Konzepte zur Kollaboration zwischen Intelligenten Geräten zum Aufbau vernetzter Städte

Zur Erlangung des akademischen Grades eines

Doktors der Ingenieurwissenschaften (Dr.-Ing.)

von der KIT-Fakultät für
Elektrotechnik und Informationstechnik,
des Karlsruher Instituts für Technologie (KIT)

genehmigte

DISSERTATION

von

Dipl. Ing. Markus Lücking
geb. in Friesoythe

Tag der mündlichen Prüfung:	26.01.2023
Hauptreferent:	Prof. Dr. rer. nat Wilhelm Stork
Korreferent:	Prof. Dr. rer. nat. Cornelius Neumann

Kurzfassung

Eine starke Urbanisierung hat in vielen Städten zu einer Verschlechterung der Lebensqualität geführt. Beispielsweise nimmt in vielen Städte die Luftqualität kontinuierlich ab. Durch den Einsatz innovativer Technologien sollte solche negative Entwicklungen reduziert werden. Jedoch hat der bisherige Einsatz von Informations- und Kommunikationstechnologien zum Aufbau isolierter Systeme geführt, die ausschließlich für statische Anwendungsszenarien konzeptioniert wurden und ungeeignet sind die Lebensqualität der Bürger zu verbessern.

Diese Arbeit beginnt mit der Entwicklung eines intelligenten Sensormoduls (Smart City Node) zur Bewältigung urbaner Herausforderungen, wie beispielsweise einer zunehmenden Luftverschmutzung. Der entwickelte Smart City Node nutzt zur effizienten Verkehrsanalyse modernste Bildverarbeitungsmethoden der künstlichen Intelligenz, um Verkehrsinformation datenschutzkonform bereitzustellen. Neben Verkehrsinformationen werden vom Sensormodul lokale Schadstoffbelastung und meteorologische Parameter bestimmt. Zur Bewältigung lokaler Luftverschmutzungen liefert der Smart City Node kostengünstige und echtzeitfähige Messungen der Bereiche Umwelt und Verkehr.

Im Rahmen dieser Arbeit werden zudem innovative Konzepte zur urbanen Vernetzung vorgestellt, um die vom Smart City Node generierte Vielzahl an Messungen in unterschiedlichen Anwendungsszenarien effizient nutzen zu können. Basierend auf einer Literaturrecherche werden Anforderungen an ein dezentrales Systems definiert, mit dem sich Messdaten verteilter Sensormodule sicher speichern und mit anderen Entitäten teilen lassen. Zusätzlich zur sicheren und transparenten Speicherung werden Konzepte zur verlässlichen Datenverwaltung entwickelt. Hierzu zählt die Identifikation, Authentifikation und Autorisierung in dezentral

verwalteten Systemen. Diese Arbeit beschreibt, wie sich digitale Identitäten eigenständig aufbauen, kontrollieren und nutzen lassen, um einzelne Datenpakete kontinuierlicher Datenströme anderen Entitäten freizugeben.

Neben technischen werden auch wirtschaftliche Herausforderungen betrachtet, die einer Kollaboration zwischen intelligenten Sensormodulen entgegenstehen. Hierzu wird analysiert, wie durch wirtschaftliche Kollaborationsanreize ein Übergang vom freiwilligen Datentransfer hin zur Datenmonetarisierung gelingen kann. Die entwickelten Konzepte werden in einem realen Verkehrsszenario evaluiert, in dem Daten zwischen einem intelligenten Sensormodul und Pkw monetarisiert werden. Die erzielten Evaluierungsergebnisse zeigen, dass die entwickelten Konzepte ein wirtschaftliches Monetarisieren von bereits geringen Datenmengen ermöglichen und somit systemübergreifende Kollaborationen fördern.

Abstract

Strong urbanization has led to a deterioration in of life quality in many cities. For example, the air quality in many cities is continuously declining. The use of innovative technologies should reduce such negative trends. However, the use of information and communication technologies to date has led to the creation of isolated systems that have been designed exclusively for static application scenarios and are not suitable for improving the life quality of citizens.

This work starts with the development of an intelligent sensor module (Smart City Node), to address urban challenges such as increasing air pollution. The developed Smart City Node uses state-of-the-art artificial intelligence image processing methods for efficient traffic analysis to provide traffic information in a privacy-compliant manner. In addition to traffic information, the sensor module also determines local pollution levels and meteorological parameters. The Smart City Node provides cost-effective measurements of the environment and traffic to tackle air pollution.

In the context of this work, innovative concepts for urban networking are presented to efficiently use the variety of measurements provided by the Smart City Node for different application scenarios. Based on a comprehensive literature review, requirements are defined for a decentralized system that can securely store and share measurement data from distributed sensor modules with other entities. In addition to secure and transparent storage, concepts for reliable data management are developed. This includes the identification, authentication and authorization in a fully decentralized system, independent from any third party authorities. This work describes how digital identities can be autonomously established, controlled

and used to share individual data packets of continuous data streams with other entities.

Next to technical also economic challenges have been taken into account, to establish cooperation between smart sensor modules. For this purpose, it is analyzed how a transition from voluntary cooperation to open data monetization can succeed in order to create economic incentives for cooperation. The developed concepts are evaluated in a real traffic scenario where data is spontaneously monetized between a smart sensor module and a passenger car. The evaluation results obtained show that the developed concepts enable economic monetization of even small amounts of data and thus promote cross-system cooperation.

Danksagung

Ich möchte mich bei allen bedanken, die zum Gelingen dieser Arbeit beigetragen haben.

Ein ganz besonderer Dank gilt meinem Doktorvater Prof. Dr. rer. nat. Wilhelm Stork für sein mir entgegengebrachtes Vertrauen. Ohne seine unkonventionellen Ideen, unsere inspirierenden Gespräche und den Freiraum zur eigenverantwortlichen Gestaltung meiner wissenschaftlichen Arbeit, wäre die vorliegende Dissertation nicht entstanden. Herzlich danken möchte ich ebenfalls Herrn Prof. Dr. rer. nat. Cornelius Neumann für die Übernahme des Korreferats und das damit verbundene Engagement.

Für die vielen Impulse und ein tolles Arbeitsumfeld möchte ich meinen Kollegen und Freunden des Forschungszentrum Informatik (FZI) danken. Während meiner Tätigkeit als wissenschaftlicher Mitarbeiter am FZI hatte ich das Vergnügen viele talentierte Studenten zu betreuen, dessen Arbeiten zum Gelingen meiner Promotion beigetragen haben und denen ebenfalls mein Dank gebührt. Zudem danke ich Niclas Kannengießer für viele anregende Diskussionen.

Ein besonderer Dank gilt meiner Familie und meinen Freuden für ihren starken Rückhalt und stetigen Ermutigungen. Vor allem danke ich von ganzem Herzen meiner Frau Duygu für ihre unerschöpfliche Geduld und stetige Unterstützung.

Inhaltsverzeichnis

Abkürzungen und Symbole

Abkürzungen

PMS	Pollution Monitoring System
SCN	Smart City Node
CNN	Convolutional Neural Network
GPU	Graphic Processing Unit
RCNN	Region Based Convolutional Neural Network
FPS	Frames per Second
SSD	Single Shot Detector
SORT	Simple Real time Tracker
YOLO	You Only Look Once
WSN	Wireless sensor networks
QoS	Quality of Service
PKI	Public Key Infrastructure
ROI	Region of Interest
DSGVO	Datenschutzgrundverordnung
V2I	Vehicle to Infrastructure

AQM	Air Quality Management
LoRaWAN	Long Range Wide Area Network
W3C	World Wide Web Consortium
DSRC	Dedicated Short Range Communication
WoT	Web of Trust
DLT	Distributed Ledger Technology
DID	Decentralized identifier
CA	Certificate Authority
RMSE	Root Mean Square Error

1 Einleitung

Dieses Kapitel leitet das Themengebiet der vorliegenden Dissertation ein. Hierzu wird auf aktuelle Herausforderung eingegangen, die Kollaboration zwischen intelligenten Sensoren und urbanen Systemen erschweren. Anschließend folgt die wissenschaftliche Zielsetzung der Arbeit, die in insgesamt vier einzelne Forschungsfragen unterteilt ist.

1.1 Motivation

In der Hoffnung auf verbesserte Lebensverhältnisse zieht es weltweit viele Menschen in die Städte. Aktuell lebt mehr als die Hälfte der Weltbevölkerung in Städten. Für das Jahr 2050 gehen Schätzungen davon aus, dass über 67 % aller Menschen in Städten leben werden [1]. In vielen Städten kann eine starke Urbanisierung zu einer Verschlechterung der Lebensqualität führen. Beispielsweise kann es durch eine Zunahme des motorisierten Individualverkehrs zu steigenden Schadstoffbelastungen kommen, bei einer gleichzeitigen Abnahme der urbanen Mobilität [2].

Viele Städte setzen auf innovative Informations- und Kommunikationstechnologien (IKT), um urbane Herausforderungen zu bewältigen. Mit Hilfe innovativer Technologien sollten intelligente Städte (engl. Smart Cities) entstehen, die negative Auswirkungen einer starken Urbanisierung auf Bürger, natürlichen Ökosysteme und städtische Infrastrukturen analysieren und Maßnahmen zur Verbesserung der urbanen Lebensqualität zu ergreifen [3].

In vielen Städten hat ein zunehmender Technologieeinsatz nicht zu verbesserten Lebensqualitäten geführt. Die genutzten konventionellen Internet of Things (IoT) Architekturen sind in ihrem Anwendungsspektrum stark limitiert, kaum konfigurierbar und nutzen ausschließlich Daten dedizierter Sensormodule. Ein Mangel an innovativen Sensormodulen und Möglichkeiten zur verlässlichen Vernetzung führen zu einer ineffizienten Nutzung verfügbarer Ressourcen. Beispielsweise werden zur kontinuierlichen Überwachung der urbanen Luftqualität ausschließlich Schadstoffkonzentrationen einiger stationärer Messstationen genutzt. Konventionelle IoT-Geräte bzw. Sensormodule ignorieren Änderungen lokaler Verkehrsverhältnisse oder meteorologischer Umgebungsbedingungen. Flexible und modulare Sensormodule sind erforderlich, um komplexe und vielschichtige Herausforderungen einer hohen Schadstoffbelastungen zu bewältigen.

Neben der Entwicklung intelligenter Sensormodule sind vor allem Möglichkeiten der Vernetzung von enormer Bedeutung. Ein Ziel vieler Smart Cities Initiativen ist es bestehende Grenzen zwischen isolierten Systemen und statischen Anwendungsszenarien aufzubrechen, um komplexe urbane Herausforderungen nicht länger isoliert zu betrachten. Viele Städte haben zusammen mit privaten Unternehmen Cloud-Plattformen aufgebaut, um Kollaborationen bzw. einen verstärkten Datenaustausch zwischen Systemen zu fördern. Obwohl viele kommerzielle Cloud-Plattformen eine Reihe nützlicher Technologien bereitstellen und Daten verschiedenster urbanere Systeme fusionieren, führt ihre Nutzung häufig zu einem Kontrollverlust und Sicherheitsbedenken. Eigentumsrechte der Unternehmen an den verwendeten Technologien und Methoden der Datenanalyse werden selten weitergegeben und erschweren eine transparente Kontrolle der Datennutzung. Dateneigentümern ist nicht klar, wer wie häufig auf ihre Daten zugreift. Darüber hinaus verfügen zentral verwaltete Plattformen über eine geringe Fehlertoleranz und Ausfallsicherheit. Eine mögliche Monopolisierung eingesetzter Technologien durch private Unternehmen, limitiert zudem einen Wissenstransfer an städtische Behörden, Bürgern oder andere Akteure außerhalb des Unternehmens [4].

Die Speicherung und Verwaltung von sensiblen Daten, wie digitale Identitäten und Zugriffsrechten durch einzelne Plattformbetreiber erschwert systemübergreifende Kollaboration zwischen intelligenten Geräten. Beispielsweise lassen sich

digitale Identitäten und Zugriffsrechte kaum von einer auf eine andere Plattformen übertragen. Solchen Identitätsisolierungen führen dazu, dass Reputation von Identitäten sich nicht über verschiedene Plattformen oder Systeme hinweg verfolgt lassen. Digitale Identitäten und Reputationen sind jedoch von enormer Bedeutung für Kollaborationen zwischen Geräten bzw. Entitäten [5]. Bestehende Methoden zur Verwaltung von Identitäten und Zugriffsrechten lassen sich aufgrund spezifischer IoT-Merkmale nicht direkt zur Vernetzung urbaner Systeme nutzen [6]. Entitäten fehlt es für Kollaborationen über Systemgrenzen hinweg, an Möglichkeiten einer verlässlichen Identifikation, Authentifikation und Autorisierung ihrer Datenströme.

Neben diesen technischen Herausforderungen zur Kollaboration zwischen Entitäten, gilt es noch wirtschaftliche Herausforderungen zu überwinden. Vor allem die Gestaltung von Anreizmechanismen zur Förderung von kollaborativen, datenbasierten Geschäftsmodellen ist mit wirtschaftlichen Herausforderungen verbunden. Monetarisierungmodelle können für Dateneigentümer Anreize schaffen, mit anderen Entitäten zu kollaborieren bzw. ihre Daten mit anderen zu teilen. Hohe Gebühren bestehender Zahlungsdienstleister erschweren jedoch die Schaffung monetärer Anreize durch eine Monetarisierung von IoT Daten. Beliebte Dienstleister, wie beispielsweise VISA, berechnen ihren Kunden für digitale Zahlungen eine Mindesttransaktionsgebühr von 0,1 bis 0,21 $ [7]. Die Gebühren kommerzieller Dienstleister übersteigen damit den Wert vieler im IoT verfügbarer Daten und machen Kleinstzahlungen unattraktiv. Ein effizientes Zahlungssystem zur Förderung von kollaborativen Geschäftsmodellen im IoT ist erforderlich, um einen Datentransfer rentabel und damit für viele Dateneigentümer interessant zu machen [8].

1.2 Zielsetzung

Das Ziel dieser Arbeit ist es, Kollaborationen zwischen intelligenten Sensormodulen zu ermöglichen. Hierzu sollen im Rahmen dieser Dissertation Voraussetzungen geschaffen werden, Daten intelligenter Sensormodule eigenständig zu

generieren, zu verwalten und zu monetarisieren. Am Beispiel eines Datenhandels zwischen einem intelligenten Sensormodul und einem Fahrzeug soll demonstriert werden, wie sich Städte an zukünftige technische Anforderungen vernetzter Systeme und kollaborativer Geschäftsmodelle anpassen lassen.

Urbane Systeme unterliegen stetigen Anpassungen aufgrund sich kontinuierlich verändernder Anforderungen. Intelligente Sensormodule zeichnen sich dadurch aus, dass sie sich neuen Anforderungen dynamisch anpassen und innovative Anwendungen fördern. Umweltsensitive Verkehrssteuerungen gehören zu solchen innovativen Anwendungen, die Messwerte der Bereiche Verkehr und Umwelt benötigen, um den urbanen Verkehr nachhaltig zu regulieren. Hinsichtlich der Entwicklung eines intelligenten Sensormoduls, befasst sich diese Arbeit mit der folgenden Fragestellung;

- Wie können lokale Aktivitäten aus den Bereichen Verkehr und Umwelt mit Hilfe eines intelligenten Sensormoduls simultan bestimmt werden?

In vielen Städten werden zwar Messungen urbaner Aktivitäten dezentral mit Hilfe von verteilten Sensormodulen gesammelt, jedoch in Cloud Plattformen zentral verwaltet. Diese zentralisierte Datenverarbeitung führt zu einer Vielzahl an Herausforderungen und limitiert Kollaborationen zwischen Modulen bzw. Dateneigentümern. Bestehende IoT Architekturen ermöglichen es Dateneigentümern weder ihre eigenen Daten vollständig zu kontrollieren noch zu verwalten. Damit sich Daten direkt zwischen Sensormodulen und Systemen teilen lassen, sind dezentrale verwaltete Systeme erforderlich. Distributed Ledger Technologien (DLTs) lassen sich zum Aufbau dezentral verwalteter Systeme nutzen [9]. Der Wechsel von konventionellen Systemen hin zu DLT-basierten Infrastrukturen reduziert Sicherheitsrisiken und ermöglicht Dateneigentümer eine sichere Datenspeicherung und Datenkontrolle. Obwohl DTLs bereits in vielen Forschungsarbeiten zur sicheren Datenspeicherung genutzt wurden, stellt die Integration von IoT Sensormodulen in eine DLT basierte Infrastruktur noch eine große Herausforderung dar. Sensormodule verfügen lediglich über stark limitierte Ressourcen und sind kaum in der Lage, sich an Konsensmechanismen vieler DLTs zu beteiligen. Im Rahmen dieser Arbeit soll der Fragestellung nachgegangen werden;

- Lassen sich die Vorteile einer DLT basierter Infrastrukturen, mit denen ressourcen-limitierter Sensormodule kombinieren?

Unabhängig von der Verfügbarkeit fehlertoleranter und dezentraler Systeme zur sicheren Datenspeicherung, finden Kollaborationen zwischen Sensormodulen und Systemen häufig nicht statt, zumal es an verlässlichen digitalen Identitäten fehlt. Ohne digitale Identitäten können Module nicht mit anderen Entitäten kommunizieren, was zu nicht vertrauenswürdigen Umgebungen führt und Kollaborationen erschwert. Infolgedessen gibt es ein starkes Interesse an Konzepten einer verlässlichen Identifikation, Authentifizierung und Autorisierung von Entitäten in dezentral verwalteten Netzwerken. Somit lautet die dritte Forschungsfrage dieser Arbeit;

- Wie lassen sich in Infrastrukturen ohne zentralisierte Autoritäten, IoT Datenströme verlässlich mit anderen Entitäten teilen?

Neben technischen Herausforderungen muss noch eine wirtschaftliche Herausforderung berücksichtigt werden, um freiwillige Kollaborationen zwischen Entitäten zu fördern.

Eine wirtschaftliche Herausforderung, die zur freiwilligen Kollaboration zwischen Entitäten bewältigt werden muss, bezieht sich auf die Gestaltung von Anreizmechanismen. In bisherigen Forschungsarbeiten [10, 9] wird die Schaffung eines monetären Anreizmechanismus empfohlen, durch den Dateneigentümer für das Teilen ihrer Daten von Datenkonsumenten vergütet werden. Im IoT liegt der Wert vieler Daten weit unterhalb der hohen Transaktionsgebühren kommerzieller Zahlungsdienstleister und den Betriebskosten vieler DLT basierter Infrastrukturen. In Anbetracht des Wertschöpfungspotenzials, das sich aus einem rentablen IoT Datenhandel ergibt, wird die Fragestellung untersucht;

- Ist es möglich geringe Datenmengen im IoT zu monetarisieren, um Kollaborationen zwischen unterschiedlichen Entitäten zu fördern?

1.3 Gliederung

Die vorliegende Arbeit ist in insgesamt acht Kapitel untergliedert. Nach einer Einleitung im ersten Kapitel, werden die für das Verständnis dieser Arbeit notwendigen Grundlagen im zweiten Kapitel vorgestellt. Dabei stehen vor allem Grundlagen aus den Bereichen des Internet of Things (IoT), der Künstlichen Intelligenz (KI) und der Distributed Ledger Technologien (DLTs) im Vordergrund. Das dritte Kapitel dieser Arbeit befasst sich mit dem Stand der Wissenschaft und Technik und stellt aktuelle Forschungsergebnisse aus den Bereichen der urbanen Sensorik, der Datenverwaltung in dezentralen Netzwerken und der Datenmonetarisierung vor. Im vierten Kapitel wird der Smart City Node präsentiert, ein intelligentes Sensormodul zu lokalen Erfassung diverser urbaner Messwerte. Anhand einer Evaluierung eines DLT basierten Sensornetzwerks zur Überwachung der urbanen Luftqualität, wird im fünften Kapitel der Frage nachgegangen, ob sich verteilte Sensormodule in einem DLT basierten Netzwerk effizient nutzen lassen. Das sechste Kapitel befasst sich mit dem eigenständigen Verwalten von Datenströmen und der hierzu notwendigen Identifikation, Authentifikation und Autorisierung von Entitäten. Die Monetarisierung von IoT Daten ist Gegenstand des siebten Kapitels. Anhand eines implementierten Datenhandels zwischen dem Smart City Node und einem Fahrzeug wird evaluiert, zu welchen Bedingungen sich Daten im IoT monetarisieren lassen. Die Arbeit endet im letzten Kapitel mit der Zusammenfassung der Ergebnisse und einem Ausblick auf weitere Fragestellung.

2 Grundlagen

In vielen Städten lassen sich bestehende Herausforderung, wie beispielsweise eine hohe Schadstoffbelastung, ohne den Einsatz neuartiger Technologien nicht erfolgreich bewältigen. Eine moderne Stadt benötigt fortschrittliche Technologien, um eine effiziente und optimale Nutzung verfügbarer Ressourcen zu gewährleisten.

Ein in diesem Kontext häufig mit vielen Erwartungen versehenes Stadtentwicklungskonzept wird in der Literatur mit dem Begriff Smart City beschrieben. Laut dem Europäischen Parlament ist eine Smart City eine Stadt, die Herausforderungen mit Hilfe von Informations- und Kommunikationstechnologien (IKT) bewältigen möchte [11]. Gemäß einer weiteren Definition von Batty et al. [12], ist eine Smart City definiert durch die Integration neuartiger Technologien in traditionelle Infrastrukturen. Basierend auf einer kontinuierlichen Integration, besteht eine Smart City aus hochgradig vernetzten Subsystemen, die Bürgern einen Echtzeitzugang zu unterschiedlichen Informationen und Dienstleistungen ermöglicht. Die Intelligenz einer Smart City kann anhand der Vernetzung diverser Subsysteme bewertet werden. Die Kategorisierung einer Stadt in einzelne Subsysteme ermöglicht es, die Komplexität einer Stadt besser analysieren und kontrollieren zu können [13]. Ein häufig zur Kategorisierung genutzter Ansatz [14], unterteilt Städte in insgesamt sechs Subsystemen; Smart Economy (Wettbewerbfähigkeit); Smart Environment (Erhaltung natürlicher Ressourcen), Smart Governance (Partizipation), Smart Living (Lebensqualität), Smart Mobility (Mobilität) und Smart People (Humankapital).

