wäre zu diesem

Zeitpunkt festgestellt worden, dass gewisse Funktionalitäten nicht vorhanden sind oder das Framework schlichtweg nicht funktionsfähig ist, hätte eine andere Technologie verwendet werden müssen. Die Kernfunktionen des Composers stellten sich als sehr robust heraus, das heisst die Modellierungssprache, die Abfragen, die Zugriffsrechte sowie die Transaktionsprozessorfunktionen waren fehlerfrei ausführbar. Des Weiteren ist für die Verwendung des Quellcodeeditors «Virtual Studio Code» ein Plugin vorhanden, welches eine Syntaxhervorhebung, eine Autovervollständigungsfunktion und eine automatische Fehlerprüfung anbietet. Jedoch hat sich insbesondere beim Testen des Netzwerks herausgestellt, dass die Interaktion mit der CLI und dem Framework eher schwerfällig wirkt. Deshalb mussten auch eigene Bash-Skripts geschrieben werden, um den Entwicklungsprozess effizienter zu gestalten. Besonders für eine automatische Userverwaltung und der Verwendung des REST-Servers mit mehreren simultan zugreifenden Anwendern konnte keine effiziente Lösung gefunden werden. An diesem Punkt wird auch ersichtlich, dass der Composer für Prototyp- und Pilotentwicklungen gedacht ist und zum aktuellen Zeitpunkt nicht für den produktiven-Operationsmodus gedacht ist, was auch entsprechend so von den Entwicklern kommuniziert wird. Die Frage, die sich für sämtliche Blockchain-Frameworks hervorhebt und es zu beantworten gibt ist die folgende: Wie robust sind die Frameworks und Technologien hinsichtlich einer produktiven Umgebung und welche Applikationen sind tatsächlich im Einsatz?

Die Entwicklung der Label-Chain wurde in kleinen Iterationsschritten durchgeführt, wobei nur der erste sowie der letzte Stand dokumentiert ist. Dieses Vorgehen wurde primär gewählt, weil es sich wie bereits erwähnt beim Composer um ein neues Framework handelt und nicht absehbar ist, welche Funktionalitäten tatsächlich ausführbar sind. Des Weiteren hatte der Autor zuvor noch keine Erfahrungen mit der Entwicklung mit diesem Framework. Dieser iterative Ansatz ist wahrscheinlich für die Umsetzung eines gesamten Blockchain-Projekts sinnvoll. Denn nicht nur die Technologien sind noch nicht vollständig ausgereift, sondern die gesamte Vorgehensweise von der Konzeptionierung des Use-Cases bis zur Umsetzung des Projekts konnte noch in keiner Arbeit vorgefunden werden. Denn bei einem Blockchain-Projekt sind mehrere unterschiedliche Unternehmen beteiligt, wodurch die Anforderungen an die Applikationen abhängig von unterschiedlich involvierten Parteien ist. Das heisst ein Wasserfallmodell oder ein linearer Ansatz zur Konzeptionierung und Umsetzung eines Blockchain-Projektes scheint zum aktuellen Wissenstand nicht sinnvoll zu sein.

Bei der Entwicklung der Label-Chain-Applikation mussten diverse Bereiche abgegrenzt werden, um dem vorgegebenen Umfang der Thesis gerecht zu werden. Beispielsweise wurden sämtliche

