

Hochschule Darmstadt

– Fachbereich Informatik–

Synergie von DLT und IOT: Anforderungsanalyse und praktische Verprobung

Abschlussarbeit zur Erlangung des akademischen Grades
Master of Science (M.Sc.)

vorgelegt von

Sebastian Kanz

Matrikelnummer: 735176

Referent : Prof. Dr. Michael Braun
Korreferent : Prof. Dr. Martin Stiemerling

ERKLÄRUNG

Ich versichere hiermit, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die im Literaturverzeichnis angegebenen Quellen benutzt habe.

Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder noch nicht veröffentlichten Quellen entnommen sind, sind als solche kenntlich gemacht.

Die Zeichnungen oder Abbildungen in dieser Arbeit sind von mir selbst erstellt worden oder mit einem entsprechenden Quellennachweis versehen.

Diese Arbeit ist in gleicher oder ähnlicher Form noch bei keiner anderen Prüfungsbehörde eingereicht worden.

Darmstadt, 15. April 2020

Sebastian Kanz

ABSTRACT

The Internet of Things (IOT) gets more and more part of the everyday life. Smart-Home solutions, latency-sensitive connected cars or the vision of a smart-city affect the research works in their respective areas. The aim is a fully-automated machine-to-machine (M2M) handling of processes to automate and simplify our everyday life. This leads to a huge amount of data needs to be processed, transmitted and stored. With the introduction of the new mobile communication standard 5G and increasingly powerful devices the transmission and processing of data is guaranteed. The question where this huge amount of data is stored and further processed is still unanswered. Besides the topic of distributed ledger technologies (DLT) gets more attention as new use cases arise which can profit from the distributed infrastructure, the trustless environment and the decentralization. It makes sense to investigate to see if the yet relatively young technologies IOT and DLT can complement each other and where there may be synergies.

This master thesis evaluates a selection of established DLTs for their suitability for the IOT environment with focus on the M2M part. The key research object is the thesis, that DLT is a suitable technology for IOT and the non-functional requirements for all DLT-IOT use cases are identical. For this purpose an IOT use case will be created which will be used for further analysis. Using a classification model requirements are identified that a DLT must satisfy in order to be suitable for the use case. The criteria are applied, evaluated and ranked to a selection of DLT implementations. As a result of the analysis Ethereum is the most suitable solution and therefore a prototypical implementation is made to check the result of the requirements evaluation and finally the research questions.

The result is a structured and comprehensible rating of multiple established DLTs and their suitability for IOT use cases as well as a DLT based prototype inspired by a real use case which serves as a verification for the developed rating. It is shown that IOT can profit from DLT under certain circumstances. The findings of this work are, that DLT is a suitable technology for decentralized and asynchronous iot use cases where multiple distrusting parties are involved. The base of all non-functional requirements are identical for all DLT-IOT usecases.

ZUSAMMENFASSUNG

Das Internet der Dinge (engl. IOT; Internet of Things) erhält immer mehr Einzug in das tägliche Leben. Smart-Home Lösungen, vernetzte und latenzempfindliche Connected-Cars oder die Vision einer Smart-City prägen die Forschungsarbeiten in den jeweiligen Bereichen. Ziel ist eine vollautomatische Machine-to-Machine (M2M) Abwicklung von Prozessen, um unseren Alltag zu automatisieren und zu vereinfachen. Dabei fallen eine Menge Daten an, die verarbeitet, übertragen und gespeichert werden müssen. Mit der Einführung des neuen Mobilfunk-Standards 5G und immer leistungsfähigeren Endgeräten sind Übertragung und Verarbeitung der Daten weitestgehend gesichert; bleibt die Frage offen, wo diese großen Datenmengen gespeichert und weiterverarbeitet werden. Daneben erfreut sich das Thema Distributed-Ledger-Technology (DLT) immer größerer Beliebtheit: Es werden täglich neue Anwendungsfälle gefunden, die durch die verteilte Infrastruktur, die Trustless-Eigenschaft und von Dezentralität profitieren. Es bietet sich eine Untersuchung an, um zu überprüfen, inwieweit diese beiden noch recht jungen Technologien IOT und DLT Synergien besitzen und sich gegebenenfalls gegenseitig ergänzen können.

Die vorliegende Masterarbeit evaluiert eine Auswahl etablierter DLTs anhand ihrer Tauglichkeit für den Einsatz im IOT-Umfeld mit Fokus auf den M2M-Bereich. Der zentrale Forschungsgegenstand ist die These, dass DLT eine geeignete Technologie für IOT darstellt, und dass alle DLT-IOT-Anwendungsfälle die gleichen nicht-funktionalen Anforderungen besitzen. Dazu wird zunächst ein IOT-Anwendungsfall erstellt, der für die weiteren Analysen verwendet wird. Anschließend werden konkrete Anforderungen mit Hilfe eines Klassifizierungsmodells aufgestellt, die eine DLT erfüllen muss, um dem Anwendungsfall gerecht zu werden. Die erstellten Kriterien werden auf eine Auswahl von DLT-Implementierungen angewandt, evaluiert und bewertet. In der Analyse stellte sich die Blockchain-Plattform Ethereum als geeignetste Lösung heraus. Mit dieser wurde eine prototypische Implementierung des Anwendungsfalls vorgenommen, um das Resultat der Anforderungsevaluierung und letztlich auch die Forschungsfrage zu überprüfen.

Das Ergebnis ist eine strukturierte und nachvollziehbare Bewertung mehrerer, am Markt etablierter DLTs, inwieweit diese für DLT-sinnvolle IOT-Anwendungsfälle geeignet sind, sowie ein DLT-basierter Prototyp, angelehnt an einen realen Use-Case, der beispielhaft als Nachweis der erarbeiteten Bewertung dient.

Es wird gezeigt, dass IOT unter gewissen Voraussetzungen von DLTs profitieren kann. Die Erkenntnisse sind, dass sich DLT als Technologie für dezentrale und asynchrone IOT-Anwendungsfälle eignet, an denen mehrere, sich gegeneinander nicht vertrauende Parteien teilnehmen. Die Basis aller

nicht-funktionalen Anforderungen sind für alle Distributed Ledger Technologies (DLT)-Internet of Things (IOT)-Anwendungsfälle gleich.

INHALTSVERZEICHNIS

I THESIS

1 EINLEITUNG	2
1.1 Motivation & Problemstellung	2
1.2 Zielsetzung & Zielgruppe	3
1.3 Methodik & Aufbau dieser Arbeit	3
2 THEORETISCHE GRUNDLAGEN	5
2.1 Distributed Ledger Technologies	5
2.1.1 Konsensprotokolle	7
2.1.2 Smart-Contracts	9
2.1.3 Dezentrale Apps (DApps)	9
2.1.4 Klassifizierung von Blockchains	10
2.1.5 Wallets	11
2.1.6 Dezentrale Identitäten	12
2.1.7 State-Channel	13
2.1.8 Blockchain als Kommunikationsprotokoll	15
2.2 Internet of Things	18
2.2.1 Digitaler Zwilling	20
3 VERWANDTE FORSCHUNGSARBEITEN	22
4 ANWENDUNGSFALL: VERMIETUNG VON HAUSHALTSGERÄTEN	
NACH DEM PAY-AS-YOU-USE PRINZIP	24
4.1 Beschreibung	24
4.2 Technische Lösungsskizze	26
4.2.1 Endgeräte	26
4.2.2 Verträge	27
4.2.3 Benutzerschnittstelle	28
4.2.4 Backend	29
5 ANFORDERUNGEN	30
5.1 Standards und Normen	30
5.2 Ableitung eines Klassifizierungsmodells	32
5.3 Anforderungsanalyse	34
5.4 Anforderungsevaluierung	37
5.4.1 System-Anforderungen	38
5.4.2 Software-Anforderungen	39
5.5 Anforderungstransfer auf DLT	45
6 AUSWAHL RELEVANTER DLTS	48
6.1 Vorgehen	48
6.2 Marktübersicht DLTs	49
6.3 Anforderungserfüllung	49
6.4 Bewertung, Ranking & Auswahl	51
7 UMSETZUNG	53
7.1 Architektur und Aufbau	53

7.2	Deployment	54
7.3	Testaufbau	55
7.4	Anforderungsumsetzung	56
7.4.1	Smart-Contracts	56
7.4.2	Oracle-Services	57
7.4.3	Zahlungsmittel	58
7.4.4	Asynchronität	59
7.4.5	Performanz	60
7.4.6	Verschlüsselung	63
8	ERGEBNISSE & FAZIT	65
8.1	Anforderungsklassifizierung	65
8.2	Machbarkeit	65
8.3	Kosten	65
8.4	Performanz	66
8.5	Sicherheit	66
8.6	Vorteile zu klassischen Ansätzen	67
8.7	Datenschutz & Privatsphäre	67
8.8	Implementierungsfortschritt	67
9	DISKUSSION	68
9.1	Wiederaufnahme These Teil 1: Eignung für IOT?	68
9.2	Wiederaufnahme These Teil 2: Technische Anforderungen immer gleich?	68
9.3	Ergebnis	69
10	AUSBLICK	70
10.1	Kostensenkung	70
10.2	Privatsphäre & Datenschutz	71
II	APPENDIX	
A	APPENDIX: ANFORDERUNGEN	74
B	APPENDIX: DLT-MARKTÜBERSICHT	78
C	APPENDIX: UMSETZUNG	83
C.1	Benutzerinteraktionen	83
C.2	Deployment	86
C.3	Kostenevaluation	87
C.4	UI	91
D	APPENDIX: CODE	92
	LITERATUR	111

ABBILDUNGSVERZEICHNIS

Abbildung 2.1	Bestandteile von DLTs	6
Abbildung 2.2	Aufbau von DApps	10
Abbildung 2.3	Taxonomie von Blockchains (vgl. [17])	11
Abbildung 2.4	Die Blockchain-Layer im Kontext des OSI-Modells	17
Abbildung 2.5	Schematische Darstellung von IOT im Kontext von DLTs	19
Abbildung 4.1	UML-Anwendungsfalldiagramm	25
Abbildung 4.2	Aktivitätsdiagramm - Ablauf des Anwendungsfalls aus Sicht der Stakeholder	27
Abbildung 4.3	Aufbau und Bestandteile eines Endgeräts	28
Abbildung 5.1	Einordnung der Begriffe und Zusammenhänge unterschiedlicher Normen und Standards	31
Abbildung 5.2	Anforderungen werden nach zwei verschiedenen Ansätzen gruppiert.	32
Abbildung 5.3	Anforderungsklassifizierung als kombiniertes Modell aus [2], [27] bzw. [26] und [25]	34
Abbildung 7.1	Architektur als UML-Komponentendiagramm	53
Abbildung 7.2	Frontend, bereitgestellt mit Heroku	55
Abbildung 7.3	Testabdeckung der Solidity Smart-Contracts	56
Abbildung 7.4	Blockzeit von Ethereum innerhalb des letzten Jahres	58
Abbildung C.1	UML-Sequenzdiagramm zur Vertragserzeugung	83
Abbildung C.2	UML-Sequenzdiagramm zur Zahlungsabwicklung	84
Abbildung C.3	Vertrag anfragen: Metamask Screenshot einer Transaktion	88
Abbildung C.4	Vertrag akzeptieren: Metamask Screenshot einer Transaktion	89
Abbildung C.5	Vertrag erzeugen: Metamask Screenshot einer Transaktion	89
Abbildung C.6	Prepaid Guthaben aufladen: Metamask Screenshot einer Transaktion	90
Abbildung C.7	Quittung einlösen: Metamask Screenshot einer Transaktion	90
Abbildung C.8	Wallet-App auf Android-Basis	91

TABELLENVERZEICHNIS

Tabelle 5.1	DLT-relevante Anforderungen	46
Tabelle 6.1	Erstauswahl von DLT-Lösungen	50
Tabelle 6.2	Erfüllung der DLT-relevanten Anforderungen	51
Tabelle 7.1	Adressen der Smart-Contracts auf dem öffentlichen Kovan Testnet	55
Tabelle 7.2	Kosten für (Einmal-) Transaktionen aus Benutzer- Sicht (oben) und Hersteller-Sicht (unten) bei einem Gas-Preis von 5 GWEI. Im Anhang (C.3) finden sich die Screenshots, die die Angaben belegen.	59
Tabelle B.1	IOT-Relevanz	79
Tabelle B.2	Blocktivity	79
Tabelle B.3	Coincodecap	80
Tabelle B.4	Github Commits past 12 months	80
Tabelle B.5	Blockchain Projekte in großen internationalen Unter- nehmen (Teil 1)	81
Tabelle B.6	Blockchain Projekte in großen internationalen Unter- nehmen (Teil 2)	82
Tabelle C.1	Adressen der Smart-Contracts auf dem öffentlichen Ropsten Testnet	86
Tabelle C.2	Basisdaten für Kostenkalkulationen, inklusive der Annahmen	87
Tabelle C.3	Einzelkosten der Transaktion	87
Tabelle C.4	Gesamtkosten (einmalig und jährlich) der Transaktio- nen aus Nutzer- und Herstellersicht	88

LISTINGS

Listing 2.1	Beispiel einer DID	12
Listing 2.2	Beispiel eines DID-Dokuments	12
Listing D.1	RentalProvider Smart-Contract	92
Listing D.2	PaymentProvider Smart-Contract	101
Listing D.3	IdentityProvider Smart-Contract	105

ABKÜRZUNGSVERZEICHNIS

API Application Programming Interface

ARP Address Resolution Protocol

BABOK Business Analysis Body of Knowledge

BFT Byzantine Fault Tolerance

CIOT Consumer IOT

DApp Distributed Application

DID Decentralized Identifier

DLT Distributed Ledger Technologies

DoD Definition of Done

DoR Definition of Ready

E2E End-to-End

EVM Ethereum Virtual Machine

IEEE Institute of Electrical and Electronics Engineers

IIBA International Institute of Business Analysis

IIOT Industrial IOT

IOT Internet of Things

ISO International Organization for Standardization

IPFS Inter-Planetary File System

M2M Machine-to-Machine

NFC Near Field Communication

OSI Open Systems Interconnection

P2P Peer-to-Peer

PMBOK Project Management Body of Knowledge

PMI Project Management Institute

PoA Proof-of-Authority

PoC Proof-of-Concept

- PoW Proof-of-Work
- RPC Remote Procedure Call
- SDK Software Development Kit
- SEBOK System Engineering Body of Knowledge
- SPoF Single-Point-of-Failure
- SWEBOK Software Engineering Body of Knowledge
- TPS Transactions per Second
- UI User-Interface
- UML Unified Modelling Language
- UX User-Experience
- VC Verifiable Credential
- W3C World Wide Web Consortium

Teil I
THESIS

EINLEITUNG

Die Blockchain ist eine Technologie, deren grundlegende Ansätze keineswegs neu sind: Vor über 1500 Jahren suchten die Einwohner der Insel Yap im Westpazifik, östlich der Philippinen, eine Lösung für ihr Zahlungsmittel-Problem. Ihre Währung - Rai - waren großen runde Steintafeln, die teils mehrere Tonnen wogen und als alltägliches Zahlungsmittel ungeeignet waren. Ihre Lösung: Die Dorfältesten merkten sich, wem welcher Rai-Stein gehörte. Fand eine Transaktion statt, so wurde diese den Dorfältesten mitgeteilt. Das Wissen, wem welcher Stein gehörte und wer von wem etwas gekauft hatte, war über mehrere Köpfe verteilt; die dezentrale Informati-onsspeicherung war geboren [21].

1991 beschrieben die Forscher Stuart Haber und W. Scott Stornetta die Idee hinter der Blockchain-Technologie [8], 2008 veröffentlichte Satoshi Nakamoto das Whitepaper zu Bitcoin [33], dicht gefolgt von Ethereum [9], welches 2013 von Vitalik Buterin erstmals vorgestellt wurde.

Und wie sieht es heute aus?

Mittlerweile ist ein ganzes Ökosystem an Blockchain- und DLT-Lösungen entstanden: Es existieren digitale Vermögenswerte wie Bitcoin, verteilte Anwendungen auf Basis des Blockchain-Protokolls wie Distributed Application (DApp)s auf Ethereum und digitale Zahlungsmittel von fast über 5000 gelisteten Kryptowährungen.

1.1 MOTIVATION & PROBLEMSTELLUNG

Das Telekommunikationsunternehmen Cisco prognostiziert, dass bis zum Jahr 2030 mehr als 500 Milliarden mit dem Internet verbundene IOT-Geräte in verschiedenen Bereichen unseres alltäglichen Lebens Einzug gehalten haben werden [15]. Vernetzte Dinge unseres Alltags wie Kühlschränke, Kaffeemaschinen, die automatisierte Supply-Chain aus dem Business-Umfeld oder eine Smart-City sind nur einige wenige Beispiele dieses Geschäftsfeldes. Obwohl das Konzept von IOT noch sehr theoretisch ist, wurden bereits einige Anwendungsfälle erarbeitet. Um das große Potential von IOT vollen-fänglich nutzbar zu machen und entsprechende Visionen umzusetzen, muss eine passende IT-Lösung für den entsprechenden Anwendungsfall bereitge-stellt werden. Viele verschiedene Hersteller und Service-Provider benötigen eine einheitliche Plattform, auf der sie ihre IOT-Geräte, Services, Geschäfts-logiken und Kunden miteinander vernetzen und ein sicheres Bezahl-system integrieren können. Es stellt sich die Frage, ob und inwiefern die zwei in-novativen Technologien DLT und IOT voneinander profitieren können und

ob sich **DLT** als skalierende, performante und sichere Technologie für **IOT**-Anwendungsfälle eignet.

1.2 ZIELSETZUNG & ZIELGRUPPE

Das Ziel dieser Arbeit ist die Untersuchung und prototypische Verprobung der folgenden These:

'**DLT** eignet sich als Technologie für **IOT** und die nicht-funktionalen Anforderungen sind für alle **DLT-IOT**-Anwendungsfälle gleich.'

Es wird gezeigt, inwieweit sich die Technologie **DLT** für **IOT**-Anwendungsfälle eignet, welche Anforderungen dafür erfüllt sein müssen und welche Implementierung für die Umsetzung in Frage kommt. Dazu wird im Verlauf der Arbeit das zu lösende Problem genauer spezifiziert und herausgearbeitet: Nachdem ein konkreter, stellvertretender **IOT**-Anwendungsfall vorgestellt wurde und alle **DLT**-relevanten Anforderungen ermittelt und evaluiert sind, ergibt sich das konkrete Problem als die Umsetzung eines speziellen **IOT**-Anwendungsfalls mit einer ausgewählten **DLT**-Lösung. Der explizite Lösungsraum, also welche Anforderungen umgesetzt werden, wird zuvor genau beschrieben. Das Problem gilt als gelöst, sobald die zuvor abgeleiteten Anforderungen mit dem Proof-of-Concept (**PoC**) erfüllt werden können.

Abschließend wird die eingangs formulierte These diskutiert und evaluiert. Diese Arbeit richtet sich an IT-Spezialisten aus dem Umfeld **DLT** und **IOT**, die sich über die Synergie beider Konzepte informieren, sowie Fachleute aus der Industrie, die entsprechende **IOT**-Anwendungsfälle ausarbeiten möchten. Ein solides Grundverständnis für die grundlegenden Konzepte und Wordings wird an dieser Stelle vorausgesetzt; auf entsprechende Grundlagenliteratur wird gegebenenfalls verwiesen.

1.3 METHODIK & AUFBAU DIESER ARBEIT

In dieser Arbeit werden die Themenbereiche '**DLT**' und '**IOT**' vorgestellt, klassifiziert und '**DLT**' als Kommunikationsprotokoll eingeordnet. Die Synergie beider Bereiche wird herausgearbeitet und es wird dem Leser vorgestellt, wie diese Technologien voneinander profitieren können (Kapitel 2).

Zur entsprechenden Einordnung dieser Arbeit werden verwandte Forschungsarbeiten vorgestellt (Kapitel 3). Ein beispielhafter **IOT**-Anwendungsfall wird entwickelt (Kapitel 4) und eine detaillierte Auflistung aller Anforderungen erarbeitet (Kapitel 5).

Im nächsten Schritt werden die ermittelten Anforderungen schrittweise auf eine Untermenge von fundamentalen Anforderungen reduziert, die relevant für **IOT** in Verbindung mit **DLT** sind. Mehrere, am Markt etablierte **DLTs** werden anschließend vorgestellt und auf Basis dieser Anforderungsunter-

menge evaluiert (Kapitel 6). Es wird geprüft, ob und inwieweit sie sich als Lösung für den **IOT**-Anwendungsfall qualifizieren. Die vielversprechendste Lösung wird in einem **PoC** prototypisch umgesetzt (Kapitel 7), um die Anforderungsliste zu evaluieren. Es wird gezeigt, dass die gewählte **DLT** zielbringend eingesetzt werden kann (Kapitel 8).

Anschließend wird diskutiert, ob und warum die nicht-funktionalen Anforderungen für **DLT**-geeignete **IOT**-Anwendungsfälle - unabhängig vom tatsächlichen Anwendungsfall selbst - stets die gleichen sind (Kapitel 9). Abschließend wird ein Ausblick über weitere, mögliche Forschungsgebiete in diesem Umfeld gegeben (Kapitel 10).

Diese Arbeit zeigt die Eignung von verschiedenen **DLTs** für **IOT**-Anwendungsfälle anhand eines beispielhaften **PoCs**. Es werden nur solche Bereiche von **IOT** betrachtet, die auch grundsätzlich für die Implementierung auf **DLTs** geeignet sind. Es gibt darüber hinaus weitere Bereiche, die sich nicht eignen, auf **DLTs** umgesetzt zu werden und diese müssen auf einer anderen technologischen Basis implementiert werden (vgl. Kapitel 2.2). Die in dieser Arbeit durchgeführte Analyse wird anhand eines **PoC** belegt. Aufgrund von Restriktionen bezüglich Zeitlimitierung und praktischer Umsetzbarkeit könnten unter Umständen nicht alle fundamentalen Anforderungen gezeigt werden, die für einen **IOT-DLT**-Anwendungsfall erfüllt sein müssen (vgl. Kapitel 7).

THEORETISCHE GRUNDLAGEN

Dieses Kapitel stellt dem Leser benötigtes Basiswissen zur Verfügung. Es wird ein grundlegendes Wissen zu den Themenbereichen **DLT** und **IOT** vermittelt und auf weitere Informationsquellen verwiesen, welche tiefergehende Informationen bereitstellen.

2.1 DISTRIBUTED LEDGER TECHNOLOGIES

Die Begriffe Blockchain und Distributed Ledger Technology (kurz: **DLT**) werden häufig synonym verwendet¹, wobei es sich bei Blockchain um eine Unterklasse von **DLT** handelt [6]. Grundsätzlich werden Daten in Blockchains zu Blöcken zusammengefasst und mittels Hashketten in eine feste Reihenfolge gebracht. **DLTs** nutzen darüber hinaus andere Strukturen als Blöcke, indem sie Daten beispielsweise durch Bäume oder Graphen anordnen.

Abbildung 2.1 zeigt die Bestandteile einer **DLT** auf. Diese werden im Folgenden detailliert beschrieben und erklärt.

Es handelt sich bei **DLTs** um dezentrale Peer-to-Peer (**P2P**)-Netzwerke, in denen Knoten (engl.: Nodes) Daten dezentral speichern, einen Konsens-Mechanismus zur Synchronisierung einsetzen und asymmetrische Ver schlüsselungsverfahren zur Integrität und Absicherung des Systems nutzen. [5]

Hauptbestandteil eines Distributed Ledgers ist der Ledger selbst (deutsch: Kassenbuch), der eine Historie aller erfolgten Transaktionen speichert. Eine Transaktion stellt eine Wert- oder Informationsübertragung zwischen Entitäten dar. Sie beinhaltet einen Sender, einen Empfänger und eine Anzahl Einheiten, die versendet werden sollen. Je nach Implementierung können weitere Inhalte wie zum Beispiel Nutzdaten oder Software-Code dazukommen. Dieser Code, auch Smart-Contract genannt, wird in einer separierten Laufzeitumgebung (Virtual Machine) ausgeführt. Durch das Zusammenspiel mehrerer Smart-Contracts ist man in der Lage, ganze Anwendungen onchain auszuführen; hierbei spricht man von sogenannten **DApps**.

Smart-Contracts können nur auf den internen (onchain) State des Ledgers zuzugreifen. Werden darüber hinaus weitere (offchain) Informationen benötigt², so können diese durch sogenannte Oracles an den Smart-Contract übermittelt werden. Diese handeln als 'Trusted Data Provider', da die bereitgestellten Informationen nicht validiert werden können. [12]

¹ In dieser Arbeit werden die Begriffe ebenfalls synonym verwendet, andernfalls wird explizit darauf hingewiesen.

² Beispiele hierfür können Wetterdaten, Aktien- und Wechselkurse oder Lottozahlen sein

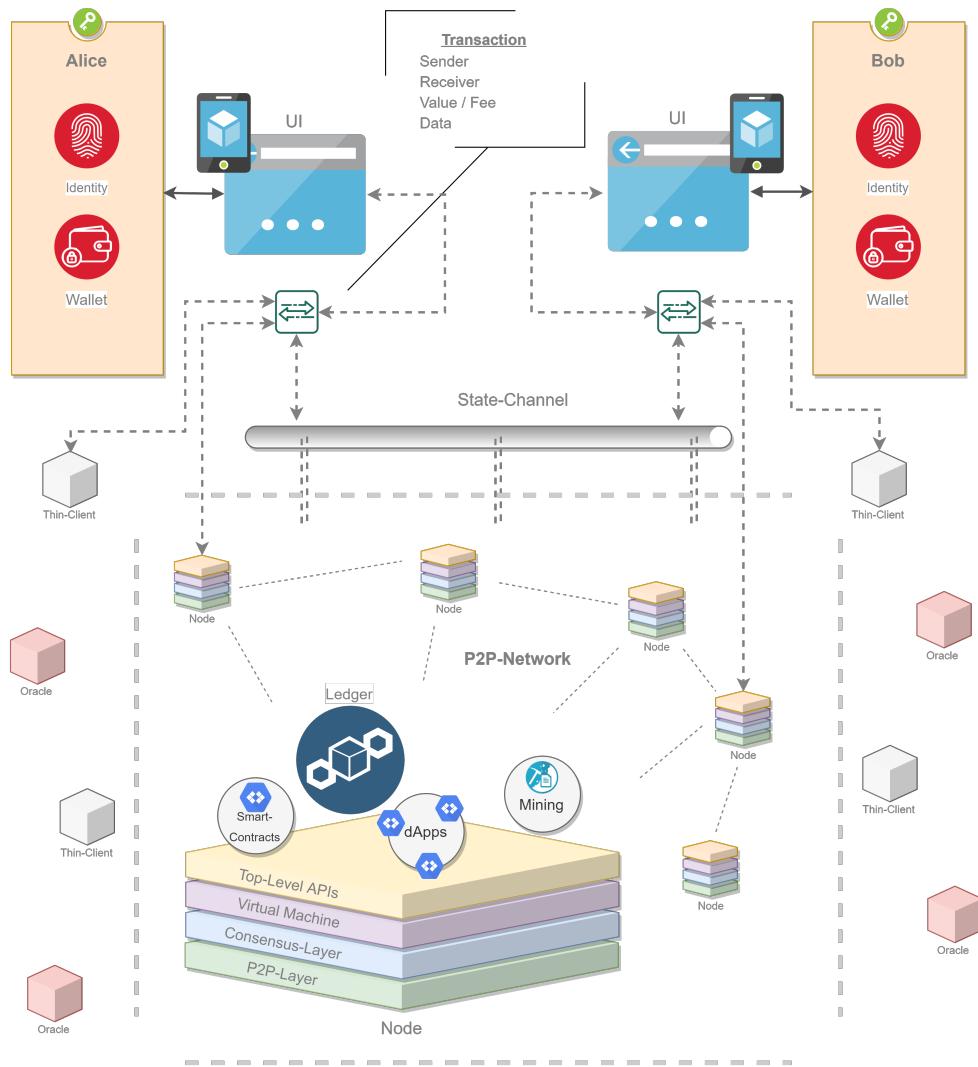


Abbildung 2.1: Bestandteile von DLTs

Transaktionen, die durch Smart-Contracts, **DApps** oder Benutzer ausgeführt werden, müssen von Nodes im Netzwerk validiert werden, bevor sie dem Ledger hinzugefügt werden können. Dazu werden diese durch komplexe Berechnungen zusammengefasst (Mining), dem lokalen Ledger hinzugefügt und anschließend an andere Knoten versendet.

Das Konsensprotokoll definiert die Regeln, wann ein Block hinzugefügt werden darf, welche Eigenschaften dieser erfüllen muss und ob das Mining korrekt durchgeführt wurde. Dürfen beliebige Nodes am Konsens teilnehmen, so spricht man von einer **Permissionless Blockchain**; sind nur privilegierte Nodes befähigt, am Konsens teilzunehmen, handelt es sich um eine **Permisioned Blockchain**. Darüber hinaus lassen sich Blockchain-Netzwerke klassifizieren, ob Transaktionen und Blöcke öffentlich erreichbar und lesbar sind (**Public Blockchain**) oder ob auch hier Restriktionen vorliegen (**Private Blockchain**).

Besondere Anforderungen, wie möglichst niedrige Transaktionskosten, ei-

ne hohe Transaktionsgeschwindigkeit, ein eingeschränkter Wirkungskreis der Anwendung oder Beschränkungen durch das Geschäftsmodell, sind einige Beispiele für die Zulassungsbeschränkung und beschränkte Teilnahme am Konsensverfahren; je nach den gegebenen Anforderungen müssen Blockchain-Protokolle für den jeweiligen Anwendungsfall gewählt oder angepasst werden. Alle Knoten, die dem Konsens-Protokoll folgen und eingehende Blöcke nach diesem Protokoll validieren, heißen Full-Nodes. Daneben existieren sogenannte Light-Clients (oft auch Thin-Clients), die nur Teile des Ledgers vorhalten und meist nur die Block-Header auf Validität überprüfen. Light-Clients sind genauso wie Oracles nicht Teil des P2P-Netzwerkes, sondern greifen mittels Application Programming Interface (API) auf die Nodes zu.

Möchte ein Benutzer (in Abbildung 2.1 durch Alice und Bob dargestellt) mit der Blockchain kommunizieren oder diese als Kommunikationsmedium nutzen, so geschieht dies ebenfalls über entsprechende APIs. Über eine grafische Benutzeroberfläche können Benutzer meist per Browser oder Smartphone Transaktionen auslösen und diese über das Blockchain-Netzwerk versenden. Jeder Benutzer besitzt eine Wallet, die aus einem öffentlichen und einem privaten Schlüssel besteht (Public / Private Key). Der Public-Key gleicht der Kontoadresse eines Bankkontos, der dazugehörige Private-Key der PIN-Nummer. Damit besitzt jeder Nutzer eine eindeutige Identität.

Möchte Alice eine Transaktion im Wert von 10€ an Bob senden, so kann sie dies auf unterschiedlichen Wegen tun. Zunächst einmal kann sie die gewünschten Informationen auf ihrem Smartphone mittels einer Wallet-App eingeben und per Knopfdruck an das Blockchain-Netzwerk übermitteln. Diese wird dort über die entsprechende API empfangen, verarbeitet und im Ledger persistiert. Bob kann ebenfalls mittels seiner Smartphone-App verfolgen, wann sich sein Kontostand ändert und wer eine Transaktion an seine Adresse gesendet hat.

Eine alternative Lösung hierzu wäre der Einsatz von sogenannten State-Channels. Diese können Alice und Bob dazu nutzen, beliebig viele Transaktionen untereinander offchain auszutauschen und lediglich die endgültige Bilanz aller untereinander ausgetauschten Transaktionen onchain in den Ledger zu übertragen.

Die Vor- und Nachteile beider Varianten sowie die in diesem Abschnitt aufgezeigten Fachbegriffe werden im weiteren Verlauf genauer erläutert.

2.1.1 Konsensprotokolle

Transaktionen und Daten müssen über das Gesamtsystem hinweg konsistent sein. Um dies und die Integrität der Daten zu gewährleisten, bedarf es eines Mechanismus, welcher sicherstellt, dass alle Knoten die gleichen Daten halten.

Solche Mechanismen werden durch Konsensprotokolle beschrieben: Es handelt sich dabei um ein Protokoll, welches Regeln definiert, wie und wel-

che Daten gespeichert und welche verworfen werden. Im Folgenden werden einige bekannte Konsensverfahren genannt und kurz vorgestellt.

PROOF-OF-WORK (PoW) Transaktionen werden zu Blöcken zusammengefasst. Diese Blöcke werden durch das Lösen eines kryptografischen Puzzles (Mining) wie zum Beispiel die Ermittlung eines Hashwertes abgesichert. Ein Knoten, der einen Block dem Ledger hinzufügen möchte, muss zuerst eine zufallsbasierte Berechnung durchführen, um dem Netzwerk die Validität zu beweisen. Andere Knoten können mit sehr wenig Aufwand überprüfen, ob die Berechnung korrekt war und der Knoten ehrlich gehandelt hat. Dieses Konsensverfahren ist meist mit einem hohen Stromverbrauch verbunden, da die zeitaufwändige Berechnung viele Ressourcen benötigt. [36]

PROOF-OF-STAKE (PoS) Unter der Annahme, dass Knoten mit hoher finanzieller Beteiligung (Stake) ehrlich agieren, um der Plattform nicht zu schaden und ihre finanziellen Mittel nicht zu gefährden, werden diese bei der Auswahl bevorzugt, eine Transaktion dem Ledger hinzuzufügen. Dieses Verfahren ist deutlich stromsparender als PoW, allerdings durch die Miteinbeziehung des Vermögens auch ungerechter im direkten Vergleich. [36]

DELEGATED-PROOF-OF-STAKE (DPOS) Dieses Verfahren ergänzt PoS um ein Delegierten-System, was die Anzahl an potentiellen Konsensknoten stark einschränkt und damit die Performance erhöht: Statt einen Konsens zwischen allen beteiligten Knoten zu finden, werden delegierte Knoten gewählt, die stellvertretend für andere über die Richtigkeit der Transaktionen abstimmen. Durch die geringere Teilnehmeranzahl am Konsens und die damit einhergehende, geringe Anzahl an benötigten Nachrichten, um zu einem gemeinsamen Ergebnis zu gelangen, wird die Performanz erhöht. Knoten, die bösartig handeln, können aus dem Konsens herausgewählt werden. [36]

PRACTICAL BYZANTINE FAULT TOLERANCE (PBFT) Um in der Lage zu sein, bis zu einem Drittel an bösartigen Knoten handhaben zu können ('The Byzantine generals problem', siehe [30]), müssen alle Knoten des Gesamtsystems bekannt sein. Dieses Verfahren löst das Konsensproblem, indem der Konsens in Runden eingeteilt wird und jede Runde Transaktionen in den Ledger übernommen werden. Indem die Knoten untereinander ihre Validierungsergebnisse austauschen, können ein Mehrheitsentscheid durchgeführt und damit die korrekten Transaktionen identifiziert werden. [36]

PROOF-OF-AUTHORITY (PoA) Dieses Verfahren wird meist in privaten und Permissioned Blockchains eingesetzt. Die Konsensknoten sind fest definiert und fungieren als Autorität des Gesamtsystems. Da kein Mining existiert, können Transaktionskosten minimal gehalten werden und das System kann aufgrund des einfachen Aufbaus des Konsens sehr gut skalieren. [36]

Detailliertere Informationen sowie weitere Konsensverfahren können [42] und [44] entnommen werden.

2.1.2 *Smart-Contracts*

Bei Smart-Contracts handelt es sich um Software-Code, der auf der Blockchain (onchain) auf allen Knoten ausgeführt wird und eine Zustandsänderung meist in Form von ausgehenden Transaktionen zur Folge hat. Smart-Contracts werden in einer abgeschirmten Laufzeit-Umgebung (engl.: Runtime-Environment) ausgeführt; im Falle von Ethereum spricht man von der Ethereum Virtual Machine (EVM). [4]

Um auf Daten und Informationen außerhalb des Blockchain-Netzwerkes zugreifen zu können, bedienen sich Smart-Contracts sogenannter Oracle-Services. Dabei handelt es sich um Informationsanbieter (Trusted Data Provider), die zum Beispiel Wetterdaten, Lottozahlen oder Nahverkehrsinformationen an einen Smart-Contract senden, damit dieser, basierend auf den empfangenen Daten, seine Logik ausführen und die Daten verarbeiten kann. Der grundlegende Nachteil von Oracle-Services liegt in der Vertrauensfrage: Während eine Blockchain grundsätzlich mittels Konsensverfahrens die Vertrauensfrage beantwortet, obliegt dem Besitzer bzw. Betreiber eines Oracles die Macht über die Richtigkeit der Daten. Dieser Problematik kann durch den Einsatz mehrerer, mittels eines separat implementierten Konsenses abgestimmter Oracle-Services entgegengewirkt werden. [12]

Mit dem Software-Code von Smart-Contracts können komplexe Logiken, so auch Vertragslogiken von Kauf- oder Mietverträgen, abgebildet und automatisiert abgearbeitet werden. Bei der Umsetzung und Automatisierung von juristischen Verträgen ist das jeweils geltende Recht eines Landes zu beachten: Die Form und der Aufbau sowie der abzubildende Inhalt eines Vertrages muss gewissen Normen entsprechen und alle benötigten Informationen enthalten, damit ein Vertrag rechtskräftig ist. [4]

2.1.3 *Dezentrale Apps (DApps)*

Eine **DApp** ist eine Anwendung, die auf dem Blockchain-Netzwerk dezentral ausgeführt wird. Die Applikationslogik wird dabei durch einen Smart-Contract oder durch den Zusammenschluss mehrerer Smart-Contracts abgebildet [10]. Eine **DApp** kann demnach - genauso wie ein einzelner Smart-Contract - nicht auf Informationen außerhalb der Blockchain zugreifen; es sei denn, Informationen werden durch Oracles bereitgestellt. Da **DApps** als solche keine dedizierte Benutzerschnittstelle besitzen, sondern lediglich über Blockchain-typische APIs erreichbar sind, trifft man **DApps** meist in Verbindung mit einer Web-Applikation an, die dem Benutzer die Interaktion ermöglicht [1].