Für die Entwicklung einer intelligenten Stadt sind von diesen sechs Subsysteme, vor allem Smart Environment und Smart Mobility, von großer Bedeutung. Beide Subsysteme profitieren besonders vom Einsatz neuartiger Technologien [15] und

lassen sich sehr gut zur zum Schutz der Lebensqualität nutzen [16]. Wie sich der Einsatz neuartiger Technologie, wie beispielsweise dem Internet der Dinge (IoT), der künstliche Intelligenz (KI) oder auch der Distributed Ledger Technologie (DLT) zum Aufbau einer Smart City nutzen lassen, wird in den folgenden Abschnitten erläutert.

2.1 Internet der Dinge

Das Internet der Dinge (IoT) beschreibt Infrastrukturen die es ermöglichen, physische und virtuelle Objekte miteinander zu vernetzen und sie durch Informations- und Kommunikationstechniken kollaborieren zu lassen. In vielen Städten werden verteilte IoT-Geräte genutzt, um drahtlose Sensornetzwerke (Wireless Sensor Network, WSN) aufzubauen. Diese aus vielen verteilten Sensormodulen bestehenden Netzwerke sammeln beispielsweise Parameter der Luftqualität und leiten diese zur Überwachung von Schadstoffgrenzwerten an andere Systeme weiter.

Die Vernetzung urbaner Subsysteme zu einer intelligenten Stadt wird aktuell durch eine Reihe von Herausforderungen bestehender IoT-Implementierungen limitiert. Zu diesen Herausforderungen zählen beispielsweise eine effiziente und sichere Datenverarbeitung, dessen erfolgreiche Bewältigung durch die folgenden Merkmale vieler IoT-Implementierungen erschwert wird:

- Datenmengen (M1): Eine stetige Zunahme an Geräte und Systemen führt zu einer ebenfalls kontinuierlich zunehmenden Datenmenge [17].
- Ressourcenbeschränkungen (M2): Die Verarbeitungsleistung vieler IoT-Geräte ist stark limitiert. Die Ausführung komplexer Algorithmen ist für viele Geräte nicht möglich [18].
- Mobilität (M3): Kompakte und energieautarke IoT Geräte lassen sich mobil an unterschiedlichen Standorten nutzen [3]

- Heterogenität (M4): IoT-Systeme bestehen aus diversen Gerätetypen unterschiedlicher Hardware und Software, sowie unterschiedlichen Kommunikationsprotokollen [19].
- Dynamik (M5): IoT-Geräte reagieren auf dynamische Veränderungen der Umgebung, was zu einem dynamischen Datentransfer führt [20].
- Ubiquität der Dienste (M6): Spezifische Anforderungen der Servicequalität (engl., Quality of Service, QoS) sollen durch die Nutzung heterogener Netzwerke und Geräten nicht negativ beeinträchtigt werden [21].

IoT-Implementierungen basieren auf mehrschichtigen Architektur (vgl., Abbildung 2.1), um Heterogenitäten zwischen IoT-Geräten und Netzwerken aufzulösen und eine Suche nach Diensten oder Daten zu erleichtern.

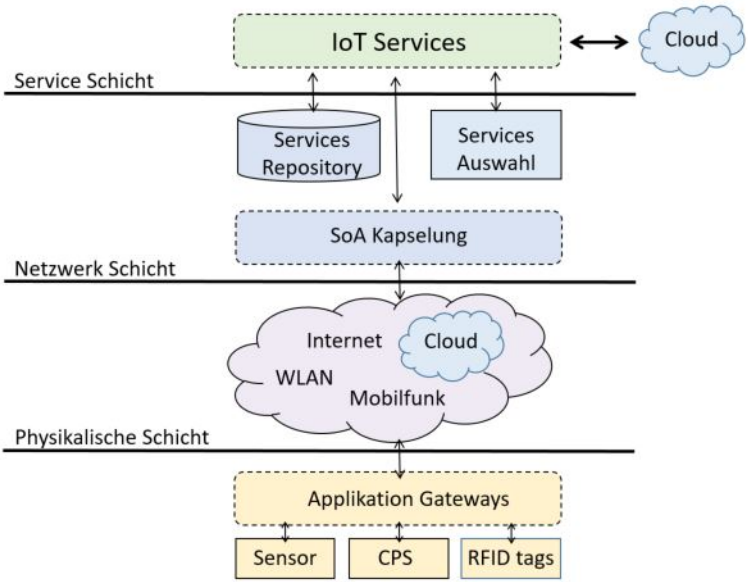

Abbildung 2.1: SoA basierte IoT Architektur [22]

Im IoT tragen vor allem service-orientierte Architekturen (engl., Service-Oriented Architectures, SOAs) dazu bei, ein hohes Maß an Interoperabilität zu gewährleisten. SOAs ermöglichen die Sammlung, Kommunikation und Interaktion zwischen Diensten bzw. Anwendungen, unter Berücksichtigung spezifischer Bedürfnisse und Anforderungen [23]. Im IoT können SOAs in die drei Schichten unterteilt werden; die Physikalische, Netzwerk und Anwendungsschicht (vgl. Abbildung 2.1) [24].

Die erste Physikalische Schicht weist viele Merkmale eines IoT Systems auf. Zumal diese Schicht aus heterogenen Geräten (M4) besteht und in der Regel nur über begrenzte Ressourcen (M2) verfügt. Eine große Anzahl an Geräten führt zu einer großen Datenmenge (M1), die je nach Funktion und Anforderung zu unterschiedlichen Zeitpunkten dynamisch erhoben werden (M5). Zudem können IoT-Geräte ein hohes Maß an Mobilität aufweisen (M3). Hinsichtlich der zweiten Netzwerkschicht können IoT-Geräten über heterogene Netzwerke (M4) miteinander kommunizieren. Heterogenitäten zwischen Netzwerken können durch eine Reihe von Faktoren, wie beispielsweise eine stark limitierte Bandbreite, zu hohen Übertragungsverzögerungen führen und somit die QoS von IoT-Dienste beeinflussen (M6). Zusätzlich kann eine limitierte Ressourcenverfügbarkeit vieler IoT-Geräte (M2) zu Verzögerungen der Datenübertragung führen, wodurch sich die QoS eines Dienstes verschlechtern kann. Merkmale der Heterogenität (M3) und Datenmenge (M1) stellen vor allem die oberste Anwendungsschicht vor enorme Herausforderungen (siehe Tabelle 2.1).

Tabelle 2.1: IoT-Merkmale unterschiedlicher SOA Schichten. Darstellung in Anlehnung an [22].

	IoT Merkmale					
SOA Schicht	**M1**	**M2**	**M3**	**M4**	**M5**	**M6**
Physikalische	X	X	X	X	X	
Netzwerk		X		X		X
Anwendung	X		X			

Im IoT werden vorwiegend Sensordaten erhoben und verarbeitet, so auch im Umwelt und Verkehrswesen. Vor allem zur Sicherstellung einer hohen Luftqualität sind Messungen lokaler Schadstoffbelastungen von enormer Bedeutung. Viele Städte versuchen Gesundheitsrisiken und Schäden durch hohe Luftverschmutzungen, durch ein effizientes Luftqualitätsmanagement (engl., Air Quality Management, AQM) zu minimieren. Zum Luftqualitätsmanagement gehört die kontinuierliche Überwachung diverser Schadstoffkonzentrationen. Mit Hilfe unterschiedliche Messsysteme sollen Bürger vor zu hohen Schadstoffkonzentrationen gewarnt und Ursachen einer schlechten Luftqualität analysiert werden [25].

In den letzten Jahren wurden beträchtliche Summen in die stationäre Schadstoffüberwachung investiert. Die von stationären Systemen stammenden Messungen, dienen primär der Überprüfung gesetzlicher Schadstoffgrenzwerte. Gemäß den von der Europäischen Union (EU) bestimmten Richtlinien zum Schutz der Menschen und Umwelt vor zu hohen Schadstoffbelastungen, darf beispielsweise der Grenzwert von 50 Mikrogramm Feinstaub (PM10) pro Kubikmeter Luft nicht mehr als an 35 Tagen pro Jahr überschritten werden [26]. Zur Überwachung der Grenzwerte nutzen stationäre Systeme hochwertige Analyseinstrumente, wie beispielsweise Massenspektrometer und Gaschromaten, um zuverlässig ein breites Spektrum unterschiedlicher Schadstoffe zu analysieren bzw. zu überwachen. Die Anschaffung, Wartung und der Betrieb solch hochwertiger Analyseinstrumente, verursachen hohe Kosten. Daher liefern Netzwerke aus stationären Messstationen sehr präzise Schadstoffkonzentrationen einer sehr geringen räumlichen Messauflösung.

Schadstoffkonzentration sind stark standortabhängig. Unterschiedliche Topologien, Vegetations- und Verkehrsverhältnisse führen bereits innerhalb weniger Meter zu starken Unterschieden der Schadstoffkonzentration. Mobile Messsysteme werden eingesetzt, um die Schadstoffkonzentration an unterschiedlichen Standorten zu bestimmen. Fahrzeuge, öffentliche Verkehrsmittel, Fahrräder oder Fußgänger werden von solchen mobilen Messsystemen als Transportmedium genutzt, um Schadstoffmessungen an diversen Orten durchzuführen [27]. Welche Analyseinstrumente in mobilen Messsystemen zum Einsatz kommen, wird stark von dem

genutztem Transportmedium bestimmt. Beispielsweise sind die Energie- und Größenanforderungen der Analyseinstrumente bei fahrzeugbasierten Systemen weniger restriktiv, als bei anderen Transportmedien. Der Einsatz von hochwertigen Analyseinstrumenten wird durch raue Umgebungsbedingungen, wie beispielsweise starke Vibrationen, und begrenzte Wartungsmöglichkeiten beschränkt. Eine Nutzung hochwertiger Analyseinstrumente ist für viele mobile Systeme kaum möglich. Verglichen mit stationären Messsystemen, ist die Qualität der von mobilen Messsystemen generierten Messungen geringer.

Mobile Systeme bewegen sich kontinuierlich auf definierten Routen durch die Stadt, um Schadstoffkonzentrationen unterschiedlicher Standorte zu jeweils einem bestimmten Zeitpunkt zu bestimmen. Für kontinuierliche Schadstoffmessungen einer hohen räumlichen Auflösung werden portable Systeme genutzt. Verglichen mit stationären und den meisten mobilen Systemen, sind die Kosten für den Aufbau und Betrieb portabler Messsysteme gering, zumal zur Schadstoffmessung kostengünstige Sensoren (engl., Low-cost Sensors, LCS) eingesetzt werden. Der Einsatz kostengünstiger Sensoren führt zu einer geringen Qualität der Messwerte, weshalb portable Sensormodule nicht zur Überwachung gesetzlicher Schadstoffgrenzwerte genutzt werden. Vielmehr werden große Netzwerke aus kostengünstigen Sensormodulen eingesetzt, um Schadstoffkonzentrationsänderungen mit einer hohen räumlichen und zeitlichen Auflösung zu bestimmen (siehe Abbildung 2.2 [28].

Neben einer intakten Umwelt, ist für die Lebensqualität ein hohe Mobilität von großer Bedeutung. Für die Entwicklung effizienter und zugleich umweltfreundlicher Verkehrssystem von entscheidender Bedeutung. Echtzeitdaten zur aktuellen Verkehrssituation sind notwendig, um durch ein intelligentes Verkehrsmanagement aktiv den Verkehrfluss zu steuern bzw. zu optimieren

Die Erhebung von Verkehrsdaten basiert auf verteilten Sensornetzwerken, die aus stationären oder mobilen Systemen bestehen. Stationären Systeme nutzen sogenannte „In-situ Technologien“, die entweder in bestehende Verkehrsinfrastrukturen integriert werden (invasive Sensoren) oder sich in unmittelbarer Straßennähe (nicht-invasive Sensoren) befinden. Zu den typischen invasiven Sensoren

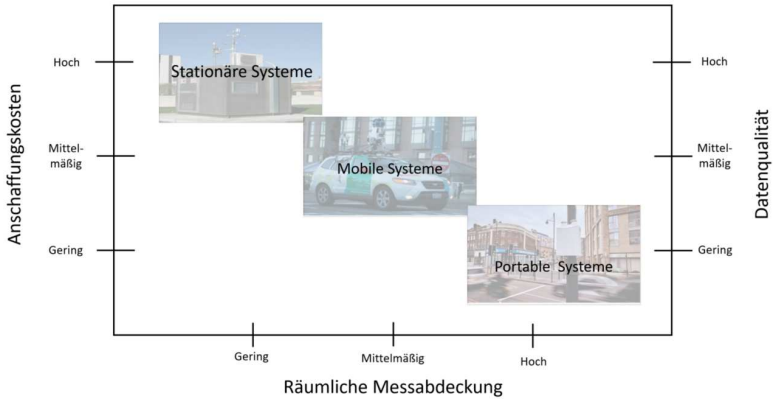

Abbildung 2.2: Vereinfachte Einordnung unterschiedlicher Systeme zur Schadstoffüberwachung. Eigene Darstellung in Anlehnung an [29]

gehören Magnetdetektoren, Schwingungssensoren und Induktionsschleifen. Momentan sind Induktionsschleifen zur Verkehrsüberwachung weit verbreitet. Induktionsschleife können Fahrzeuge durch Magnetfeldänderung detektieren. Mit Hilfe von sogenannten Doppelschleifen, zwei in einem bestimmten Abstand installierte Induktionsschleifen, ist es ebenfalls möglich die Geschwindigkeit unterschiedlicher Fahrzeuge zu messen. Die Installation und Wartung invasiver Sensoren, ist mit hohen Kosten verbunden, zumal Induktionsschleifen fest in Fahrbahnen installiert werden [30].

Nicht invasiven Sensoren werden oft am Straßenrand angebracht und lassen sich ohne aufwändige Installation zur Verkehrsanalyse nutzen. Zu den nicht invasiven Sensoren zählen beispielsweise akustische LIDAR (engl., light detection and ranging) und optische Sensoren, wie beispielsweise Kameras. Vor allem der Einsatz von Verkehrsüberwachungskameras hat in den letzten Jahren stark an Bedeutung gewonnen, zumal sich aus Bilddaten verschiedenste Informationen zum Verkehr automatisiert gewinnen lassen. Verglichen mit anderen nicht invasiven Sensoren, sind Kameras günstig in der Anschaffung und können flexibel an einer Vielzahl von Standorten installiert werden. Je nach Sichtfeld werden simultan mehrere

Fahrspuren analysiert. Die Genauigkeit einer kamerabasierten Verkehrsüberwachung ist vom verfügbaren Sichtfeld und sich ändernden Umgebungsbedingungen abhängig. Hierzu zählen beispielsweise Änderungen der Witterungsbedingungen oder Belichtung [31]. Zusätzlich muss bei den Auswertungen kamerabasierte Verkehrsdaten auf die Privatsphäre einzelner Verkehrsteilnehmer geachtet werden, zumal Videodaten personenbezogene und sensible Daten, wie beispielsweise Gesichter einzelner Verkehrsteilnehmer, beinhalten können. Die Auswertung solcher Daten unterliegt der Datenschutz-Grundverordnung (DSGVO) und darf damit nicht ohne eine Erlaubnis des Dateneigentümers stattfinden [32].

Obwohl stationäre Sensoren erfolgreich seit Jahren zur Verkehrsüberwachung eingesetzt werden, beziehen sich die aus diesen Sensornetzwerken stammende Daten oft nur auf einen sehr begrenzten Verkehrsraum, zumal Installations- und Wartungskosten einem flächendeckenden Einsatz entgegenstehen. In den letzten Jahren wurde an der Integration der in Ad-hoc Fahrzeugnetzen (engl., Vehicular Ad Hoc Network, VANET) generierten Daten in Verkehrsüberwachungssysteme gearbeitet, um Verkehrssituation zeitnah und großflächig zu erfassen [33]. Dabei agieren Verkehrsteilnehmer als mobile Sensoren, die sich einander über selbstorganisierte VANETs mit Verkehrsinformationen versorgen. Bei VANETs handelt es sich um eine spezielle Ausprägung dezentralisierter Netzwerke, dessen Netzwerkknoten aus Fahrzeugen und straßennahen Infrastruktureinheiten (engl. roadside units, RSUs) bestehen. Unterschiedliche Netzwerkknoten können sich ohne feste Infrastruktur oder übergeordneten Netzwerkknoten spontan zu selbstorganisierenden Netzwerken unterschiedlicher Topologie zusammenschließen. Innerhalb einer bestimmten Funkreichweite können Daten via Funkverbindungen unter Netzwerkknoten als auch mit externen Netzwerken, wie beispielsweise dem Internet, ausgetauscht werden. Innerhalb eines VANETs können Daten zwischen Netzwerkknoten entweder im sogenannten Single-Hop oder Multi-Hop Kommunikationsmodus übertragen werden. Bei der Single-Hop Datenübertragen werden die Daten direkt von einem Netzwerkknoten (Sender) an andere Netzwerkknoten (Empfänger) gesendet, wohingegen bei der Multi-Hop Datenübertragung, die Daten vom einzelnen Netzwerkknoten (Sender) über mehrere, intermediäre Netzwerkknoten (hops) hinweg weitergeleitet werden. Je nachdem über wie viele

Netzwerkknoten die Daten weitergeleitet werden, ergibt sich eine Reichweite der Datenübertragung, die nicht mehr durch die Funkreichweite einzelner Netzwerkknoten (Sender) begrenzt ist [34].

In spontan entstehenden und sich selbstorganisierten VANETs, ohne feste Netzwerkinfrastruktur, kommt der Kommunikation (Funkübertragung) zwischen den einzelnen Netzwerkknoten eine besondere Rolle hinzu. Seit vielen Jahren wird von der IEEE (Institute of Electrical and Electronics Engineers) an der Optimierung und Standardisierung der Funkübertragung in VANETs gearbeitet. Spezifikationen der physischen Übertragungsschichten des ISO/OSI Referenzmodells sind unter dem Namen Dedicated Short Range Communication (DSRC) bekannt und nutzen zur drahtlosen Datenübertragung das Frequenzband von 5,850 bis 5,925 gHz. Dieses Frequenzband wurde von der IEEE durch das 802.11p-Protokoll in sieben Kommunikationskanäle unterteilt. Von diesen sieben verfügbaren Kommunikationskanälen, dient ein Kanal einem sicherheitsrelevanten und sechs Kanäle, einem nicht sicherheitsrelevanten bzw. allgemeinen Datenaustausch [35].

2.2 Künstliche Intelligenz

Das IoT ist zu einem bedeutsamen Bestandteil vieler Smart-City-Anwendungen geworden. Durch die Installation von Sensormodulen in den verschiedensten Bereichen, wie beispielsweise dem Umweltmonitoring, werden täglich immense Datenmengen generiert. Eine effiziente Verarbeitung der heterogenen und großen Datenmengen, ist mit diversen Herausforderungen verbunden und bedarf effizienter Methoden der Datenverarbeitung. Fortschrittliche Methoden aus dem Bereich der Künstlichen Intelligenz (KI) ermöglichen eine effiziente Analyse große Datenmengen. Eine wachsende Datenmengen diverser Sensornetzwerke kann zudem die Genauigkeit vieler KI basierter Auswertungen verbessern. KI basierte Analysemethoden sind zur intelligenten und präventiven Steuerung urbaner Aktivitäten erforderlich [36]. Beispielsweise können KI basierte Analysemethoden genutzt werden, um komplexe und mehrschichtige Verkehrsprobleme effizient zu lösen.

Die Menge an Verkehrsdaten nimmt aufgrund einer zunehmende Anzahl vernetzter Fahrzeuge und drahtloser Sensornetzwerke kontinuierlich zu. Dieses rasche Wachstum an Daten ist für viele bestehende Verkehrsmanagementsysteme zu einer großen Herausforderung geworden. Herkömmliche Systeme sind kaum in der Lage, den Anforderungen einer zur echtzeitfähigen Verkehrssteuerung erforderlichen Datenanalyse gerecht zu werden. Im Verkehrswesen sind die Einsatzmöglichkeiten KI-basierter Methoden vielfältig und reichen von einer Verkehrsanalyse hin zur Optimierung von Lichtsignalanlagen. Vor allem Deep Neural Netze (DNN), rekurrente neuronale Netze (RNN), neuronale Faltungsnetze (CNN) und Tiefes Q-Netz (DQN) werden häufig genutzt (siehe Abbildung 2.3) [37].

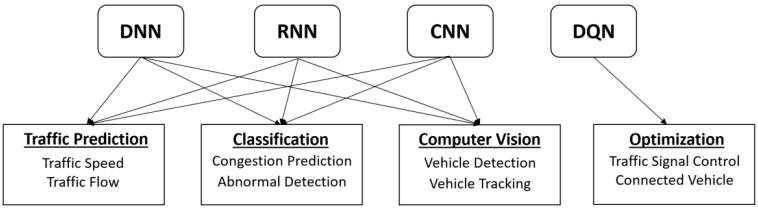

Abbildung 2.3: KI Anwendungsbeispiele im Bereich der Mobilität [37]

Vor allem die automatisierte Erkennung und Verfolgung von Objekten, wie beispielsweise Fahrzeugen, hat in den letzten Jahren sehr stark von Entwicklungen CNN-basierter Methoden profitiert. Intelligenten Verkehrsleitsystemen ist es bereits möglich Verkehrsinformationen direkt aus Videodaten zu extrahieren. Hierzu sind im Wesentlichen drei Prozessschritte notwendig; (i) die Objekterkennung und -verfolgung um Objektinformationen zu extrahieren [38], (ii) die Verkehrsanalyse um den Verkehrszustand zu bestimmen [39] und (iii) die anschließende Verkehrsteuerung zur Optimierung des Verkehrsflusses [40].