integrationsaufwendige Bereiche nicht berücksichtigt. Insofern konnten zu diesem Zeitpunkt weder die Transportunternehmen zur Verfolgung der tatsächlichen Ware, noch der Finanzfluss berücksichtigt werden. Das angestrebte Ziel dieser Applikation, den Finanzfluss und Warenfluss zu vereinigen, konnte daher nicht vollständig erfüllt werden. Denn diese einzelnen Bereiche müssten intensiv mit Partnerunternehmen erarbeitet werden. Beispielsweise müsste um eine durchgängige Sendeverfolgung zu erreichen, sämtliche beteiligten Transportunternehmen kontaktiert werden und eine Lösung mit zusätzlichen Komponenten wie RFID oder IoT-Sensoren erarbeitet werden. Jedoch konnte bereits bei der Diskussion über den Einsatz von Blockchain in SCM festgestellt werden, dass die Verlinkung von einem digitalen Gut zu einem physisch existierenden Objekt ein ungelöstes Problem ist. Die Integration von Finanzdienstleistungen muss insbesondere auch bei der Erarbeitung des wirtschaftlichen Teils des Konzepts betrachtet werden. Denn diese Handelsplattform wird ab dem Zeitpunkt sehr wertvoll, sobald die Zahlungen oder Garantien für den Kauf von Ware vorhanden sind. Sobald beispielsweise ein Händler ein Angebot bestätigt, wird überprüft ob dieser zahlungsfähig ist und ob die entsprechenden Zertifikate für die entsprechenden Produkte vorhanden sind. Insofern wird die gesamte Plattform mit jeder zusätzlich integrierten Funktion vertrauenswürdiger und der gesamte Markt profitiert davon. Deshalb sollten diese Bereiche zwingend vor einer Fortsetzung des Projekts weiter untersucht werden.

Die Funktionalitäten der Label-Chain-Applikation konnten anhand der geschriebenen Testfälle evaluiert werden. Sämtliche 25 Testfälle konnten erfolgreich implementiert werden. Damit konnte gezeigt werden, dass die entwickelte Blockchain-Applikation die entsprechenden Anforderungen erfüllt und das System erwartungsgemäss läuft. Insofern ist dieser Prototyp ein Beweis dafür, dass es mit dem aktuell zur Verfügung stehenden Blockchain-Frameworks möglich ist eine Anwendung zu erstellen, mit welcher die Akteure einer Supply-Chain im Nahrungsmittelbereich ihre unterschiedlichen Rollen mit den dazugehörigen Funktionen wahrnehmen können. Jedoch gilt es klar zu definieren, dass es sich lediglich um einen Prototypen handelt und die finanzielle und der physische Warenfluss noch nicht vollständig abgebildet sind. Falls jedoch beispielsweise die finanzielle Komponente intergiert würde, könnte das Konzept der Label-Chain einen neuen Standard einer vertrauenswürdigen Handelsplattform bilden. Das heisst, es könnte ein fairer und transparenter Handel mit zertifizierten Nahrungsmitteln ermöglicht werden, was zu diesem Zeitpunkt im Markt noch nicht vorhanden ist. Insofern hat ein solches Konzept zum heutigen Wissenstand ein Potenzial zur Stärkung des Images, der Transparenz und der Effizienz der Labels.

