

Bachelor-Thesis an der Hochschule Luzern - Technik & Architektur

Titel	Identity of Things mit IOTA am Beispiel eines Trackingsystems in der Supply Chain
Diplomandin/Diplomand	Pfammatter, Florence
Bachelor-Studiengang	Bachelor Wirtschaftsingenieur Innovation
Semester	HS19
Dozentin/Dozent	Weingärtner, Tim
Expertin/Experte	Schimpel, Ulrich

Abstract Deutsch

Identity of Things (IDoT), das Identitätsmanagement von Dingen, ist in Anbetracht der rasch zunehmenden Zahl vernetzter Geräte ein wichtiges Forschungsthema. Bei der Entwicklung von Lösungen zu IDoT wird auch die Verwendung von Distributed Ledger Technologien (DLT) diskutiert. Dadurch soll die Unabhängigkeit eines Subjekts (Self Sovereign Identity – SSI) gestärkt und Datensicherheit, Datenschutz und Manipulationsmöglichkeiten berücksichtigt werden. In dieser Arbeit wird IDoT mit der Distributed Ledger Technologie IOTA anhand eines Trackingsystems in der Supply Chain betrachtet. Durch den Anwendungsfall werden technische und unternehmerische Chancen und Risiken beim Einsatz der genannten Technologien identifiziert. Nach der Umfrage mit Stakeholdern der Logistikbranche und einer Analyse zur Notwendigkeit eines Distributed Ledgers wurde der ursprüngliche Anwendungsfall und die dazugehörige Lösung abgeändert. Das überarbeitete Lösungskonzept ist ein Trackingsystem für Liefereinheiten, welches auf das Tracking von Positionsdaten spezialisiert ist. Ein explorativer Prototyp und dazu passende Experimente testen die Tauglichkeit des überarbeiteten Lösungskonzepts. Die Experimente zeigen, dass Verifiable Claims und Sensordaten mit IOTA auf einfache Weise verwaltet werden können. Jedoch verhindern Sicherheitsmängel, z. B. beim Management des Lesezugriffs, eine Verwendung in Produktionsumgebung. Werden diese Probleme gelöst, bieten IDoT und DLT eine subjektspezifische Nachverfolgbarkeit für eine sichere Digitalisierung der Supply Chain.

Alle Rechte vorbehalten. Die Arbeit oder Teile davon dürfen ohne schriftliche Genehmigung der Rechteinhaber weder in irgendeiner Form reproduziert noch elektronisch gespeichert, verarbeitet, vervielfältigt oder verbreitet werden.

Sofern die Arbeit auf der Website der Hochschule Luzern online veröffentlicht wird, können abweichende Nutzungsbedingungen unter Creative-Commons-Lizenzen gelten. Massgebend ist in diesem Fall die auf der Website angezeigte Creative-Commons-Lizenz.

Abstract Englisch

Identity of Things (IDoT), the identity management for things, is, considering the fast-growing number of connected devices, an important research topic. An enabling technology for IDoT are Distributed Ledgers: Using Distributed Ledgers should foster the independence of a subject (Self Sovereign Identity – SSI) and thus address data security, data privacy and manipulation possibilities. This paper examines IDoT and the Distributed Ledger Technology IOTA with the example of a tracking system in the supply chain. The aim of this thesis is to identify technical and entrepreneurial chances and risks for the given use case. After the survey of stakeholders in logistics and an analysis of the need for a Distributed Ledger, the original use case and its solution were modified. The revised solution represents a tracking system for packaging units with focus on tracking positional data. Finally, an explorative prototype and corresponding experiments tested the solution concept. The experiments show that Verifiable Claims and sensor data can easily be managed with IOTA. However critical security issues, e.g. in read access management, prevent the current solution from being realized in a production environment. When these security issues are resolved, IDoT, supported by a Distributed Ledger, represents the ideal solution to ensure traceability and transparency for the digitalization in the supply chain.

Ort, Datum

Luzern, 22.12.19

© **Florence Pfammatter, Hochschule Luzern – Technik & Architektur**

Die in der Abschlussarbeit gewählte männliche Form bezieht sich immer zugleich auf weibliche und männliche Personen.

Inhaltsverzeichnis

Abbildungsverzeichnis	VI
Tabellenverzeichnis	VII
Abkürzungsverzeichnis	VIII
1 Einleitung	9
1.1 Ausgangssituation	9
1.2 Problemstellung.....	9
1.3 Zielsetzung	9
1.4 Struktur der Arbeit.....	9
2 Methodik	11
2.1 Literaturrecherche	11
2.2 Kundenprofile.....	12
2.3 Online-Umfrage zur Bedürfniserfassung.....	12
2.4 Exploratives Vorgehensmodell	12
3 Grundlagen	13
3.1 Grundlagen Identity of Things	13
3.1.1 Wichtige Begriffe im Identitätsmanagement.....	13
3.1.2 Traditionelle Identitätsmanagementsysteme	14
3.1.3 Self-Sovereign Identity und Dezentrales Identitätsmanagement	15
3.1.4 Anforderungen für Identity of Things	17
3.1.5 Erkenntnisse Identity of Things.....	18
3.2 Übersicht zu IOTA	18
3.2.1 Einführung in Distributed Ledger Technologien.....	18
3.2.2 Einführung in IOTA	19
3.2.3 Masked Authenticated Messaging (MAM)	21
3.3 DLT-basierte Geschäftsmodelle in der Supply Chain	23
3.3.1 Herausforderungen in der Supply Chain	23
3.3.2 Fallstudie DLT-basierte Lösungen in der Supply Chain	23
3.3.3 Erkenntnisse DLT-basierte Geschäftsmodelle	25
4 Anwendungsfall Fahrdaten-Trackingsystem.....	26
4.1 Kundenprofile für beschriebenen Anwendungsfall.....	26
4.1.1 Ergebnisse Erstellung Kundenprofile.....	28

5	Prüfung in unternehmerischer Hinsicht.....	29
5.1	Eignung eines Distributed Ledgers	29
5.1.1	Ergebnisse Eignung eines Distributed Ledgers	32
5.2	Umfrage mit Stakeholdern der Logistikbranche	33
5.2.1	Ergebnisse Umfrage	37
5.3	Überarbeiteter Anwendungsfall.....	38
6	Technische Lösung.....	39
6.1	Konzept	39
6.1.1	Entscheidungen	40
6.1.2	Beschreibung der Systemabläufe.....	42
6.1.3	Wahl der Experimente.....	45
6.2	Experiment Identitätsmanagement mit IOTA	46
6.2.1	Ergebnisse Identitätsmanagement mit IOTA	50
6.3	Experiment Masked Authenticated Messaging	51
6.3.1	Ergebnisse Masked Authenticated Messaging	55
6.4	Funktionales Testen.....	55
6.4.1	Ergebnisse Funktionales Testing	56
7	Zusammenfassung der Ergebnisse	60
7.1	Erkenntnisse Literaturrecherche.....	60
7.2	Ergebnisse Überprüfung in unternehmerischer Hinsicht.....	61
7.3	Ergebnisse Technische Umsetzung	62
7.3.1	Tauglichkeit der Systemlösung	63
8	Schlussbetrachtung und Ausblick.....	65
8.1	Reflexion	65
8.2	Empfehlungen	66
8.3	Zukünftiger Forschungsbedarf	67
	Literaturverzeichnis.....	LXVIII
	Anhang	LXXI

Abbildungsverzeichnis

Abbildung 1 Ablauf der Forschungsarbeit	11
Abbildung 2 Network-based und Claim-based Identitätsmanagement	15
Abbildung 3 Self-Sovereign Identity Architektur	16
Abbildung 4 Directed Acyclic Graph (DAG)	19
Abbildung 5 MAM Channels und Channel Splitting	22
Abbildung 6 Flow Chart «Do you Need a Blockchain? »	31
Abbildung 7 Architektur des Prototyps	39
Abbildung 8 MAM Channel Architektur	41
Abbildung 9 Ablauf Use Case 1	43
Abbildung 10 Ablauf Use Case 2	44
Abbildung 11 Ablauf Use Case 3	45
Abbildung 12 Versuchsaufbau Experiment Identitätsmanagement mit IOTA	46
Abbildung 13 Erstellung eines Identitätsdokuments für einen Raspberry Pi	47
Abbildung 14 Payload einer MAM-Transaktion	47
Abbildung 15 Message im MAM Explorer	48
Abbildung 16 Verifikation gescheitert	48
Abbildung 17 Erfolgreiche Verifikation	49
Abbildung 18 Update sichtbar auf MAM Explorer	49
Abbildung 19 Abgefragte GNSS-Daten	52
Abbildung 20 MAM-State Initialisierung mit und ohne eigenen Seed	53
Abbildung 21 Überschreiben von Nachrichten sichtbar auf MAM Explorer	53
Abbildung 22 MAM State Objekt	54
Abbildung 23 Website mit abgerufenen MAM Messages	54
Abbildung 24 Test API Trackinggerät	57
Abbildung 25 User Interface Authentifizierung	57
Abbildung 26 Erstellung einer Liefereinheit	58
Abbildung 27 Trackingdaten abrufen	59

Tabellenverzeichnis

Tabelle 1 Kundenprofil Transport- und Logistikunternehmen.....	26
Tabelle 2 Kundenprofil Grenzkontrolle	27
Tabelle 3 Kundenprofil Produktionsunternehmen	27
Tabelle 4 Verwendete Hardware finaler Prototyp.....	40
Tabelle 5 Anforderungen basierend auf dem ersten Systemablauf.....	56
Tabelle 6 Zusammenfassung Antworten zur Analyse "Do you Need a Blockchain?"	61
Tabelle 7 Anforderungen an ein Trackingsystem.....	62

Abkürzungsverzeichnis

DAG	Directed Acyclic Graph
DPKI	Decentralized Public Key Infrastructure
DID	Decentralized Identifier
DL	Distributed Ledger
DLT	Distributed Ledger Technologie
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GNSS	Global Navigation Satellite Systems
IAM	Identity and Access Management
IdM	Identitätsmanagement
IDoT	Identity of Things
IdP	Identity Provider
IoT	Internet of Things
M2M	Machine-to-Machine
RP	Relying Party
SSI	Self-Sovereign Identity
TTP	Trusted Third Party
UUID	Universally Unique Identifier
VC	Verifiable Claim
W3C	World Wide Web Consortium

1 Einleitung

Die folgende Arbeit baut auf der unten beschriebenen Ausgangssituation auf. Zum besseren Verständnis des Hauptteils wird die Problemstellung, Zielsetzung und Struktur der Arbeit in diesem Kapitel beschrieben.

1.1 Ausgangssituation

Bei einer Zahl von über 20 Mia. vernetzten Geräten im Jahr 2020 ergeben sich hohe Anforderungen an das Identitätsmanagement im Internet of Things (IDoT – Identity of Things) (Gartner, 2017).

Basierend auf Blockchain oder anderen Distributed Ledger Technologien werden neue Identitätsmanagementsysteme wie Self-Sovereign Identity (SSI) entwickelt, die Datensicherheit, Datenschutz und Manipulationsmöglichkeiten berücksichtigen sollen.

In der Supply Chain spielt die Identifizierung von Identitäten und das Tracking der dazugehörigen Daten eine wichtige Rolle. In dieser Arbeit wird ein explorativer Prototyp entwickelt, der IDoT auf Basis der Distributed Ledger Technologie IOTA in einem Anwendungsfall der Supply Chain veranschaulichen soll.

1.2 Problemstellung

Im Rahmen einer Bachelorthesis wird für das Departement Informatik an der Hochschule Luzern ein Proof of Concept eines IOTA-basierten Trackingsystems in der Supply Chain erarbeitet. Dabei werden sowohl technische wie auch unternehmerische Aspekte berücksichtigt. Die Entwicklung eines Geschäftsmodells ist jedoch nicht Teil dieser Arbeit.

1.3 Zielsetzung

Ziel dieser Arbeit ist die Entwicklung eines Proof of Concepts für ein Trackingsystems in der Logistik. Dadurch soll ein konkreter Anwendungsfall von Identity of Things mit IOTA im Supply Chain Management erarbeitet werden. Anhand einer Literaturrecherche und Umfragen sollen zudem aktuelle Entwicklungen im Supply Chain Management zum Thema Distributed Ledger Technologien aufgezeigt werden.

1.4 Struktur der Arbeit

Die vorliegende Thesis startet mit den theoretischen Grundlagen zu den Themen Identity of Things und IOTA. Der Schwerpunkt liegt dabei auf der Erarbeitung von Konzepten und der Erklärung von Begriffen, die für das Verständnis der weiteren Arbeit relevant sind. Ebenfalls Teil der Theorie ist ein kurzer Überblick zu den aktuellen Herausforderungen im Supply Chain Management und einer Fallstudie von Blockchain-basierten Geschäftsmodellen in der Supply Chain.

In der Methodik wird der für diese Arbeit verwendete Forschungsansatz vorgestellt.

Der Hauptteil dieser Arbeit bildet die Beschreibung einer DLT-basierten Geschäftsidee für die Supply Chain und der Prüfung dieser Idee mittels einer Online-Umfrage, der Durchführung von Experimenten und der Entwicklung eines explorativen Prototyps.

In den Ergebnissen werden die im Entwicklungsprozess identifizierten Erkenntnisse analysiert und dafür genutzt, die Idee schrittweise zu revidieren.

Am Ende werden die Vorgehensweise und die Ergebnisse reflektiert. Der Abschluss bilden Empfehlungen an Personen und/oder Organisationen, die sich für die Umsetzung einer DLT-basierten Lösung mit IDoT in der Supply Chain interessieren. Im letzten Kapitel werden zudem Vorschläge gemacht, wie diese Arbeit fortgeführt werden könnte.

2 Methodik

Im folgenden Kapitel werden die in dieser Forschungsarbeit verwendeten Methoden näher beschrieben. Dazu gehören eine Literaturrecherche, die Erstellung von Kundenprofilen, eine Online-Umfrage und die Entwicklung eines explorativen Prototyps mit der Durchführung von Experimenten. In der Abbildung 1 ist das Vorgehen dieser Arbeit illustriert.

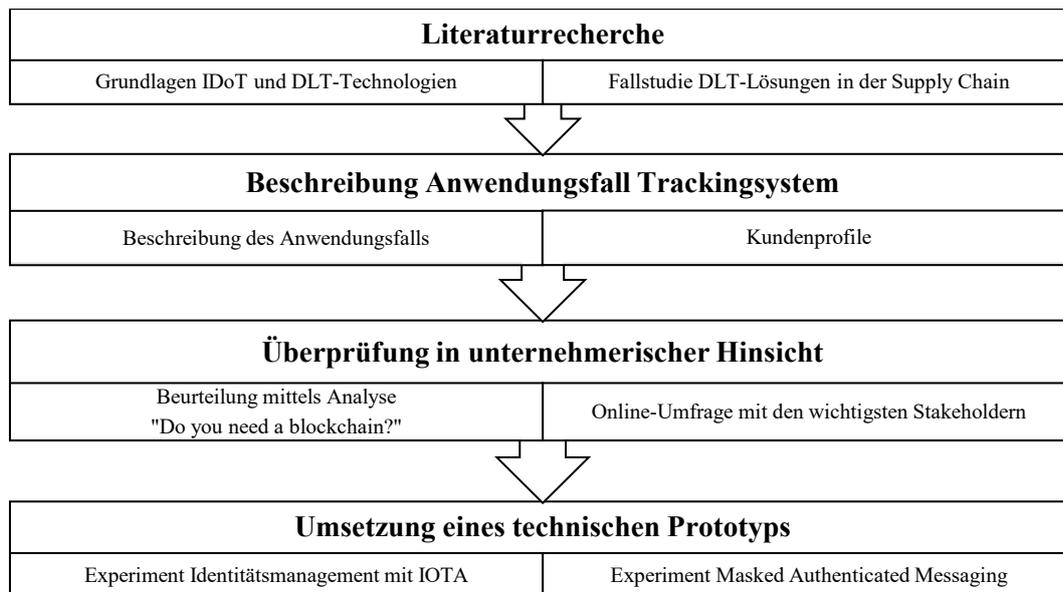


Abbildung 1 Ablauf der Forschungsarbeit

Quelle: Eigene Darstellung

Ziel dieser Vorgehensweise ist es, ein vor Definition des Projekts entwickelter Anwendungsfall in wirtschaftlicher Sicht zu überprüfen, gegebenenfalls Änderungen vorzunehmen und schlussendlich eine technische Lösung dafür vorzuschlagen.

Die unternehmerische Komponente wird durch die Online-Umfrage mit den wichtigsten Stakeholder stichprobenhaft überprüft. Eine weitere Analyse erfolgt durch den Leitfaden «Do you Need a Blockchain?» von (Wüst & Gervais, 2018).

Die Umsetzung eines Prototyps testet die technische Machbarkeit der Lösungsidee und zeigt Schwierigkeiten auf, die bei der Entwicklung einer Lösung auftreten können.

2.1 Literaturrecherche

Die Literaturrecherche dient einem grundlegenden Verständnis der beiden Hauptthemen dieser Arbeit: Identity of Things und IOTA. Der zweite Teil der Recherche widmet sich den aktuellen Herausforderungen im Supply Chain Management und existierenden DLT-Geschäftsmodellen in diesem Bereich.

Das Verständnis der Grundlagen spielt insbesondere im technischen Teil der Arbeit eine Rolle. Die Erkenntnisse zur Recherche «Herausforderungen in der Supply Chain» sollen zudem für die Revidierung des Anwendungsfalls im weiteren Verlauf der Arbeit nützlich sein.

2.2 Kundenprofile

In der Beschreibung des Anwendungsfalls werden die Bedürfnisse der einzelnen Stakeholder beschrieben. Dafür wird für jeden Stakeholder ein Kundenprofil erstellt, das die Pains und Gains sowie die Aufgaben eines Nutzers im Hinblick auf ein bestimmtes Thema aufzeigt.

Das Kundenprofil ist Teil der Design Thinking Methode *Value Proposition Canvas*. Ein Value Proposition Canvas hilft, Service und Produkte direkt mit den Bedürfnissen einer Stakeholdergruppe abzustimmen.

Aufgrund des wesentlich höheren Aufwands wird auf eine klassische Stakeholder-Analyse verzichtet. Würde später auf Basis dieser Arbeit ein Geschäftsmodell entwickelt, wird die detailliertere Betrachtung der Stakeholder jedoch empfohlen.

2.3 Online-Umfrage zur Bedürfniserfassung

Die wichtigsten Stakeholder des Anwendungsfalls werden in einer qualitativen Online-Umfrage befragt. Dabei soll herausgefunden werden, ob und inwiefern ein Bedürfnis nach einem (Fahr-)daten-Tracking in der Supply Chain und spezifisch in der Logistik besteht. Die Umfrage wird mit *survio.com* durchgeführt und beinhaltet ca. 10-15 offene, Single Choice und Multiple Choice Fragen. Die Fragen im Originalformat sind im Anhang nachlesbar. Die Umfrage wird anonym durchgeführt.

Der Vorteil einer Online-Umfrage gegenüber persönlichen Interviews ist der kleinere Zeitaufwand: Durch eine Online-Umfrage können mehr Personen befragt werden und der Standort der befragten Personen ist irrelevant.

2.4 Exploratives Vorgehensmodell

Für die Umsetzungsphase wird ein exploratives Vorgehensmodell verfolgt. Laut Wieczorrek und Mertens stehen im Fokus des explorativen Prototypings «die Prozesse und die Ausprägung der Funktionalitäten des späteren Systems» (2011, S. 95).

Ein explorativer Prototyp bildet eine Kommunikationsgrundlage für verschiedene Parteien und ist eine Basis für weitere genauer spezifizierte Prototypen (Wieczorrek & Mertens, 2011, S. 95). Durch die explorative Vorgehensweise soll die Lösung eines IOTA-basierten Trackingsystems in der Supply Chain auf seine Tauglichkeit getestet werden. Das explorative Vorgehensmodell eignet sich für frühe Ideenstadien wie in dieser Arbeit. Andere Vorgehensmodelle sind dafür weniger geeignet, da sie bereits einen gewissen Detailgrad der Systemspezifikation verlangen.

3 Grundlagen

Nachfolgend werden die wichtigsten Grundlagen zu Identitätsmanagement und Distributed Ledger Technologien (DLT) mit Schwerpunkt IOTA vermittelt.

Das Kapitel «DLT-basierte Geschäftsmodelle in der Supply Chain» beschreibt Herausforderungen im Supply Chain Management und nennt anschliessend verschiedene Geschäftsmodelle, die DLT als Enabler-Technologie für Supply Chain-Lösungen verwenden.

3.1 Grundlagen Identity of Things

Identitätsmanagement umfasst «das Erschaffen, das Management und die Verwendung von digitalen Identitäten» (Alpár, Hoepman & Siljee, 2011, S. 1). Identitätsmanagement ist kein neuer Begriff; neu sind jedoch die Anforderungen, die heutige Identitäts- und Zugriffsmanagementsysteme (IAM) besonders im Bereich Internet of Things (IoT) zu erfüllen haben. Gründe dafür sind z. B. die immer stärkere Vernetzung der Industrie (Alpár et al., 2011, S. 1), die Diversität der vernetzten Dinge (Chen, Liu & Chai, 2015) und der Datenaustausch über Unternehmensgrenzen hinweg (Alpár et al., 2011, S. 1).

Das rasante Wachstum von IoT hat zu einer neuen Kategorie von Identitätsmanagement geführt: dem *Identity of Things (IDoT)*. IDoT befasst sich damit, wie Geräte und deren Daten im Internet of Things identifiziert und gesichert werden können. Ein weiterer Aspekt von IDoT ist das Zugriffsmanagement auf die Geräte und deren Daten. (Rowe, Myracle & Simmons, 2018).

3.1.1 Wichtige Begriffe im Identitätsmanagement

Das *NGN Identity Management Framework* der International Telecommunication Union (ITU) beschreibt eine Identität als Information, «die ausreicht, um ein Subjekt in einen bestimmten Kontext zu identifizieren» (Bertino & Takahashi, 2011, S. 21; ITU-T Study Group 13). Eine Identität setzt sich laut der Empfehlung «ITU-T Y.2720» aus drei Datentypen zusammen:

Identifizier: Für die Identifizierung wird einem Subjekt eine eindeutige Abfolge von Zahlen oder Buchstaben zugewiesen (Bertino & Takahashi, 2011, S. 21). Ein Beispiel dafür ist ein Universally Unique Identifier (UUID), ein Public Key oder ein Decentralized Identifier (DID) (siehe S.16). Identifizierer müssen eindeutig d.h. kollisionsfrei sein (Mühle, Grüner, Gayvoronskaya & Meinel, 2018, S. 82).

Credential: Ein Credential ist ein Dokument mit Daten, das eine oder mehrere Behauptungen (Claims) untermauert (Bertino & Takahashi, 2011, S. 21). Ebenfalls Teil des Credentials sind Metadaten wie z. B. der Aussteller des Credentials und die Gültigkeitsperiode. Die Begriffe Claim und Credential werden oft synonym verwendet. Ein traditionelles Beispiel für einen Credential ist ein Digitales Zertifikat.

Unterschieden wird zwischen einem gewöhnlichen und einem *Verifiable Claim (VC)*: Ein Verifiable Claim ist durch eine Signatur des Ausstellers eindeutig verifizierbar (Mühle et al., 2018, S. 84).

Attribut: Attribute beschreiben die Charakteristik eines bestimmten Subjekts. Ein Beispiel dafür ist das Geburtsdatum einer Person.

Bevor verschiedene Identitätsmanagementsysteme vorgestellt werden, soll hier eine konzeptuelle Übersicht von Identitätsmanagement gegeben werden. Die Akteure in einem Identitätsmanagement-System entsprechen meist einem der folgenden drei Grundtypen. Die geläufigen Fachbegriffe sind in Englisch (Bertino & Takahashi, 2011, S. 25-28):

Identity Holder / Subject:	Dabei handelt es sich um die Partei, für die eine digitale Identität erstellt werden soll.
Identity Provider (IdP) / Issuer:	Diese Partei stellt einem Subjekt eine Identität aus. Dabei identifiziert sie relevante Attribute des Subjekts und hält diese in einem Credential fest.
Relying Party (RP) / Verifier:	Die Relying Party oder der Verifier ist die Partei, die ein Subjekt eindeutig identifizieren können muss. Dies kann z.B. für das Anbieten eines Dienstes (Service Provider), für die Nutzung von Ressourcen und/oder für die Unterscheidung von anderen Subjekten notwendig sein.