Die Verkehrsanalyse basierend auf Verkehrsvideos umfasst Aufgaben der automatischen Erkennung, Verfolgung und Re-Identifikation unterschiedlicher Verkehrsteilnehmer [41]. Verkehrsanalysen nutzen Multiple Object Tracking (MOT) Methoden, mit denen sich Trajektorien mehrerer bewegter Verkehrsteilnehmer in

Videosequenzen automatisch erfassen lassen. Diese Methoden folgen einem sogenannten Tracking-by-Detection-Paradigma und lassen sich in eine Erkennungs- und eine Trackingphase unterteilen. Die erste Erkennungsphase nutzt Objektdetektoren, um Objekte in einzelnen Bildern zu lokalisieren und zu klassifizieren. In einer folgenden Trackingphase werden anschließend die Trajektorien erfolgreich detektierter Objekte bestimmt (vgl. Abbildung 2.4).

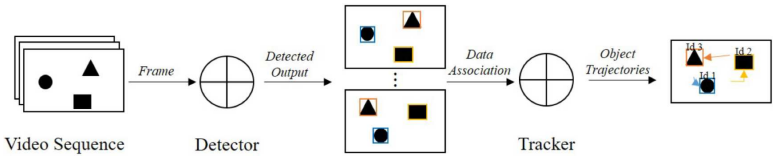

Abbildung 2.4: Skizze zur Veranschaulichung des Tracking by Detection Paradigmas [37]

KI-basierte Modelle erzielen vor allem große Erfolge bei der Extraktion von Merkmalen und der Klassifizierung von Objekttypen. Prinzipiell lassen sich Objekterkennungsmethoden in einstufige und zweistufige Methoden unterteilen. Einstufige Methoden, wie beispielsweise You Only Look Once (Yolo) [42] oder Single Shot Detection (SSD) [43], führen Erkennungen direkt durch und erzielen hohe Erkennungsgeschwindigkeit. Zweistufige Methoden detektieren zunächst Regionen, in denen sich Objekt befinden können und detektieren anschließend Objekte. Verglichen mit einstufigen Methoden erzielen zweistufige Methoden, wie beispielsweise Fast R-CNN, eine höhere Genauigkeit bei einer geringeren Erkennungsgeschwindigkeit.

Nach der Objekterkennung folgt die Objektverfolgung. Die hierzu genutzten Tracking-Methoden lassen sich in Single Object Tracking (SOT) und Multiple Object Tracking (MOT) unterscheiden. SOT basierte Methoden der Objektverfolgung benötigen keine Objekterkennung, da diese Methoden ein bestimmtes Objekt von Anfang an verfolgen. Bekannte SOT Methoden sind Kalman-Filter [44] und Partikelfilter [45]. MOT Methoden hingegen folgen dem Paradigma des Tracking-by-Detection, bei dem die Tracking-Methoden in jedem Frame auf die resultierende Ausgabe der Objekterkennung reagieren. Zu einer bekannten MOT Methoden gehören derzeit DeepSORT, eine Erweiterung des SORT-Algorithmus.

Ein wichtigster Bestandteil eines Verkehrsmanagements ist die Fahrzeugzählung. Nachdem erfolgreich Erkennungs- und Verfolgungsprozesse ausgeführt wurden, um Fahrzeuge zu erkennen und zu überwachen, wird eine virtuelle Linie für Zählungen von Fahrzeugen festgelegt. Passiert ein detektiertes Fahrzeuge eine solche Linie, wird das Fahrzeug gezählt. Dieses Konzept ist sowohl für die Personen- als auch für Fahrzeugzählung weit verbreitet [46, 47].

2.3 Distributed Ledger Technologien

Distributed Ledger Technologien (engl., Technik verteilter Kassenbücher, DLTs) haben in den letzten Jahren eine Vielzahl neuartiger Anwendungen ermöglicht. Vor allem Bereiche des *Datenzugriffsmanagements, Reputationsmanagement und digitaler Bezahlvorgänge* haben vom Einsatz moderner DLT profitieren.

DLTs ermöglichen den Aufbau digitaler Infrastrukturen durch den Betrieb von hochverfügbaren Datenbanken (Distributed Ledger), die von physisch verteilten Speicher- und Rechengeräten (DLT-Knoten), in einer nicht vertrauenswürdigen Umgebung verwaltet werden [48]. Nicht vertrauenswürdige Umgebungen sind gekennzeichnet durch betrügerisches Verhalten einzelner DLT-Knoten, wie beispielsweise der Ausgabe falscher Informationen [49]. Im Allgemeinen speichern und verwalten DLT-Knoten eine lokale Kopie aller Daten eines Distributed Ledgers. Neue Daten werden in Form von Transaktionen den lokal gespeicherten Kopien des Distributed Ledgers hinzugefügt. Sobald DLT-Knoten neue Transaktionen erhalten, validieren DLT-Knoten diese anhand von digitalen Signaturen anderer DLT-Knoten. Gültige Transaktionen werden von DLT-Knoten gespeichert und an weitere DLT-Knoten im Distributed Ledger weitergeleitet. Nachdem andere DLT-Knoten neue Transaktionen ebenfalls validiert haben, werden die Transaktionen im Distributed Ledger gespeichert [50].

Umfangreiche und schnelle Entwicklung im Bereich der DLT haben zu zahlreiche Distributed Ledger Varianten geführt, die zumindest umgangssprachlich gerne als

Blockchain bezeichnet werden, sich aber stark von den Eigenschaften einer Blockchain unterscheiden. Distributed Ledger lassen sich gemäß ihres Konzeptes, Designs, ihrer Eigenschaften und Merkmalen differenzieren [51] (vgl. Abbildung 2.5). DLT Konzepte beschreiben die Validierung und Speicherung von Transaktionen. Zu den bekanntesten DLT Konzepten gehören Blockchains [52], blockgerichtete azyklische Graphen (blockDAG) [53] und transaktionsbasierte gerichtete azyklische Graphen (TDAG)[54]. Blockchains gehören beispielsweise zu DLT Konzepten, in denen Transaktionen in Form von Blöcken gespeichert werden, die kryptografisch mit vorherigen Blöcken verbunden eine Kette bilden. Wohingegen in TDAGs überhaupt keine Blöcke gebildet und Transaktionen direkt miteinander verknüpft werden. Zu jedem DLT Konzept gibt es verschiedene Implementierungen, die DLT Designs. Beispielsweise repräsentieren Bitcoin und Ethereum unterschiedliche DLT Designs eines gemeinsamen DLT Konzepts. Während beim Bitcoin DLT Design alle 10 Minuten ein neuer Block mit einer festen Blockgröße von 1 MB erstellt wird, entstehen beim Ethereum DLT Design im Durchschnitt alle 17 Sekunden neue Blöcke einer variablen Blockgröße [50]. DLT Designs können anhand von bestimmten Eigenschaften, wie beispielsweise der Leistungsfähigkeit oder Anonymität, differenziert werden. Diesen Eigenschaften können in unterschiedlichen Ausprägungen vorliegen. So ist für die Leistungsfähigkeit einer Implementierung beispielsweise das Merkmale Transaktionsdurchsatz von enormer Bedeutung [55].

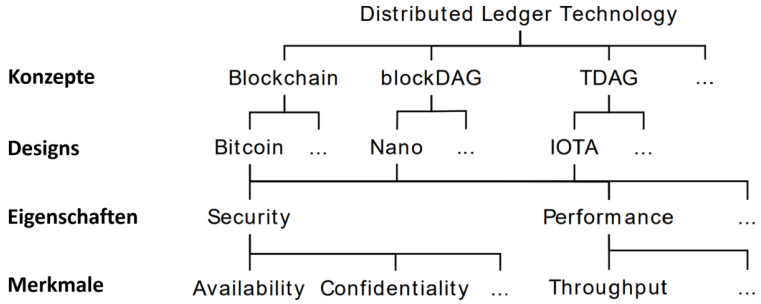

Abbildung 2.5: Terminologie der Distributed Ledger Technologien [51]

DLT-Knoten verfügen über eine lokale Kopie eines Distributed Ledgers, weshalb alle Knoten synchronisieren werden müssen, um einen konsistenten Zustand des Distributed Ledgers zu erzielen. Zur Synchronisierung der verteilten DLT-Knoten werden Konsensmechanismen (engl., consensus mechanism) genutzt, die über individuelle Ausprägungen hinsichtlich ihrer Finalität oder Fehlertoleranz verfügen [56]. Die Finalität eines Konsensmechanismus kann in eine totale und probabilistische Finalität unterteilt werden. Bei Konsensmechanismen die eine totale Finalität anstreben, einigen sich alle DLT-Knoten eines Distributed Ledgers auf einen gemeinsamen Zustand bzw. neu hinzuzufügende Transaktionen. Bei der probabilistischen Finalität hängt jeder DLT-Knoten einzelne gültige Transaktionen an seine lokale Kopie des Distributed Ledger und propagiert seine Aktualisierungen an andere DLT-Knoten. Diese neuen Transaktionen sind noch nicht vom Distributed Ledger validiert und daher solange manipulierbar, bis eine bestimmte Anzahl von aufeinander folgenden älteren Transaktionen (oder Blöcken), an neue Transaktionen hinzugefügt wurden. Die Wahrscheinlichkeit, dass eine aufgenommene Transaktion aus dem Distributed Ledger ausgeschlossen wird, sinkt mit zunehmender Anzahl der angehängten Transaktionen (oder Blöcken). Der Zeitraum zwischen dem Hinzufügen einer Transaktion an den Distributed Ledger und dem Zeitpunkt, an dem die Transaktion mit einer bestimmten Wahrscheinlichkeit validiert ist, wird als Bestätigungslatenz bezeichnet.

Konsensmechanismen erzeugen einen Konsens zwischen allen validierenden DLT-Knoten, auch wenn einige DLT-Knoten vorübergehend nicht verfügbar sind oder böswillig handeln. Hinsichtlich der Fehlertoleranz wird im Wesentlichen zwischen crash- und byzantinisch fehlertoleranten Konsensmechanismen unterschieden. Die Crash-Fehlertoleranz bezieht sich auf die Fähigkeit eines Konsensmechanismus, trotz (vorübergehend) nicht verfügbarer DLT-Knoten einen Konsens zwischen allen verfügbaren DLT-Knoten zu erreichen. Die Verfügbarkeit einzelner DLT-Knoten kann beispielsweise durch Latenzen oder dem Ausfall einzelner Hardwarekomponenten beeinflusst werden. Byzantinische fehlertolerante Konsensmechanismen können zusätzlich mit böswilligem Verhalten einzelner DLT-Knoten umgehen [57]. Die Fehlertoleranz eines Konsensmechanismus beschreibt bis zu welchem Schwellenwert ein Konsensus zwischen DLT-Knoten

noch erzielt werden kann. Byzantinisch fehlertolerant Konsensmechanismen können beispielsweise einen Anteil von bis zu 33% an böswilligen DLT-Knoten [58] tolerieren.

Distributed Ledger unterscheiden sich ebenfalls hinsichtlich ihrer Lese- und Schreibberechtigungen. Es wird unterschieden zwischen; private-permissionless, private-permissioned, public-permissionless oder public-permissioned Distributed Ledgern [59]. Die Begriffe public und private beziehen sich auf die Leseberechtigungen der DLT-Knoten in einem Distributed Ledger. In einem public Distributed Ledger ist die Teilnahme an am Distributed Ledger nicht auf bestimmte DLT-Knoten beschränkt. Es ist keine Registrierung bzw. Autorisierung der DLT-Knoten erforderlich. Wohingegen in einem private Distributed Ledger die Teilnahme ausschließlich bekannten bzw. autorisierten DLT-Knoten möglich ist. Vergleichbar mit Schreibberechtigungen in konventionellen Datenbanken, beziehen sich die Begriffe permissioned und permissionless auf die Berechtigung der DLT-Knoten am Konsensmechanismus teilzunehmen und Transaktionen zu validieren. Public-permissionless Distributed Ledger zeichnen sich durch eine gute Skalierbarkeit aus, zumal eine Vielzahl an DLT Knoten an der Konsensfindung beteiligt ist, wohingegen private-permissioned Distributed Ledger überwiegend für eine vergleichsweise kleine Anzahl an bekannten DLT Knoten konzeptioniert werden und sich durch eine höhere Bestätigungslatenz auszeichnen.

Neben der Speicherung von Transaktionen können Distributed Ledger ebenfalls Smart Contracts ausführen. Ein Smart Contract ist ein Programm, welcher innerhalb einer Transaktion enthalten ist, die auf einem Distributed Ledger gespeichert und dessen korrekte Ausführung durch einen Konsensusmechanismus garantiert wird [60]. Smart Contracts können genutzt werden, um Geschäftsprozesse zu automatisieren. Die Nutzung von Smart Contracts in einem public-permissionless Distributed Ledger wird limitiert durch Kosten, gemessen in sogenannten Gaseinheiten, die für auszuführende Smart Contract Berechnungen aufzubringen sind. Sofern eine Transaktion in einem public-permissionless Distributed Ledger eine Funktion eines Smart-Contract aufruft, führen alle DLT-Knoten den Smart Contract unter Verwendung der angegebenen Daten und Parameter einzeln aus. Die Kosten die aufzubringen sind um einen Smart-Contract auszuführen, sind somit

proportional zu den verbrauchten Ressourcen der DLT-Knoten. Smart Contract können nur solange ausgeführt werden, bis alle auf einer Smart Contract Adresse gespeicherten Gaseinheiten verbraucht sind [61].

In der bekanntesten DLT-Architektur, der Blockchain, werden Transaktionen in Blöcken sequentiell mit den des jeweils vorhandenen Blöcken verknüpft und in bestimmten Zeitintervallen einem Distributed Ledger hinzugefügt. Aufgrund dieser sequentiellen Transaktionsverarbeitung verfügen viele Blockchains über einen geringen Transaktionsdurchsatz. DLT-Konzepte dessen Struktur auf gerichteten azyklischen Graphen (DAGs) basieren, erzielen einen hohen Transaktionsdurchsatz (vgl., Abbildung 2.6) [62]. Der IOTA Tangle repräsentiert ein solches DLT-Konzept, das vor allem für Anwendungen im IoT konzeptioniert wurde [63].

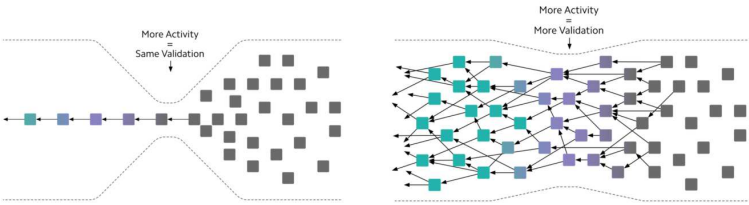

Abbildung 2.6: Validierungsstruktur einer Blockchain und des IOTA Tangles [64]

Transaktionen des IOTA Tangle starten mit einem Seed. Ein Seed besteht aus einer Kombination aus 81 Zeichen der Buchstaben A-Z und der Zahl 9. Die Generierung eines Seeds kann zufällig und ohne eine zentrale Autorität erfolgen. Mit einem Seed lassen sich private Schlüssel und Transaktionsadressen erstellen. Transaktionsaussteller können mit privaten Schlüsseln belegen, dass Sie eine bestimmte Addresse bzw. die dazugehörigen IOTA Token besitzen. Alle Transaktionsadressen werden mit der Kerl-Hash-Algorithmus (Keccak 384) [65] aus einem privaten Schlüssel erzeugt, welcher sich aus einem Seed, einem Addressindex und einer Sicherheitsstufe generieren lässt. Hierzu wird zunächst ein Subseed erstellt, indem der Seed sowie eine Addressenindex mit der Keccak 384 gehasht werden. Dieser Subseed wird anschließend mittels des Hashalgorithmus jeweils 27 Mal je Sicherheitsstufe gehasht. Die Länge des privaten Schlüssels hängt somit

von der gewählten Sicherheitsstufe ab. Anschließend wird der private Schlüssel in mehrere Schlüsselfragmente aufgeteilt, die wiederrum gehasht werden, um sogenannte Digests zu bilden. Digests werden anschließend kombiniert und erneut gehasht, um eine Transaktionsadresse zu generieren [54].

Ist eine Transaktionsadresse erstellt, können auf dieser Adresse Transaktionen gespeichert werden. Hierzu müssen Transaktionsaussteller zwei Kriterien erfüllen: erstens muss jede neue Transaktion zwei im IOTA Tangle speicherte Transaktionen (Tips) bestätigen, zweitens muss jede Transaktion über eine gültige Nonce (Number only use once) verfügen. Im IOTA Tangle wird ein konsistenter Zustand durch gegenseitige Transaktionsbestätigungen bzw. Mehrfachbestätigungen erzielt. Eine Transaktion gilt im IOTA Tangle als bestätigt, sobald von einer einzelnen Transaktion aus Verifizierungspfade zu sämtlichen Tips führen (vgl. Abbildung 2.6). Desto schneller neue Transaktionen an den IOTA Tangle angehängt werden, desto geringer ist die Bestätigungslatenz einzelner Transaktionen. Somit kommt es mit einer steigenden Anzahl neuer Transaktionen zu einer gleichzeitigen Abnahme der Bestätigungslatenz. Jede Transaktion benötigt neben einer Mehrfachbestätigung noch eine gültige Nonce, um eine Transaktion dem IOTA Tangle hinzuzufügen. Eine gültige Nonce wird durch eine Hash-Funktion berechnet, dessen Hash-Wert mit einer vom IOTA-Protokoll definierten Anzahl von Nullen übereinstimmen muss [66]. Sofern der Hash-Wert nicht mit der angestrebten Anzahl von Nullen übereinstimmt, muss der Transaktionsaussteller die Hash-Funktion erneut ausführen, bis er eine gültige Nonce gefunden wurde. Dieser Prozess der gültigen Nonce Berechnung soll den Distributed Ledger vor Spam Angriffen schützen. Da Nonce Berechnungen vom Transaktionsaussteller selbst ausgeführt werden, entstehen im Gegensatz zu anderen public-permissionless Distributed Ledgern keine Gebühren zur Konsensfindung. Somit können Transaktionen auch ohne den Besitz von Kryptowährungen, wie beispielsweise dem Bitcoin, versendet werden.

Zu den größten Schwächen des IOTA Tangle gehört der aktuelle Einsatz eines Koordinators. Dieser veröffentlicht in regelmäßigen Abständen signierte Transaktionen, die sogenannte Meilensteine. Transaktionen im IOTA Tangle sind erst dann gültig, wenn sie der Koordinator direkt oder indirekt durch einen Meilenstein

bestätigt wurden. Der Koordinators setzt zwar Kontrollpunkte (Checkpoints), um vor Angriffen wie etwa dem Double-Spending zu schützen, er hat aber keinen Einfluss auf den Konsensmechanismus und kann beispielsweise keine neuen IOTA Token erschaffen oder bestehende Token entwenden. An der Abschaffung des Koordinators (Coordicide [67]) wird gearbeitet und es befindet sich eine erste vollständig dezentrale Version des IOTA Tangle (IOTA 2.0-DevNet [68]) in der Testphase.

2.3.1 Datenzugriffsmanagement

Im Wesentlichen befasst sich ein Datenzugriffsmanagement mit dem Identifizieren, Authentifizieren und Autorisieren von Entitäten in virtuellen Netzwerken. Eine Identifizierung erfolgt, wenn eine Entität behauptet über bestimmte Identitätsattribute zu Verfügung. Dies kann durch einen Benutzernamen oder sonstige Identifikatoren erfolgen, die eine Entität eindeutig identifizieren. Eine Authentifizierung prüft Berechtigungsnachweise (engl., Credentials), wie beispielsweise ein Passwort einer Identität. Auf Grundlage einer nachgewiesenen Identität werden während einer Autorisierung Zugriffsrechte auf Daten erteilt. Die hierzu genutzten Zugriffsrechte beschreiben, auf welche Daten eine Identität innerhalb eines bestimmen Systems zugreifen kann [69].

Basierend auf der Anzahl und Vielfalt an digitalen Identitäten hat sich das Identitätsmanagement vom isolierten hin zu verteilten Modell entwickelt [70]. Das Isolated User Identity Modell repräsentiert ein einfaches Modell eines Identitätsmanagements, welches alle identitätsbezogenen Daten zentral in einem einzigen System eigenständig verwaltet. Identifikatoren und Credentials sind nur in einem System gültig, weshalb Entitäten oft zahlreiche Teilidentitäten besitzen, um sich in verschiedenen Systemen zu authentifizieren. Aufgrund der Vielzahl an Systemen, die innerhalb einer vernetzten Stadt existieren können, werden zentralisierte Modelle mit der Verwaltung vieler spezifischer Identitäten und Credentials überlastet. Modelle eines verteilen Identitätsmanagements werden genutzt, um das Verwalten von vielen Identitäten zu reduzieren. Verteilte Modelle erlauben es Entitäten

Authentifizierungs- und Autorisierungsfunktionen über Systemgrenzen hinweg zu nutzen. Im Wesentlichen bestehen solche Modelle aus einer Gruppe von Organisationen, die Vertrauensbeziehungen aufgebaut haben, um Informationen über Entitäten auszutauschen. Entitäten müssen sich nur bei einem Identitätsanbieter registrieren, um unterschiedliche Dienstleistungen in diversen Systemen nutzen zu können [71].

Isolierte und verteilte Modelle bestehender Identitätsmanagementsysteme erfordern stets einen Identitätsanbieter. Hierdurch kommt es für Entitäten zu einem Kontrollverlust der eigenen digitalen Identität. Entitäten müssen Identitätsanbieter vertrauen. Entitäten haben keine vollständige Kontrolle darüber, wer im welchen Kontext ihre Daten nutzt. Darüber hinaus sind Entitäten an einzelne Identitätsanbieter gebunden und können ihre digitale Identität nicht selbstständig in andere Systeme übertragen [72].