Da eine Datenhaltung onchain sehr kostenintensiv ist, bietet es sich an, diese offchain zu speichern. Im Sinne einer dezentralen Anwendung bietet sich

hierbei der Einsatz von Technologien wie Inter-Planetary File System (IPFS)³ an. Daten können dezentral und kostengünstig außerhalb des Blockchain-Netzwerkes aufbewahrt, allerdings onchain eindeutig referenziert werden. In Abbildung 2.2 wird ein beispielhafter Aufbau einer DApp aufgezeigt.

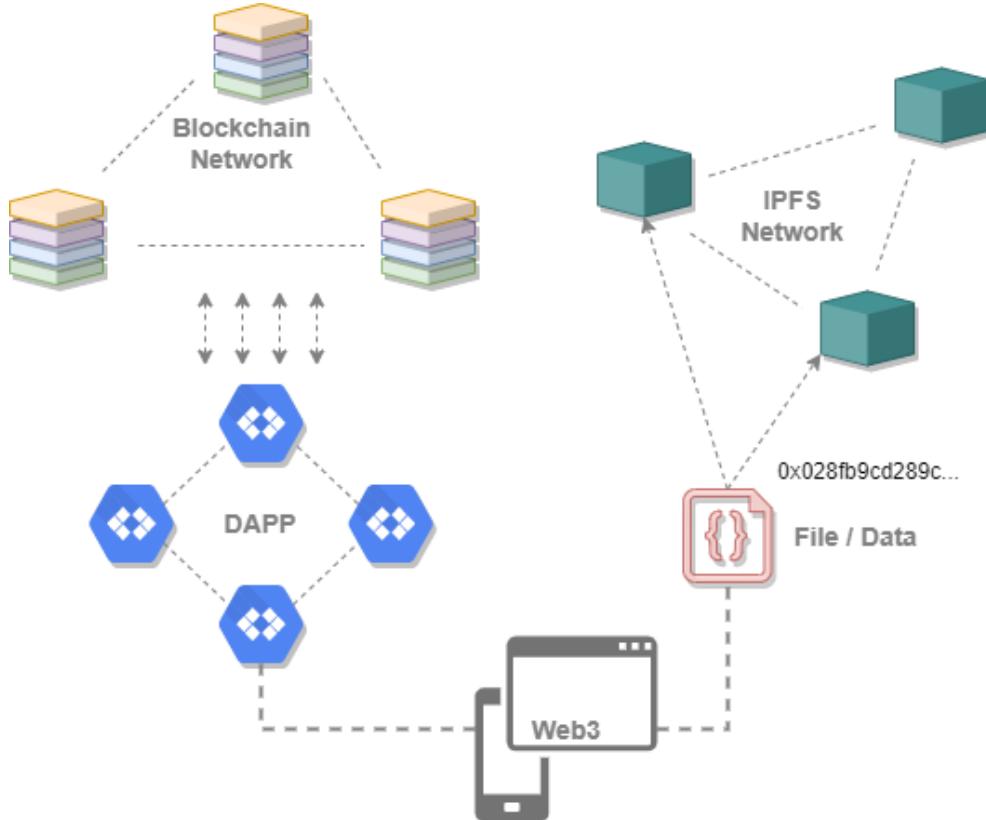


Abbildung 2.2: Aufbau von DApps

DApps haben den Vorteil, dass sie alle Stärken der Blockchain besitzen: Sie sind dezentral organisiert, manipulations- und ausfallsicher [1]. Durch Kryptowährungen wie Ether oder andere ERC20-Tokens können Zahlungsabwicklung nativ integriert werden. Auf der anderen Seite sind zum Beispiel Performanz und Ausführungskosten an die Kapazitäten und Eigenschaften des Blockchain-Netzwerkes gebunden. Damit sind zeitkritische oder Performanz-lastige Anwendungen nicht oder nur in Ausnahmefällen für eine Implementierung auf einer Blockchain geeignet.

2.1.4 Klassifizierung von Blockchains

Blockchains können nach Zheng u. a. (vgl. "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", [42]) klassifiziert werden, indem man die Sichtbarkeit von Informationen sowie die aktive Teilnahme von Netzwerknoten am Konsensmechanismus betrachtet. Ist die Block-

³ Dezentrales, verteiltes Dateisystem, basierend auf einem P2P-Netz. Dateien werden versiert und sind mittels Fingerprint(Hashing) eindeutig identifizierbar.

chain öffentlich erreichbar und können Transaktionen und Blöcke von beliebigen Knoten eingesehen werden, so handelt es sich um eine öffentliche (Public) Blockchain. Ist der Zugang zum Blockchain-Netzwerk beschränkt und können nur berechtigte Knoten Transaktionen und Blöcke einsehen, so spricht man von einer privaten (Private) Blockchain. Eine besondere Form der Private-Blockchain ist die Konsortial-Blockchain; hierbei handelt es sich oftmals um einen Zusammenschluss mehrerer Entitäten, meist Unternehmen, welche die Zugangsbeschränkung zur Blockchain verwalten. Zur besseren Verständlichkeit können Private- und Public-Blockchains analog zu Intranet (firmenintern) und Internet (weltweit für jeden zugänglich) gesehen werden.

Darüber hinaus lassen sich Blockchains laut Zheng u. a. über die Teilnahme am Konsensprotokoll klassifizieren: Ist jeder Netzwerkknoten, der die Blockchain erreichen und damit Informationen einsehen kann (unabhängig von Public oder Private), berechtigt, am Konsensverfahren teilzunehmen, so spricht man von einer beschränkungslosen (Permissionless) Blockchain. Ist das Konsensverfahren auf privilegierte Knoten beschränkt, so handelt es sich um eine zugangsbeschränkte (Permissioned) Blockchain. Die vorgestellten Klassifizierungen in Public, Private, Permissioned und Permissionless lassen sich darüber hinaus kombinieren, wodurch es vier mögliche Arten von Blockchains gibt. Abbildung 2.3 stellt diese schematisch dar und listet dazu einige bekannte Umsetzungen auf.

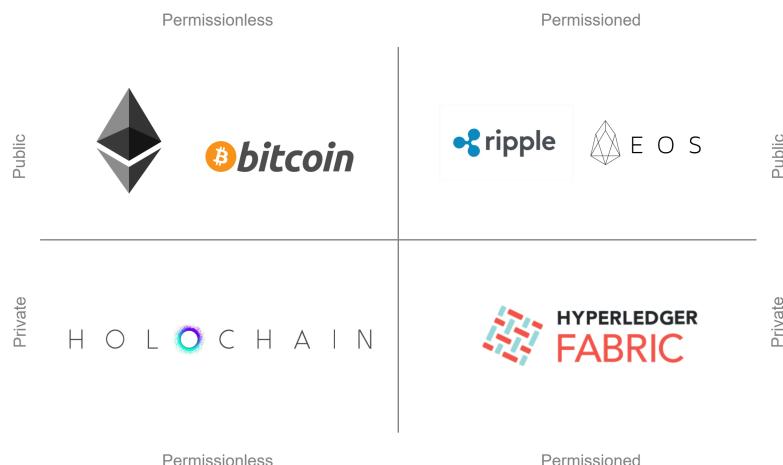


Abbildung 2.3: Taxonomie von Blockchains (vgl. [17])

Die bekanntesten Vertreter Bitcoin und Ethereum sind öffentliche und beschränkungslose Blockchains, an denen jeder teilnehmen kann und alle Daten öffentlich einsehbar sind. Die Klassifizierung ergibt sich als logische Konsequenz aus besonderen Anforderungen an die Blockchain: So können Transaktionskosten, Transaktionsgeschwindigkeiten, der Wirkungskreis der Anwendung oder das Geschäftsmodell Argumente für die Zulassungsbefreiung und beschränkte Teilnahme am Konsensverfahren sein. Daraus resultiert, dass Blockchain-Protokolle je nach gegebenen Anforderungen des Anwendungsfalls ausgewählt und abgewägt werden müssen.

2.1.5 Wallets

Einer Wallet ist ein Kontostand zugeordnet, sie besteht aus einem privaten Schlüssel (Private Key) und dem dazugehörigen öffentlichen Schlüssel (Public Key) und hat einen eindeutigen Eigentümer - den Besitzer des Private Keys. Der Public Key ist (in den meisten Fällen) die öffentliche Adresse, die für Transaktionen genutzt wird und entspricht in etwa einer Kontonummer einer Bank. Der Private Key fungiert als PIN-Nummer und ist nur dem Eigentümer der Wallet bekannt.

Multisignatur-Wallets sind Wallets, auf deren Inhalt nur durch den Einsatz mehrerer Private Keys zugegriffen werden kann. Dabei wird ein Multisignatur-Wallet von n Schlüsseln erzeugt. Um auf den Inhalt zugreifen zu können, bedarf es der Signaturen von t von n Schlüsseln. Dadurch können verschiedene Anwendungsfälle wie zum Beispiel Treuhandkonten (2 von 3), Zwei-Wege-Authentifizierungen (2 von 2) und viele weitere abgedeckt werden. [18]

Multisignatur-Wallets können entweder Teil des Blockchain-Protokolls sein und damit nativ unterstützt oder beispielsweise durch die Umsetzung mittels Smart-Contract realisiert werden. Letzteres ist dabei denkbar einfach: Es handelt sich um Code, der erst dann eine Transaktion ausführt, wenn mit t von n der hinterlegten Schlüssel unterschrieben wurde. Die Höhe von t und n ist im Code festgelegt.

2.1.6 Dezentrale Identitäten

Eine Identität zeichnet sich durch eine Menge von Informationen, Daten und Eigenschaften aus, die diese eindeutig identifizieren. Nur der Inhaber einer Identität kann mit dieser auch agieren, da er der einzige ist, der Zugriff auf die geschützten Informationen hat, die die Identität des Inhabers bestätigen. Diese können zum Beispiel ein Passwort, eine Geburtsurkunde, ein Fingerabdruck oder Ähnliches sein.

Eine dezentrale Identität ist laut [40] eine neuartige Technologie, die es dem Inhaber einer solchen erlaubt, seine Identität digital, dezentral und sicher durch den Einsatz asymmetrischer Verschlüsselung selbst zu verwalten. Sie ist kryptografisch verifizierbar und der Inhaber entscheidet selbst, welche Informationen er teilen möchte und welche nicht. Das World Wide Web Consortium (W3C) entwickelt aktuell (Stand: Dezember 2019) einen Industrie-Standard, der zur Verifizierung und Authentifizierung persönlicher Informationen vor Dritten im Web 3.0 eingesetzt werden soll und sich derzeit in der Version 1.0 befindet [39]. Eine dezentrale Identität besteht aus einer Decentralized Identifier (DID), welche weltweit einzigartig ist, und einem dazugehörigen DID-Dokument, welches Informationen über den beschriebenen Gegenstand enthält. Die folgenden Beispiele zeigen eine DID und ein dazugehöriges DID-Dokument (entnommen aus [39]).