9 Fazit

Der Fokus dieser Arbeit liegt auf der Untersuchung des Anwendungspotenzials der Blockchain-Technologie. Dazu wird in einem ersten Schritt in Form einer Vorstudie nach wissenschaftlichen Arbeiten über mögliche Anwendungsfelder der Blockchain gesucht. Durch diese gesammelte Variation an wissenschaftlichen Publikationen konnte ein Überblick zum aktuellen Forschungstand im Bereich der Anwendungsfelder der Blockchain gewonnen werden. Der festgelegte zu untersuchende Bereich, also der Einsatz von Blockchain im Zusammenhang mit dem Supply-Chain-Management, gab anfänglich den Eindruck eines vielversprechenden Anwendungsfeldes, da die Rückverfolgbarkeit bei einer Supply-Chain eine elementare Funktion darstellt. Jedoch stellte sich nachträglich heraus, dass dies nicht der Fall ist. Denn eine blosse Rückverfolgbarkeit der Güter innerhalb einer Supply-Chain, ist insbesondere beim ausgewählten Fall der Label-Chain effizienter mit konventionellen Technologien, wie beispielsweise einer gemeinsam verwendbaren Datenbank, zu erreichen. Da die Labels als vertrauenswürdige Intermediäre zwischen Kunden und Produzenten agieren, können sie de facto als vertrauenswürdige Drittpartei bezeichnet werden. Eine weitere Problematik für den Einsatz von Blockchain im SCM ist der Link zwischen der physischen und digitalen Welt, respektive ob ein Produkt authentisch ist und den digitalen Angaben in der Blockchain entspricht. Trotz vorhandenen Technologien wie RFID oder IoT-Sensoren, konnte keine abschliessende Antwort auf diese Problematik gefunden werden. Des Weiteren kam auch bei dieser Thematik erneut die Frage des Vertrauens zwischen interagierenden Business-Partnern auf oder anders formuliert, weshalb tatsächlich ein verteiltes System für die Lösung eines Problems benötigt wird, welches effizienter von einer Drittpartei gelöst werden kann. An diesem Punkt kann bereits von einer philosophischen Diskussion gesprochen werden, nämlich ob jeder Beteiligte bereit ist, einer möglicherweise mächtigen Institution aus Performanz und Kostengründen seine Daten anzuvertrauen oder ob der Wille da ist, ein verteiltes System gemeinsam zu betreuen. Aus diesen eben genannten Gründen war es sinnvoll, eine grössere Anzahl an Konzepten zu entwerfen, um dasjenige mit dem grössten Potenzial für die Umsetzung des Prototyps weiter zu verfolgen. Das entworfene Artefakt der Label-Chain ist eines, bei welchem ein neuer Standard einer vertrauenswürdigen Handelsplattform angestrebt wird. Das heisst die Zielsetzung der Label-Chain, einen faireren und transparenteren Handel mit zertifizierten Nahrungsmittel Label-übergreifend zu ermöglichen, hat zum aktuellen Wissensstand das grösste Potenzial.

Bei der technischen Umsetzung dieses Konzepts konnten sämtliche Kernfunktionen erfolgreich implementiert werden, jedoch ohne die tatsächliche physische Rückverfolgung und ohne

sämtliche Integration von Finanz-Services. Dies war auch nicht das Ziel des Prototyps, dass gilt es es in weiterführenden Projekten zu untersuchen. Die verwendeten Blockchain-Frameworks, also der Hyperledger Fabric und der Hyperledger Composer, stellten sich als robust heraus und sämtliche gewünschten Funktionalitäten konnten erfolgreich mit den Mocha-Testfällen evaluiert werden. Deshalb liegt das grösste noch zu lösende Problem hinsichtlich des Einsatzes dieser Frameworks, bei der Reife der Technologien für die Verwendung in einem produktiven Umfeld oder anders formuliert: Sind die Blockchain-Technologien tatsächlich «production-ready»? Zudem sollten die weiteren Entwicklungen im Angebot von Blockchain-Services und branchenspezifischen Frameworks beobachtet werden. Abschliessend gilt es zu erwähnen, dass in einigen untersuchten Fällen das Potenzial der Blockchain zu hoch eingeschätzt wird, es aber durchaus Bereiche gibt, in welchen der Einsatz einer Blockchain-Technologie sinnvoll ist.

Das gewählte Forschungsdesign, anlehnend an die Design Science Methodologie nach Peffers et al. (2007) und Hevner et al. (2004), stellte sich nachträglich als ein gutes Instrument heraus, um den Einsatz einer Technologie über sämtliche tangierende Aspekte zu betrachten und so einen Gesamtüberblick zu erlangen. Insofern konnte in dieser IS-Arbeit die wirtschaftlichen sowie die technologischen Komponenten, also der gesamte Prozess von der Konzeptionierung bis zur Umsetzung, betrachtet werden. Jedoch impliziert dies auch, dass es keinen fokussierten Forschungsbereich gab und in sämtlichen Teilen Umfangsabgrenzungen vorgenommen werden mussten. Trotzdem ist dieser Ansatz, besonders bei einer Technologie wie der Blockchain, eine passende Vorgehensweise zur Forschung über ein solch breites Feld. Insofern konnten die gewünschten Zielsetzungen dieser Arbeit erfüllt und entsprechende Antworten zu der Forschungsfrage gefunden werden.