Basierend auf diesen Nachteilen einer eingeschränkten Kontrolle und Interoperabilität digitaler Identitäten, wurde verstärkt an Modellen eines benutzerzentrierten Identitätsmanagement gearbeitet. In einem benutzerzentrierten Identitätsmanagement steht die von der Entität selbstständig verwaltete digitale Identität im Fokus. Entitäten sollen als einzige Autorität ihre eigenen digitalen Identitäten schaffen, kontrollieren, übertragen, ändern und löschen können. Es sollte der jeweiligen Entität obliegen, durch eine selektive Datenfreigabe selbstbestimmt darüber zu verfügen, wer welche Daten nutzen darf. Ein weiteres Ziel eines benutzerzentrierten Identitätsmanagementsystems besteht in der Reduktion digitaler Identitäten. Anstatt für jedes System oder jede Anwendung eine neue Identität zu erstellen, sollten Entitäten über interoperable sowie transportable Identitäten verfügen, um sich mit einer Identität in verschiedenen Systemen zu authentifizieren [73]. Zu den bekanntesten Wissenschaftlern im Bereich benutzerzentrierten Identitätsmanagementmodelle gehört Christopher Allen. Auf ihn sind die folgenden zehn Prinzipien zurückzuführen, anhand derer sich selbst-verwaltete und benutzerzentrierten digitale Identitäten (engl., Self Sovereign Identities, SSIs) definieren lassen [74].

- Kontrolle: Entitäten müssen immer in der Lage sein ihre Identitäten zu kontrollieren, sie zu nutzen, zu aktualisieren oder zu verbergen.

- Zugriff: Entitäten sollten direkten Zugriff auf ihre eigene Identität und alle zugehörigen Daten haben.
- Transparenz: Entitäten sollte es möglich sein zu verstehen, wie Identitäten verwaltet werden.
- Dauerhaftigkeit: Identitäten müssen langlebig sein, zumindest so lange, wie es Entitäten wünschen.
- Portabilität: Identitätsbezogene Informationen über Identitäten müssen portabel sein.
- Interoperabilität: Identitäten sollten in vielen verschiedenen Anwendungen nutzbar sein.
- Einverständnis: Entitäten müssen der Verwendung ihrer Identitäten und der gemeinsamen Nutzung aller zugehörigen Daten zustimmen.
- Minimierung: Die Offenlegung von Informationen muss minimiert werden.
- Schutz: Die Rechte von Entitäten müssen geschützt werden, wenn es einen Konflikt zwischen den Bedürfnissen des Netzwerks und den Rechten der Entitäten gibt, sollte letztere Priorität haben.

Inspiriert von diesen zehn Prinzipien hat das World Wide Web Consoritum (W3C) mehrere Standards und Protokolle geschaffen, um die Entwicklung von benutzerzentrierten Identitäten voranzutreiben. Ein vom W3C definierter Standard befasst sich mit den Decentralized Identifiers (DIDs) [75]. DIDs sind eindeutige Identifikatoren für selbst-verwaltete digitale Identitäten und werden als URI (Uniform Resource Identifier) genutzt. Ähnlich den URLs (Uniform Recouse Locators) im Internet, können mit DIDs Identitätsschnittstellen gebildet werden. Dabei können DIDs von Entitäten eigenständig erstellt und selbstständig mit Hilfe kryptografischer Funktionen kontrolliert werden. DIDs verweisen auf DID Dokumente, die Metadaten enthalten, um den Besitz und die Kontrolle eines DID zu belegen. Zu diesen Metadaten gehören beispielsweise Attribute, mit denen sich Entitäten

beschreiben lassen und öffentliche Schlüssel (engl., public keys) zur Überprüfung digitaler Signaturen.

Überprüfbare Nachweise (engl., Verifiable Credential) werden genutzt, um das Vertrauen in Identitäten zu stärken. Bei den Verifiable Credentials (VCs) handelt es sich um das elektronische Äquivalent zu den physischen Nachweisen, wie beispielsweise dem Personalausweis oder Führerschein. Gemäß den Empfehlungen vom W3C können Verifiable Credential mit flexiblen Inhalten versehen werden, um sich in den verschiedensten Systemen nutzen zu lassen. Ein Verifiable Credential kann aus einem oder mehreren Verifiable Claims bestehen. Ein Claim beschreibt zunächst eine Eigenschaft einer Entität, die deren Identität beschreibt. Im Wesentlichen besteht ein Claim aus dem Claim-Inhalt (Eigenschaft), Information auf wen sich der Claim bezieht (Claim Target) und dem Claim Aussteller (Claim Issuer). Ein Claim wird von einem Aussteller in der Regel durch eine digitale Signatur bestätigt. Claims können von allen Entitäten bestätigt werden, unabhängig von zentralen Zertifizierungsstellen. Wie sehr eine Bestätigung eines Claims das Vertrauen in einen überprüfbaren Nachweis stärkt, wird bestimmt durch das Vertrauensverhältnis zwischen der prüfenden und der Claim bestätigenden Entität.

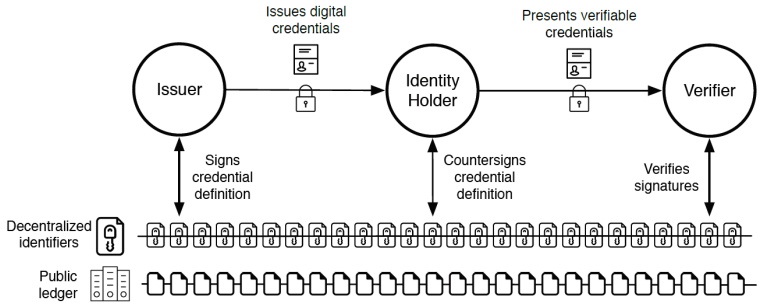

Abbildung 2.7: Illustration eines auf einem Distributed Ledger basierenden Identitätsmanagement [76]

Der bestehende W3C Standard hat nicht festgelegt, wie überprüfbare Nachweise zwischen Entitäten ausgetauscht werden, dennoch stehen zentralisierte Systeme

zum Datenaustausch von überprüfbare Nachweisen im klaren Widerspruch mit den Prinzipien selbst-verwalteter digitaler Identitäten. Hierzu gehört beispielsweise der Kontrollverlust digitaler Identitäten und die fehlende Transparenz gültiger überprüfbarer Nachweise. Der Aufbau und der Betrieb eines zentralisierten Systems zum Datenaustausch ist zudem mit hohen Kosten verbunden, die durch Lizenzen oder Gebühren kompensiert werden müssen. Dezentrale Systeme wie DLTs bieten hingegen enorme Chancen zur Schaffung selbst-verwalteter digitaler Identitäten. Mit Hilfe der DLTs lassen sich selbst verwaltende Systemen aufbauen und betreiben. Diese Technologien ermöglichen einen zugangsfreien (public-permissionless) und sicheren Datenaustausch zwischen beliebigen Entitäten und das manipulationssichere Speichern von Transaktionen. Mittels DLTs lassen sich dezentrale Systeme aufbauen, bei denen verschiedenen Entitäten miteinander kollaborieren und Daten vertrauensvoll miteinander austauschen, ohne dabei einen Datenkontrollverlust zu erleiden. Entitäten können auf einem Distributed Ledger gespeichert Dokument, wie beispielsweise Verifiable Claims, jederzeit auf dessen Echtheit prüfen. Hierzu wird der Hash-Wert eines Dokuments, das auf einem Distributed Ledger gespeichert ist, mit dem Hash-Wert eines zu prüfenden Dokumentes verglichen. Sind die Hash-Werte identisch, handelt es sich um dasselbe Dokument (vgl., Abbildung 2.7). DLTs können zur Datensicherung und zum Echtheitsnachweis von Daten beitragen und damit einen wichtigen Baustein zum Aufbau von selbst-verwaltete digitale Identitäten liefern [77, 78, 79].

2.3.2 Reputationsmanagement

Der Datenaustausch zwischen verschiedenen Systemen wird dadurch limitiert, dass keine oder aber unvollständige Informationen über die Verlässlichkeit einer Entität verfügbar sind. Das Risiko Daten mit möglicherweise unbekannten und böswilligen Entitäten auszutauschen, hemmt einen Datenaustausch und damit eine urbane Vernetzung. Die Verlässlichkeit einer Entität kann mit Hilfe von Reputationen bestimmt werden. Möchte beispielsweise ein Sensormodule mit einem anderen unbekannten IoT-Gerät Daten austauschen, so müssen hierzu zunächst Informationen über das IoT-Gerät verfügbar sein. Reputationssysteme

sammeln, aggregieren und verteilen Informationen bzw. Reputation über Entitäten, um Handlungen von Entitäten zu charakterisieren und Vorhersagen über deren zukünftige Handlungen zu ermöglichen [80]. Gemäß einer Definition von Mui et al. [81], repräsentiert eine Reputation eine Wahrnehmung über eine Entität, die auf Meinungen und Erfahrungen anderer Entitäten beruht. Reputation unterstützen Entitäten in Entscheidungen, welchen fremden Entitäten sie wie sehr vertrauen wollen. Ein wichtiges Ziel vieler Reputationssysteme liegt somit in der Förderung eines Vertrauensaufbaus zwischen unbekannten Entitäten [82].

Viele Reputationssysteme repräsentieren zugangsfreie Systeme, denen Entitäten jederzeit beitreten können. In solchen Systemen können Entitäten böswillig handeln, um Vorteile gegenüber anderen Entitäten zu erzielen. Damit Reputationssysteme sich nutzen lassen, sind zentrale Autoritäten erforderlich [83].

In einem zentral verwaltetem Reputationssysteme übernimmt eine zentrale Autorität alle Aufgaben der Reputationsverwaltung. Hierzu zählt die Berechnung und Speicherung von Reputation, sowie die Überwachung von Entitäten, um sich böswillig verhaltende Entitäten zu identifizieren und aus dem System auszuschließen. Das Vorhandensein einer zentralen Autorität macht es notwendig, dass alle Entitäten der zentralen Autorität vertrauen müssen. Die von Autoritäten gespeicherten Reputationen verfügen über einen hohen finanziellen Wert und stehen im Fokus vieler Cyberattacken. Zudem erschweren zentral verwaltete Reputationen eine Übertragung von Reputation zwischen Systemen. Entitäten können ihre Reputation nicht portabel in ein neues System bzw. Anwendung übertragen und müssen sich systemspezifische Reputationen neu aufbauen.

Dezentral verwaltete Systeme können Limitierungen eines zentralisierten Reputationssystems beheben. In einem Reputationssysteme ohne Autoritäten müssen Entitäten kollaborieren, um nicht vertrauenswürdigen Entitäten zu identifizieren und evtl. zu isolieren. Häufig können dezentral verwaltete Reputationssysteme die Integrität einer Reputation nicht gewährleisten und stellen keine zuverlässigen Mechanismen bereit, um Entitäten beim eigenständigen Verwalten ihrer Reputation unterstützen [84].

DLT können Mechanismen bereitstellen, um eine effiziente Verwaltung von Reputation in zugangsfreien Systemen zu ermöglichen [83]. Beispielsweise können Reputation unveränderlich, überprüfbar und nachvollziehbar in Distributed Ledgern gespeichert werden. Eine nachträgliche Manipulation von Reputationen durch einzelne Entitäten ist nicht möglich. In einem Distributed Ledger gespeicherte Reputationen können manipulationssicher in verschiedenen Systemen und Anwendungen genutzt werden [85, 86].

2.3.3 Peer-to-Peer Bezahlsystem

Aufgrund von diversen Finanzkrisen haben viele Menschen das Vertrauen in Finanzintermediäre, wie beispielsweise Banken, verloren. Der Bedarf an einem elektronischen Zahlungssystem, das auf kryptographischen Beweisen statt auf Vertrauen basiert, gehörte zu den wichtigsten Motivationen, die zur Entwicklung der Distributed Ledger Technology geführt haben. Im November 2008 wurde unter dem Pseudonym Satoshi Nakamoto der Artikel „Bitcoin: A Peer-to-Peer Electronic Cash System “ veröffentlicht [52]. Die Kryptowährungen Bitcoin und dazu gehörende Blockchain ermöglichten digitale Zahlungen ohne Finanzintermediäre.

Der Erfolg der DLTs und das Vertrauen in die Kryptowährungen Bitcoin, ist zum einen großen Teil darauf zurückzuführen, dass sich durch DLTs sogenannte Doppelausgaben (engl., Double-Spending) bei der Übertragung virtueller Vermögenswerte erfolgreich in dezentralen Systemen vermeiden lassen [50]. Werden digitale Vermögenswerte beliebig oft vervielfachen, entstehen Doppelausgaben. Beispielsweise könnte eine Person (Alice) einer anderen Person (Bob) einen Bitcoin senden und dann gleichzeitig denselben Bitcoin verwendet, um eine dritte Person (Carl) zu bezahlen. In zentralen Systemen können einzelne Autoritäten Doppelausgaben verhindern. Hierzu werden alle Transaktion eines digitalen Vermögenswertes überprüft, um einen konsistenten Zustand des Vermögenswertes zu erzielen.

In dezentralen Systemen, in denen Personen digitale Vermögenswerte eigenständig verwalten und direkt tauschen, werden Doppelausgaben dadurch vermieden,

dass jede einzelne Transaktion eines Vermögenswertes öffentlich gemacht wird. Somit können alle Teilnehmer eines dezentralen, öffentlichen Systems die Gültigkeit einer Transaktion überwachen. Desweitern, müssen sich alle Teilnehmer auf einen Zustand aller gültigen Transaktionen einigen. In der Blockchain wird dieser konsistente Zustand aller Vermögenswerte durch Konsensusmechanismen erzielt, wie beispielsweise dem Proof of Work (PoW). Sollte beispielsweise ein Nutzer tatsächlich eine Bitcoin Doppelausgabe durchführen wollen, indem er einen einzelnen Bitcoin gleichzeitig an zwei unterschiedliche Empfänger sendet, so wird dank Konsensusmechanismus, nur eine der beiden Transaktionen validieren. Auch wenn Konsensusmechanismen Doppelausgaben verhindern und damit einen sichere Übertragung von virtuellen Zahlungen in offenen Systemen ermöglichen, führt der Einsatz vieler Konsensusmechanismen zu einem begrenzten Transaktionsdurchsatzes und einer verzögerten Transaktionsbestätigung. Während zentrale Zahlungssysteme, wie beispielsweise VISA bis zu 65.000 Zahlungstransaktionen pro Sekunde verarbeiten, sind in einer öffentlichen und frei zugänglichen (public permissionless) Blockchain etwa sieben Transaktionen pro Sekunde möglich [87]. Zudem fallen in vielen Distributed Ledgern hohe Transaktionsgebühren an, wodurch der Einsatz von Kryptowährungen für tägliche Zahlungen weiter stark eingeschränkt wird [88].

Zahlungskanäle (engl., Payment Channels) werden genutzt, um eine Vielzahl an elektronischen Zahlungen zu geringen Transaktionskosten zu ermöglichen. Zahlungskanäle sind Zustandskanäle, dessen Zustand den Saldo einer Krypotwährung repräsentieren. Viele Zahlungskänale nutzen hierzu eine Kombination aus Multi-Signature Adressen und Multi-Signature Transaktionen. Möchten Alice und Bob mehrere Zahlungen mittels eines einfachen Zahlungskanals austauschen, senden beide Parteien zunächst einen bestimmen Betrag an eine gemeinsam erstellte Multi-Signature Addresse. Diese gemeinsam Multi-Signature Addresse setzt sich zusammen aus den privaten Schlüsseln beider Parteien. Das sich auf dieser Multi-Signature Addresse befindlichen Saldo kann ausschließlich durch Multi-Signature Transaktionen beider Parteien modifiziert werden. Gültige Transaktionen müssen von beiden Parteien signiert werden. Ein Zahlungskanal kann jederzeit geschlossen werden, indem eine Partei eine gültige Multi-Signature Transaktionen dem

Distributed Ledger sendet. Multi-Signature Transaktionen können direkt zwischen den zwei Parteien Alice und Bob getauscht werden. Eine kontinuierliche Kommunikation über einen Distributed Ledger ist nicht erforderlich, zumal alle getauschten Multi-Signature Transaktionen nicht zwangsläufig vom Distributed Ledger validiert werden müssen. Hierdurch erfolgt eine beliebig kleine Stückelung von Zahlungen. Zahlungskanäle eignen sich insbesondere zur feingranularen Abrechnung geringer Datenmengen [89].

3 Stand der Wissenschaft und Technik

Das Ziel dieser Arbeit ist die Förderung von Kollaborationen zwischen intelligenten Geräten durch Möglichkeiten der Datenmonetarisierung. Die Datenmonetarisierung beginnt zunächst mit der Datengenerierung. Der erste Abschnitt dieses Kapitels befasst sich mit aktuellen Technologien und Methoden der Datenerfassung in den urbanen Bereichen Umwelt und Verkehr. Anschließend werden aktuelle Ergebnisse zum Verwalten von Datenströmen vorgestellt. Es wird vor allem auf Methoden einer verlässlichen Identifikation und Authentifizierung eingegangen. Der letzte Abschnitt dieses Kapitels befasst sich mit Möglichkeiten der Datenmontarisierung und aktuellen Herausforderungen, die ein Monetarisierung von Daten zwischen Geräten erschweren.

3.1 Urbane Sensormodule

Serviceorientierte Architektur (SoAs) sind für viele Städte zu einem unverzichtbaren Instrument geworden, um urbane Aktivitäten zu analysieren und verfügbare Ressourcen effizient zu nutzen. Vor allem für die Überwachung der urbanen Luftqualität sind verteilte Sensormodule (Physikalische Schicht) von enormer Bedeutung. Im Bereich der Umweltüberwachung erfassen verteilte Sensormodule häufig die folgenden Schadstoffe; Feinstaub (PM) (2,5 µm und 10 µm), Stickoxide (NOx), Kohlenmonoxid (CO), Ozon (O3) und Kohlendioxid (CO2). Zudem werden oft Temperatur und Luftfeuchtigkeit zur Sensorkalibrierung gemessen (vgl. Abbildung 3.1). Messungen der Schadstoffkonzentration erfolgen

mit Hilfe kommerzieller Sensoren. Feinstaubmessungen nutzen häufig optische und Gasmessungen elektrochemische Sensoren.

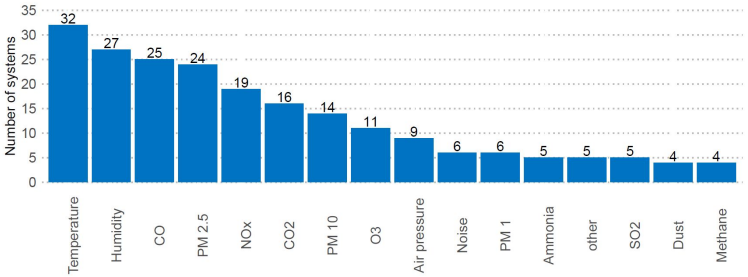

Abbildung 3.1: Übersicht verschiedener Luftschadstoffe und Umweltparameter [90]

Hinsichtlich der Netzwerkschicht einer SoA werden oft private Netzwerke zur Datenübertragung genutzt [90]. Private drahtlose Netzwerke nutzen für die Übermittlung der erfassten Messwerte klassische Kommunikationstechnologien, wie beispielsweise Mobilfunk. Alternativ werden Long Range Wide Area Networks (LoRaWANs) zur Datenübertragung genutzt, zumal sich über LoRaWANs Daten kostengünstig über große Reichweiten übertragen lassen. Andere Technologien wie Bluetooth oder ZigBee werden seltener eingesetzt, da ihre geringe Übertragungsreichweite die Überwachung der Luftqualität in großen städtischen Gebieten erschwert.

Neuartige IoT-spezifische Kommunikationstechnologien, wie beispielsweise das Message Queuing Telemetry Transport (MQTT), werden kaum in Studien zur Analyse der Luftqualität eingesetzt. Selten werden ebenfalls innovative Vehicle to Infrastructure (V2I) Netze für die Luftüberwachung genutzt. Dabei könnten V2I Netze eine flächendeckende Infrastruktur und effiziente Kommunikation für die Datenerfassung im städtischen Kontext ermöglichen und somit die Überwachung der urbanen Luftqualität verbessern [91].

Die Entwicklung intelligenter Sensormodule zur Analyse der urbanen Luftqualität wird maßgeblich durch limitiert, dass ausschließlich Schadstoffkonzentrationen und einige meteorologische Parameter lokal bestimmt werden. Eine simultane

Messung aller relevanter Parameter, einschließlich ihrer gegenseitigen Abhängigkeiten und ihrer gemeinsamen zeitlichen und räumlichen Dynamik, erfolgt nicht. Beispielsweise ignorieren Sensormodule den Einfluss der lokalen Verkehrsdichten auf gemessene Schadstoffkonzentrationen. Die Kombination von Messung aus dem Umwelt und Verkehrsbereich stellt eine enorme und interdisziplinäre Herausforderung dar.

Eine Erweiterung bestehender Sensormodule um kommerzielle Verkehrsmodule, wie beispielsweise einem Radargerät, ist für eine kostengünstige und konfigurierbare Verkehrsüberwachung nicht möglich. Zur kostengünstigen Verkehrsüberwachung wurde untersucht, wie sich der urbane Verkehr mittels bereits verfügbaren Verkehrskameras überwachen lässt. Hierzu wurden die von Verkehrskameras erfassten Daten zur Verkehrsanalyse an weitere Systeme bzw. Verkehrsleitsysteme übermittelt. Aufgrund der Menge an Videos, die von verteilten Verkehrskameras übertragen werden, kann es jedoch zu einer Überlastung der genutzten Netzwerke und zu großen Übertragungsverzögerungen kommen. Bereits heute generieren die in Städten installierte Kameras mehrere Terabyte an Daten [92].

Neben einer verlässlichen und echtzeitfähigen drahtlosen Übertragung großer Datenmengen, bestehen eine weitere Herausforderung im Schutz der Privatsphäre gefilmter Verkehrsteilnehmer. Bisherige Ansätze zum Schutz der Privatsphäre fokussierten sich auf eine Nachbearbeitung der Videos durch das Löschen von Erkennungsmerkmale wie Gesichtern [93]. Solche Ansätze der Datennachverarbeitung setzen voraus, dass Bürger den Unternehmen bzw. Institutionen der Verkehrsüberwachung vollständig vertrauen, ihre sensiblen Daten nicht zu missbrauchen. Gefilmte Bürger haben keine vollständige Transparenz über die Verarbeitung ihrer persönlichen Daten. Die öffentliche Akzeptanz für die Nutzung von Verkehrskameras zur Verkehrsüberwachung ist in vielen europäischen Städten gering [94].