Der Lebenszyklus einer digitalen Identität kann grob in die vier Phasen Erstellung, Nutzung, Aktualisierung/Update und Auflösung/Ungültigerklärung eingeteilt werden (Bertino & Takahashi, 2011, S. 30). Die Auflösung der Identität sollte auf keinen Fall vernachlässigt werden, da sonst die Gefahr eines Identitätsmissbrauch steigt.

3.1.2 Traditionelle Identitätsmanagementsysteme

Im folgenden Kapitel werden für einen besseren Vergleich zwei übliche Arten von Identitätsmanagementsystemen vorgestellt. Anschliessend werden daraus weiterentwickelte Konzepte wie *Self-Sovereign Identity* und *Dezentrales Identitätsmanagement* in Verbindung mit DLT genauer betrachtet.

Identitätsmanagementsysteme lassen sich unter anderem in die zwei folgenden Gruppen kategorisieren: *Claim-based* und *Network-based*.

Bei einem Network-based Identitätsmanagementsystem wie z.B. OpenID¹ oder Shibboleth² wird das Subjekt von der Relying Party (RP) an einen Identity Provider (IdP) verwiesen, der das Subjekt

¹ <http://openid.net/developers/specs/>

² <http://shibboleth.internet2.edu/>

authentifiziert und ihm bei erfolgreicher Authentifizierung ein Token für die Authentifizierung gegenüber der RP ausstellt. (Schmidt, Russello, Krontiris & Lian, 2012, S. 38).

In einem Claim-based Identitätsmanagementsystem wie z.B. Idemix³ oder U-Prove⁴ wird das Subjekt von der RP darüber informiert, welche Voraussetzungen es für eine erfolgreiche Authentifizierung erfüllen muss. Basierend darauf schickt das Subjekt der RP dann ein Claim, der von einem oder mehreren IdPs bestätigt wurde. (Schmidt et al., 2012, S. 38).

Wie in Abbildung 2 ersichtlich, ist der grösste Unterschied zwischen Network-based und Claim-based Identitätsmanagement, dass bei Claim-based IdM keine Weitergabe von subjektbezogenen Informationen zwischen IdP und RP stattfindet. Claim-based Identitätsmanagementsysteme weisen deshalb einen höheren Datenschutz für das Subjekt auf (Alpár et al., 2011, S. 2). «U» steht in der Abbildung für User und ist gleichbedeutend zu Subjekt oder Identity Holder.

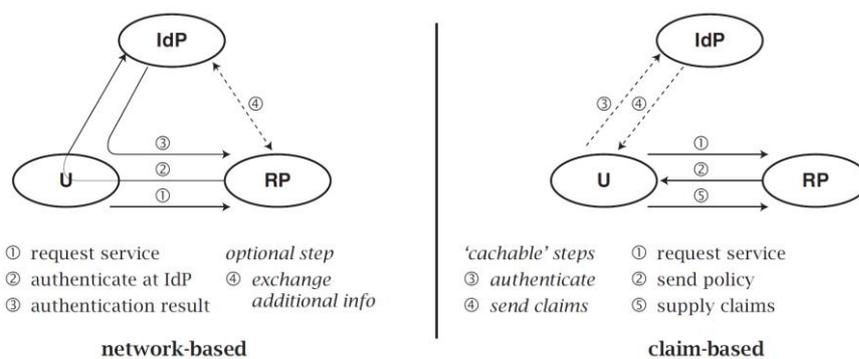


Abbildung 2 Network-based und Claim-based Identitätsmanagement

Quelle: Alpár et al., 2011, S. 3

3.1.3 Self-Sovereign Identity und Dezentrales Identitätsmanagement

Eine besondere Form von Claim-based Identitätsmanagement ist Self-Sovereign Identity (SSI). Dabei verwalten Subjekte ihre Digitale Identität völlig selbständig (Mühle et al., 2018, S. 81). Das World Wide Web Consortium (W3C) nennt als entscheidenden Unterschied zum klassischen Claim-based Identitätsmanagement, dass Identitäten bei SSI unabhängig von Diensten bzw. Service Providern also der Relying Party existieren (Mühle et al., 2018, S. 81). Diese User-zentrierte (user-centric) Art von Identitätsmanagement gibt dem Subjekt eine höhere Kontrolle über seine eigene Identität (Pohlmann, 2019, S. 164). Im folgenden Kapitel wird genauer auf SSI eingegangen und eine Umsetzung mit einem Distributed Ledgers diskutiert.

³ <https://hyperledger-fabric.readthedocs.io/en/release-1.3/idemix.html#what-is-idemix>

⁴ <https://www.microsoft.com/en-us/research/project/u-prove/>

In einem DLT-basierten Identitätsmanagementsystem steht anstelle der Registrierungsbehörde (traditionell der Identity Provider) ein Distributed Ledger. Auf dem Distributed Ledger wird der Identifier des Nutzers und unter Umständen der dazugehörige Verifiable Claim aufbewahrt (Mühle et al., 2018). Eine Darstellung einer Blockchain-basierten SSI Architektur ist in Abbildung 3 ersichtlich.

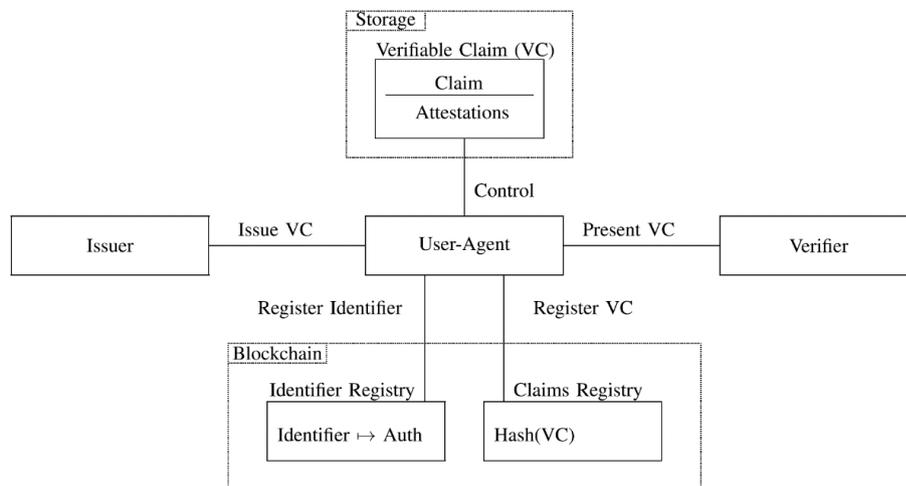


Abbildung 3 Self-Sovereign Identity Architektur

Quelle: Mühle et al., 2018, S. 82

Mühle et al. (2018) unterscheiden zwischen zwei möglichen SSI-Architekturen: *Identifier-Registry* und *Claim-Registry Model*. Die Modelle unterscheiden sich im Speicherort des *Identity Claims*:

In einem Identifier-Registry Model wird der Identity Claim *off-chain* vom Subjekt resp. User aufbewahrt. Die Relying Party, in diesem Kontext Claim-Verifier genannt, kann für die Verifizierung den Identifier auf dem Distributed Ledger und den angegebenen Identifier im Identity Claim vergleichen. (Mühle et al., 2018). Im Unterschied dazu, wird in einem Claim-Registry Model nicht nur der Identifier auf dem Distributed Ledger aufbewahrt, sondern auch der Hash des dazugehörigen Identity Claims (siehe Abbildung 3).

Die Verbindung zwischen Subjekt und Identifier kann durch Asymmetrische Kryptographie erreicht werden (Mühle et al., 2018, S. 82). Konkret kann jeder, der den mit dem Identifier verbundenen Public Key auf dem Distributed Ledger einsehen kann, verifizieren, ob es sich beim Schlüssel für die Signatur des Credentials um den passenden Private Key handelt. Decentralized Public Key Infrastructure (DPKI), die Verbindung von IAM mittels asymmetrischer Kryptographie und Distributed Ledger Technologie kann hier aus Platzgründen nicht detailliert behandelt werden. Bei Interesse empfiehlt sich der Artikel «Decentralized Public Key Infrastructure» von Allen et al. (2015).

Ein Punkt, in dem DLT-basierte IdM-Systeme sich häufig von klassischen IdM-Systemen unterscheiden, ist die Art der Identifier: Decentralized Identifiers (DIDs) sind «eine neue Art von Identifier, die eine verifizierbare, dezentrale digitale Identität unabhängig von einem zentralisierten Registry, einem Identity Provider oder einer Zertifizierungsbehörde ermöglichen sollen» (Reed et al.,

2019). Ein DID ist eine URL, die ein Subjekt direkt mit einem Identity Credential, dem DID-Dokument, verbindet. Teil des DID-Dokuments ist unter anderem die Angabe von Methoden, wie ein Claim verifiziert, und wie mit dem dazugehörigen Subjekt auf vertrauenswürdige Weise (trusted) interagiert werden kann. (Reed et al., 2019).

Für jeden Distributed Ledger wird ein DID-Schema mit einem separaten Namespace verwendet. Für IOTA existiert ein erstes DID-Schema, TangleID⁵ (Bsp. did:tangle:123456789abcdefghi), welches jedoch nicht von der IOTA Foundation selbst entwickelt wurde. Eine Liste aller zurzeit registrierten DID-Methoden ist von der W3C Community Group auf GitHub veröffentlicht (<https://w3c-ccg.github.io/did-method-registry/>)

3.1.4 Anforderungen für Identity of Things

In diesem Kapitel werden drei Aspekte genannt, die bei einem Identitätsmanagementsystem für das Internet of Things berücksichtigt werden müssen:

Identifizier

Das IoT wird aus einer Vielzahl von Geräten mit unterschiedlichen Eigenschaften gebildet. IoT-Identifizier wie IPv6-Adressen, RFID-Chips, QR-Codes, bis hin zu Autonummernschildern, müssen unter einem gemeinsamen Identitätsmanagementsystem zusammengefasst werden können. Dafür ist ein Mapping zwischen den klassischen Identifiern und einem übergreifenden Identity Name Service (z. B. den weiter oben beschriebenen DIDs) notwendig (Friese, Heuer & Kong, 2014). Unter Umständen sind mehrere Identifizier für verschiedene Kontexte nötig (*Context-based Identity*).

Datenschutz

Datenschutz (auch bekannt unter *Privacy*) spielt nicht nur bei IdM für Personen eine Rolle. Auch bei IDoT entstehen schützenswerte personenbezogene Daten. Deshalb müssen auch in diesem Kontext GDPR-Prinzipien⁶ wie Recht auf Zugriff, Recht auf Löschung, Daten-Portabilität und Vertraulichkeit berücksichtigt werden. Self-Sovereign Identity bietet dafür eine mögliche Lösung. Eine direkte Gegenüberstellung von GDPR- und SSI-Prinzipien findet sich im Artikel «Privacy Implication and Technical Requirements Toward GDPR Compliance» (Arai, Bhatia & Kapoor, 2020, S. 362).

Informationssicherheit

Die sichere Aufbewahrung von Credentials und kryptographischem Material müssen auf einem einfachen IoT-Gerät sichergestellt werden können. *End-to-End-Security* bedeutet, dass von der Feldebene bis zur Nutzerapplikation, Datensicherheit und Schutz vor Manipulation sichergestellt wird.

⁵ <https://github.com/TangleID/TangleID>

⁶ General Data Protection Regulation/Datenschutz-Grundverordnung (<https://dsgvo-gesetz.de/>)

Dafür braucht es spezielle Vorkehrungen im Bereich der Hardware, aber auch auf Ebene der Kommunikation resp. des Datenaustauschs von Geräten.

Nebst diesen Anforderungen spielen auch Authentifizierung und Zugriffskontrolle eine wichtige Rolle. Die besondere Herausforderung dabei ist, dass diese beiden Funktionen über Applikations- und Unternehmensgrenzen hinweg, und zeitlich über den ganzen Lebenszyklus der Identität, gemanagt werden müssen.

3.1.5 Erkenntnisse Identity of Things

Während in klassischen IdM-Systemen der Identity Provider die zentrale Rolle im Identitätsmanagement innehat, rückt beim dezentralen IdM das Subjekt resp. der Nutzer (User-centric IdM) ins Zentrum.

Die Anforderungen im Identity of Things können mit Self-Sovereign Identity und dezentralem Identitätsmanagement erreicht werden. DLT-basierte IdM-Systeme bieten mit DIDs zudem einen standardisierten Identity Name Service an, der die Interaktion (z.B. Art der Authentifizierung) mit dem IoT-Gerät definiert. Für die Verwaltung von Identifiern und Credentials über den ganzen Lebenszyklus und über Unternehmensgrenzen hinweg ist ein Distributed Ledger ideal.

3.2 Übersicht zu IOTA

Die folgenden Kapitel geben eine Einführung in Distributed Ledger Technologien und IOTA.

3.2.1 Einführung in Distributed Ledger Technologien

Im Jahr 2008 wurde die Idee einer Kryptowährung von Satoshi Nakamoto, einem Pseudonym für eine unbekannt Persönlichkeit, erstmals eingeführt. Bitcoin wurde damals als elektronisches Peer-to-Peer Zahlungssystem vorgestellt (Rayes & Salam, 2019, S. 269). Schnell wurde erkannt, dass die Technologie hinter Bitcoin; Blockchain, sich nicht nur für Zahlungssysteme, sondern für verschiedenste Anwendungen in einer Vielzahl von Anwendungsgebieten eignet.

Blockchain kann als Kassenbuch verstanden werden, dessen Kopie in einem Netzwerk unter allen Teilnehmern verteilt wird. Spezifischer handelt es sich bei Blockchain, um ein verteiltes Hinzufügedatenbanksystem, dass aus einer Kette von Blocks mit Transaktionen besteht. Die Blocks enthalten jeweils einen Zeitstempel und sind kryptographisch so miteinander verlinkt, dass sie sich nur schwer manipulieren lassen⁷ (Rayes & Salam, 2019, S. 272).

⁷ Eine Manipulation ist nur möglich, wenn eine Person mehr als 51 % der Rechenleistung im Netzwerk besitzt (Sybil Attacke)

Eine Transaktion ist ein Bündel von Informationen, welches mit dem privaten Schlüssel einer Person signiert ist. Dabei kann es sich um eine Transaktion mit monetärem Wert handeln z.B. Alice sendet Bob fünf Bitcoins⁸ oder um eine *Zero-Value-Transaktion*, einer Transaktion ohne monetären Wert, z.B. eine Transaktion mit der Information: «Der Temperatursensor XYZ misst 25 Grad Celsius».

In der folgenden Arbeit werden verteilte Kassenbücher, wie Blockchain eines ist, unter dem Begriff Distributed Ledger zusammengefasst. Ein Distributed Ledger hat gegenüber einer herkömmlichen Datenbank folgende Vorteile (Rayes & Salam, 2019, S. 272):

- Unveränderbarkeit
- Zeitliche Historie von Transaktionen
- Dezentrale Architektur und Konsensus
- keine Abhängigkeit zu einer *Trusted Third Party*,
Vertrauen durch die Technologie

3.2.2 Einführung in IOTA

Nebst Blockchain gibt es noch andere Arten von Distributed Ledgern, die jedoch einen wesentlich kleineren Bekanntheitsgrad haben als Blockchain. Ein Beispiel ist der *Directed Acyclic Graph* (gerichteter zyklensfreier Graph). In der Abbildung 4 ist diese mathematische Struktur visualisiert.

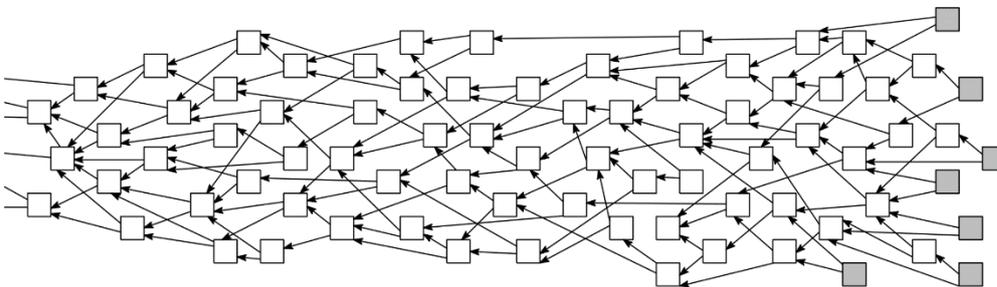


Abbildung 4 Directed Acyclic Graph (DAG)

Quelle: Popov, 2019, S. 10

IOTA ist die bekannteste Kryptowährung, die auf einem Directed Acyclic Graph (DAG) basiert. Die Währung wurde 2015 mit dem Ziel eingeführt, Machine-to-Machine (M2M) Micropayments im IoT zu ermöglichen (Popov, 2019, S. 1). Im Folgenden soll anhand eines Vergleichs zu Bitcoin eine Einführung in IOTA gegeben werden. Ein direkter Vergleich innerhalb einer Tabelle kann im Anhang nachgeschaut werden.

⁸ Fünf Bitcoins entsprachen zu diesem Zeitpunkt einem Wert von ca. 44'000 CHF.

Eines der fundamentalen Unterschiede zwischen IOTA und vielen anderen Kryptowährungen ist, dass bei IOTA für eine Transaktion keine Transaktionsgebühr anfällt. Es gibt bei IOTA auch kein klassisches Mining⁹ wie bei Bitcoin: Jeder Teilnehmer, der möchte, dass seine Transaktion in den Tangle (umgangssprachlich für IOTAs DAG) aufgenommen wird, muss einen Proof of Work erbringen. Dies tut er, indem er zwei andere nicht-verifizierte Transaktionen (Tips)¹⁰, genannt Trunk und Branch, verifiziert und ein kryptographisches Puzzle löst. So können Spamming und Sybil Attacken verhindert werden. (Popov, 2019).

Da es kein Mining gibt, werden auch keine neuen Tokens generiert. Sämtliche Tokens wurden bereits bei der Erstellung des IOTA Tangles kreiert (Popov, 2019, S. 2). Die Anzahl existierender Tokens liegt bei $(3^{33}-1) / 2$, was der Zahl 2'779'530'283'277'761 entspricht (IOTA Foundation, 2019a, Units of IOTA tokens). Für bessere Lesbarkeit wird IOTA oft in SI-Einheiten angegeben.

Die Tatsache, dass jede Transaktion zwei andere Transaktionen verifizieren muss, um selber in den Tangle aufgenommen zu werden, führt zu einer hohen Skalierbarkeit des Systems: Je mehr Teilnehmer Transaktionen machen möchten, desto mehr potenzielle Verifizierende gibt es.

Das Mainnet von IOTA ist wie Bitcoin *public* und *permissionless*. Einen eigenen privaten Tangle zu erstellen, ist ebenfalls möglich.

Da der IOTA-Tangle selber noch zu klein ist, um sich vor Sybil-Attacken in genügendem Masse zu schützen, wurde die zusätzliche Absicherung «Coordicide» eingeführt. Dabei handelt es sich um mehrere Nodes, die von der IOTA Foundation unterhalten werden, und in regelmässigen Abständen wertlose Transaktionen, sogenannte Meilensteine, an *IRI-Nodes (Full Nodes)*¹¹ senden. Ist eine Transaktion im Tangle nicht von dieser Meilenstein-Transaktion referenziert, gilt sie als ungültig und wird entfernt (*IOTA Einsteiger Guide*, 2019). Der Coordicide wird als zentralistisches Organ im dezentralen System kritisiert. Er soll deshalb in Zukunft durch andere Sicherheitsmechanismen ersetzt werden (IOTA Foundation, 2019b).

Wie bei Bitcoin gibt es auch bei IOTA das Konzept von Adressen; Konten von denen aus Transaktionen gesendet und empfangen werden können (*IOTA Einsteiger Guide*, 2019). Allerdings

⁹ Bei Bitcoin ist Mining das Erstellen eines neuen Blocks mittels Proof of Work. Teilnehmer des Netzwerks, die ihre Rechenleistung dafür zur Verfügung stellen, heissen Miners. Rayes und Salam (2019, S. 272).

¹⁰ Bei einem Tip handelt es sich um eine Transaktion, die noch nicht in den Tangle aufgenommen wurde. Die zu verifizierenden Transaktionen werden mittels Tip Selection ausgewählt. Tip Selection basiert auf dem Monte Carlo Random Walk Algorithmus. Popov (2019, S. 3).

¹¹ «Ein IRI-Node ist ein Server, der das IOTA-Netzwerk unterstützt und am Leben hält, ohne IRI-Node gibt es kein IOTA-Netzwerk. Auf jedem dieser Nodes ist die Hauptsoftware, die sogenannte "IOTA Reference Implementation (IRI)" installiert, sowie die Transaktions-Datenbank (der Tangle)» IOTA Einsteiger Guide (2019, Nodes).

verwendet IOTA das Signatur Schema *Winternitz One-Time Signature*, bei dem aus Sicherheitsgründen eine Adresse nur einmal zum Signieren verwendet werden kann. Deshalb verfügt jeder Teilnehmer über einen Seed, ein eindeutiges geheimes Kennwort mit 81 Stellen, mit dem bis zu 9^{57} verschiedene Adressen generiert werden können. Der Grund für die Verwendung dieses Signatur Schemas ist, dass es quantensicher sein soll. (IOTA Foundation, 2019a, Adresses and Signatures).

Eine weitere Spezialität IOTAs ist, dass Daten in einem balancierten ternären System dargestellt werden d. h. dass die kleinste Informationseinheit (sonst Bit genannt) die Werte -1, 0 und 1 annehmen kann. Seeds, Adressen und andere Daten werden in Trytes (drei Trits) zusammengefasst. Für die 27 möglichen Kombinationen eines Trytes verwendet IOTA das «Tryte Alphabet»: Es ordnet jeder möglichen Kombination einen Buchstaben des Alphabets oder die Zahl 9 zu.

IOTA verfügt über eine Vielzahl von weiteren Konzepten und Entwicklungsprojekten, die hier aus Platzgründen nicht erklärt werden können. Nennenswert ist z.B. das Protokoll «Qubic», welches Smart Contracts¹² und Oracles¹³ ermöglichen soll (*IOTA Einsteiger Guide*, 2019).

Die spezifischen Vorteile von IOTA sind nebst den üblichen eines Distributed Ledgers (IOTA Foundation, 2019a, What is IOTA?):

- Informationssicherheit
- Keine Transaktionsgebühren
- Skalierbarkeit

Auf ein Protokoll von IOTA soll im folgenden Kapitel noch genauer eingegangen werden, da es für die technische Umsetzung eine wichtige Rolle spielt.

3.2.3 Masked Authenticated Messaging (MAM)

«Masked Authenticated (MAM) ist ein Datenkommunikationsprotokoll auf dem IOTA-Tangle, welches das Veröffentlichen und Abrufen von Nachrichten (*Messages*) in verschlüsselten Streams, sogenannten Channels, ermöglicht» (IOTA Foundation, 2019a, MAM).

Gewöhnliche Zero-Value-Transaktionen werden auf dem IOTA-Tangle weder signiert noch von Nodes auf ihre Authentizität verifiziert. Durch MAM erhalten die im MAM-Channel veröffentlichten Zero-Value-Transaktionen die Signatur des Channel-Besitzers. Teilnehmer, welche die MAM-

¹² «Ein Smart Contract ist ein Vertrag auf Software-Basis, bei dem unterschiedlichste Vertragsbedingungen hinterlegt werden können» Mitschele (2019). Der Vertrag kann beim Eintreten bestimmter Konditionen automatisch ausgeführt werden.

¹³ Datenquelle oder Anbieter außerhalb des Tangles. IOTA Einsteiger Guide (2019).

Transaktionen abrufen, können die Signatur überprüfen und die Nachrichten entschlüsseln. (IOTA Foundation, 2019a, MAM).

Bei jeder Veröffentlichung einer Nachricht wird die Adresse der Transaktion als Channel-ID verwendet. Diese ist nötig, um den Channel zu abonnieren und Nachrichten vom Channel abzurufen.

MAM kennt drei verschiedene Modi. Um diese zu verstehen, ist es hilfreich zu wissen, dass MAM auf einem Merkle Tree Signatur Schema¹⁴ basiert. Der Root des Merkle Trees wird für das Signieren der verschlüsselten Nachricht verwendet (IOTA Foundation, 2019a, MAM channels):

Public: Die *Channel-ID* (Adresse der Transaktion) entspricht dem Root. Alle Nachrichten im Channel können somit mit der Channel-ID entschlüsselt werden.

Private: Als Channel-ID wird der Hash des Roots verwendet. Nur wer den ursprünglichen Root kennt, kann die Nachrichten entschlüsseln.

Restricted: Dabei handelt es sich um eine Erweiterung des Privaten Modus. Die Channel-ID ist der Hash des Roots und eines *Side Keys*, eines geheimen Schlüssels. Nur wer den Root und den Side Key kennt, kann Nachrichten entschlüsseln. Der Side Key kann geändert werden, so dass Teilnehmer den Zugang zu den Nachrichten wieder verlieren.