10 Literaturverzeichnis

Adhami, S., Giudici, G., & Martinazzi, S. (2017). *Why Do Businesses Go Crypto? An Empirical Analysis of Initial Coin Offerings* (pp. 1–19). Milan: Università Bocconi, Milan-ITALY. Retrieved from https://ssrn.com/abstract=3046209

Andersen, E. S., Grude, K. V., & Haug, T. (2009). *Goal directed project management: effective techniques and strategies* (4th ed). London; Philadelphia: Kogan Page Limited.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., … Yellick, J. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. *ArXiv:1801.10228 [Cs]*. Retrieved from http://arxiv.org/abs/1801.10228

Anhang A. (2018, February 14). Anhang A, Bio Suisse Interne Dokumentation Supply Chain.

Anhang B. (2018). *Anhang B, Videoaufnahme der Besprechung Stakeholderanalyse und Konsortien, Nik Kessler & Oliver Gaede*. Altstetten.

Anhang C. (2018). Anhang C, GitHub Repository Master Thesis “Label-Chain”, Nik Kessler (Version 1.0.0). ZHAW. Retrieved from https://github.com/kesslnik/label-chain

Anhang D. (2018, April 21). Anhang D, Sammlung von unterschiedlichen Zertifikaten, Aus der Datenbank von ProCert & Bio Inspecta. Retrieved from https://www.bio-suisse.ch/de/kontrolleundzertifizierung.php

Baker, K. (2018). *Corda*. Retrieved from https://github.com/corda/corda (Original work published 2016)

Bio Suisse. (o.J.a). Die Marke Bio Suisse. Retrieved February 6, 2018, from https://www.bio-suisse.ch/de/diemarke.php

Bio Suisse. (o.J.b). Supply Chain Monitor Prozess. Retrieved March 3, 2018, from https://international.biosuisse.ch/de/scm.prozess

Bio Suisse. (2017a). *BIO SUISSE STATUTEN*. Retrieved from https://www.bio-suisse.ch/media/Ueberuns/ZahFak/statuten_ab_1-1-2018_d.pdf

Bio Suisse. (2017b). Jahresbericht. Retrieved February 18, 2018, from https://jahresbericht.biosuisse.ch/de/bericht

Bio Suisse. (2017c). Verbandsrechnung. Retrieved February 18, 2018, from https://jahresbericht.biosuisse.ch/de/verbandsrechnung

Bracher, K. (2013, April 6). Ärger über Bio-Importe bei den Bauern | NZZ. *Neue Zürcher Zeitung*. Retrieved from https://www.nzz.ch/schweiz/aerger-ueber-bio-importe-bei-den-bauern-1.18059640

Breitinger, E. (2012, January 18). Leichtes Spiel für Bio-Betrüger. *SALDO*, 8–9.

Castellanos, A. F., Coll-Mayor, D., & Notholt, J. A. (2017). Cryptocurrency as Guarantees of Origin: Simulating a Green Certificate Market with the Ethereum Blockchain (pp. 367–372). Presented at the IEEE International Conference on Smart Energy Grid Engineering.

CoinMarketCap. (2017, October 30). Cryptocurrency Market Capitalizations | CoinMarketCap. Retrieved October 30, 2017, from https://coinmarketcap.com/all/views/all/

Digiconomist. (2017). Bitcoin Energy Consumption Index. Retrieved November 25, 2017, from https://digiconomist.net/bitcoin-energy-consumption

European Comission. (o.J.). Economic Operators Registration and Identification number (EORI). Retrieved May 12, 2018, from https://ec.europa.eu/taxation_customs/business/customs-procedures/general-overview/economic-operators-registration-identification-number-eori_en

Everledger Ltd. (2017). Everledger | A Digital Global Ledger. Retrieved November 7, 2017, from https://www.everledger.io/

Eyal, I., & Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In *International conference on financial cryptography and data security* (pp. 436–454). Springer.