Bisherige Analyse von Verkehrsvideos durch zentrale verwaltete Systeme folgen dem Tracking-by-Detection-Paradigma (vgl. Abschnitt 2.2). Zur Erkennung verschiedenster Verkehrsteilnehmer lassen sich unterschiedliche Detektoren nutzen,

dessen Aufgabe ist es Verkehrsteilnehmer verlässlich zu lokalisieren und klassifizieren. Basierend auf den enormen Entwicklungen im Bereich der KI basierten Bildverarbeitung, haben vor allem objektbasierte Detektoren an Bedeutung gewonnen [95]. Zu den objektbasierten Detektoren gehören vor allem Convolutional Neural Networks (CNNs) [96]. Anders als bei den erscheinungsbasierten oder bewegungsbasierten Detektoren, müssen für den Einsatz von CNNs zur Objekterkennung keine Objektmerkmale manuell definiert werden, zumal CNNs Merkmale selbstständig erlernen. Zu den bekanntesten objektbasierten Detektoren gehören R-CNNs (Region Based Convolutional Neural Networks [97]), die prinzipiell in drei Hauptmodulen eingeteilt werden können. Das erste Modul enthält ein Segmentierungsalgorithmus, der als „Selektive Suche“ bezeichnet wird. Ziel des Segmentierungsalgorithmus ist es, Bildabschnitten (Regionen) mit einer hohen Objektwahrscheinlichkeit zu lokalisieren. Das zweite Modul besteht aus CNNs, welche aus allen vorgeschlagenen Regionen Merkmalsvektoren generiert. In einem dritten Modul werden die extrahierten Merkmalsvektoren anschließend mit Hilfe eines SVM (Support Vector Machine [98]) Algorithmus zur Objektklassifizierung weiterverarbeitet.

R-CNN Detektoren benötigten langen Berechnungszeiten zur Objektdetektion, weshalb schnellere CNN basierte Detektoren entwickelt wurden. Hierzu zählen vor allem die Detektoren Fast R-CNN [99] und Faster R-CNN [100]. Beim Fast R-CNN Detektor wird nicht für jede Region ein separates CNN zur Merkmalsextraktion genutzt, sondern ausschließlich ein gemeinsames CNN für alle Regionsvorschläge eines Bildes. Verglichen mit dem R-CNN Detektor, konnte durch diese Änderung die Berechnungszeiten des Fast R-CNN massiv reduziert werden. Der Faster R-CNN Detektor fokussiert sich auf die Auswahl der zu untersuchenden Regionen, um die Berechnungszeit des Detektors zu minimieren. Faster R-CNNn nutzt ein trainiertes Region Proposal Network (RPN), anstatt einer selektiven Suche zur Bestimmung von Regionsvorschlägen. Aufgrund dieser weiteren Optimierung, wird der Faster R-CNN Detektor häufig für Verkehrsvideoanalysen genutzt. [101, 102, 103].

Neben zweistufigen Detektoren (wie dem CNN), können auch einstufige Detektoren zur Verkehrsanalyse genutzt werden. Zu den bekanntesten einstufigen

Detektoren gehört YOLO [42]. YOLO Detektoren ermöglichen zeitgleich eine Lokalisierung und Objektklassifizierung. Hierzu wird jedes Bild in ein SxS Raster unterteilt. Innerhalb eines solchen Rasters N werden Begrenzungsrahmen (engl., Bounding Boxes) und dessen Konfidenz bestimmt. Die Konfidenz der insgesamt SxSxN Boxen repräsentiert die Wahrscheinlichkeit, ob innerhalb einer Bounding Box tatsächlich ein gesuchtes Objekt enthalten ist. Die meisten dieser Boxen haben niedrige Konfidenzwerte und werden unterhalb eines bestimmten Schwellwertes nicht weiter betrachtet. Ein wichtiger Vorteil der einstufigen Detektoren gegenüber den zweistufigen Detektoren liegt vor allem in der Verarbeitungsgeschwindigkeit, gemessen in Bilder pro Sekunde (engl., Frames per Second, FPS).

Beim Einsatz von KI basierten Methoden der Objekterkennung und Verfolgung ist vor allem das Verhältnis zwischen Ressourcenverbrauch und Analysegenauigkeit relevant. Im Allgemeinen führt die Verarbeitung jedes Bildes mit hoher Auflösung, zur hohen Genauigkeit, wenn auch zeitgleich zu einem hohen Ressourcenbedarf. Wie sich hohe Genauigkeiten und Verarbeitungsgeschwindigkeit von zentralisierten Systemen auf kleiner Edge Geräte mit starken Ressourcenbeschränkungen übertragen lassen, ist nicht bekannt.

3.2 Datenverwaltung in dezentralen Netzwerken

Mit dem kontinuierlichen Anstieg urbaner Sensoren wächst die Menge potenziell verfügbarer Daten. Neben dem Erheben von verlässlichen Messdaten unterschiedlichster Bereiche, ist ebenfalls die Datenverwaltung mit großen Herausforderungen der Datensicherheit und des Datenschutzes verbunden [104, 105]. Viele Herausforderungen basieren auf den besonderen Merkmalen konventioneller IoT Implementierungen (vgl. Abschnitt 2.1). Hierzu gehört beispielsweise der verlässliche Datenaustausch zwischen großen heterogenen Netzwerken und IoT-Geräten, die über stark limitierte Rechenressourcen und Möglichkeiten der Energieversorgung verfügen.

Public-Key-Infrastrukturen (PKIs) gehören zu den wichtigsten Technologien, die einen sicheren Informationsaustausch über das IoT ermöglichen. Eine PKI erstellt digitale Zertifikate, speichert diese Zertifikate sicher in einem zentralen Repository bzw. Speicher und widerruft diese bei Bedarf. Basierend auf einer zunehmenden Vernetzung im IoT, sind digitale Zertifikate zur Identifizierung und Authentifizierung von IoT-Geräten von enormer Bedeutung.

In vielen Städten übernehmen zentral verwaltete Plattformen alle zur gemeinsamen Datennutzung notwendigen Aufgaben der Identifizierung, Authentifizierung und Autorisierung. Plattformbetreiber übernehmen zusätzlich Aufgaben der Datenspeicherung nach einheitlichen Datenmodellen und die Implementierung spezifischer Business Intelligence (BI) Dienste [106]. Aufgrund der Vielzahl an Aufgaben, die Plattformen im IoT übernehmen können, lassen sich in der Literatur diverse Beispiele [107, 108, 109] zentralisierter Data-Sharing Plattformen finden.

Trotz der vielen Aufgaben und Vorteile, die ein Einsatz zentral verwalteter Data-Sharing-Plattform mit sich bringt, ist für einen erfolgreichen Plattformbetrieb eine vertrauenswürdige Instanz notwendig. Vor allem PKI Infrastrukturen sind Risiken ausgesetzt, die sich durch Ausfälle oder Manipulationen einzelner Zertifizierungsstellen (engl., certification authorities, CAs) ergeben. Zentral verwaltete Plattformen verfügen über eine eingeschränkte Datensicherheit und sind anfällig für böswillige Angriffe. Beispielsweise könnten Plattformbetreiber die Daten eines Dateneigentümers entsprechend ihren eigenen Interessen verändern und Datenkonsumenten manipulierte Daten bereitstellen [110]. Zusätzlich leiden viele zentralisierte Plattform unter einer geringen Skalierbarkeit. Eine starke Zunahme an vernetzten IoT-Geräten, Dateneigentümern und Datenkonsumenten wird die Anzahl an Transaktionen zum Datenaustausch dramatisch ansteigen lassen. Dieser Anstieg wird vor allem bei zentralisierten Plattformen zu Instabilitäten und langen Verarbeitungszeiten führen und zudem die Wahrscheinlichkeit eines Zusammenbruchs der Plattform erhöhen [111].

Ein potenziell schädlicher Einfluss böswillige Plattformbetreiber kann durch eine End-zu-End Datenverschlüsselung gemildert werden. Hierzu werden Daten vom Dateneigentümer verschlüsselt, noch bevor diese auf einer Plattform gespeichert

werden. Böswilligen Plattformbetreibern liegen somit ausschließlich verschlüsselte Daten vor, wodurch das Risiko einer nicht unautorisierten Manipulation oder Datenweitergabe stark reduziert wird. Sofern die zur Entschlüsselung der Daten notwendigen Schlüssel vorliegen, kann der Datenkonsumenten auf gespeicherte Daten zugreifen.

Damit keine einzelne Autorität die Verwaltung genutzter Schlüssel verantworten muss und keine Abhängigkeiten zu einzelnen Autorität entstehen, haben sich viele Forschungsarbeiten [112, 113, 114] mit dem Einsatz von DLTs zur Verwaltung von Schlüsseln und Zugangsrechten befasst. Eine automatisierte Zugriffskontrolle wird häufig mit Hilfe von Smart-Contracts realisiert. Beispielsweise speichern Dateneigentümer Informationen über verfügbare IoT-Geräte in einen Smart Contract. Jeder Datenkonsument der diese Daten erhalten möchte, muss zunächst die Kosten für die Ausführung eines Smart-Contracts aufbringen. Die vom Datenkonsumenten hierzu an einem Distributed Ledger gesendete Transaktion wird zu den im Smart Contract festgelegten Bedingungen durchgeführt. Sind alle im Smart Contract definierten Zugriffsbedingungen erfüllt, empfangen IoT-Gateways die Datenanfrage. Anschließend werden die angefragten Daten entsprechend den im Smart Contract definierten Zugriffsrichtlinien entschlüsselt [114].

Damit Daten zeitnah zwischen Systemen und Entitäten geteilt werden, werden ausschließlich geringe Datenmengen in öffentlich zugänglichen (public-permissionless) Distributed Ledgern gespeichert. Die Speicherung von Rohdaten und Metadaten wird voneinander entkoppelt. Metadaten werden in einem Distributed Ledger frei zugänglich gespeichert, wohingegen Rohdaten verschlüsselt außerhalb eines Distributed Ledger gespeichert werden. Metadaten können beispielsweise Informationen zur Identität des Dateneigentümers, des IoT-Gerätes oder der Speicheradresse der Daten, sowie einen Hashwert der Rohdaten beinhalten. Datenkonsumenten können die Integrität der Daten überprüfen, indem sie den Hashwert der außerhalb des Distributed Ledgers gespeicherten Daten, mit dem innerhalb eines Distributed Ledgers gespeicherten Hashwert vergleichen.

Für einen sicheren Datentransfer in dezentral organisierten Netzwerken ist es notwendig, digitale Identitäten eigenständig aufbauen und verlässlich kontrollieren

zu können. Zudem müssen Möglichkeiten geschaffen werden, die Vertrauenswürdigkeit anderer Einheiten eigenständig bewerten zu können. Die Möglichkeit Vertrauen zwischen Entitäten aufzubauen und zu quantifizieren, gilt als treibende Kraft für Kollaborationen bzw. das Teilen von Daten in verteilten Infrastrukturen. DLTs können den Aufbau von Vertrauensbeziehungen zwischen Entitäten fördern, indem das Verhalten von Entitäten sicher und transparent gespeichert wird. Eine auditierbare Speicherung des Verhaltens einzelner Entitäten, fördert ein verantwortungsvolles Handeln und reduziert Möglichkeiten böswilliger Entitäten den Betrieb verteilter Infrastrukturen zu stören [115]. Das Management von Vertrauensbeziehungen ist an Authentifizierungsmechanismen gebunden und basiert in verteilten Systemen auf dezentralen Vertrauensmodell. Das Web of Trust (WoT) repräsentiert ein dezentrales Vertrauensmodell, bei dem die Authentizität von öffentlichen Schlüsseln und ihren Besitzern auf Vertrauenswerten basieren. Zwar entfällt beim Einsatz eines WoT Vertrauensmodells die Notwendigkeit einer zentralen Zertifizierungsstelle, dennoch gibt es offene Herausforderungen bei der Behandlung der Aktualisierung von Vertrauensbeziehungen, der Gewährleistung der Privatsphäre und dem initialen Aufbau von Vertrauensbeziehungen [116].

In bisherigen Studien zu Aufbau eines verteilten Identitäts- und Vertrauensmanagement fehlen detaillierte Informationen zur Skalierbarkeit und den Transaktionskosten. Die Ausführung von Smart Contracts in public permissionless Distributed Ledgern führt zu hohen Transaktionskosten und ist für viele IoT Szenarien nicht rentabel. Darüber hinaus bleibt unklar, wie außerhalb eines Distributed Ledgers gespeicherten Daten verlässlich gespeichert werden, um Risiken einer geringen Datenverfügbarkeit zu minimieren.

3.3 Datenmonetarisierung

Viele Städte möchten ihre Infrastrukturen mit Hilfe modernster Technologie aufzurüsten. Angesichts stark limitierter Budgets ist die Finanzierung vieler Infrastrukturprojekte schwierig und macht die Suche nach innovativen Geschäftsmodellen erforderlich. Neben traditionellen Geschäftsmodellen, wird für viele Städte

bzw. Dateneigentümer, das Generieren von zusätzlichen Einnahmen durch das Teilen von Daten immer bedeutsamer. Die Zunahme an Daten und vernetzten Systemen, erhöht zudem die wirtschaftliche Bedeutung einer Datenmonetarisierung im IoT [117].

Eine Datenmonetarisierung beschreibt einen Prozess der Datennutzung, mit dem Ziel eines quantifizierbaren und wirtschaftlichen Nutzens [118]. Anders als bei einer Datenfreigabe, wie sie beispielsweise zwischen Unternehmen einer Lieferkette stattfinden, besteht der Kerngedanke der Datenmonetarisierung in der Generierung von Einnahmen [119]. Die Generierung von Einnahmen durch IoT-Daten ist durch eine direkte oder indirekte Monetarisierung möglich. Die direkte Monetarisierung bezieht Einnahmen direkt aus Datentransaktionen. Bei der indirekten Monetarisierung werden Daten genutzt, um neue Dienstleistungen oder Produkte zu produzieren, die anschließend verkauft werden [120]. Beispielsweise könnten Städte durch bestehende Überwachungssystemen Daten zur aktuellen Verkehrssituation oder Parkplatzauslastung erzeugen und diese direkt an Navigationsunternehmen gewinnbringend verkaufen. Wohingegen eine indirekte Datenmonetarisierung durch das Veräußern von Verkehrsprognosen möglich wäre.

Die direkte als auch indirekte Monetarisierung von großen und heterogenen Datenströme ist eine anspruchsvolle Aufgabe. Zumeist werden Daten über einen Datenmarktplatz gehandelt. Ein Datenmarktplatz kann als eine digitale Plattform verstanden werden, die Aufgaben der Datenmonetarisierung übernimmt. Neben der Datenspeicherung durch einen Plattformbetreiber, gehört hierzu die Registrierung der Nutzer und Geräte, das Vermitteln von Datenangeboten und die Abwicklung von digitalen Zahlungen. Betreiber eines Marktplatzes können potenzielle Datenlieferanten auswählen, die den Anforderungen eines Datenkonsumenten entsprechen und somit durch die Vermittlung beider Parteien einen Datenhandel erleichtern.

Wie auch andere zentralisierte Plattformen, lassen sich viele Datenmarktplätze im IoT kaum sinnvoll nutzen. Neben Limitierungen hinsichtlich der Skalierbarkeit der Plattformen und dem Kontrollverlust der gespeicherten Daten, schränken vor allem hohe Verwaltungskosten für Zahlungsdienstleistungen die Monetarisierung

der Daten stark ein. Eine Möglichkeit diese Limitierungen zu umgehen, ist der Aufbau eines dezentralen Marktplatzes, der auf Peer-to-Peer (P2P) Kommunikationsmodellen basiert. In einem dezentral verwalteten Datenmarktplatz für Daten von IoT-Geräten können Datenverwaltungsaufgaben und Zahlungen mit Hilfe von Smart Contracts durchgeführt werden [121]. Wurde eine Zahlung durch einen Smart Contract durchgeführt, können die außerhalb eines Ledgers gespeicherten Daten freigegeben werden [10]. Die Zahlung von außerhalb des Ledgers gespeicherten Daten, kann als riskant eingestuft werden, da eine Datenlieferung nicht zwangsläufig erfolgen muss. Mit Hilfe eines Reputationsmanagements können potenzielle Konsumenten vor dem böswilligen Verhalten einzelner Entitäten geschützt werden, zumal mit Reputationen das Risiko eines möglichen Datenhandels mit unbekannten Entitäten bewertet werden kann[122].

Trotz vieler Anstrengungen einen Datenmarktplatz zum Handel von Daten im IoT aufzubauen, um Daten zu monetarisiernen, bleiben noch viele Fragen offen. So führt das Speichern von Datenströmen in sequentiellen Blöcken und außerhalb eines Distributed Ledgers, zu hohen Übertragungslatenz gehandelter Daten. Zudem kommt es zu Verzögerungen durch die Ausführungsdauer der zur Zahlung genutzten Smart-Contracts. In einem public permissonless Distributed Ledger, wie beispielsweise Ethereum, kann es Minuten dauern bis Smart-Contract vom Netzwerk bestätigt und damit Zahlungen getätigt werden. Zudem fallen hohe Ausführungskosten der Smart-Contracts an, die einen Datenhandel für viele Konsumenten schnell unrentabel machen können. Experimentelle Untersuchungen [122] haben belegen können, dass Datenkonsumenten einen Kompromiss eingehen müssen, zwischen der Ausführungsdauer einer dezentralen Marktplatztransaktion und den Ausführungskosten, die für die Bestätigung einer Eingangstransaktion entstehen. Echtzeitdatenströme verlieren jedoch tendenziell an Wert, wenn sie nicht nahezu in Echtzeit nutzen lassen. Bestehende Arbeiten und Konzepte liefern daher keine Antwort auf eine effiziente und rentable Monetarisierung von Datenströmen im IoT.

4 Intelligentes Sensormodul

Das folgende Kapitel befasst sich mit der Entwicklung eines intelligenten Sensormoduls, um lokale Aktivitäten aus den Bereichen Verkehr und Umwelt simultan zu bestimmen. Anhand eines konzeptionierten und implementierten Prototypen wird die Funktionsfähigkeit des entwickelten Sensormoduls nachgewiesen.

Einige Ergebnisse dieses Kapitels stammen aus einer wissenschaftlichen Veröffentlichungen [K1] des Autors in Zusammenarbeit mit weiteren Co-Autoren.

4.1 Smart City Node

Eine Zunahme des motorisierten Individualverkehrs, bei einer gleichzeitigen starken Verdichtung urbaner Räume, hat in vielen Städten zu hohen Schadstoffkonzentrationen gefügt. Zum Schutz der Bürger erfolgt eine Überwachung lokaler Schadstoffkonzentrationen in Städten durch einige wenige stationäre Messstationen. Die hohe Messgenauigkeit dieser Stationen erfordert zugleich hohe Investitions- und Wartungskosten. Aufgrund der hohen Kosten ist eine Überwachung der Luftqualität in gesamten urbanen Raum mit stationären Messstationen nicht möglich. Die wenigen Messungen stationärer Messstationen, werden daher mit weiteren Messungen portabler Sensormodule ergänzt [123, 124]. Diese portablen Sensoren liefern zwar weniger präzise Schadstoffmessungen, können jedoch aufgrund ihre geringen Investitionskosten flächendeckend im urbanen Raum verteilt werden, um raumzeitliche Analysen innerstädtischer Schadstoffverteilungen zu unterstützen.

Stationäre Messstationen und portable Sensormodule liefern lokale Schadstoffkonzentationen, jedoch keine Informationen der am Messstandort vorherrschenden meteorologischen Bedingungen oder anthropogenen Schadstoffemissionsquellen. Eine Analyse gemessener Schadstoffkonzentationsänderungen ist ohne solche Parameter aus dem Bereich Umwelt und Verkehr kaum möglich.

Meteorologische Bedingungen wirken sich auf die Bildung, den Transport und die Akkumulation von Luftschadstoffen aus [125]. Viele verschiedene Studien [126, 127, 128, 129] haben zeigen können, dass meteorologische Parameter wie beispielsweise Windgeschwindigkeit und -richtung, Temperatur, relative Luftfeuchtigkeit oder Niederschlag die Luftqualität erheblich beeinflussen können. Beispielsweise kann die Windgeschwindigkeit einen Einfluss haben auf die Vermischung und den Transport von Luftschadstoffen [126]. Sinkende Lufttemperaturen in der Nacht können eine Temperaturinversion erzeugen, die als Barriere wirkt und die Diffusion von Feinstaub hemmt [127]. Änderungen der relativen Luftfeuchtigkeit können chemische Reaktionen auf den Partikeloberflächen beschleunigen und somit die Größenverteilung von Partikeln beeinflussen. Niederschlagsperioden können gasförmige Verunreinigungen beseitigen und Partikel aus der Luft sedimentiert [129, 130].

In städtischen Gebieten gehört der Straßenverkehr zu den wichtigsten anthropogenen Schadstoffemissionsquellen und trägt erheblich zu direkten Schadstoffemissionen von Kohlenstoffmonoxid (CO), Stickoxiden (NOx), schwarzem Kohlenstoff (BC), Feinstaub (PM) und anderen Schadstoffen bei [131]. Beispielsweise entsteht Kohlenstoffmonoxid durch die unvollständige Verbrennung kohlenstoffhaltiger Materialien und Feinstaub durch den Abrieb von Fahrzeugreifen [132]. Unterschiedlichen Studien haben bereits einen starken Anstieg verschiedener Schadstoffkonzentration in der Nähe stark befahrener Straßen belegen können [131, 130]. Ohne Informationen zur Verkehrssituation am Messstandort, sind Schwankungen der Schadstoffkonzentrationen und Zusammensetzung schwer nachzuvollziehen.

Trotz der Vielzahl an möglichen Wechselwirkungen zwischen Messgrößen der Bereiche Umwelt und Verkehr, werden in bisherigen Studien und Systemen hauptsächlich Schadstoffkonzentrationen gemessen. Automatische, kostengünstige und kontextbezogene Messungen sind für die Entwicklung einer intelligenten Stadt von enormer Bedeutung. Beispielsweise können solche Messungen aus den Bereichen Verkehr und Umwelt genutzt werden, um die Entwicklung von Schadstoffprognosemodellen und damit einer umweltsensitiven Verkehrssteuerungen zu fördern. Eine umweltsensitive Verkehrssteuerungen könnte sich Korrelationen zwischen dem Verkehrsaufkommen, meteorologischen Parameter und Änderungen der Schadstoffkonzentration zu Nutze machen, um Bürgern eine hohe Mobilität und Luftqualität zu gewährleisten [133]. Permanente Fahrverbote oder sonstige verkehrspolitische Maßnahmen, mit denen die Mobilität und damit die Lebensqualität der Bürger eingeschränkt werden, wären nicht notwendig.