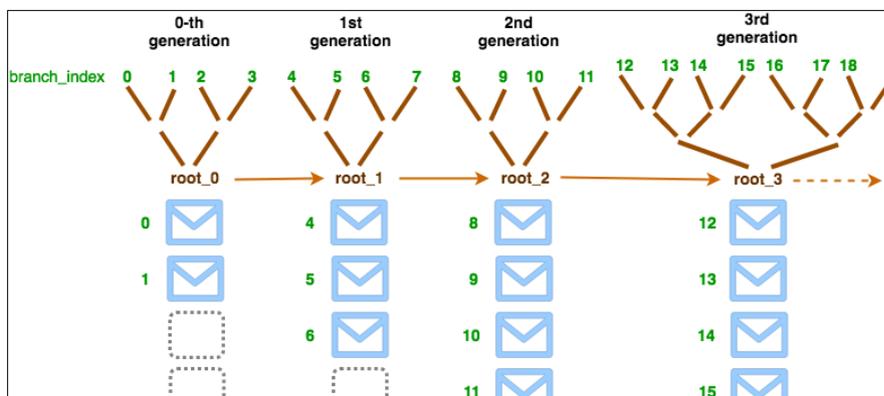


Abbildung 5 MAM Channels und Channel Splitting

Quelle: Medium, 2018, MAM Eloquently Explained

Für jeden Channel gibt es einen Merkle Tree (Abbildung 5). Ist die maximale Anzahl von Nachrichten pro Merkle Tree erreicht, wird ein neuer Channel mit einem nächsten Merkle Tree erstellt. Der Channel kann bereits gewechselt werden, bevor der alte Channel voll ist. Dies wird Channel Splitting

¹⁴ Merkle Trees ermöglichen eine effiziente Überprüfung von Daten. Die Blätter eines Merkle Trees sind gehashte Datenpakete. Die Hashes werden dann in einer baumartigen Struktur zusammengehasht bis nur noch ein Hash, der Root, übrigbleibt.

genannt. Die Grösse des Channels ist abhängig von der Grösse des Merkle Trees und kann mit dem Attribut *size* definiert werden. (Medium, 2018, MAM Eloquently Explained).

Jede Message enthält das Feld *nextRoot*. Dabei handelt es sich um den Root des nächsten Merkle Trees. Mit dieser Information ist es möglich, den Channel vorwärts zu verfolgen. Das Rückwärtsverfolgen eines Channels ist nicht möglich. (Handy, 2017).

Mehr Details zu MAM und die Implementation eines MAM Channels werden in Kapitel 6.3 diskutiert.

3.3 DLT-basierte Geschäftsmodelle in der Supply Chain

Dieses Kapitel zeigt aktuelle Herausforderungen im Supply Chain Management auf und stellt dann Beispiele von DLT-basierten Lösungen in der Supply Chain vor.

3.3.1 Herausforderungen in der Supply Chain

Die Supply Chain ist ein System von Organisationen, Personen, Aktivitäten, Informationen und Ressourcen, die dazu beitragen, ein Produkt oder ein Service von der Produktionsquelle zum Endnutzer zu bringen. Die Supply Chain beinhaltet nicht nur den Fluss von Gütern, sondern auch von Geld, Information, Ideen und Innovation; und Risiko.

Nach einer Studie von der Beratungsgesellschaft Emporias mit 104 deutschen Industrieunternehmen klagen 47 % der befragten Unternehmen über eine grosse oder sehr grosse Störanfälligkeit in der Supply Chain. Der hauptsächliche Grund dafür seien Kommunikations- und Informationsprobleme im Schnittstellenbereich. Zudem beurteilen nur 40 % der befragten Manager die Abläufe in der Lieferkette als ideal. Auch die Kostentransparenz ist bei einer Mehrheit der befragten Unternehmen verbesserungsfähig. (Emporias Management Consulting GmbH & Co. KG., 2017).

Zu den genannten internen Problemen in der Lieferkette kommen erhöhte Anforderungen an Supply Chain Management (SCM) durch äussere Einflüsse. Beispiele dafür sind Globalisierung und Outsourcing, zunehmende Komplexität der Produkte (viele Teilkomponenten), Anforderungen von Endkunden bezüglich Umweltfreundlichkeit, Ethik und Produktqualität bei niedrigerem Preis, verschärfte Gesetze zu Transparenz und Nachverfolgbarkeit sowie kurz- und langfristige Marktveränderungen.

Im Fokus der Verbesserung stehen folglich insbesondere die Effizienz (hohe Qualität in kurzer Zeit), die Nachverfolgbarkeit und Transparenz sowie die Flexibilität der Supply Chain. Verbesserung in diesen Bereichen führen dann auch zu einer Senkung von Kosten und einer Minimierung von Risiken.

3.3.2 Fallstudie DLT-basierte Lösungen in der Supply Chain

Die folgende Liste von Beispielen zeigt, welche Probleme in der Supply Chain zurzeit mit Distributed Ledger Technologien gelöst werden. Ziel dieser Studie ist es, bestimmte Muster für Geschäftsmodelle mit DLT in der Supply Chain zu identifizieren und weitere potenzielle Anwendungsfelder daraus

abzuleiten. Die Beispiele stammen aus der Studie beschrieben in «Blockchain's Roles in Meeting Key Supply Chain Management Objectives» (Kshetri, 2018).

TradeLens – Effizienz durch Digitalisierung von Shipping-Dokumenten für Container

Maersk ist mit 18-20 % Marktanteil das grösste Container Shipping Unternehmen der Welt. Im September 2016 hat Maersk zusammen mit IBM ein Proof of Concept (PoC) für das Tracking von Containern und die Digitalisierung der damit verbundenen Shipping-Dokumenten erarbeitet. Groenfeldt (2017) beschreibt, dass eine einfache Fracht tiefgekühlter Ware von Ostafrika nach Europa mit bis zu 30 Leuten und Organisationen in Kontakt kommt. Dies führt laut IBM zu mehr als 200 Interaktionen zwischen SC-Teilnehmern. Durch digitale mit Blockchain abgesicherte Aufzeichnungen können diese Interaktionen drastisch reduziert und somit signifikant an Kosten gespart werden. Das Pilotprojekt wurde mit Schneider Electric durchgeführt. Die verwendete Blockchain ist private und permissioned basierend auf *Hyperledger Fabric* (Groenfeldt, 2017).

Die aus dem Projekt entstandene Plattform TradeLens wurde 2018 von IBM und Maersk gelauncht. Mittlerweile (Stand Juni 2019) verwenden bereits 15 Containerschiffe die Plattform und weitere Partner wie Global Container Terminals Inc. (GCT) nehmen am Projekt teil. (Pope, 2019).

Modum – Nachverfolgbarkeit durch Tracking von Medizinprodukten

Modum ist ein Schweizer Start-up, das 2016 in Zürich gegründet wurde. Modum will eine Sensorlösung kombiniert mit Blockchain anbieten, welche die Temperatur von pharmazeutischen Produkten während dem Transport überwacht. Die gesammelten Daten sollen mittels Smart Contracts auf Ethereum gegen regulatorische Referenzwerte verglichen werden. Bei starken Abweichungen wird Lieferant und Empfänger der Fracht kontaktiert. Modum startete 2016 ein Pilotprojekt. Das Start-up ist noch in der Entwicklungsphase. (Kshetri, 2018, S. 84).

Everledger – Nachverfolgbarkeit und Transparenz durch Tracking von Luxusgütern

Everledger ist ein Start-up aus London, welches 2015 von Leanne Kemp gegründet wurde. Everledger ermöglicht die Absicherung und Überprüfung von Produkten wie Diamanten, Mineralien, Wein und Kunst mittels Blockchain-Technologie. Dabei werden jedem Produkt eine eindeutige Identität zugewiesen und Produktdaten über die ganze Supply Chain gesammelt. Mit den gesammelten Daten kann schlussendlich ein Zertifikat für das Produkt ausgestellt werden. Beim Tracking von Weinflaschen werden RFID-Tags am Korken angebracht, die einen möglichen Manipulationsversuch registrieren. (Kshetri, 2018). So kann eine Manipulation des Systems bereits auf Feldebene verhindert werden. Everledger basiert auf *Hyperledger Fabric*. Durch das Produkt konnten bereits 800'000 Diamanten erfasst werden (Cavus, 2016). Die *TrustChain-Initiative* von IBM verfolgt eine ähnliche Anwendung (Wiggers, 2019).

Provenance – Nachverfolgbarkeit und Transparenz durch Tracking von Lebensmitteln

Provenance ist ein junges Unternehmen, welches Blockchain-basierte Lösungen für die Lebensmittel- und Handelsbranche anbietet. Ein erstes Pilotprojekt wurde 2016 in der Fischereiindustrie in Indonesien durchgeführt. Dabei wurde mit Technologien wie Smart Tagging Fisch getrackt und dessen Herkunft verifiziert. Mittlerweile nutzen über 200 Händler und Produktionsunternehmen für verschiedenste Produkte die Lösung von Provenance (Provenance). Weitere Projekte in der Lebensmittelbranche sind *FoodTrust*, eine Lösung von IBM angewendet z.B. bei Walmart, und das *Food Trust Framework* von Alibaba, PwC, AusPost und Blackmores. (Kshetri, 2018, S. 83).

3.3.3 Erkenntnisse DLT-basierte Geschäftsmodelle

Die Fallstudien zeigen, dass bereits einige DLT-Lösungen für die Verbesserung von Nachverfolgbarkeit und Transparenz in der Supply Chain existieren. Dies entspricht einer der intuitivsten Anwendungsarten eines Distributed Ledgers und ist deshalb gut nachvollziehbar. Produkte, die einen hohen Wert haben (Edelsteine, Wein, Kunst) oder Produkte, deren Transport heikel ist (Lebensmittel, Medikamente), sind für ein Tracking besonders geeignet.

Der Aspekt Nachhaltigkeit spielt ebenfalls eine Rolle und führt dazu, dass Blockchain auch für das Tracking von Kosmetikprodukten oder Kleidern verwendet wird (Beispiel Provenance). Der Nutzen dieser Art von Anwendungsfall ist eine zusätzliche Absicherung resp. einen Mehrwert für den Endkunden. Mit dem Verkauf von Zertifikaten oder erhöhter Zahlungsbereitschaft von Endkunden profitiert auch der Produzent direkt von der Anwendung.

Einen Schritt weiter gehen Projekte, die nicht nur die Nachverfolgbarkeit und Transparenz in der Supply Chain erhöhen, sondern die Supply Chain Prozesse direkt optimieren. Dafür eignet sich der Fall «TradeLens» als Anschauungsbeispiel: Durch die Digitalisierung von Shipping-Dokumenten mittels einer Blockchain-basierten Plattform kommt es zu weniger Interaktionen der Supply Chain-Beteiligten. Dies führt zu einer erheblichen Effizienzsteigerung in der Supply Chain, was die Prozesskosten massiv senkt. Die Anfangshürde für solche Anwendungen sind Investitionskosten für die Blockchain-Plattform, die erst aufgebaut werden muss.

Distributed Ledger-Lösungen für die direkte Erhöhung der Effizienz und Flexibilität der Supply Chain wurden in der Recherche nur mit *TradeLens* gefunden. Anfangs wurde mit der Studie von Emporias (2017) Kommunikation im Schnittstellenbereich als gravierendes Problem in der Supply Chain identifiziert. Wenn Distributed Ledger-Lösungen dieses Problem adressieren, indem sie eine verlässliche Plattform für standardisierte digitale Interaktion zwischen Prozessbeteiligten bieten, kann die Effizienz und Flexibilität der Supply Chain gesteigert werden. In diesem Bereich ist deshalb noch ein grosses Potenzial für Anwendungsfälle.

4 Anwendungsfall Fahrdaten-Trackingsystem

In diesem Teil wird ein DLT-basiertes Fahrdatentrackingsystem für eine bessere Nachverfolgbarkeit in der Logistik vorgestellt. Dieser Anwendungsfall wird dann in den zwei folgenden Kapitel «Prüfung in unternehmerischer Hinsicht» und «Technische Lösung» genauer betrachtet und auf seine Stichhaltigkeit und Umsetzbarkeit überprüft.

Die Idee ist es, einem Fahrzeug für Gütertransport eine eindeutige auf IOTA abgesicherte Identität zuzuweisen, und mithilfe eines Trackinggeräts dann die Lieferrouten des Fahrzeugs aufzuzeichnen und ebenfalls über IOTA zu sichern.

Ein Ablauf dieses Trackings könnte so aussehen:

1. Ein LKW wird auf einem Distributed Ledger registriert und erhält somit eine eindeutige Identität.
2. Während der Fahrt werden Positionsdaten live aufgezeichnet und an das Logistikunternehmen, welches das Fahrzeug besitzt, übertragen.
3. Bei Grenzkontrollen erhalten Beamte temporär limitierten Zugang zu den aufgezeichneten Daten und können so sicherstellen, dass der LKW die Strecke gefahren ist, die angegeben wurde.
4. Der temporär und auf spezifische LKWs begrenzte Zugang zu Fahrdaten gäbe den Kunden von Logistikunternehmen, z. B. Produktionsfirmen, mehr Sicherheit, dass Ihre Ware zuverlässig ausgeliefert wird.

Der Nutzen der Anwendung betrifft drei Stakeholder, für die im folgenden Teilkapitel Kundenprofile erstellt wurden.

4.1 Kundenprofile für beschriebenen Anwendungsfall

Die wichtigsten Kundenprofile für diesen Anwendungsfall sehen wie folgt aus:

Tabelle 1 Kundenprofil Transport- und Logistikunternehmen

Transport- und Logistikunternehmen	
<p><i>Job to be done:</i></p> <p>Live-Tracking von eindeutig unterscheidbaren LKWs</p>	<p><i>Pains:</i></p> <ul style="list-style-type: none"> - Hohe Komplexität bei der Einteilung der verfügbaren Ressourcen - Vertrauen in die Fahrer, das Fahrzeit effizient genutzt wird
<p><i>Use Cases:</i></p> <ul style="list-style-type: none"> - Optimierung der Transportwege - Optimierung der Lieferprozesse 	<p><i>Gains:</i></p> <p>Optimale Ressourceneinteilung und effiziente Lieferprozesse</p>

Transport- und Logistikunternehmen (siehe Tabelle 1) spielen bei der Implementierung des beschriebenen Trackingsystems eine entscheidende Rolle: Das Tracking von Daten eines Lieferfahrzeugs ist nur möglich, wenn das Transportunternehmen die dafür benötigte Infrastruktur installiert. Diese Installation kommt für das Unternehmen in Frage, wenn das Trackingsystem einen echten Nutzen generiert und sich deshalb eine Investition darin lohnt. Einen solchen Nutzen könnte die Optimierung von Transportwegen und Lieferprozessen darstellen, die durch Live-GPS-Tracking möglich wird.

Tabelle 2 Kundenprofil Grenzkontrolle

Grenzkontrolle	
<p><i>Job to be done:</i> Prüfen der Herkunft eines Gutes</p>	<p><i>Pains:</i> Abgesehen von den Transportpapieren haben die Behörden keine Informationen zum Fahrzeug, das überprüft werden muss.</p>
<p><i>Use Cases:</i> Überprüfen eines LKWs</p>	<p><i>Gains:</i> Verlässliche Informationen zur Herkunft und dem Lieferweg eines spezifischen LKWs</p>

Grenzkontrollen (siehe Tabelle 2) könnten die aufgezeichnete Fahrdaten als verlässliche Datenquelle nutzen. Im Gegensatz zu den bisher bekannten Blockchain-Projekten, bei der nur Informationen zur Herkunft eines Produkts oder bestimmten Supply Chain Stationen nachgewiesen werden, ist bei einem GPS-Trackingsystem das ununterbrochene Nachverfolgen des gesamten Lieferwegs möglich.

Tabelle 3 Kundenprofil Produktionsunternehmen

Produktionsunternehmen	
<p><i>Job to be done:</i> Optimierung der Supply Chain</p>	<p><i>Pains:</i></p> <ul style="list-style-type: none"> - Unbekannte Vorgeschichte der Teil-produkte - Fehlende Details zur Auslieferung der Ware
<p><i>Use Cases:</i> Optimierung der Supply Chain eines bestimmten Produkts durch Betrachten der dazugehörigen Logistikprozesse</p>	<p><i>Gains:</i> Übersicht zur ganzen Supply Chain und detaillierte Informationen zur Auslieferung der fertigen Produkte</p>

Bei der Intra-Logistik haben Produktionsunternehmen volle Kontrolle über die Logistik-Prozesse. Dies ist bei der Inbound- und Outbound-Logistik nicht gegeben. Dort sind Produktionsunternehmen angewiesen auf die effiziente und sorgfältige Arbeitsweise ihrer Zulieferer und Verteiler. Gerade bei der zeitkritischen Auslieferung von Produkten wären mehr Details zum Lieferprozess interessant.

Viele BC-Projekte in der SC zeichnen Informationen punktuell auf. Eine erste Aufnahme der Informationen findet beispielsweise beim Erhalt der Rohstoffe statt, ein zweites nach der Herstellung eines Teilprodukts usw. Dabei ist die Aufzeichnung der Daten abhängig von einzelnen Teilnehmern

der Lieferkette: Diese sind dafür verantwortlich in ihrem Bearbeitungsschritt dem Produkt einen digitalen Stempel zu geben. Bei einer kontinuierlichen Aufzeichnung der Daten durch vorinstallierte Geräte, ist diese Abhängigkeit nicht gegeben.

Das oben beschriebene Tracking ist ein Beispiel für eine kontinuierliche Datenaufzeichnung, die unabhängig von Intermediären geschieht. Voraussetzung ist die im Vorfeld installierte Infrastruktur: In diesem Fall ein Gerät, welches am LKW befestigt oder integriert wird und Positionsdaten sicher aufzeichnet und auf den Distributed Ledger hochlädt.

Im folgenden Kapitel wird die Idee in unternehmerischer Hinsicht überprüft und mit den resultierenden Ergebnissen revidiert.

4.1.1 Ergebnisse Erstellung Kundenprofile

Der Nutzen des geschilderten Anwendungsfalls lässt sich nach der Erstellung der Kundenprofile in drei Punkten zusammenfassen:

- Das Trackingsystem soll Logistikunternehmen die Möglichkeit geben, die gefahrenen Routen zu überprüfen und Lieferrouten und -prozesse zu optimieren.
- Der limitierte Zugang zu den aufgezeichneten Daten gibt Auftraggebern mehr Transparenz im Lieferprozess
- Der limitierte Zugang zu den aufgezeichneten Daten gibt Behörden die Möglichkeit, Gütertransporte besser zu überprüfen

Als Resultat werden für die Online-Umfrage Logistikunternehmen und Kunden der Logistikunternehmen, z. B. Produktionsunternehmen, als Zielpublikum gewählt. Auf die Befragung von Behörden wird aus Aufwandsgründen verzichtet.

5 Prüfung in unternehmerischer Hinsicht

Die Stichhaltigkeit der beschriebenen Idee im letzten Kapitel wird durch die Befragung von Logistikunternehmen und den Kunden von Logistikunternehmen, einfachheitshalber Produktionsunternehmen genannt, überprüft. Ebenfalls überprüft wird die Notwendigkeit eines Distributed Ledgers nach den Kriterien des Artikels «Do you Need a Blockchain?» (Wüst & Gervais, 2018). Ausgehend von den Ergebnissen der Fallstudie in den Grundlagen und den folgenden Analysen wird der Anwendungsfall dann revidiert.

5.1 Eignung eines Distributed Ledgers

Wüst und Gervais diskutieren im Beitrag «Do you Need a Blockchain?» anlässlich der Crypto Valley Conference 2018, in welchen Anwendungsfällen eine Blockchain Sinn macht. Das Evaluationsverfahren kann auch für IOTA angewendet werden. Dabei müssen aber einige Unterschiede zwischen Tangle und Blockchain berücksichtigt werden:

Bei einer Blockchain ist der Datendurchsatz langsamer, je mehr Nodes Teil des Netzwerks sind. Dies bedeutet, dass eine öffentliche Blockchain aus diesem Aspekt betrachtet einen niedrigeren Datendurchsatz hat als eine private Blockchain.

Die Beziehung von Grösse des Tangles und Datendurchsatz ist bei IOTA hingegen genau umgekehrt: Je mehr Transaktionen durchgeführt werden, desto schneller wird eine einzelne Transaktion verifiziert. Das hat damit zu tun, dass jede Transaktion zwei andere Transaktionen verifizieren muss, bevor sie in den Tangle aufgenommen wird. Somit hat ein öffentlicher Tangle unter Berücksichtigung dieses einen Aspekts einen höheren Datendurchsatz als einen privaten Tangle¹⁵.

Durch die Beantwortung der Fragen im Evaluationsverfahren soll der beschriebene Anwendungsfall nun beurteilt werden. Der Flow Chart in Abbildung 6 visualisiert den Ansatz.

Müssen Datenzustände gespeichert werden?

Die erste relevante Frage bei der Entscheidung für oder gegen einen Distributed Ledger ist, ob im betrachteten Anwendungsfall Datenzustände gespeichert werden müssen. Ist dies nicht der Fall, ist weder eine Blockchain noch eine klassische Datenbank nötig (Wüst & Gervais, 2018).

Bei der Aufzeichnung von Lieferwegen müssen Positionsdaten gespeichert werden, damit Transportunternehmen Ihre Fahrzeuge verfolgen können und für die Behörden einen Beweis der

¹⁵ Der Datendurchsatz ist auch noch abhängig vom Sicherheitslevel bei der Adressengenerierung. Dieser kann bei einem privaten Tangle frei gewählt werden.

gefahrenen Strecke erbracht werden kann. Somit macht ein Distributed Ledger, aus dieser Perspektive betrachtet, Sinn.

Gibt es mehrere Parteien mit Schreibzugriff?

Bei dieser Frage geht es darum, ob mehrere Teilnehmer die Möglichkeit haben sollen, Informationen auf den Distributed Ledger zu schreiben. Gibt es nur eine Partei, die Schreibzugriff hat, könnte auch eine normale Datenbank verwendet werden.

Bei Anwendungen im Internet of Things ist die Voraussetzung von mehreren Schreibenden gegeben: Viele Geräte müssen die Möglichkeit haben, gleichzeitig Daten aufzuzeichnen. Ein Einwand dagegen ist, dass man diese Geräte auch zu einer einzigen Partei zusammenfassen kann, wenn die Geräte alle denselben Besitzer haben.

Die Trackinggeräte im beschriebenen Anwendungsfall würden vermutlich alle dem gleichen Transportunternehmen gehören. Obwohl ein Gerät Daten selbständig aufzeichnet, wäre es deshalb dennoch nicht ganz unabhängig. Somit ist die Legitimität eines Distributed Ledgers aus dieser Perspektive gesehen nicht gegeben.

Ist eine Trusted Third Party ständig online verfügbar?

Wüst und Gervais (2018) schreiben in Ihrer Veröffentlichung, dass eine ständig online verfügbare Trusted Third Party (TTP) in der Supply Chain theoretisch immer vorhanden sei. Praktisch müsse von Fall zu Fall bestimmt werden, ob dem so ist. Eine TTP könnte laut Wüst und Gervais (2018) als einzig Schreibender auf dem Ledger die verifizierende Partei für eine Datenzustandsänderung sein.

Im beschriebenen Anwendungsfall könnte für die Identifizierung der Tracking-Geräte ein zentrales Authentifizierungssystem als TTP verwendet werden und die Daten bei erfolgreicher Authentifizierung in eine herkömmliche Datenbank geschrieben werden, die von einer neutralen Partei verwaltet wird.

Dabei wäre aber bei Unregelmäßigkeiten die Nachverfolgbarkeit nicht im gleichen Masse gegeben und das zentrale Authentifizierungssystem der *Single Point of Failure* im System. Das Zugriffsmanagement auf die Positionsdaten müsste nach der Definition gemeinsamer Regeln aller SC-Teilnehmer von der TTP dynamisch gehandhabt werden.

Sind alle schreibenden Parteien bekannt?

Im beschriebenen Anwendungsfall wären alle schreibenden Parteien bekannt, da nur identifizierte Trackinggeräte Schreibzugriff hätten. Die SC-Teilnehmer sind ebenfalls bekannt.

Wenn alle Parteien bekannt sind, ist entweder ein public permissioned oder ein private permissioned Distributed Ledger sinnvoll. Bei IOTA können durch private oder restricted MAM-Channels Daten permissioned veröffentlicht werden.

Wird allen schreibenden Parteien vertraut?