Listing 2.1: Beispiel einer DID

did:example:123456789abcdefghi

Listing 2.2: Beispiel eines DID-Dokuments

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:example:123456789abcdefghi",
  "authentication": [
    {
      "id": "did:example:123456789abcdefghi#keys-1",
      "type": "RsaVerificationKey2018",
      "controller": "did:example:123456789abcdefghi",
      "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
    }
  ],
  "service": [
    {
      "id": "did:example:123456789abcdefghi#vcs",
      "type": "VerifiableCredentialService",
      "serviceEndpoint": "https://example.com/vc/"
    }
  ]
}
```

Durch den Einsatz von Blockchain-Technologie können **DIDs** manipulationssicher, hochverfügbar und für jeden zugänglich gespeichert werden. Die **DID** besteht aus drei Teilen: Zunächst dem Schlüsselwort 'did', welches beschreibt, dass es sich um eine **DID** handelt. Anschließend folgt die DID-Methode (im Beispiel: `example`), die definiert, wie die **DID** aufzulösen und weitere Informationen zu dieser Identität zu finden sind. Der letzte Teil ist eine ID (vgl. 2.1), die für jede Methode einzigartig ist und somit eindeutig ermittelt werden kann.

In diesem Kontext existieren sogenannte Verifiable Credentials (**VCs**), die einer **DID** von vertrauenswürdigen Instanzen ausgestellt werden können. Dabei handelt es sich um verifizierbare Berechtigungsnachweise. Der Aussteller bescheinigt dem Empfänger eine bestimmte Eigenschaft und stellt einen Service-Endpoint zur Verfügung, an dem ein Dritter diesen **VC** verifizieren kann. [39]

So kann zum Beispiel eine Universität mit ihrer eigenen **DID** 'did:hda:12345' einem Student 'did:test:sebastiankanz' ein **VC** ausstellen, welches Studenten bescheinigt, aktuell an der Universität eingeschrieben zu sein. Möchte sich ein Student nun an der Universitätsbibliothek authentifizieren, so kann er dort das **VC** der Universität vorzeigen und bekommt Zugriff auf die Bibliotheksausleihe. Die Bibliothek kann das **VC** verifizieren, indem er unter der Methode 'hda' die Universität identifiziert und anschließend die Signaturen überprüft.

2.1.7 State-Channel

Blockchains⁴ gehen aufgrund ihrer Beschaffenheit einen Kompromiss ein. Durch das Konsensprotokoll ist unabhängig von Blockgröße und Netzwerkkapazität ein natürliches Limit gegeben: Das Bitcoin-Netzwerk ist beispielsweise durch die komplexe Berechnung von Proof-of-Work (PoW) auf eine Blockzeit von 10 Minuten beschränkt. Ist die Blockgröße sehr klein, können Blöcke sehr schnell über das Netzwerk propagiert, allerdings nur wenige Transaktionen auf einmal übertragen werden. Ist die Blockgröße sehr groß, ist es sehr schwer für Knoten, sich zu synchronisieren. Dafür können mehr Transaktionen auf einmal übertragen werden.

Durch diese Limitierung von Blockgröße und Blockdauer sind im Fall von Bitcoin derzeit (Stand 01/2020) durchschnittlich etwa 7 Transaktionen pro Sekunde möglich [31]. Andere Implementierungen nutzen gegebenenfalls andere Konsensmechanismen und andere Parameter, allerdings liegen auch dort natürliche Schranken vor. Es wird deutlich, dass mit steigenden Anforderungen vor allem an die Transaktionsverarbeitung pro Zeitintervall (meistens Transactions per Second (TPS)) eine verbesserte Performanz und neue Lösungsansätze erforderlich werden. Es wird eine Lösung für die schlechte Skalierung von Blockchains gesucht. [31]

Als eine mögliche Antwort auf das Skalierungsproblem von Blockchains werden sogenannte State-Channels entwickelt. Ziel ist es dabei, jegliche Arten von Status-ändernden Operationen off-chain zu prozessieren, die typischerweise auf der Blockchain ausgeführt und onchain gespeichert werden. Dadurch können die Anzahl an Zugriffen auf die Blockchain sowie die Anzahl an Transaktionen verringert und gleichzeitig die Interaktionszeit zwischen einzelnen Parteien verbessert werden. Im Kontext von Zahlungen (Payments) werden dadurch sogenannte Micro-Payments ermöglicht; bei State-Channels, die sich auf die Zahlungsabwicklung beschränken, spricht man von Payment-Channels. Diese können schneller und günstiger als normale Transaktionen erfolgen. Die Kosten solcher Micro-Payments können sehr gering gehalten werden, da nicht alle Transaktionen auf der Blockchain gespeichert werden. [16]

Die Grundidee dabei ist folgende: Alice und Bob reservieren einen Teil ihres Vermögens auf der Blockchain, sodass sie vorerst nicht darüber verfügen können und eröffnen einen Payment-Channel zueinander. Diese Transaktion, also das Eröffnen des Payment-Channels, wird auf der Blockchain gespeichert. Das Volumen des Channels, also das Vermögen, dass Alice und Bob nun zwischen einander austauschen können, entspricht der Summe der reservierten Vermögen. Ihr gewünschtes Vermögen, welches für den Payment-Channel reserviert werden soll, kann entweder mittels Multisignatur-Wallet (vgl. Kap. 2.1.5) oder Smart-Contract (vgl. Kap. 2.1.2) reserviert werden. Alice und Bob haben nun einen State von jeweils 50 Euro. Anschließend können sich beide signierte off-chain Transaktionen schicken (also nicht über

⁴ Hinweis: Es handelt sich bei dieser Betrachtung primär um Public Blockchains unabhängig vom eingesetzten Konsensverfahrens. Das Skalierungsproblem kann allein durch die Beschränkung auf eine Private Blockchain meist gelöst werden.

das Blockchain-Netzwerk). Diese Transaktionen enthalten den neuen State: Überweist Bob 10 Euro an Alice, so ändert sich der State von Alice von 50 Euro auf 60 Euro. Schickt Bob erneut eine Transaktion von 10 Euro, so ändert sich der State von Alice auf 70 Euro. Diesen Vorgang können beide nun solange wiederholen, wie sie möchten; solange sie sich in dem Volumen von 100 Euro bewegen. Zum Schließen eines Channels senden Alice oder Bob eine Transaktion an das Blockchain-Netzwerk, welche den finalen State enthält (im Beispiel hat Alice 70 Euro und Bob 30 Euro). Für theoretisch unendlich viele Transaktionen zwischen Alice und Bob müssen lediglich die eröffnende und die schließende Transaktion des Payment-Channels onchain gespeichert werden.

Einen weiteren, großen Vorteil liefert die durch den State-Channel ermöglichte Asynchronität von Transaktionen. Befinden sich Teilnehmer nicht im Blockchain-Netzwerk (zum Beispiel durch Konnektivitätsprobleme), so können keine Transaktionen durchgeführt werden. Hängen reale Aktionen wie zum Beispiel das Öffnen einer Schranke oder das Prozessieren einer Aktion mit einer Blockchain-Statusaktualisierung zusammen, so würde bei Konnektivitätsverlust der reale Prozess zum Stillstand kommen, bis die Verbindung wiederhergestellt wird. State-Channel könnten hierbei eingesetzt werden, um eine redundante Verbindung zu schaffen, die auch bei Nicht-Erreichbarkeit der Blockchain genutzt werden könnte. Einige Beispiel-Implementierungen von State-Channels sind Bitcoins Lightning Network [35], Ethereums Raiden Network oder die Implementierung von Neo namens Trinity [41].

Eine weitere Möglichkeit, Blockchain-Anwendungen zu skalieren, kann durch den Einsatz von Side-Chains [28] geschaffen werden. Hierbei handelt es sich um separate Blockchains, die parallel zur Haupt-Blockchain (auch oft Eltern-Blockchain oder Main-Chain genannt) laufen. Um eine Side-Chain zu eröffnen, muss zunächst der Beweis erbracht werden, dass alle Assets, deren Status in der Side-Chain verändert werden sollen, auf der Main-Chain gesperrt oder reserviert sind, sodass der Eigentümer temporär nicht über diese verfügen kann (beispielsweise durch Zero-Knowledge Proofs, siehe [34]). Diese gesperrten Assets können anschließend in die Side-Chain transferiert werden. Dort kann der Status verändert werden; beispielsweise kann eine Geld-Transaktion durchgeführt werden. Soll ein Asset zurück auf die Main-Chain transferiert werden, so muss der Beweis erbracht werden, dass dieses Asset auf der Side-Chain gesperrt wurde. Dadurch werden Effekte wie das Double-Spending verhindert.

Bei Lösungsansätzen wie State-Channels und Side-Chains spricht man von dem sogenannten Layer-2 Ansätzen: Unter diesem Begriff werden Ansätze verstanden, die nicht direkt auf der Blockchain selbst (Layer-1), sondern auf einem separaten System ausgeführt werden.

2.1.8 Blockchain als Kommunikationsprotokoll

Das Open Systems Interconnection ([OSI](#)) Modell gilt seit Mitte der 80er-Jahre als Standard zur Einordnung von Netzwerkprotokollen. Es wurde von der International Organization for Standardization ([ISO](#)) entwickelt und besteht aus sieben Schichten ([43], [3]):

PHYSICAL LAYER Die Übertragung des Bit-Datenstroms über ein physikalisches Medium (Hardware) findet auf dieser Ebene statt.

DATA LINK LAYER Diese Schicht kapselt Daten in Datenframes; es werden grundlegende Funktionalitäten zur Fehlererkennung und Fehlerbehebung bereitgestellt. Bekannte Protokolle dieser Ebene sind zum Beispiel Ethernet und Address Resolution Protocol ([ARP](#)).

NETWORK LAYER Diese Schicht kapselt Daten in Datenpaketen und implementiert Sequenznummern, Flusskontrolle und Funktionalitäten fürs Routing.

TRANSPORT LAYER Diese Schicht ist zuständig für die Ende-zu-Ende Übermittlung von Daten, die sie vom Session Layer empfängt. Die Daten werden in sogenannte Segmente unterteilt und über das Netzwerk versendet und auf der Empfängerseite ebenfalls von der Transport-Schicht wieder zusammengesetzt.

SESSION LAYER Kommunikationskanäle, Sessions genannt, werden auf dieser Schicht geöffnet, geschlossen und verwaltet.

PRESENTATION LAYER Diese Schicht ist zuständig für Datenkonvertierungen, -kompressionen und stellt Funktionalitäten wie Ver- und Entschlüsselung bereit.

APPLICATION LAYER Diese Schicht stellt die Schnittstelle zum Benutzer dar.

Bei einem dezentralen Netzwerk wie [DLT](#) liegt es nahe, eine Einordnung in das [OSI](#) Modell durchzuführen. Dazu werden die verschiedenen Bestandteile eines [DLTs](#) vorgestellt und den Schichten des [OSI](#) Modells zugeordnet. Die Schichten eins bis drei (Physical, Data Link und Network) werden hierbei nicht betrachtet, da die Kommunikation über das Internet erfolgt und auf bekannten Protokollen wie Ethernet und IP aufbaut.

Eine Blockchain basiert auf einem [P2P](#)-Netz, in dem alle Knoten miteinander verbunden sind und miteinander kommunizieren können. Diese Kommunikation geschieht nach dem Ende-zu-Ende Prinzip und nicht nach dem Punkt-zu-Punkt Prinzip. Die [P2P](#)-Kommunikation erfolgt meist über die entsprechenden Transportprotokolle TCP oder UDP, welche Daten als Segmente zwischen Sender und Empfänger austauschen. Demnach findet die [P2P](#)-Kommunikation auf dem Transport-Layer (Schicht 4) statt.

Das Konsensprotokoll legt zum einen fest, welche Knoten am Konsensverfahren partizipieren dürfen und welche nicht. Dazu werden Verbindungen

zu anderen Knoten aufgebaut und ggfs. wieder geschlossen. Zum anderen wird definiert, welchem Schema die Kommunikation folgt. Eingehende Datensegmente der P2P-Schicht werden entgegengenommen und in Form von Transaktionen gemäß der Konsensregeln verarbeitet. Die Ergebnisse werden wiederum an die P2P-Schicht zurückgespiegelt und über das Netzwerk an die anderen Knoten publiziert. Diese Vorgänge sind in den Session-Layer des OSI-Modells einzuordnen.

Die virtuelle Maschine einer Blockchain sorgt dafür, dass die Verarbeitungsschritte auf allen Knoten zum selben Ergebnis führen. Dazu werden Smart-Contracts aus Transaktionen extrahiert, in Byte-Code übersetzt und in separierten Laufzeitumgebungen ausgeführt. Verschlüsselte Nutzdaten von Transaktionen werden ebenfalls in dieser Laufzeitumgebung entschlüsselt. Die Funktionen der Smart-Contracts werden der nächst-höheren Schicht zur Verfügung gestellt. Darüber hinaus werden Daten, die in Byte-Form aus Smart-Contracts entstehen, konvertiert und in Form von Transaktionen an die untere Ebene weitergereicht. Diese Funktionalitäten können in den Presentation-Layer (Schicht 6) eingeordnet werden.

Die Schnittstellen zum Benutzer stellen Top-Level-APIs dar, über die der Benutzer mit der Blockchain kommunizieren kann. Sendet ein Benutzer eine API-Anfrage an einen Node, kann dieser gemäß des Protokoll-Stacks Aktionen in die unteren Schichten weiterleiten und in das Netzwerk propagieren. API-Calls werden in diesem Kontext meist von einer Web-Anwendung abgesendet und die Ergebnisse mittels User-Interface (UI) dem Benutzer präsentiert. Damit stellen die genannten API-Calls eine Schnittstelle zum Benutzer bzw. zur Benutzeranwendung dar und können dem Application-Layer (Schicht 7) zugeordnet werden.

In Abbildung 2.4 werden die zugeordneten Schichten der Blockchain noch einmal aufgezeigt und mit den sieben Schichten des OSI-Modells dargestellt.

Der Duden [19] definiert den Begriff Protokoll als „Festlegung von Standards und Konventionen für eine reibungslose Datenübertragung zwischen Computern“. Ein Kommunikationsprotokoll ist gemäß des Gabler Wirtschaftslexikons [22] „eine Übermittlungsvorschrift bei der Datenübertragung, die die gesamten Festlegungen für Steuerung und Betrieb der Datenübermittlung in einem Übermittlungsabschnitt [...] umfasst“. Diese Definitionen zusammen mit der Einordnung der Blockchain-Technologie in das OSI-Modell suggerieren, dass es sich dabei um ein Kommunikationsprotokoll handelt. Zusammen mit der Zahlungsabwicklung und der Abbildung von Eigentumsverhältnissen beziehungsweise von Eigentumsübergängen spricht man auch von einem sogenannten „Value Exchange Protocol“[7].

Durch die Einordnung in das OSI-Modell kann auch die Sinnfrage beantwortet werden, weshalb die Blockchain-Technologie eine vielversprechende Alternative zu klassischen IT-Systemen darstellt: Betrachtet man die Technologie objektiv, abseits des Hypes und des Anwendungsfalls der Kryptowährungen, so erkennt man eine junge Technologie mit hohem Potenzial. Die Blockchain als Kommunikationsprotokoll gibt dem modernen Softwa-

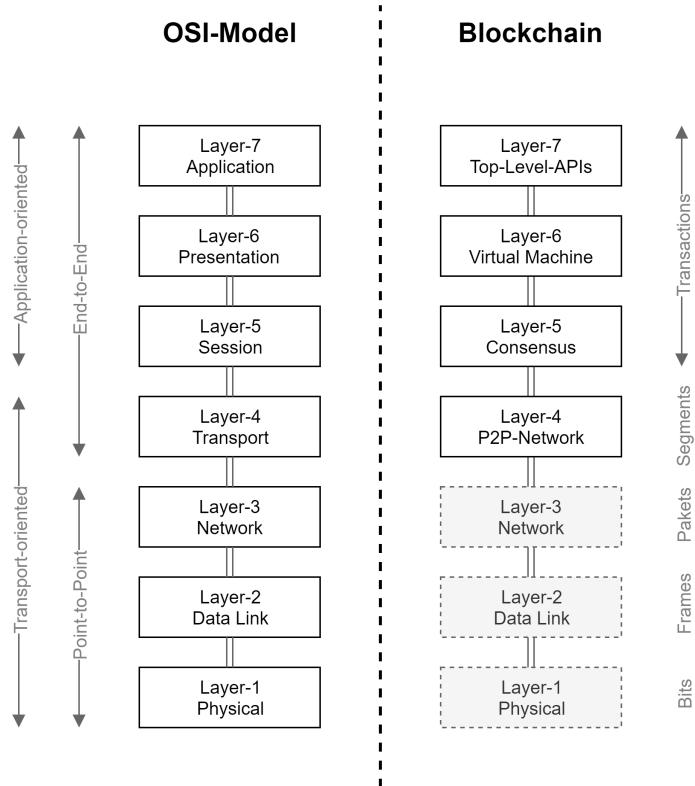


Abbildung 2.4: Die Blockchain-Layer im Kontext des OSI-Modells

reentwickler umfangreiche Werkzeuge und Out-of-the-Box Funktionalität über vier Schichten des **OSI**-Modells hinweg an die Hand. Eine dezentrale Plattform mit integrierter Datenbank, Security, Ver- und Entschlüsselung, P2P-Netzwerkkommunikation, Entwicklungs- und Laufzeitumgebung für dezentrale Anwendungen, sicherer Zahlungsabwicklung und hoher Verfügbarkeit ist oftmals per Knopfdruck binnen Sekunden erstellt. Alle diese Bestandteile und Funktionalitäten sind in der technischen Spezifikation einer jeden Blockchain in Form eines Kommunikationsprotokolls enthalten und klar definiert.

2.2 INTERNET OF THINGS

Der Begriff Internet der Dinge - kurz **IOT** - ist ein Sammelbegriff und bezeichnet die Vernetzung von Gegenständen untereinander (meist über das Internet). Es wird eine autonome Machine-to-Machine (**M2M**)-Kommunikation ermöglicht, die wiederum den Automatisierungsgrad in dem jeweiligen Einsatzgebiet erhöht. Das bedeutet, dass die Kommunikation zwischen den **IOT**-Geräten selbstständig erfolgt, also ohne das Eingreifen eines Menschen. Nach [37] lässt sich das Themenfeld **IOT** in zwei Bereiche untergliedern: Consumer **IOT** (**CIOT**) und Industrial **IOT** (**IIOT**). **CIOT** findet Anwendungen im privaten Umfeld, vor allem geht es hier um Smart-Home und die damit verbundenen Applikationen: Smart-Gardening, Smart-Lights, intelligente Türschließsysteme und Heizungssteuerungen. **IIOT** fokussiert sich auf

den kommerziellen Bereich und versucht Anwendungen im deutlich größeren Stil zu entwickeln: Die Bereiche Automotive, Energie und Supply-Chain sind hierbei einige wichtige Vertreter und treten als Smart-Factory, Smart-City, Connected-Cars und Weitere in Erscheinung. Die Abbildung 2.5 gibt eine Übersicht über die grobe IOT-Architektur im Kontext von DLT.

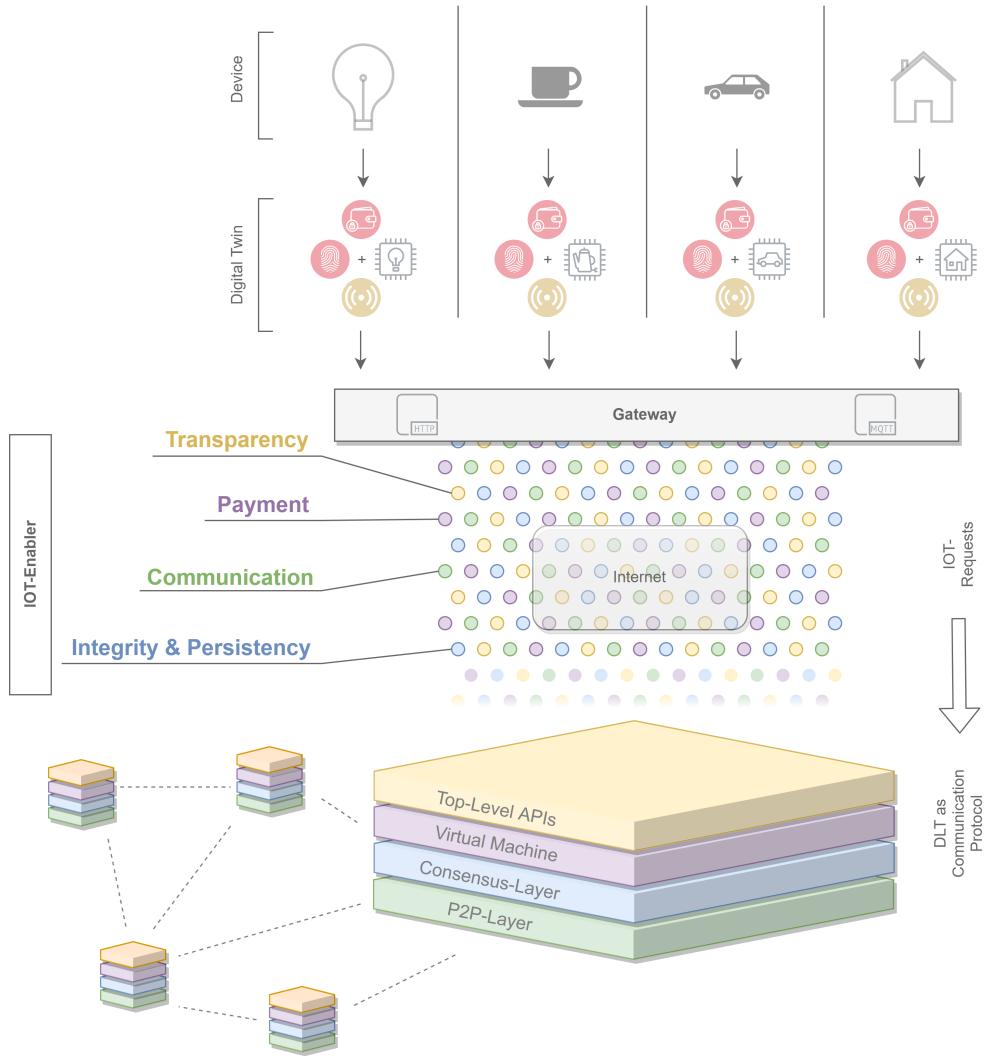


Abbildung 2.5: Schematische Darstellung von IOT im Kontext von DLTs

Um physische Geräte miteinander zu vernetzen, werden sogenannte digitale Zwillinge (engl.: Digital Twins) erzeugt. Dabei handelt es sich um virtuelle Abbildungen der Geräte, die mittels Sensoren und Aktoren miteinander verbunden sind. Somit können Zustandsänderungen vom physischen Teil zum virtuellen Teil übertragen werden und umgekehrt. Jedes Gerät besitzt eine eindeutige Identität, die im Blockchain-Umfeld mittels dezentraler Identität abgebildet wird (vgl. 2.1.6). Darüber hinaus und abhängig vom Anwendungsfall besitzen Geräte eine Wallet, um automatisierte Bezahlvorgänge M2M durchzuführen. Jedes Gerät hat eine bestimmte Funktionalität und trägt einen Teil zum IOT-System bei, wobei die Geräte über ein lokales Gate-

way mit dem Internet verbunden sind. Dabei kann es sich um einen WLAN-Router, einen Mobilfunk-Chip oder eine andere Art von Gateway handeln. Die Kommunikation erfolgt über gängige Kommunikationsprotokolle wie MQTT, HTTP oder - wie im Falle von Blockchain - über das Blockchain-Protokoll. **IOT**-Anfragen werden über das Blockchain-Netzwerk prozessiert; aus Sicht eines **IOT** Geräte-Herstellers und Konsumenten formulieren Christidis und Devetsikiotis in [14] die Vorteile davon wie folgt:

„From the manufacturer's side, the current centralized model has a high maintenance cost consider the distribution of software updates to millions of devices for years after they have been long discontinued. From the consumer's side, there is a justified lack of a trust in devices that phone home in the background and a need for a security through transparency approach.“ Christidis und Devetsikiotis nennen zwei zentrale Kerneigenschaften eines Distributed Ledgers: Zum einen die Verteilung und die einfache Anbindung und Erreichbarkeit von **IOT**-Geräten, die die Wartung seitens des Herstellers erleichtern können. Zum anderen sprechen die Autoren die Vertrauensfrage seitens der Kunden in Bezug auf Datensicherheit und Privatsphäre an. Hier kann die Blockchain-Technologie nach Christidis und Devetsikiotis „Sicherheit durch Transparenz“ erzielen und für eine größere Akzeptanz sorgen.

Der Einsatz von Blockchain-Technologie ist allerdings nicht immer ratsam oder möglich. So kann beispielsweise aufgrund des Anwendungsfalls oder aufgrund von technischen Beschränkungen und Gegebenheiten der Einsatz eines **DLTs** im **IOT**-Umfeld unvorteilhaft sein. Erstes könnte zum Beispiel eine Smart-Home Anwendung sein, die eine Temperaturregelung und Überwachung der eigenen vier Wände vorsieht. Ein dezentraler Ledger wäre hier überdimensioniert und für diesen Zweck überqualifiziert. Der Aufwand stünde in keinem Verhältnis zum Nutzen. Darüber hinaus zeigt dieser **IOT**-Anwendungsfall auch keine Charakteristika einer **DLT**-Anwendung auf: Es handelt sich um eine einzige beteiligte Partei in einem vertrauten Umfeld mit nur wenigen Endgeräten. Auf der anderen Seite können technische Hürden den Einsatz von **DLT** verhindern. Gerade im Automotive-Bereich ist die Verarbeitung von Sensor- und Aktordaten in Echtzeit ein kritischer Punkt. Dezentrale Ledger eignen sich hierzu nicht, da sie nicht in der Lage sind, zeitkritische Anwendungen zu betreiben.

Es wird deutlich, dass die Beschaffenheit des **IOT**-Anwendungsfalls sehr entscheidend dazu beiträgt, ob der Einsatz einer Blockchain-Lösung sinnvoll ist oder nicht. Die Blockchain bietet aufgrund ihrer Kern-Eigenschaften einige **IOT**-Enabler nativ an: Transparente und überprüfbare Prozesse aller Geräte, integrierte und automatisierte **M2M**-Zahlungsabwicklung, **P2P**-Kommunikation sowie Datenintegrität und -persistenz.

2.2.1 Digitaler Zwilling

Ein digitaler Zwilling (engl. Digital Twin) ist nach Sallaba, Siegel und Becker eine virtuelle Kopie physikalischer Objekte. Digitale Zwillinge werden in automatisierten IT-Prozessen benötigt, da sie als Schnittstelle zwischen

physischer Welt und deren digitalen Pendant fungieren. Der Zustand eines physikalischen Objekts wird in den digitalen Zwilling gespiegelt, welcher wiederum eine digitale Zustandsüberwachung und die Manipulation seines physischen Gegenstücks ermöglicht. [37]

Der Ansatz von digitalen Zwillingen und die Thematik IOT haben gegenseitig enormen Einfluss aufeinander und befähigen einander zu neuen Anwendungsfällen. Diese können unter Anderem die Abbildung von Fabriken und Maschinen in digitale Automatisierungsprozesse sein, indem die Geräte und Teile mit Sensoren, Konnektivität und einer Steuerungslogik ausgestattet werden. Dadurch können Predictive Maintenance, Bedarfsplanungen und Prozessoptimierungen durchgeführt werden.

Im Umfeld Blockchain und IOT werden die Begriffe Digital Twin und Dezentrale Identität oft synonym verwendet, da beide ein physikalisches Objekt virtuell abbilden. Dezentralen Identitäten beschreiben als W3C-Standard die konkrete Umsetzung, wie virtuelle Identitäten nach der Idee eines Digital Twins standardisiert erzeugt und verwaltet werden können.

VERWANDTE FORSCHUNGSSARBEITEN

Die Themenbereiche **DLT** und **IOT** sind bereits an vielen Stellen untersucht und beschrieben worden. Darüber hinaus existieren auch einige Werke, die sich mit den Synergien zwischen beiden Themenbereichen befassen.

In "A Review on the Use of Blockchain for the Internet of Things" ([20]) werden **IOT**-Szenarien vorgestellt, die mit Blockchain umsetzbar sind. Es werden Anwendungsfälle aus den Bereichen Gesundheit, Logistik und Smart-City aufgezeigt. Darüber hinaus gehen die Autoren Fernández-Caramés und Fraga-Lamas auf die praktischen Limitierungen ein, die durch Blockchain-Lösungen entstehen und beschreiben, an welchen Stellen weitere Forschung betrieben werden muss. Das Resultat ist, dass die Autoren keine allgemeingültige Blockchain-Lösung für **IOT**-Anwendungsfälle identifizieren konnten, die Technologie aber ihrer Meinung nach großes Potential mit sich führe.

Eine ausführliche Untersuchung vieler Konsensalgorithmen hinsichtlich Tauglichkeit für **IOT** wurde von Salimitari und Chatterjee in "A Survey on Consensus Protocols in Blockchain for IoT Networks" ([36]) durchgeführt. Darüber hinaus werden einige der bekanntesten DLT-Implementierungen wie Hyperledger Fabric, Corda, Ethereum, Bitcoin und weitere gegenübergestellt und hinsichtlich Skalierbarkeit, Durchsatz, Latenz und weiteren untersucht. Es werden gewünschte Eigenschaften identifiziert, die eine **DLT** mitbringen sollte, um für Anwendungsfälle im **IOT**-Umfeld geeignet zu sein. Die Autoren Salimitari und Chatterjee unterscheiden nicht nach unterschiedlichen Anforderungen verschiedener Anwendungsfälle sondern betrachten **IOT** als Gesamtes. Das Fazit lautet, dass es derzeit keine konkrete **DLT**-Implementierung gebe, die alle Anforderungen von **IOT** vollumfänglich erfülle. Es müsse ein bestehender Konsensalgorithmus erweitert oder die Vorteile verschiedener Implementierungen kombiniert werden.

In "Blockchain as a Service for IoT" ([38]) wird untersucht, wo Blockchain-Knoten in einem **IOT**-Umfeld gehostet werden können. Die Autoren Samaniego und Deters beschreiben, dass die Umsetzung eines Blockchain-Knoten auf einem **IOT**-Device aufgrund von fehlender Rechenleistung, hohem Stromverbrauch und geringer Bandbreite keine ratsame Lösung sei. Es wird die Umsetzung mittels Cloud- oder Fog-Computing vorgeschlagen. Als Ergebnis von Performance-Messungen kommen die Autoren zu dem Schluss, dass das Fog-Computing eine bessere Lösung darstelle als die Cloud-Variante.

Die Autoren Han, Gramoli und Xu von "Evaluating Blockchains for IoT" ([23]) sind der Überzeugung, dass Konsensalgorithmen, die auf dem Byzantinischen Fehler basieren, Potential bieten, um hoch-skalierende Anwendungen zu betreiben und geeignet für **IOT** zu sein. Dazu untersuchen sie verschiedene Byzantine Fault Tolerance (**BFT**) Konsensalgorithmen und führen Performance-Tests durch. Die abschließende Erkenntnis der Autoren ist,

dass weitere Forschung zur Lösung des Konsensproblems im **IOT**-Umfeld nötig sei.

Nach den Autoren Maroufi, Abdolee und Tazehkand von "On the Convergence of Blockchain and Internet of Things (IoT) Technologies" ([32]) können **IOT** und **DLT** voneinander profitieren, man müsse jedoch zunächst Lösungen für Probleme wie den hohen Ressourcenverbrauch, zeitliche Verzögerungen, Bandbreite und Weitere lösen. Dazu beschreiben sie die einzelnen Komponenten sowie gängige Konsensverfahren einer Blockchain. Es werden Konsensverfahren und bestehende **DLTs** vorgestellt und nach Aspekten wie Durchsatz, Latenz, Sicherheit und Ressourcenverbrauch untersucht. Die Autoren unterscheiden nicht in unterschiedliche **IOT**-Anwendungsfälle und kommen zu dem Ergebnis, dass einheitliche Protokolle für **IOT**-Anwendungen auf **DLTs** definiert werden müssen und weitere Forschung besonders im Umfeld Konsensmechanismen notwendig sei.

ANWENDUNGSFALL: VERMIETUNG VON HAUSHALTSGERÄTEN NACH DEM PAY-AS-YOU-USE PRINZIP

Qualitativ sehr hochwertige Haushaltsgeräte und Geräte für den professionellen Einsatz im Gastronomie-Umfeld haben hohe Anschaffungskosten, die sich der Privatanwender oder der Inhaber eines kleinen Gewerbes oftmals nicht leisten kann. Ein professioneller Kaffeevollautomat, eine leistungsfähige Spülmaschine oder eine Waschmaschine, die für hohe Kapazitäten ausgelegt ist, können Anschaffungskosten im vier bis fünfstelligen Euro-Bereich haben. Eine naheliegende Möglichkeit besteht hier bei der Nutzung von Anbietern, die Haushaltsgeräte für eine monatliche oder jährliche Gebühr vermieten. So gibt es beispielsweise Anbieter für Kaffeemaschinen wie Tchibo oder Nespresso, die ihre Produkte direkt vermieten, oder Anbieter, die als Zwischenhändler fungieren und sich auf die Vermietung von Haushaltsgeräten verschiedener Hersteller spezialisiert haben. Dabei kommen klassische Miet- und Bezahlmodelle zum Einsatz, wobei es sich meistens um monatliche oder jährliche Mietgebühren handelt. Einen neuartigen Ansatz verfolgt das Unternehmen Winterhalter mit ihrem Pay-per-Wash Ansatz (vgl. [45]). Hier bezahlt der Kunde keine monatliche Mietgebühr, sondern pro Waschgang; die Berechnung erfolgt also auf dem tatsächlichen Verbrauch des Kunden und nicht auf einer kalkulierten Pauschale.

Dieses Kapitel beschreibt einen IOT-Anwendungsfall, der die oben beschriebene Problematik aufgreift und das von der Firma Winterhalter eingeführte Pay-per-Wash Bezahlmodell einen Schritt weiterführt. Dabei interagieren verschiedene Stakeholder miteinander nach einem Pay-as-You-Use Prinzip auf einer einheitlichen Plattform.

4.1 BESCHREIBUNG

Kunden mieten Haushaltsgeräte (im Consumer-Bereich oder für den professionellen Einsatz) wie Kaffeemaschinen oder Waschmaschinen je nach Anbieter zum Nulltarif von verschiedenen Herstellern, die ihre Geräte auf einer Plattform zur Miete anbieten. Der genaue Verbrauch (Anzahl Kaffees, Menge an gewaschener Wäsche, Wasserverbrauch, etc.) wird mittels integrierter Sensoren an den Geräten erfasst und auf der Plattform persistiert. Damit wird ein genaues, vom tatsächlichen Verbrauch abhängiges Abrechnungsmodell umgesetzt: Kunden zahlen nur das, was sie auch wirklich verbrauchen. Regelmäßige Reinigungen seitens der Kunden werden erfasst und durch ein entsprechendes Rabattmodell verrechnet. Serviceleistungen wie Wartung und Reparatur durch entsprechende Dienstleister können über die zugrundeliegende Plattform geplant, gesteuert und abgerechnet werden.

Die Lieferung von Geräten, Ersatzteilen und Konsumgütern wie Kaffee oder Waschmittel erfolgt durch Lieferanten. Die Bestellung und Abrechnung wird über die Plattform koordiniert.

Die folgende Abbildung 4.1 veranschaulicht den erläuterten Anwendungsfall.

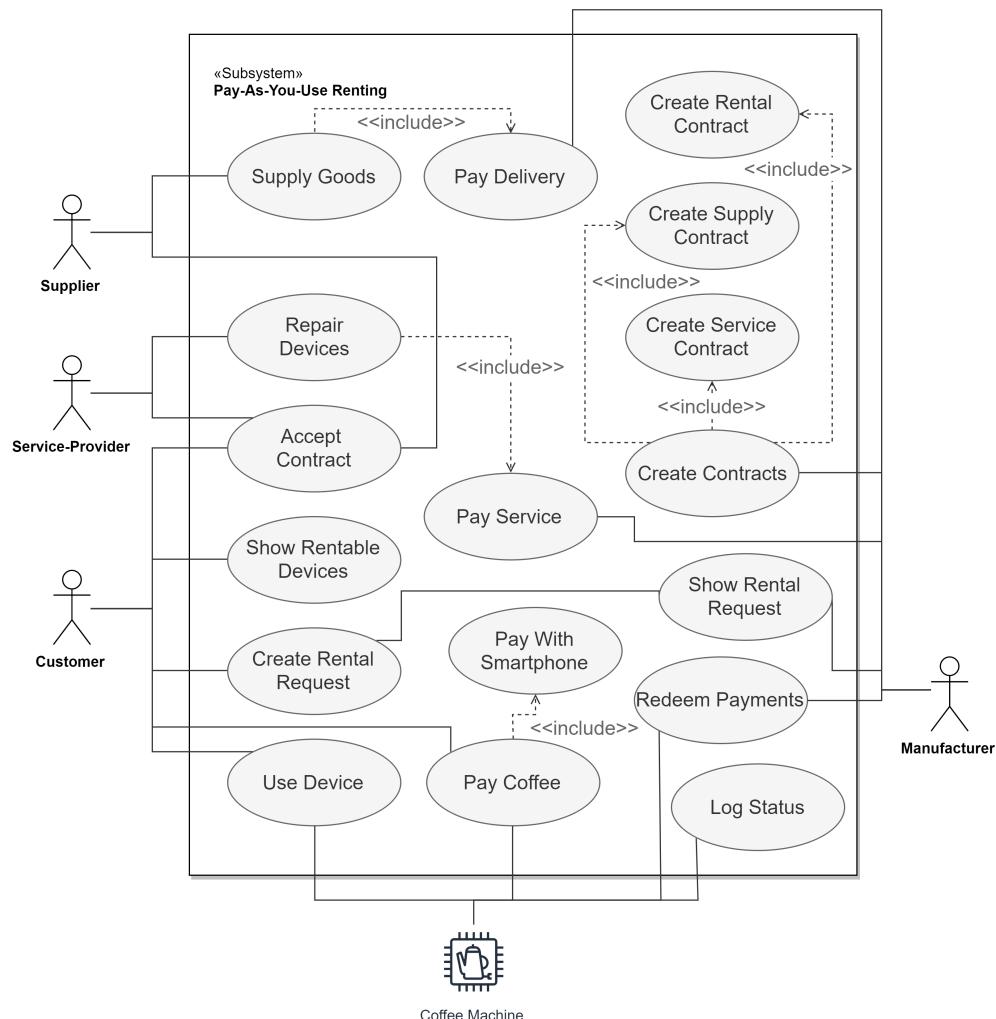


Abbildung 4.1: UML-Anwendungsfalldiagramm

Der vorgestellte Anwendungsfall lässt sich dem Teilgebiet **IiOT** (vgl. Kapitel 2.2) zuordnen und beinhaltet das Zusammenspiel mehrerer Stakeholder:

HERSTELLER Der Hersteller der Geräte entwickelt und produziert die zu vermietenden Haushaltsgeräte und bietet diese zur Vermietung an Kunden auf der Plattform an. Er vertreibt Ersatzteile sowie Pflege- und Zusatzprodukte zu seinen Geräten, die Kunden und Service-Dienstleister erwerben können. Die vermieteten Geräte des Herstellers können Service-Dienstleister selbstständig und automatisiert für eine Reparatur oder eine Wartung beauftragen. Die Beauftragung und Abrechnung erfolgt über die Plattform. Für vermietete Geräte erhält

der Hersteller nach einem Pay-as-You-Use Prinzip eine Bezahlung der Kunden entsprechend ihres Verbrauches.

LIEFERANT Der Lieferant ist für die Lieferung der Geräte und Zusatzprodukte an die Kunden und Service-Dienstleister zuständig. Er holt die Ware beim Hersteller ab und liefert diese aus; die benötigten Adressinformationen sind auf der Plattform hinterlegt. Die Bezahlung für die Auslieferung erfolgt über die Plattform und berechnet sich automatisch über die Distanz der Lieferstrecke und der Abmessung der Ware.

KUNDE Der Kunde mietet Geräte vom Hersteller. Die Bestellung und Abrechnung erfolgt über die Plattform nach einem Pay-as-You-Use Prinzip. Die regelmäßige Reinigung der Geräte wird auf der Plattform protokolliert. Bei Einhaltung der vorgeschriebenen Reinigungsintervalle erhält der Kunde eine vertraglich festgelegte Gutschrift, bei Nicht-Beachten eine entsprechende Gebühr. Darüber hinaus kann der Kunde Konsumgüter wie Kaffee und Reinigungsmittel über die Plattform bestellen; dies geschieht vollautomatisch über das Gerät: Sobald die Menge des Produktes ein gewisses Limit unterschreitet, beauftragt das Gerät selbstständig den Kauf und die Anlieferung der Produkte über die Plattform.

SERVICE-DIENSTLEISTER Der Service-Dienstleister ist zuständig für die Wartung und Reparatur der Geräte und wird von den Geräten über die Plattform beauftragt.

Die Abbildung 4.2 zeigt den groben Ablauf beginnend mit der Mietanfrage eines Kunden bis zur monatlichen Bezahlung der Teilnehmer für ihre Leistungen.

4.2 TECHNISCHE LÖSUNGSSKIZZE

In dieser Arbeit wird der oben beschriebenen Anwendungsfall basierend auf einer **DLT**-Lösung prototypisch umgesetzt. Neben den beteiligten Stakeholdern besteht das Gesamtsystem aus einem Frontend, das jedem Stakeholder die für ihn relevanten Funktionen zur Verfügung stellt und Informationen anzeigt. Das Backend des Systems besteht aus einer **DLT**-Lösung¹.

4.2.1 Endgeräte

Jedes Gerät besitzt eine Wallet und damit einen eindeutigen Public-Key sowie eine eindeutige Referenz zu dessen Eigentümer (Hersteller). Befindet sich ein Gerät in Vermietung, so existiert zwischen dem Mieter (Kunde) und dem Vermieter (Hersteller) ein Vertrag, der auf der Plattform persistiert wird. Das Gerät hat über eine Remote Procedure Call (**RPC**)-**API** Zugriff auf diese

¹ Die konkrete Implementierung, die als Backend-System eingesetzt wird, wird im Laufe dieser Arbeit ermittelt.

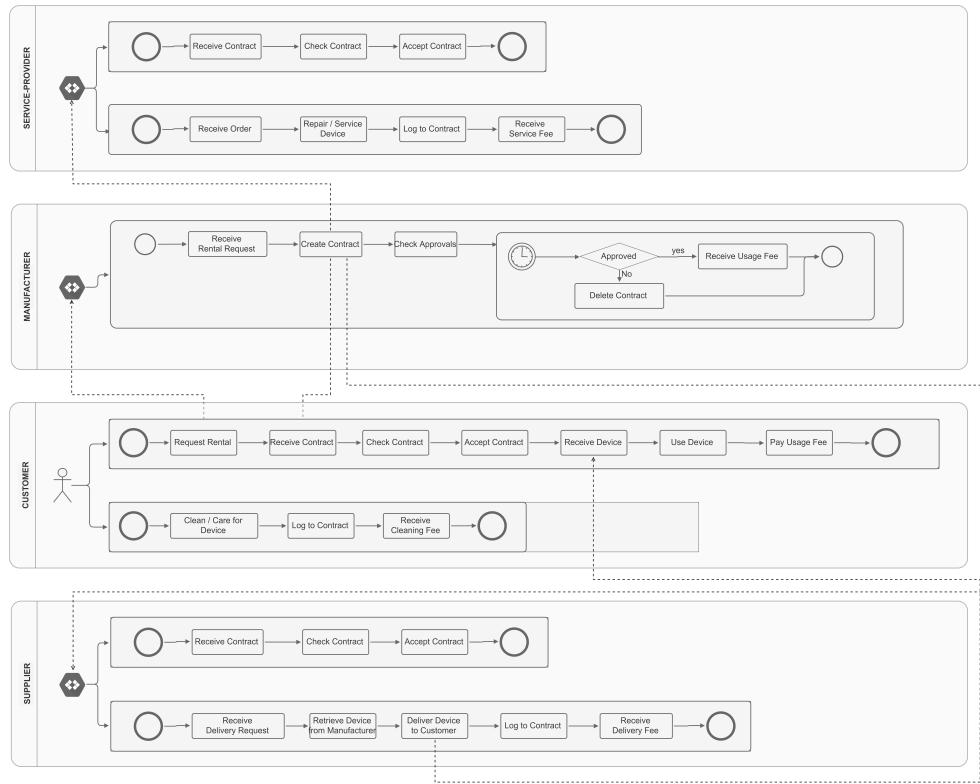


Abbildung 4.2: Aktivitätsdiagramm - Ablauf des Anwendungsfalls aus Sicht der Stakeholder

Plattform und damit auf den Vertrag, in dem wichtige Informationen zu den Rahmenbedingungen wie der Dauer des Vertragsverhältnisses oder die Kosten einer verbrauchten Einheit enthalten sind. Die Sensoren zum Registrieren des Verbrauchs und des Gerätestatus befinden sich auf dem Gerät selbst. Diese melden alle gesammelten Daten an eine Sammelstelle am Gerät. Dort werden die Daten aufbereitet, nach der Geräte logik verarbeitet und gesammelt. In einem regelmäßigen Intervall meldet das Gerät alle relevanten Daten wie Nutzung, Reinigungs- und Wartungsarbeiten und sonstige Informationen an den verknüpften Vertrag, der wiederum die entsprechenden Geld-Transfers in die Wege leitet (siehe unten). In Abbildung 4.3 wird ein Endgerät schematisch dargestellt.

4.2.2 Verträge

Verträge (Mietverträge, Service-Verträge, Lieferverträge) werden von allen beteiligten Parteien digital unterschrieben und im Backend gespeichert. Sie enthalten verschiedene Informationen, unter anderem über die Vertragslaufzeit, die Kosten sowie die zu erbringenden Leistungen der Parteien. Der Vertrag beinhaltet Mechanismen zur Begutschriftung und zur Belastung der Konten aller Beteiligten; die folgende Auflistung nennt alle wichtigen Geld-Transfers:

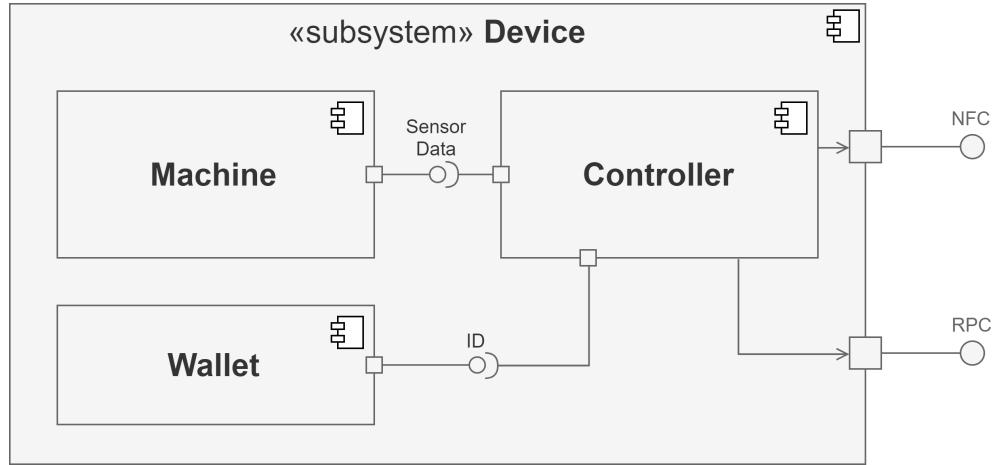


Abbildung 4.3: Aufbau und Bestandteile eines Endgeräts

- Nutzung durch den Kunden (Sender ist der Kunde, Empfänger ist der Hersteller)
- Reinigung durch den Kunden (Sender ist der Hersteller, Empfänger ist der Kunde)
- Wartung durch den Service-Dienstleister (Sender ist der Hersteller, Empfänger ist der Service-Dienstleister)
- Lieferung durch den Lieferanten (Sender ist der Absender, Empfänger ist die Lieferant)

4.2.3 Benutzerschnittstelle

Das Frontend stellt eine grafische Benutzerschnittstelle bereit, die je nach Stakeholder die relevanten Informationen und Funktionalitäten anzeigt. Um an der Plattform teilnehmen zu können, muss ein Registrierungsprozess durchlaufen und die Rolle bestimmt werden (Hersteller, Kunde, ...). Jeder Rolle ist der Zugriff auf eine Ansicht gestattet:

HERSTELLER-ANSICHT Eine Übersicht über alle Geräte sowie deren Status, ob sie sich derzeit in Vermietung befinden, gibt dem Hersteller Aufschluss über die momentane Gesamtlage. Laufende Verträge können eingesehen und aktuelle Mietanfragen bearbeitet werden.

KUNDEN-ANSICHT Die gemieteten Geräte sowie die damit verbundenen, laufenden Verträge werden angezeigt. Es besteht Transparenz über Verbrauchs- und Statusinformationen, die die Geräte an die Plattform übermitteln. Laufende Kosten und aktueller Verbrauch werden übersichtlich dargestellt. Es können Verträge gekündigt und neue Geräte angemietet werden.

SERVICE-DIENSTLEISTER-ANSICHT Eine Übersicht über alle aktuell laufenden Service-Verträge wird angezeigt. Alle Meldungen über Service-

Anfragen und Aufträge werden aufgelistet. Die Einnahmen durch Reparaturen und Services sowie der Kontostand werden detailliert dargestellt.

LIEFERANTEN-ANSICHT Eine Übersicht über alle aktuell laufenden Lieferverträge wird angezeigt. Die Einnahmen durch Auslieferungen sowie der Kontostand werden detailliert dargestellt.

4.2.4 *Backend*

Als dezentrale Plattform verwaltet und speichert das Backend alle Verträge sowie die Identitäten, Konten (Wallets) und Interaktionen der oben aufgelisteten Stakeholder. Die Implementierung auf einer **DLT** kann in zwei verschiedenen Ausprägungen erfolgen, welche im Folgenden kurz dargelegt werden:

Die einfachste Lösung, eine **DLT** zur Versionierung und Speicherung von Daten einzusetzen, entspricht einer simplen, dezentralen Hash-Datenbank. Hierbei wird der Status, bestehend aus Mietverträgen, Kontoständen, Benutzerinteraktionen und weiteren, als Hashwert abgebildet und in der **DLT** persistiert. Somit wird ein einfaches Logging ermöglicht; die Stärken einer **DLT** werden allerdings nicht eingesetzt.

Die zweite Variante setzt die Stärken einer **DLT** geschickt ein und geht weit über das einfache Dokumentieren von Revisionsständen hinaus: Informationen wie Benutzerinteraktionen, Miet- und Service-Verträge werden in die Blockchain geschrieben. Darüber hinaus geschieht die Vertragsabwicklung wie Zahlungstransaktionen, Vertragslogiken, etc. direkt auf der Blockchain. Es werden umfangreiche Geschäftslogiken abgebildet und manipulationssicher verarbeitet. Zahlungen werden instantan ohne Integration eines Drittanbieters wie zum Beispiel PayPal oder Kreditkartenanbieter abgewickelt und können nachvollziehbar und transparent persistiert werden.

Zusammengefasst bedeutet das, dass die optimale Lösung dieses Anwendungsfalls auf Basis einer **DLT** die Fähigkeiten dieser voll ausnutzt, indem Logging, Vertragsabwicklung, Payment und Manipulationssicherheit onchain ausgeführt werden.

Das Ziel der Umsetzung dieses Anwendungsfalls ist die Implementierung der zweiten Variante, um einen realistischen Anwendungsfall zielbringend zu implementieren und um einen entsprechenden Mehrwert durch den Einsatz einer **DLT** zu generieren.

ANFORDERUNGEN

In diesem Kapitel werden die Anforderungen für den im vorherigen Kapitel aufgezeigten Anwendungsfall aufgestellt. Ziel ist es, die **DLT**-relevanten Anforderungen zu identifizieren, um dadurch im nächsten Kapitel eine geeignete **DLT**-Lösung zu finden. Dazu werden zunächst einige Standards vorgestellt, wie Anforderungen klassifiziert und eingeordnet werden können. Diese Standards werden anschließend in einem optimierten Modell zusammengeführt und auf die konkreten Anforderungen angewandt. Die Klassifizierung dient als Werkzeug zur Einteilung der unübersichtlichen Gesamtmenge der Anforderungen und soll die weitere Identifikation **DLT**-relevanter Anforderungen vereinfachen. Als Zwischenergebnis existieren verschiedene Anforderungsklassen, die auf **DLT**-Relevanz geprüft werden. Durch schrittweises Ausschließen und Reduzieren der Anforderungsklassen werden jene Klassen identifiziert, die für die Umsetzung auf einer **DLT**-basierten Lösung entscheidend sind.

5.1 STANDARDS UND NORMEN

In diesem Abschnitt werden die verwendeten Standards und Normen aufgelistet und kurz beschrieben:

BABOK Das Business Analysis Body of Knowledge (**BABOK**) wird vom International Institute of Business Analysis (**IIBA**) herausgegeben und stellt einen Leitfaden für die Business-Analyse dar, genauere Informationen können [26] entnommen werden. Es unterteilt in sogenannte Knowledge-Areas und vermittelt Techniken und Kompetenzen im Umfeld der Business-Analyse. Anforderungen werden im **BABOK** nach Abstraktionsebene gruppiert: Die Business-Ebene, die Anforderungen abstrakt aus Sicht der gesamten Organisation betrachtet, die Stakeholder-Ebene, die die Anforderungen aus Sicht der verschiedenen Stakeholder beschreibt und die Solution-Ebene, die in funktionale und nicht-funktionale Anforderungen unterscheidet. Darüber hinaus gibt es eine Transition-Ebene, die temporäre Übergangsanforderungen zwischen dem Ausgangs- und dem Zielzustand des Gesamtsystems beschreibt.

PMBOK Das Project Management Body of Knowledge (**PMBOK**) wird vom Project Management Institute (**PMI**) herausgegeben und ist der State-of-the-Art Standard im Bereich Projektmanagement, siehe [27]. Das Werk teilt seine Sektionen ebenfalls wie das **BABOK** in sogenannte Knowledge-Areas ein und kennt die gleiche Gruppierung im Bereich Anforderungsmanagement. Neben der Einteilung in Business, Stake-

holder, Solution und Transition Anforderungen kennt das **PMBOK** noch Quality und Project Anforderungen.

SWEBOK Das Software Engineering Body of Knowledge (**SWEBOK**) wurde von dem Institute of Electrical and Electronics Engineers (**IEEE**) erstellt und stellt ein Standardwerk aus dem Bereich Software-Engineering dar, genauere Informationen können [2] entnommen werden. Anforderungen werden in System- und Software-Anforderungen unterteilt. Letztere werden untergliedert in Funktionale, Nicht-Funktionale, Produkt und Prozess-Anforderungen.

SEBOK Das System Engineering Body of Knowledge (**SEBOK**) wurde unter Anderem von der **IEEE** erstellt und stellt ein Standardwerk aus dem Bereich System-Engineering dar, genauere Informationen können der Quelle [13] entnommen werden. Anforderungen werden sehr detailliert unterteilt, unter Anderem in die Klassen Functional, Usability, Interface, Performance, Policies and Regulations, etc.

ISO 29148 Die Norm 29148 der **ISO** beschreibt das Anforderungs-Engineering **ISO** als Teilbereich des Software-Engineering, genauere Informationen können [24] entnommen werden. Anforderungen werden ähnlich wie beim **SEBOK** untergliedert in Functional, Usability und Interface. Darüber hinaus kennt die Norm Human Factors und Process Anforderungen.

ISO 25010 Die Norm 25010 der **ISO** beschreibt Qualitätskriterien eines Software-Produktes, siehe [25]. Die Kriterien Performance-Efficiency, Compatibility, Usability, Reliability, Security, Maintainability, Portability sowie deren Unterkriterien werden zur detaillierten Beschreibung von Nicht-Funktionalen Anforderungen eingesetzt.

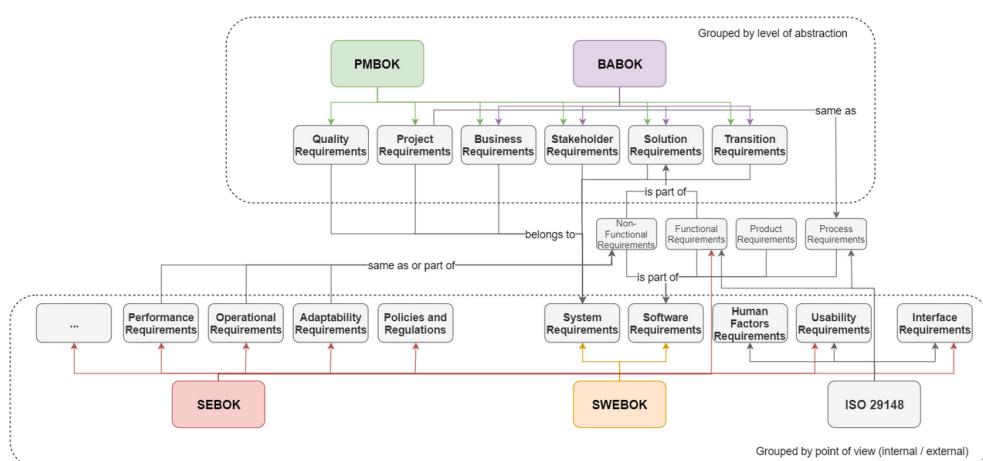


Abbildung 5.1: Einordnung der Begriffe und Zusammenhänge unterschiedlicher Normen und Standards

Das Schaubild 5.1 zeigt die unterschiedlichen Normen und Standards grafisch auf und stellt die verschiedenen Anforderungsgruppierungen zueinander in Beziehung.

Grundsätzlich unterscheiden die vorgestellten Ansätze zur Anforderungsklassifizierung zwei Sichtweisen: PMBOK und BABOK unterscheiden Anforderungen nach Abstraktionslevel während SWEBOK, SEBOK und ISO29148 primär nach der Perspektive der Stakeholder gruppieren. Das Schaubild 5.2 stellt diesen Zusammenhang grafisch dar.

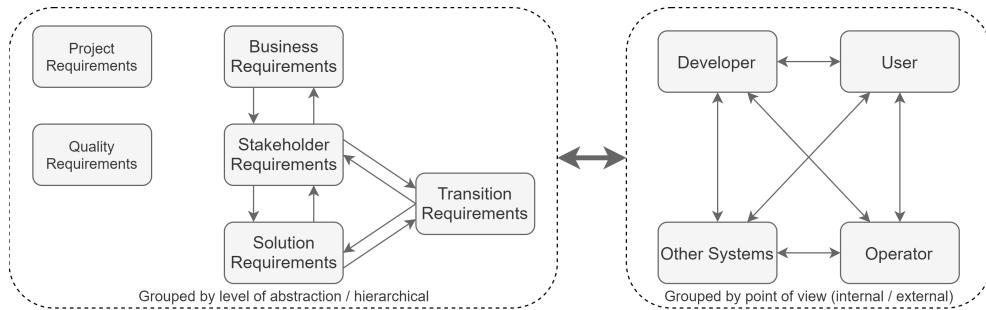


Abbildung 5.2: Anforderungen werden nach zwei verschiedenen Ansätzen gruppiert.

5.2 ABLEITUNG EINES KlassifizierungsmODELLS