Das im Rahmen dieser Arbeit entwickelte intelligente Sensormodul, im nachfolgenden auch Smart City Node (SCN) genannt, erhebt Messung unterschiedlicher Schadstoffkonzentrationen, der aktuellen Verkehrssituation sowie meteorologische Parameter. Mit der Möglichkeit kontextbezogene Schadstoffmessungen durchzuführen, erlaubt der SCN einen neuen Blick auf urbane Aktivitäten und Initiativen. Hierzu besteht der SCN im Wesentlichen aus vier Modulen (vgl. Abbildung 4.1). Zu diesen vier Modulen gehört ein Sensor-, Datenverarbeitungs-, Datenübertragungs- und Energieversorgungsmodul.

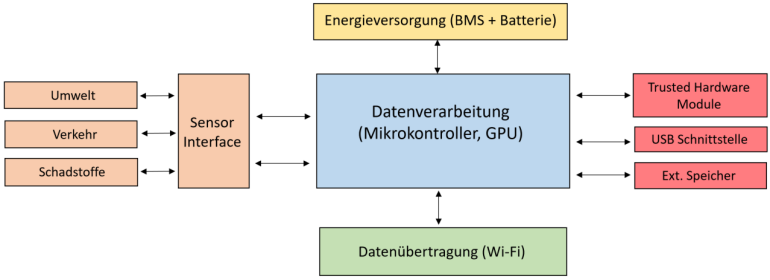

Abbildung 4.1: Schematische Darstellung wesentlicher Module des Smart City Nodes (SCN)

4.1.1 Sensormodul

Das Sensormodul des SCN besteht aus unterschiedlichen Sensoren zur simultanen Messungen unterschiedlichster urbaner Parameter. Zu diesen Parametern gehören Schadstoffkonzentrationen, meteorologische Umweltparameter und Messwerte zu aktuellen Verkehrssituation (vgl., Tabelle 4.1). Die Bereitstellung unterschiedlichster Parameter erfolgt durch eine Vielzahl an Sensoren. Diese unterschiedlichen Sensoren repräsentieren modulare Subsysteme innerhalb des Sensormoduls des SCN.

Tabelle 4.1: Übersicht der Messgrößen des Smart City Nodes (SCN)

Schadstoffkonzentation	Meteorologische Parameter	Verkehr
CO	Luftdruck	Verkehrsstärke
NO2	Niederschlag	Geschwindigkeitsschätzung
PM1	Relative Luftfeuchte	
PM2,5	Temperatur	
PM10	Windgeschwindigkeit	
	Windrichtung	

Schadstoffe

Ein Subsystem des Sensormoduls des SCN dient der Bestimmung unterschiedlicher Schadstoffkonzentration. Zu den häufig gemessen Schadstoffkonzentrationen gehört Feinstaub. Feinstaub kann bis tief in die Lunge vordringt und einen großen Schaden auf Mensch und Umwelt haben. Ein in vielen Studien [134, 135, 136] evaluierter und kostengünstiger Feinstaubsensor, ist der optische Partikelzähler OPC-N3 des Unternehmens Alphasense [137]. Der OPC-N3 bestimmt Feinstaubkonzentrationen unterschiedlicher Partikeldurchmesser, wie dem PM1 (weniger als 1 μm), PM2,5 (weniger als 2,5 μm) und PM10 (weniger als 10 μm) bei einer hohen zeitlichen Auflösung von 1 Hz. Der OPC-N3 ist zusätzlich mit Sensoren

zur Messung der Temperatur und relativen Luftfeuchte ausgestattet, um dessen Einfluss auf die Zuverlässigkeit der Partikelmessung zu berücksichtigen.

Zusätzlich zum OPC-N3 verfügt der SCN noch über weitere Gassensoren, um Schadstoffkonzentationen von Stickstoffdioxid (NO2) und Kohlenmonoxid (CO) zu bestimmen. Die hierzu eingesetzten elektrochemischen Gassensoren des Unternehmens Alphasense gehören aufgrund ihrer geringen Herstellungskosten und Selektivität zu beliebten Schadstoffsensoren [138, 139, 140].

Die elektrochemischen Gassensoren verwenden eine Drei-Elektroden-Zelle, um einen Strom zu erzeugen, der linear proportional zum Volumenanteil eines Zielgases ist. Jede Zelle besteht aus drei Elektroden, einer Arbeitselektrode (WE), einer Referenzelektrode (RE) und einer Gegenelektrode (CE) [141]. Alle Elektroden sind in eine Elektrolytlösung eingebettet, die durch eine semipermeable Membran von der Atmosphäre getrennt ist. Das Zielgas, wie beispielsweise CO, diffundiert durch die Membran in den Elektrolyten, wo es mit der WE in Kontakt kommt und entweder oxidiert oder reduziert wird [142]. Die anderen beiden Elektroden (RE, CE) werden genutzt, um die chemische Reaktion der WE auszugleichen und eine stabile Umgebung wie Äquivalentstrom und stabiles Potenzial bereitzustellen. Die resultierende Spannung zwischen RE und WE erzeugt einen Signalstrom, der mit der Zielgaskonzentration korreliert [143]. Die folgende Gleichung wird genutzt, um Gaskonzentrationen zu bestimmen,

$$p(\text{ Zielgas }) = \frac{(WE_u - WE_e) - n_T \cdot (AE_u - AE_e)}{n_{T_S} \cdot S} \tag{4.1}$$

Gemäß dem Alphasense-Benutzerhandbuch müssen beide Sensorausgangsspannungen, die WE_i und RE_i, um einen Nullpunktsversatz (WE_0; RE_0) von typischerweise 225-245 mV korrigiert werden. Die korrigierte WE-Spannung wird von der korrigierten RE-Spannung subtrahiert und durch die Empfindlichkeit S von typischerweise 0,175-0,18 mV/ppm sowie einen Temperaturkorrekturfaktor n_{T_S} dividiert.

Umwelt

Ein weiteres Sensorsubmodul zur Erfassung meteorologischer Bedingungen ist mit verschiedenen Sensoren ausgestattet, um Änderungen der Windrichtung, Geschwindigkeit, Niederschlag, Lichtstrahlung, Temperatur, relative Luftfeuchtigkeit und Luftdruck zu messen. Zu diesem Zweck nutzt der SCN eine kommerzielle Wetterstation (Argent Data Systems 80422), die mit einem Anemometer, einer Windfahne und einem Regensensor ausgestattet ist. Zusätzlich zur Wetterstation nutzt der SCN einen Lichtsensor (Adafruit SI1145), um Informationen zur lokalen Sonneneinstrahlung und Bewölkung zu erhalten. Beispielsweise können Messungen der Sonneneinstrahlung wichtige Informationen liefern, um die Entstehung von Ozon zu analysieren [144]. Der Lichtsensor erfasst Lichtintensitäten im Infrarotspektrum mit einer Wellenlänge zwischen 550 nm-1000 nm. Ein Atmosphärensensor (Bosch BME280) wird verwendet zur Erfassung der Lufttemperatur, der relativen Luftfeuchtigkeit und des Umgebungsdrucks. Dieser Atmosphärensensor misst die Lufttemperatur in einem Bereich von -40 °C bis 85 °C mit einer Genauigkeit von ± 1 °C, die relative Luftfeuchtigkeit von 20-80 % mit einer Genauigkeit von 3 %, sowie den atmosphärischen Druck in einem Bereich von 300 Pa bis 1100 hPa mit einer Genauigkeit von ± 1 hPa.

Verkehr

Der Stadtverkehr gehört zu den größten Emissionsquellen urbaner Luftverschmutzungen [145]. Detaillierte Informationen über den Stadtverkehr sind von enormer Bedeutung, um Änderungen der urbanen Luftqualität zu analysieren. Zur Charakterisierung des urbanen Verkehrs können Informationen der Verkehrsintensität und Geschwindigkeitsmessungen einzelner Verkehrsteilnehmer dienen. Die Verkehrsintensität beschreibt die Anzahl der an einem Messstandort vorbeifahrenden Fahrzeuge pro Minute. Aus bisherigen Studien [146, 147] ist bekannt, dass eine erhöhte Verkehrsintensität zu einer erhöhten Schadstoffkonzentration führen kann. Zudem können variierenden Motorbelastungen durch Beschleunigungs- und Bremsvorgänge zu Änderungen der Schadstoffkonzentration führen [148].

Tabelle 4.2: Technische Eigenschaften der genutzten GPU und Kamera zu automatisierten Verkehrsanalyse

Komponente	**Technische Eigenschaften**	
NVIDIA Jetson Nano	Prozessor	ARM Cortex A57, 1.42 GHz
	GPU	128 CUDA cores, 472 GFLOPS
	Speicher	4 GB 64-bit LPDDR4
	Energieverbrauch	20 Watt
	Größe	100x80x29 mm
Raspberry Pi Camera V2.1	Bildsensor	Sony IMX219
	Auflösung	8 Megapixel
	Video	1080p @ 30 fps
	Größe	25x23,8x9 mm

Der SCN ermöglicht lokale Messungen der Verkehrsintensität und der Geschwindigkeiten einzelner Verkehrsteilnehmer zur Charakterisierung des urbanen Verkehrs. Alle Messungen werden direkt auf dem SCN durchgeführt. Im Wesentlichen wird hierzu eine Kamera zur Datenaufnahme und eine Grafikkarte (engl., Graphics Processing Unit, GPU) zur direkten Datenverarbeitung der aufgezeichneten Verkehrsbilder genutzt. Im Vergleich zu anderen Sensoren (vgl. Abschnitt 3.1) sind Kameras günstig in der Anschaffung, einfach zu warten und können für verschiedene Messszenarien konfiguriert werden. Die direkte Verarbeitung großer Datenmengen auf dem SCN folgt einem sog. „Edge Computing Prinzip“ und ermöglicht es sensible und personenbezogene Daten zur Verkehrsanalyse zu nutzen, ohne dabei die Privatsphäre der im öffentlichen und überwachten Raum befindlichen Personen zu gefährden. Eine dezentrale Datenverarbeitung auf verteilten Edge Geräten wie dem SCN führt zu geringeren Datenübertragungszeiten, zumal lediglich Ergebnisse der Verkehrsanalyse und keine Verkehrsvideos versendet werden. Die Videoverarbeitung auf dem SCN ist stark limitiert durch die verfügbaren Rechenressourcen. Viele Algorithmen zur echtzeitfähigen Videoverarbeitung benötigen teure Hardwarebeschleuniger und lassen sich auf kostengünstigen und ressourcen-limitierten Sensormodulen kaum nutzen.

Der SCN nutzt eine GPU als Hardwarebeschleuniger zur echtzeitfähigen Verkehrsanalyse. Beim der genutzten GPU handelt es sich um eine NVIDIA Maxwell mit einer Spitzenleistung von 472 GFLOPs, die auf einem Jetson Nano Board betrieben wird (vgl., Tabelle 4.2). Das Jetson Nano Board wurde speziell für Anwendungen entwickelt, bei denen die Kriterien Baugröße, Stromverbrauch und Anschaffungspreis von besonderer Bedeutung sind. Verglichen mit anderen Hardwarebeschleunigern, wie beispielsweise dem Jetson AGX Xavier Board oder dem Intel Movidius Neural Compute Stick, zeichnet sich das Jetson Nano Board durch eine gutes Verhältnis zwischen Hardwarebeschleunigung und Anschaffungskosten aus und wird in vielen Edge Computing Anwendungen genutzt [149, 150].

Die Verkehrsanalyse des SCN ist in unterschiedliche Prozessschritte unterteilt (siehe Abbildung 4.2). Zu diesen Prozessschritten gehören die Initialisierung, Detektion sowie Klassifizierung, Verfolgung und Geschwindigkeitsschätzung detektierter Verkehrsteilnehmern.

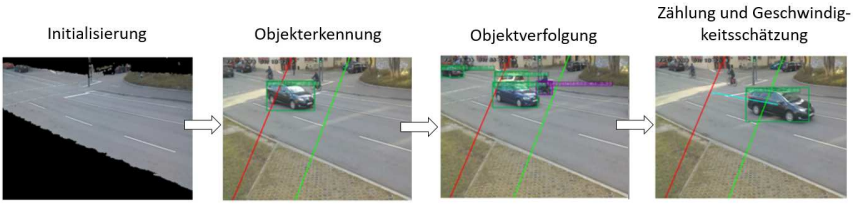

Abbildung 4.2: Prozessschritte zur kamerabasierten Verkehrsanalyse des Smart City Node (SCN)

Initialisierung

Der erste Prozessschritt der Initialisierung hat das Ziel die Region of Interest (ROI) eines Bildes automatisch zu bestimmen, um Verkehrszählungen und Geschwindigkeitsmessungen unterschiedlicher Verkehrsteilnehmer zu ermöglichen. Die Initialisierung startet mit einer Bildsegmentierung. Die Bildsegmentierung soll die zu analysierende Datenmenge reduzieren, um eine erhöhte Datenverarbeitungsgeschwindigkeit bzw. Verkehrsanalyse zu erzielen. Die genutzte Bildsegmentierung basiert auf der Annahme, dass sich bewegende Verkehrsteilnehmer ausschließlich auf Verkehrsstraßen befinden und ruhende Verkehrsteilnehmer nicht

in einer Verkehrsanalyse berücksichtigt werden müssen. Während der Verkehrsanalyse werden alle Bildsegmente ignoriert, in denen keine sich bewegenden Verkehrsteilnehmer identifiziert werden. Zur Bildsegmentierung wird ein Gaussian Mixture-Bases background/foreground Separator (MOG2) und K-nearest neighbour (KNN) background Separator verwendet [151]. Mit Hilfe dieser Separatoren wird ein statischer Bildhintergrund definiert. Zum Bildhintergrund gehören alle Bildsegemente in denen keine sich bewegenden Pixel erkannt wurden.

Anschließend wird vom Verkehrsmodul die Fahrbahnmarkierungen erkannt. Hierzu wird zunächst der Bildvordergrund in denen sich bewegende Pixel befinden, in einen Grauraum transformiert. Nach dieser Transformation werden alle nicht weißen Pixel identifizieren und vom Bildvordergrund gelöscht. Aufgrund der genormten Formen von Fahrbahnmarkierung ist es möglich, die weiß gefärbten Pixel entweder einem Cluster der Randstreifen mit durchgehenden Konturen oder einem Cluster der Fahrbahnmarkierung mit nicht durchgehenden Konturen zuzuordnen. Im Anschluss einer erfolgreichen Pixel- und Konturenerkennung sind die Koordinaten der erkannten Fahrbahnmarkierungen bekannt und können zu Definition der ROI genutzt werden. Die ROI ist als Fläche im Bild definiert, die Verkehrsteilnehmer zur Verkehrsanalyse passiert werden muss. Zur Bestimmung des ROI werden Koordinaten der detektieren Fahrspurmarkierung genutzt. Senkrecht zu den detektieren Fahrspurmarkierung werden zwei Linien definiert, die innerhalb des Bildvordergrunds die ROI definieren. Gemäß den genormten Abständen der detektieren Fahrspurmarkierungen beträgt der Abstand zwischen beiden Linien drei Meter.

Detektion und Klassifizierung

Für die Klassifizierung von Verkehrsteilnehmern im segmentierten Bildvordergrund wird ein Single Shot Detector (SSD) Model [152] genutzt, das auf einer MobileNetV2-Architektur [153] basiert. Unterschiedliche Studien [154, 155] haben zeigen können, dass auf Edge-Geräten mit begrenzten Rechenressourcen, SSD-MobileNet-Architekturen eine hohe Objekterkennungsgenauigkeit erzielen können. Das SSD Model wurde mit Hilfe eines öffentlich zugänglichen Datensatzes Common Objects in Context (COCO) trainiert [156]. Zusätzlich wurde

der Datensatz um weitere Trainingsbilder erweitert, um die Modellgenauigkeit zu verbessern.

Nach einem erfolgreichen Modelltraining wird für jede Aufnahme des segmentierten Bildvordergrunds eine Ausgabe generiert. Diese Ausgabe beinhaltet Bounding Boxen erkannter Objekten und einen Wahrscheinlichkeitsscore der Objektklassifikationsgenauigkeit. Mittels eines Non-Max Surppresion (NMS) Algorithmus werden anschließend mehrere Bounding Boxen um ein einzelnes Objekt zusammengeführt, um die Objekterkennungsgenauigkeit zu verbessern.

Objektverfolgung

Nach einer erfolgreichen Erkennung erfolgt die Objektverfolgung. In urbanen Verkehrssituationen, mit einer Vielzahl an Verkehrsteilnehmern, stellt eine verlässliche Objektverfolgung eine große Herausforderung dar. Vor allem Verdeckungen einzelner Objekte über mehrere Bilder hinweg, können Objektverfolgungen negativ beeinträchtigen. Der Simple Real Time Tracker (SORT) [157] Algorithmus wird häufig zur Objektverfolgung genutzt. Verglichen mit anderen Algorithmen zur Objektverfolgung, zeichnet sich der SORT Algorithmus vor allem durch eine effiziente Objektzuordnung aus. Der SORT-Algorithmus weist allen Objekten eine bestimmte ID zu und erstellt eine Liste der verfolgten Objekte, um trotz temporärer Verdeckungen eine verlässliche Objektverfolgung zu erzielen.

Geschwindigkeitsschätzung

Im letzten Teilprozess werden korrekt erkannte und über mehrere Bilder hinweg verfolgte Verkehrsteilnehmer gezählt. Detektierte Verkehrsteilnehmer werden vom Verkehrsmodul gezählt, sobald sie ein der beide ROI Linien passieren. Je nachdem welche Linie zunächst passiert wird, ist eine Zählung in beide Verkehrsrichtungen möglich. Fehlerhafte Zählungen einzelner Verkehrsteilnehmer, die auf einer einzelnen Linie verkehrsbedingt halten müssen und somit eventuell mehrfach gezählt werden, können durch den Einsatz einer ROI Fläche werden vermieden.

Zusätzlich zur Verkehrszählung erfolgt eine Geschwindigkeitsschätzung. Hierzu wird jedem erkannten Verkehrsteilnehmer beim Passieren einer der beiden ROI

Linie ein Zeitstempel zugewiesen. Anhand beider Zeitstempel die von Verkehrsteilnehmer beim Passieren beide ROI Linien erstellt werden und dem bekannten Abstand zwischen beiden ROI Linien bzw. Fahrbahnmarkierungen, erfolgt eine Geschwindigkeitsmessung. Diese Messung beruht auf der Annahme, dass Verkehrsteilnehmer beim Passieren des ROI Bereichs sich mit einer konstanten Geschwindigkeit fortbewegen.

4.1.2 Datenübertragung

Die Datenübertragungseinheit besteht aus einem High-Speed Packet Access (HSPA)-Modul (Huawei E3372) und einer 4G Außenantenne (B4BE 7-27-05SP) zur Verbesserung der Konnektivität. Drahtlose 4G Mobilfunknetze verfügen über eine geringe Kommunikationslatenz, eine hohe Netzwerkabdeckung und eine hohe Datenübertragungsrate, verglichen mit anderen drahtlosen Netzwerktechnologien wie beispielsweise SIGFOX.

Mit Hilfe des bandbreiten und energieeffizienten Message Queue Telemetry Transport (MQTT) Protokolls [158] werden Daten über drahtlose Mobilfunknetze übertragen. Aufgrund eines geringen Protokolloverhead wird MQTT vor allem in IoT Szenarien für die Übertragung kleiner Datenmengen verwendet, wohingegen bekannte Protokolle wie das Hyper Text Transfer Protocol (HTTP), vorzugsweise für die Sammlung großer Datenmengen in Big-Data-Anwendungen genutzt werden. Batteriebetriebene IoT-Geräte können über das MQTT-Protokoll geringe Datenmengen, wie beispielsweise Messwerte, deutlich schneller [159] und energieeffizienter [160] übertragen. Das MQTT-Protokoll unterstützt einen offenen, einfach einzurichtenden und skalierbaren Rollout von drahtlosen Sensornetzwerken, basiert auf einer Publish/Subscribe-Architektur, die mit einem Secure Sockets Layer (SSL) gesichert wird. Die Publish/Subscribe-Architektur basiert auf einem zentralen Server (MQTT-Broker), mit dem sich sowohl Sender als auch Empfänger von Nachrichten verbinden und Daten über sogenannte Topics senden (veröffentlicht) oder empfangen (abonniert). Zum Beispiel veröffentlicht der SCN Sensordaten in

einem bestimmten Topic, wie beispielsweise der Verkehrsbelastung. Server können Topics abonnieren, um die vom SCN generierten Messwerte zu empfangen. Auf diese Weise können Daten eines SCN mit einer Vielzahl unterschiedlicher Server bzw. Anwendungen geteilt werden.

4.1.3 Datenverarbeitung

Alle Sensordaten werden direkt auf dem SCN verarbeitet. Die Datenverarbeitungseinheit des SCN besteht aus einem Mikrocontroller zum Sammeln und Formatieren aller Messwerte und einem vertrauenswürdigen Hardwaremodul (Zymkey [161]) zum digitalen Signieren der generierten Daten. Die Datenverarbeitung beginnt mit dem periodischen Sammeln und Formatieren aller Messwerte. Alle Daten werden im Datenformat JavaScript Object Notation (JSON) mit Informationen über die Messung, Messeinheit, Sensorgeräteinformationen, Zeitstempel und Standort des SCN gespeichert. Auf diese Weise werden Daten in einem einheitlichen Datenformat und einer einheitlichen Struktur dargestellt. Die formatierten Daten werden von einem vertrauenswürdigen Hardwaremodul digital signiert. Zu digitalen Signatur nutzt das vertrauenswürdige Hardwaremodul den Elliptic Curve Digital Signature Algorithm (ECDSA) [162]. Der hierzu notwendige private Schlüssel befindet sich in einem manipulationssicheren Speicher des SCNs. Die Authentizität der Messwerte und Metadaten kann durch Prüfen digitaler Signaturen mit dem öffentlichen Schlüssel des sendenden SCN verifiziert werden.