Selbst wenn Supply Chain Teilnehmer ein grundsätzliches Vertrauen ineinander haben, sind die Prozesse in der Supply Chain nicht verlässlich. Es muss davon ausgegangen werden das auch integrale Parteien Fehler im Lieferprozess machen. Das Nachvollziehen dieser Fehler ist für die Effizienz und Optimierung der Supply Chain wichtig. Aus dieser Perspektive macht einen Distributed Ledger Sinn.

Da es sich bei den schreibenden Parteien direkt um die Trackinggeräte handelt, muss die Vertrauenswürdigkeit von IoT-Geräten ebenfalls diskutiert werden. Wüst und Gervais (2018) nennen im Zusammenhang mit IoT das Problem der fehlenden Verbindung zwischen realer und digitaler Welt. Wenn den IoT-Geräten und deren Daten nicht vertraut wird, ist die Absicherung über einen Distributed Ledger sinnlos. Die Vertrauenswürdigkeit der Geräte ist abhängig von der Zuverlässigkeit und der Manipulierbarkeit der IoT-Geräte. Hier ist deshalb keine pauschale Antwort möglich.

Ist öffentliche Nachverfolgbarkeit verlangt?

Ist keine öffentliche Nachverfolgbarkeit verlangt, empfehlen Wüst und Gervais (2018) aus Datenschutz- und Performanz-Gründen eine private permissioned Blockchain. In diesem Bereich unterscheidet sich die Entscheidungsfindung für IOTA: Aus Performanz-Gründen empfiehlt sich auch wenn keine öffentliche Nachverfolgbarkeit verlangt wird ein public permissioned Tangle. Der Datenschutz kann, wie bereits erwähnt, mit einem restricted MAM-Channel gewährleistet werden.

Die Nachverfolgbarkeit von Lieferrouten sollte nicht öffentlich sein. Der Zugriff auf die Positionsdaten muss äusserst vorsichtig gehandhabt werden, da es sich im Hinblick auf den Fahrer um personenbezogene Daten handelt.

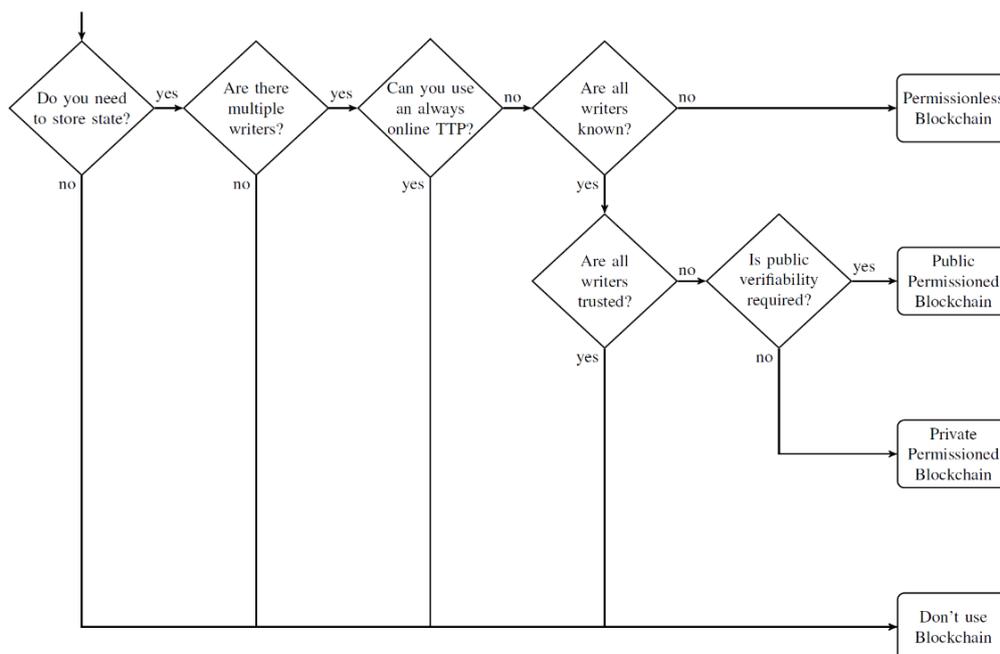


Abbildung 6 Flow Chart «Do you Need a Blockchain? »

Quelle: Wüst & Gervais, 2018

5.1.1 Ergebnisse Eignung eines Distributed Ledgers

Weil die Trackinggeräte, die Positionsdaten über den Ledger aufzeichnen würden, vermutlich alle dem gleichen Unternehmen gehören würden, ist die Absicherung über einen Distributed Ledger fraglich: Eine Manipulation der Geräte wird vereinfacht und könnte die aufgezeichneten Daten nutzlos machen.

Sollten dennoch Daten zur Nachverfolgbarkeit gesammelt werden, könnte alternativ zu einem Distributed Ledger eine herkömmliche Datenbank verwendet werden, auf die Produktionsunternehmen und Behörden durch ein Authentifizierungssystem temporär Lesezugriff erhalten. Die Identität der Trackinggeräte müsste dann von einer TTP, z. B. dem Gerätehersteller, vergeben werden und fortwährend vom Authentifizierungssystem verifiziert werden. Offen bleibt bei dieser alternativen Lösung jedoch, wie der Zugriff auf die Positionsdaten und die Autorisierung für die Identitätsgenerierung konkret gehandhabt wird.

Im beschriebenen Anwendungsfall soll die Transparenz der Lieferrouten erhöht werden. Die erhöhte Transparenz führt aber in diesem Fall nicht zu direkten finanziellen Einsparungen oder zu einer Minimierung von Risiken.

Der Anwendungsfall muss somit in den folgenden Punkten überarbeitet werden:

- Die Unabhängigkeit der Trackinggeräte muss sichergestellt werden.
- Ein absehbarer finanzieller Nutzen oder eine Risikominimierung (finanzieller Nutzen auf Zeit) muss für alle Stakeholder eindeutig sein. Dies wäre z.B. gegeben, wenn dank der erhöhten Nachverfolgbarkeit und Transparenz, kritische Tätigkeiten digitalisiert resp. automatisiert werden könnten, die sonst manuell ausgeführt würden.
- Ein Distributed Ledger sollte nur verwendet werden, wenn mehrere unabhängige Parteien Schreibzugriff haben sollen.

5.2 Umfrage mit Stakeholdern der Logistikbranche

Eine qualitative Online-Umfrage mit mehrheitlich offenen Fragen untersucht, ob Transportunternehmen und Kunden von Transportunternehmen, vereinfacht Produktionsunternehmen genannt, interessiert am Tracking von Lieferfahrzeugen oder Lieferware sind. Für beide Arten von Stakeholdern wurde eine separate Online-Umfrage erstellt (siehe Anhang S. 73). Ein Grossteil der beiden Varianten stimmt aber überein. Insgesamt haben sieben Unternehmen an der Umfrage teilgenommen. Die Befragung ist deshalb mehr eine Stichprobe als eine umfassende Analyse der Stakeholder-Bedürfnisse auf dem Markt.

In den folgenden Abschnitten werden die Fragen und Antworten der Unternehmen im Detail aufgeführt. Eine Frage zur LSVA-Steuer wurde verworfen, nachdem klar wurde, dass ein neues Gesetz den Transportunternehmen einen digitalen Fahrtenschreiber vorschreibt.¹⁶

Wie viele Fahrzeuge beinhaltet Ihr Transportunternehmen?

Diese Frage dient dazu, die Grösse der Transportunternehmen besser einzuschätzen. Die befragten Transportunternehmen haben zwischen 600 und 1'100 Fahrzeugen. Dazu kommen in einem Fall noch 1'100 Anhänger und 100 Lieferwagen.

Mit welchen Transportmitteln arbeiten Sie oder Ihre Zulieferer bzw. Verteiler?

Diese Frage richtet sich an Produktionsunternehmen. Bei der separaten Umfrage für Transportunternehmen war diese Frage überflüssig, da sämtliche Befragten, Schwerlastverkehr nutzen. Alle vier befragten Unternehmen nutzen Schwerlastverkehr. Zwei Unternehmen nutzen zusätzlich Schienentransport, davon nutzt eines noch Schiffstransport.

Wie organisieren Sie die verfügbaren Ressourcen (Fahrer, Fahrzeuge)?

Genannt wird das Time Management System (TMS). Ein anderes Transportunternehmen teilt die Aufträge meist am Vortag mit möglichst optimalem Routing auf die Fahrzeuge auf, um Leerfahrten zu vermeiden. Ein drittes Transportunternehmen erklärt, dass ca. 70 % der Fahrzeuge mit einem Stammfahrer besetzt sind. Die restlichen Fahrzeuge müssen täglich oder wöchentlich mit einem Fahrer besetzt werden. Die Disposition macht die Fahrzeug- und Fahrerplanung anhand der aktuellen Auftragslage.

Bei den befragten Produktionsunternehmen wird die Planung der Ressourcen grösstenteils vom Transportunternehmen übernommen. In einem Fall verfügt ein Unternehmen über eigene Fahrzeuge;

¹⁶ Die neuen EU-Regelungen führen dazu, dass in der Europäischen Union sämtliche ab dem 15. Juni 2019 neu zum Verkehr zugelassenen Fahrzeuge, die von der Verordnung (EU) Nr. 165/2014 betroffen sind, mit einem «intelligenten Fahrtenschreiber» ausgerüstet werden müssen» Bundesamt für Strassen (2019).

diese werden mittels Fahrzeugplanlisten geplant. Überlasten werden, wenn nötig, durch externe temporäre Mitarbeiter und Mietfahrzeuge abgedeckt.

Ein Unternehmen, das mit einem der grössten Transporteure weltweit zusammenarbeitet, spricht sich täglich mit dem Transporteur ab. Dieser teilt die Fahrzeuge dann nach seiner Erfahrung ein. Saisonale Schwankungen spielen bei der Einteilung eine wichtige Rolle.

Für die Anmeldung der Anlieferungen wird in einem Fall eine spezielle Software, die Anlieferarrampendispositionssoftware als Kommunikationsmittel zwischen Disposition des Zulieferers und dem Unternehmen verwendet.

Welche Probleme ergeben sich dabei?

Probleme bei der Ressourcenplanung sind unter anderem Schwankungen der Sendungszahlen und die Unberechenbarkeit wie lange die Bearbeitung eines Auftrags durch den Fahrer schlussendlich geht. Diese Unberechenbarkeit kommt durch mögliche Verzögerungen wie Stau und ungewisse Wartezeiten bei Kunden. Ein Transportunternehmen nennt die vielen plan- und unplanmässigen Faktoren (z. B. Unfall und Krankheit, Werkstatt- und Prüftermine), welche die Ressourceneinteilung beeinflussen, als grösste Herausforderung.

Ein Produktionsunternehmen nennt als Herausforderung die Einschätzung des tatsächlichen Aufwands für Kundenbestellungen. Falscheinschätzungen können zu einer Überkapazität bei Auslieferungen führen. Als weiteres Problem bei der Ressourceneinteilung werden kurzfristige Änderungen genannt. Die Abstimmung zwischen aktueller Verkehrslage (bei einem Bahnunternehmen) und Dienstplänen unter Einhaltung des Arbeitszeitgesetzes sei schwierig.

Wie stellen Sie sicher, dass Fahrer auch tatsächlich die vereinbarte Strecke fahren?

Diese Frage richtet sich an Transportunternehmen: In zwei Fällen werden die laufenden Aufträge direkt über eine Fahrzeug-Applikation getrackt. Das Ziel der nächsten Lieferung kann direkt in Google Maps oder einem Navigationssystem angezeigt werden. Die Fahrstrecke kann im Nachhinein durch die Disposition überprüft werden. In einem Fall wird ein separates Gerät für die Auftragsabarbeitung verwendet.

Wie stellen Sie sicher, dass die Zulieferung bzw. die Verteilung Ihrer Ware effizient geschieht?

Diese Frage richtet sich ausschliesslich an Produktionsunternehmen. Ein Unternehmen mit eigenen Fahrzeugen antwortete, dass Abweichungen mittels eines Dispositionstools nachverfolgt und analysiert werden können. Wenn «Mehrkilometer» vom Fahrer nicht plausibel erklärt werden können, werde dieser entsprechend geschult.

Ein anderes Unternehmen, zahlt seine Sendungen nach dem GU-Tarif, einer Pauschale, bei dem die Dauer des Lieferprozesses keine Rolle spielt¹⁷. Auch in einem zweiten Fall, ist die Effizienz einzig vom Transportunternehmen abhängig: Die Anlieferung und Verteilung der Ware werde direkt durch den Spediteur optimiert.

Würde Ihnen ein Live-Tracking (Zeit und Ort) eines Fahrzeugs oder eines Warencontainers für bessere Nachverfolgbarkeit weiterhelfen?

Transportunternehmen:

Zwei der befragten Transportunternehmen besitzen bereits ein Trackingsystem für Fahrzeuge. In einem Fall wird der Standort des Fahrzeugs auf einer Karte dargestellt und bei jeder Richtungsänderung neu übermittelt. Bei einer geraden Strecke wird der Standort nach 15 Minuten übermittelt. Ein Unternehmen beantwortet die Frage mit Ja, nennt aber als Bedingung, dass auch Staus sowie Angaben zu möglichen Ankunftszeiten am Destinationsort sichtbar sein sollten.

Produktionsunternehmen:

Ein Unternehmen besitzt selber ein Trackingsystem und empfindet das System als hilfreich. Jedoch wird bewusst nicht das Fahrzeug mit direktem Bezug zum Fahrer aufgezeichnet, sondern die Ware. Ein zweites Unternehmen arbeitet mit einem Transportunternehmen zusammen, dass Tracking ebenfalls einsetzt. Auf einer Website kann der Endkunde seine Sendungsnummer eingeben und dann sehen, wo sich das Fahrzeug gerade befindet. Die ungefähre Zustellzeit kann ebenfalls berechnet werden. Ein Unternehmen würde ein Live-Tracking nicht als hilfreich empfinden.

Ein weiteres Unternehmen, dass über Live-Tracking verfügt, würde sich besonders für die Aufzeichnung der Grösse «Voraussichtliche Ankunftszeit» interessieren.

Was sind die dringendsten Probleme Ihrer Branche?

Transportunternehmen:

Mehrfach genannt wird die Verkehrslage bzw. Verkehrsüberlastung in der Schweiz. Weitere Probleme sind fehlende Standards in Sachen Visibilität für die Kunden: Viele Anbieter haben keine standardisierten Meilensteine innerhalb des Transportprozesses. Dies erschwere die Informationsbeschaffung und führe zu mehr manueller Arbeit und physischen Dokumenten, was die Effizienz sinken lässt. Problematisch seien zudem die immer kürzeren Bestellintervalle.

Produktionsunternehmen:

Zwei der befragten Unternehmen bestätigen die in der Recherchephase identifizierten Probleme der Supply Chain: Koordination, Kommunikation unter den verschiedenen Teilnehmern und hoher

¹⁷ Anmerkung: Die Optimierung des Lieferprozesses scheint für das Unternehmen deshalb von geringem Interesse zu sein.

administrativer Aufwand durch viele Schnittstellen. Eine weitere Herausforderung seien hohe Anforderungen im Bereich Produktivität und Qualität.

Wenn ein Transportfahrzeug oder eine Liefereinheit eindeutig identifiziert, live verfolgt werden und GPS-Daten nicht-manipulierbar aufgezeichnet werden könnten – würde Ihnen dies helfen?

Transportunternehmen:

Zwei der befragten Unternehmen beantworten diese Frage mit Ja, ein Unternehmen mit Nein. Die Begründung für das Nein ist, dass die GPS-Daten nur intern von Belang und deshalb nicht kritisch seien. Sie müssten deshalb auch nicht z. B. mittels einer Blockchain abgesichert werden.

Produktionsunternehmen:

Drei der befragten Unternehmen beantworten diese Frage mit Ja, ein Unternehmen mit Nein. Die Begründung für das Nein ist, dass GPS-Daten bereits aufgezeichnet würden. Die Aufzeichnung der Grösse «Voraussichtliche Ankunftszeit» wäre hilfreicher.

Welche Informationen wären für Sie bei einem (Fahr-)daten-Tracking evtl. auch interessant?

Als Auswahl wurden die vier Grössen «Gewicht der Ladung», «Feuchtigkeit», «Temperatur» und «Wann und wo die Ladeklappe geöffnet wurde» und «Andere», angegeben.

Transportunternehmen:

Von den angegebenen Grössen wird besonders «Gewicht der Ladung» und «Wann und wo die Ladeklappe geöffnet wurde», als hilfreich empfunden. Andere hilfreiche Grössen sind die Standzeit beim Kunden, das Handling von Tauschgeräten und Unregelmässigkeiten. Ein Unternehmen gibt an, nebst der Feuchtigkeit, bereits alle angegebenen Grössen zu messen.

Produktionsunternehmen:

Zwei der befragten Stakeholder fänden keine der angegebenen Grössen für ein Tracking interessant. Ein Unternehmen fände ein Tracking vom Gewicht der Ladung und der möglichst genauen Bestimmung der Ankunftszeit interessant. Ebenfalls einmal genannt werden die Feuchtigkeit, Temperatur und «Wann und wo die Ladeklappe geöffnet wurde».

Haben Sie bereits Projekte mit Blockchain oder Distributed Ledger Technologien allgemein, welche eine bessere Nachverfolgbarkeit von Lieferware oder Produkten zum Ziel haben?

Diese Frage soll einen Anhaltspunkt geben, ob die befragten Unternehmen, Distributed Ledger Technologien als mögliche Lösung für eine bessere Nachverfolgbarkeit sehen und nutzen.

Von allen befragten Unternehmen hat nur ein Transportunternehmen ein Projekt mit einer Distributed Ledger Technologie. Ein anderes Unternehmen antwortete, dass die Thematik nicht fremd sei und beobachtet werde.

5.2.1 Ergebnisse Umfrage

Die Antworten zur Online-Umfrage gaben hilfreiche Aufschlüsse darüber, wie Gütertransportunternehmen Ihre Ressourcen einteilen, wie Sie Nachverfolgbarkeit gewährleisten und wo es noch Verbesserungspotenzial gibt.

Die Antworten zeigen, dass die Ressourceneinteilung nach wie vor mit grösserem Aufwand verbunden ist. Die Zusammenarbeit zwischen Logistikunternehmen und Kunde ist intensiv und komme z. T. täglich vor. Die meisten genannten Probleme bei der Ressourcenplanung haben mit der Planungsunsicherheit zu tun.

Die Fahrstrecken werden bereits jetzt von allen Logistikunternehmen aufgezeichnet und z. T. live verfolgt. Ein Unternehmen betonte, dass bewusst nicht das Fahrzeug mit dem Fahrer, sondern die Ware verfolgt würde. Dieser datenschutzrechtliche Aspekt sollte bei einem Prototyp berücksichtigt werden. Ein Live-Tracking wird mit einer mehrheitlichen Zustimmung von mehr als 66% als hilfreich empfunden. Mehrfach genannt wurde der Nutzen einer präzisen Schätzung der Ankunftszeit am Destinationsort.

Bei der Frage, welche Grössen für ein Live-Tracking interessant sind, nannten einige Unternehmen zusätzliche Datengrössen zur gegebenen Auswahl, was zu interessanten Anregungen führte. Aufgrund der kleinen Antwortzahl und der Divergenz der Antworten lässt sich für diese Frage keine quantitative Beurteilung machen.

Basierend auf diesen Ergebnissen soll der Anwendungsfall in folgenden Bereichen überarbeitet werden:

- Anstelle von Fahrzeugen sollen Liefereinheiten wie z. B. ein Warencontainer eines einzelnen Unternehmens getrackt werden. Dies ermöglicht Produktionsunternehmen das Verfolgen ihrer Liefereinheit und schützt die Privatsphäre des Fahrers.
- Die Ankunftszeit und das Erkennen von Unregelmässigkeiten für eine bessere Planbarkeit spielen eine wichtige Rolle. Diese Grössen sollten in einem Anwendungsfall berücksichtigt werden.

5.3 Überarbeiteter Anwendungsfall

Aufgrund der Ergebnisse aus der Analyse «Do you Need a Blockchain?» und der Online-Umfrage wurde der Anwendungsfall überarbeitet. Eine abgeänderte Form des Anwendungsfalls ist hier beschrieben.

Ein Ablauf könnte so aussehen:

1. Ein Produktionsunternehmen registriert eine Liefereinheit mit der geplanten Ankunftszeit und -datum, die es gerne an das Logistikunternehmen abgeben möchte. Die Liefereinheit erhält eine eindeutige Identität, die mit der Geräteidentität des Trackinggeräts verbunden ist.
2. Das Logistikunternehmen sammelt die Aufträge und erstellt dann selber einen damit verbundenen Frachtschein. Nach Start des Lieferprozesses erhalten Logistikunternehmen temporär Zugriff auf die Trackingdaten der Liefereinheiten.
3. Unregelmässigkeiten werden entdeckt, indem die Positionsdaten von Liefereinheiten der gleichen Fracht verglichen werden.
4. Behörden erhalten über den digitalen Frachtschein temporären Zugriff zu den Informationen der Liefereinheiten der Fracht. Bei erfolgreicher Prüfung erhält der Frachtschein die Signatur der Behörden.
5. Sender erhalten eine Verifikation, dass die Liefereinheit angekommen ist, sobald eine bestimmte Position erreicht oder z.B. eine elektronische Schranke passiert wurde.
6. Empfänger erhalten eine Meldung, wenn eine Lieferung angekommen ist. Damit hat der Sender seine Pflichten gegenüber dem Empfänger erfüllt. Wird die Liefereinheit nicht oder stark verspätet abgeliefert, kann auf Basis der Trackingdaten ein Schadenersatz gefordert werden.

Die Verwendung eines Distributed Ledgers macht hier im Gegensatz zum ursprünglichen Anwendungsfall viel mehr Sinn:

- Mehrere Parteien schreiben Informationen in den Distributed Ledger (Logistikunternehmen – Frachtschein, Produktionsunternehmen – Liefereinheit, Behörden – Signatur Frachtschein)
- Die Nachverfolgbarkeit und Datentransparenz haben direkte finanzielle Einsparungen zum Resultat: Einerseits können dank der erhöhten Nachverfolgbarkeit und Transparenz kritische Tätigkeiten automatisiert werden, die sonst manuell ausgeführt würden. Andererseits dienen die Daten als Beweismittel, wenn es zu Fehlern im Lieferprozess kommt, die zu kostenintensiven Verzögerungen führen.

6 Technische Lösung

In diesem Teil der Arbeit wird ein technisches Lösungssystem für den geänderten Anwendungsfall des vorigen Kapitels beschrieben. Mithilfe von Experimenten werden dann einzelne Aspekte des Systems genauer betrachtet und die Lösung auf ihre Tauglichkeit überprüft. Im Anschluss daran wird die Funktionalität des Systems getestet und der Systemprototyp in Bezug auf die Anforderungen eines wirklichen Trackingsystems analysiert.

6.1 Konzept

Für den im Kapitel 5.3 beschriebenen Anwendungsfall wird hier ein technisches Lösungskonzept vorgestellt. Teil dieses Konzepts ist die Beschreibung von vier Use Cases, Teilaktivitäten des beschriebenen Anwendungsfalls, die im Rahmen des Prototyps genauer betrachtet werden sollen. Das Systemverhalten wird durch Sequenzdiagramme der einzelnen Use Cases beschrieben.

Die Abbildung 7 zeigt die Architektur des Prototyps. Die Wahl der einzelnen Komponenten und Gestaltung der Architektur wird im folgenden Kapitel begründet.