Die Vorteile mehrerer der vorgestellten Ansätze zur Anforderungsklassifizierung können kombiniert werden, indem Anforderungen stufenweise in Unterklassen unterteilt werden. Dabei wird sich der Klassifizierung des [2], [27] bzw. [26] und [25] bedient und die folgende Einordnung erstellt:

SYSTEM-ANFORDERUNGEN Anforderungen dieser Klasse beziehen sich auf das Gesamtsystem.

SOFTWARE-ANFORDERUNGEN Anforderungen dieser Klasse beziehen sich auf die Softwarekomponente des Gesamtsystems.

BUSINESS-ANFORDERUNGEN Diese Anforderungen gehören zu der Klasse der System-Anforderungen und beschreiben Anforderungen, die sich an das Geschäftsmodell hinter dem Gesamtsystem richten. Der Schwerpunkt liegt auf dem Mehrwert für die Organisation und dem damit verbundenen Nutzen des Gesamtsystems.

Leitfrage: „Welche Geschäftsfälle gibt es und wie werden diese abgedeckt? Welche Richtlinien und Vorgaben müssen beachtet werden?“

STAKEHOLDER-ANFORDERUNGEN Diese Anforderungen gehören zu der Klasse der System-Anforderungen und beschreiben Anforderungen, die die Interessen der beteiligten Stakeholder widerspiegeln und sich keiner anderen Klasse zuordnen lassen.

Leitfrage: „Was muss das Gesamtsystem aus Sicht von [Stakeholder] können?“

TRANSITION-ANFORDERUNGEN Diese Anforderungen gehören zu der Klasse der System-Anforderungen und beschreiben den Übergang vom IST-Zustand des Systems in den SOLL-Zustand. Beispiele hierfür sind benötigte Anwenderschulungen oder Datenkonvertierungen.
Leitfrage: „Was muss gegeben sein, damit sich das Gesamtsystem von Zustand A in den Zustand B überführen lässt?“

PROJEKT-ANFORDERUNGEN Diese Anforderungen gehören zu der Klasse der System-Anforderungen und beschreiben die Rahmenbedingungen an das Entwicklungsprojekt. Beispiele hierfür können die Projektsprache und Dokumentationsrichtlinien sein.
Leitfrage: „Welche Rahmenbedingungen sind dem Entwicklungsprojekt gegeben?“

QUALITÄT-ANFORDERUNGEN Als Unterklasse der System-Anforderungen beschreiben die Qualität-Anforderungen die Qualitätsansprüche an das System und die Entwicklung und definieren Akzeptanzkriterien ähnlich zu Definition of Ready (DoR) bzw. Definition of Done (DoD).
Leitfrage: „Welche Qualitätsansprüche werden an das Gesamtsystem gestellt?“

NICHT-FUNKTIONALE ANFORDERUNGEN Diese Anforderungen werden gemäß ISO-Norm 25010 zur Software-Qualität definiert und sind Teil der Software-Anforderungen. Dazu zählen zum Beispiel die Performance, die Kompatibilität und die Benutzbarkeit. Eine ausführliche Aufzählung aller Klassen unter dem Sammelbegriff der nicht-funktionalen Anforderungen sowie die genauen Definitionen der Begriffe kann unter [25] eingesehen werden.

Leitfrage: „Wie gut muss die Software etwas können?“

FUNKTIONALE ANFORDERUNGEN Diese Unterklasse der Software-Anforderungen beschreibt, was das Software-System leisten muss und welche Aufgaben es erfüllen muss.

Leitfrage: „Was muss die Software können?“

PROZESS-ANFORDERUNGEN Als Untergruppe der Software-Anforderungen bündelt diese Klasse alle Anforderungen, die den Prozess beschreiben, damit die Software so wird, wie gefordert. Typischerweise sind Anforderungen an den Softwareentwicklungsprozess enthalten.

Leitfrage: „Was ist beim Entwickeln der Software zu beachten?“

Die Abbildung 5.3 fasst die Anforderungstypen zusammen und stellt sie hierarchisch strukturiert dar. Es wird deutlich, dass das entwickelte Modell beide Sichtweisen (vgl. Abbildung 5.2) aufgreift. Auf Seite der

System-Anforderungen werden verschiedene Abstraktionslevel wie zum Beispiel die Business-Anforderungen und die Stakeholder-Anforderungen unterschieden. Stakeholder-Anforderungen wiederum spiegeln die Interessen der Beteiligten wider und betrachten die Anforderungen zusammen mit den Software-Anforderungen aus unterschiedlichen Perspektiven.

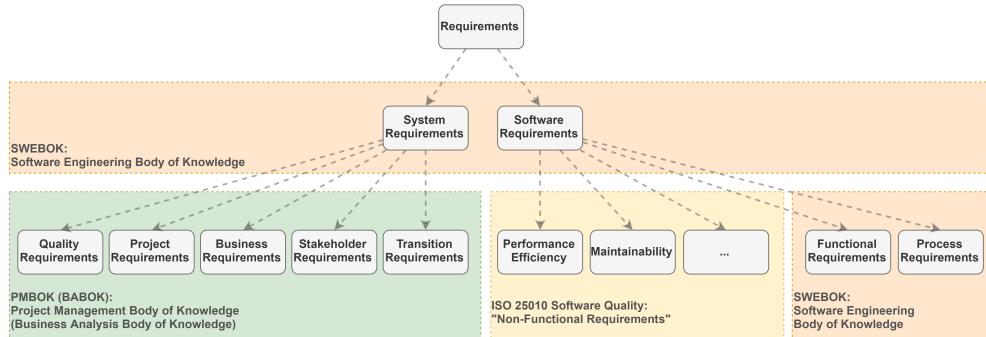


Abbildung 5.3: Anforderungsklassifizierung als kombiniertes Modell aus [2], [27] bzw. [26] und [25]

5.3 ANFORDERUNGSANALYSE

In diesem Abschnitt werden die Anforderungen zu dem in Kapitel 4 vorgestellten Anwendungsfall ermittelt. Dazu werden zunächst alle beteiligten Stakeholder identifiziert und kurz beschrieben. Anschließend werden aus der jeweiligen Perspektive heraus User-Stories gebildet und die daraus abgeleiteten Tasks aufgelistet. Eine detaillierte Beschreibung aller daraus resultierenden Anforderungen sowie die genaue Zuordnung zu den User-Stories sind im Anhang A zu finden.

Die Rollen Hersteller, Kunde, Service-Dienstleister und Lieferant wurden bereits unter 4.1 beschrieben. Die folgende Auflistung zeigt weitere Anforderungsrollen, die über die bereits genannten hinausgehen:

PLATTFORM-BETREIBER Der Plattform-Betreiber ist verantwortlich für den Betrieb der Plattform und ist hauptsächlich an einem stabilen System und einer einfachen Wartung der Software interessiert.

IT-SECURITY-BEAUFRAGTER Für den IT-Security-Beauftragten stehen alle sicherheitsrelevanten Themen im Fokus. Dazu zählen insbesondere Verschlüsselung, Datensicherheit und Datenschutz sowie die Authentizität von Daten.

BUSINESS-DEVELOPER Der Business-Developer beschäftigt sich mit der Unternehmensentwicklung und hat Anforderungen an das Geschäftsmodell, die Wirtschaftlichkeit und die Zielerreichung des Gesamtsystems.

SYSTEM-ARCHITEKT Für den Software-Architekten stehen alle Fragen rund um die IT-Architektur der Plattform im Vordergrund. Dazu zählen APIs, Modularisierung und der generelle Aufbau der Software.

Um konkrete Anforderungen zu erstellen, werden Userstories aus der Perspektive jedes Stakeholders erarbeitet. Userstories beschreiben eine Funktionalität des Systems, welche aus Sicht der jeweiligen Rolle benötigt wird, um ein bestimmtes Ziel zu erreichen oder einen bestimmten Zweck zu erfüllen. Somit haben alle Userstories die einheitliche Grundstruktur:

„Als [Rolle] möchte ich [Funktion], um [Ziel / Zweck] zu erreichen.“

Zu jeder User-Story werden Tasks beschrieben, die die User-Stories in logische Teile untergliedern. Im letzten Schritt werden diese Tasks feingranular in Anforderungen unterteilt. Die Klassifizierung wird anschließend nach dem erarbeiteten Modell aus [5.2](#) durchgeführt.

Die erste Userstory (A1) fasst grundlegende Tätigkeiten über das Agieren auf der Plattform als Akteur (Hersteller, Kunde, Service-Dienstleister, Lieferant, Endgerät) zusammen. Dies beinhaltet sämtliche Interaktionen und Bedingungen, die für alle Akteure gleich sind. Die Userstory A1 beinhaltet vier Tasks:

- Die Zugangsberechtigung zur Plattform ist in fünf Anforderungen untergliedert, vier davon sind als *Funktionale Anforderungen* klassifiziert, eine als *Security Anforderung*.
- Die Kommunikation zwischen Rollen ist durch fünf Anforderungen definiert und beinhaltet eine *Funktionale Anforderung*, drei *Security Anforderungen* und eine *Performance-Efficiency Anforderung*.
- Die Vertragsgestaltung ist in elf Tasks untergliedert, zwei davon sind *Security*, neun *Funktionale Anforderungen*.
- Grafische Oberflächen, die alle Akteure zur Interaktion mit der Plattform benötigen, sind in zwei *Funktionale Anforderungen* unterteilt.

Userstories M1 bis M3 stellen die Anforderungen aus Sicht eines Manufacturers dar:

- Userstory M1 beschreibt die Vermietung von Endgeräten und beinhaltet zwei Tasks mit insgesamt sechs Anforderungen. Fünf der sechs Anforderungen sind *Funktionale Anforderungen*, eine wurde als *Portability Anforderung* klassifiziert.
- Userstory M2 beschreibt das Erzeugen von Verträgen und beinhaltet einen Task mit drei Anforderungen, welche alle der Klasse der *Funktionalen Anforderungen* zugeordnet wurden.

- Userstory M₃ beschreibt die Abrechnung von Verträgen und beinhaltet zwei Tasks mit insgesamt drei Anforderungen, wobei eine Anforderung als *Funktionale Anforderung*, eine als *Performance-Efficiency Anforderung* und eine als *Security Anforderung* bestimmt wurde.

Die Userstories C₁ bis C₃ zeigen die Sicht des Customers:

- Userstory C₁ beschreibt die Ansicht verfügbarer Geräte, also eine Oberfläche, die dem Customer bereitgestellt werden muss, auf der er alle zur Miete verfügbaren Geräte gelistet bekommt. Diese Userstory beinhaltet zwei Tasks mit insgesamt zwei *Funktionalen Anforderungen*.
- Userstory C₂ beschreibt die Wartung und Reinigung der Geräte durch den Customer und beinhaltet vier Tasks mit insgesamt sechs Anforderungen. Dabei handelt es sich um vier *Funktionale Anforderungen*, eine *Security Anforderung* und eine *Performance-Efficiency Anforderung*.
- Userstory C₃ beschreibt die Bedienbarkeit aus Nutzersicht und beinhaltet zwei Tasks mit insgesamt drei Anforderungen. Dabei handelt es sich um eine *Transition Anforderung* und zwei *Usability Anforderungen*.

Die Userstories SP₁ und SP₂ sind aus Sicht des Service-Providers beschrieben:

- Userstory SP₁ beschreibt das Anbieten eigener Service-Dienstleistungen auf der Plattform mit einem Task und zwei *Funktionalen Anforderungen*.
- Userstory SP₂ beschreibt das Abschließen von Service-Aufträgen nach getätigtem Service an den Geräten vor Ort und ist unterteilt in zwei Tasks mit je zwei *Funktionalen Anforderungen*.

Die Userstories SEC₁ bis SEC₃ sind aus Sicht des Security-Beauftragten beschrieben:

- Userstory SEC₁ beschreibt die sichere Zahlungsabwicklung und ist in zwei Tasks mit insgesamt fünf Anforderungen unterteilt. Dabei handelt es sich um zwei *Funktionale Anforderungen* und drei *Security Anforderungen*.
- Userstory SEC₂ beschreibt die sichere Kommunikation mittels signierter Nachrichten und untergliedert sich in zwei Tasks mit insgesamt zwei *Quality Anforderungen*.
- Userstory SEC₃ beschreibt die Manipulationssicherheit und ist in zwei Tasks mit insgesamt drei *Security Anforderungen* unterteilt.

Die Userstories BD₁ bis BD₄ sind aus Sicht des Business-Developers beschrieben:

- Userstory BD₁ beschreibt das Geschäftsmodell und beinhaltet zwei Tasks mit insgesamt sechs Anforderungen, wobei fünf davon als *Funktionale Anforderungen* und eine als *Business Anforderung* klassifiziert wurden.

- Userstory BD₂ beschreibt den Zugang von Geschäftspartnern zu der Plattform und ist in zwei Tasks mit insgesamt drei Anforderungen untergliedert. Diese wurden als *Business Anforderung*, *Transition Anforderung* und *Stakeholder Anforderung* klassifiziert.
- Userstory BD₃ beschreibt die Plattform als Hersteller-übergreifend und ist in drei Tasks mit insgesamt drei Anforderungen unterteilt. Dabei wurden eine Anforderung als *Business Anforderung* und zwei als *Compatibility Anforderungen* klassifiziert.
- Userstory BD₄ beschreibt die Abrechnungsmodelle der Plattform und ist in einen Task mit zwei Anforderungen unterteilt. Dabei handelt es sich um eine *Business Anforderung* und einer *Maintainability Anforderung*.

Die Userstories SA₁ und SA₂ sind aus Sicht des System-Architekten beschrieben:

- Userstory SA₁ beschreibt die einfache Einbindung der Plattform in bestehende Infrastruktur und enthält einen Task mit einer *Process Anforderung*.
- Userstory SA₂ beschreibt die Robustheit des Gesamtsystems bei Ausfällen und ist in zwei Tasks mit je zwei Anforderungen unterteilt. Dabei handelt es sich um zwei *Security Anforderungen* und zwei *Reliability Anforderungen*.

Die Userstory P₁ ist aus Sicht des Plattform-Betreibers beschrieben:

- Userstory P₁ beschreibt die automatisierte Bereitstellung der Software und ist in zwei Tasks mit je einer Anforderung untergliedert. Diese sind als *Maintainability Anforderung* und als *Portability Anforderung* klassifiziert.

Insgesamt wurden 19 Userstories beschrieben, die in 39 Tasks unterteilt wurden. Die 83 daraus resultierenden Anforderungen wurden klassifiziert, sodass sich 9 Level-1 *System-Anforderungen* und 74 Level-1 *Software-Anforderungen* ergaben. Für jede Level-2 Klasse unterhalb der *System-Anforderungen* wurden Anforderungen ermittelt - bis auf die Klasse der Projekt-Anforderungen. Im Rahmen dieser Arbeit wird ein **PoC** entwickelt, womit diese Arbeit aus Sicht der Anforderungserstellung als Entwicklungsprojekt angesehen werden kann. Rahmenbedingungen wie die zeitliche Begrenzung des Projektes oder den Reifegrad eines **PoCs** könnten als Projekt-Anforderungen definiert werden. Da dies aber keine konkrete Auswirkung auf den Anwendungsfall als solchen hat, wird an dieser Stelle auf diese Klasse verzichtet. Bei der Entwicklung eines marktreifen Produktes in einem realen Entwicklungsprojekt ist diese Klasse allerdings zu beachten.

Auf Seiten der Software-Anforderungen werden alle Level-2 Klassen abgedeckt. Die Subklasse *Functionality-Suitability Anforderungen* erhält im Modell eine eigene Klasse, da es sich um Funktionale Anforderungen handelt.

5.4 ANFORDERUNGSEVALUIERUNG

Die Anforderungsevaluierung hat zum Ziel, die im vorherigen Abschnitt beschriebenen und klassifizierten Anforderungen schrittweise zu reduzieren, um die **DLT**-relevanten Anforderungen zu identifizieren. Dabei handelt es sich um Anforderungen, die relevant für eine technische Umsetzung auf Basis einer **DLT**-Lösung sind.

Um die Relevanz für den Kontext **DLT** festzustellen, wurde die Anforderungsliste mit den Fachexperten der Abteilung für Distributed Ledger Technologies der Firma MaibornWolff GmbH in mehreren Diskussionsrunden durchgearbeitet und nach Einschätzung der Experten entsprechend gewertet.

5.4.1 *System-Anforderungen*

Die erste Level-2 Subklasse der *System-Anforderungen* ist die Klasse der *Quality Anforderungen*. Diese Klasse definiert die Qualitätskriterien, die die Plattform erfüllen muss. Anforderungen dieser Klasse fungieren oft als Enabler für weitere Anforderungen anderer Klassen. Für den beschriebenen IOT-Anwendungsfall wurden zwei Anforderungen identifiziert, die dieser Klasse zuzuordnen (Anforderungen SEC2.1.1, SEC2.2.1) und Teil der Userstory SEC2 sind. Sie beschreiben, dass die Verwendung von HTTPS bzw. SSL/TLS ein vorgeschriebenes Qualitätskriterium ist. Darüber hinaus müssen Passwortregeln hinterlegbar sein, um die Sicherheit der auf der Plattform verwendeten Passwörter zu gewährleisten. Es wird deutlich, dass die Anforderungen dieser Klasse primär Rahmenbedingungen darstellen und keine direkten Auswirkungen auf die technische Basis haben. Diese Qualitätsansprüche, die mit den genannten Anforderungen einhergehen, haben keine Auswirkung auf eine mögliche Umsetzung der Plattform durch eine **DLT**-Lösung. Damit werden die Anforderungen im weiteren Verlauf nicht tiefergehend betrachtet.

Die zweite Level-2 Subklasse der *System-Anforderungen* ist die Klasse der *Project Anforderungen*, die Rahmenbedingungen an das Projekt beschreiben. Die Entwicklung des **PoC** im Rahmen dieser Arbeit stellt ein solches Entwicklungsprojekt dar, ist allerdings für die Betrachtung in diesem Kontext hinsichtlich **DLT**-Relevanz nicht weiter zu berücksichtigen. Die *Project Anforderungen* werden entsprechend nicht in die weitere Analyse miteinbezogen.

Die dritte Level-2 Subklasse der *System-Anforderungen* ist die Klasse der *Business-Anforderungen*, die die Geschäftsfälle und -anforderungen von einer abstrakteren Perspektive betrachten. Im Fokus stehen die Bedürfnisse und Rahmenbedingungen des Unternehmens, welches die Plattform beauftragt hat. Im Rahmen des IOT-Anwendungsfalls wurden vier Anforderungen dieser Klasse identifiziert (Anforderungen BD1.1.1, BD2.1.1, BD3.1.1 und

BD4.2.1); betroffen sind die Userstories BD1 bis BD4. Die Anforderungen decken das Abrechnungsmodell Pay-As-You-Use ab und beschäftigen sich mit der aktuellen und zukünftigen geschäftlichen Ausrichtung der Plattform. Letzteres hat keine Auswirkungen auf die technische Basis, die die zugrundeliegende Plattform verwendet: Es handelt sich um keine Technologie-entscheidende Anforderung. Anforderung BD4.2.1 beschreibt, dass ein Pay-As-You-Use Abrechnungsmodell in einem Vertrag abgebildet wird. Diese Anforderung ist **DLT**-relevant: Zum einen impliziert diese Anforderung, dass eine zugrundeliegende **DLT**-Plattform in der Lage ist, Verträge abzubilden: Im Umfeld von **DLTs** bietet sich die Abwicklung der Vertragslogik mittels Smart-Contracts an. Zum anderen muss gewährleistet sein, dass die Smart-Contract Implementierung mächtig genug ist, um das Abrechnungsmodell Pay-As-You-Use codieren zu können. Diese Anforderung muss in die weitere Analyse miteinbezogen werden.

Die vierte Level-2 Subklasse der *System-Anforderungen* ist die Klasse der *Stakeholder-Anforderungen*, welche Anforderungen speziell aus der Sicht einzelner Stakeholder beschreiben, die mit anderen Klassen noch nicht abgedeckt werden konnten. Im Kontext des Anwendungsfalls wurde eine Anforderung identifiziert (BD2.2.1), die dieser Klasse zuzuordnen ist und zur Userstory BD2 gehört. Es wird der Onboarding-Prozess eines Geschäftspartners beschrieben, indem dieser als Partner identifiziert werden muss. Dieser Prozess muss entsprechend der Anforderungen gestaltet werden, womit es sich um eine abstrakte Beschreibung dessen, wie ein Prozess auszusehen hat, handelt. Es werden keine technischen Details gefordert, wodurch keine Abhängigkeiten zu der technischen Umsetzung der Plattform entstehen. Damit ist diese Klasse für die weitere Analyse nicht relevant und kann vernachlässigt werden.

Die fünfte Level-2 Subklasse der *System-Anforderungen* ist die Klasse der *Transition Anforderungen*, die sämtliche Anforderungen von einem IST-Zustand (zeitlich vor der Einführung der Plattform) in einen SOLL-Zustand (zeitlich nach Einführung der Plattform) beinhaltet. Zwei Anforderungen (Anforderungen C3.1.1 und BD2.1.2) wurden identifiziert, die dieser Klasse zuzuordnen und Teil der Userstories C3 und BD2 sind. Es handelt sich in dem vorliegenden Kontext um Anforderungen, die die schnelle Erlernbarkeit durch den Benutzer sowie die Schulung von Mitarbeitern zur Nutzung der Plattform beschreiben und somit die User-Experience (**UX**) in den Vordergrund stellen. Da es sich in diesem Fall um Aufbau, Verständlichkeit und Benutzbarkeit einer grafischen Oberfläche (Schnittstelle zum Benutzer) handelt, kann diese Klasse ebenfalls vernachlässigt werden.

5.4.2 Software-Anforderungen

Anforderungen dieser Level-1 Klasse stellen den Großteil aller Anforderungen dar. In einem realistischen Entwicklungsprojekt sind die individuellen Rahmenbedingungen, Qualitätskriterien, Business-Richtlinien und Integrationsrichtlinien des jeweiligen Unternehmens zu beachten. Die in dieser Arbeit aufgestellten System-Anforderungen decken nur die grundlegendsten Anforderungen dieser Kategorie ab. Die *Software-Anforderungen*, die in diesem Abschnitt evaluiert werden, sind unabhängig von den *System-Anforderungen* stets dieselben.

Die erste Level-2 Subklasse der *Software-Anforderungen* sind die *Process Anforderungen*, die Anforderungen an den Entwicklungsprozess der Software stellen. Für den vorliegenden IOT-Anwendungsfall wurde eine Anforderung (SA1.1.1) ermittelt, die zu der Userstory SA1 gehört. Während der Entwicklung ist darauf zu achten, dass die Modularität der Softwarekomponenten gewahrt bleibt, damit diese später unabhängig voneinander bereitgestellt und gewartet werden können. Dies hat keine Auswirkung auf die Umsetzung auf Basis einer *DLT*-Lösung. Im Allgemeinen haben Anforderungen dieser Klasse einerseits eine technische Relevanz, da sie zum Beispiel einzusetzende Technologien für Schnittstellen beschränken oder die Art und Weise definieren, wie Software entwickelt werden soll. Andererseits kann jede Software durch den Einsatz einer geeigneten Middleware miteinander verbunden werden, sollten vorhandene Schnittstellen und Softwarekomponenten nicht Standard-konform oder kompatibel sein. Somit können die Anforderungen dieser Klasse ebenfalls vernachlässigt werden.

Die zweite Level-2 Subklasse der *Software-Anforderungen* sind die *Funktionalen Anforderungen*, die beschreiben, welche Funktionalität die Plattform anbieten muss. Für den vorliegenden IOT-Anwendungsfall wurden 46 solcher Anforderungen ermittelt, die insgesamt zehn Userstories betreffen. Um die Übersichtlichkeit zu bewahren, wurde diese Klasse in verschiedene, logische Abschnitte gegliedert. Diese wurden nach der inhaltlichen Thematik der Anforderungen definiert und folgen keiner speziellen Klassifizierung.

GUI 12 der 46 Anforderungen dieser Klasse betreffen direkt oder indirekt die grafische Darstellung für den Benutzer. Es handelt sich hierbei lediglich um das Frontend, welches Daten aufbereitet darstellt und Schaltflächen zur Interaktion mit dem Backend bereitstellt. Somit werden die Anforderungen dieser Klasse für weiterführende Analysen nicht beachtet. Konkret handelt es sich um die Anforderungen A1.1.4, A1.3.4, A1.4.1, A1.4.2, M2.1.1, M2.1.2, M2.1.3, C1.1.1, C1.2.1, SP1.1.1, SP1.1.2 und SP2.2.1.

ENDGERÄT 15 der 46 Anforderungen beziehen sich auf Funktionalitäten, die das Endgerät bereitstellen muss, um auf der Plattform vermietet

werden zu können. Dabei geht es primär um die Konnektivität zu der Plattform, die Funktionsweise der verbauten Sensoren sowie der Kommunikation mit dem Customer und dem Service-Provider. Die Endgeräte fungieren in ihrer Rolle als Peripherie; es kann sich um Haushaltsgeräte aller Art handeln - von der Kaffeemaschine bis zur Waschmaschine. Die Schnittstellen hin zur Plattform sind klar definiert. Auf der einen Seite wird deutlich, dass die meisten Anforderungen an die Geräte unabhängig von der technischen Umsetzung der Plattform sind und keinen Einfluss auf deren Umsetzung haben. Bei Inkompatibilität eines Endgeräts zur Plattform wäre der Einsatz einer Middleware sinnvoll, die die Integration zur Plattform sicherstellen könnte. Eine Möglichkeit wäre die Verwendung eines lokalen Gateways, das die Daten der Geräte konvertiert und an die Plattform übermittelt. Standardmäßig sollten die Geräte die Kommunikation mit der Plattform bereits Hersteller-seitig gewährleisten. Auf der anderen Seite spielt gerade die Konnektivität eine ganz entscheidende Rolle: Die Tatsache, dass Endgeräte nicht jederzeit mit der Plattform verbunden sind - bedingt durch Verbindungsprobleme oder Ähnliches - stellt eine zentrale Anforderung an die zugrundeliegende Plattform dar. Um auch im Offline-Modus mit seinem Umfeld interagieren zu können, zum Beispiel um einen Kaffee zu servieren, muss das Gerät zeitnah auf Benutzereingaben reagieren, da ansonsten ein schlechtes Benutzererlebnis entstünde. Würde das Gerät erst dann reagieren, wenn es alle benötigten Informationen von der Plattform erhalten hat, also nachdem es wieder eine Verbindung aufbauen konnte, wäre der Anwendungsfall inpraktikabel und hätte keine wirtschaftliche Daseinsberechtigung. Deshalb muss es möglich sein, dass das Gerät voll funktionsfähig arbeitet, auch wenn es keine Konnektivität zur Plattform hat. Anlaufende Kosten und Informationsengpässe müssen handhabbar sein und zu einem späteren Zeitpunkt synchronisierbar sein. Diese Anforderung hat eine sehr hohe **DLT**-Relevanz und muss für die folgende Analyse genaustens berücksichtigt werden. (Anforderungen M1.1.1, M1.1.2, M1.1.3, M1.2.1, M1.2.2, M1.2.3, M1.2.4, M3.1.1, C2.1.1, C2.1.2, C2.3.1, C2.4.1, SP2.1.1, SP2.1.2 und SP2.2.2)

KOMMUNIKATION Drei der 46 Anforderungen beziehen sich auf die Kommunikation zwischen Akteuren auf der Plattform (Anforderungen A1.2.1, A1.3.1 und A1.3.3). Anforderung A1.3.1 beschreibt die Kommunikation über Verträge, die die Akteure der Plattform miteinander abschließen können. Im Kontext einer **DLT**-Lösung bedeutet das, dass die Plattform in der Lage sein muss, einen Vertrag abzubilden (siehe Business-Anforderungen oben). Diese Anforderung hat eine **DLT**-Relevanz und muss in der weiteren Analyse betrachtet werden. Die übrig gebliebenen zwei Anforderungen beschreiben allgemeinere Aspekte der Kommunikation auf der Plattform und können vernachlässigt werden.

FINANZEN Sieben der 46 Anforderungen (A1.3.11, SEC1.1.1, SEC1.1.3, BD1.2.1, BD1.2.2, BD1.2.3 und BD1.2.5) beschreiben den Geldfluss zwischen Akteuren aufgrund ihrer vertraglichen Vereinbarungen. Geldtransfers werden geloggt und vor Ausführung überprüft. Diese Anforderungen sind für eine Umsetzung auf einer **DLT**-Lösung nicht relevant, da sie lediglich die Richtung und Menge des Geldflusses sowie Rahmenbedingungen an Geldtransfers festlegen. Damit allerdings erbrachte Leistungen kostenpflichtig gemäß des Abrechnungsmodells abgerechnet werden können, muss die Plattform zum einen das Abrechnungsmodell implementieren und zum anderen ein digitales Zahlungsmittel bereitstellen. Erstes kann auf einer **DLT**-Lösung mittels Smart-Contracts umgesetzt werden. Zweiteres bedarf einer internen Währung, um Leistungen nach Verbrauch abzurechnen. Damit sind diese zwei Anforderungen relevant und müssen in der weiteren Analyse beachtet werden.

ROLLENMANAGEMENT Drei der 49 Anforderungen (A1.1.2, A1.1.3 und A1.1.5) definieren das Rollenmanagement und den Zugang zu der Plattform mittels Registrierung und Anmeldung. Letzteres stellt keine Relevanz dar, da es sich um eine standardmäßige Zugangsbeschränkung handelt und nicht abhängig von der Backend-Lösung ist. Im Gegensatz dazu werden Rollen in den Verträgen genutzt, um Berechtigungen der Akteure zu prüfen. Es handelt sich um Informationen, die von Verträgen auf der Plattform einsehbar sein müssen. Content- oder allgemein Informationsprovider, die Informationen auf einer **DLT**-Umgebung bereitstellen, nennt man Oracles (siehe Kapitel 2.1.2). Hier liegt eine Relevanz in Bezug auf die Umsetzung auf Basis einer **DLT**-Lösung vor und muss im weiteren Verlauf beachtet werden.

VERTRAGSKONSTRUKT Sechs der 49 Anforderungen (A1.3.2, A1.3.6, A1.3.7, A1.3.8, A1.3.10 und BD1.2.4) beschreiben das Vertragskonstrukt: Eigenschaften wie Individualität und Zugriffsregelung haben keinen Einfluss auf die technische Lösung, wohingegen die Komplexität und Editierbarkeit (drei Anforderungen) große Relevanz haben. Zum einen muss die Implementierung eines Vertrages mittels Smart-Contracts auch komplexe Konstrukte abbilden können. Zum anderen sind Smart-Contracts - sind sie einmal in der **DLT** gespeichert - unveränderbar und können als solches nicht überarbeitet werden. Die zugrundeliegende **DLT**-Technologie muss also einen entsprechenden Mechanismus anbieten, um Smart-Contracts zu warten und zu aktualisieren. Darüber hinaus handelt es sich bei den Verträgen, die mittels Smart-Contracts abgebildet werden sollen, um rechtskräftige Miet- und Serviceverträge. Demnach müssen die Implementierungen rechtssicher und rechtskonform abgebildet werden können. Diese Punkte sind bei der Wahl der **DLT**-Lösung zu beachten.

Die dritte Level-2 Subklasse der *Software-Anforderungen* unter dem Sammelbegriff der *Nicht-Funktionalen Anforderungen* heißt *Kompatibilität* (Compa-

tibility). Für den vorliegenden IOT-Anwendungsfall wurden zwei solcher Anforderungen ermittelt (BD3.2.1, BD3.3.1), welche die Userstory BD3 betreffen. Die Kompatibilität stellt die Fähigkeit des Gesamtsystems dar, Informationen mit anderen System auszutauschen und sich eine Umgebung mit anderen Systemen zu teilen. Es handelt sich hierbei um Anforderungen, die im Kontext des IOT-Anwendungsfalls keine Relevanz für die Wahl der technischen Basis haben. Sollten Systeme nicht kompatibel sein, so könnte im Zweifelsfall eine Middleware für die Übersetzung bzw. die Kompatibilität sorgen. Somit werden die Anforderungen dieser Klasse für die weitere Analyse nicht weiter beachtet.

Die vierte Level-2 Subklasse der *Software-Anforderungen* unter dem Sammelbegriff der *Nicht-Funktionalen Anforderungen* nennt sich *Wartbarkeit* (Maintainability). Anforderungen dieser Klasse stellen die Fähigkeit des Gesamtsystems dar, effizient wartbar zu sein um z.B. die Funktionalität zu erweitern und zu verbessern. Konkret im Kontext des IOT-Anwendungsfalls beziehen sich die Anforderungen BD4.2.2 und P1.1.1 der zwei Userstories BD4 und P1 auf den Aufbau der Software: Einzelne Module können separat gewartet werden und die Testabdeckung ist hoch genug, damit die Wartung einzelner Module keine unerwünschten Nebeneffekte mit sich führt. Es handelt sich also um generische Anforderungen, die keinen Bezug zur technischen Umsetzung haben und daher keine DLT-Relevanz besitzen. Somit wird diese Anforderungsklasse im weiteren Verlauf nicht weiter berücksichtigt.

Die fünfte Level-2 Subklasse der *Software-Anforderungen* unter dem Sammelbegriff der *Nicht-Funktionalen Anforderungen* lautet *Performance-Effizienz* (Performance-Efficiency) und beschreibt die Leistung des Gesamtsystems in Bezug auf die zur Verfügung stehenden Ressourcen. Die Anforderungen dieser Klasse (A1.2.2, M3.2.1 und C2.4.2) im konkreten Anwendungsfall betreffen drei Userstories (A1, M3 und C2) und beschreiben alle das zeitliche Verhalten von übermittelten Daten: Die Kommunikation zwischen Akteuren, Geräten und Verträgen auf der Plattform wird sofort übermittelt. Es werden keine Daten zurückgehalten, aggregiert oder zeitverzögert übermittelt. Diese Anforderungen treffen keine Aussage über die Verarbeitungsdauer der Daten und haben damit keine Relevanz in Bezug auf die Wahl der technischen Basis. Somit werden die Anforderungen dieser Klasse für die weitere Analyse ignoriert.

Die sechste Level-2 Subklasse der *Software-Anforderungen* unter dem Sammelbegriff der *Nicht-Funktionalen Anforderungen* heißt *Portabilität* (Portability) und beschreibt die Fähigkeit des Gesamtsystems von einer Hardware bzw. Umgebung in eine andere migriert zu werden. In diesem Kontext existiert eine Anforderung (P1.2.1) der Userstory P1, welche die automatisierte Installation und Bereitstellung der Software definiert. Hierbei handelt es sich nicht um eine Technologie-entscheidende Anforderung. Demnach wird diese Anforderungsklasse in der weiteren Analyse nicht beachtet.

Die siebte Level-2 Subklasse der *Software-Anforderungen* unter dem Sammelbegriff der *Nicht-Funktionalen Anforderungen* nennt sich *Ausfallsicherheit* (Reliability) und beschreibt, wie gut ein System unter bestimmten Bedin-

gungen die geforderten Funktionalitäten durchführen kann. Anforderung SA2.2.2 definiert, dass die Plattform keinen Single-Point-of-Failure (**SPoF**) besitzen darf. Dies zeigt eine generelle Eigenschaft auf und ist im Kontext eines dezentralen Systems wie des **DLTs** nicht weiter von Relevanz. Daneben fordert Anforderung SA2.2.1, dass die Plattform in der Lage ist, bis zu 10.000 Endgeräte zu verarbeiten, ohne Einbußen in der Funktionalität oder der Geschwindigkeit der Verarbeitung. Diese Anforderung muss bei der Wahl der zugrundeliegenden **DLT**-Lösung beachtet werden, da hierbei Performanz und Verfügbarkeit beeinträchtigt werden.

Die achte Level-2 Subklasse der *Software-Anforderungen* unter dem Sammelbegriff der *Nicht-Funktionalen Anforderungen* wird als *Sicherheit* (Security) bezeichnet und befasst sich mit der Thematik rund um Software- und Datensicherheit. Diese Klasse beinhaltet 16 Anforderungen (A1.1.1, A1.2.3, A1.2.4, A1.2.5, A1.3.5, A1.3.9, M3.2.2, C2.2.1, SEC1.1.2, SEC1.2.1, SEC1.2.2, SEC3.1.1, SEC3.1.2, SEC3.2.1, SA2.1.1 und SA2.1.2) aus sechs Userstories (A1, M3, C2, SEC1, SEC3 und SA2). Die vorliegenden Anforderungen lassen sich grob in vier Subkategorien untergliedern: Verantwortlichkeit, Authentizität, Vertraulichkeit und Integrität. Verantwortlichkeit beinhaltet fünf Anforderungen, die unter Anderem die eindeutige Identifikation der Akteure sowie die Protokollierung von Aktivitäten und deren Zuordnung zu Accounts beschreiben. Während es sich bei dem Großteil um allgemeine Richtlinien handelt und dieser nicht von der konkreten technischen Umsetzung abhängig ist, so ist die generelle Identifikation von großer Relevanz für die Umsetzung auf Basis einer **DLT**-Lösung. Um einem Account (im Kontext von **DLT** auch Wallet) eine natürliche Person oder ein Unternehmen eindeutig zuordnen zu können, bedarf es einer Instanz, die auf der Plattform agiert und diese Informationen bereitstellt. Eine mögliche Umsetzung im Kontext **DLT** wäre die Implementierung eines entsprechenden Oracles, welches Personen und Unternehmen einer Wallet zuordnet und umgekehrt.

Die nächste Subkategorie - Authentizität - beinhaltet eine Anforderung, die die Zugriffsbeschränkung zu den Wallets (Konten) beschreibt. Da Wallets auf einer **DLT** eine Kombination aus einem öffentlichen und einem privaten Schlüssel sind und der private der PIN-Nummer eines Kontos entspricht, besteht eine implizite Zugriffsbeschränkung; es liegt hierbei keine **DLT**-Relevanz vor.

Der Inhalt von Nachrichten zwischen Akteuren sowie der Vertragsinhalt abgeschlossener Verträge unterliegt der Vertraulichkeit, darf also nur von beteiligten bzw. berechtigten Akteuren eingesehen werden. Da Transaktionen auf **DLT**-Lösungen generell öffentlich einsehbar sind, liegt hier eine **DLT**-Relevanz vor: Es muss dafür gesorgt werden, dass der Inhalt von Transaktionen und Smart-Contracts vertraulich behandelt werden kann.

Die Subkategorie Integrität hat den größten Anteil: Insgesamt acht Anforderungen wurden für den vorliegenden Anwendungsfall ermittelt, wobei Dateninkonsistenzen, Datenverlust und Manipulationssicherheit im Fokus stehen. Diese Eigenschaften entsprechen in etwa dem, was einen Distributed Ledger ausmacht, und sind deshalb zunächst einmal nicht weiter relevant.

vant in Bezug auf die Umsetzung mittels eines **DLT**. Die Abbildung eines Vertrags muss allerdings so gestaltet werden, dass der Vertragsgegenstand nicht manipuliert werden kann. Dies ist bei der Implementierung des Vertrags zu beachten und hat demnach eine Auswirkung auf die **DLT**-Relevanz und muss in der weiteren Analyse beachtet werden.

Die neunte Level-2 Subklasse der *Software-Anforderungen* unter dem Sammelbegriff der *Nicht-Funktionalen Anforderungen* heißt *Benutzbarkeit* (Usability) und befasst sich mit dem Thema **UX**. Diese Klasse beinhaltet zwei Anforderungen (C3.1.2 und C3.2.1) der Userstory C3 und besitzt keine **DLT**-Relevanz, da es um die Schnittstelle zum Endbenutzer geht und nicht um die technologische Basis der Plattform. Somit wird diese Klasse nicht weiter beachtet.

In den vorherigen Abschnitten wurden alle **DLT**-relevanten Anforderungen der verschiedenen Klassen identifiziert. Die Tabelle 5.1 fasst diese zusammen. Im Laufe der Untersuchung auf **DLT**-Relevanz wurde deutlich, dass die Einteilung nach Anforderungsklassen nur einen geringen Beitrag zur Identifikation der relevanten Anforderungen leisten kann. Selbst die Einteilung in verschiedene Themenbereiche konnte nur einen kleinen Mehrwert liefern, indem die Übersichtlichkeit - trotz der hohen Anzahl an Anforderungen - gewahrt werden konnte. Mögliche Gründe und Auswirkungen werden später in Kapitel 8 aufgezeigt und diskutiert. Dennoch konnte die Klassifizierung dazu eingesetzt werden, um aus den unterschiedlichen Perspektiven heraus eine möglichst umfassende Anforderungsliste zu generieren.

5.5 ANFORDERUNGSTRANSFER AUF DLT

Die Gesamtmenge der 84 Anforderungen wurde eingehend analysiert; dabei wurden 15 **DLT**-relevante Anforderungen identifiziert. Um geeignete **DLTs** auszuwählen, die für eine prototypische Verprobung in Frage kommen, werden die relevanten Anforderungen im Folgenden in **DLT**-Eigenschaften übersetzt.

SMART-CONTRACTS Acht der **DLT**-relevanten Anforderungen (A1.3.1, A1.3.2, A1.3.5, A1.3.7, A1.3.8, A1.3.9, A1.3.10 und BD4.2.1) beschreiben das Erstellen, das Ändern und den Aufbau von Verträgen. Damit **DLTs** Vertragsregeln prüfen und entsprechende Aktionen in die Wege leiten können, setzt dies voraus, dass die Implementierung Smart-Contracts unterstützt.

ORACLE-SERVICES Drei der **DLT**-relevanten Anforderungen (A1.1.1, A1.1.3, A1.1.5) beschreiben die Identifizierung und Verifizierung von Stakeholdern und deren Rollen. Diese Informationen können auf **DLTs** mittels Oracle-Services publiziert, gepflegt und genutzt werden. Daher ist es notwendig, dass die zugrundeliegende Implementierung Oracle-Services implementiert.

ID	Inhalt	Level-1	Level-2
A1.1.1	Jeder Akteur auf der Plattform kann eindeutig identifiziert werden.	Software	Security
A1.1.3	Ein Akteur agiert immer mit einer bestimmten Rolle auf der Plattform: Manufacturer, Customer, Supplier, Service-Provider oder Gerät. Ein Akteur kann mehrere Rollen haben.	Software	Functional
A1.1.5	Ein Akteur hat eine (mehrere) verifizierte Rolle(n).	Software	Functional
A1.2.5	Akteure können nur den Inhalt ihrer eigenen Nachrichten einsehen.	Software	Security
A1.3.1	Akteure schließen Verträge über die Plattform ab.	Software	Functional
A1.3.2	Verträge sind rechtlich bindend.	Software	Functional
A1.3.5	Der Vertragsgegenstand kann nicht durch Dritte manipuliert werden.	Software	Security
A1.3.7	Akteure können komplexe Vertragskonstrukte umsetzen. Verträge haben einen Status. Diese können "Aktiv", "In Erzeugung" oder "Inaktiv" sein.	Software	Functional
A1.3.8	Akteure können ihre Verträge im Nachhinein ändern.	Software	Functional
A1.3.9	Akteure können nur ihre eigenen Verträge ändern.	Software	Security
A1.3.10	Eine Vertragsänderung bedarf der Zustimmung aller beteiligten Akteure.	Software	Functional
A1.3.11	Erbrachte Leistungen werden kostenpflichtig verrechnet.	Software	Functional
M1.1.3	Geräte sind nicht immer mit der Plattform verbunden.	Software	Functional
BD4.2.1	Ein Abrechnungsmodell wird in einem Vertrag abgebildet.	System	Business
SA2.2.1	Die Plattform ist in der Lage, die Kommunikation und Datenverarbeitung bei bis zu 10.000 Endgeräten durchzuführen.	Software	Reliability

Tabelle 5.1: DLT-relevante Anforderungen

ZAHLUNGSMITTEL Die Anforderung A1.3.11 beschreibt die kostenpflichtige Abrechnung erbrachter Leistungen. Übersetzt in die DLT-Welt bedeutet das, dass die Implementierung ein Zahlungsmittel bereitstellen muss, damit erbrachte Leistungen gemäß des Pay-As-You-Use Modells abgerechnet werden können.

ASYNCHRONITÄT Die Anforderung M1.1.3 definiert, dass Endgeräte, bedingt durch Verbindungsprobleme oder Ähnliches nicht dauerhaft mit der Plattform verbunden sind. Da eine erbrachte Dienstleistung, wie zum Beispiel eine erzeugte Tasse Kaffee, sofort abgerechnet und bei Nicht-Vorhandensein von Guthaben gar nicht erst erzeugt werden soll, muss die Implementierung eine Form von Asynchronität umsetzen. Das bedeutet, dass Transaktionen auch außerhalb des Netzwerkes manipulationssicher und korrekt durchgeführt werden müssen. Dies kann durch die Implementierung von State-Channels erfolgen.

PERFORMANZ Anforderung SA2.2.1 definiert die Performanz des Systems nach folgenden Annahmen: Bei durchschnittlich 2.5 Tassen Kaffee pro Arbeitstag (kalkuliert mit neun Stunden) und Mitarbeiter und einer Verteilung von 40 Mitarbeitern auf eine Kaffeemaschine ergibt sich bei einer Auslastung von 10.000 vermieteten Kaffeemaschinen eine benötigte Performanz von 31 Transaktionen pro Sekunde ($2.5 * 40 * 10.000 / 32.400 = 31$).

VERSCHLÜSSELUNG Anforderung A1.2.5 fordert, dass Akteure nur den Inhalt ihrer eigenen Nachrichten einsehen können. Um dies zu ermöglichen, muss der Payload von Transaktionen sowie der Inhalt von Smart-Contracts verschlüsselt und damit nur für beteiligte Parteien einsehbar sein.

AUSWAHL RELEVANTER DLTS

In den vorherigen Kapiteln wurden der beispielhafte Anwendungsfall sowie dessen **DLT**-relevante Anforderungen aufgezeigt. In diesem Kapitel wird darauf aufbauend eine Marktübersicht möglicher **DLTs** gegeben und auf die Erfüllung der Anforderungen überprüft.

6.1 VORGEHEN

Es muss ein geeignetes Vorgehen erarbeitet werden, um aus der unüberschaubaren Menge an Blockchain-Lösungen eine passende Untermenge auszuwählen und dabei keine wichtigen Implementierung zu übersehen. Im Folgenden werden vier mögliche Kriterien vorgestellt, nach denen Blockchain-Lösungen bewertet werden können:

BUSINESS RELEVANCE Mitte April 2019 veröffentlichte das Wirtschaftsmagazin Forbes einen Artikel [11], der die eingesetzten Blockchain-Technologien großer, internationaler Unternehmen auflistet. Die daraus abzuleitende Relevanz für das internationale Business-Umfeld im Bereich Blockchain stellt einen Indikator dar, der bei der Auswahl einer Blockchain-Lösung berücksichtigt werden muss. Es wurden alle Blockchain-Implementierungen berücksichtigt, die mehr als zwei große Unternehmen betreffen.

GITHUB ACTIVITY Die Mehrheit der Blockchain-Entwicklungsprojekte sind open-source Projekte; der Quellcode ist meist frei verfügbar und auf Github öffentlich einsehbar. Ein wichtiger Indikator für Auswahl einer **DLT**-Lösung ist die Aktivität der Entwickler auf Github: Es wird bewertet, wie regelmäßig Weiterentwicklungen stattfinden und wie interessiert die Community die Änderungen verfolgen. Je größer die Aktivität und Beliebtheit, desto wahrscheinlicher werden aktuelle Forschungsergebnisse und Neuerungen in die Lösung eingebaut. Um diese Werte vergleichen zu können, wurde sich der Quellen www.coincodecap.de und www.cryptomismo.de bedient: Die Anzahl an Commits, aktiven Entwicklern, interessierten Beobachtern und weiteren Kennzahlen wurde gewichtet und bewertet. Das Ergebnis ist ein Ranking der aktivsten Blockchain-Projekte auf Github.