Follow My Vote, Inc. (2017). Blockchain Technology in Online Voting. Retrieved November 7, 2017, from https://followmyvote.com/online-voting-technology/blockchain-technology/

Freeman, R. E. (2010). *Strategic Management: A Stakeholder Approach*. Cambridge University Press.

Frohlich, M. T., & Westbrook, R. (2002). Demand chain management in manufacturing and services: web-based integration, drivers and performance. *Journal of Operations Management*, *20*(6), 729–745. https://doi.org/10.1016/S0272-6963(02)00037-2

Gartner Inc. (2017, August 15). Gartner Identifies Three Megatrends That Will Drive Digital Business Into the Next Decade. Retrieved October 29, 2017, from //www.gartner.com/newsroom/id/3784363

Gogerty, N., & Zitoli, J. (2011). DeKo: An electricity-backed currency proposal. Retrieved from http://ssrn.com/abstract=1802166

Harrison, K. (2018, March 16). Getting started on the IBM Blockchain Platform Starter Plan. Retrieved May 15, 2018, from https://www.ibm.com/blogs/blockchain/2018/03/getting-started-on-the-ibm-blockchain-platform-starter-plan/

Herbert, Z. (2017, February 6). Why blockchains are the future of cloud storage. Retrieved November 5, 2017, from https://blog.sia.tech/why-blockchains-are-the-future-of-cloud-storage-91f0b48cfce9

Hevner, A. R., March, S. T., & Ram, S. (2004). DESIGN SCIENCE IN INFORMATION SYSTEMS RESEARCH. *MIS Quarterly*, *28*(1), 75–105.

Hyperledger. (2017a). Ledger — hyperledger-fabricdocs master documentation. Retrieved May 3, 2018, from http://hyperledger-fabric.readthedocs.io/en/master/ledger/ledger.html#world-state

Hyperledger. (2017b, September 12). Meet the TSC: Arnaud Le Hors, IBM. Retrieved March 20, 2018, from https://www.hyperledger.org/blog/2017/09/12/3431

Hyperledger. (2018). Release Notes — hyperledger-fabricdocs master documentation. Retrieved April 8, 2018, from http://hyperledger-fabric.readthedocs.io/en/release-1.1/releases.html

Hyperledger Composer. (o.J.a). Access Control Language. Retrieved May 3, 2018, from https://hyperledger.github.io/composer/latest/reference/acl_language.html

Hyperledger Composer. (o.J.b). Deploying Business Networks. Retrieved May 4, 2018, from https://hyperledger.github.io/composer/latest/business-network/bnd-deploy.html

Hyperledger Composer. (o.J.c). Deploying to a multi-organization Hyperledger Fabric. Retrieved May 12, 2018, from https://hyperledger.github.io/composer/latest/tutorials/deploy-to-fabric-multi-org

Hyperledger Composer. (o.J.d). Installing pre-requisites for Composer. Retrieved April 22, 2018, from https://hyperledger.github.io/composer/latest/installing/installing-prereqs.html

Hyperledger Composer. (o.J.e). Introduction Hyperledger Composer. Retrieved April 8, 2018, from https://hyperledger.github.io/composer/latest/introduction/introduction.html

Hyperledger Composer. (o.J.f). Modeling Language. Retrieved May 1, 2018, from https://hyperledger.github.io/composer/latest/reference/cto_language.html

Hyperledger Composer. (o.J.g). Transaction Processor Functions. Retrieved May 3, 2018, from https://hyperledger.github.io/composer/latest/reference/js_scripts.html

Hyperledger Composer. (o.J.h). Using Queries and Filters with Business Network Data. Retrieved May 3, 2018, from https://hyperledger.github.io/composer/latest/business-network/query.html

Hyperlegder. (2017). Prerequisites — hyperledger-fabricdocs master documentation. Retrieved April 22, 2018, from http://hyperledger-fabric.readthedocs.io/en/release-1.1/prereqs.html

IBM Blockchain. (2018, April 20). IBM Food Trust - IBM Blockchain. Retrieved May 23, 2018, from https://www.ibm.com/blockchain/solutions/food-trust/technology/