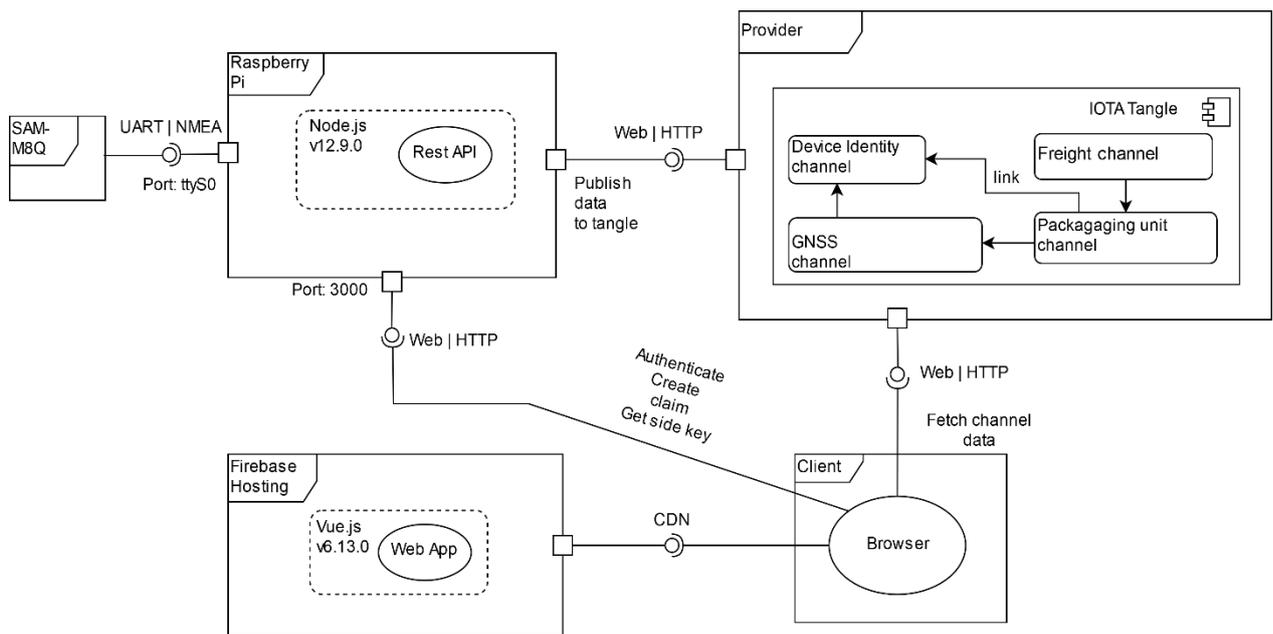


Abbildung 7 Architektur des Prototyps

Quelle: Eigene Darstellung

Die Tabelle 4 fasst die verwendete Hardware zur besseren Nachvollziehbarkeit zusammen:

Tabelle 4 Verwendete Hardware finaler Prototyp

<i>Hardware</i>	<i>Erhältlich unter</i>
Raspberry Pi 3B+	https://www.pi-shop.ch/raspberry-pi-3-model-b
GNSS-Modul SAM-M8Q	https://fpvracing.ch/de/messelektronik/2683-matek-gps-ublox-sam-m8q.html
Li-Polymer Akku 5V 5000mAh	https://www.pi-shop.ch/li-polymer-power-bank-pb-a5200-externer-lade-akku-5v-5000mah

6.1.1 Entscheidungen

In diesem Abschnitt werden Entscheidungen zur Architektur des Prototyps begründet.

Identitätsmanagement

Das System basiert auf einem Claim-based IdM-Ansatz. Wie bereits in den Grundlagen beschrieben bringt dieser Ansatz einen höheren Datenschutz für die Subjekte im Vergleich zu einem Network-based Ansatz mit sich. Zudem kann Claim-based IdM als dezentrale Lösung umgesetzt werden. Die Credentials der Subjekte sollen in Anlehnung an SSI auf dem Subjekt selber gespeichert werden. Gleichzeitig soll ein Hash des Credentials auf dem IOTA Tangle veröffentlicht werden. Auf die Nutzung von DIDs wird verzichtet: IOTA verfügt zwar eine DID-Lösung. Diese ist jedoch nicht von offizieller Stelle entwickelt. Dessen Zuverlässigkeit kann deshalb zu wenig eingeschätzt werden.

Tracking

Im System sollen Positionsdaten, genauer GNSS-Daten, getrackt werden. Für das Tracking wird das GNSS-Modul SAM-M8Q verwendet. Es soll einen guten Empfang über den ganzen Lieferweg sicherstellen.

IoT-Gerät

Für die Aufbewahrung von Credentials und der Veröffentlichung der Trackingdaten auf dem Tangle wird ein Raspberry Pi 3B+ verwendet. Die Verwendung eines Raspberry Pi's hat den Vorteil, dass die gut dokumentierte und am weitesten entwickelte Client Library von IOTA in JavaScript in einer Node.js-Umgebung verwendet werden kann. IOTA verfügt jedoch auch eine von der Community entwickelte Client Library in C, die z. B. in Kombination mit einem Arduino verwendet werden könnte.

Interaktion mit User

Die Darstellung der Trackingdaten und die Interaktion der User mit dem IoT-Gerät soll anhand einer Web Applikation veranschaulicht werden. Dadurch wird der Systemablauf fassbarer und eine

Kommunikationsgrundlage für Stakeholder ohne tiefe technische Kenntnisse wird geschaffen. Der Fokus liegt jedoch nicht auf dem Design des UI's sondern auf der Funktionalität der Web Applikation. Durch das Client Delivery Network von Firebase-Hosting wird eine gute Verfügbarkeit der Web Applikation unabhängig vom Ort sichergestellt. Alternativ könnte zu Lernzwecken eine Ausführung von Scripts über ein Terminal verwendet werden.

MAM Channels

Für die Absicherung von Credentials und Trackingdaten sollen verschiedene MAM-Channels verwendet werden. Die gewählte MAM-Channel-Architektur soll Abhängigkeiten zwischen Objekten veranschaulichen und gleichzeitig ein einfaches Side Key Management ermöglichen. Die Abbildung 8 zeigt einen Vorschlag, wie MAM Channels durch ihren Inhalt verknüpft werden können. Der Vorteil dieser Verknüpfung ist, dass Trackingdaten so einen direkten Bezug zur Lieferware haben.

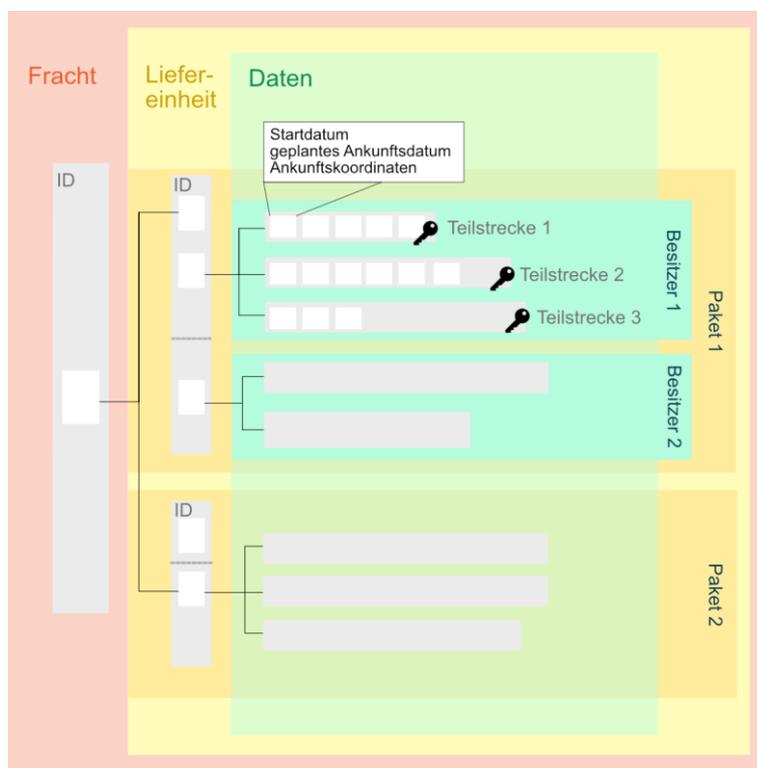


Abbildung 8 MAM Channel Architektur

Quelle: Eigene Darstellung

Die grauen Boxen in Abbildung 8 repräsentieren MAM-Channels. Liefereinheiten sollen direkt mit Trackingdaten verknüpft werden, indem im Credential der Liefereinheit auf den Tracking-Channel verwiesen wird. Für jede Teilstrecke im Lieferprozess wird der Side Key des Channels geändert, so dass Personen aus vorigen Teilstrecken den Zugriff auf die Daten verlieren. Bei einem Besitzerwechsel einer Liefereinheit wird der Credential der Liefereinheit aktualisiert, so dass der ehemalige Besitzer den Zugriff auf die neuen Trackingdaten verliert. Eine zusätzliche Verknüpfung zum MAM-Channel für die Identität des Trackinggeräts wäre ebenfalls denkbar. Mehrere

Liefereinheiten können in einem Frachtschein-Credential zusammengefasst werden. Im Credential des Frachtscheins können die Channel-Roots der Liefereinheiten verschlüsselt aufgeführt werden.

Netzwerk

Die Verfügbarkeit einer REST API auf dem Raspberry Pi ermöglicht das Speichern und Aktualisieren von Identitäten und das Starten einer Trackingsequenz. Die Konnektivität zur REST API des Raspberry Pi's wird mit remote.it (www.remote.it/), einem Anbieter für virtuelles privates Internet, sichergestellt. Es ist im Vergleich zur Exposition eines Ports des Raspberry Pi's, durch Port Forwarding des Routers, eine sichere Option.

6.1.2 Beschreibung der Systemabläufe

Mithilfe von Sequenzdiagrammen werden hier vier verschiedene Systemabläufe beschrieben. Aufgrund der programmierspezifischen Begriffe sind die Abbildungen dazu in Englisch.

Geräteauthentifizierung und anschließende Registrierung einer Liefereinheit durch Sender

Am Anfang des Lieferprozess registriert ein Sender eine Liefereinheit. Dabei wird zuerst die Identität des Trackinggeräts verifiziert, welches die Liefereinheit über den ganzen Lieferprozess überwachen wird. Idealerweise würde eine Box oder ein Container mit einem fest fixierten Trackinggerät verwendet. Alternativ könnten auch zuerst die Informationen zur Liefereinheit registriert werden und dann automatisch einem freien Trackinggerät zugewiesen werden.

Im Prototyp wird eine Variante verwendet, wo das Trackinggerät bereits an der Liefereinheit befestigt ist und dann mittels QR Code die Registrierung der Liefereinheit erfolgt. In Abbildung 9 wird der Ablauf dieses Use Cases visualisiert.

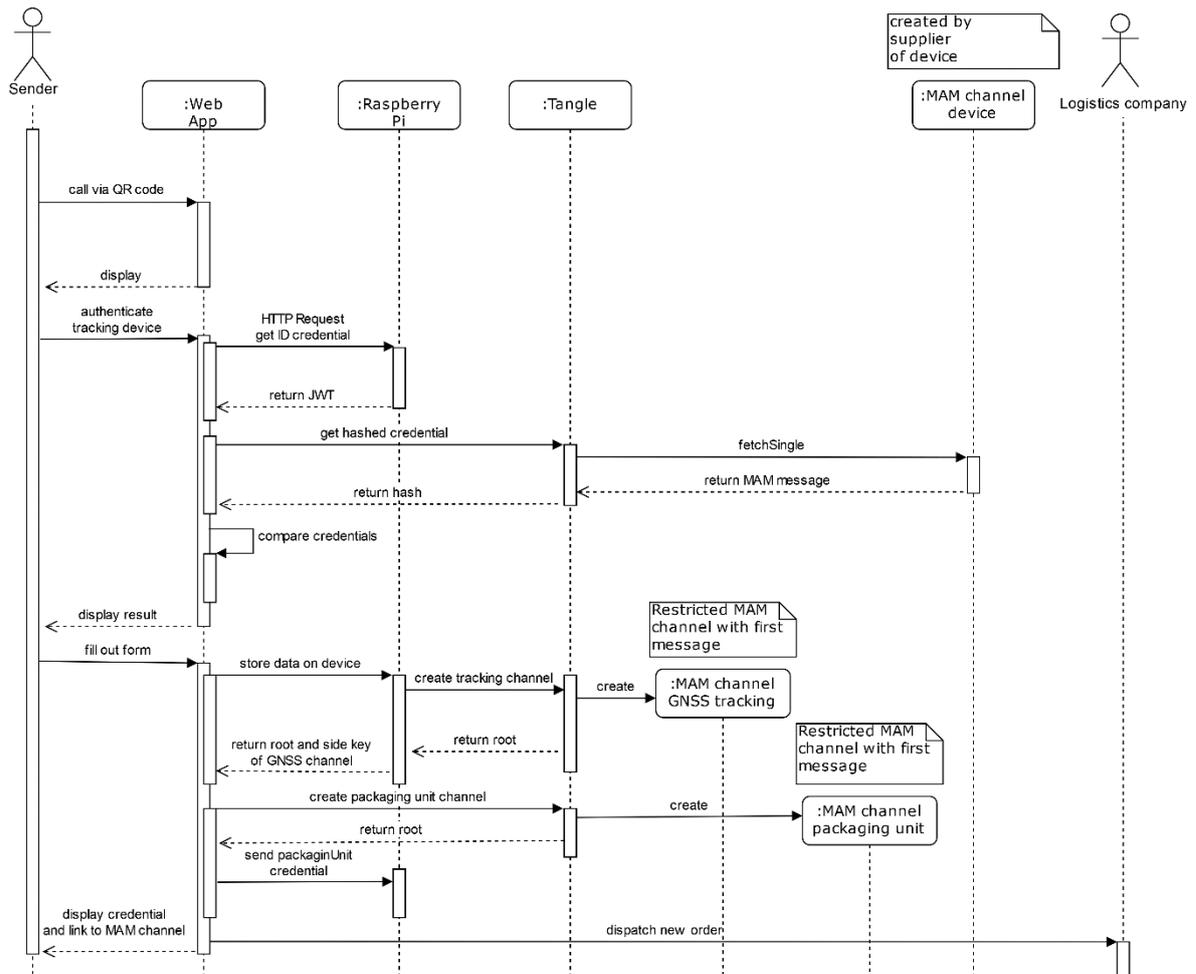


Abbildung 9 Ablauf Use Case 1

Quelle: Eigene Darstellung

Vor der Registrierung einer neuen Liefereinheit wird die Identität des verwendeten Trackinggeräts überprüft. Bei erfolgreicher Identifizierung und gültiger Identität kann eine Liefereinheit zum Tracking registriert werden. Dabei generiert der Raspberry Pi einen neuen GNSS-Tracking-Channel und startet das Tracking. Der Root des Channels und der Side Key wird an die Web Applikation zurückgesendet und kann dort verschlüsselt im Credential für die Liefereinheit aufgeführt werden. Der Credential wird gehasht und auf einen neuen MAM-Channel hochgeladen.

Am Schluss wird das neu erstellte Dokument für die Liefereinheit dem Sender angezeigt und der Link zum Tracking-Channel mitgegeben. Das Dokument wird als neuer Auftrag an das Logistikunternehmen versendet.

Erfassen eines Frachtscheins und Zugriff auf Trackingdaten durch Logistikunternehmen

Im zweiten Systemablauf resp. Use Case fasst das Logistikunternehmen Liefereinheiten zu einer Fracht zusammen: Dafür erstellt das Unternehmen einen Frachtschein, der auf dem Tangle in einem neuen MAM-Channel abgespeichert wird. Nach erfolgreicher Erstellung des Frachtscheins, wird eine Anfrage an das Trackinggerät für den Schlüssel zur Entschlüsselung des Roots im Credential der Liefereinheit gesendet. Nach Erhalt des Schlüssels hat das Logistikunternehmen Zugriff auf die Trackingdaten und kann die Liefereinheit tracken (Abbildung 10).

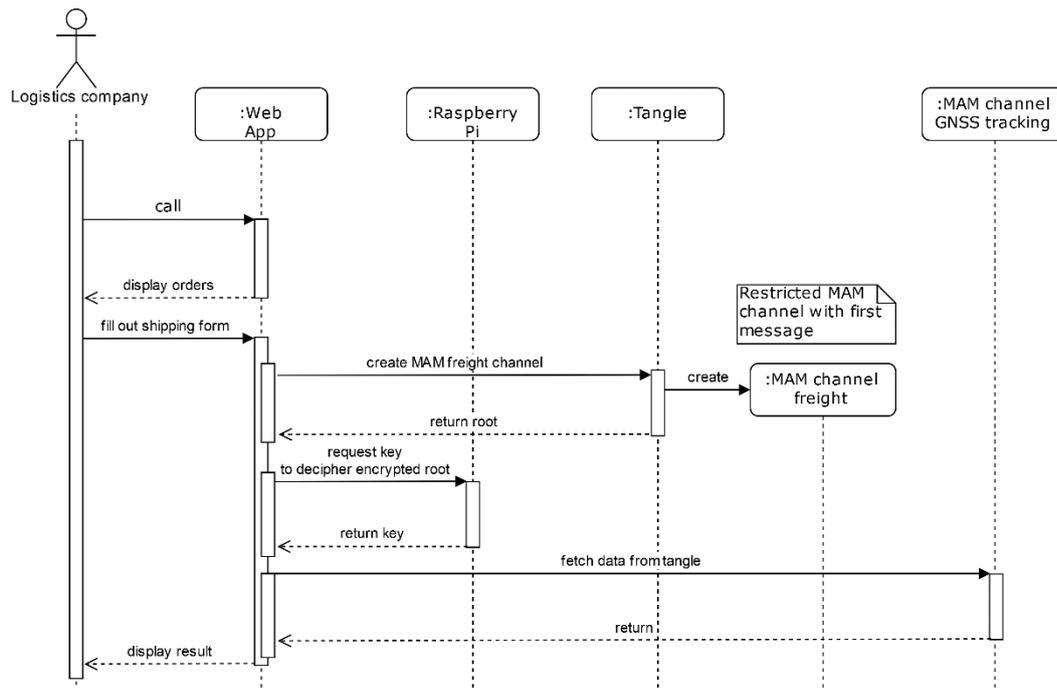


Abbildung 10 Ablauf Use Case 2

Quelle: Eigene Darstellung

Kontrolle einer Fracht durch Behörde

Die Kontrolle einzelner Liefereinheiten ist dank dem Aufruf via QR-Code möglich. Dabei können sowohl der Credential der Liefereinheit als auch die Trackingdaten überprüft werden. Nach einer Überprüfung wird der Side Key des Tracking-Channels geändert, so dass die Behörde den Zugriff auf die Trackingdaten wieder verliert. Dies bringt auch ein Update des Credentials der Liefereinheit mit sich, da dieser nun einen neuen Root für den Zugang zum Tracking-Channel speichern muss.

Was in diesem Prototyp nicht im Detail umgesetzt ist, ist die Überprüfung des digitalen Frachtscheins mit anschließender Signatur des Frachtscheins vonseiten der Grenzkontrolle. Dies würde eine Aktualisierung des Frachtscheins auf dem Tangle mit sich bringen. Dazu müsste man sich auch Gedanken machen, wie die Behörden den Frachtschein erhalten und wo dieser aufbewahrt wird.

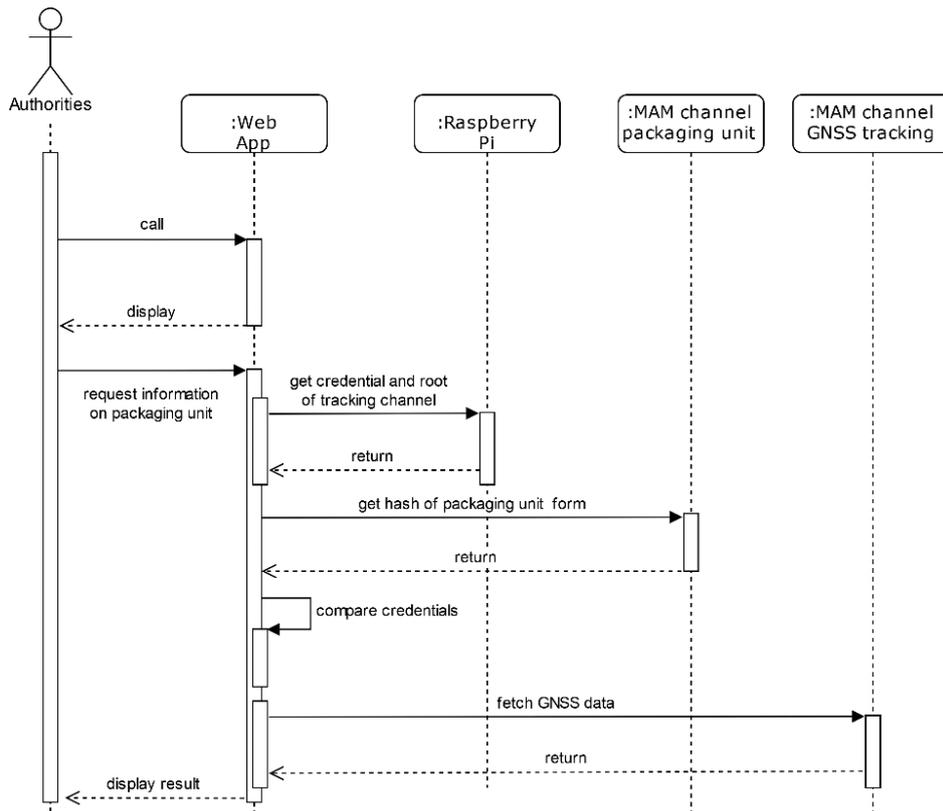


Abbildung 11 Ablauf Use Case 3

Quelle: Eigene Darstellung

Geräteauthentifizierung bei der Ankunft und Stopp des Trackings

Ein vierter Use Case wäre denkbar für die Ankunft der Liefereinheit beim Empfänger. Dank des GNSS-Trackings kann automatisch erkannt werden, wann der Destinationsort erreicht ist.

Bei einer Ankunft kann das Tracking somit automatisch gestoppt und eine Nachricht an den Sender geschickt werden, dass die Lieferung erhalten wurde. Dieser könnte dann den Status der Lieferung im Credential aktualisieren und den Lieferprozess für beendet erklären.

Im Zusammenhang mit IDoT kann beim Empfänger auch eine elektronische Schranke, die Liefereinheiten anhand der Geräteauthentifizierung durchlässt, implementiert werden. Dies wäre besonders interessant bei heiklen Fabrikarealen, bei denen strenge Kontrollen herrschen.

6.1.3 Wahl der Experimente

Durch die Experimente sollen einzelne Aspekte des finalen Prototyps besser untersucht werden. Zudem erfolgt anhand der Experimente eine Vertrautmachung mit der Technologie IOTA.

Ein zentraler Aspekt des beschriebenen Lösungssystems ist die Erstellung und Verwaltung von Credentials für verschiedene Subjekte resp. das Identitätsmanagement dieser Subjekte über den IOTA Tangle. Deshalb wird ein Experiment durchgeführt, in dem ein Identitätsdokument für ein Subjekt erstellt, auf dem IOTA Tangle abgesichert und anschliessend vom Subjekt selber verwaltet wird.

Eine wichtige Komponente sind zudem MAM-Channels: MAM-Channels sind die einzig sinnvolle Art, wie Zero-Value-Transaktionen auf dem Tangle gemacht werden können. Andere Zero-Value-Transaktionen werden nicht verifiziert. Es ist deshalb kritisch, dass MAM die Anforderungen des Anwendungsfalls erfüllt. Deshalb soll ein zweites Experiment zu MAM gemacht werden, bei dem Sensordaten auf MAM-Channels veröffentlicht und dann abgerufen werden.

Mit den Erkenntnissen aus den zwei oben beschriebenen Experimenten könnten dann in weiteren Experimenten die vier weiter oben beschriebenen Use Cases umgesetzt und getestet werden.

6.2 Experiment Identitätsmanagement mit IOTA

In diesem Experiment werden die Themen IDoT, SSI und Identitätsmanagement mit IOTA praktisch angewendet. Die Forschungsfrage für dieses Experiment lautet:

Wie kann ein Identitätsdokument mit IOTA self-sovereign verwaltet werden?

Bei diesem Experiment werden mehrere Skripts über ein Terminal ausgeführt. Es wird bewusst auf eine einzige Applikation verzichtet, damit Lernende die einzelnen Funktionen verstehen und schrittweise durch das Tutorial gehen können. Die Use Case Spezifikation kann im Anhang nachgelesen werden (S. 79). Die Abbildung 12 zeigt den Versuchsaufbau des Experiments.

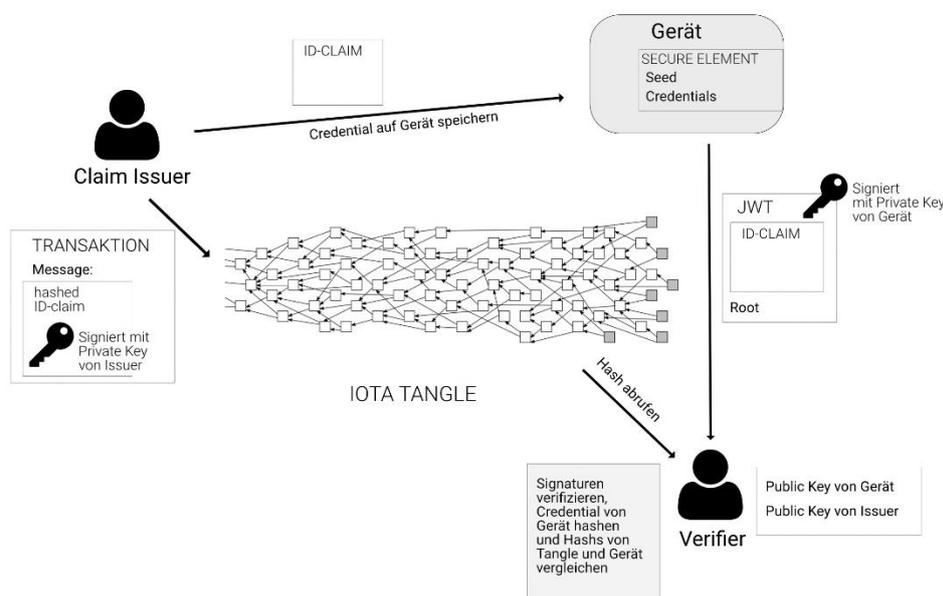


Abbildung 12 Versuchsaufbau Experiment Identitätsmanagement mit IOTA

Quelle: Eigene Darstellung

Der Claim Issuer erstellt ein Identitätsdokument für ein Gerät. Dieses wird auf dem Gerät gespeichert. Gleichzeitig wird eine Transaktion mit dem Hash des Dokuments auf dem IOTA Tangle veröffentlicht. Möchte eine Partei nun die Identität des Geräts verifizieren, kann er das Identitätsdokument des Geräts hashen und mit dem Hash auf dem Tangle vergleichen.