BLOCKCHAIN ACTIVITY Die Website www.blocktivity.info misst die Aktivität einer Blockchain-Plattform, indem es die Anzahl an Operationen (Transaktionen, Votes, Blogposts, etc.) verschiedener Zeitpunkte mit der Marktkapitalisierung in Relation setzt. Darüber hinaus werden Angaben über die tatsächlich verwendeten und noch verfügbare Kapazitäten der Lösungen gemacht. Diese Angaben helfen, verschiedene

Lösungen gegenüberzustellen und Kapazitäten abzuschätzen. Für die Relevanz im Kontext der Marktübersicht wurden die besten zehn Lösungen hinsichtlich Blockchain-Aktivität berücksichtigt.

IOT SUITABILITY Da diese Arbeit von der Synergie zwischen **DLT** und **IOT** handelt, bietet es sich an, das Themenfeld **IOT** bei der Auswahl zu berücksichtigen. Dazu wurden die zehn wertvollsten (nach Marktkapitalisierung) Blockchain-Lösungen, die als **IOT**-Lösung bei der Informationsplattform www.cryptoslate.com geführt werden, berücksichtigt.

Darüber hinaus fokussiert sich diese Arbeit auf eine Auswahl eigenständiger Blockchains; ERC-Token¹ oder ähnliche Implementierungen (Blockchains basierend auf anderen Blockchains) wurden nicht weiter beachtet. Die genauen Daten der einzelnen Kriterien sind im Anhang dieser Arbeit zu finden.

6.2 MARKTÜBERSICHT DLTS

Nach den im vorherigen Abschnitt vorgestellten Kriterien wurden 30 Blockchain-Lösungen identifiziert. Eine detaillierte Übersicht der Einzel-nachweise ist im Anhang zu finden. Die Kriterien wurden folgendermaßen gewichtet: Die Business-Relevanz wird als wichtigstes Kriterium bewertet. Die IOT-Zugehörigkeit wird wichtiger als die Aktualität aber etwas geringer als die Business-Relevanz bewertet. Die Aktualität der Blockchain unterteilt sich in Blockchain-Aktivität und Github-Aktivität; diese werden gleich, al-lerdings geringer als die IOT-Zugehörigkeit gewichtet.

Alle Lösungen werden überprüft, ob sie eine oder mehrere Kriterien erfüllen. Für jedes erfüllte Kriterium wurden der Lösung entsprechend der Gewich-tungen Punkte angerechnet. Die Tabelle 6.1 listet die Erstauswahl gemäß der genannten Kriterien auf.

Die Blockchain-Lösung Ethereum führt die Rangliste mit vier Punkten an; das Schlusslicht stellt unter Anderem Zcash mit einem Punkt dar. Um für die weitere Betrachtung von Interesse zu sein, muss eine Lösung zu den Top10 (nach Punkten) gehören; dies entspricht 2 Punkten. Dadurch ergeben sich 11 mögliche Kandidaten (mit mind. 2 Punkten) für die Untersuchung, inwieweit diese die **DLT**-relevanten Anforderungen (vgl. Tabelle 5.1) erfüllen.

6.3 ANFORDERUNGSERFÜLLUNG

In Kapitel 5.5 wurden die zurvor als **DLT**-relevant eingestuften Anforderun-
gen in den Kontext **DLT** übersetzt. Dabei ergaben sich sechs Funktionali-täten, die eine Blockchain-Lösung implementieren muss, um für den Ein-satz im vorliegenden Anwendungsfall geeignet zu sein. Diese waren Smart-Contracts, Zahlungsmittel, Oracle-Services, Asynchronität, Performanz und Verschlüsselung. Die Tabelle 6.2 zeigt die 11 verbliebenen Kandidaten und deren Anforderungserfüllung alphabetisch geordnet auf. Dabei wird bewer-tet, ob eine Anforderung erfüllt ist [*yes*] oder nicht [*no*]. Kann eine Anfor-

¹ Blockchains basierend auf einem Ethereum-Standard; keine eigenständige Blockchain.

	Business Relevance	Github Activity	Blockchain Activity	IOT	TOTAL
	2	1	1	1,5	
Bitcoin	x	x			3
Bitcoin SV			x		1
BitcoinCash	x	x			3
Cardano		x			1
Corda	x				2
Cosmos		x			1
EOS		x	x		2
Ethereum	x	x	x		4
Hyperledger	x				2
INT Chain				x	1,5
IOST			x		1
IoT Chain				x	1,5
IOTA		x		x	2,5
KIN			x		1
LBRY Credits		x			1
Lisk		x			1
Monero		x			1
Nano			x		1
Particl		x			1
Quorum	x				2
Ripple	x				2
Ruff				x	1,5
SDChain				x	1,5
Steem			x		1
Stellar		x	x		2
Syscoin		x			1
Telos			x		1
Tron		x	x		2
WAVES		x			1
Zcash		x			1

Tabelle 6.1: Erstauswahl von DLT-Lösungen

	Smart- Contracts	Payment	Oracle- Services	Perf (TPS)	Async.	Tx Encrypt.
Bitcoin	(yes)	yes	(yes)	<10	yes	no
BitcoinCash	(yes)	yes	(yes)	<100	no	no
Corda	yes	(yes)	yes	~1000	yes	yes
EOS	yes	yes	yes	>1000	yes	no
Ethereum	yes	yes	yes	>10	yes	yes
Hyperledger	yes	(yes)	yes	-	yes	yes
IOTA	no	yes	no	>100	yes	yes
Quorum	yes	yes	yes	<1000	yes	yes
Ripple	no	yes	no	>1000	yes	no
Stellar	yes	yes	(yes)	>1000	yes	no
Tron	yes	yes	yes	<1000	yes	no

Tabelle 6.2: Erfüllung der DLT-relevanten Anforderungen

derung nur teilweise, sehr schwierig, oder nur unter bestimmten Voraussetzungen erfüllt werden, so wurde diese Anforderung entsprechend mit [(yes)] bewertet. Die Informationen der Tabelle wurden den technischen Spezifikationen oder den offiziellen Internetseiten der jeweiligen Lösungen entnommen.

Die Performanz bei privaten Blockchains (vgl. Kapitel 2.1.4) wurde ausgeklammert oder nicht angegeben, da diese sehr stark von der zugrundeliegenden Hardware abhängig ist. Darüber hinaus handelt es sich bei den Performanz-Werten um grobe Richtwerte, die teilweise nur unter Laborbedingungen erreicht werden können. Die tatsächlichen Tageswerte weichen zum Teil deutlich davon ab, daher sind diese Werte als Richtwerte zu verstehen und in der folgenden Bewertung als solche zu handhaben.

6.4 BEWERTUNG, RANKING & AUSWAHL

Tabelle 6.2 zeigt mögliche DLT-Kandidaten und deren Erfüllung der übersetzten, DLT-relevanten Anforderungen auf. Die zentrale Anforderung ist die Ermöglichung von asynchronen Transaktionen bei Verbindungsverlust von Endgeräten. Lediglich Bitcoin-Cash bietet diese Funktionalität nicht, womit es als möglicher Kandidat ausscheidet. Eine weitere, entscheidende Anforderung ist die Bereitstellung von Smart-Contract Funktionalität. Dies ist sowohl bei IOTA als auch bei Ripple nicht gegeben, wodurch beide im weiteren Verlauf nicht mehr betrachtet werden. Die Möglichkeit, Transaktionen oder Smart-Contracts zu verschlüsseln, sodass nur beteiligte Parteien den Inhalt einsehen können, ist bei Bitcoin, Bitcoin-Cash, EOS, Ripple, Stellar und Tron nicht gegeben, weshalb diese im weiteren Verlauf vernachlässigt werden. Übrig bleiben Corda, Ethereum, Hyperledger und Quorum. Corda und

Hyperledger bieten beide keine native Währung an; es besteht allerdings die Möglichkeit, beispielsweise mittels Smart-Contracts eine Token-Lösung umzusetzen. Corda, Quorum und Hyperledger sind für den Einsatz in privaten Blockchains vorgesehen, Ethereum kann darüber hinaus auch als Public-Blockchain zum Einsatz kommen. Bezuglich der Performanz steht Ethereum mit etwa 20 Transaktionen pro Sekunde vergleichsweise schlecht dar. Es zeichnet sich ab, dass die vier Lösungen Corda, Hyperledger, Ethereum und Quorum mögliche Kandidaten für eine prototypische Verprobung des vorliegenden Anwendungsfalls sind. Quorum ist in der Lage, sämtliche Anforderungen zu erfüllen. Es handelt sich um eine von der US-Bank JPMorgan entwickelte Blockchain basierend auf Ethereum. Dabei werden neue Ethereum-Releases mit Mechanismen für erhöhte Privatsphäre, alternativen Konsensmechanismen und als private oder permissioned Blockchain bereitgestellt. Hierbei liegt allerdings auch die Problematik, die ebenfalls Corda und Hyperledger betreffen: Die zentrale Trustless-Eigenschaft geht in privaten und zugangsbeschränkten Blockchains verloren und die Transparenz wird verringert. Darüber hinaus werden die Eintrittshürden für die Teilnahme am Blockchain-Netzwerk stark erhöht. Aufgrund dessen und der Tatsache, dass Quorum zum größten Teil aus Ethereum-Quellcode besteht, fällt für die praktische Verprobung in dieser Arbeit die Wahl der Blockchain-Lösung auf Ethereum. Die nicht optimalen Transaktionsraten werden an dieser Stelle vernachlässigt; aktuelle Entwicklungen bezüglich der Skalierungsansätze von Blockchains (vgl. Kapitel 2.1.7) lassen darauf hoffen, mittelfristig eine deutlich verbesserte Performanz erzielen zu können.

UMSETZUNG

In diesem Kapitel wird die prototypische Verprobung des Anwendungsfalls vorgestellt; dazu werden die Architektur und der Aufbau der Implementierung aufgezeigt. Das Vorgehen für das Testing und das Deployment werden vorgestellt und Betrachtungen zu Datenschutz und Privatsphäre durchgeführt. Die Anforderungserfüllung wird geprüft und für alle **DLT**-relevanten Anforderungen im Detail untersucht. Im Fokus dieser Betrachtungen steht die Eignung von **DLT** für den **IOT**-Anwendungsfall.

7.1 ARCHITEKTUR UND AUFBAU

Die prototypische Verprobung des Anwendungsfalls wurde auf Basis der Ethereum-Blockchain umgesetzt. Die Gesamtarchitektur wurde mittels Unified Modelling Language (**UML**)-Komponentendiagramm modelliert und ist in Abbildung 7.1 zu sehen.

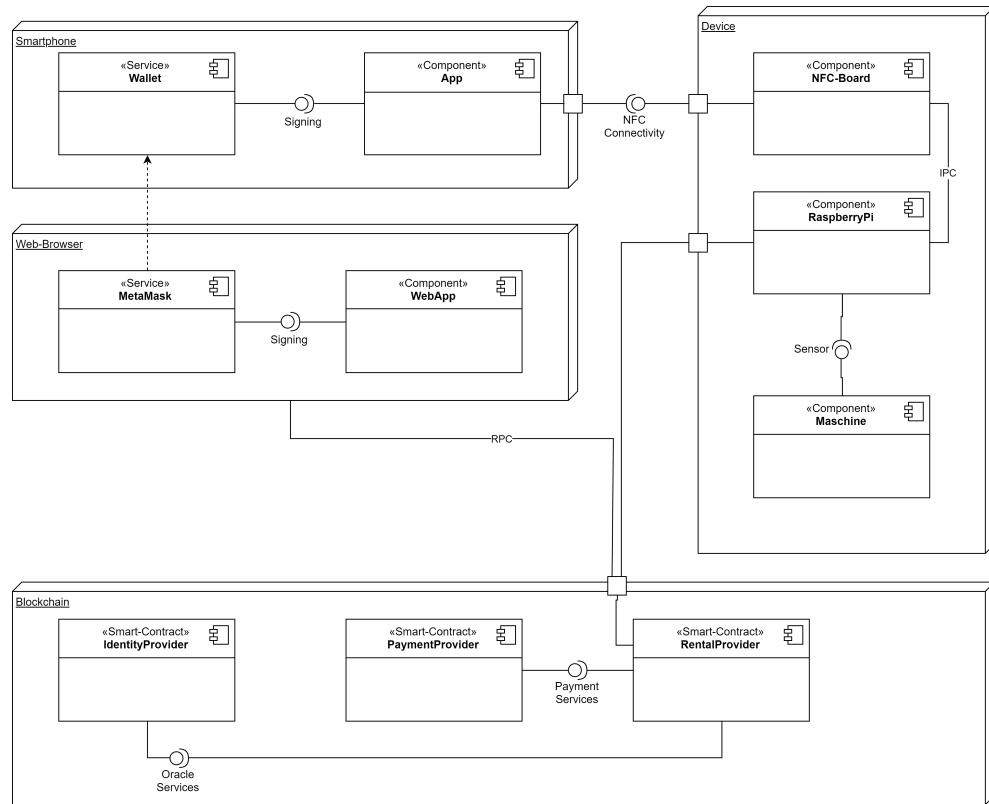


Abbildung 7.1: Architektur als UML-Komponentendiagramm

Die Umsetzung wurde zunächst so vorgenommen, dass ein Benutzer durch ein Unternehmen dargestellt wird. Die Mitarbeiter eines Unterneh-

mens, die den Kaffee konsumieren, sind vorerst nicht als eigenständige Akteure auf der Plattform tätig und agieren über ihr Unternehmen mit den Geräten.

Jeder Benutzer besitzt eine Wallet, auf die nur er mittels des passenden Private-Keys Zugriff hat. Diese Wallet wird benötigt, um den Benutzer zu identifizieren und Bezahlvorgänge durchzuführen. Über das Browser-Plugin Metamask¹ kann der Benutzer Zahlungen innerhalb der Web-App autorisieren und sich dort anmelden. Die Web-App wurde als React-Anwendung entwickelt und wird im Browser ausgeführt. Per [RPC](#) ist sie in der Lage, auf Informationen innerhalb der Blockchain zuzugreifen und mit Smart-Contracts zu interagieren. Es wurden drei Smart-Contracts entwickelt: Der IdentityProvider fungiert als Oracle-Service und hält Informationen über Identitäten und deren Rollen. Der PaymentProvider ist zuständig für die Zahlungsabwicklungen und hält Payment-Channel und Zahlungshistorien der Verträge. Letztere werden über den RentalProvider abgebildet, angefragt und verwaltet. Der zentrale Gegenstand des Mietvertrages im vorliegenden Anwendungsfällen ist die Kaffeemaschine. Diese besitzt interne Sensoren, um über den aktuellen Zustand zu informieren. Die Maschine als Ganzes wird ergänzt durch ein NFC-Modul und einen daran angeschlossenen Raspberry-Pi Einplatinencomputer. Dieser übernimmt die Kommunikation mit den Gerät-internen Sensoren, dem NFC-Modul und der Blockchain und stellt damit das Herzstück des Geräts dar. Mit einem Smartphone ist der Benutzer in der Lage, mit der Kaffeemaschine per Near Field Communication ([NFC](#)) zu kommunizieren². Die dazu notwendige App greift zur Identifikation und Autorisierung von Bezahlvorgängen auf das hinterlegte Wallet zu. Es handelt sich dabei um die gleiche Wallet, welche auch in der Web-App hinterlegt wurde und auf welche mittels Metamask zugegriffen wird.

7.2 DEPLOYMENT

Die Smart-Contracts wurden auf dem öffentlichen Kovan-Testnet bereitgestellt. Es handelt sich bei Kovan um ein Proof-of-Authority ([PoA](#))-Netzwerk, das zu Testzwecken ausgewählt wurde, da die Blockzeit bei nur etwa vier Sekunden (vgl. <https://kovan.etherscan.io/>) liegt. Das Ropsten-Testnet, welche auf [PoW](#) basiert und dem Mainnet am ähnlichsten ist, benötigt für das Münzen eines Blocks etwa 15 Sekunden³. Tabelle 7.1 listet die Adressen auf, unter denen die Smart-Contracts erreichbar sind.

Das Frontend wurde per Heroku deployed und ist unter <https://dlt-iot-synergy.herokuapp.com/> erreichbar. Nach eigenen Angaben handelt es sich bei Heroku um eine "Platform as a Service (PaaS), die Entwickler dazu befähigt, Anwendung vollumfänglich in der Cloud zu bauen und

¹ Verbreitetes Ethereum-Wallet Plugin für Chrome und Firefox

² Voraussetzung hierfür ist ein funktionsfähiger NFC-Chip im Smartphone

³ Im Laufe der Entwicklung kam es vor, dass Transaktionen teils mehrere Minuten benötigten, bis sie durch das Netzwerk bestätigt wurden. Deshalb wurde zunächst auf Kovan umgeschwenkt.

Smart-Contract	Kovan-Adresse
Rental-Provider	0xf25F1F12630158d963a9609950C3e379c65617dA
Identity-Provider	0xA17351BfA16dAE1FD285e11AcC00882Eb459C7cb
Payment-Provider	0x7d17DA28604A7bB2E121D634012C086A6BbF6E2e

Tabelle 7.1: Adressen der Smart-Contracts auf dem öffentlichen Kovan Testnet

zu betreiben". Mittels Git push-Befehl kann aus dem lokalen Repository der Code in eine Heroku-App deployed werden.

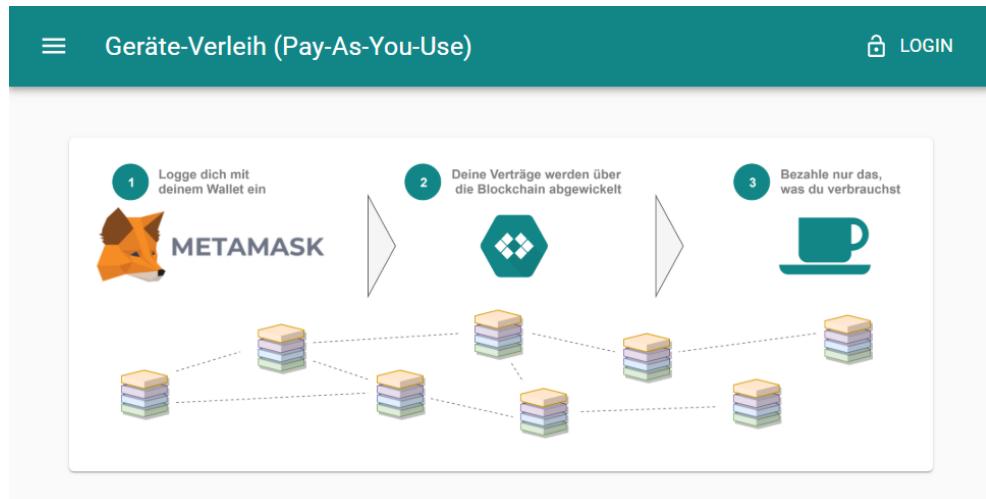


Abbildung 7.2: Frontend, bereitgestellt mit Heroku

Die Smartphone-App wurde lokal auf einem Android-Device von Samsung installiert.

7.3 TESTAUFBAU

Für Smart-Contracts auf Ethereum-Basis existiert die Truffle-Suite, die ein umfangreiches Toolset für die Entwicklung und das Testen von Smart-Contracts bereitstellt. Der Entwicklungsprozess wird durch eine lokale Blockchain-Umgebung vereinfacht, die das Deployment und Testing beschleunigt.

Mittels Unit-Tests wurde sichergestellt, dass die Funktionalität gemäß den Anforderungen gegeben ist. Die Testabdeckung wurde durch das Tool `solidity-coverage` überprüft, die Ergebnisse werden in Abbildung 7.3 dargestellt. Die Grafik zeigt die prozentuale und absolute Abdeckung von Statements, Funktionen und Code-Zeilen an.

End-to-End ([E2E](#))-Tests wurden manuell durchgeführt: Alle Bestandteile der gesamten Anwendung wurden gestartet und der Anwendungsfall Schritt für Schritt durchgeführt. Aus Benutzersicht konnten alle Funktionalitäten erfolgreich getestet werden. Das Erstellen und Abschließen von Miet-

File		Statements		Functions		Lines	
Ownable.sol	<div style="width: 100%;"> </div>	100%	5/5	100%	3/3	100%	6/6
RentalProvider.sol	<div style="width: 96.64%;"> </div>	96.64%	144/149	96.15%	25/26	96.79%	151/156
IdentityProvider.sol	<div style="width: 96.36%;"> </div>	96.36%	53/55	100%	17/17	95.83%	46/48
PaymentProvider.sol	<div style="width: 93.55%;"> </div>	93.55%	58/62	86.67%	13/15	93.75%	60/64

Abbildung 7.3: Testabdeckung der Solidity Smart-Contracts

verträgen über die Web-App erfolgte ebenso wie die Abrechnung mittels Smartphone reibungslos.

7.4 ANFORDERUNGSUMSETZUNG

In Kapitel 5.5 wurden die zuvor identifizierten Anforderungen in DLT-Spezifika übersetzt, um für die darauffolgende Auswahl eines geeigneten DLTs überprüfbar zu sein. Diese lauteten:

- Smart-Contracts
- Oracle-Services
- Zahlungsmittel
- Asynchronität
- Performanz
- Verschlüsselung

Im Folgenden werden diese überprüft, ob und inwieweit den Anforderungen gerecht werden konnte.

7.4.1 Smart-Contracts

Die implementierten Smart-Contracts wurden nach bestem Wissen und Gewissen umgesetzt. Damit ein Smart-Contract rechtskonform agiert und um die Vertragslogik nach geltendem deutschen Recht korrekt abzubilden, bedarf es ausführlicher rechtlicher Beratung durch entsprechende Experten und Anwälte. Dieser zeitaufwändige Prozess wurde im Rahmen dieser Arbeit nicht durchgeführt. Bei einer Implementierung, die über die Machbarkeitsstudie hinausgeht und produktiv eingesetzt werden soll, muss dieser Punkt berücksichtigt werden. Damit wurde die Anforderung A1.3.2 nicht erfüllt.

Das Anpassen der Smart-Contracts aufgrund von Vertragsänderung oder ähnlichen Anpassungen wurde durch die Anforderung A1.3.8 gefordert. Sie beschreibt, dass Verträge im Nachhinein aktualisierbar sein müssen. Die Vertragslogik wurde mittels Smart-Contract umgesetzt: Einmal in der Blockchain gespeichert, sind Daten nicht mehr veränderlich. Es gibt

dennoch Möglichkeiten, einen benötigten Mechanismus einzubauen, um die Verträge im Nachhinein anzupassen. Dazu kann man sich sogenannter Proxy-Smart-Contracts bedienen. Die Grundidee dabei ist, wie in einem Netzwerk, ein zentrales Eingangstor zu haben, welches fest definiert ist und sich später nicht mehr ändert. Dieser Proxy verweist dann auf die jeweils aktuelle Version des benötigten Smart-Contracts. Ändert sich der Code durch Vertragsänderungen oder sonstige Updates, kann die aktualisierte Version in die Blockchain transferiert werden. Anschließend wird dem Proxy die Adresse des neuen Contracts mitgeteilt. Bei Anfragen an den Proxy leitet dieser den Anfragenden fortan an den neuen Vertrag weiter (der alte Vertrag bleibt dennoch weiterhin bestehen). Diese Umsetzung wurde im Zuge dieser Masterarbeit nicht geleistet, da die Umsetzung dieses Ansatzes viel Zeit und Aufwand benötigt, um die gewünschten Funktionalitäten zuverlässig zu implementieren und ein umfangreiches Toolset dazu bereits existiert. Da diese Arbeit als Machbarkeitsstudie aufgebaut wurde, wurde an dieser Stelle auf die Implementierung verzichtet. Es sei auf das Software Development Kit ([SDK](#)) und die auditierten Smart-Contracts von OpenZeppelin (<https://openzeppelin.com/>) verwiesen; dort wird ein umfangreiches Toolset zur Entwicklung robuster Smart-Contracts angeboten sowie Templates bereitgestellt, die das Upgrade-Management eines Smart-Contracts übernehmen. Die Nicht-Umsetzung dieser Anforderung verhindert nicht das Aufzeigen der generellen Machbarkeit.

7.4.2 *Oracle-Services*

Der Identity-Provider Smart-Contract wurde als Oracle Smart-Contract implementiert. Er hält Informationen zu Identitäten und Rollen. Diese Informationen werden nach dem Deployment außerhalb des Blockchain-Netzwerkes generiert und durch den Eigentümer des Smart-Contracts durch onchain Transaktionen an den Identity-Provider propagiert. Ab diesem Zeitpunkt fungiert der Smart-Contract als Oracle und kann durch andere Smart-Contracts nach den gespeicherten Informationen angefragt werden.

Das Aktualisieren und Entfernen von Informationen obliegt dem Besitzer des Smart-Contracts und ist als Sicherheitsmechanismus angedacht. Somit kann kein Dritter falsche Informationen oder Duplikate an das Oracle senden. Dieser Aufbau erfordert allerdings ein hohes Maß an Vertrauen gegenüber dem Oracle-Erststeller; da es sich allerdings um den Hersteller selbst handelt und dieser auch Besitzer der [IOT](#)-Geräte ist, kommt es im vorliegenden Anwendungsfall zu keinen Vertrauensproblemen. Wie bereits im Grundlagenkapitel (vgl. Kap. [2.1.2](#)) aufgezeigt, können auch mehrere Oracles verschiedener Anbieter parallel existieren, um den dezentralen Charakter der Anwendung zu stärken. Die vorgenommene Implementierung könnte auch erweitert werden, dass mehrere Eigentümer gemeinsam für die bereitgestellten Informationen verantwortlich sind und diese gemeinsam pflegen und aktualisieren.

7.4.3 Zahlungsmittel

Mit der Umsetzung auf der Ethereum-Plattform können Zahlungen mittels Ether abgewickelt werden. Darüber hinaus existieren Implementierungen auf Ether-Basis, sogenannte Token, die ebenfalls als Zahlungsmittel genutzt werden können. Um den massiven Kursschwankungen von Ethereum entgegenzuwirken, können sogenannte Stable-Coins eingesetzt werden, die durch besondere Algorithmen oder Einlagenabsicherung die Schwankungen unterbinden. Der Einfachheit halber wurde in dieser Arbeit Ether als Zahlungsmittel eingesetzt.

Eine zentrale Fragestellung, die sowohl Betreiber als auch Benutzer der Plattform interessiert, lautet: Was kostet die Nutzung? Die folgenden Berechnungen wurden auf Basis des Wechselkurses vom 06.02.2020 für 196.04€ pro 1ETH durchgeführt.

Der GAS-Preis⁴ ist ein Heelpunkt, mit dem die Bestätigungszeit von Transaktionen beeinflusst werden kann. Setzt man diesen auf einen hohen Wert (beispielsweise größer als 12 GWEI⁵), so werden Miner diese Transaktion bevorzugt behandeln, da sie an ihr entsprechend mehr verdienen. Somit hängt die Performance direkt an den Transaktionskosten, wobei eine natürliche Grenze vorliegt: Wie der Abbildung 7.4 zu entnehmen ist, liegt die Block-Zeit von Ethereum bei etwa 15 Sekunden. Unabhängig vom bezahlten GAS-Preis kann diese Grenze nicht unterschritten werden, da immer mindestens eine Blockzeit vergehen muss, damit die Transaktion in den Ledger aufgenommen wird.



Abbildung 7.4: Blockzeit von Ethereum innerhalb des letzten Jahres, Quelle: etherscan.io

Um eine einheitliche Kalkulation vorzunehmen, wird in den folgenden Berechnungen ein GAS-Preis von 5 GWEI angenommen; dieser Preis wurde auch für das Testen eingesetzt. Die Korrelation zwischen Preis und Performance wurde bereits erläutert. Wird eine erhöhte Performance benötigt, so kann dies mit einem höheren GAS-Preis erzielt werden.

⁴ GAS ist eine Ethereum-interne Einheit, mit der Rechenoperationen gemessen werden.

⁵ 1 WEI ist die kleinste Währungseinheit, mit der beispielsweise GAS bezahlt wird. 1GWEI = 1 Giga-WEI oder 10^9 WEI oder 10^{-9} ETH

In Tabelle 7.2 ist zu sehen, dass die Kosten für einen Benutzer zur Vertragserzeugung bei 35 Cent liegen. Die Transaktionsgebühr zum Aufladen des Payment-Channels ist mit drei Cent pro Aufladung verschwindend gering. Aus der Perspektive des Herstellers liegen die Kosten pro Vertragssinteraktion etwas höher bei 42 Cent zur Erstellung und 15 Cent für das Einlösen einer Quittung. Bei einer Endausbaustufe von 400.000 Benutzern und 10.000 Maschinen beläuft sich die jährliche Gebühr für das Einlösen der Quittungen (unter der Annahme, dass alle Quittungen einmal pro Woche eingelöst werden) auf 78.000€ bei einem Umsatz von 82.000.000€. Zu Vertragsbeginn fallen einmalig 4.200€ Gebühren an; diese werden vom Hersteller getragen. Die dieser Kalkulation zugrundeliegenden Werte sind im Anhang in den Tabellen C.2, C.3 und C.4 zu finden.

	GAS	ETH	EUR
Vertrag anfragen	197964	~ 0.00099	0.19
Vertrag annehmen	162743	~ 0.000814	0.16
Prepaid aufladen	28805	~ 0.000144	0.03
Vertrag erstellen	426609	~ 0.002133	0.42
Quittung einlösen	157927	~ 0.00079	0.15

Tabelle 7.2: Kosten für (Einmal-) Transaktionen aus Benutzer-Sicht (oben) und Hersteller-Sicht (unten) bei einem Gas-Preis von 5 GWEI. Im Anhang (C.3) finden sich die Screenshots, die die Angaben belegen.

Die derzeitige Transaktionsübertragung läuft direkt zwischen den beteiligten Parteien und der Blockchain, ohne dass dabei ein Intermediär zwischen geschaltet ist. Das ist in einem dezentralen System auch generell wünschenswert, führt aber dazu, dass im vorliegenden Anwendungsfall die Transaktionskosten von jeder Partei selbst getragen werden müssen. Dies ist aus Sicht des Herstellers meist weniger problematisch als aus Sicht der Benutzer, die häufig zu Beginn weder eine Wallet noch Kenntnis von Blockchains und deren Besonderheiten besitzen. Ein umfangreicher Onboarding-Prozess ist notwendig, um den Benutzer in das neue Blockchain-Ökosystem einzuführen. Dabei ist auch das Konzept der Transaktion und den damit verbundenen Kosten meist neu. Ein möglicher Ansatz, um den Benutzern (oder auch anderen Parteien) diese Kosten zu ersparen und das Onboarding zu vereinfachen, sind sogenannte Meta-Transaktionen (vgl. Kap. 10).

7.4.4 Asynchronität

Die Asynchronität der Kommunikation von IOT-Geräten ist ein zentraler Aspekt, der bei IOT-Anwendungsfällen berücksichtigt werden muss. Bei temporärem Konnektivitätsverlust müssen die Geräte dennoch in der Lage sein, ihrer Funktion nachzukommen und Daten zu einem späteren Zeitpunkt syn-

chronisieren zu können. Die vorgenommene Implementierung hat diese Anforderung durch den Einsatz von Payment-Channels umgesetzt. Diese wurde nicht nur zur Lösung des Skalierungsproblems (vgl. Kap. 2.1.7) eingesetzt, sondern darüber hinaus zur Einführung asynchroner Kommunikation zwischen Gerät und Blockchain genutzt. Die mittels Smart-Contract umgesetzten Payment-Channel erlauben es den Geräten, Zahlungsquittungen zu einem späteren Zeitpunkt einzulösen und damit die Benutzerinteraktion auch bei Konnektivitätsverlust aufrecht zu erhalten. Die Implementierung wurde wie folgt umgesetzt:

Bei Vertragseröffnung wird gleichzeitig zwischen Kaffeemaschine und Benutzer ein Payment-Channel eröffnet. Dieser wird mit einem Betrag aufgeladen (Prepaid; 12,50€), sodass schon vor der ersten Benutzung der Maschine ein Betrag zur Verbuchung zur Verfügung steht. Möchte der Benutzer einen Kaffee von der Maschine erhalten, so erstellt diese eine Quittung und überträgt diese per NFC an das Smartphone des Benutzers. Dieser kann anschließend mit seinem auf dem Smartphone befindlichen Private-Key die Quittung signieren und der Kaffeemaschine damit bestätigen, diesen Kauf durchgeführt zu haben. Die Kaffeemaschine bekommt anschließend die signierte Quittung per NFC zurückgesendet und kann die Signatur überprüfen. Ist diese korrekt, wird der Kaffee ausgegeben. Dieser Vorgang passiert off-chain und wird nicht per Transaktion an die Blockchain übermittelt. Dieser Vorgang kann nun so oft wiederholt werden, bis das Guthaben im Payment-Channel aufgebraucht ist. Ist dies der Fall, so muss der Benutzer zunächst sein Guthaben neu aufladen. Die Kaffeemaschine hält die zuletzt signierte Quittung so lange vor, bis ein definierter Zustand eintritt⁶. Anschließend schickt sie diese Quittung per Transaktion an die Blockchain und erhält das entsprechend signierte Guthaben aus dem Payment-Channel.

7.4.5 *Performanz*

Anforderung SA2.2.1 bezieht sich auf die Performanz, welche bei Ethereum mit etwa 20 Transaktionen pro Sekunde für eine direkte, synchrone Kommunikation nicht ausreichend ist. Um dieses Problem zu lösen, werden Payment-Channel (vgl. Kap. 2.1.7 und 7.4.4) eingesetzt: Dadurch kann die Zahl von etwa 1 Mio. Transaktionen pro Tag (31 TPS) auf ein Bruchteil (durchschnittlich 1,3 TPS) reduziert werden. Die genauen Kennzahlen werden im Folgenden detailliert betrachtet:

Aus Kostengründen wurden Tests und Deployment auf dem öffentlichen Kovan-Testnet durchgeführt. Eine produktionsreife Implementierung würde auf dem Ethereum-Mainnet betrieben werden, weshalb in diesem Abschnitt einige theoretische Betrachtungen und Hochrechnungen durchgeführt werden, um Aussagen über die Performanz der Gesamtanwendung treffen zu

⁶ Da eine Kaffeemaschine in der Regel nicht in der Nacht benutzt wird, könnte im Zeitraum zwischen 6 Uhr abends und 6 Uhr Morgens die Synchronisation stattfinden, sofern das Prepaid-Guthaben unter ein festgelegtes Minimum sinkt.

können.

Durch den Einsatz von Payment-Channels wurde ein Skalierungsansatz gewählt, welcher eine Menge von offchain Transaktionen auf zwei onchain Transaktionen reduziert (Öffnen und Schließen des Channels). Die folgenden Transaktionen werden onchain ausgeführt und haben eine Auswirkungen auf die Performanz:

VERTRÄGE ERSTELLEN Die Erstellung der Verträge benötigt insgesamt drei Transaktionen: Die Anfrage des Benutzers, die Erstellung des Vertrages durch den Hersteller und das Annehmen durch den Benutzer.

AUFLADEN DES PREPAID-GUTHABENS Durch Annehmen des Mietvertrages überweist der Benutzer initial einen Betrag an den Payment-Channel (das Öffnen des Channels geschieht bei der Vertragserzeugung). Ist das Guthaben aufgebraucht, so muss der Benutzer erneut eine Transaktion an den Payment-Channel senden, um sein Prepaid-Guthaben wieder aufzuladen.

EINLÖSEN VON QUITTUNGEN Das Schließen des Payment-Channels⁷ erfolgt durch eine Transaktion der Maschine an den Payment-Channel.

Zusammengefasst bedeutet das, dass drei Transaktionen anfallen pro Benutzer und Vertrag und eine Transaktion pro Maschine und Vertrag in einem Zeitintervall zwischen Vertragsbeginn und dem Zeitpunkt, wenn das Guthaben auf dem Payment-Channel aufgebraucht ist. An dieser Stelle sei angemerkt, dass die Anzahl an Transaktionen, die vom Benutzer ausgehen, nicht direkt gesteuert werden können. Um zu vermeiden, dass ein Benutzer zu geringe Beträge an den Payment-Channel transferiert, ist es von Vorteil, diesen beim Onboarding (also beim Erstellen des Mietvertrages) zu befragen, wie viel Kaffee er (und seine Mitarbeiter) im Durchschnitt konsumieren. Je nachdem, wie lange der Betrag auf dem Payment-Channel ausreichen soll, kann dem Benutzer ein Vorschlag zur Höhe des aufzuladenden Betrags gemacht werden. Der Benutzer entscheidet selbst, wann er einen Vertrag abschließen oder sein Prepaid-Guthaben aufladen möchte. Geht man jedoch mehrheitlich von passiveren Benutzern aus, die sich an den Empfehlungen der Plattform orientieren, kann man die Zahl der Transaktionen zumindest lenken.

Die Implementierung wurde so umgesetzt, dass ein Benutzer auf eine Kaffeemaschine Zugriff hat. Ein Benutzer entspricht in diesem Fall einem Unternehmen, dass wiederum durchschnittlich 40 Mitarbeiter für eine Kaffeemaschine einkalkuliert. Es existiert ein Payment-Channel pro Unternehmen und Kaffeemaschine, den die Mitarbeiter eines Unternehmens nutzen können. Andere Bezahlmodelle, in denen zum Beispiel der Mitarbeiter selbst den Kaffee bezahlt, sind ebenfalls umsetzbar. Hierbei kann auf

⁷ In dieser Implementierung wird der Payment-Channel nicht geschlossen, sondern bleibt dauerhaft bestehen. Das Transferieren von Geld erfolgt durch eine Redeem-Funktion, die Gelder und Guthaben zwischen Customer und Manufacturer transferiert.

den Einsatz von **DIDs** und **VCs** gesetzt werden, um Berechtigungen und Mitarbeiterverhältnisse abzubilden und nachzuweisen.

Die folgenden Berechnungen basieren auf der Annahme, dass sich im finalen, produktiven Umfeld etwa 10.000 Maschinen gleichzeitig im Einsatz befinden, ein Payment-Channel genug Guthaben für eine Woche Kaffee-Konsum hält. Dabei ist eine Kaffeemaschine durchschnittlich für ein Büro von 40 Mitarbeitern zuständig. Die grundlegenden Annahmen und Basiswerte, die dieser Kalkulation zugrundeliegen, sind im Anhang detailliert in den Tabellen [C.2](#), [C.3](#) und [C.4](#) aufgelistet.

Gemäß des Deutschen Kaffeeverbandes konsumiert jeder Deutsche im Schnitt 164 Liter Kaffee pro Jahr (vgl. [\[29\]](#)). Bei 0,2 Liter Fassungsvermögen einer Tasse ergibt das 820 Tassen Kaffee pro Jahr und Person. Das Jahr 2020 hat 230 Arbeitstage (bei 30 Tagen Urlaub pro Jahr), wodurch sich etwa 2.240 Tassen pro Tag und Person ergeben. Bei einem kalkuliertem Kaffeepreis von 0,25€ pro Tasse ergibt sich ein Umsatzvolumen pro Maschine und Woche von 157,69€. Nach der Annahme, dass das Prepaid-Guthaben eines Payment-Channels eine Arbeitswoche ausreichen soll, muss dieser mit mindestens 157,69€ aufgeladen werden; durch einen einkalkulierten Puffer und um einen glatten Betrag zu erreichen, wurde mit 200€ gerechnet. Das wöchentliche Aufladen geschieht durch eine onchain Transaktion, wodurch sich eine Auslastung von 10.000 Transaktionen pro Woche ergibt. Das Einlösen der Quittungen erzeugt ebenfalls 10.000 Transaktionen pro Woche, die durch die Maschinen ausgelöst werden. Zusammen ergeben sich demnach 20.000 Transaktionen pro Woche (5 Tage) bei dem vorliegenden IOT-Anwendungsfall mit 400.000 Personen und 10.000 Kaffeemaschinen. Damit würden insgesamt 0,046 Transaktionen pro Sekunde⁸ erzeugt; bei einer Transaktionsgeschwindigkeit von 15 TPS entspricht das etwa 0,3% der Auslastung des gesamten Ethereum-Netzwerkes.

Um die Transaktionen von Maschinen und Benutzern zu entkoppeln, wird folgende Lösung vorgeschlagen: Das Einlösen der Quittungen durch die Maschinen erfolgt in den Nachtstunden, da hier kein Kaffee konsumiert wird und demnach auch keine Aufladungen des Prepaid-Guthabens stattfinden. Damit nicht alle Maschinen gleichzeitig Transaktionen auslösen und damit den Transaktionspuffer verstopfen, können geeignete Mechanismen eingesetzt werden. Mögliche Ansätze wären:

- Erstellen einer mathematischen Funktion, die die Adressen der Kaffeemaschinen (bekannte Liste) als Input-Parameter verarbeitet und jeder Kaffeemaschine einen festgelegten Zeitraum zur Einlösung der Quittungen zuschreibt. Dieser Mechanismus könnte onchain im Payment-Channel hinterlegt werden und für die notwendige Lastverteilung sorgen.

⁸ 20.000 Transaktionen / 432.000 Sekunden (pro Arbeitswoche) = 0,046 Transaktionen pro Sekunde

- Verwendung einer Zufallsfunktion, die lokal auf den Maschinen ausgeführt wird und den Zeitpunkt des Einlösens zufällig bestimmt.
- Einlösen der Quittungen bei Unterschreiten eines Mindest-Guthabens. Verteilungsaspekt gegeben durch das unterschiedliche Konsumverhalten der Benutzer.

Das Aufladen des Prepaid-Guthabens durch den Benutzer kann nicht direkt beeinflusst werden (siehe oben), wird aber überwiegend zu den Tageszeiten durchgeführt werden. Hierbei können Engpässe entstehen, sobald viele Benutzer zur gleichen Zeit Transaktionen auslösen, wodurch das Aufladen länger dauern kann. Mögliche Ansätze zur Vorbeugung wären:

- Unterschiedlich hohe Empfehlungen geben, wie viel Euro aufgeladen werden sollen.
- Benutzer zu unterschiedlichen Zeiten an das Aufladen erinnern.
- Benutzer in Kategorien einteilen (Kaffee-Liebhaber, Gelegenheits-Konsument, ...) und entsprechende Aufladesummen und -zeitpunkte variieren.
- Implizit: Durch unterschiedliche Startzeitpunkte der Verträge verschieben sich auch die Lasten.

7.4.6 Verschlüsselung

Anforderung A1.2.5 beschreibt die Verschlüsselung von Transaktionsdaten, sodass Inhalte nur vom Eigentümer oder dem Adressaten einsehbar sind. Diese Funktionalität ist für das Zeigen der Machbarkeit einerseits nicht notwendig, für die Implementierung eines Live-Systems jedoch essentiell. Eine gängige Methode, um den Payload einer Transaktion zu verschlüsseln, wäre beispielsweise der Einsatz sogenannter Zero-Knowledge-Proofs [34], die aber über den Fokus dieser Arbeit hinausgehen. Mit Hilfe dieses Ansatzes, die Kenntnis eines Geheimnisses zu beweisen ohne den Inhalt dabei preiszugeben, können in Kombination mit der Blockchain-Technologie Anwendungen entwickelt werden, die die Benutzerdaten vollständig schützen, ohne dabei an Funktionalität einzubüßen. Diese Anforderung wurde im Rahmen dieser Arbeit nicht umgesetzt.

7.4.6.1 Datenschutz & Privatsphäre

Im **DLT**-Umfeld, als auch im **IOT**-Umfeld, sind Datenschutz und Privatsphäre zwei essentielle Themenbereiche, mit denen sich auseinandergesetzt werden muss, nicht zuletzt, um eine hohe Benutzerakzeptanz zu erzielen. Die Implementierung des vorliegenden Anwendungsfalls diente als Machbarkeitsstudie und ist in der aktuellen Form noch nicht produktiv einsetzbar. Aufgrund von zeitlichen Beschränkungen konnten die Themen

Datenschutz und Privatsphäre bei dieser Implementierung nur geringfügig berücksichtigt werden. Im Folgenden werden Schwachpunkte aufgezeigt, die mögliche Risiken in Bezug auf diese Themenstellung bergen. Ansätze, die diesen Punkten präventiv entgegenwirken und wirksame Mechanismen zur Wahrung der Privatsphäre werden im Kapitel 10 vorgeschlagen.

KAFFEEKONSUM Außenstehende können nachvollziehen, wie viele Tassen pro Tag im Durchschnitt pro Account konsumiert wurden. Es können keine genauen Uhrzeiten, sondern nur der Abrechnungszeitraum (zum Beispiel eine Woche) festgestellt werden. Die Anzahl realer Personen hinter einem Account ist nicht nachvollziehbar.

VERTRAGSDTLS Informationen zu Kosten, Vertragslaufzeiten, und Accounts von Maschine und Vertragspartnern können von Dritten eingesehen werden.

IDENTITÄT Es ist öffentlich einsehbar, in welcher Rolle (Benutzer, Hersteller, etc.) ein Account auf der Plattform agiert. Weitere Details zu Identitäten sind nicht verfügbar.

ERGEBNISSE & FAZIT

In dieser Arbeit wurde ein beispielhafter **IOT**-Anwendungsfall erarbeitet und in nachvollziehbaren Schritten auf **DLT**-Tauglichkeit evaluiert. Dazu wurden Anforderungen aufgestellt, klassifiziert und anhand verschiedener **DLT**-Lösungen theoretisch überprüft. Die prototypische Verprobung wurde daraufhin auf Basis von Ethereum durchgeführt. Mit dieser Implementierung wurden die Anforderungen weitestgehend erfüllt, Abweichungen davon wurden im vorherigen Kapitel genannt und begründet. Die folgenden Ausführungen untergliedern die Ergebnisse in sieben Kategorien und fassen die Erkenntnisse zusammen.

8.1 ANFORDERUNGSKLASSIFIZIERUNG

Das Klassifizierungsmodell aus Kapitel [5.2](#) wurde ursprünglich erarbeitet, um die Anforderungen des Anwendungsfalles in Klassen einzuteilen, damit auf dieser Ebene eine Aussage zur **DLT**-Relevanz getroffen werden kann. Das erarbeitete Modell eignete sich gut, um Anforderungen einfach und aus verschiedenen Perspektiven heraus zu identifizieren. Die These, damit auch eine vereinfachte Klassifizierung vornehmen zu können, wurde verworfen, da das Modell die Einordnung nicht erleichterte und für diesen Aspekt nicht den erhofften Mehrwehrt erbrachte. Die Klassifizierung als solche konnte allerdings genutzt werden, um möglichst alle Bereiche und Perspektiven verschiedener Stakeholder in Bezug auf die Anforderungsermittlung abzudecken. Die Überprüfung auf **DLT**-Relevanz muss nach wie vor auf der Anforderungsebene durchgeführt und für jede Anforderung separat überprüft werden.

8.2 MACHBARKEIT

Dieser Anwendungsfall ist für die Umsetzung auf Basis eines **DLTs** geeignet. Die Implementierung wurde erfolgreich umgesetzt, getestet und damit die Machbarkeit nachgewiesen. Inwieweit die generelle Machbarkeit über diesen Anwendungsfall hinaus geht und ob es möglich und sinnvoll ist, jegliche Art von **IOT**-Anwendungsfällen auf Basis von **DLT** umzusetzen, ist damit nicht geklärt. Die Diskussion über diese Thematik wird in Kapitel [9.1](#) wiederaufgenommen.

8.3 KOSTEN

In Kapitel [8.3](#) werden die Kosten des Anwendungsfall detailliert aufgeschlüsselt. Die Endausbaustufe sieht 400.000 Benutzer und 10.000 Kaffeemaschinen

vor, die durch den Anwendungsfall prozessiert werden. Damit ergibt sich ein errechneter Gesamtumsatz von 82.000.000€ pro Jahr bei jährlichen Gebühren von 78.000€. Um alle Verträge mit den Benutzern initial abzuschließen ergeben sich Kosten in Höhe von 4.200€ für den Hersteller. Aus Benutzersicht belaufen sich die monatlichen Gebühren zur Nutzung auf 3 Cent und initiale Kosten für den Vertragsabschluss von 35 Cent. Mit steigenden Nutzer-, Vertrags- und Gerätzahlen auf der Plattform werden nach aktueller Implementierung diese Preise steigen¹; eine effizientere Implementierung ist denkbar und kann dies vermeiden.

8.4 PERFORMANCE

Die Performance aus Benutzersicht muss in zwei Nutzungsphasen unterteilt werden: Das initiale Vertragserstellen ist ein asynchroner Prozess, der das Zutun beider Vertragsparteien erfordert und demnach nicht exakt gemessen werden kann. Überträgt man diesen Prozess auf den analogen Prozess einer Angebotsanfrage bis hin zum Vertragsabschluss, so stellt man hier allein durch die Digitalisierung einen deutlichen Geschwindigkeitszuwachs fest. Die reine Prozessierungsdauer von der Anfrage bis zum Zustandekommen des Vertrages entspricht drei onchain Transaktionen und damit im Durchschnitt der Größenordnung von wenigen Minuten. Die eigentliche Nutzung, also das Interagieren des Benutzers mit der Kaffeemaschine, erfolgt instantan und bietet dem Benutzer eine optimale Performance und damit ein gutes Benutzererlebnis.

Aus Herstellersicht existieren keine zeitkritischen Prozesse, da es nicht darauf ankommt, dass ein Vertrag innerhalb von Sekunden zustandekommt, da der Zeitpunkt der Vertragsbestätigung durch den Kunden nicht beeinflussbar ist. Das Einlösen einer Quittung ist mit einer onchain Transaktion binnen weniger Sekunden (weniger einer Minute) erfolgt und befindet sich damit in einem akzeptablen zeitlichen Rahmen.

8.5 SICHERHEIT

Dem Anwendungsfall liegt ein Rollen- und Benutzermanagement zugrunde, das Berechtigungen überprüft und Zugriffe beschränkt. Der zentrale Sicherheitsaspekt ist der Private-Key jedes Benutzers. Es existiert in der aktuellen Implementierung kein Mechanismus, welcher den Verlust oder den Diebstahl eines Private-Keys kompensiert. Die Ethereum Blockchain wird als extrem sicher eingestuft; Manipulationen oder Angriffe auf das System sind nur mit extrem hohem Aufwand und immensen Kosten verbunden. Die Sicherheit der implementierten Smart-Contracts muss von Experten vor einem Produktiveinsatz eingehend überprüft werden, damit Schäden durch Dritte oder Fehler im Code vermieden werden können.

¹ Jede Smart-Contract Rechenoperation benötigt GAS. Eine Schleife, die alle existierenden Verträge durchläuft und überprüft, hat mit steigender Vertragszahl auch steigende Schleifen-durchläufe.

8.6 VORTEILE ZU KLASISCHEN ANSÄTZEN

Es wurde gezeigt, dass die Implementierung des **IOT**-Anwendungsfalles durch den Einsatz der **DLT**-Technologie in verschiedenen Bereichen profitieren konnte. Ein schnelles Prototyping konnte durch die bereitgestellte Infrastruktur der Blockchain sowie den umfangreichen Entwicklungswerkzeugen schnell umgesetzt werden, sodass frühzeitig erste, vorzeigbare Ergebnisse vorlagen. Durch das Bereitstellen eines vollumfänglichen Kommunikationsprotokolls (vgl. Kap. 2.1.8) konnte sich bei der Entwicklung auf die Kernpunkte konzentriert werden. Die enorm hohe Ausfall- und Manipulationsicherheit sind zwei große Pluspunkte, mit denen die Implementierung durch den Einsatz der Ethereum-Blockchain implizit aufwarten kann.

8.7 DATENSCHUTZ & PRIVATSPHÄRE