Die Verarbeitung und das digitale Signieren von Daten direkt auf dem SCN hat den Vorteil, dass nicht autorisierte Personen einen direkten physischen Zugang benötigen, um Hardwaremodule des SCN zu manipulieren. Der SCN befindet sich an öffentlichen Orten und ein unbefugter Zugriff kann nicht vollständig ausgeschlossen werden. Daher wurden physische Manipulationserkennungsfunktionen des vertrauenswürdigen Hardwaremoduls aktiviert, um das Risiko eines unbefugten physischen Zugriffs auf den SCN zu minimieren. Diese vom Zymkey bereitgestellten physischen Manipulationserkennungsfunktionen umfassen die Erkennung von ungewöhnlichen Orientierungsänderungen und Erschütterungen durch einen

Beschleunigungssensor des Zymkey. Darüber hinaus wurde die Integritätsschaltungen des Zymkey aktiviert, um Schaltkreisunterbrechungen zu erkennen. Die Integritätsschaltung wurde an der Öffnung des SCN Gehäusedeckels platziert, um ein Öffnen des Gehäuses zu detektieren. Sollte eine unbefugte Person den SCN öffnen, und hierdurch die Integritätsschaltung unterbrechen (physikalische Zerstörung des Schaltkreises), werden alle auf dem Zymkey gespeicherten privaten Schlüssels des SCN gelöscht. Von diesem Moment an werden keine digital signierten Messwerte mehr versendet.

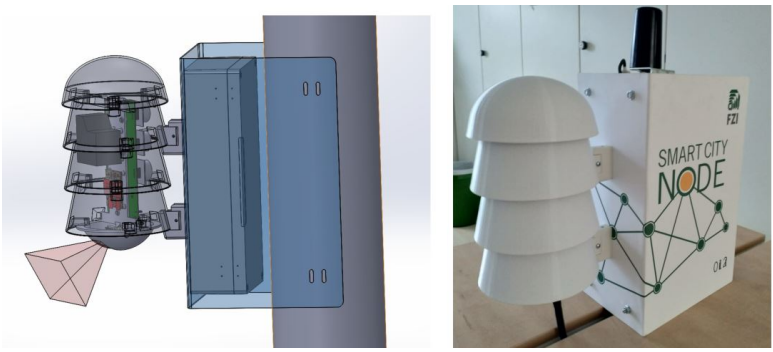

Abbildung 4.3: Konzeptionierter und implementierter Smart City Node (SCN)

4.1.4 Gehäuse

Alle Sensormodule sind in einem 3D-gedruckten Gehäuse untergebracht, das einer sogenannten Stevensonhülle ähnelt [163]. Die Stevensonhülle schützt die genutzte Elektronik gegen Witterungseinflüsse und ermöglicht zeitgleich eine gute Belüftung des Gehäuses. Die Abmessungen des 3D-gedruckten Gehäuses (Radius und Länge) betragen 12 cm x 21 cm (vgl., Abbildung 4.3).

Komponenten der Datenverarbeitung und Datenübertragung des SCN, sowie der Energieversorgung, sind in einem separaten und spritzwasserdichten Gehäuse untergebracht. Die von diesen Komponenten erzeugte Abwärme kann Messungen der genutzten Sensoren in der Stevensonhülle nicht beeinflussen. Zudem wird eine

unerwünschte Elektromagnetische Interferenz (EMI) zwischen den unterschiedlichen Komponenten vermieden.

4.2 Evaluierung

Evaluierungsmessungen sollen die Funktionstüchtigkeit des entwickelten SCN Prototypen untersuchen. Hierzu wurden unter realen Bedingungen diverse Messungen des SCN durchgeführt. Die durchgeführten Evaluierungsmessungen lassen sich in Kalibrierungsmessungen und weitere exemplarische Messungen unterteilen.

4.2.1 Kalibrierung

Die Genauigkeit der genutzten und entwickelten Sensoren kann durch Störungen, basierend auf Gasen oder aber schwankenden Umgebungsbedingungen, beeinträchtigt werden. Beispielsweise können stark schwankende Belichtungsverhältnisse die Messgenauigkeit einer kamerabasierten Verkehrszählung beeinflussen. Ohne ein angemessenes Verständnis der erzielten Messdatenqualität kann es zu fehlerhaften Analysen der Messungen kommen. Daten von unbekannter Qualität können zu falschen Entscheidungen führen, weshalb die Quantifizierung der Messwertunsicherheiten für das Verständnis von Messdaten unerlässlich ist.

Es existieren keine weltweit etablierten und standardisierten Protokolle zur Kalibrierung kostengünstiger Schadstoffsensoren. Eine gängige Strategie zur Kalibrierung besteht in einem Vergleich der Ungenauigkeit kostengünstiger Schadstoffsensoren mit präzisen, stationären Messstationen [164]. Für eine solche Feldkalibrierung unter realen Bedingungen wurde der SCN auf dem Dach einer stationären Messstation in Augsburg installiert (vgl., Abbildung 4.4a).

Die stationäre Messstation am Königsplatz in Augsburg zur Überwachung der urbanen Luftqualität ist als verkehrsbezogene Messstation ausgewiesen. Die Messstation liegt in einer breiten Straßenschlucht (vgl., Abbildung 4.4b).

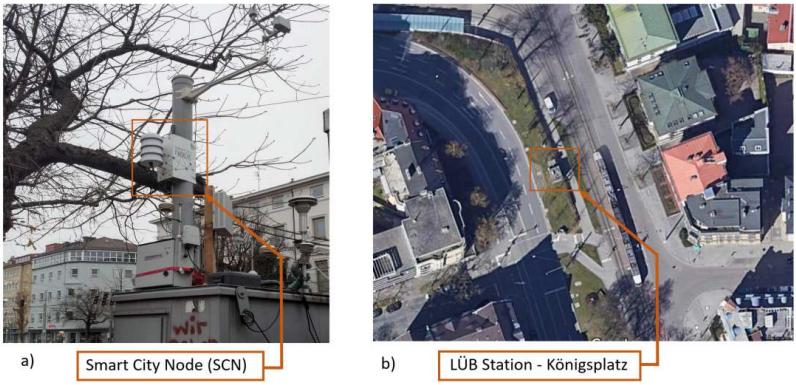

Abbildung 4.4: Feldkalibrierung des SCN am Königsplatz Augsburg

Die im SCN genutzten kommerziellen Gassensoren wurden vom Hersteller im Labor kalibriert. Es gibt jedoch keine Garantien, dass die Spezifikationen der Sensoren unter realen Bedingungen eingehalten werden können. Verschiedene Studien haben gezeigt, dass die Genauigkeit von Schadstoffsensoren aufgrund von Änderungen der Umweltbedingungen erheblich schwankt [165, 166]. Zur Bewertung dieser Schwankungen wurde eine Feldkalibrierung mittels der stationären Messstation am Königsplatz in Augsburg [164] durchgeführt. Ziel der Feldkalibrierung ist es, eine erhöhte Messgenauigkeit der eingesetzten Sensoren zu erzielen. Hierzu wurden die vom Hersteller AlphaSense gelieferten Werte der Elektrodenspannung (vgl. Gleichung 4.1) anhand stündlicher Messwerte der stationären Messstation korrigiert. Mit Hilfe von Ausgleichsrechnungen (Parameter-Fitting) wurden die Werte der Elektrodenspannung neu bestimmt, um für den gewählten Messstandort und Zeitraum die Sensorgenauigkeiten des SCN erhöht. Beispielsweise konnte die Wurzel der mittleren Fehlerquadratsumme (engl., Root Mean Square Error, RMSE) des NO2 Sensors von 12,9 auf 8,4 $\mu g/m^3$ reduziert werden (siehe Abbildung 4.5).

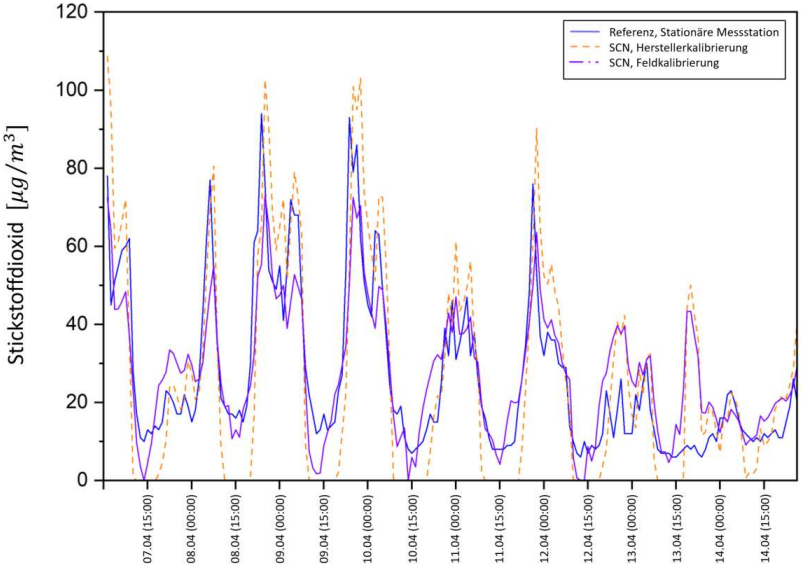

Abbildung 4.5: Kalibrierungsmessungen des Stickstoffdioxidsensors am Königsplatz in Augsburg

Die erzielte Sensorgenauigkeit der CO, NO2 und PM Sensoren wurde nach der durchgeführten Feldkalibrierung mit Hilfe eines Determinationskoeffizient (R^2) bestimmt. Das R^2 ist ein Maß für die Güte linearer Regressionsmodelle und kann einen Wert von Null bis Eins annehmen. Je größer R^2, desto besser stimmen die Messungen des SCN mit den Referenzmessungen der stationären Messstation am Königsplatz überein. Die Bewertung der Sensorgenauigkeit für den ausgewählten Messstandort und Zeitraum zeigte, dass die erzielten Sensorgenauigkeiten des SCN nicht mit Werten bisheriger Veröffentlichungen übereinstimmen (vgl. Tabelle 4.3).

Die dargestellten R^2 Koeffizienten unterschiedlichster Veröffentlichungen repräsentieren exemplarische Vergleichswerte ähnlicher Messungen. Es gilt zu beachten, dass R^2 Koeffizienten eines Sensors von einer Reihe verschiedener Kalibrierungsspezifikationen abhängen, die einen direkten Vergleich unterschiedlicher Kalibrierungsmessungen erschweren. Zu diesen Spezifikationen gehören beispielsweise die Dauer der Messungen, Jahreszeit und der Messstandort.

Tabelle 4.3: Übersicht der erzielten Sensorgenauigkeiten (R^2) nach einer Feldkalibrierung am Königsplatz

Schadstoffe	Smart City Node	Stand der Technik
CO	0,49	0,79 [167]
NO2	0,67	0,82 [168]
PM10	0,65	0,71 [169]

Die durchgeführten Kalibrierungsmessungen (vlg., Tabelle 4.3 verdeutlichen, dass der SCN mit Hilfe seiner kostengünstigen Schadstoffsensoren vor allem zur Detektion signifikanter Konzentrationsänderungen geeignet ist und sind nicht zur Überwachung von Grenzwerten nutzen lässt.

Zusätzlich zu den Kalibrierungsmessungen der kommerziellen Schadstoffsensoren, erfolgte eine Kalibrierung des eigens entwickelten Verkehrsmoduls, zumal wechselnde Umgebungsbedingungen und Verkehrssituationen die Verlässlichkeit einer kamerabasierten Verkehrsanalyse beeinflussen [170]. Beispielsweise können die über den Tagesverlauf wechselnde Lichtverhältnisse sich negativ auf die Verlässlichkeit einer bilderbasierten Verkehrszählung auswirken. Zur Kalibrierung des entworfenen Verkehrsmoduls wurden Kalibrierungsmessungen für unterschiedliche Kamerasichtfelder, Verkehrsdichten und Sichtverhältnisse durchgeführt. Die Verlässlichkeit einer Verkehrszählung wurde anhand der Genauigkeit (engl., accuracy) definiert. Die Genauigkeit bestimmt den prozentualen Unterschied zwischen von SCN gezählten Verkehrsteilnehmern zu manuell gezählten Verkehrsteilnehmern. Aufgrund der Möglichkeit, dass sich False Positive (FP) und False Negative (FN) Zählungen gegenseitig kompensieren, wird neben der Genauigkeit noch die Wiedererkennung (engl., Recall) einer Verkehrszählung mitberücksichtigt.

Unterschiedliche Kameraausrichtungen führen zu unterschiedlichen Kamerasichtfeldern. Anhand von drei Kameraausrichtungen wurde der Einfluss unterschiedlicher Sichtfelder auf die Zuverlässigkeit der Verkehrszählung bewertet (siehe Abbildung 4.6).

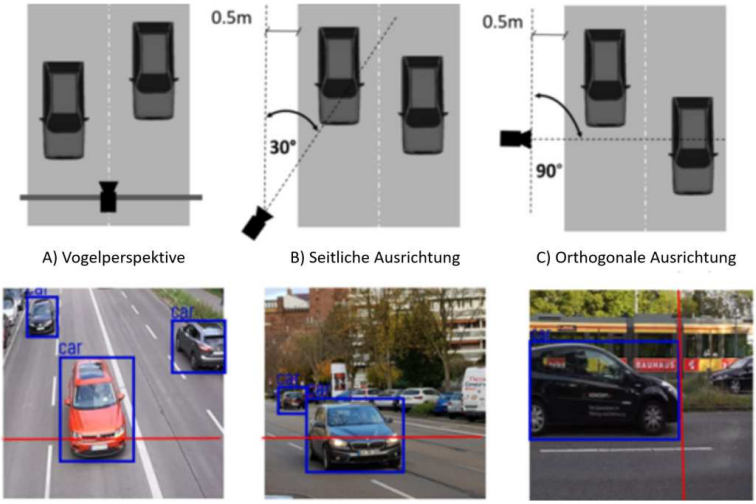

Abbildung 4.6: Unterschiedliche Kameraausrichtungen des SCN zur Kalibrierung des Verkehrsmoduls

Die durchgeführten Verkehrszählungen unterschiedlicher Kameraausrichtung haben zeigen können, dass das Sichtfeld einen hohen Einfluss auf die Verlässlichkeit einer Zählung hat. Zählungen aus der Vogelperspektive (vgl., Abbildung 4.6) erfolgten mit einer sehr hohen Genauigkeit von 99 % und einem Recall von 99 %. Aus dieser Perspektive betrachtet, ist die relative Größe der Fahrzeuge in der Nähe der genutzten ROI Linie am größten, wodurch eine hohe Zählgenauigkeit erzielt wird. Für die Kameraausrichtung aus einer weiteren Position B (siehe Abbildung 4.6) wurde eine hohe Genauigkeit von 99 % bei einer geringeren Wiedererkennung von 93 % gemessen. Verglichen mit der vorherigen Kameraausrichtung, werden dem Verkehrsmodul durch die Kameraausrichtung B weniger Bilder zur Zählung bereitgestellt, wodurch die Verlässlichkeit der Verkehrszählung beeinflusst wird. Vor allem die Kameraausrichtung der Position C (vgl., Abbildung 4.6) hat einen großen Einfluss auf die Verlässlichkeit der Verkehrszählung, zumal mit einer Abtastrate von 20 fps kaum Bilder mit Fahrzeugen zur korrekten Verkehrszählung aufgenommen werden. Eine hohe relative Objektgeschwindigkeit ist zurückzuführen auf ein stark limitiertes Sichtfeld der Kamera

bzw. einer vertikalen Ausrichtung und einem geringen Abstand der Kamera zur Straße.

Die Verkehrsdichte schwankt je nach Tageszeit und kann durch die Anzahl der simultan zu erkennenden Objekte einen Einfluss auf die Verlässlichkeit der Verkehrszählung haben. Aus der Vogelperspektive wurde untersucht, wie sich die Anzahl der simultan zu verfolgenden Verkehrsteilnehmer auf eine Verkehrszählung auswirkt. Die erzielten Ergebnisse belegen, dass die Verarbeitungszeit für eine Objekterkennung mit der Anzahl der Objekte pro Bild zunimmt. Beispielsweise wurde eine Verarbeitungszeit von 0,14 s benötigt, um 24 Verkehrsteilnehmer simultan auf einem Bild zu identifizieren und zu zählen. Im Vergleich hierzu, lag die zum Zählen von vier Verkehrsteilnehmern pro Bild benötigte Verarbeitungszeit bei 0,10 s. Aufgrund einer effizienten Datenverarbeitung ist es dem SCN möglich, Verkehrsszenarien mit einer hohen Anzahl an Verkehrsteilnehmern verlässlich zu analysieren.

Im urbanen Umfeld ist der SCN unterschiedlichen Sichtverhältnissen ausgesetzt, die sich auf die Verlässlichkeit der Verkehrszählung auswirken können [171]. Ein Vergleich der Verkehrszählungen an einem sonnigen Nachmittag mit Zählungen bei Sonnenuntergang hat zeigen können, dass mit einer Abnahme der Belichtungsverhältnisse die Zählgenauigkeit um 24 % und der Recall um 18% abnimmt. Eine geringere Verlässlichkeit der Verkehrszählung ist darauf zurückzuführen, dass sich bei schlechten Belichtungen die Objektformen der Verkehrsteilnehmer nicht verlässlich erkennen lassen. Beispielsweise sind bei schlechten Sichtverhältnissen vor allem die Scheinwerfer diverser Verkehrsteilnehmer erkennbar, aber nicht deren zur Identifikation notwendige Konturen.

4.2.2 Messungen

Direkt an der stationären Messstation am Königsplatz in Augsburg wurde unterschiedliche Messungen des SCN durchgeführt. Ziel der durchgeführten Messungen ist es, die Funktionsfähigkeit des entwickelten Prototyps unter realen Bedingungen nachzuweisen.

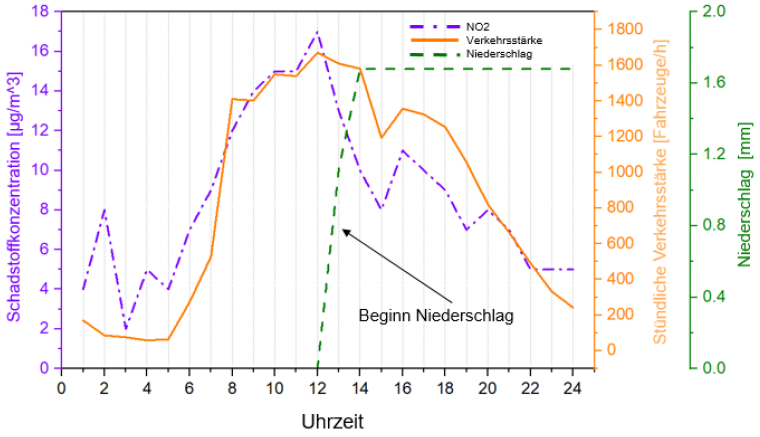

Abbildung 4.7: Stündlicher Verlauf der Schadstoffkonzentration NO2, Verkehrsstärke und Niederschlags

Im Messzeitraum wurden vor allem nach Korrelationen zwischen der Verkehrsstärke, meteorologischen Parametern (Niederschlag, Windgeschwindigkeit) und Schadstoffkonzentrationen (NO2, PM10) gesucht. Messungen des SCN zeigen eine typische Verkehrszunahme in den Morgenstunden und eine Verkehrsabnahme am späten Nachmittag. Zudem ist zu erkennen, dass die lokale NO2 Schadstoffbelastung durch lokalen Niederschlag reduziert wird (vgl., Abbildung 4.7). Es ist anzunehmnen, dass der Niederschlag die NO2 Konzentration in der Atmosphäre reduziert.

In diesen Messungen ist zudem zu erkennen, wie ein Anstieg der lokalen Windgeschwindigkeit die Feinstaubkonzentration reduzieren kann (vgl., Abbildung 4.8).

Anstatt einen Anstieg der Feinstaubbelastung analog zum Anstieg der Verkehrsstärke zu beobachten, sinkt die gemessene Feinstaubkonzentation. Informationen zur Windgeschwindigkeit am SCN legen nahe, dass sich durch eine erhöhte Windgeschwindigkeit der von vorbeifahrenden Fahrzeugen emittierte Feinstaub besser in der Atmosphäre verteilt.

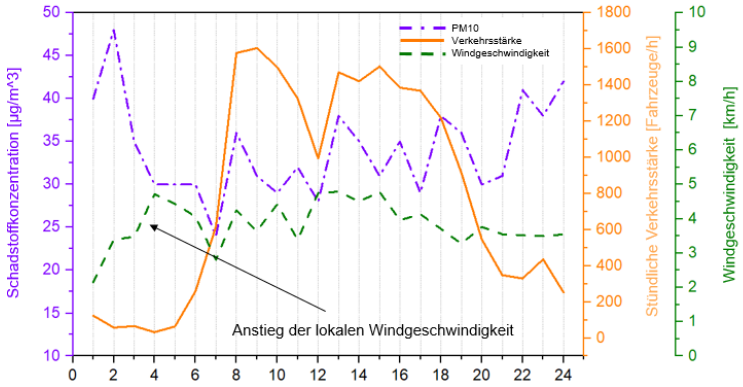

Abbildung 4.8: Stündlicher Verlauf der Schadstoffkonzentration PM10, Verkehrsstärke und Windgeschwindigkeit

Weitere Messungen an unterschiedlichen Standorten und Jahreszeiten sind erforderlich, um Korrelationen zwischen Verkehrsdichten, Schadstoffkonzentrationsänderungen und meteorologischen Parametern verlässlich untersuchen zu können.

Eine wichtige Komponente des SCN ist das eigens entwickelte Verkehrsmodul. Mit Hilfe dieses Moduls wurde das tägliche Verkehrsaufkommen am Messstandort untersucht . Neben der Verkehrsstärke bestimmt das Verkehrsmodul des SCN ebenfalls die durchschnittliche Geschwindigkeit vorbeifahrender Fahrzeuge (vgl., Abbildung 4.9).