Identitätsdokument erstellen

In einem ersten Schritt wird ein Identitätsdokument, auch Verifiable Identity Claim genannt, vom Claim Issuer erstellt und dann auf dem Raspberry Pi abgespeichert. Dabei handelt es sich um ein einfaches JSON-Dokument mit einem Identifizier z.B. einer UUID, dem Public Key des Geräts, der Adresse des Issuers auf dem IOTA Tangle, dem Namen oder der URL des Issuers, Gerätangaben und Besitzer des Geräts und Ablaufdatum des Identitätsdokuments. Je nach Anwendung und Gerät sind andere Attribute gefragt. Der Credential sollte aber mindestens einen Identifizier für das Subjekt haben und eine Angabe zum Aussteller des Identitätsdokuments. In der Abbildung 13 ist die Erstellung eines solchen Identitätsdokuments gezeigt.

```
$ node generateClaim.js
Claim: {
  subject: 'f5768dbd-36c0-4109-80ad-8b0fcc43aaa8',
  devicePubKey: 'MIGfMA0GCsGqGSIB3DQEBAQUAA4GNADCBiQKBgQCT0dA8wN524+wb5gqaU5uiliT155LoNqDIA2SI5P7VgGsYaH6zByB5jA7+muYCF
UWHnwUpU4DtEB6D59XgGRLfstxuy0Ib7lw1stsHaQW1UmZ5d040lwQW2bMHvm1CwEEa0kVij+d6hsMhPTuFnbu1C3KQ1GbCTEe50ClvN8DPQIDAQAB',
  issuerAddress: 'WMOTSUHSXGELOPMDAHFSYXUGEHNIMGVUOSUHSVUZYPQAQMSOXCWTEIKKYBCNVCBNS9EWE9IVLDNAW',
  issuer: 'https://publicRoadsAdministration.com/',
  data: { deviceOwner: 'Transport GmbH', deviceModel: 'Raspberry Pi 3B+' },
  expirationDate: '01/01/2023'
}
File claim_f5768dbd-36c0-4109-80ad-8b0fcc43aaa8.json created successfully.
```

Abbildung 13 Erstellung eines Identitätsdokuments für einen Raspberry Pi

Quelle: Eigene Darstellung

Abspeichern auf dem IOTA Tangle

Anschliessend wird das Identitätsdokument mit der Hashfunktion SHA256 gehasht. Das Hashen des Claims ist aus Performance-Gründen ab einer bestimmten Grösse des Claims sinnvoll: Das Herunterladen von Nachrichten vom Tangle braucht schon bei einer Dateigrösse von einem Megabyte beträchtlich Zeit.

```
Published {
  message: '2e2bd876794b81c85345e177d7bba49ad5f25186e270207d135baba603cfae1a',
  timestamp: '2019-11-1 22:31:35'
}

Root: YLH9ZOUY9IU9YMPUSGDJPBJUPJYPTFCAOGXCCAQCDTWSALVVIROVSOCHXHDROFCMEDPLDHGPDALRKOTH

Verify with MAM Explorer:
https://mam-explorer.firebaseio.com/?provider=https%3A%2F%2Fnodes.devnet.iota.org&mode=public&root=YLH9ZOUY9IU9YMPUSG
DJPBJUPJYPTFCAOGXCCAQCDTWSALVVIROVSOCHXHDROFCMEDPLDHGPDALRKOTH
```

Abbildung 14 Payload einer MAM-Transaktion

Quelle: Eigene Darstellung

Die Abbildung 14 zeigt die *Payload* der MAM-Transaktion. In der *Message* ist der Hash in Trytes gespeichert. Dazu kommt ein Zeitstempel für den Zeitpunkt der Veröffentlichung. Die erfolgreiche Veröffentlichung des Credentials kann online mit dem MAM Explorer unter [mam-explorer.firebaseio.com](https://mam-explorer.firebaseio.com/?provider=https%3A%2F%2Fnodes.devnet.iota.org&mode=public&root=YLH9ZOUY9IU9YMPUSGDJPBJUPJYPTFCAOGXCCAQCDTWSALVVIROVSOCHXHDROFCMEDPLDHGPDALRKOTH) überprüft werden. Der Eintrag mit Index 0 in Abbildung 15 zeigt die oben veröffentlichte Message.



Abbildung 15 Message im MAM Explorer

Quelle: mam-explorer.firebaseio.com, 2019

Verifizieren der Identität bei Authentifikation des Geräts

Bei Self-Sovereign Identity authentifiziert sich das Gerät gegenüber einer Partei ohne die Unterstützung einer zusätzlichen vertrauenswürdigen Institution. Dies ist aufgrund des gespeicherten Hashs auf dem IOTA Tangle nun auch in diesem Experiment möglich.

Der Claim Verifier, die Partei, gegenüber der sich ein Gerät authentifiziert, schickt eine Anfrage an den Raspberry Pi. Diese Anfrage könnte auch eine Authentifizierung des Verifiers selber beinhalten. Im Experiment wurde dieser zusätzliche Schritt jedoch nicht berücksichtigt.

Für die Kommunikation zwischen Claim Verifier und Gerät wurde einfachheitshalber ein Web Socket-Verbindung verwendet. Die sichere Übertragung des Claims geschieht mit einem JSON Web Token (JWT). Bei Erhalt des Tokens prüft der Verifier zuerst die Signatur des Tokens mit dem Public Key des Raspberry Pi's. Anschließend wird der entschlüsselte Inhalt des Tokens, das Identitätsdokument, gehasht und mit dem Hash des Tangles verglichen.

```

$ node verifyData.js
Valid signature. Decoded payload:
{
  subject: '24ba85fd-ba3c-4cac-92a3-1d4e7ec69bcf',
  devicePubKey: 'MIGfMA0GCsQsIb3DQEBAQUAA4GNADCBiQKBgQCTOdA8wN524+wb5gqaU5uiliT1S5LoNqDIA2SI5P7VgGsYah6zByB5jA7+muYCFsHaQw1UmZ5d040lwQW2bMHvm1CwEEaOkVij+d6hsMhPTuFnbu1C3KQlGbCTEe50ClvN8DPQIDAQAB',
  issuerAddress: 'WwOTSUHSMXGELOPMDAHFSYXUGEHNIMGVUOSUHSIVVUZYPQAQMSOXCWTEKKYBCNVCBNBS9EWE9IVLDAW',
  issuer: 'https://publicRoadsAdministration.com/',
  data: { deviceOwner: 'Transport GmbH', deviceModel: 'Raspberry Pi 3B+' },
  expirationDate: '01/01/2025'
}
Hashed claim: c8376ebc1b49725f54085198c461db1266e0f368837f1b5946df6a567e8116ef
Decoded message: e1af979eb90cf94658c025b7ccd90f1a7e9dba1a962393b482e45f9f0f60aacc
Wrong claim provided

```

Abbildung 16 Verifikation gescheitert

Quelle: Eigene Darstellung

Die Abbildung 16 zeigt die Ausführung der Verifizierungsfunktion ohne WebSocket über Node JS. Im ersten Beispiel ist zwar die Signatur des Tokens valid, d. h. das Token stammt vom Raspberry Pi, aber der Claim stimmt nicht mit dem des IOT Tangles überein. In Abbildung 17 ist auch das Identitätsdokument valid.

```

$ node verifyData.js
Valid signature. Decoded payload:
{
  subject: '048c828d-ad35-45aa-a05c-2a8cf9294561',
  devicePubKey: 'MIGfMA0GCsGqGSIB3DQEBAQUAA4GNADCBiQKBgQCTOdA8wN524+wb5gqaU5uiliT1S5L0nQDIA2SI5P7VgGsYah6zByB5jA7+muYCFUWHnWupU4DtEB6D59XgGRLfstxuyOIb7lw1stsHaQw1UmZ5d040lwQw2bMHvm1CwEEaOkVij+d6hsMhPTuFnbu1C3KQlGbCTEe50ClvN8DPQIDAQAB',
  issuerAddress: 'WWOTSUHSMXGELOPMDAHFSYXUGEHNIMGVUOSUHSISVVUZYPQAQMSOXCWTIEKKYBCNVCBNBS9EWE9IVLDNAW',
  issuer: 'https://publicRoadsAdministration.com/',
  data: { deviceOwner: 'Logistics GmbH', deviceModel: 'Raspberry Pi 3B+' },
  expirationDate: '01/01/2027'
}
Hashed claim: e1af979eb90cf94658c025b7ccd90f1a7e9dba1a962393b482e45f9f0f60aacc
Decoded message: e1af979eb90cf94658c025b7ccd90f1a7e9dba1a962393b482e45f9f0f60aacc
Hashes do match: Provided claim is valid.

```

Abbildung 17 Erfolgreiche Verifikation

Quelle: Eigene Darstellung

Update oder Deaktivierung der Identität

Das Aktualisieren der Identität ist möglich, indem ein neues Identitätsdokument mit den geänderten Attributen sowohl auf dem Gerät selber wie auch auf dem IOTA Tangle abgespeichert wird. Ein Löschen des Identitätsdokuments im eigentlichen Sinne ist nicht möglich. Das Identitätsdokument kann nur ungültig gemacht werden: Dies kann beispielsweise durch ein ungültiges Datum bei einem neu hochgeladenen Identitätsdokument erreicht werden. Wenn ausschliesslich ein neuer Hash auf den IOTA Tangle hochgeladen, das Gerät aber nicht mit dem passenden Identitätsdokument abgeglichen wird, wird das Identitätsdokument ebenfalls als ungültig erkannt.

Damit ein veraltetes Identitätsdokument nicht fälschlicherweise als gültig erkannt wird, muss der Verifier zwingend immer der neuste Root des Channels erhalten. In der Abbildung 18 ist das Beispiel gezeigt, wenn ein alter Root verwendet wird und zwei Identitätsdokumente vom IOTA Tangle abgerufen werden. Bei einem *singleFetch()* würde nur der Hash des veralteten Identitätsdokuments abgerufen.

```

0
{
  "message": "2e2bd876794b81c85345e177d7bba49ad5f25186e270207d135baba603cfae1a",
  "timestamp": "2019-11-1 22:31:35"
}

1
{
  "message": "e1af979eb90cf94658c025b7ccd90f1a7e9dba1a962393b482e45f9f0f60aacc",
  "timestamp": "2019-11-1 22:37:12"
}

```

Abbildung 18 Update sichtbar auf MAM Explorer

Quelle: mam-explorer.firebaseio.com, 2019

Sicherheitsaspekte

Bei der Durchführung des Experiments wurde nach Möglichkeiten gesucht, den Claim sowie auch den Private Key des Raspberry Pi's sicher aufzubewahren und kryptographische Algorithmen in einer geschützten Umgebung auszuführen. Dafür sollte ein Secure Element verwendet werden. Ein Secure Element ist eine Komponente eines Systems, die als Root of Trust fungiert. Ein Root of Trust ist für die Systemverifizierung, Software- und Daten-Integrität, Vertraulichkeit und Integritätsnachweis zu anderen Instanzen verantwortlich (van Tilborg & Jajodia, 2011, S. 45).

Auf dem Markt existieren einige wenige Lösungen von Secure Elementen, die speziell für Distributed Ledger-Anwendungen entwickelt wurden: Eine davon ist das Secure Element von Riddle & Code. Damit ist die Generierung und Verwaltung von Public und Private Keys und das Verwenden dieser Schlüsselpaare zum Signieren und Verschlüsseln für eine Blockchain möglich.

Ein Secure Element von Riddle & Code wurde mit einem Arduino getestet. Dabei hat sich herausgestellt, dass die generierten Schlüsselpaare nicht zur direkten Verwendung mit IOTA geeignet sind, da IOTA das spezielle Verschlüsselungsverfahren Winternitz One-Time-Signature braucht. Ein weiterer Punkt, weshalb von einer Verwendung in diesem Experiment abgesehen wurde, ist die mangelnde Dokumentation für das Produkt.

6.2.1 Ergebnisse Identitätsmanagement mit IOTA

Das Experiment «Identitätsmanagement mit IOTA» konnte erfolgreich umgesetzt werden. Die Funktionen Registrierung, Aktualisierung, Deaktivierung und Verifikation einer Identität wurden alle realisiert.

Beim Experiment wurde ein Identitätsdokument für einen Raspberry Pi über den IOTA-Tangle registriert, verwaltet und verifiziert. Für die Umsetzung wurde das in den Grundlagen beschriebene Claim Registry Model verwendet.

Eine erste Erkenntnis ist, dass die Erstellung des MAM-Channels für die Geräteidentität von einer vertrauenswürdigen Partei, z. B. des Unternehmens, welches die Geräte produziert, registriert werden muss. Würde sich ein Gerät selber ein Identitätsdokument ausstellen, könnte dies ausgenutzt werden und wäre deshalb wenig glaubwürdig. Die Erstellung des MAM-Channels muss durch die vertrauenswürdige Partei passieren, damit jede Transaktion die Signatur dieser Partei erhält.

In dem das signierte Identitätsdokument aber statt auf einer vom Claim Issuer verwalteten Datenbank auf dem Gerät selber gespeichert wird, kann der Gedanke von Self-Sovereign Identity umgesetzt werden. Für die Speicherung des Dokuments auf dem Gerät ist eine sichere Verbindung notwendig. Gerade auf einem IoT-Gerät ist eine Herausforderung das sichere Aufbewahren des Identitätsdokuments und des Private Keys des Geräts. Der Private Key wird bei der Authentifizierung des Geräts für das Signieren des JSON-Web Tokens verwendet. Ein Secure Element könnte für das

Aufbewahren des Identitätsdokuments und von Private Keys sowie dem Signieren mit gewöhnlichen Signatur Schemen wie z. B. ECDSA oder RSA verwendet werden.

Eine Herausforderung ist ein Update des Identitätsdokuments: Ein Update des Identitätsdokuments wie z. B. ein Besitzerwechsel oder eine Änderung des Ablaufdatums des Identitätsdokuments muss durch die Partei, die den MAM Channel erstellt hat, vorgenommen werden. Denkbar wäre auch einen Ansatz mit *Multi-Signatures*, bei dem mehrere Parteien einem Update zustimmen müssen. Findet nur ein Update und keine Deaktivierung der Identität statt, muss auch das gespeicherte Identitätsdokument auf dem Gerät aktualisiert werden.

Ein Vorteil und Herausforderung zugleich ist, dass ein MAM-Channel nach vorne verfolgt werden kann. Das bedeutet, dass eine Person im Besitz eines alten Roots sämtliche neueren Identitätsdokumente dazu betrachten kann. Zudem sollte stets garantiert werden, dass ein Claim-Verifier den neusten Root erhält: Ansonsten wird das ungültige Identitätsdokument eines Geräts unter Umständen als valid angesehen, obwohl es auf dem Tangle in einer Update-Transaktion als ungültig erklärt wurde.

6.3 Experiment Masked Authenticated Messaging

Im zweiten Experiment soll das Datenkommunikationsprotokoll MAM am Beispiel von Daten eines GPS-Moduls praktisch angewendet werden. Die Use Case Spezifikation kann im Anhang nachgelesen werden (S. 80). Die Forschungsfrage für dieses Experiment lautet:

Wie können Positionsdaten über den IOTA Tangle abgesichert und einer dritten Partei verfügbar gemacht werden?

Positionsdaten mit einem GNSS-Modul erhalten

Das GNSS (Global Navigation Satellite Systems) umfasst Satelliten-Systeme wie GPS (Global Positioning System), durch die eine geographische Position ermittelt, im Gelände navigiert oder die exakte Zeit bestimmt werden kann (PNT: Positioning, Navigation and Timing) (Zogg, 2014, S. 9).

«Durch die Satelliten-Navigation können Koordinaten, Höhe und Zeit bestimmt werden» (Zogg, 2014, S. 9). Das zugrunde liegende Prinzip auf dem Satelliten-Systeme aufgebaut sind, ist die Signallaufzeitmessung. Für mehr Informationen zum Funktionsprinzip von GNSS empfiehlt sich die Bedienungsanleitung «GPS und GNSS: Grundlagen der Ortung und Navigation mit Satelliten» (Zogg, 2014).

In einem ersten Versuch wurde das GPS-Antennenmodul PAM-7Q¹⁸ von u-blox mit einem Arduino und einem Raspberry Pi sowohl im Gebäude wie auch draussen getestet: Bei den Tests wurden zu

¹⁸ www.u-blox.com/de/product/pam-7q-module

wenig GPS-Signale empfangen, um Daten an den Raspberry Pi oder Arduino zu liefern. Beim zweiten verwendeten Positionierungsmodul handelt es sich um das GNSS-Antennenmodul SAM-M8Q¹⁹, das neben GPS/QZSS-Signalen auch Signale der Satelliten-Systeme Galileo und GLONASS empfängt. Im Freien lieferte das Modul zuverlässig Daten. Bei einem Erstgebrauch muss mit einer Setup-Zeit von bis zu 20 Minuten bis zum ersten Signal gerechnet werden.

Die GNSS-Daten werden mit dem NMEA-Protokoll (National Marine Electronics Association) über UART auf das Empfängergerät übertragen. Der Aufbau des NMEA-Protokolls ist grob im Dokument «Aufbau des NMEA-Protokolls» unter www.zogg-jm.ch beschrieben (Zogg, o. J.).

Hochladen der GNSS-Daten in einen MAM Channel auf dem IOTA Tangle

Für das Parsen der GNSS-Daten wurde GPS.js verwendet. Bei den abgefragten Daten handelt es sich, wie in Abbildung 19 ersichtlich, konkret um das Längengrad, Breitengrad, die Höhe (Altitude), die Geschwindigkeit und die Anzahl verarbeiteten Datenpunkte.

```
Serial port /dev/ttyS0 is opened and configured.
Messages will appear all 15 sec. Please wait...
{
  time: 2019-11-05T08:57:10.000Z,
  lat: 47. [REDACTED],
  lon: 8. [REDACTED],
  alt: 497,
  speed: 0.838956,
  processedLines: 180
}
{
  time: 2019-11-05T08:57:25.000Z,
  lat: 47. [REDACTED],
  lon: 8. [REDACTED],
  alt: 497.2,
  speed: 0.457444,
  processedLines: 360
}
{
  time: 2019-11-05T08:57:40.000Z,
  lat: 47. [REDACTED],
  lon: 8. [REDACTED],
  alt: 501.8,
  speed: 0.14816000000000001,
  processedLines: 540
}
```

Abbildung 19 Abgefragte GNSS-Daten

Quelle: Eigene Darstellung

In einem nächsten Schritt wird ein MAM-Channel auf IOTA erstellt. Dabei wird ein *MAM State Object* initialisiert, das den Zustand des Channels repräsentiert. Die Initialisierung kann mit oder ohne eigenen Seed passieren. Wird kein eigener Seed angegeben, wird ein zufällig generierter Seed für die Initialisierung verwendet. Das bedeutet, dass bei jedem Programmstart ein neuer, vom alten Seed unabhängiger, Channel erstellt wird, was aus Nachverfolgbarkeitsgründen fraglich ist.

¹⁹ www.u-blox.com/de/product/sam-m8q-module

```
//Initialise MAM state
let mamState = Mam.init(provider)
```

```
//Initialise MAM state
let mamState = Mam.init(provider,seed)
```

Abbildung 20 MAM-State Initialisierung mit und ohne eigenen Seed

Quelle: Eigene Darstellung

Wird ein eigener Seed verwendet und das State Objekt durch wiederholten Programmstart mehrmals neu initialisiert, kann es wie im Beispiel in Abbildung 21 zu einer Überschreibung von Nachrichten kommen: Das bedeutet, dass eine MAM Message einer bereits benutzten Adresse überschrieben wird, da bei der Neu-Initialisierung des State Objects der *Branch-Index* (Index der Adresse) wieder auf Null zurückgesetzt wird.

In der Abbildung 21 ist das Überschreiben einer alten MAM Message gezeigt. MAM Messages werden jeweils zeitlich geordnet (alt zu neu) abgerufen. Das heisst die älteste Message sollte den kleinsten Index im MAM Explorer haben. Die Abbildung 21 zeigt ein Beispiel, wo eine neuere Nachricht den kleinsten Index hat: Sie hat die alte Nachricht auf dem Index 0 überschrieben.



Abbildung 21 Überschreiben von Nachrichten sichtbar auf MAM Explorer

Quelle: mam-explorer.firebaseio.com, 2019

Für das Problem wurde in der Recherchephase keine Lösung gefunden. Da ein Seed wie ein normaler Private Key einmalig ist und bestimmte Adressen nur durch diesen Seed erzeugt werden können, müsste für eine gute Nachverfolgbarkeit eigentlich immer der gleiche Seed verwendet werden. Es wäre zwar denkbar, dass eine Partei mehrere Seeds besitzt; dies macht aber das Verifizieren von Signaturen komplizierter.

Gerade im IoT-Bereich muss damit gerechnet werden, dass es regelmässig zu Programmunterbrüchen kommt (z. B. durch Stromunterbruch). Während der Durchführung des Experiments wurde deshalb nach Lösungen gesucht, wie der MAM State gespeichert werden kann, so dass er auch nach einem Programmabsturz noch zur Verfügung steht. Da es sich beim MAM State Objekt um ein simples JSON Objekt handelt, konnte der MAM State fortwährend in einem JSON-File gespeichert werden.

6.3.1 Ergebnisse Masked Authenticated Messaging

Im zweiten Experiment wurden die Daten eines GNSS-Moduls in einem restricted MAM Channel auf IOTA gesichert und dann über eine Website abgerufen.

Das junge Protokoll MAM ist eher spärlich dokumentiert und die API-Funktionen für das Abrufen von Nachrichten sind mit einigen Unklarheiten noch potenzielle Fehlerquellen. Jedoch ist die Erstellung eines MAM Channels unkompliziert und das grundlegende Prinzip in der «IOTA Developer Documentation» gut erklärt. Durch die Popularität von MAM wächst die Anzahl von Code-Beispielen zudem rasch.

Ein Problem, welches während dem Ausführen des Experiments entdeckt wurde, ist die Möglichkeit, alte Nachrichten in einem MAM-Channel zu überschreiben. Diese Möglichkeit sollte verhindert werden, da sie die Nachverfolgbarkeit des Distributed Ledgers untergräbt. Konkret muss verhindert werden, dass das Gerät die Möglichkeit hat, eine bereits genutzte Adresse für die Veröffentlichung einer MAM Transaktion noch einmal zu nutzen. Dies ist auch ein Sicherheitsproblem, da eine Adresse nur einmal zum Signieren verwendet werden sollte.

Bei einem Neustart des Programms wird das MAM State Object üblicherweise mit *MAM.init(provider)* oder *MAM.init(provider,seed)* neu initiiert. Wenn ein Seed für die Initialisierung verwendet wird, führt dies genau zum oben beschriebenen Problem. Deshalb wurde das State Objekt bei jeder neuen Transaktion in einer Datei gespeichert und bei einem Neustart direkt aus dieser Datei gelesen. Dadurch wird der Zustand des Counts beibehalten.

Wie im ersten Experiment, gibt es auch in diesem Experiment Sicherheitsaspekte, die nicht berücksichtigt werden konnten. Der Raspberry Pi und das GNSS-Modul sind ein leicht angreifbares Ziel. Das ist insofern problematisch, weil bei fehlender Datenintegrität die Unveränderlichkeit eines Distributed Ledgers keinen Sinn mehr macht, weil das Vertrauen in die Daten selbst fehlt.

Aspekte, die in diesem Experiment nicht berücksichtigt werden konnten, in einer Produktionsumgebung aber eine wichtige Rolle spielen, sind das Management von Public Keys, Side Keys bzw. Channel-Zugriff und Authentifizierung der Observer.