IBM Research. (2018). Crypto-anchors and Blockchain - IBM Research. Retrieved March 31, 2018, from https://www.research.ibm.com/5-in-5/crypto-anchors-and-blockchain/

Jepsen, A. L., & Eskerod, P. (2009). Stakeholder analysis in projects: Challenges in using current guidelines in the real world. *International Journal of Project Management*, *27*(4), 335–343. https://doi.org/10.1016/j.ijproman.2008.04.002

Kandaswamy, R., & Chesini, F. (2017). How to Determine If You Need a Blockchain Project, and If So, What Kind? *G00320247*, 6.

Kandaswamy, R., & Furlonger, D. (2017). How to Develop a Business Case for Blockchain Projects. *G00323011*, 8.

Kärkkäinen, M. (2003). Increasing efficiency in the supply chain for short shelf life goods using RFID tagging. *International Journal of Retail & Distribution Management*, *31*(10), 529–536. https://doi.org/10.1108/09590550310497058

Kasey Panetta. (2017, June 5). Are You Ready for Blockchain? [Infographic]. Retrieved March 30, 2018, from https://www.gartner.com/smarterwithgartner/are-you-ready-for-blockchain-infographic/

Kharpal, A. (2016, October 3). Richard Branson: Blockchain could create 'economic revolution' in emerging markets. Retrieved October 29, 2017, from https://www.cnbc.com/2016/10/03/richard-branson-blockchain-could-create-economic-revolution-in-emerging-markets.html

Le Hors, A. (2018, March). *Blockchain for Business based on Hyperledger Fabric*. Presented at the IBM Swiss Blockchain Day, Rueschlikon.

Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability. In *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)* (pp. 468–477). https://doi.org/10.1109/CCGRID.2017.8

Lux, T. (2017, September 29). FINMA trifft Abklärungen bei ICOs. Retrieved November 4, 2017, from https://www.finma.ch/de/news/2017/09/20170929-mm-ico/

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, *20*(3), 709. https://doi.org/10.2307/258792

McAllister, D. J. (1995). AFFECT- AND COGNITION-BASED TRUST AS FOUNDATIONS FOR INTERPERSONAL COOPERATION IN ORGANIZATIONS. *Academy of Management Journal*, *38*(1), 24–59. https://doi.org/10.2307/256727

Mertens, P. (2009). *Studienführer Wirtschaftsinformatik: 2009*. (K. Kurbel, Ed.) (1. Aufl). Wiesbaden: Gabler.

Michael, K., & McCathie, L. (2005). The pros and cons of RFID in supply chain management. In *International Conference on Mobile Business (ICMB'05)* (pp. 623–629). https://doi.org/10.1109/ICMB.2005.103

mochajs.org. (2018, May 8). Mocha - the fun, simple, flexible JavaScript test framework. Retrieved May 16, 2018, from https://mochajs.org/

Mozilla Developer Network. (2018, May 11). async function. Retrieved May 12, 2018, from https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Statements/async_function

Müller, J. (2017, September 30). Der Krypto-Boom scheucht die Schweizer Behörden auf | NZZ. *Neue Zürcher Zeitung*. Retrieved from https://www.nzz.ch/wirtschaft/der-boom-der-kryptowaehrungen-scheucht-die-schweizer-behoerden-auf-ld.1319369

Mulligan, C., Zhu Scott, J., Warren, S., & Rangaswami, J. (2018). *Blockchain Beyond the Hype - A Practical Framework for Business Leaders* (White Paper). Switzerland. Retrieved from http://www3.weforum.org/docs/48423_Whether_Blockchain_WP.pdf

Nakamoto, S. (2008). Bitcoin A Peer-to-Peer Electronic Cash System. Retrieved October 29, 2017, from https://bitcoin.org/bitcoin.pdf

Newcombe, R. (2003). From client to project stakeholders: a stakeholder mapping approach. *Construction Management and Economics*, *21*(8), 841–848. https://doi.org/10.1080/0144619032000072137

Peck, M. E. (2017). Blockchain world-Do you need a blockchain? This chart will tell you if the technology can solve your problem. *IEEE Spectrum*, *54*(10), 38–60.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Petersen, M., Hackius, N., & Kersten, W. (2016). Blockchain für Produktion und Logisitk. *ZWF Zeitschrift Für Wirtschaftlichen Fabrikbetrieb*, *10*(111), 626–629.