Die Aspekte Datenschutz und Privatsphäre wurden in der vorliegenden Implementierung nicht berücksichtigt. Das Konzept sieht allerdings Mechanismen vor, die für die notwendige Sicherheit sorgen und die Mängel (vgl. Kap. 7.4.6.1) adressieren; darüber hinaus werden in Kapitel 10 weitere Ansätze aufgezeigt, um den Datenschutz und die Privatsphäre der Stakeholder zu wahren.

8.8 IMPLEMENTIERUNGSFORTSCHRITT

Ziel dieser Arbeit war es, zu zeigen, dass der ausgewählte **IOT**-Anwendungsfall durch den Einsatz eines **DLTs** umsetzbar ist. Dadurch konnte der ursprünglich skizzierte Anwendungsfall (vgl. Kap. 4) nicht vollumfänglich umgesetzt werden. Die Dazunahme von Service-Providern und Lieferanten oder darüber hinaus noch weiteren Stakeholdern ist eine Möglichkeit, den Anwendungsfall weiter auszubauen. Dazu würden weitere Vertragstypen wie Service- und Lieferverträge mittels eigener Smart-Contracts implementiert und an das bestehende System angehängt werden.

DISKUSSION

Dieses Kapitel befasst sich mit der zu eingangs aufgestellten These:

'DLT eignet sich als Technologie für IOT und die nicht-funktionalen Anforderungen sind für alle DLT-IOT-Anwendungsfälle gleich.'

9.1 WIEDERAUFAHME THESE TEIL 1: EIGNUNG FÜR IOT?

Der erste Teil der These stellt die Erwartung auf, dass **DLT** eine geeignete Technologie darstellt, um **IOT**-Anwendungsfälle umzusetzen. Nach ausführlicher Bearbeitung und Überprüfung in dieser Arbeit kann zunächst festgehalten werden, dass **DLT** eine geeignete Technologie für die Umsetzung dieses Anwendungsfalles darstellt. Die Umsetzung ist erfolgreich; eine geeignete Implementierung wurde vorgenommen, die den Anwendungsfall auf Basis von Ethereum prototypisch evaluiert. Eine generelle Aussage für das gesamte Anwendungsgebiet **IOT** ist damit nicht getroffen und kann auch nicht vollständig validiert werden. Anwendungsfälle, die ähnliche Charakteristika aufzeigen wie die vorliegende Umsetzung, können mit hoher Sicherheit von einer **DLT**-Implementierung profitieren; die Vorteile hierfür wurden in Kapitel 2.1.8 aufgezeigt. Dem entgegen stehen zeitkritische oder Performanzlastige **IOT**-Anwendungen, die nicht auf Basis eines **DLTs** implementiert werden können, da beispielsweise die benötigte Echtzeitkommunikation nicht gegeben ist. Darüber hinaus sind auch Anwendungen, die nur einen einzigen Stakeholder betreffen, oder nur an einer Lokalität ausgeführt werden, nicht für **DLTs** ausgelegt, da dabei nicht von der Dezentralität und dem No-Trust Environment profitiert werden kann. Demnach wird der erste Teil der These korrigiert, um die Erkenntnisse dieser Arbeit korrekt widerzuspiegeln. Damit ergibt sich folgende, mit dieser Arbeit validierte Aussage:

'DLT eignet sich als Technologie für dezentrale und asynchrone IOT-Anwendungsfälle, an denen mehrere, sich gegeneinander nicht vertrauende Parteien teilnehmen.'

9.2 WIEDERAUFAHME THESE TEIL 2: TECHNISCHE ANFORDERUNGEN IMMER GLEICH?

Der zweite Teil der These stellt die Erwartung auf, dass die nicht-funktionalen Anforderungen für alle **DLT-IOT**-Anwendungsfälle gleich sind. Wie bereits erläutert, beschränkt sich die Eignung von **DLT** auf eine Untergruppe aller **IOT**-Anwendungsfälle. Diese weisen die gleichen oder zumindest ähnlichen Charakteristika auf wie der vorliegende Anwendungsfall. Die

in Tabelle 5.1 als relevant klassifizierten, nicht-funktionalen Anforderungen betreffen die Unterbereiche Sicherheit und Zuverlässigkeit. Namentlich handelt es sich um die Eindeutigkeit, Manipulationssicherheit, Zugriffsbeschränkung und Performanz; dies sind Eigenschaften, die jede produktiv eingesetzte IOT-Anwendung garantieren muss. Die Performanz kann dabei abhängig vom Anwendungsfall variieren, ist allerdings durch die Wahl des DLTs variabel gestaltbar.

Es handelt sich um Anforderungen, die einerseits von jedem IOT-Anwendungsfall gefordert werden, aber auf der anderen Seite keine Vollständigkeit abbilden. Es ist denkbar, dass es Anwendungsfälle gibt, die über die genannten, nicht-funktionalen Anforderungen hinaus weitere Besonderheiten mit sich bringen. Demnach sind Eindeutigkeit, Manipulationssicherheit, Zugriffsbeschränkung und Performanz als Basis eines jeden DLT-IOT-Anwendungsfalles zu verstehen und damit für alle gleich. Auf Grundlage dieser Ausführung wird der zweite Teil der These wie folgt geändert, um den Erkenntnissen gerecht zu werden:

'... die Basis aller nicht-funktionalen Anforderungen sind für alle DLT-IOT-Anwendungsfälle gleich.'

9.3 ERGEBNIS

Die Überprüfungen beider Teile der Ausgangsthese führt zu folgendem Gesamtergebnis, welches lautet:

'DLT eignet sich als Technologie für dezentrale und asynchrone IOT-Anwendungsfälle, an denen mehrere, sich gegeneinander nicht vertrauende Parteien teilnehmen und die Basis aller nicht-funktionalen Anforderungen sind für alle DLT-IOT-Anwendungsfälle gleich.'

AUSBLICK

Mit dieser Arbeit wurde die Machbarkeit von **IOT**-Anwendungsfällen durch **DLT** nachgewiesen. Die vorliegende Implementierung kann als Grundlage für weitere Ausbaustufen des Anwendungsfalls dienen und eine Vorlage für die Umsetzung anderer IQT-Anwendungsfälle auf Basis eines **DLTs** sein. Mögliche Verbesserungen, Weiterentwicklungen und alternative Ansätze werden in diesem Ausblick aufgezeigt und vorgestellt. Dabei wurden Handlungsfelder identifiziert, die Optimierungspotential bieten und in denen weitere Forschung betrieben werden kann:

10.1 KOSTENSENKUNG

Um die Akzeptanz und die Verbreitung von **IOT**-Anwendungsfällen weiterhin zu vergrößern, ist es wichtig, die Kosten für die Nutzung zu reduzieren. Dies betrifft sowohl die Kosten aus Benutzersicht als auch aus Sicht des Herstellers. Mit steigender Anzahl an **IOT**-Geräten wird es für den dauerhaften Fortbestand eines Anwendungsfalles existenziell, die Kosten so gering wie möglich zu halten. Die Umsetzung einer dezentralen Public-Blockchain ohne Transaktionskosten ist derzeit noch nicht erreicht, um solche Anwendungsfälle zu begünstigen. Ein möglicher Forschungsaspekt liegt in der Erarbeitung eines Konsensmodells, dass ohne Transaktionskosten auskommt. Solange dies nicht erreicht ist, kann man zumindest versuchen, die Zahl der Transaktionen und damit auch die Nutzungskosten so gering wie möglich zu halten. Jede Transaktion und jede Codezeile innerhalb eines Smart-Contracts kostet Geld. Um die Vorteile von onchain Transaktionen nicht zu verlieren und dennoch die genannten Punkte sinnvoll zu adressieren, bietet sich ein hybrides Modell aus on- und offchain Verarbeitung an. Ein möglicher Ansatz wäre die dezentrale Datenhaltung mittels **IPFS**: Durch ein ausgeklügeltes Versionierungssystem in Kombination mit kryptographischen Hashfunktionen können eindeutige Hashes über Dateien und Informationen erzeugt und mittels dieser Hashes eine Verknüpfung zwischen onchain Informationsverarbeitung und offchain Datenhaltung geschaffen werden.

Eine andere, temporäre Lösung könnte mit der Verlagerung der Kosten einhergehen: Das Implementieren von Proxy Smart-Contracts, die als Relay fungieren und es erlauben, signierte Transaktionen im Namen eines Dritten an das Blockchain-Netzwerk zu senden. Solche Metatransaktionen ermöglichen, dass signierte Transaktionen von Alice über den Account von Bob an den Distributed Ledger transferiert werden können. Im Proxy Smart-Contract ist festgelegt, welcher Account in wessen Namen Transaktionen tätigen darf; diese Berechtigungen können jederzeit angepasst werden. Dabei

muss der ursprüngliche Absender die Transaktion nach wie vor signieren, lediglich die Übermittlung und damit das Tragen der Transaktionskosten läuft über einen Dritten. Im konkreten Anwendungsfall würde dies das Onboarding des Benutzers stark erleichtern, da dieser zur Nutzung der Plattform nicht zunächst Ether erwerben müsste. Darüber hinaus kann dadurch die Akzeptanz der Benutzer erhöht werden. Die Transaktionsgebühren können durch den Hersteller oder Betreiber der Plattform getragen und somit die Benutzbarkeit drastisch erhöht werden.

10.2 PRIVATSPHÄRE & DATENSCHUTZ

Durch die onchain Datenhaltung und Informationsverarbeitung mittels Smart-Contract können alle Vorteile, die ein [DLT](#) bietet (vgl. Kap. 2.1.8), zielbringend eingesetzt werden. Dies bringt allerdings auch Nachteile mit sich, die sich vor allem negativ auf die Privatsphäre und den Datenschutz auswirken - alle Informationen sind öffentlich und für jedermann einsehbar. Dies ist besonders bei personenbezogenen Daten nicht wünschenswert und muss in Produktivumgebungen verhindert werden. Durch die dezentrale Datenhaltung mittels [IPFS](#) oder ähnlichen Technologien wurde ein erster Ansatz aufgezeigt, Daten auch außerhalb der Blockchain aufzubewahren. Dennoch hat der Benutzer keine volle Kontrolle mehr über seine Daten, da diese den eigenen Zugriffsbereich verlassen und über das Internet repliziert werden. Das Konzept von Zero-Knowledge Proofs geht hierbei deutlich weiter: Eigene Daten werden nicht mehr an Dritte übertragen, sondern es wird ein mathematisch verifizierbarer Beweis erstellt, ohne den genauen Inhalt des Beweises preiszugeben [34]. So können beispielsweise Informationen zur eigenen Identität oder Zugangsberechtigungen mittels Zero-Knowledge Proof nachgewiesen werden. Konkret bedeutet das, dass das Rollenmanagement des vorliegenden Anwendungsfalles durch das Oracle entfallen und man in einer Rolle agieren könnte, ohne diese oder die eigene Identität preiszugeben. Auch könnten die Quittungen des Payments und damit die Nachvollziehbarkeit des Kaffeekonsums verschleiert werden, indem diese durch Zero-Knowledge Proofs ersetzt würden und damit lediglich der Beweis erbracht würde, dass ein Account berechtigt ist, eine bestimmte Menge Ether zu empfangen.

Ein weiterer, wichtiger Aspekt in Bezug auf Datenschutz ist das Konzept des Private-Keys: Das Sicherheitskonzept basiert vollständig auf der Annahme, dass der Private-Key jedes Stakeholders geheim und unzugänglich für Dritte ist. Dieser [SPoF](#) kann durch besondere Maßnahmen vermieden werden. Ein möglicher Ansatz wäre der Einsatz von onchain-Wallets, die mittels Smart-Contracts implementiert werden und Sicherheitskonzepte wie Guards zulassen: Ein Guard ist ein anderer Account, dem der Inhaber des Wallets vertraut und der im Falle des Verlusts des Private-Keys oder eines Angriffes das Konto sperren, einen neuen Private-Key für den Benutzer hinterlegen oder andere Sicherheitsmaßnahmen durchführen kann. Dabei ist der Einsatz von mehreren Guards möglich, wobei die Berechtigungen dieser angepasst

und durch besondere Bedingungen beschränkt werden können. Dadurch könnten präventiv Maßnahmen gegen den Missbrauch von Datenschutz-relevanten Informationen durchgeführt werden, falls der Private-Key eines Stakeholders korrumptiert wird.

Teil II
APPENDIX

A

APPENDIX: ANFORDERUNGEN

Story	Description	Task	Description	Requirement	Description	Class Level-1	Class Level-2	Non-Functional	Non-Functional Subcategory
Story A1 "Agieren auf Plattform"	"Als Akteur möchte ich in meiner Rolle als [X] auf der Plattform agieren."	Task A1.1	Akteure können sich an der Plattform registrieren und gemäß ihrer Rolle miteinander agieren.	Requirement A1.1.1	Jeder Akteur auf der Plattform kann eindeutig identifiziert werden.	Software	NonFunctional	Security	Accountability
				Requirement A1.1.2	Ein Akteur registriert sich und meldet sich auf der Plattform an, bevor er dort agieren kann.	Software	Functional		
				Requirement A1.1.3	Ein Akteur agiert immer mit einer bestimmten Rolle auf der Plattform: Manufacturer, Customer, Supplier, Service-Provider oder Gerät. Ein Akteur kann mehrere Rollen haben.	Software	Functional		
				Requirement A1.1.4	Es existiert eine Oberfläche, auf die jeder Akteur Zugriff hat. Dort kann er sich registrieren und anmelden.	Software	Functional		
				Requirement A1.1.5	Ein Akteur hat eine (mehrere) verifizierte Rolle(n).	Software	Functional		
		Task A1.2	Akteure können über die Plattform miteinander kommunizieren.	Requirement A1.2.1	Akteure kommunizieren über die Plattform.	Software	Functional		
				Requirement A1.2.2	Die Kommunikation der beteiligten Akteure wird sofort übermittelt.	Software	NonFunctional	PerformanceEfficiency	Time behavior
				Requirement A1.2.3	Die Kommunikation zwischen den Akteuren ist nachvollziehbar und eindeutig zuordnbar.	Software	NonFunctional	Security	Accountability
				Requirement A1.2.4	Die Kommunikation zwischen den Akteuren kann nicht gelöscht oder manipuliert werden.	Software	NonFunctional	Security	Integrity
				Requirement A1.2.5	Akteure können nur den Inhalt ihrer eigenen Nachrichten einsehen.	Software	NonFunctional	Security	Confidentiality
		Task A1.3	Akteure können über die Plattform Verträge miteinander abschließen.	Requirement A1.3.1	Akteure schließen Verträge über die Plattform ab.	Software	Functional		
				Requirement A1.3.2	Verträge sind rechtlich bindend.	Software	Functional		
				Requirement A1.3.3	Akteure können Verträge ablehnen oder annehmen.	Software	Functional		
				Requirement A1.3.4	Es existiert eine Oberfläche, auf die jeder Akteur Zugriff hat. Dort kann er Vertragsanfragen erstellen. Auf der Empfängerseite muss eine Oberfläche existieren, die diese Anfragen anzeigt.	Software	Functional		
				Requirement A1.3.5	Der Vertragsgegenstand kann nicht durch Dritte manipuliert werden.	Software	NonFunctional	Security	Integrity
				Requirement A1.3.6	Akteure haben Zugriff auf alle Vertragsinformationen.	Software	Functional		
				Requirement A1.3.7	Akteure können komplexe Vertragsstrukturen umsetzen. Verträge haben einen Status. Diese können "Aktiv", "In Erzeugung" oder "Inaktiv" sein.	Software	Functional		
				Requirement A1.3.8	Akteure können ihre Verträge im Nachhinein ändern.	Software	Functional		
				Requirement A1.3.9	Akteure können nur ihre eigenen Verträge ändern.	Software	NonFunctional	Security	Confidentiality
				Requirement A1.3.10	Eine Vertragsänderung bedarf der Zustimmung aller beteiligten Akteure.	Software	Functional		
		Task A1.4	Akteure benötigen grafische Oberflächen zum Agieren auf der Plattform.	Requirement A1.4.1	Es existiert eine Oberfläche, auf die der Akteur Zugriff hat. Dort hat er eine Übersicht über alle seiner Verträge sowie aggregierte Informationen wie Anzahl aller Verträge, Kontostand, etc. Es werden ebenfalls aktuelle Verträge angezeigt, die angenommen und abgelehnt werden können.	Software	Functional		
				Requirement A1.4.2	Es existiert eine Oberfläche, auf die der Akteur Zugriff hat. Dort hat er eine detaillierte Übersicht über einen seiner Verträge und kann sich Detailinformationen dazu ansehen. Außerdem sieht er eine Übersicht über alle Nachrichten, die mit diesem Vertrag in Verbindung stehen und den Vertrag bearbeiten.	Software	Functional		
Story M1 "Geräte vermieten"	"Als Manufacturer möchte ich meine Geräte über die Plattform vermieten können, um meinen Umsatz zu steigern."	Task M1.1	Die Geräte können auf der Plattform vermietet werden.	Requirement M1.1.1	Ein Gerät ist Eigentum eines Manufacturers.	Software	Functional		
				Requirement M1.1.1	Ein Manufacturer kann beliebig viele Geräte besitzen und über die Plattform vermieten.	Software	Functional		
		Task M1.2	Die Geräte benötigen Sensoren, um Fehler und Defekte zu detektieren.	Requirement M1.2.1	Geräte können Fehlerzustände detektieren. Tritt ein Fehler auf, wird dieser dem Customer über ein Display angezeigt.	Software	Functional		
				Requirement M1.2.2	Geräte können Defekte detektieren. Tritt ein Fehler auf, wird dieser über die Plattform an den Service-Provider (Service-Vertrag) gemeldet.	Software	Functional		
				Requirement M1.2.3	Ein Defekt (Defektes, Material, unididaktische Ausklüsse, etc.) hindert das Gerät am Durchführen seiner Tätigkeit und muss durch einen Service-Provider behoben werden.	Software	Functional		
Story M2 "Verträge erzeugen"	"Als Manufacturer möchte ich in der Lage sein, Verträge anzulegen, um meine Geräte über die Plattform vermieten zu können."	Task M2.1	Ein Manufacturer kann Verträge erzeugen.	Requirement M1.2.4	Ein Fehlerzustand (leerer Wassersbehälter, geöffnete Abdeckung, etc.) hindert das Gerät am Durchführen seiner Tätigkeit und kann meistens durch den Customer behoben werden.	Software	Functional		
				Requirement M2.1.1	Es existiert eine Oberfläche, auf die der Manufacturer Zugriff hat. Dort kann er Mietverträge erzeugen und als Antwort auf seine Metanfrage an den Customer senden.	Software	Functional		
				Requirement M2.1.2	Es existiert eine Oberfläche, auf die der Manufacturer Zugriff hat. Dort kann er alle Service-Provider und deren Dienstleistungen einsehen. Service-Verträge erzeugen und an einen Service-Provider senden.	Software	Functional		
Story M3 "Verträge abrechnen"	"Als Manufacturer benötigt ein korrekte, nutzungsbabhängige und automatische Abrechnung der vermieteten Geräte, die regelmäßig aktualisiert wird, sowie der erbrachten Dienstleistungen, um den Umsatz aufrecht zu erhalten."	Task M3.1	Die Geräte müssen den Verbrauch detektieren.	Requirement M2.1.3	Es existiert eine Oberfläche, auf die der Manufacturer Zugriff hat. Dort kann er alle Supplier einsehen, Lieferverträge erzeugen und an den Supplier senden.	Software	Functional		
				Requirement M3.1.1	Geräte detektieren den Verbrauch (Kaffeemaschine: Anzahl Kaffees) und senden diesen an die Plattform.	Software	Functional		
		Task M3.2	Die Geräte müssen die Verbrauchsdaten an die Plattform melden.	Requirement M3.2.1	Geräte senden den Verbrauch nach Fertigstellung des Produktes sofort an die Plattform.	Software	NonFunctional	PerformanceEfficiency	Time behavior
				Requirement M3.2.2	Die Verbrauchsdaten der Geräte können nicht manipuliert werden.	Software	NonFunctional	Security	Integrity
Story C1 "Ansicht verfügbarer Geräte"	"Als Customer möchte ich verfügbare Haushaltsgeräte angezeigt bekommen, um das passende Gerät mieten zu können."	Task C1.1	Es muss eine Auflistung aller verfügbaren (mietbaren) Geräte existieren.	Requirement C1.1.1	Es existiert eine Oberfläche, auf die der Customer Zugriff hat. Dort hat er die Möglichkeit, alle verfügbaren Geräte aufzulisten.	Software	Functional		
				Requirement C1.2.1	Der Customer hat Zugriff auf eine detaillierte Beschreibung des Geräts.	Software	Functional		
		Task C1.2	Es müssen alle für den Customer relevanten Informationen über das Gerät vorhanden und einsehbar sein.	Requirement C2.1.1	Geräte detektieren eine Reinigung (Produktbehälter leeren, etc.).	Software	Functional		
				Requirement C2.1.2	Geräte detektieren eine Wartung (Entkalken, etc.).	Software	Functional		
		Task C2.1	Das Gerät muss die Reinigung / Wartung durch den Customer detektieren können.	Requirement C2.1.1	Geräte detektieren eine Reinigung (Produktbehälter leeren, etc.).	Software	Functional		
				Requirement C2.1.2	Geräte detektieren eine Wartung (Entkalken, etc.).	Software	Functional		

Story C2 "Geräte warten"	"Als Customer möchte ich die gemieteten Geräte reinigen und warten können, um dafür vom Hersteller eine Gutschrift auf mein Vertragskonto zu erhalten."	Task C2.2	Es muss sichergestellt werden, dass eine Reinigung / Reparatur dem Gerät bzw. dessen Sensoren nicht vorgespielt werden kann.	Requirement C2.2.1	Detektierte Reinigungen / Wartungen können nicht manipuliert oder dem Gerät vorgespielt werden.	Software	NonFunctional	Security	Integrity
		Task C2.3	Der Customer muss vom Gerät eindeutig identifiziert werden können.	Requirement C2.3.1	Das Gerät kann den Customer indentifizieren.	Software	Functional		
		Task C2.4	Die Reinigung / Wartung muss an die Plattform übertragen werden und gemäß des Vertrages abgerechnet werden.	Requirement C2.4.1	Das Gerät sendet detektierte Reinigungen / Wartungen an die Plattform.	Software	Functional		
				Requirement C2.4.2	Das Gerät sendet detektierte Reinigungen / Wartungen nach Abschluss direkt an die Plattform.	Software	NonFunctional	PerformanceEfficiency	Time behavior
Story C3 "Einfache Bedienbarkeit der Plattform"	"Als Customer möchte ich eine intuitive, einfach zu bedienende Oberfläche, um mich gut auf der Plattform zurechtzufinden."	Task C3.1	Ein Customer muss zunächst mit der Plattform bekannt gemacht werden.	Requirement C3.1.1	Ein Customer erhält eine initiale Einführung über die Plattform bei der ersten Anmeldung.	System	Transition		
				Requirement C3.1.2	Die Funktionen der Plattform sind für den Customer schnell erlernbar und leicht verständlich.	Software	NonFunctional	Usability	Learnability
		Task C3.2	Die Plattform muss optisch ansprechend sein.	Requirement C3.2.1	Die Plattform ist für den Customer optisch ansprechend.	Software	NonFunctional	Usability	User interface aesthetics
Story SP1 "Dienstleistungen bereitstellen"	"Als Service-Provider möchte ich meine Angebotspalette auf der Plattform anbieten können."	Task SP1.1	Ein Service-Provider muss seine angebotenen Dienstleistungen auf der Plattform eingeben können.	Requirement SP1.1.1	Es existiert eine Oberfläche, auf die der Service-Provider Zugriff hat. Dort kann er alle Dienstleistungen, die er anbietet, sowie Detailsinformationen, wie zum Beispiel Kosten der Dienstleistung, eintragen und damit auf der Plattform verfügbar machen.	Software	Functional		
				Requirement SP1.1.2	Es existiert eine Oberfläche, auf die der Service-Provider Zugriff hat. Dort kann er bereits angebotene Dienstleistungen editieren oder löschen.	Software	Functional		
Story SP2 "Service-Aufträge abschließen"	"Als Service-Provider möchte ich nach der Durchführung der Wartung des Smartphones am Gerät den Service-Auftrag abschließen."	Task SP2.1	Der Service-Provider kann mit dem Gerät per Smartphone kontaktlos kommunizieren.	Requirement SP2.1.1	Gerät und Service-Provider können miteinander kommunizieren.	Software	Functional		
				Requirement SP2.1.2	Ein Gerät kann den Service-Provider eindeutig identifizieren.	Software	Functional		
		Task SP2.2	Es wird eine App benötigt, mit der der Service-Provider seine Identität und die durchgeführte Wartung am Gerät bestätigen kann.	Requirement SP2.2.1	Es existiert eine Smartphone-Oberfläche, auf die der Service-Provider Zugriff hat. Darüber kann er Wartungen abschließen.	Software	Functional		
				Requirement SP2.2.2	Ein Service-Provider kann einen Service-Auftrag starten und beenden, wenn er sich in der Nähe des Geräts befindet.	Software	Functional		
Story SEC1 "Sichere Zahlungsabwicklung"	"Als IT-Security-Beauftragter möchte ich sichergestellt wissen, dass die Zahlungsabwicklung auf der Plattform sicher und voll funktionsfähig ist."	Task SEC1.1	Es muss sichergestellt werden, dass Geldtransfers vom Sender an den Empfänger durchgeführt werden.	Requirement SEC1.1.1	Geldtransfers werden auf der Plattform geloggt.	Software	Functional		
				Requirement SEC1.1.2	Bei Nicht-Ausführung von Geld- und Nachrichtentransfers werden die Parteien benachrichtigt.	Software	NonFunctional	Security	Integrity
				Requirement SEC1.1.3	Die Plattform prüft Geldtransfers vor Ausführung.	Software	Functional		
		Task SEC1.2	Es muss sichergestellt werden, dass Sender und Empfänger des Geldes eindeutig identifizierbar sind.	Requirement SEC1.2.1	Jeder Akteuer besitzt eine (mehrere) eindeutige Kontonummer(n).	Software	NonFunctional	Security	Accountability
				Requirement SEC1.2.2	Konten sind zugriffsgeschützt.	Software	NonFunctional	Security	Authenticity
Story SEC2 "Sichere Kommunikation und signierte Nachrichten"	"Als IT-Security-Beauftragter möchte ich eine verschlüsselte Kommunikation mit der Plattform, damit meine Daten nicht in die Hände von Dritten gelangen."	Task SEC2.1	Die Kommunikation zwischen Akteuren und der Plattform muss verschlüsselt werden.	Requirement SEC2.1.1	Sämtliche Verbindungen sind per SSL/TLS zu verschlüsseln.	System	Quality		
		Task SEC2.2	Aktuelle Sicherheitsstandards müssen verwendet werden.	Requirement SEC2.2.1	Es können Passwortregeln hinterlegt werden. Die Einhaltung dieser Regeln wird überprüft.	System	Quality		
Story SEC3 "Manipulations sicherheit"	"Als IT-Security-Beauftragter möchte ich eine manipulations sichere Plattform, um die Integrität und Echtheit der Daten zu gewährleisten."	Task SEC3.1	Es müssen Vorkehrungen gegen Manipulationen getroffen werden.	Requirement SEC3.1.1	Der Zugang zu den Backend-Systemen wird protokolliert und nur Berechtigten gestattet.	Software	NonFunctional	Security	Accountability
				Requirement SEC3.1.2	Manipulationen werden durch den Einsatz kryptographischer Methoden verhindert.	Software	NonFunctional	Security	Integrity
		Task SEC3.2	Es ist nachvollziehbar, wer wann auf die Plattform zugegriffen hat.	Requirement SEC3.2.1	Alle Aktivitäten auf der Plattform werden geloggt.	Software	NonFunctional	Security	Accountability
Story BD1 "Geschäftsmodell"	"Als Business-Developer möchte ich mit dem Geschäftsmodell Pay-As-You-Use einen größeren Kundenbereich ansprechen und den Umsatz steigern."	Task BD1.1	Das Pay-As-You-Use Abrechnungsmodell muss in einem Vertrag abgebildet werden können.	Requirement BD1.1.1	Vermietete Geräte werden nach dem Pay-As-You-Prinzip abgerechnet.	System	Business		
		Task BD1.2	Es ist vertraglich festgelegt, welcher Akteur für welche Dienstleistung wie viel Geld bezahlt bzw. erhält.	Requirement BD1.2.1	Customer bezahlen jede verbrauchte Einheit (z.B. pro Tasse Kaffee) des gemieteten Geräts an den Manufacturer. Die genauen Kosten sind vom Gerät abhängig und werden durch den Manufacturer festgelegt.	Software	Functional		
				Requirement BD1.2.2	Manufacturer bezahlen Customer für jede durchgeführte Wartung des vermieteten Geräts. Die Höhe der Zahlung ist im Mietvertrag geregelt.	Software	Functional		
				Requirement BD1.2.3	Manufacturer bezahlen Service-Provider für jede erbrachte Service-Leistung. Die Höhe der Zahlung ist im Service-Vertrag geregelt.	Software	Functional		
				Requirement BD1.2.4	Verträge sind individuell gestaltbar.	Software	Functional		
				Requirement BD1.2.5	Manufacturer bezahlen Supplier für jede erbrachte Lieferung. Die Höhe der Zahlung ist im Liefervertrag geregelt.	Software	Functional		
Story BD2 "Plattform für Partner"	"Als Business-Developer möchte ich eine Plattform, die für Partner wie Service-Provider oder Supplier leicht zugänglich ist."	Task BD2.1	Partner agieren auf der Plattform.	Requirement BD2.1.1	Auf der Plattform agieren Geschäftspartner (Service-Provider, Supplier, etc.).	System	Business		
		Task BD2.2	Partner müssen als solche identifiziert sein.	Requirement BD2.1.2	Die Nutzung der Plattform ist intuitiv und schnell erlernbar. Umfangreiche Mitarbeiter Schulungen zur Benutzung der Plattform sind nicht notwendig.	System	Transition		
				Requirement BD2.2.1	Der Prozess zur Prüfung, dass es sich z.B. bei einem Service-Provider auch tatsächlich um einen solchen handelt, ist benutzerfreundlich und so schnell und einfach wie möglich umsetzbar.	System	Stakeholder		
Story BD3 "Hersteller-übergreifende Plattform"	"Als Business-Developer möchte ich in Zukunft eine Plattform nutzen, auf der Hersteller unterschiedlicher Branchen ihre Produkte nach dem Pay-As-You-Use Prinzip vermitteln können, um dem Kunden eine breiteren Produktpalette zu bieten."	Task BD3.1	Die Plattform muss zukünftig weitere Hersteller zulassen, um ein ganzes Ökosystem von Geräten, allen Art dem Customer zugänglich zu machen.	Requirement BD3.1.1	Es können in Zukunft weitere Hersteller auf der Plattform ihre Geräte zur Miete anbieten.	System	Business		
		Task BD3.2	Ein Gerät muss auf der Plattform generisch repräsentiert werden und darf nicht von einem bestimmten Produktyp oder Hersteller abhängig sein.	Requirement BD3.2.1	Die Plattform kann Geräte unterschiedlicher Art anbinden und abrechnen.	Software	NonFunctional	Compatibility	Interoperability
				Requirement BD3.3.1	Die Plattform kann unterschiedliche Vertragsarten abbilden und abrechnen.	Software	NonFunctional	Compatibility	Interoperability
Story BD4 "Vertragsgestaltung"	"Als Business-Developer möchte ich die Plattform dazu nutzen, künftig andere Vertragsarten unterschiedlicher Geschäftsfelder und Kunden zu gewinnen."	Task BD4.1	Die Einbindung von Verträgen sowie deren Struktur muss möglichst modular und unabhängig geschehen, damit später andere Verträge integriert werden können.	Requirement BD4.2.1	Ein Abrechnungsmodell wird in einem Vertrag abgebildet.	System	Business		
				Requirement BD4.2.2	Einzelne Bestandteile der Plattform beeinflussen sich gegenseitig nicht und können leicht ausgetauscht werden.	Software	NonFunctional	Maintainability	Modularity
Story SA1 "Modularer Aufbau"	"Als System-Architekt möchte ich eine modulare aufgebauten Plattform, damit diese später leichter erweitert werden kann."	Task SA1.1	Funktionalitäten werden in Modulen gekapselt und als Service bereitgestellt.	Requirement SA1.1.1	Ein Software-Modul wird unabhängig von anderen Modulen bereitgestellt und gewartet.	Software	Process		
		Task SA2.1	Die Plattform kann im Falle eines Crashes alle Daten konsistent halten.	Requirement SA2.1.1	Bei Ausfall einzelner Komponenten gehen keine Daten verloren.	Software	NonFunctional	Security	Integrity
Story SA2	"Als System-Architekt möchte ich SPOFs und Datenverlust vermeiden."			Requirement SA2.1.2	Bei Ausfall einzelner Komponenten entstehen keine Dateninkonsistenzen.	Software	NonFunctional	Security	Integrity

"Redundanz"	"damit das System auch im Fehlerfall weiter funktionsfähig ist."	Task SA2.2	Requirement SA2.2.1	Die Plattform ist in der Lage, die Kommunikation und Datenverarbeitung bei bis zu 10.000 Endgeräten durchzuführen.	Software	NonFunctional	Reliability	Availability	
			Requirement SA2.2.2	Die Plattform ist nicht von einer einzelnen Komponente (SPOF) abhängig.	Software	NonFunctional	Reliability	Availability	
Story P1 "Deployment & Testing"	"Als Betreiber der Plattform möchte ich eine automatisierte korrekte Bereitstellung der Plattform, um meinen Aufwand zu reduzieren."	Task P1.1	Es wird nur getestete Software bereitgestellt.	Requirement P1.1.1	Für alle Software-Komponenten existieren hinreichende Tests, die Test-Abdeckung beträgt 80%.	Software	NonFunctional	Maintainability	Testability
		Task P1.2	Die Bereitstellung ist automatisiert.	Requirement P1.2.1	Die Software wird automatisiert durch Skripte installiert und bereitgestellt.	Software	NonFunctional	Portability	Installability

B

APPENDIX: DLT-MARKTÜBERSICHT

Name	Blockchain	Marketcap	Price	Volume
IOTAMIOTA	\$456.91M	\$0.16438	\$5,388,399	-1.16%
IoTeXIOTX	\$19.11M	\$0.00354	\$1,873,820	-0.78%
WaltonchainWTC	\$15.29M	\$0.35410	\$1,762,594	-5.61%
RobotinaROX	\$13.18M	\$0.04337	\$128,840	+0.06%
IoT ChainITC	\$9M	\$0.10783	\$1,769,855	-1.07%
INT ChainINT	\$6.58M	\$0.01732	\$1,032,942	+1.77%
RuffRUFF	\$5.11M	\$0.00521	\$904,692	+1.24%
XensorXSR	\$3.58M	\$0.01008	\$5,971,333	-38.27%
ArtfinityAT	\$3.03M	\$0.02406	\$8,018,680	-0.54%
SDChainSDA	\$2.23M	\$0.00149	\$12,165	-12.22%

Tabelle B.1: IOT-Relevanz, <https://cryptoslate.com/cryptos/iot> (Stand: 30.12.19 10:00 Uhr)

Name	Activity	Average (7d)	Record	Market Cap	AVI
EOS	56,068,563Op	52,464,432Op	74,568,958Op	\$ 2.6 B	6,837
TLOS	6,973,820Op	6,886,382Op	32,217,207Op	\$ 0.013 B	175,396
IOST	1,542,547Op	955,269Op	1,651,712Op	\$ 0.061 B	7,893
XLM	1,186,730Op	1,277,089Op	1,391,425Op	\$ 0.923 B	404
KIN	1,160,424Op	1,080,820Op	5,258,216Op	\$ 0.004 B	87,014
TRX	1,069,788Op	1,148,209Op	5,306,869Op	\$ 0.930 B	362
STEEM	996,699Op	996,699Op	2,522,380Op	\$ 0.047 B	6,671
NANO	592,744Op	663,973Op	1,007,236Op	\$ 0.090 B	2,072
ETH	509,869Op	566,058Op	1,372,918Op	\$ 15 B	11
BSV	443,946Op	479,188Op	900,436Op	\$ 1.8 B	77

Tabelle B.2: Blocktivity, <https://blocktivity.info/> (Stand: 31.12.19 10:00 Uhr)

Name	Commits	Stars	Releases	Active Authors	Languages
Ethereum (ETH)	10270	89285	97	524	14
LBRY Credits (LBC)	13999	10826	261	170	12
Lisk (LSK)	31697	7874	92	69	5
Cosmos (ATOM)	4890	9198	98	284	13
Stellar (XLM)	5281	6627	174	168	14
WAVES (WAVES)	18262	2367	32	163	17
EOS (EOS)	12230	17557	81	134	16
IOTA (MIOTA)	10316	7759	79	145	15

Tabelle B.3: Coincodecap, <https://coincodecap.com/coins> (Stand: 29.12.2019 14:30 Uhr)

Crypto	Commits	Contributors	Watchers
Bitcoin	1921	100	41697
Ethereum	851	100	25146
EOS	1783	100	10764
Tron	2796	99	2325
Monero	844	100	4177
Zcash	475	100	4110
Lisk	6586	62	2685
Syscoin	2388	100	108
Particl	2146	100	91
BitcoinCash	1277	100	872

Tabelle B.4: Github Commits past 12 months, <https://www.cryptomiso.com/> (Stand: 29.12.2019 14:30 Uhr)

Hyperledger Fabric	Ethereum	Corda
Allianz SE	Amazon	Allianz SE
Amazon	Anheuser-Busch InBev	Anheuser-Busch InBev
BBVA	BBVA	BBVA
BNP Paribas	BNP Paribas	BNP Paribas
Broadridge	BP PLC	HPE
Comcast	Ciox Health	ING
HPE	Citigroup	Intel
ING	Coinbase	Maersk
Intel	Comcast	Microsoft
Microsoft	Fidelity	Nasdaq
Nasdaq	Foxconn	PNC
Northern Trust	Google	Siemens
PNC	HPE	State Farm
Santander	HTC	UBS
SAP SE	Intel	
Seagate Technology	Microsoft	
Siemens	Northern Trust	
State Farm	Overstock	
UBS	Samsung	
Visa	Siemens	
Walmart	UBS	

Tabelle B.5: Blockchain Projekte in großen internationalen Unternehmen (Teil 1),
[21] (Stand: 29.12.19 17:00 Uhr)

Quorum	Bitcoin	Hyperledger Sawtooth	Ripple
BP PLC	Bitfury	Cargill	Coinbase
Broadridge	Coinbase	CVS Health	PNC
Comcast	Comcast	Intel	Santander
HPE	Fidelity		
ING	Google		
JPMorgan Chase	HTC		
Microsoft	Overstock		
SAP SE			
State Farm			
UBS			

Tabelle B.6: Blockchain Projekte in großen internationalen Unternehmen (Teil 2),
[\[21\]](#) (Stand: 29.12.19 17:00 Uhr)

APPENDIX: UMSETZUNG

C.1 BENUTZERINTERAKTIONEN

Der vorliegende IOT-Anwendungsfall beinhaltet verschiedene Benutzerinteraktionen, die anhand der folgenden UML-Sequenzdiagramme dargestellt und erläutert werden.

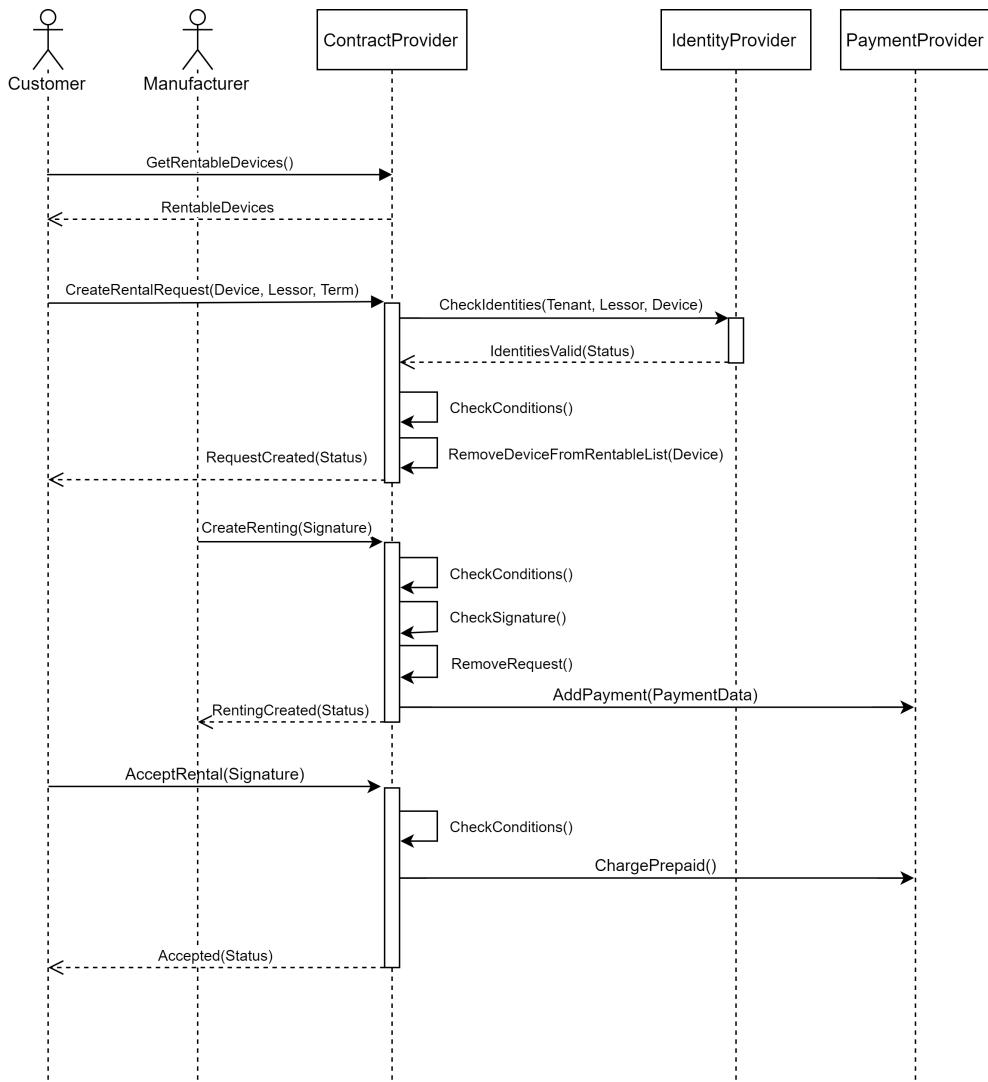


Abbildung C.1: UML-Sequenzdiagramm zur Vertragserzeugung

Die Vertragserzeugung kann grob in drei Schritte untergliedert werden und wird initial durch den Benutzer ausgelöst. Im ersten Schritt hat der Benutzer über das Web-Frontend Zugriff auf die verfügbaren Miet-Geräte.

Aus diesen Geräten wählt er eines aus und erzeugt eine Mietanfrage, die per API-Call an den RentalProvider Smart-Contract gesendet wird. Dieser führt Überprüfungen aus wie die Kontrolle der Identitäten, Inhalte der Mietanfrage und markiert nach erfolgreicher Prüfung das Gerät als reserviert, sodass es kein anderer Benutzer anmieten kann. Der zweite Schritt wird durch den Hersteller des Gerätes gestartet: Dieser kann die Mietanfrage prüfen und anschließend akzeptieren, indem er einen von ihm signierten Mietvertrag an den RentalProvider sendet. Lehnt er die Anfrage ab, so wird die Mietanfrage gelöscht und das Gerät als wieder verfügbar markiert. Stimmen die Daten des Mietvertrages und ist die Signatur valide, wird der Mietvertrag gespeichert und ein dazugehöriger Payment-Channel eröffnet. Der letzte Schritt wird wieder durch den Benutzer ausgeführt: Der vom Hersteller erzeugte Mietvertrag kann geprüft und die Vertragsbedingungen (Vertragslaufzeiten, Kosten, etc.) eingesehen werden. Akzeptiert der Benutzer den Mietvertrag durch seine Signatur, wechselt dieser in den Status aktiv. Gleichzeitig transferiert der Benutzer ein Startguthaben von seinem Wallet auf den zum Mietvertrag angelegten Payment-Channel. Die Benutzung kann anschließend sofort erfolgen.

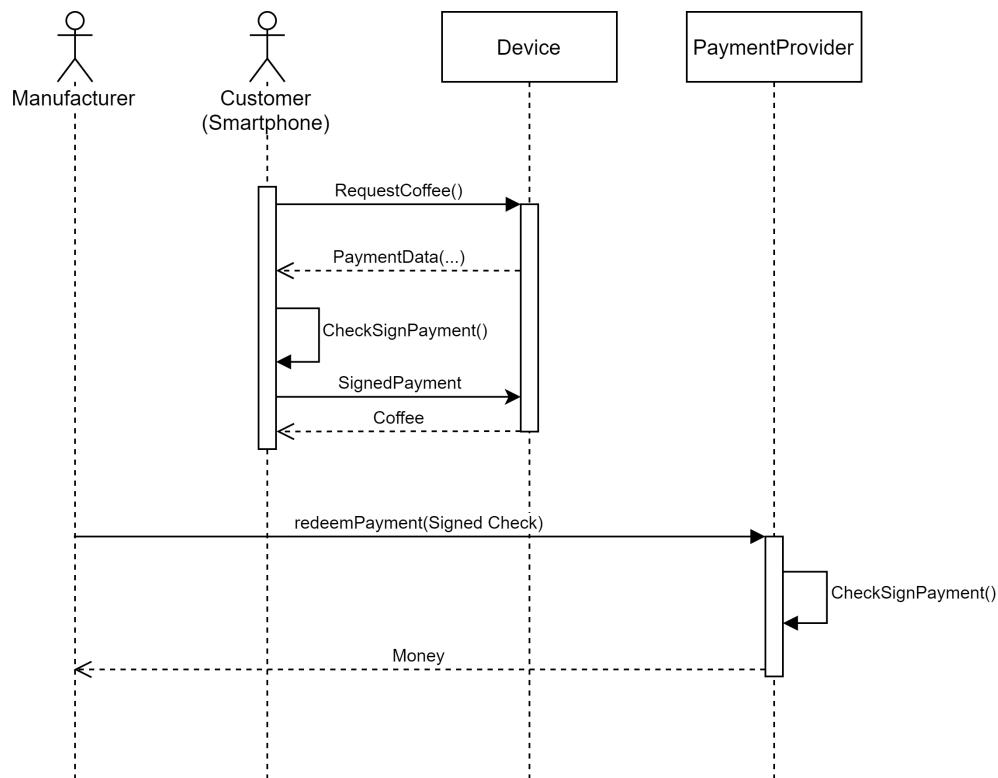


Abbildung C.2: UML-Sequenzdiagramm zur Zahlungsabwicklung

Ein aktiver Mietvertrag ist Voraussetzung für die erfolgreiche Benutzung der Kaffeemaschine, da ansonsten kein Kaffee serviert wird. Fragt der Benutzer mittels Knopfdruck eine Tasse Kaffee an, erzeugt die Maschine eine

Quittung, die bestätigt, dass der Kunde in einem festgelegten Zeitraum¹ eine bestimmte Anzahl Kaffees zu einem festgelegten Preis konsumiert hat. Diese Quittung wird mittels NFC an das Smartphone des Benutzers gesendet, dort überprüft, mittels des Private-Keys signiert und anschließend über die gleiche Schnittstelle zurückgesendet. Ist die Signatur korrekt, serviert die Maschine die vereinbarte Menge Kaffee. Alle zahlungsrelevanten Informationen liegen zu diesem Zeitpunkt lokal auf der Maschine. Wird die Maschine kompromittiert oder führt ein interner Fehler zum Verlust der signierten Quittung, besteht keine Möglichkeit, die Zahlungen geltend zu machen. Sofern eine Konnektivität zum Internet besteht, können verschiedene Mechanismen implementiert werden, um die Zahlungsinformationen zu schützen. Der eigentliche Bezahlvorgang, also das Transferieren von Geldern, erfolgt durch das Übertragen der signierten Quittung an den PaymentProvider der Smart-Contract. Dieser überprüft die Quittung sowie die Signatur des Benutzers und transferiert die quittierte Menge Geld (in diesem Fall Ether) an den Hersteller. In der vorliegenden Implementierung wird die Quittung durch die Maschine im Namen des Herstellers eingelöst. Diese Umsetzung ist nicht optimal, da der Private-Key des Herstellers damit lokal auf der Maschine vorliegen muss, wurde allerdings aufgrund der Einfachheit so umgesetzt. Ein Optimierungsansatz hierzu wird im Kapitel 10 vorgestellt. Der Zeitpunkt, wann eine Maschine eine Quittung einlösen sollte, wird in Abschnitt 7.4.4 genauer betrachtet.

¹ Beginn des Zeitraums ist zu anfangs der Vertragsbeginn; wurde bereits eine Bezahlung durch Schließen des Payment-Channels eingelöst, so wird der Startzeitpunkt der folgenden Quittung auf den Zeitpunkt des Schließens gesetzt.

C.2 DEPLOYMENT

Smart-Contract	Ropsten-Adresse
Rental-Provider	0x851ED36AC125a04A7384d485DoE5b710d1e8AB96
Identity-Provider	0xA17351BfA16dAE1FD285e11AcC00882Eb459C7cb
Payment-Provider	0x182B60f63AE760B137D479E00e823boC027736eE

Tabelle C.1: Adressen der Smart-Contracts auf dem öffentlichen Ropsten Testnet

C.3 KOSTENEVALUATION

Beschreibung	Anzahl	Einheit	Annahme
GAS-Price	5	GWEI	
ETH-Kurs	196,04	Euro	
Anzahl Kaffeemaschinen	10.000	Maschinen	x
Mitarbeiter pro Kaffeemaschine	40	Mitarbeiter	x
Mitarbeiter gesamt	400.000	Mitarbeiter	
Liter Kaffee pro Jahr pro Person	164	Liter	
Tassen Kaffee (0,2l) pro Jahr	820	Tassen	
Arbeitstage (abzgl. 30 Tage Urlaub)	230	Tage	
Tassen Kaffee (0,2l) pro Tag	2,24	Tassen	
Prepaid-Guthaben ausreichend für	5	Tage (Arbeitswoche)	
Preis pro Tasse Kaffee	0,25	Euro	x
Umsatzvolumen pro Maschine und Woche	157,69		
Prepaid Guthaben pro Maschine aufladen	200	Euro	x (inkl. Puffer)
Gesamtumsatz (jährlich)	82.000.000	Euro	
Gesamtumsatz pro Maschine (jährlich)	8.200	Euro	

Tabelle C.2: Basisdaten für Kostenkalkulationen, inklusive der Annahmen

Sender	Transaktion	GAS	WEI	ETH	Euro
Hersteller	Vertrag erstellen	426.609	2.133.045	0,002133	0,42
Hersteller	Quittung einlösen	157.927	789.635	0,00079	0,15
Kunde	Vertrag anfragen	197.964	989.820	0,00099	0,19
Kunde	Vertrag annehmen	162.743	813.715	0,000814	0,16
Kunde	Prepaid aufladen	28.805	144.025	0,000144	0,03

Tabelle C.3: Einzelkosten der Transaktion

Tx.	Tx. pro Maschine (einmalig)	Tx.-Kosten pro Maschine (einmalig)	Tx.-Kosten aller Maschinen (einmalig)	Tx. pro Maschine (jährlich)	Tx.-Kosten pro Maschine (jährlich)	Tx.-Kosten aller Maschinen (jährlich)
	Anzahl	Euro	Euro	Anzahl	Euro	Euro
Vertrag erstellen	1	0,42	4.200,00	0	0,00	0,00
Quittung einlösen	0	0,00	0,00	52	7,80	78.000,00
Vertrag anfragen	1	0,19	-	0	0,00	-
Vertrag annehmen	1	0,16	-	0	0,00	-
Prepaid aufladen	0	0,00	-	41	1,23	-

Tabelle C.4: Gesamtkosten (einmalig und jährlich) der Transaktionen aus Nutzer- und Herstellersicht

Abbildung C.3: Vertrag anfragen: Metamask Screenshot einer Transaktion

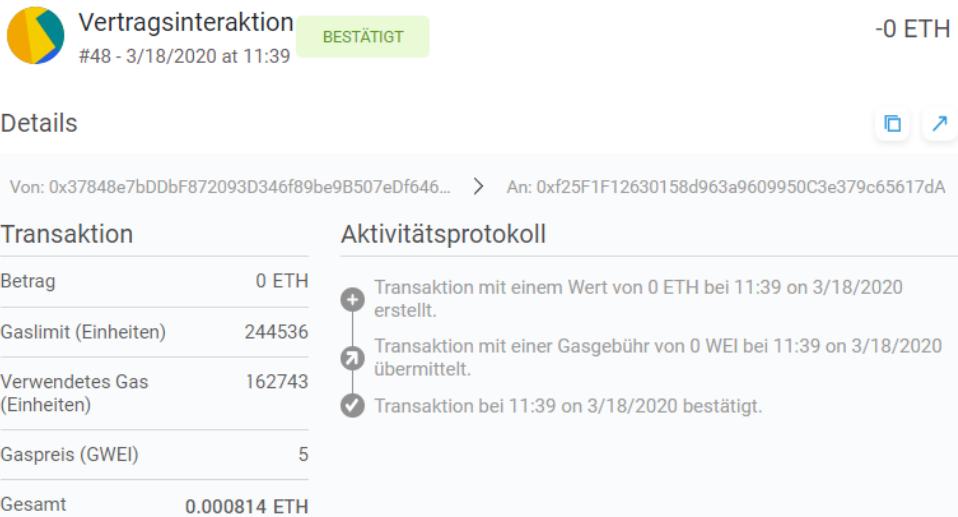


Abbildung C.4: Vertrag akzeptieren: Metamask Screenshot einer Transaktion

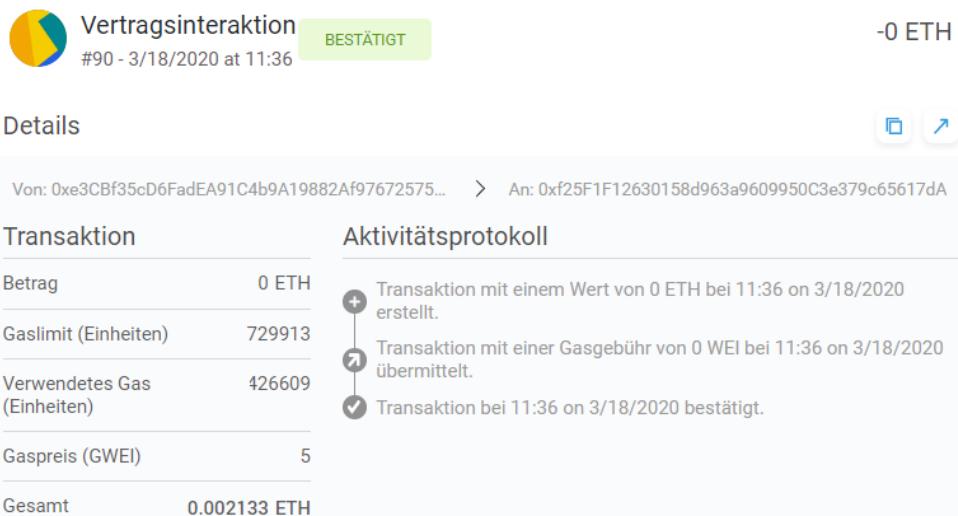


Abbildung C.5: Vertrag erzeugen: Metamask Screenshot einer Transaktion



Vertragsinteraktion #51 - 3/18/2020 at 11:50

BESTÄTIGT

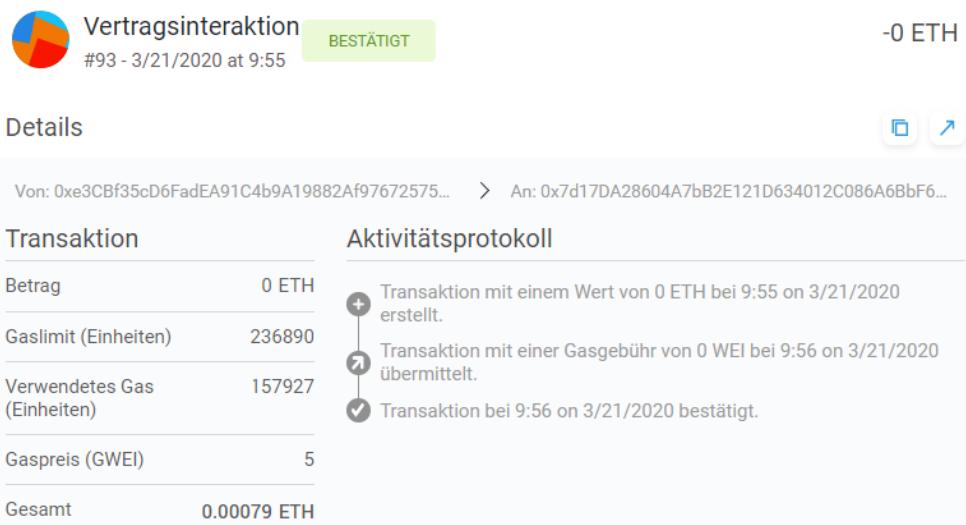
-0.05101 ETH

Details

Von: 0x37848e7bDDbF872093D346f89be9B507eDf646... > An: 0x7d17DA28604A7bB2E121D634012C086A6BbF6...

Transaktion		Aktivitätsprotokoll
Betrag	0.05101 ETH	Transaktion mit einem Wert von 0.05101 ETH bei 11:50 on 3/18/2020 erstellt.
Gaslimit (Einheiten)	43207	Transaktion mit einer Gasgebühr von 0 WEI bei 11:50 on 3/18/2020 übermittelt.
Verwendetes Gas (Einheiten)	28805	Transaktion bei 11:51 on 3/18/2020 bestätigt.
Gaspreis (GWEI)	5	
Gesamt	0.051154 ETH	

Abbildung C.6: Prepaid Guthaben aufladen: Metamask Screenshot einer Transaktion



Vertragsinteraktion #93 - 3/21/2020 at 9:55

BESTÄTIGT

-0 ETH

Details

Von: 0xe3CBf35cD6FadEA91C4b9A19882Af97672575... > An: 0x7d17DA28604A7bB2E121D634012C086A6BbF6...

Transaktion		Aktivitätsprotokoll
Betrag	0 ETH	Transaktion mit einem Wert von 0 ETH bei 9:55 on 3/21/2020 erstellt.
Gaslimit (Einheiten)	236890	Transaktion mit einer Gasgebühr von 0 WEI bei 9:56 on 3/21/2020 übermittelt.
Verwendetes Gas (Einheiten)	157927	Transaktion bei 9:56 on 3/21/2020 bestätigt.
Gaspreis (GWEI)	5	
Gesamt	0.00079 ETH	

Abbildung C.7: Quittung einlösen: Metamask Screenshot einer Transaktion

C.4 UI



Abbildung C.8: Wallet-App auf Android-Basis

D

APPENDIX: CODE

Listing D.1: RentalProvider Smart-Contract