6.4 Funktionales Testen

In diesem Kapitel wird die Einhaltung von Anforderungen an den finalen Prototyp überprüft. Aufgrund des frühen Stadiums des Prototyps werden Use Cases manuell durchgespielt. Da nur der erste Use Case, die Geräteauthentifizierung und anschließende Registrierung einer Liefereinheit durch den Sender, im Detail umgesetzt wurde, werden nur die Anforderungen aus diesem Use Case getestet. In der Tabelle 5 sind die wichtigsten Anforderungen für diesen Use Case aufgeführt.

Tabelle 5 Anforderungen basierend auf dem ersten Systemablauf

#	Anforderungen
1	Das Trackinggerät muss auf Anfrage fähig sein, mittels eines Credentials seine Identität eigenständig auszuweisen.
2	Das Trackingsystem muss einem Verifier die Möglichkeit bieten, die Identität eines Trackinggeräts ohne Hilfe einer TTP über den IOTA Tangle verifizieren zu können.
3	Das Trackingsystem muss einem Produktionsunternehmen die Möglichkeit bieten, ein mit IOTA verifizierbarer Credential für eine Liefereinheit zu erstellen.
4	Das Trackingsystem muss einem Produktionsunternehmen die Möglichkeit bieten, ein Tracking von Positionsdaten für eine Liefereinheit zu starten .
5	Das Trackingsystem muss einem Produktionsunternehmen die Möglichkeit bieten, ein Tracking von Positionsdaten für eine Liefereinheit zu stoppen .
6	Die Stromversorgung für das Trackinggerät soll über die Dauer einer Lieferung (definiert 9h) sichergestellt sein.
7	Das Trackingsystem muss berechtigten Personen ermöglichen, Transaktionen zu Trackingdaten direkt auf dem IOTA Tangle nachzusehen.
8	Das Trackingsystem soll berechtigten Personen die Möglichkeit geben, Trackingdaten einer Liefereinheit abgesichert über den IOTA Tangle abzurufen.

6.4.1 Ergebnisse Funktionales Testing

In diesem Kapitel werden die Testresultate aufgeführt. Die Vorbedingungen für die Tests werden, falls vorhanden, direkt im Text genannt.

Ergebnisse Test Anforderung #1 – Ausweisen der Identität des Trackinggeräts

Bei diesem Test wurde ein Credential in Form eines JSON Web Tokens über die Verbindung von remote.it abgerufen. Voraussetzung dafür ist eine Internetverbindung des Raspberry Pi's. Die REST API wird über den NodeJS-Prozessmanager PM2 automatisch gestartet.

Die Tests wurden mit Postman, einer Kollaborationsplattform für die Entwicklung von APIs, durchgeführt. In der Abbildung 24 ist ein Beispiel einer API-Abfrage gezeigt.

Die Korrektheit des JSON Web Tokens wird im Rahmen der Anforderung #2 getestet. Eine manuelle Verifikation des Tokens ist auf <https://jwt.io/> möglich. Alle Testiterationen zeigten eine erfolgreiche Abfrage der API (siehe Anhang für konkrete Resultate).

Step 2: Register packaging unit

Commodity group e.g. cameras, laptops

Series number

Value of item

in

Number of items

Owner

Delivery date

Producer Device CONNECTED

Congrats you made an order!

Order

Subject: dd39f1a9-876b-47f6-887b-c73f337a6ea8

Commodity Group: Cameras

Series Number: 151071

Number of Items: 18

Price of Item: 399.95 USD

Owner: Sony

Tracking Root:
GNOELHLIKVMY9VEOGAFXBVCUXFTUJWY

Root Credential Packaging Unit:
KUVQAPFVUZ9FUVLGVHWHVIVPOHGLZRYM

Check on tangle: <https://mam-explorer.firebaseio.com/?provider=https%3A%2F%2Fnodes.devnet.iota.org&mode=ractrina4&>

Abbildung 26 Erstellung einer Liefereinheit

Dabei wurde festgestellt, dass ein neues Credential jeweils das alte Credential überschreibt, da der MAM State nicht gespeichert wird. Während dies im Experiment «Masked Authenticated Messaging» nicht erwünscht war, kann dies hier von Vorteil sein, weil so auch Personen mit altem Root das neuere Identitätsdokument abrufen. Allerdings ist die mehrmalige Verwendung einer Adresse zum Signieren einer Nachricht verboten.

Ergebnisse Test Anforderung #4 und #5 – Starten und Stoppen eines Trackings

Das Starten und Stoppen eines Trackings wurden über manuelle API-Aufrufe getestet. Das Stoppen eines Trackings funktioniert problemlos. Die Übergabe des Roots bei einem Start des Trackings dauert hingegen zu lange. Beim Start des Trackings muss auch berücksichtigt werden, dass das IoT-Gerät GNSS-Empfang haben sollte, um Daten auf dem Tangle zu veröffentlichen. Ist diese Voraussetzung nicht gegeben, sollte keine Transaktion gemacht und folglich kein Root zurückgegeben werden.

Ergebnisse Test Anforderung #6 – Sichere Stromversorgung über eine Lieferstrecke

Der Akku muss die Stromversorgung während einer Lieferung sicherstellen können. Als zeitliche Referenz wird hier die max. erlaubte Fahrzeit eines LKW-Fahrers von 9 Stunden²² genommen. Während dieser Zeit sollte ein ununterbrochenes Tracking von Liefereinheiten möglich sein. Danach müsste der Akku aufgeladen werden. Bei einem Akku von 5000 mAh und einem pessimistisch geschätzten Verbrauch von 0.5A würde die Laufzeit theoretisch 10 Stunden betragen. Bei Tests kam die Akkulaufzeit auf ca. 6 Stunden.

²² <https://www.dasag.ch/arv-1-chauffeurverordnung/>

Ergebnisse Test Anforderung #8 – Trackingdaten über den IOTA Tangle abrufen

Für das Testen dieser Anforderung wurden Trackingdaten über IOTA veröffentlicht und dann über eine Website abgerufen. Voraussetzung dafür sind der Besitz eines korrekten Roots und des korrekten Side Keys. Die Abbildung 27 zeigt das erfolgreiche Abrufen der Positionsdaten.

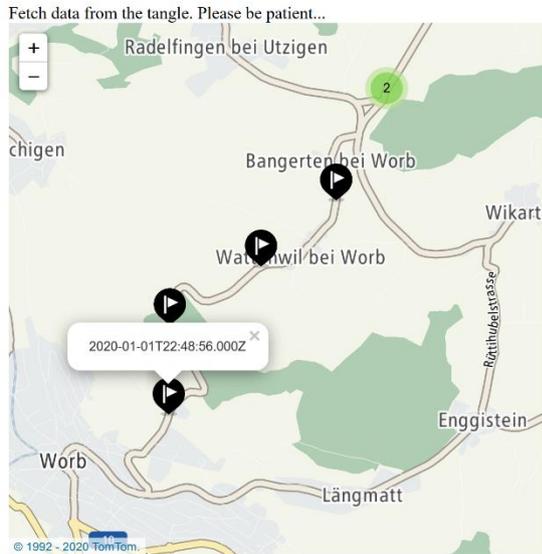


Abbildung 27 Trackingdaten abrufen

7 Zusammenfassung der Ergebnisse

Dieses Kapitel beschreibt die wichtigsten Ergebnisse dieser Arbeit. Detaillierte Ergebnisse zu einer einzelnen Methodenanwendung sind jeweils am Ende des jeweiligen Kapitels aufgeführt.

7.1 Erkenntnisse Literaturrecherche

In der Literaturrecherche wurde das Thema IDoT, IOTA und DLT-basierte Geschäftsmodelle in der Supply Chain betrachtet. Aus den Erkenntnissen der einzelnen Themen ergibt sich ein grösseres Bild des Potenzials von IDoT mit IOTA in der Supply Chain:

Eine der Hauptherausforderungen im Supply Chain Management sind Kommunikations- und Informationsprobleme zwischen verschiedenen Stakeholdern. Externe Entwicklungen wie die Globalisierung und erhöhte Anforderungen von Kunden bezüglich Umweltfreundlichkeit, Ethik und Produktqualität bei gleichem Preis sowie verschärfte Gesetze und kurz- und langfristige Marktveränderungen fordern das Supply Chain Management zusätzlich heraus.

Die Effizienz (hohe Qualität in kurzer Zeit), die Nachverfolgbarkeit und Transparenz sowie die Flexibilität der Supply Chain müssen gesteigert werden, um den neuen Anforderungen zu genügen und Kosten und Risiken im Griff zu behalten.

Ein Supply Chain-übergreifendes Informationssystem kann zu einer besseren Nachverfolgbarkeit von Produkten und Services, einer effizienteren Kollaboration der Beteiligten und einer Optimierung der Abläufe in der Supply Chain sowie einer schnellen und automatisierten Antwort auf Veränderungen führen. Für eine erhöhte Glaubwürdigkeit und das dezentrale Management eines Informationssystems über die ganze Supply Chain ist ein Distributed Ledger ideal.

Ein Identitätsmanagementsystem in der Supply Chain kann dazu genutzt werden, einem konkreten Objekt wie z. B. einem Produkt oder einem Sensor für die Messung von Lieferdaten eine eindeutige Identität zuzuordnen und so das Tracking und Tracing des Objekts und objektbezogenen Daten zu ermöglichen. Die Objektidentität und objektbezogenen Daten können dabei zur Absicherung auf dem Distributed Ledger hinterlegt werden. Abstrakte Objekte wie z. B. Supplier-Verträge, Risikoabsicherungen und Aufträge können ebenfalls über einen Distributed Ledger verwaltet werden.

Die Anforderungen an ein solches System wie geeignete Identifier, Datenschutz, Datenspeicherung, sowie Informationssicherheit, Authentifizierung und Zugriffskontrolle können mit Self-Sovereign Identity und Dezentralem Identitätsmanagement erreicht werden.

Die Wahl des verwendeten Distributed Ledgers ist abhängig von den Anforderungen des spezifischen Anwendungsgebiets. Gerade im Internet of Things spielt die Höhe des Datendurchsatzes und der Transaktionskosten eine grosse Rolle. Diesbezüglich hat IOTA Vorteile gegenüber anderen Distributed Ledgern, da die Architektur des Tangles (DAG) als sehr skalierbar gilt und für eine

Transaktion keine Transaktionsgebühren anfallen. Das IOTA-Kommunikationsprotokoll MAM ermöglicht die Verifizierung von Zero-Value-Transaktionen und somit die beschränkte Veröffentlichung von z. B. IoT-Daten trotz der Verwendung eines public, permissionless Ledgers.

7.2 Ergebnisse Überprüfung in unternehmerischer Hinsicht

In diesem Teil der Arbeit werden die Ergebnisse der Analyse «Do you Need a Blockchain?» (Wüst & Gervais, 2018) und der Online-Umfrage präsentiert.

Für den ursprünglich angedachten Anwendungsfall eines Trackings von Fahrzeugdaten ist ein Distributed Ledger nicht notwendig. Im beschriebenen Anwendungsfall würden alle IoT-Geräte, die Daten über den Distributed Ledger absichern, demselben Logistikunternehmen gehören.

Eine Manipulation der Geräte wäre somit möglich und würde die aufgezeichneten Daten nutzlos machen. Die untenstehende Tabelle fasst die Antworten zur Analyse noch einmal zusammen. Wegen der Antwort auf Frage 2 und 3 ist ein Distributed Ledger nicht sinnvoll.

Tabelle 6 Zusammenfassung Antworten zur Analyse "Do you Need a Blockchain?"

#	Fragen	Antwort	Bedeutung der Antwort
1	Müssen Datenzustände gespeichert werden?	<i>ja</i>	DL macht Sinn
2	Gibt es mehrere Parteien mit Schreibzugriff?	<i>nein</i>	Kein DL nötig
3	Ist eine TTP ständig online verfügbar?	<i>ja</i>	Kein DL nötig
4	Sind alle schreibenden Parteien bekannt?	<i>ja</i>	Permissioned Blockchain, restricted MAM bei IOTA
5	Wird allen schreibenden Parteien vertraut?	<i>nein</i>	DL macht Sinn
6	Ist öffentliche Nachverfolgbarkeit verlangt?	<i>nein</i>	Permissioned Blockchain, restricted MAM bei IOTA

Die Antworten aus der Online-Umfrage stimmen mit den Ergebnissen aus der Literaturrecherche überein: Eine Herausforderung für die befragten Parteien ist unter anderem die Komplexität bei der Koordination und Kommunikation innerhalb der Supply Chain. Ebenfalls problematisch sind nicht-standardisierte Prozesse und der hohe administrative Aufwand.

Interessant für die Unternehmen ist nebst dem Tracking von Kilometerdaten das Tracking von Grössen, die Unregelmässigkeiten anzeigen (z. B. «Wann und wo Ladeklappe geöffnet wurde» und Gewicht der Ladung) und Grössen, aufgrund derer eine Optimierung des Lieferprozesses angestrebt werden kann (z. B. Standzeit beim Kunden).

Die untenstehende Graphik fasst die evaluierten Anforderungen an ein Trackingsystem noch einmal zusammen. Im Pfeil rechts sind die Massnahmen im abgeänderten Anwendungsfall beschrieben, um diese Anforderungen zu erreichen.

Tabelle 7 Anforderungen an ein Trackingsystem

Anforderung	Massnahme
Unabhängigkeit der schreibenden Parteien	- Trackinggeräte gehören verschiedenen Parteien
Absehbarer finanzieller Nutzen für alle direkt beteiligten Stakeholder	- Optimierung der Lieferprozesse - Beweis von kostenintensiven Lieferverzögerungen
Berücksichtigung des Datenschutzes beteiligter Personen	- Anstelle von Fahrzeugen werden Liefereinheiten getrackt
Optimierung der Prozesse	- Schnelle Überprüfbarkeit für Behörden - Bessere Planbarkeit der Lieferankunft - Automatisierte Frachtschein- und Auftragerstellung
Nachverfolgbarkeit von Unregelmässigkeiten	- Vergleich von Positionsdaten mehrerer Liefereinheiten in der gleichen Fracht möglich - Nachverfolgbarkeit von Lieferverzögerungen möglich

7.3 Ergebnisse Technische Umsetzung

In diesem Kapitel werden die Erkenntnisse aus den Experimenten und der Umsetzung des finalen Prototyps beschrieben. Nachfolgend werden erst die Forschungsfragen der einzelnen Experimente beantwortet und diskutiert. Danach wird die Tauglichkeit des vorgestellten Lösungssystems diskutiert.

Wie kann ein Identitätsdokument mit IOTA self-sovereign verwaltet werden?

Durch die Umsetzung des Experiments *Identitätsmanagement mit IOTA* konnte diese Frage beantwortet werden. Die Funktionen Registrierung, Aktualisierung, Deaktivierung und Verifikation einer Identität wurden mit dem Claim Registry-Ansatz mithilfe von MAM-Channels realisiert. Bei der Umsetzung des Experiments sind einige Herausforderungen aufgetaucht, die bei der Lösungsumsetzung beachtet werden müssen:

Das sichere Übertragen und Aufbewahrung eines Identitätsdokuments auf einem IoT-Gerät ist ein ungelöstes Problem. Dies hat weniger mit der Technologie IOTA als vielmehr mit Claim-based IDoT allgemein zu tun.

Eine weitere Herausforderung ist das Management des Lesezugriffs auf einen MAM Channel: Da ein MAM Channel nach vorne verfolgt werden kann, ist es möglich mit einem alten Root sämtliche neuere Identitätsdokumente zu betrachten. Dem kann nur durch die Änderung des Side Keys in einem restricted Channel entgegengewirkt werden.

Identitätsdokumente können mit dem dazugehörigen Root selbst dann noch aufgerufen werden, wenn es bereits neuere Versionen des Identitätsdokuments auf dem IOTA Tangle gibt. Was ebenfalls verhindert werden sollte, ist die erfolgreiche Verifizierung eines veralteten Identitätsdokuments durch das Abrufen eines veralteten Roots. Für diese beiden Probleme gibt es in IOTA keine automatisierte

Lösung. Der Systementwickler muss sich selber darum kümmern, dass ein sorgfältiges Root-Management den Missbrauch von alten Identitätsdokumenten verhindert.

Wie können Positionsdaten über den IOTA Tangle abgesichert und einer dritten Partei verfügbar gemacht werden?

Das Abspeichern von GNSS-Daten auf dem Tangle konnte mit restricted MAM-Channel umgesetzt werden. Ein gravierendes Problem, welches vom derzeitigen MAM-Protokoll jedoch nicht gelöst wird, ist die Möglichkeit, alte Nachrichten in einem MAM-Channel zu überschreiben.

Dies untergräbt die Nachverfolgbarkeit im Ledger und macht deshalb eine Absicherung der Daten unnötig. Ein Distributed Ledger sollte so gestaltet sein, dass auch bei Fehlern der schreibenden Parteien, die Nachverfolgbarkeit sichergestellt ist.

Distributed Ledger Technologien schaffen das Vertrauen, welches vorher Trusted Third Parties gegeben haben. Dies heisst aber auch, dass die Anwendungsarchitektur so definiert werden muss, dass das Vertrauen bestmöglich garantiert werden kann. Ein Claim Verifier muss die Möglichkeit haben, die Verifikation der Geräteidentität mit dem IOTA Tangle selbstständig durchzuführen. Findet die Verifikation über einen Server und nicht direkt im Browser statt, ist ein Teil dieses Vertrauens schon wieder von einer weiteren Partei abhängig.

Eine generelle Erkenntnis ist, dass die Manipulationsfähigkeit des ganzen Systems kritisch betrachtet werden muss. Kann kein Minimum an Datenintegrität garantiert werden, macht auch die Unveränderlichkeit eines Distributed Ledgers keinen Sinn, weil das Vertrauen in die Daten selbst fehlt. Crypto-Chips helfen dabei IoT-Geräte sicherer zu machen und so das Vertrauen in IoT-Daten zu steigern. Lösungen wie Oracles adressieren dieses Problem auf eine andere Art. Die Recherchephase für die beiden Experimente hat jedoch gezeigt, dass es im Bereich End-to-End-Security für Distributed Ledger Technologie Anwendungen noch viel Potenzial gibt.

7.3.1 Tauglichkeit der Systemlösung

Das angedachte Lösungskonzept für den entwickelten Anwendungsfall in dieser Arbeit beschreibt detaillierte Lösungen zu einzelnen Teilprozessen im Anwendungsfall. Dabei werden nicht nur Kern- sondern auch Nebenprozesse wie das Side Key- und Root-Management für den Lesezugriff auf den Distributed Ledger berücksichtigt. Die beschriebene Architektur des Prototyps ist jedoch für eine Produktionsumgebung nicht geeignet:

Die Sicherheit des Systems ist nicht gewährleistet:

- Credentials, Private Keys und Seeds werden in einer unsicheren Umgebung aufbewahrt.
- Kryptographische Operationen werden in einer unsicheren Umgebung ausgeführt. Zum Beispiel wird die Erstellung eines Credentials für eine Liefereinheit im Browser des Clients gemacht.

- Die Datenintegrität kann nicht gewährleistet werden.

Die Verwendung eines Raspberry Pi's für eine einzelne Liefereinheit ist ineffizient:

- Die Lösung ist zu teuer.
- Die Stromversorgung des Geräts kann nicht über 9h sichergestellt werden.

Während MAM-Channels rein architektonisch äusserst geeignet für den Anwendungsfall dieser sind, da sie abgegrenzte, private Gefässe für die Verwaltung von einzelnen Identitäten und Trackingdaten bieten, wird das junge Kommunikationsprotokoll noch nicht als reif für Implementierungen abseits von Pionierprojekten empfunden.

8 Schlussbetrachtung und Ausblick

Das folgende Kapitel reflektiert die verwendeten Methoden und die Ergebnisse dieser Arbeit. Im Kapitel 8.2 und 8.3 werden Empfehlungen gemacht und dann Themen mit weiteren Forschungsbedarf vorgeschlagen.

8.1 Reflexion

Das Ziel dieser Forschungsarbeit war die Entwicklung eines Proof of Concepts für ein Trackingsystem in der Supply Chain. Durch die Betrachtung eines spezifischen Anwendungsfalls sollten technische und unternehmerische Chancen evaluiert werden.

Durch den Vergleich von Herausforderungen in der Supply Chain und vorhandenen Lösungen konnte ein unternehmerisches Potenzial von DLT und IDoT in der Supply Chain entdeckt werden, welches noch nicht in der Literatur beschrieben gefunden wurde. Dabei handelt es sich um die Nutzung von DLT für eine höhere Effizienz- und Flexibilität der Supply Chain.

Aufgrund der kleinen Antwortzahl in der Online-Umfrage konnte dieses Potenzial jedoch nicht verifiziert werden. Die theoretische Prognose müsste in intensiver Zusammenarbeit mit Stakeholdern überprüft werden. Durch den fehlenden Industriepartner in dieser Forschungsarbeit war eine derartige Zusammenarbeit nicht möglich.

Die gewählte Vorgehensweise war für den gegebenen Kontext nur teilweise geeignet: Aufgrund des frühen Ideenstadiums wurde viel Zeit benötigt, einen soliden Anwendungsfall herzuleiten. Dies ging auf Kosten der technischen Umsetzung: Mit weiteren Experimenten hätte ein direkter Bezug zu den Ergebnissen der bisherigen Arbeit erreicht und das Lösungskonzept in seiner Ganzheit überprüft werden können. Denkbar wäre z. B. ein Experiment zur Thematik «Erkennen von Unregelmässigkeiten» oder «Überprüfen der Ankunftszeit» gewesen.

Nichtsdestotrotz konnten durch die durchgeführten Experimente, technische Risiken evaluiert werden. Der entwickelte Prototyp zeigt Schwierigkeiten bei der Umsetzung einer Lösung auf, kann aufgrund seiner Maturität jedoch nicht für die umfassende Bestimmung von Anforderungen verwendet werden.

Diese Arbeit bietet einen ersten Überblick zu einem Schnittstellenthema, dass in den letzten Jahren massiv an Bedeutung zugenommen hat. Dieser Überblick kann als Anstoss für weitere Forschungsprojekte mit direktem Kontakt zur Industrie genutzt werden.

8.2 Empfehlungen

Die nachfolgenden Empfehlungen richten sich an Personen und/oder Organisationen, die sich für die Umsetzung einer DLT-basierten Lösung mit IDoT in der Supply Chain interessieren.

Fokus der Lösung auf Effizienz und Flexibilität der Supply Chain

Wie bereits in den Ergebnissen erwähnt, lohnt sich der Fokus auf Effizienz und Flexibilität einer Supply Chain, da dadurch direkte Kosteneinsparungen und Minimierung von Risiken für alle Supply Chain Teilnehmer erreicht werden können. Konkret kann dies erreicht werden, in dem SC-Teilnehmer vermehrt digital interagieren. Mittels digitaler Identitäten können Personen und Dinge dabei eindeutig identifiziert werden. Ein Distributed Ledger sorgt dafür, dass die digitalen Interaktionen nachverfolgbar und bindend sind. Informations- oder Identitätsmanagementsysteme, die diese Funktionen anbieten, haben einen echten Mehrwert für alle Beteiligten der Supply Chain.

Nachverfolgen von Unregelmässigkeiten und Beweisgrössen

Die Analyse «Do you Need a Blockchain?» zeigt, dass ein Distributed Ledger nicht in jedem Anwendungsfall Sinn macht. Vereinfacht macht die Verwendung eines Distributed Ledgers nur dort Sinn, wo mehrere Parteien ohne externe Kontrolle in einem System interagieren wollen und Datenzustände zu Beweis Zwecken im Nachhinein noch verfügbar sein müssen. In der Online-Umfrage gaben die teilnehmenden Unternehmen Beispiele für Daten, die Unregelmässigkeiten und Optimierungspotenzial im Lieferprozess aufzeigen: «Wann und wo die Ladeklappe geöffnet wurde», das Gewicht der Ladung, die Standzeit beim Kunden oder die voraussichtliche Ankunftszeit. Diese Grössen sollten für ein Tracking in Betracht gezogen werden.

Vertrauen in ein System als Ganzes schaffen

Ein identifiziertes Problem für das Internet of Things ist die Schwierigkeit, digitale Daten direkt mit einem realen Zustand zu verknüpfen. Ein Distributed Ledger kann Datenzustände absichern, jedoch kann damit nicht sichergestellt werden, dass die Daten integer sind und die Realität zuverlässig abbilden. In der Fallstudie «DLT-basierte Lösungen in der Supply Chain» wurde ein Beispiel gefunden, wie dieses Problem erfolgreich gelöst wurde: Bei einem Weinkorken wird ein RFID-Tag so angebracht, dass eine Manipulation des Tags direkt registriert wird und das digitale Zertifikat des Weins unbrauchbar macht. Solche Absicherungen auf Feldebene sind ein hilfreiches Mittel gegen Manipulationsversuche vor der Aufzeichnung auf einem Distributed Ledger.