Peterson, K., Deeduvanu, R., Kanjamala, P., & Boles, K. (2016). *A Blockchain-Based Approach to Health Information Exchange Networks*.

Ramachandran, A., & Kantarcioglu, D. (2017). Using Blockchain and smart contracts for secure data provenance management. *ArXiv Preprint ArXiv:1709.10000*.

Rist, M. (2017, September 30). Banken drehen Kryptowährungen den Geldhahn zu | NZZ. *Neue Zürcher Zeitung*. Retrieved from https://www.nzz.ch/wirtschaft/banken-drehen-kryptowaehrungen-den-geldhahn-zu-ld.1319371

Roehrs, A., da Costa, C. A., & da Rosa Righi, R. (2017). OmniPHR: A distributed architecture model to integrate personal health records. *Journal of Biomedical Informatics*, *71*, 70–81. https://doi.org/10.1016/j.jbi.2017.05.012

Schürer, C., & Kressbach, M. (2012, January 3). Konsum - Gefälschte Bio-Produkte in der Schweiz. Retrieved March 3, 2018, from https://www.srf.ch/sendungen/kassensturz-espresso/themen/konsum/gefaelschte-bio-produkte-in-der-schweiz

Sharma, P. K., Chen, M.-Y., & Park, J. H. (2017). A Software Defined Fog Node based Distributed Blockchain Cloud Architecture for IoT. *IEEE Access*, 1–10. https://doi.org/10.1109/ACCESS.2017.2757955

Skuchain. (o.J.). Skuchain: Empower my supply chain | Empower my supply chain. Retrieved April 17, 2018, from http://www.skuchain.com/

Smith, S. (2018). *The Composer REST Server*. Retrieved from https://github.com/hyperledger/composer/wiki/Composer-REST-Server

The Linux Foundation. (2017). Hyperledger Composer. Retrieved April 8, 2018, from https://www.hyperledger.org/projects/composer

The SolarCoin Foundation. (2017). SolarCoin. Retrieved November 26, 2017, from https://solarcoin.org/

Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID blockchain technology. In *2016 13th International Conference on Service Systems and Service Management (ICSSSM)* (pp. 1–6). https://doi.org/10.1109/ICSSSM.2016.7538424

Valenta, M., & Sandner, P. (2017). *Comparison of Ethereum, Hyperledger Fabric and Corda* (p. 8). Frankfurt: Frankfurt School Blockchain Center. Retrieved from http://explore-ip.com/2017_Comparison-of-Ethereum-Hyperledger-Corda.pdf

Vukolić, M. (2016). The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. In J. Camenisch & D. Kesdoğan (Eds.), *Open Problems in Network Security* (Vol. 9591, pp. 112–125). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-39028-4_9

Wirtschaftslexikon24. (2017). Konsortium - Wirtschaftslexikon. Retrieved March 20, 2018, from http://www.wirtschaftslexikon24.com/d/konsortium/konsortium.htm

Wüst, K., & Gervais, A. (2017). *Do you need a Blockchain?* (p. 7). Zürich: Department of Computer Science, ETH Zürich.

Yadav, M. (2017). *Exploring Signals for Investing in an Initial Coin Offering (ICO)* (pp. 1–14). Berlin: Technische Universität Berlin. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3037106

Yi, S., Hao, Z., Qin, Z., & Li, Q. (2015). Fog Computing: Platform and Applications (pp. 73–78). IEEE. https://doi.org/10.1109/HotWeb.2015.22

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends (pp. 557–564). IEEE. https://doi.org/10.1109/BigDataCongress.2017.85