```
pragma solidity >= 0.5.0 < 0.7.0;

import "./IdentityProvider.sol";
import "./PaymentProvider.sol";
import "./Ownable.sol";

contract RentalProvider is Ownable {

    enum AgreementState {
        Pending,
        Active,
        Terminated
    }

    RentalRequest[] public requests;
    RentalAgreement[] public agreements;
    address[] public rentableDevices;

    struct RentalRequest {
        address tenant;
        address lessor;
        address device;
        uint256 contractTerm;
    }

    struct RentalAgreement {
        address payable tenant;
        bytes tenantSignature;
        address payable lessor;
        bytes lessorSignature;
        address device;
        uint usageFee;          // 
        uint contractTerm;     //unix timestamp
        uint creation;         //unix timestamp
        AgreementState state;
        bytes32 paymentAgreementHash;
    }

    address public oracle_addr;
    address public paymentProvider_addr;

    constructor () public {
```

```

        owner = msg.sender;
    }

    function init() public onlyOwner {
        IdentityProvider oracle = IdentityProvider(oracle_addr);
        rentableDevices = oracle.getKnownDevices();
    }

    function destroy() public {
        require(msg.sender == owner, "Only owner can call this function.");
        selfdestruct(owner);
    }

    function getRentableDevices() public view returns (address[] memory){
        return rentableDevices;
    }

    function deviceIsRentable(address _device) public view returns (bool)
    {
        bool found = false;
        for(uint i = 0; i < rentableDevices.length; i++) {
            if(_device == rentableDevices[i]) {
                found = true;
            }
        }
        return found;
    }

    function createRequest(address _device, address _lessor, uint256 _term
    ) public {
        require(isKnownParticipant(msg.sender, 2));
        require(isKnownParticipant(_device, 5));
        require(isKnownParticipant(_lessor, 1));
        require(deviceIsRentable(_device));
        IdentityProvider oracle = IdentityProvider(oracle_addr);
        require(_lessor == oracle.getIdentityOwner(_device));
        require(!agreementExists(msg.sender, _device));
        require(!requestExists(msg.sender, _lessor, _device, _term));
        requests.push(RentalRequest(msg.sender, _lessor, _device, _term));
        removeDeviceFromRentableList(getRentableDeviceListIndex(_device));
    }

    function removeRequest(address _tenant, address _lessor, address _device,
    uint256 _term) public {
        require(isKnownParticipant(msg.sender, 1));
        require(msg.sender == _lessor);
        require(requestExists(_tenant, _lessor, _device, _term));
        uint index = 0;
        for(uint i = 0; i < requests.length; i++) {
            if(requests[i].tenant == _tenant && requests[i].lessor == _lessor
            && requests[i].device == _device && requests[i].contractTerm
            == _term) {

```