Eine wichtige Thematik bei der Verwendung mit Distributed Ledgern ist das Management des Lese- und Schreibzugriffs. Die Komplexität dessen, wurde am Beispiel des Managements von Roots und Side Keys beim Kommunikationsprotokoll MAM von IOTA klar. Die Mitberücksichtigung dieser Nebenprozesse ist für die Informationssicherheit und den Datenschutz von zentraler Bedeutung.

Eine Distributed Ledger-Lösung, die das Vertrauen in Daten sicherstellen soll, sollte so gestaltet werden, dass sie auch für Leute, die wenig technisches Vorwissen haben, nachvollziehbar ist. Bei der

Arbeit mit IOTA wurde das Problem erkannt, dass das manuelle Überprüfen der Signatur einer Transaktion nicht einfach ist, da eine Partei nicht mit einer einzelnen Adresse auf dem Tangle verbunden werden kann²³. Der Verifikationsvorgang z. B. beim Überprüfen eines Identity Credentials sollte zudem so unabhängig von Dritten wie möglich gestaltet werden.

Zuletzt muss gerade im Internet of Things die Informationssicherheit über das ganze System kritisch hinterfragt werden. Für IoT-Geräte wurden in der Recherchephase keine umfassenden Lösungen gefunden, die eine sichere Interaktion mit einem Distributed Ledger garantieren. Das sichere Aufbewahren von Seeds, Private Keys und Credentials und die Durchführung von kryptographischen Algorithmen auf einfachen IoT-Geräten ist ein Thema, welches weiterer Forschung bedarf.

8.3 Zukünftiger Forschungsbedarf

Wie bereits in der Reflexion erwähnt, kann diese Arbeit als Anstoss für weitere Forschungsarbeiten dienen.

Weiter geforscht werden kann zum Beispiel im Zusammenhang mit IOTA: Die Weiterentwicklung der IOTA-Technologie wird von der IOTA Foundation und der IOTA Community sehr aktiv vorangetrieben. Durch die Weiterentwicklung von IOTA können vermutlich einige der beschriebenen Herausforderungen in dieser Arbeit gelöst werden. Zum Beispiel wird ab 2020 daran gearbeitet, zusätzliche Signaturschemen anzubieten. Das Kommunikationsprotokoll MAM wird ebenfalls komplett überarbeitet. Dabei sollen bestehende Probleme am jetzigen Protokoll gelöst und einige wichtige Funktionen dazugefügt werden. Die relevanteste Neuigkeit für diese Arbeit ist die Entwicklung eines offiziellen «Unified Identity Protocol's». Das Unified Identity Protocol hat einen Fokus auf IDoT und soll ein Identitätsmanagement mit IOTA durch die Verwendung von Verifiable Claims und DIDs ermöglichen (Millenaar & Yarger, 2019). Die Entwicklung einer Systemlösung auf Basis des Unified Identity Protocols wäre äusserst interessant.

Auch die Betrachtung von alternativen Distributed Ledgern wäre wertvoll. Smart Contracts sind in IOTA noch in einem frühen Entwicklungsstadium. Mit einem anderen Distributed Ledger könnte die Verwendung von Smart Contracts für ein Trackingsystem vermutlich besser untersucht werden.

Der in dieser Arbeit beschriebene Anwendungsfall sollte in direkter Zusammenarbeit mit einem Industriepartner weiterentwickelt werden. Empfehlenswert ist die Diskussion des Anwendungsfalls und des dazugehörigen Lösungskonzepts mit Stakeholdern und die anschliessende Überarbeitung der Anforderungen. Darauf basierend könnte ein erstes Minimum Viable Product (MVP) erstellt werden, mit dem mehrere Feldtests in einer realen Supply Chain-Umgebung durchgeführt werden.

²³ Wie in den Grundlagen erwähnt, kann eine Partei aufgrund des verwendeten Signatur Schemas Winternitz One Time Signature bis zu 9^{57} verschiedene Adressen haben.

Literaturverzeichnis

- Allen, C., Brock, A., Buterin, V., Callas, J., Dorje, D., Lundkvist, C. et al. (Web Of Trust, Hrsg.). (2015). *Decentralized Public Key Infrastructure. A White Paper from Rebooting the Web of Trust*. Verfügbar unter <https://github.com/WebOfTrustInfo/rwot1-sf/blob/master/final-documents/dpki.pdf>
- Alpár, G., Hoepman, J.-H. & Siljee, J. (Februar 2011). *The Identity Crisis. Security, Privacy and Usability Issues in Identity Management*. Verfügbar unter <http://arxiv.org/pdf/1101.0427v1>
- Arai, K., Bhatia, R. & Kapoor, S. (2020). *Proceedings of the Future Technologies Conference (FTC) 2019* (Bd. 1070). Cham: Springer International Publishing.
- Bertino, E. & Takahashi, K. (2011). *Identity management. Concepts, technologies, and systems* (Information security and privacy series). Boston: Artech House.
- Bundesamt für Strassen. (2019). *Einführung des intelligenten Fahrtschreibers*, Bundesamt für Strassen. Zugriff am 24.10.2019. Verfügbar unter <https://www.astra.admin.ch/astra/de/home/fachleute/fahrzeuge/digitaler-fahrtschreiber/einfuehrung-intelligenter-fahrtschreiber.html>
- Cavus, M. (2016, 30. Mai). *Die Blockchain Evolution*. Verfügbar unter <https://www.digitale-exzellenz.de/die-blockchain-evolution/>
- Chen, J., Liu, Y. & Chai, Y. (2015). An Identity Management Framework for Internet of Things. In *2015 IEEE 12th International Conference on e-Business Engineering* (S. 360-364). IEEE.
- Emporias Management Consulting GmbH & Co. KG. (2017). *Supply Chain Management in Industrieunternehmen*, Emporias Management Consulting GmbH & Co. KG. Verfügbar unter <https://www.emporias.de/wp-content/uploads/2017/11/EMPORIAS-Auszug-Studie-Supply-Chain-Management.pdf>
- Friese, I., Heuer, J. & Kong, N. (2014). Challenges from the Identities of Things. Introduction of the Identities of Things discussion group within Kantara initiative. In *2014 IEEE World Forum on Internet of Things (WF-IoT)* (S. 1-4). IEEE.
- Gartner. (02.2017). *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*, Gartner. Verfügbar unter <https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016>
- Groenfeldt, T. (März 2017). *IBM And Maersk Apply Blockchain To Container Shipping*, Forbes. Verfügbar unter <https://www.forbes.com/sites/tomgroenfeldt/2017/03/05/ibm-and-maersk-apply-blockchain-to-container-shipping/#553da743f05e>
- Handy, P. (2017, 04. November). *Introducing Masked Authenticated Messaging*, IOTA Foundation. Verfügbar unter <https://blog.iota.org/introducing-masked-authenticated-messaging-e55c1822d50e>

- IOTA Foundation. (2019a). *IOTA. Developer Documentation*, IOTA Foundation. Verfügbar unter <https://docs.iota.org/>
- IOTA Foundation. (2019b). *The Coordicide*, IOTA Foundation. Zugriff am 09.11.2019. Verfügbar unter https://files.iota.org/papers/Coordicide_WP.pdf
- (2019). *IOTA Einsteiger Guide*. Verfügbar unter <https://iota-einsteiger-guide.de>
- ITU-T Study Group 13. ITU-T Rec. Y.2720 (01/2009) NGN identity management framework.
- Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, 39, 80-89.
- Medium. (02.2018). *MAM Eloquently Explained*, Medium. Verfügbar unter <https://medium.com/coinmonks/iota-mam-eloquently-explained-d7505863b413>
- Millenaar, J. F. & Yarger, M. (2019). *The Case for a Unified Identity. Our Vision for a Unified Identity Protocol on the Tangle for Things, Organizations, and Individuals*, IOTA Foundation. Verfügbar unter https://files.iota.org/comms/IOTA_The_Case_for_a_Unified_Identity.pdf
- Mitschele, A. (2019). *Smart Contract*, Springer Gabler. Verfügbar unter <https://wirtschaftslexikon.gabler.de/definition/smart-contract-54213/version-372222>
- Mühle, A., Grüner, A., Gayvoronskaya, T. & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, 30, 80-86.
- Pohlmann, N. (2019). *Cyber-Sicherheit*. Wiesbaden: Springer Fachmedien Wiesbaden.
- Pope, S. (2019, 16. Oktober). *Blockchain To Be A Gamechanger For Global Shipping*, Forbes. Verfügbar unter <https://www.forbes.com/sites/stephenpope/2019/10/16/blockchain-to-be-a-gamechanger-for-global-shipping/>
- Popov, S. (2019, 03. April). *The tangle*, Jinn Labs. Zugriff am 12.10.2019. Verfügbar unter http://www.tangleblog.com/wp-content/uploads/2016/11/IOTA_Whitepaper.pdf
- Provenance. *Case Studies*, Provenance. Zugriff am 14.11.2019. Verfügbar unter www.provenance.org
- Rayes, A. & Salam, S. (2019). *Internet of Things From Hype to Reality*. Cham: Springer International Publishing.
- Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R. & Sabadello, M. (2019). *Decentralized Identifiers (DIDs) v1.0. Core Data Model and Syntaxes*. Verfügbar unter <https://www.w3.org/TR/did-core/>
- Rowe, G., Myracle, J. & Simmons, D. (2018). *Identity of Things (IDoT)*, TechVision Research. Verfügbar unter <https://techvisionresearch.com/>
- Schmidt, A. U., Russello, G., Krontiris, I. & Lian, S. (2012). *Security and Privacy in Mobile Information and Communication Systems* (Bd. 107). Berlin, Heidelberg: Springer Berlin Heidelberg.

- Van Tilborg, H. C. A. & Jajodia, S. (2011). *Encyclopedia of Cryptography and Security*. Boston, MA: Springer US.
- Wieczorrek, H. W. & Mertens, P. (2011). Vorgehen in IT-Projekten. In H. W. Wieczorrek & P. Mertens (Hrsg.), *Management von IT-Projekten* (Xpert.press, S. 55-102). Berlin, Heidelberg: Springer Berlin Heidelberg.
- Wiggers, K. (2019, 24. September). *Everledger raises \$20 million to track assets with blockchain tech*, VentureBeat. Verfügbar unter <https://venturebeat.com/2019/09/24/everledger-raises-20-million-to-track-assets-with-blockchain-tech/>
- Wüst, K. & Gervais, A. (2018). Do you Need a Blockchain? In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)* (S. 45-54). Verfügbar unter <https://ieeexplore.ieee.org/document/8525392/>
- Zogg, J.-M. (o. J.). *Aufbau des NMEA-Protokolls. Aufbau des NMEA Protokolls*. Zugriff am 05.11.2019. Verfügbar unter http://www.zogg-jm.ch/Dateien/aufbau_des_nmea.pdf
- Zogg, J.-M. (2014). *GPS und GNSS: Grundlagen der Ortung und Navigation mit Satelliten. User's Guide*, u-blox. Verfügbar unter http://www.zogg-jm.ch/Dateien/Update_Zogg_Deutsche_Version_Jan_09_Version_Z4x.pdf

Anhang

Vergleich IOTA und Bitcoin	LXXII
Fragebogen für Transport- und Logistikunternehmen.....	LXXIII
Fragebogen für Produktionsunternehmen	LXXVI
Use Case Spezifikation Experiment 1	LXXIX
Use Case Spezifikation Experiment 2	LXXX
Testresultat Anforderung #1	LXXXI

Vergleich IOTA und Bitcoin

Tabelle 8 Vergleich IOTA und Bitcoin

<i>Kryptowährung</i>	<i>IOTA</i>	<i>Bitcoin</i>
Architektur/Technologie	Directed Acyclic Graph	Blockchain
Transaktionsgebühren	keine	Hohe Transaktionsgebühren
Konsensus	Kein Mining (max. 2.8 Peta IOTA), Transaktionsvalidierung bei jeder neuen Transaktion	Mining (max. 21 Mio. Bitcoin = 2.1 Peta Satoshis)
Konsensus-Algorithmus	Proof of Work	Proof of Work
Read Permission	Public	Public
Write Permission	Permissionless	Permissionless
Skalierbarkeit	Je mehr Teilnehmer desto schneller	Je mehr Teilnehmer desto langsamer
Signaturschema	Winternitz One-Time Signature	ECDSA
Verwendung	IoT M2M Micropayments	Zahlungsmittel, Investition/Spekulation

Fragebogen für Transport- und Logistikunternehmen

Fragebogen Trackingsystem Logistik

Fragebogen Trackingsystem Logistik

Vielen Dank für Ihre Zeit und Aufmerksamkeit!

Diese Umfrage ist Teil eines Forschungsprojekts der Hochschule Luzern Informatik. Es werden keine kritischen Informationen erhoben. Die Auswertung ist nur zu Forschungszwecken.

Bei Fragen melden Sie sich bitte bei florence.pfamatter@stud.hslu.ch

FRAGEBOGEN FÜR LOGISTIK- und TRANSPORTUNTERNEHMEN

Falls es sich bei Ihrem Unternehmen nicht um ein solches handelt, beantworten Sie die Fragen bitte einfach so gut es geht.

1. Wieviele Fahrzeuge beinhaltet Ihr Transportunternehmen?

2. Wie organisieren Sie die verfügbaren Ressourcen? (Fahrer, Fahrzeuge)

3. Welche Probleme ergeben sich dabei?

Fragesupport: *Welche Herausforderungen haben Sie oder Mitarbeitende Ihres Unternehmens im Logistik-Alltag? Welche Probleme gibt es bei der Planung und Einteilung der Ressourcen?*

4. Wie stellen Sie sicher, dass Fahrer auch tatsächlich die vereinbarte Strecke fahren?

5. Würde Ihnen ein Live-Tracking (Zeit und Ort) eines Fahrzeugs bei der Streckenplanung und für Nachverfolgbarkeit weiterhelfen?

Fragebogen Trackingsystem Logistik

6. Bezüglich der LSVA-Taxe: Wie kann die Behörde bei Ihren Fahrzeugen nachvollziehen, wieviele Kilometer diese gefahren sind?

Fragesupport: *Die leistungsabhängige Schwerverkehrsabgabe ist eine vom Gesamtgewicht, der Emissionsstufe sowie den gefahrenen Kilometern in der Schweiz und dem Fürstentum Liechtenstein abhängige eidgenössische Abgabe.*

7. Was sind die dringendsten Probleme Ihrer Branche (Transport & Logistik)?

Fragesupport: *Wo sehen Sie in Ihrer Branche Platz für Verbesserung?*

8. Wenn ein Lastwagen eindeutig identifiziert, live verfolgt werden und GPS Daten nicht-manipulierbar aufgezeichnet werden könnten – würde Ihnen dies helfen?

Fragesupport: *Wählen Sie eine Antwort*

- Ja
 Nein
 Weiss nicht

9. Falls Sie die letzte Frage mit Nein beantwortet haben, wieso nicht?

10. Welche Informationen wären für Sie bei einem Fahrdaten-Tracking evtl. auch interessant?

Fragesupport: *Falls Sie während der Fahrt kontinuierlich Daten zu Ihren Fahrzeugen erhalten könnten, welche Daten wären für Sie relevant?*

- Gewicht der Ladung
 Feuchtigkeit
 Temperatur
 Wann und wo die Ladeklappe geöffnet wurde
 Andere...
 Andere... (Antwort 6)
 Andere... (Antwort 7)
 Keine

Fragebogen Trackingsystem Logistik

11. Haben Sie bereits Projekte mit Blockchain oder Distributed Ledger Technologien allgemein, welche eine bessere Nachverfolgbarkeit von Lieferware oder Produkten zum Ziel haben?

Fragesupport: *Mit der Blockchain-Technologie können Sie Informationen nicht-manipulierbar speichern.*

12. Ich würde gerne mehr Informationen zur Forschungsarbeit erhalten.

Fragesupport: *Falls Sie nach Abschluss dieser Forschungsarbeit über Ergebnisse informiert werden möchten oder mehr Details zum Inhalt dieser Arbeit wünschen, können Sie nach Anklicken des untenstehenden Felds Ihre E-Mail-Adresse angeben.*

Nein danke.

Ja, bitte benachrichtigen Sie mich per Mail (E-Mail-Adresse einfügen):

13. Was ich noch sagen möchte:

Vielen Dank für Ihre Antworten!

Falls Sie Fragen oder Anmerkungen haben, dürfen Sie sich gerne melden unter florence.pfamatter@stud.hslu.ch.

Fragebogen für Produktionsunternehmen

Fragebogen Trackingsystem Supply Chain

Fragebogen Trackingsystem Supply Chain

Vielen Dank für Ihre Zeit und Aufmerksamkeit!

Diese Umfrage ist Teil eines Forschungsprojekts der Hochschule Luzern Informatik. Es werden keine kritischen Informationen erhoben. Die Auswertung ist nur zu Forschungszwecken.

Bei Fragen melden Sie sich bitte bei florence.pfamatter@gmail.com

FRAGEBOGEN FÜR UNTERNEHMEN MIT GRÖßERER LOGISTIK-ABTEILUNG ODER HÄUFIGER ZUSAMMENARBEIT MIT ZULIEFER VERTEILERN

Falls es sich bei Ihrem Unternehmen nicht um ein solches handelt, beantworten Sie die Fragen bitte einfach so gut es geht.

1. Mit welche Transportmitteln arbeiten Sie oder Ihre Zulieferer bzw. Verteiler?

Fragesupport: *Wählen Sie eine oder mehr Antworten*

- Schwerlastverkehr
- Schiffstransport
- Flugtransport
- Schienentransport

2. Wie organisieren Sie die verfügbaren Ressourcen? (Fahrer, Fahrzeuge, Planbarkeit Zulieferer/Verteiler)

3. Welche Probleme ergeben sich dabei?

Fragesupport: *Welche Herausforderungen haben Sie oder Mitarbeitende Ihres Unternehmens im Logistik-Alltag? Welche Probleme gibt es bei der Planung und Einteilung der Ressourcen?*

4. Wie stellen Sie sicher, dass die Zulieferung bzw. die Verteilung Ihrer Ware effizient geschieht?

Fragesupport: *Können Sie z.B. sicherstellen, dass ein Fahrer der kürzeste Weg für die Verteilung Ihrer Ware nimmt?*

Fragebogen Trackingsystem Supply Chain

5. Würde Ihnen ein Live-Tracking (Zeit und Ort) eines Fahrzeugs oder eines Warencontainers für bessere Nachverfolgbarkeit weiterhelfen?

Die Frage 6 betrifft nur Unternehmen mit eigenen LKW's. Trifft dies nicht auf Ihr Unternehmen zu, dürfen Sie diese Frage leer lassen.

6. Bezüglich der LSVA-Taxe: Wie kann die Behörde bei Ihren Fahrzeugen nachvollziehen, wieviele Kilometer diese gefahren sind?

Fragesupport: *Die leistungsabhängige Schwerverkehrsabgabe ist eine vom Gesamtgewicht, der Emissionsstufe sowie den gefahrenen Kilometern in der Schweiz und dem Fürstentum Liechtenstein abhängige eidgenössische Abgabe.*

7. Was sind die dringendsten Probleme Ihrer Branche im Bezug auf die Supply Chain?

Fragesupport: *Wo gibt es Verbesserungspotenzial in der Supply Chain? Was würde zu einem besseren Supply Chain Management führen?*

8. Wenn ein Transportfahrzeug oder eine Liefereinheit eindeutig identifiziert, live verfolgt werden und GPS Daten nicht-manipulierbar aufgezeichnet werden könnten – würde Ihnen dies helfen?

Fragesupport: *Wählen Sie eine Antwort*

- Ja
 Nein
 Weiss nicht

9. Falls Sie die letzte Frage mit Nein beantwortet haben, wieso nicht?

Fragebogen Trackingsystem Supply Chain

10. Welche Informationen wären für Sie bei einem (Fahr-)daten-Tracking evtl. auch interessant?

Fragesupport: Falls Sie während der Fahrt kontinuierlich Daten zu Ihrer Liefereinheit erhalten könnten, welche Daten wären für Sie relevant?

- Gewicht der Ladung
- Feuchtigkeit
- Temperatur
- Wann und wo die Ladeklappe geöffnet wurde
- Andere...
- Andere... (Antwort 6)
- Andere... (Antwort 7)
- Keine

11. Haben Sie bereits Projekte mit Blockchain oder Distributed Ledger Technologien allgemein, welche eine bessere Nachverfolgbarkeit von Lieferware oder Produkten zum Ziel haben?

Fragesupport: Mit der Blockchain können Sie Informationen nicht-manipulierbar speichern.

12. Ich würde gerne mehr Informationen zur Forschungsarbeit erhalten.

Fragesupport: Falls Sie nach Abschluss dieser Forschungsarbeit über Ergebnisse informiert werden möchten oder mehr Details zum Inhalt dieser Arbeit wünschen, können Sie nach Anklicken des untenstehenden Felds Ihre E-Mail-Adresse angeben.

- Nein danke.
- Ja, bitte benachrichtigen Sie mich per Mail (Email-Adresse einfügen):

13. Was ich noch sagen möchte:

Vielen Dank für Ihre Antworten! Falls Sie Fragen oder Anmerkungen haben, dürfen Sie sich gerne melden unter unterflorencia.pfammatter@stud.hslu.ch

Use Case Spezifikation Experiment 1

Tabelle 9 Use Case Spezifikation Experiment 1

Name	Identitätsmanagement mit IOTA
Kurzbeschreibung	Registrieren, Verwalten und Verifizieren eines Identity-Claims für einen Raspberry Pi über den IOTA-Tangle
Akteure	Claim-Issuer und Claim-Verifier
Auslöser	Claim-Issuer möchte Raspberry Pi eindeutige, verifizierbare Identität zuweisen
Vorbedingungen	Laptop mit Internetverbindung und Node JS (Version 10 oder höher) Raspberry Pi
Nachbedingungen	Signierter Identity-Claim ist auf Raspberry Pi abgelegt Der Hash davon ist auf dem IOTA Tangle gespeichert
Ablauf	<ol style="list-style-type: none"> 1. Signierter Identity-Claim wird in Form eines JSON-Dokuments auf dem Raspberry abgespeichert 2. Erstellung eines Identity-Channels auf dem IOTA-Tangle für Raspberry Pi 3. Hash des signierten Identity-Claims wird im Identity-Channel veröffentlicht 4. Der Claim-Verifier fordert Raspberry Pi zur Authentifizierung auf 5. Raspberry Pi schickt Claim-Verifier signierter Identity-Claim 6. Identity-Claim des Raspberry's wird mit Hash auf IOTA-Tangle verglichen
Ausnahmen	Bei Schritt 2 könnte statt einer Registrierung auch ein Update oder eine Deaktivierung der Identität erfolgen
Systemgrenzen	Die Authentifizierung des Claim-Verifiers gegenüber dem Raspberry Pi wird nicht berücksichtigt Notwendige Sicherheitsnahmen (Schutz Private Key auf Raspberry Pi) werden diskutiert aber nicht umgesetzt

Use Case Spezifikation Experiment 2

Tabelle 10 Use Case Spezifikation Experiment 2

Name	Masked Authenticated Messaging für GPS-Daten
Kurzbeschreibung	Erstellen eines restricted Channels für Sensor-Daten, Senden der Sensordaten und Abfragen der Sensor-Daten
Akteure	Observer
Auslöser	
Vorbedingungen	Laptop mit Internetverbindung und Node JS (Version 10 oder höher) Raspberry Pi mit Internetverbindung und Node JS (Version 10 oder höher) GPS Modul mit UART Verbindung zum Raspberry Pi
Nachbedingungen	Daten des GPS-Moduls werden auf einem restricted MAM-Channel veröffentlicht, der Observer kann diese mit dem passenden Side Key abrufen
Ablauf	<ol style="list-style-type: none"> 1. GPS-Modul sendet Daten über UART an Raspberry Pi 2. Raspberry Pi veröffentlicht in regelmässigen Abständen ein Datenpaket in einem restricted MAM-Channel auf dem IOTA Tangle 3. Mittels eines Schlüssels (Side Key) hat Partei Lesezugriff auf MAM-Channel und fetcht die Daten (über Node JS oder im Browser)
Ausnahmen	Änderung des Side Key, um Lesezugriff von Parteien zu entziehen
Systemgrenzen	Die Authentifizierung des Observers gegenüber dem Raspberry Pi wird nicht berücksichtigt Notwendige Sicherheitsnahmen werden nicht umgesetzt

Testresultat Anforderung #1