```

        index = i;
    }
}
for (uint i = index; i<requests.length-1; i++){
    requests[i] = requests[i+1];
}
requests.pop();
//delete requests[requests.length-1];
//requests.length--;
}

function getRequestsAsLessor() public view returns(address[] memory,
    address[] memory, address[] memory, uint256[] memory) {
require(isKnownParticipant(msg.sender, 1));
uint count = 0;
for(uint i = 0; i < requests.length; i++) {
    if(requests[i].lessor == msg.sender) {
        count++;
    }
}
address[] memory tenants = new address[](count);
address[] memory lessors = new address[](count);
address[] memory devices = new address[](count);
uint256[] memory terms = new uint256[](count);
uint index = 0;
for(uint i = 0; i < requests.length; i++) {
    if(requests[i].lessor == msg.sender) {
        tenants[index] = requests[i].tenant;
        lessors[index] = requests[i].lessor;
        devices[index] = requests[i].device;
        terms[index] = requests[i].contractTerm;
        index++;
    }
}
return (tenants, lessors, devices, terms);
}

function getRequestsAsTenant() public view returns(address[] memory,
    address[] memory, address[] memory, uint256[] memory) {
require(isKnownParticipant(msg.sender, 2));
uint count = 0;
for(uint i = 0; i < requests.length; i++) {
    if(requests[i].tenant == msg.sender) {
        count++;
    }
}
address[] memory tenants = new address[](count);
address[] memory lessors = new address[](count);
address[] memory devices = new address[](count);
uint256[] memory terms = new uint256[](count);
uint index = 0;
for(uint i = 0; i < requests.length; i++) {

```

```

        if(requests[i].tenant == msg.sender) {
            tenants[index] = requests[i].tenant;
            lessors[index] = requests[i].lessor;
            devices[index] = requests[i].device;
            terms[index] = requests[i].contractTerm;
            index++;
        }
    }
    return (tenants, lessors, devices, terms);
}

function requestExists(address _tenant, address _lessor, address _device, uint256 _term) public view returns (bool){
    for(uint i = 0; i < requests.length; i++) {
        if(requests[i].tenant == _tenant && requests[i].lessor == _lessor
            && requests[i].device == _device && requests[i].contractTerm
            == _term ) {
            return true;
        }
    }
    return false;
}

function removeDeviceFromRentableList(uint index) public {
    require(index < rentableDevices.length);
    require(index >= 0);
    for (uint i = index; i<rentableDevices.length-1; i++){
        rentableDevices[i] = rentableDevices[i+1];
    }
    rentableDevices.pop();
    //delete rentableDevices[rentableDevices.length-1];
    //rentableDevices.length--;
}

function getRentableDeviceListIndex(address _device) public view
    returns (uint) {
    for(uint i = 0; i < rentableDevices.length; i++) {
        if(_device == rentableDevices[i]) {
            return i;
        }
    }
    revert();
}

/// @notice asks registered oracle whether the identity is known or
/// not
/// @param _addr the address of the identity address
/// @param _roleID the role of the identity
/// @return a boolean whether or not the identity is known
function isKnownParticipant(address _addr, uint _roleID) public view
    returns(bool) {
    IdentityProvider oracle = IdentityProvider(oracle_addr);
}

```

```

        if(oracle.identityExists(_addr) && oracle.getIdentityRole(_addr)
            == _roleID) {
            return true;
        } else {
            return false;
        }
    }

    /// @notice sets the oracle address
    /// @dev only callable by owner
    /// @param _addr the address of the oracle
    function registerIdentityProvider(address _addr) public onlyOwner {
        oracle_addr = _addr;
    }

    /// @notice sets the PaymentProvider address
    /// @dev only callable by owner
    /// @param _addr the address of the PaymentProvider
    function registerPaymentProvider(address _addr) public onlyOwner {
        paymentProvider_addr = _addr;
    }

    function verify(address _tenant, address _lessor, address _device,
        uint256 _fee, uint256 _term, bytes memory _sig, address _signer)
        public pure returns (bool) {
        (uint8 v, bytes32 r, bytes32 s) = splitSignature(_sig);
        bytes32 hashCalc = keccak256(abi.encodePacked(_tenant,_lessor,_
            _device,_fee,_term));
        bytes memory prefix = "\x19Ethereum Signed Message:\n32";
        return ecrecover(keccak256(abi.encodePacked(prefix, hashCalc)), v, r
            , s) == _signer;
    }

    /// @notice creates a rentalAgreement
    /// @param _tenant address of the tenant
    /// @param _lessorSignature signature of lessor of rentalAgreement
    /// @param _device address of device
    /// @param _usageFee fee for usage in wei
    /// @param _contractTerm timestamp, when rentalAgreement times out
    function createRenting(address _tenant, bytes memory _lessorSignature,
        address _device, uint _usageFee, uint _contractTerm) public {
        require(verify(_tenant, msg.sender, _device, _usageFee, _contractTerm, _lessorSignature, msg.sender));
        //check if sender is Manufacturer, tenant is Customer and device is
        //Device
        require(isKnownParticipant(msg.sender, 1));
        require(isKnownParticipant(_tenant, 2));
        require(isKnownParticipant(_device, 5));
        //check contractTerm to be in future!
        require(_contractTerm > now);
        //check that no rentalAgreement with same parameters exists
        require(!agreementExists(_lessorSignature));
    }
}

```

```

//already removed by request!
//removeDeviceFromRentableList(getRentableDeviceListIndex(_device));

removeRequest(_tenant, msg.sender, _device, _contractTerm);

bytes32 paymentAgreementHash = keccak256(abi.encodePacked(now, _tenant, msg.sender));
PaymentProvider paymentProvider = PaymentProvider(paymentProvider_addr);
paymentProvider.addPaymentAgreement(paymentAgreementHash, msg.sender, address(uint160(_tenant)), _device);

agreements.push(RentalAgreement(address(uint160(_tenant)), new bytes(65), msg.sender, _lessorSignature, _device, _usageFee, _contractTerm, now, AgreementState.Pending, paymentAgreementHash));
}

function agreementExists(bytes memory _lessorSignature) public view
returns (bool) {
for(uint i = 0; i < agreements.length; i++) {
if(keccak256(agreements[i].lessorSignature) == keccak256(_lessorSignature)) {
return true;
}
}
return false;
}

function agreementExists(address _tenant, address _device) public view
returns (bool) {
require(isKnownParticipant(_tenant, 2));
require(isKnownParticipant(_device, 5));
for(uint i = 0; i < agreements.length; i++) {
if(agreements[i].device == _device && (agreements[i].state == AgreementState.Pending || agreements[i].state == AgreementState.Active)) {
return true;
}
}
return false;
}

function getIDs(uint _stateID) public view returns (uint[] memory) {
uint count = 0;
for(uint i = 0; i < agreements.length; i++) {
if((agreements[i].tenant == msg.sender || agreements[i].lessor == msg.sender) && agreements[i].state == AgreementState(_stateID))
) {
count++;
}
}
}

```

```

        }
    }
    uint[] memory rentalAgreementIDs = new uint[](count);
    uint index = 0;
    for(uint i = 0; i < agreements.length; i++) {
        if((agreements[i].tenant == msg.sender || agreements[i].lessor ==
            msg.sender) && agreements[i].state == AgreementState(_stateID)
            ) {
            rentalAgreementIDs[index] = i;
            index++;
        }
    }
    return rentalAgreementIDs;
}

function getByID(uint _id) public view returns (address, bytes memory,
    address, bytes memory, address, uint, uint, uint, uint, bytes32)
{
    require(_id < agreements.length);
    RentalAgreement memory agreement = agreements[_id];
    require(msg.sender == agreement.tenant || msg.sender == agreement.
        lessor);
    return (agreement.tenant, agreement.tenantSignature, agreement.
        lessor, agreement.lessorSignature, agreement.device, agreement.
        usageFee, agreement.contractTerm, agreement.creation, uint256(
        agreement.state), agreement.paymentAgreementHash);
}

function accept(uint _id, bytes memory _signature) public payable {
    require(_id < agreements.length);
    require(now < agreements[_id].contractTerm);
    require(agreements[_id].state == AgreementState.Pending);
    require(agreements[_id].tenant == msg.sender);
    require(recoverSigner(getRentalAgreementHash(_id), _signature) ==
        msg.sender);
    require(msg.value > 0);
    agreements[_id].tenantSignature = _signature;
    agreements[_id].state = AgreementState(1);
    PaymentProvider paymentProvider = PaymentProvider(paymentProvider_
        addr);
    paymentProvider.charge.value(msg.value)(agreements[_id].
        paymentAgreementHash);
}

function splitSignature(bytes memory _sig) internal pure returns (uint
    8 v, bytes32 r, bytes32 s) {
    require(_sig.length == 65);
    assembly {
        // first 32 bytes, after the length prefix.
        r := mload(add(_sig, 32))
        // second 32 bytes.
        s := mload(add(_sig, 64))
    }
}

```

```

        // final byte (first byte of the next 32 bytes).
        v := byte(0, mload(add(_sig, 96)))
    }
    if (v < 27) {
        v += 27;
    }

    require (v == 27 || v == 28);
    return (v, r, s);
}

function recoverSigner(bytes32 _message, bytes memory _sig) internal
    pure returns (address) {
    (uint8 v, bytes32 r, bytes32 s) = splitSignature(_sig);
    return ecrecover(_message, v, r, s);
}

function getRentalAgreementHash(uint _id) public view returns (bytes
    32) {
    require(_id < agreements.length);
    bytes32 message = keccak256(abi.encodePacked(agreements[_id].tenant,
        agreements[_id].lessor, agreements[_id].device, agreements[_id
        ].usageFee, agreements[_id].contractTerm));
    bytes memory prefix = "\x19Ethereum Signed Message:\n32";
    return keccak256(abi.encodePacked(prefix, message));
}

function terminate(uint _agreementID) public {
    require(_agreementID < agreements.length);
    RentalAgreement memory rentalAgreement = agreements[_agreementID];
    require(rentalAgreement.state == AgreementState.Active);
    require(msg.sender == rentalAgreement.tenant || msg.sender ==
        rentalAgreement.lessor);
    agreements[_agreementID].state = AgreementState.Terminated;

    PaymentProvider paymentProvider = PaymentProvider(paymentProvider_
        addr);
    paymentProvider.empty(agreements[_agreementID].paymentAgreementHash)
        ;

    rentableDevices.push(rentalAgreement.device);
}

// struct EIP712Domain {
//     string name;
//     string version;
//     uint256 chainId;
//     address verifyingContract;

```

```

//      bytes32 salt;
// }
//
// struct RentalSignatureObject {
//     address tenant;
//     address lessor;
//     address device;
//     uint256 fee;
//     uint256 term;
// }
//
// bytes32 constant public EIP712DOMAIN_TYPEHASH = keccak256(
//     "EIP712Domain(string name,string version,uint256 chainId,
//     address verifyingContract,bytes32 salt)"
// );
//
// bytes32 constant public RENTALSIGNATUREOBJECT_TYPEHASH = keccak256(
//     "RentalSignatureObject(address tenant,address lessor,address
//     device,uint256 fee,uint256 term)"
// );
//
// bytes32 public DOMAIN_SEPARATOR;

// constructor () public {
//     DOMAIN_SEPARATOR = hash(EIP712Domain({
//         name: "Device Rental",
//         version: '1',
//         chainId: 1579447585291,
//         // verifyingContract: this
//         verifyingContract: address(this),
//         salt: bytes32(0xf2d857f4a3edcb9b78b4d503bfe733db1e3f6cdc2b
//             7971ee739626c97e86a558)
//     }));
// }
//
// function hash(EIP712Domain memory eip712Domain) internal pure
// returns (bytes32) {
//     return keccak256(abi.encode(
//         EIP712DOMAIN_TYPEHASH,
//         keccak256(abi.encodePacked(eip712Domain.name)),
//         keccak256(abi.encodePacked(eip712Domain.version)),
//         eip712Domain.chainId,
//         eip712Domain.verifyingContract,
//         eip712Domain.salt
//     ));
// }
//
// function hash(RentalSignatureObject memory _sigObj) internal pure
// returns (bytes32) {
//     return keccak256(abi.encode(
//         RENTALSIGNATUREOBJECT_TYPEHASH,
//         keccak256(abi.encode(_sigObj.tenant)),
//         _sigObj.leaseId,
//         _sigObj.leaseTerm,
//         _sigObj.leaseFee,
//         _sigObj.leaseStatus
//     ));
// }

```

```

//      keccak256(abi.encode(_sigObj.lesser)),
//      keccak256(abi.encode(_sigObj.device)),
//      keccak256(abi.encode(_sigObj.fee)),
//      keccak256(abi.encode(_sigObj.term))
//      // keccak256(bytes(mail.contents))
//    );
// }

// 
// function verify(address _tenant, address _lessor, address _device,
//   uint256 _fee, uint256 _term, bytes memory _sig, address _signer)
public view returns (bool) {
//  (uint8 v, bytes32 r, bytes32 s) = splitSignature(_sig);
//  // Note: we need to use 'encodePacked' here instead of 'encode'.
//  RentalSignature0bject memory sigObj = RentalSignature0bject(_
//  tenant, _lessor, _device, _fee, _term);
//  bytes32 digest = keccak256(abi.encodePacked(
//    "\x19\x01",
//    DOMAIN_SEPARATOR,
//    hash(sigObj)
//  ));
//  return ecrecover(digest, v, r, s) == _signer;
// }

```

Listing D.2: PaymentProvider Smart-Contract

```

pragma solidity >= 0.5.0 < 0.7.0;
import "./Ownable.sol";

/// @notice https://programtheblockchain.com/posts/2018/02/23/writing-a-
// simple-payment-channel

contract PaymentProvider is Ownable {

  struct PaymentAgreement {
    address payable sender;
    address payable receiver;
    address device;
    uint256 balance;
    uint256 numPayments;
    mapping(bytes32 => bool) usedSignatures;
    mapping(uint256 => Usage) history;
  }

  struct Usage {
    uint256 timestampStart;
    uint256 timestampEnd;
    uint256 units;
    uint256 cost;
  }

  mapping(bytes32 => PaymentAgreement) public paymentAgreements;

```

```

address private rentalProvider;

/// @notice sets the rentalProvider address
/// @dev only callable by owner
/// @param _addr the address of the rentalProvider
function registerRentalProvider(address _addr) public onlyOwner {
    rentalProvider = _addr;
}

function addPaymentAgreement(bytes32 _hash, address payable _receiver,
    address payable _sender, address _device) public {
    PaymentAgreement memory tmp;
    tmp.sender = _sender;
    tmp.receiver = _receiver;
    tmp.device = _device;
    tmp.balance = 0;
    tmp.numPayments = 0;
    paymentAgreements[_hash] = tmp;
}

// The sender can charge the channel
function charge(bytes32 _hash) public payable {
    require(msg.sender == paymentAgreements[_hash].sender || msg.sender
        == rentalProvider);
    paymentAgreements[_hash].balance = paymentAgreements[_hash].balance
        + msg.value;
}

function getSender(bytes32 _hash) public view returns (address) {
    require(msg.sender == paymentAgreements[_hash].sender || msg.sender
        == paymentAgreements[_hash].receiver);
    return paymentAgreements[_hash].sender;
}

function getReceiver(bytes32 _hash) public view returns (address) {
    require(msg.sender == paymentAgreements[_hash].sender || msg.sender
        == paymentAgreements[_hash].receiver);
    return paymentAgreements[_hash].receiver;
}

function getDevice(bytes32 _hash) public view returns (address) {
    require(msg.sender == paymentAgreements[_hash].sender || msg.sender
        == paymentAgreements[_hash].receiver);
    return paymentAgreements[_hash].device;
}

function getBalance(bytes32 _hash) public view returns (uint256) {
    require(msg.sender == paymentAgreements[_hash].sender || msg.sender
        == paymentAgreements[_hash].receiver);
    return paymentAgreements[_hash].balance;
}

```

```

function getPaymentHistory(bytes32 _hash) public view returns(uint
256[] memory, uint256[] memory, uint256[] memory, uint256[] memory
) {
    uint count = paymentAgreements[_hash].numPayments;
    uint256[] memory timestampsStart = new uint256[](count);
    uint256[] memory timestampEnd = new uint256[](count);
    uint256[] memory units = new uint256[](count);
    uint256[] memory costs = new uint256[](count);
    for (uint i = 0; i<count; i++){
        timestampsStart[i] = paymentAgreements[_hash].history[i].
            timestampStart;
        timestampEnd[i] = paymentAgreements[_hash].history[i].
            timestampEnd;
        units[i] = paymentAgreements[_hash].history[i].units;
        costs[i] = paymentAgreements[_hash].history[i].cost;
    }
    return (timestampsStart, timestampEnd, units, costs);
}

function empty(bytes32 _hash) public {
    require(msg.sender == paymentAgreements[_hash].receiver || msg.
        sender == rentalProvider);
    paymentAgreements[_hash].sender.transfer(paymentAgreements[_hash].
        balance);
    paymentAgreements[_hash].balance = 0;
}

// The receiver can pay out his balance by presenting a signed
// amount from the sender. The receiver will be sent that amount but
// the channel will stay open.
// The rest of the balance is kept in the channel and not payed out
// back to the sender.
function redeem(bytes32 _hash, uint256 _timestampStart, uint256 _-
    timestampEnd, uint256 _units, uint256 _cost, bytes memory _-
    signature, address _device) public {
    bytes32 paymentHash = keccak256(abi.encodePacked(_hash, _-
        timestampStart, _timestampEnd, _units, _cost, _signature, _-
        device));
    require(paymentAgreements[_hash].usedSignatures[paymentHash] ==
        false, "Signature already used!");
    require(_timestampStart < _timestampEnd, "timestampStart lower than
        timestampEnd!");
    require(_device == paymentAgreements[_hash].device, "Device invalid
        !");
    require(_cost <= paymentAgreements[_hash].balance, "Not enough money
        !");
    require(msg.sender == paymentAgreements[_hash].receiver, "You must
        be the receiver in order to redeem a payment!");
    require(isValidSignature(paymentAgreements[_hash].sender, _-
        timestampStart, _timestampEnd, _units, _cost, _device, _-
        signature), "Signature invalid!");
}

```

```

        uint256 num = paymentAgreements[_hash].numPayments;
        paymentAgreements[_hash].history[num] = Usage(_timestampStart, -
            timestampEnd, _units, _cost);
        paymentAgreements[_hash].numPayments++;

        uint256 totalCosts = _cost * _units;

        paymentAgreements[_hash].receiver.transfer(totalCosts);
        paymentAgreements[_hash].usedSignatures[paymentHash] = true;
        paymentAgreements[_hash].balance = paymentAgreements[_hash].balance
            - totalCosts;
    }

    // The sender can extend the expiration at any time.
    // function extend(uint256 newExpiration) public {
    //     require(msg.sender == sender);
    //     require(newExpiration > expiration);
    //     //
    //     expiration = newExpiration;
    // }

    // If the timeout is reached without the receiver closing the channel,
    // then
    // the ether is released back to the sender.
    // function claimTimeout() public {
    //     require(now >= expiration);
    //     selfdestruct(sender);
    // }

    //#####
    //Helper#####
    //

    /// @notice gets the address of this contract
    function getAddress() public view returns (address) {
        return address(this);
    }

    function isValidSignature(address _sender, uint256 _timestampStart,
        uint256 _timestampEnd, uint256 _units, uint256 _cost, address _device,
        bytes memory _signature) public view returns (bool) {
        bytes32 message = prefixed(keccak256(abi.encodePacked(this, _timestampStart, _timestampEnd, _units, _cost, _device)));

        // Check that the signature is from the payment sender.
        return recoverSigner(message, _signature) == _sender;
    }

    function splitSignature(bytes memory sig) public pure returns (uint8,
        bytes32, bytes32) {
        require(sig.length == 65);

        bytes32 r;

```

```

bytes32 s;
uint8 v;

assembly {
    // first 32 bytes, after the length prefix
    r := mload(add(sig, 32))
    // second 32 bytes
    s := mload(add(sig, 64))
    // final byte (first byte of the next 32 bytes)
    v := byte(0, mload(add(sig, 96)))
}
if (v < 27) {
    v += 27;
}

require (v == 27 || v == 28);

return (v, r, s);
}

function recoverSigner(bytes32 message, bytes memory sig) public pure
    returns (address) {
    uint8 v;
    bytes32 r;
    bytes32 s;

    (v, r, s) = splitSignature(sig);

    return ecrecover(message, v, r, s);
}

// Builds a prefixed hash to mimic the behavior of eth_sign.
function prefixed(bytes32 hash) public pure returns (bytes32) {
    return keccak256(abi.encodePacked("\x19Ethereum Signed Message:\n"
        32", hash));
}
}

```

Listing D.3: IdentityProvider Smart-Contract

```

pragma solidity >= 0.5.0 < 0.7.0;

import "./Ownable.sol";
// import "./DateLib.sol";

/// @title IdentityProvider
/// @author Sebastian Kanz
/// @notice Taken from: https://github.com/jrkosinski/oracle-example/blob/part2-step1/oracle/contracts/BoxingOracle.sol
/// @notice Collects and provides information on identities
contract IdentityProvider is Ownable {
    mapping(address => Identity) identities;

```

```

address[] knownDevices;
address[] knownManufacturers;
address[] knownServiceProviders;
address[] knownSuppliers;

// using DateLib for DateLib.DateTime;

//defines an identity
struct Identity {
    string name;
    uint256 date;          //GMT timestamp of date of registration
    Role role;
    address ownedBy;
    bool exists;
}

//possible roles of identities
enum Role {
    None,
    Manufacturer,
    Customer,
    ServiceProvider,
    Supplier,
    Device
}

constructor () public {
    owner = msg.sender;
    // addTestData();
}

/// @notice checks whether the identity is known or not
/// @param _identity the identity address to analyze
/// @return returns true if the identity is known
function identityExists(address _identity) public view returns (bool)
{
    if(identities[_identity].exists) {
        return true;
    } else {
        return false;
    }
}

/// @notice gets the role of the identity
/// @param _identity the identity address to analyze
/// @return a string representative of the Role. If the identity is
///         unknown it returns the default (Role.None)
function getIdentityRoleName(address _identity) public view returns (
    string memory) {
    Role role = identities[_identity].role;
    if(role == Role.Manufacturer) {
        return "Manufacturer";
    }
}

```

```

        } else if(role == Role.Customer) {
            return "Customer";
        } else if(role == Role.ServiceProvider) {
            return "ServiceProvider";
        } else if(role == Role.Supplier) {
            return "Supplier";
        } else if(role == Role.Device) {
            return "Device";
        } else {
            return "None";
        }
    }

    /// @notice gets the owner of the identity (if it is a device)
    /// @param _identity the identity address to analyze
    /// @return an address. If the identity is owned by no one it returns
    ///         the default address (0x0...)
    function getIdentityOwner(address _identity) public view returns (
        address) {
        return identities[_identity].ownedBy;
    }

    /// @notice gets the role of the identity
    /// @param _identity the identity address to analyze
    /// @return a uint. If the identity is unknown it returns the default
    ///         (0)
    function getIdentityRole(address _identity) public view returns (uint)
    {
        return uint(identities[_identity].role);
    }

    /// @notice gets the creation time of the identity
    /// @param _identity the identity address to analyze
    /// @return a unix timestamp. If the identity is unknown it returns
    ///         the default (0)
    function getIdentityCreationTime(address _identity) public view
        returns (uint256) {
        return identities[_identity].date;
    }

    /// @notice gets the name of the identity
    /// @param _identity the identity address to analyze
    /// @return a unix string. If the identity is unknown it returns the
    ///         default (empty string)
    function getIdentityName(address _identity) public view returns (
        string memory) {
        return identities[_identity].name;
    }

    /// @notice adds a new identity
    /// @dev only callable by owner of smart contract

```

```

/// @param _name the name of the identity
/// @param _roleID the role of the identity as integer representative
/// @param _identity the identity address to analyze
/// @param _owner the owner of the identity
function addIdentityOwnedBy(string memory _name, uint _roleID, address
    _identity, address _owner) onlyOwner public {
    require(!identityExists(_identity));
    require(identityExists(_owner));
    require(_roleID == 5);
    Identity memory newIdentity = Identity(_name, now, Role(_roleID), _
        owner, true);
    identities[_identity] = newIdentity;
    knownDevices.push(_identity);
}

/// @notice adds a new identity
/// @dev only callable by owner of smart contract
/// @param _name the name of the identity
/// @param _roleID the role of the identity as integer representative
/// @param _identity the identity address to analyze
function addIdentity(string memory _name, uint _roleID, address _
    identity) onlyOwner public {
    require(!identityExists(_identity));
    require(_roleID > 0 && _roleID != 5);
    Identity memory newIdentity = Identity(_name, now, Role(_roleID), -
        identity, true);
    identities[_identity] = newIdentity;
    if(Role(_roleID) == Role.Manufacturer) {
        knownManufacturers.push(_identity);
    } else if(Role(_roleID) == Role.ServiceProvider) {
        knownServiceProviders.push(_identity);
    } else if(Role(_roleID) == Role.Supplier) {
        knownSuppliers.push(_identity);
    } else if(Role(_roleID) != Role.Customer) {
        revert("This should not happen.");
    }
}

/// @notice deletes an identity
/// @dev only callable by owner of smart contract
/// @param _identity the identity address to analyze
/// @return a boolean whether or not deleting was successful
function deleteIdentity(address _identity) onlyOwner public returns (
    bool) {
    if(identityExists(_identity)) {
        identities[_identity] = Identity("", 0, Role.None, address(0x0),
            false);
        return true;
    } else {
        return false;
    }
}

```

```

/// @notice tests the connection to the smart contract
/// @dev only for testing purposes
/// @return always true
function testConnection() public pure returns (bool) {
    return true;
}

/// @notice gets the address of this contract
function getAddress() public view returns (address) {
    return address(this);
}

/// @notice adds test identities
/// @dev only callable by owner of smart contract
function addTestData() onlyOwner public {
    addIdentity("Manufacturer", uint(Role.Manufacturer), address(0xe3CBf
        35cD6FadEA91C4b9A19882Af976725753dD));
    addIdentity("Customer1", uint(Role.Customer), address(0x37848e7bDDbF
        872093D346f89be9B507eDf6462b));
    addIdentity("Customer2", uint(Role.Customer), address(0x8Ef5906034be
        23248EF49C38fEf9f17265ab044F));
    addIdentityOwnedBy("Device1", uint(Role.Device), address(0xf00C699c
        96E05f919EE1C57B824a29cC6216352E), address(0xe3CBf35cD6FadEA91C4
        b9A19882Af976725753dD));
    addIdentityOwnedBy("Device2", uint(Role.Device), address(0xCF5f7aa
        0103662Ef67cF453F7d4A6bFDfF04057e), address(0xe3CBf35cD6FadEA91C
        4b9A19882Af976725753dD));
    addIdentityOwnedBy("Device3", uint(Role.Device), address(0x4A21C369a
        3B7f4C56eC4DcBAB706C30897Cb1845), address(0xe3CBf35cD6FadEA91C4b
        9A19882Af976725753dD));
    addIdentityOwnedBy("Device4", uint(Role.Device), address(0xEa05a
        247562D4865F6e2a5d9347EeB61C966A214), address(0xe3CBf35cD6FadEA
        91C4b9A19882Af976725753dD));
}

function getKnownManufacturers() public view returns(address[] memory)
{
    return knownManufacturers;
}

function getKnownServiceProviders() public view returns(address[]
    memory){
    return knownServiceProviders;
}

function getKnownSuppliers() public view returns(address[] memory){
    return knownSuppliers;
}

function getKnownDevices() public view returns(address[] memory){
    return knownDevices;
}

```

```
    }  
}
```

LITERATUR

- [1] .
- [2] Alain Abran und James W. Moore, Hrsg. *Guide to the Software Engineering Body of Knowledge: 2004 Version SWEBOK*. Los Alamitos, CA: IEEE Computer Society Press, 2005. ISBN: 0-7695-2330-7. URL: <http://www2.computer.org/portal/web/swebok/2004guide>.
- [3] Mohammed Alani. *Guide to OSI and TCP/IP Models*. Jan. 2014. ISBN: 978-3-319-05152-9. DOI: [10.1007/978-3-319-05152-9](https://doi.org/10.1007/978-3-319-05152-9).
- [4] Maher Alharby und Aad van Moorsel. "Blockchain-based Smart Contracts: A Systematic Mapping Study". In: (2017). URL: [http://arxiv.org/abs/1710.06372](https://arxiv.org/abs/1710.06372).
- [5] Anton Badev u. a. "Distributed Ledger Technology in Payments, Clearing, and Settlement". In: *Finance and Economics Discussion Series 2016* (Dez. 2016). DOI: [10.17016/FEDS.2016.095](https://doi.org/10.17016/FEDS.2016.095).
- [6] I. Bashir. *Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained*. Packt Publishing, 2017. ISBN: 9781787125445. URL: <https://books.google.de/books?id=dMJbMQAACAAJ>.
- [7] Kariappa Bheemaiah. "Block Chain 2.0: The Renaissance of Money". In: *wired* (2015). URL: <https://www.wired.com/insights/2015/01/block-chain-2-0/>.
- [8] Binance. *Die Geschichte der Blockchain*. 2019. URL: <https://www.binance.vision/de/blockchain/history-of-blockchain>.
- [9] Vitalik Buterin. *Ethereum: A next-generation smart contract and decentralized application platform*. 2013. URL: <https://github.com/ethereum/wiki/wiki/White-Paper>.
- [10] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng und V. C. M. Leung. "Decentralized Applications: The Blockchain-Empowered Software System". In: *IEEE Access* 6 (2018), S. 53019–53033.
- [11] Michael del Castillo. "Blockchain 50: Billion Dollar Babies". In: *Forbes* (2019). URL: <https://www.forbes.com/sites/michaeldelcastillo/2019/04/16/blockchain-50-billion-dollar-babies/#6dfb0c0657cc>.
- [12] K. Chatterjee, A. K. Goharshady und A. Pourdamghani. "Probabilistic Smart Contracts: Secure Randomness on the Blockchain". In: *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. 2019, S. 403–412.

- [13] R.J. Cloutier (Editor in Chief). *The Guide to the Systems Engineering Body of Knowledge (SEBoK)*. v.2.0. BKCASE. The Trustees of the Stevens Institute of Technology, International Council on Systems Engineering, Institute of Electrical und Electronics Engineers Computer Society, 2019.
- [14] K. Christidis und M. Devetsikiotis. "Blockchains and Smart Contracts for the Internet of Things". In: *IEEE Access* 4 (2016), S. 2292–2303. ISSN: 2169-3536. doi: [10.1109/ACCESS.2016.2566339](https://doi.org/10.1109/ACCESS.2016.2566339).
- [15] Cisco. *Internet of Things*. 2016. URL: <https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf>.
- [16] Jeff Coleman, Liam Horne und Xuanji Li. *Counterfactual: Generalized State Channels*. 2018. URL: <http://l4.ventures/papers/statechannels.pdf>.
- [17] Arnold Daniels. *The rise of private permissionless blockchains*. 2018. URL: <https://medium.com/ltonetwork/the-rise-of-private-permissionless-blockchains-part-2-62553256953d>.
- [18] Liping Deng, Huan Chen, Jing Zeng und Liang-Jie Zhang. *Research on Cross-Chain Technology Based on Sidechain and Hash-Locking*. Hrsg. von Shijun Liu, Bedir Tekinerdogan, Mikio Aoyama und Liang-Jie Zhang. 2018.
- [19] *Duden – Deutsches Universalwörterbuch*. 9. Aufl. Bibliographisches Institut, 2019. ISBN: 978-3-411-98217-2. URL: <http://www.duden.de/>.
- [20] T. M. Fernández-Caramés und P. Fraga-Lamas. "A Review on the Use of Blockchain for the Internet of Things". In: *IEEE Access* 6 (2018), S. 32979–33001. ISSN: 2169-3536. doi: [10.1109/ACCESS.2018.2842685](https://doi.org/10.1109/ACCESS.2018.2842685).
- [21] Forbes. *Blockchain's Secret 1,000 Year History*. 2018. URL: <https://www.forbes.com/sites/oliversmith/2018/03/23/blockchains-secret-1000-year-history/#6871020e18d2>.
- [22] *Gabler Wirtschafts Lexikon*. 16. Aufl. Gabler Verlag, 2004. ISBN: 978-3-663-10128-4. URL: <https://www.springer.com/gp/book/9783663101284>.
- [23] R. Han, V. Gramoli und X. Xu. "Evaluating Blockchains for IoT". In: *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. 2018, S. 1–5. doi: [10.1109/NTMS.2018.8328736](https://doi.org/10.1109/NTMS.2018.8328736).
- [24] IEEE. "Systems and software engineering – Life cycle processes – Requirements engineering". In: *ISO/IEC/IEEE 29148:2011(E)* (2011).
- [25] ISO/IEC. *ISO/IEC 25010 System and software quality models*. Techn. Ber. 2010.
- [26] Iiba. *Babok: A Guide to the Business Analysis Body of Knowledge*. Bd. 3. International Institute of Business Analysis, 2015. ISBN: 9781927584026. URL: <https://books.google.de/books?id=ogxTrgEACAAJ>.
- [27] Project Management Institute. *A Guide to the Project Management Body of Knowledge(PMBOK Guide)*. 4th. PMI global standard. Project Management Institute, 2010. ISBN: 9781933890661.

- [28] Sandra Johnson, Peter Robinson und John Brainard. "Sidechains and interoperability". In: *CoRR* abs/1903.04077 (2019). URL: <http://arxiv.org/abs/1903.04077>.
- [29] Deutscher Kaffeeverband. *Kaffee statt Kicker: Darum ist Bürokaffee so wichtig*. 2019. URL: <https://www.kaffeeverband.de/de/presse/kaffee-statt-kicker-darum-ist-buerokaffee-so-wichtig>.
- [30] Leslie Lamport, Robert Shostak und Marshall Pease. *The Byzantine Generals Problem*. Association for Computing Machinery, 2019. ISBN: 9781450372701.
- [31] M Macdonald, Lisa Liu-Thorrold und R Julien. *The Blockchain: A Comparison of Platforms and Their Uses Beyond Bitcoin*. Feb. 2017. DOI: [10.13140/RG.2.2.23274.52164](https://doi.org/10.13140/RG.2.2.23274.52164).
- [32] Mohammad Maroufi, Reza Abdolee und Behzad Mozaffari Tazehkand. "On the Convergence of Blockchain and Internet of Things (IoT) Technologies". In: *CoRR* abs/1904.01936 (2019). arXiv: [1904.01936](https://arxiv.org/abs/1904.01936). URL: <http://arxiv.org/abs/1904.01936>.
- [33] Satoshi Nakamoto. *Bitcoin: A peer-to-peer electronic cash system*. 2009. URL: <http://www.bitcoin.org/bitcoin.pdf>.
- [34] Alexandre Miranda Pinto. *An Introduction to the Use of zk-SNARKs in Blockchains*. Hrsg. von Panos Pardalos, Ilias Kotsireas, Yike Guo und William Knottenbelt. Cham: Springer International Publishing, 2020, S. 233–249. ISBN: 978-3-030-37110-4.
- [35] Joseph Poon und Thaddeus Dryja. *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*. 2016. URL: <https://lightning.network/lightning-network-paper.pdf>.
- [36] Mehrdad Salimitari und Mainak Chatterjee. "A Survey on Consensus Protocols in Blockchain for IoT Networks". In: 2018.
- [37] Milan Sallaba, Dirk Siegel und Sebastian Becker. *IoT powered by Blockchain - How Blockchains facilitate the application of digital twins in IoT*. Techn. Ber. Deloitte, Blockchain Institute, 2018.
- [38] M. Samaniego und R. Deters. "Blockchain as a Service for IoT". In: *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. 2016, S. 433–436. DOI: [10.1109/ithings-GreenCom-CPSCom-SmartData.2016.102](https://doi.org/10.1109/ithings-GreenCom-CPSCom-SmartData.2016.102).
- [39] W3C. *Decentralized Identifier*. 2019. URL: <https://www.w3.org/TR/did-core/>.
- [40] D. J. Weitzner. "Whose Name Is It, Anyway? Decentralized Identity Systems on the Web". In: *IEEE Internet Computing* 11.4 (2007), S. 72–76.
- [41] JC XU, Zhoudong Ji und Yanbo Li. *An Off-chain Scaling Solution for Neo*. 2018. URL: <https://trinity.tech/#/writepaper>.

- [42] Z. Zheng, S. Xie, H. Dai, X. Chen und H. Wang. "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends". In: *2017 IEEE International Congress on Big Data (BigData Congress)*. 2017, S. 557–564.
- [43] H. Zimmermann. "OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection". In: *IEEE Transactions on Communications* 28.4 (1980), S. 425–432. ISSN: 1558-0857. DOI: [10.1109/TCOM.1980.1094702](https://doi.org/10.1109/TCOM.1980.1094702).
- [44] Sorin Zoican, Marius Vochin, Roxana Zoican und Dan Galatchi. "Blockchain and Consensus Algorithms in Internet of Things". In: Nov. 2018. DOI: [10.1109/ISETC.2018.8583923](https://doi.org/10.1109/ISETC.2018.8583923).
- [45] winterhalter. *PAY PER WASH*. 2020. URL: https://www.pay-per-wash.biz/de_de/.