Für den untersuchten Straßenabschnitt ist eine maximale Geschwindigkeit von 50 km/h zulässig. Gemäß den durchgeführten Geschwindigkeitsmessungen, liegt die durchschnittliche Fahrzeuggeschwindigkeit knapp unterhalb der maximal zulässigen Geschwindigkeit . Diese Ergebnisse deuten darauf hin, dass für den beobachteten Straßenabschnitt die Verkehrsteilnehmer die zulässige Geschwindigkeit nicht immer erreichen können. Beispielsweise kann ein steigendes bzw. sehr hohes Verkehrsaufkommen zu gegenseitigen Behinderungen führen.

Die mit Hilfe des SCN durchgeführten Verkehrsanalysen können zur Kategorisierung von Verkehrsbereichen genutzt werden. Die Portabilität des SCN ermöglicht

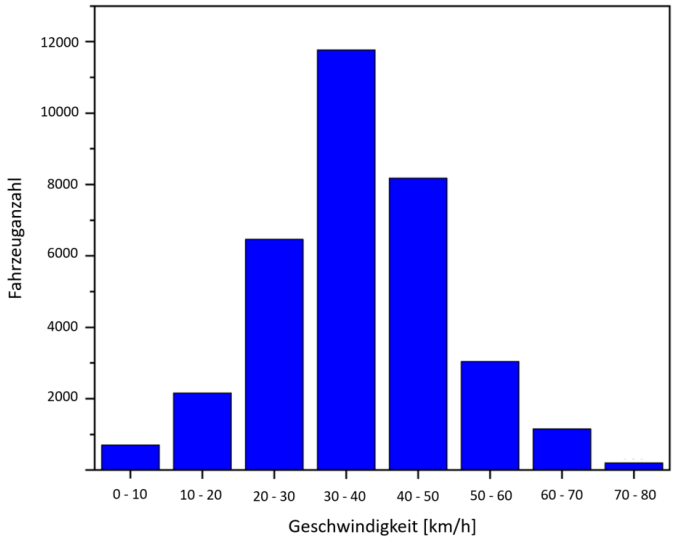

Abbildung 4.9: Geschwindigkeitsverteilung analysierter Verkehrsteilnehmer

es, flexibel bestimmte Straßenabschnitte zu analysieren, um beispielsweise den Einfluss straßenbaulicher Änderungen auf das Verkehrsverhalten zu untersuchen.

5 Pollution Monitoring System

Dieses Kapitel befasst sich mit der zweiten Fragestellung dieser Arbeit und soll aufzeigen, wie sich die Vorteile DLT basierter Infrastrukturen mit portablen Sensormodulen kombinieren lassen. Hierzu wurde ein eines dezentralen Überwachungssystems für Umweltverschmutzung (engl. Pollution Monitoring System) entworfen und evaluiert werden. Basierend auf einer umfassenden Literaturrecherche wurden zunächst Anforderungen an ein dezentrales Pollution Monitoring Systems (PMS) ermittelt. Anhand der ermittelten Anforderungen erfolgte eine Konzeptionierung und prototypische Implementierung eines DLT basierten PMS. Die Dimensionierung des PMS beruht auf einem Benchmark unterschiedlicher digitales Signaturverfahren und Konsensusmechanismen. Zur Evaluierung des PMS wurden unterschiedliche Messungen am implementierten Prototypen durchgeführt.

Die Ergebnisse dieses Kapitels stammen aus wissenschaftlichen Veröffentlichungen [1J, J3] des Autors in Zusammenarbeit mit weiteren Co-Autoren.

5.1 Anforderungen

Die ermittelten Anforderungen an ein PMS mit portablen Sensormodulen basieren auf einer umfassenden Literaturrecherche. Die durchgeführte Literaturrecherche hat wissenschaftliche Forschungsergebnisse analysiert, die sich mit Zielen, Herausforderungen und Best Practices bei der Entwicklung eines PMS mit portablen

Sensormodulen befassen. Der Stand der Technik und Forschung bildet die Grundlage der ermittelten funktionalen und nicht-funktionalen Anforderungen eines PMS.

Aus funktionaler Sicht sollte das PMS Messwerte von verteilten, portablen Sensormodulen sammeln und verarbeiten [28, 172]. Das PMS sollte ausschließlich Messungen von autorisierten Sensormodulen verarbeiten. Ein Identitätsmanagement für Sensormodule und Betreiber des PMS ist notwendig, um es Sensormodulen zu ermöglichen, sich beim PMS an bzw. abzumelden [173]. Zudem sollten aufgezeichnete Sensordaten über die urbane Luftqualität bzw. Schadstoffkonzentration, den Bürgern zugänglich gemacht werden. Neben Sensormodulen sollen auch Organisationen oder Personen ihre Identität nachweisen, sofern sie sich am Aufbau und Betrieb eines PMS beteiligen möchten. Bürgern sollte es ebenfalls möglich sein zu erfahren, welche aufgezeichneten Sensordaten von welcher Organisation des PMS bereitgestellt wurden.

Zur Bestimmung der Nicht-funktionalen Anforderungen wurden Forschungsergebnisse gemäß gängiger Methoden [174, 175] analysiert. Forschungsergebnisse aus den bekannten wissenschaftlichen Datenbanken der ACM DigitalLibrary, EBSCOhost, IEEEXplore, ProQuest und ScienceDirecet, wurden anhand eines Suchstring durchsucht. Der genutzte Suchstring bestand aus den folgenden Suchbegriffen, („WSN* OR LPWAN* OR sensor* OR network*“) und („blockchain* OR ’distributed ledger technology*“). Anhand dieses Suchstrings wurden 217 Dokumente gefunden, von denen 16 Duplikate und 155 inhaltlich nicht relevante Dokumente ausgeschlossen wurden. Die übrigen relevanten Dokumente wurden mittels einer offenen und axialen Kodierung analysiert. Die offene Kodierung bestand in der Auflistung der Ziele und Anforderungen relevanter Dokumente. Wurde beispielsweise in einer wissenschaftlichen Veröffentlichung ein hohes Maß nachweisbarer Datenintegrität durch digitale Signaturen anstrebten, wurde zu dieser Veröffentlichung die Anforderung einer hohen Integrität notiert. Die axiale Kodierung bestand in Berücksichtigung von Gründen und Konsequenzen identifizierte Anforderungen, um ähnliche Anforderungen miteinander zu verknüpften. Beispielsweise wurden die Anforderungen Integrität [176] und Unveränderlichkeit [177] zu der Anforderung Integrität [178] zusammengefasst. In

Tabelle 5.1: Nicht funktionale Anforderung an ein PMS.

Genauigkeit	Das PMS sollte Messdaten mit einer Genauigkeit erfassen, die den Mindestanforderungen beabsichtigter Analysen entsprechen.	[179]
Verfügbarkeit	Der gewählte Distributed Ledger des PMS sollte mit einer sehr hohen Wahrscheinlichkeit zu jedem Zeitpunkt funktionieren.	[178]
Bandbreite	Die maximale Bandbreite sollte ausreichen, um allen im PMS angeschlossenen Geräten eine Übertragung von Sensornachrichten zu ermöglichen.	[180]
Zensurresistenz	Konsortiumsmitglieder im PMS sollten andere Konsortiumsmitglieder nicht absichtlich daran hindern können, mit dem PMS zu interagieren.	[178]
Energieverbrauch	Der Energieverbrauch der portablen, batteriebetriebenen Sensormodule sollte gering sein, um für eine erforderliche Messperiode die verteilten Module mit Energie zu versorgen	[181]
Unabhängigkeit	Alle Komponenten des PMS sollten unabhängig von proprietärer Hardware und Software sein.	[178]
Integrität	Übermittelte und im Distributed Ledger gespeicherten Daten sollten gegen unbefugte (oder unbeabsichtigte) Änderung oder Löschung geschützt sein.	[176]
Nachweisbarkeit	Konsortiumsmitglieder ist es nicht möglich Informationen zu manipulieren.	[182]
Portabilität	Konsortiumsmitglieder können das PMS flexibel und unabhängig von Umgebungsbedingungen einrichten und betreiben.	[183]
Zuverlässigkeit	Trotz beliebiger Ausfälle sollte das PMS Sensornachrichten ohne Inkonsistenzen verarbeiten und speichern.	[184]
Skalierbarkeit	Effizienter Umgang des PMS mit einer abnehmenden oder zunehmenden Anzahl an benötigten Ressourcen.	[180]
Durchsatz	Die maximale Anzahl der erwarteten Sensornachrichten pro Sekunde sollte vom PMS verarbeitet werden.	[180]
Transparenz	Die gespeicherten Sensornachrichten, Sensormodule und Eigentümer der Sensormodule sollten im PMS sichtbar sein und den entsprechenden Identitäten zugeordnet werden.	[184]

der Tabelle 5.1 sind alle 13 identifizierten nicht-funktionale Anforderungen eines dezentralen PMS gelistet.

5.2 Architektur mit portablen Sensormodulen

Das PMS besteht im Wesentlichen aus vier technischen Komponenten: Sensormodul, Gateway, einer PKI und einem Distributed Ledger (vgl. Abbildung 5.1). Das PMS wird aus einem Konsortium unterschiedlicher Organisationen, Unternehmen und Bürgern aufgebaut und betrieben. Keine einzelne Organisation kontrolliert zu keinem Zeitpunkt das gesamte PMS. Zur Teilnahme am PMS muss sich jedes Konsortiumsmitglied zunächst in der PKI registrieren. Durch eine transparente Verwaltung der Identitäten der Sensormodule, sowie Konsortiumsmitglieder, wird eine hohe Datenintegrität und Nachweisbarkeit erzielt [185]. Im Anschluss einer erfolgreichen Registrierung kann jedes Konsortiumsmitglied seine registrierten Sensormodule im städtischen Gebieten positionieren und Messwerte der urbanen Luftqualität erfassen. Die Sensormodule signieren nach jedem Messintervall die gesammelten Messwerte. Digital signierte Messwerte werden über drahtlose Netzwerke an umliegende Gateways gesendet, um anschließend an DLT-Knoten eines Distributed Ledger weitergeleitet zu werden. Digitale Signaturen empfangener Messwerte werden von DLT-Knoten durch einen Smart-Contract überprüft. Messwerte mit gültigen digitalen Signatur werden in Distributed Ledger gespeichert. Die im Distributed Ledger gespeicherten Messwerte stehen alle Konsortiumsmitgliedern zur Verfügung. Zudem werden alle Messwerte über eine Programmierschnittstelle (engl., application programming interface, API) eines jeden Konsortiumsmitglieds, veröffentlicht.

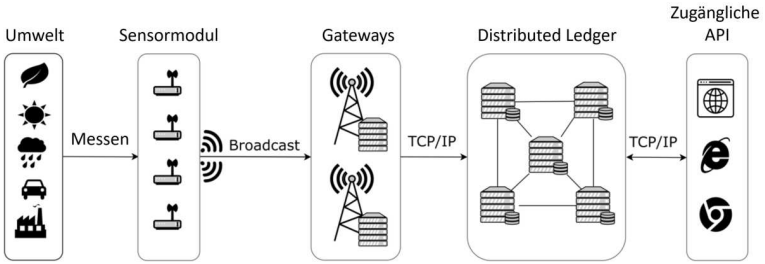

Abbildung 5.1: Schematische Darstellung der PMS-Architektur

5.3 Design und Implementierung

Viele Faktoren, wie beispielsweise Umwelteinflüsse und Software- oder Hardwarefehler, können das Verhalten des PMS beeinflussen und lassen sich nur schwer durch mathematische Modelle beschreiben [186]. Die Evaluierung des PMS bezüglich der ermittelten Anforderungen (vgl. Tabelle 5.1) erfolgt anhand von experimentellen Messungen eines implementieren Prototypen der vorgestellten PMS-Architektur. Zur Implementierung wurden batteriebetriebene Sensormodule, digitale Signaturen, das offene LoRa Kommunikationsprotokoll, LoRa Gateways und ein Distributed Ledger genutzt. Bestehenden Empfehlungen [187] zur Dimensionierung eines PMS zur Überwachung der urbanen Luftqualität, wie beispielsweise der Festlegung eines Messintervalls, wurden berücksichtigt.

5.3.1 Sensormodul

Für die Implementierung des PMS wurde nicht der SCN genutzt, sondern ein eigens entwickeltes und sehr kostengünstiges Sensormodul geringerer Funktionalität. Der Fokus der Evaluierung des PMS liegt nicht auf der Datenerfassung bzw. der Messung diverser urbaner Parameter, sondern vielmehr auf der verlässlichen Datenverarbeitung von Messdaten verteilter Sensormodule.

Die für das PMS eigens entwickelten Sensormodule besteht im Wesentlichen aus fünf Komponenten, einem Sensor zur Erfassung physikalischer Größen, einem Mikrocontroller zur Datenverarbeitung, einer Energieversorgung, einer Einheit zur drahtlosen Datenübertragung und Peripheriegeräten wie einem GPS-Modul (siehe Abbildung 5.2). Auf einem Mikrocontroller (MCU) werden alle Daten lokal verarbeitet. Ein GPS-Modul dient zur Lokalisierung der Sensormodule und ein LPWAN-Chip zur drahtlosen Übermittlung der Sensornachrichten. Der Mikrocontroller eines jeden Sensormoduls besteht aus einem ESP32-MCU [188]. Verglichen mit anderen Mikrocontroller zeichnet sich der ESP32 vor allem durch geringe Anschaffungskosten und einen geringen Stromverbrauch aus. Zur Messung

der Umweltparameter nutzt das Sensormodule einen kostengünstigen Feinstaubsensor (Nova SDS011) sowie einen Feuchtigkeit- und Temperatursensor (Grove DHT22). Informationen zum jeweiligen Messstandort und Messzeitpunkt werden vom Mikrocontroller mit Hilfe eines angeschlossenen GPS-Moduls (Ublox Neo-6M) ermittelt. Anschließend werden alle Messwerte mit dem privaten Schlüssel eines jeden Sensormoduls digital signiert. Die hierzu genutzten privaten Schlüssel werden in einem verschlüsselten Speicher (eFuse) des Mikrocontrollers gesichert. Mit Hilfe der LPWAN-Technologie werden signierten Sensornachrichten energieeffiziente vom Sensormodul an alle umliegenden Gateways übertragen. Hierzu nutzt das Sensormodul einen LPWAN-Chip (Semtech LoRa Transceiver SX1276), der mit einer externen angebrachten Antenne eine Datenübertragungsreichweite von bis zu 10 km erzielen kann.

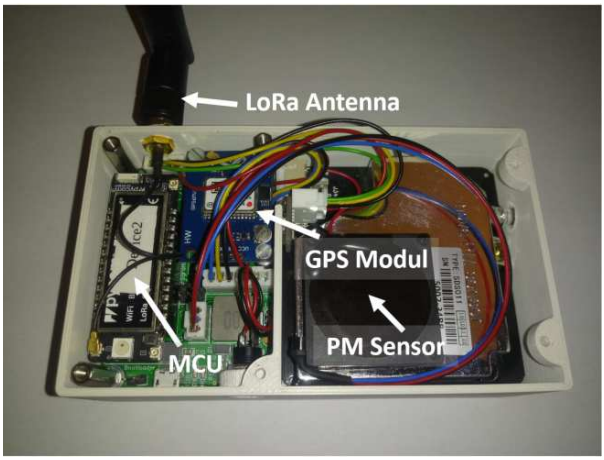

Abbildung 5.2: Portables Sensormodul zur Evaluierung des PMS

Messungen zur Überwachung der Luftqualität erfolgen meist im öffentlichen Raum und ermöglichen nicht autorisierten Person einen freien Zugriff auf die Software und Hardware verteilter Sensormodule. Ein freier Zugriff auf Sensormodule kann die Authentizität der ermittelten Messdaten und damit des gesamten PMS gefährden. Der zum digitalen Signieren von Messdaten notwendige private

Schlüssel eines Sensormoduls, wird durch eine Flash-Verschlüsselung auf dem Modul vor möglichen Manipulationen geschützt. Der zur Flash-Verschlüsselung genutzte Advanced Encryption Standard (AES)-Schlüssel, wird in einer elektronischen Fuse (eFuse) des Mikrocontrollers gespeichert. Bei der eFuse handelt es sich um einen einmalig programmierbaren Speicher. Änderungen der innerhalb einer eFuse gespeicherten AES-Schlüssel, sind nach einer Aktivierung der Flash-Verschlüsselung nicht möglich [189]. Unbefugte haben somit keinen Zugriff auf sensible Daten, wie beispielsweise einen privaten Schlüssel eines Sensormoduls. Zusätzlich werden Sensormodule durch das Aktivieren eines gesicherten Boot Prozesses (engl. Secure Boot) des Mikrocontrollers vor nicht autorisierten Manipulationen geschützt. Der Secure Boot Prozess prüft kryptografisch alle vom Mikrocontroller auszuführenden Programme [190]. Durch das Signieren und Verifizieren von Programmen, können Manipulationen erkannt und dessen Ausführung vermieden werden [191].

5.3.2 Drahtlose Datenübertragung

Kommunikationsprotokolle

Im IoT werden zur energieeffizienten, drahtlosen Übertragung kleiner Datenmengen innerhalb geringer Reichweiten von 1 bis 10 km, häufig drei Low Power Wide Area (LPWA)-Technologien genutzt. Zu diesen Technologien zählen NB-LTE, Sigfox und LoRa [192]. NB-LTE nutzt ein lizenziertes Frequenzband, um Daten ohne wesentliche Einschränkungen zu übertragen. Die Datenübertragung innerhalb eines lizenzierten Spektrums gilt als zuverlässig, verglichen mit der Übertragung in einem nicht lizenzierten Spektrum [193]. Das NB-LTE Protokoll nutzt ein Random-Access Verfahren, bei dem die Datenübertragung nicht von einer zentralen Einheit vollständig verwaltet wird. Im Vergleich zu Technologien wie LoRa, die nicht lizenzierte Spektren nutzen, verbraucht diese Verfahren zusätzliche Energie [194] und ist damit für den Aufbau eines PMS mit batteriebetriebenen Sensormodulen nicht geeignet.

LoRa und Sigfox nutzen unlizenzierte ISM Frequenzbänder zur Datenübertragung. Die Übertragung geringer Datenmengen über viele Kilometer via LoRa oder Sigfox ist frei von Gebühren. Verglichen mit LoRa, ist bei der Sigfox Technologie die Uplink-Datenrate und maximale Datengröße limitiert. Diese Limitierungen erhöhen die Übertragungsreichweite und verringert den zur Übertragung notwendigen Energieverbrauch. Aufgrund der limitierten Größe übertragbarer Nachrichten von 16 Bytes, ist Sigfox für das konzeptionierte PMS nicht geeignet. Die von den Sensormodulen zu übertragenden Sensornachrichten haben eine Größe von 121 Bytes. Von allen dargestellten Technologien (siehe Tabelle 5.3) ist LoRa am besten für den Aufbau des skizzierten PMS (siehe Abbildung 5.1) geeignet. Zur Kommunikation in urbanen Gebieten wird eine vordefinierte LoRa Konfiguration mit einem Spreizfaktor von neun; einer Coderate von eins und einer Bandbreite von 250 kHz, genutzt [195].

Das Messintervall der Sensormodule hat einen großen Einfluss auf die Dimensionierung des PMS. Beispielsweise bestimmt die Häufigkeit der Messungen den Energieverbrauch des Sensormoduls. Das Messintervall zur Bestimmung der urbanen Luftqualität kann von einer Messung pro Minute [196] bis hin zu einer Messung pro Stunde [197] variieren und wird bestimmt durch die Wahrscheinlichkeit einer Überschreitung der lokalen Schadstoffbelastung [198]. Zur Überwachung urbaner Luftverunreinigungen wurde ein Messintervall von fünf Minuten gewählt.

Netzwerkarchitektur

Tabelle 5.3: Vergleich unterschiedlicher LPWAN-Protokolle [194].

Kriterium	NB-LTE	Sigfox	LoRa
Uplink Datenrate	20 kB/s	100 B/s	300 B/s-50 kB/s
Max. Datengröße	1600 B	12 B	243 B
Reichweite	1 km	10 km	2 bis 5 km
Private Netzwerke	No	No	Yes
ISM band	No	Yes	Yes
Limitierungen	No	Yes	Yes

Low Power Wide Area Netzwerk (LPWAN) gehört zu einer Klasse von Netzwerkprotokollen, mit der sich batteriebetriebenen Sensormodule, Gateways, Netzwerkserver und Anwendungsserver verbinden lassen. LoRaWAN gehört zu den bekanntesten Kommunikationsprotokollen der LPWANs. Die Sensormodule nutzen LoRaWAN, um energieeffizient mit umliegenden Gateways zu kommunizieren. Stationäre Gateways senden empfangene Messwerte anschließend über das Transmission Control Protocoll (TCP) und das Internetprotokoll (IP) an Netzwerkserver. Netzwerkserver authentifizieren empfangene Messwerte, bevor sie diese an Anwendungsserver senden. Somit werden nur Daten von registrierten Sensormodule von Anwendungsservern, wie beispielsweise einem Distributed Ledger, verarbeitet [199].

Die sich zwischen Gateways und Anwendungsservern befindlichen und meist öffentlichen Netzwerkserver vieler LoRaWAN, wie beispielsweise dem The Things Network, werden in der Regel von privaten Organisationen betrieben. Öffentliche Netzwerkserver sind in der Lage, Messwerte von Sensormodulen zurückzuweisen bzw. nicht weiterzuleiten. Aufgrund eines potenziellen Verlustes der Datenintegrität durch Netzwerkserver [200], sollten öffentliche und bereits verfügbare LoRaWANs nicht zum Aufbau eines verlässlichen PMS genutzt werden. Zur vollständigen Kontrolle der Netzwerkkommunikation wird ein eigenes Netzwerk aufgebaut, bestehend aus Sensormodulen, Gateways und Anwendungsservern. Jedes Konsortiumsmitglied kann individuell ein eigenes LoRaWAN einrichten, um Messwerte von Sensormodulen über Gateways direkt an den Anwendungsserver bzw. einen Distributed Ledger zu senden.

Digitale Signaturen

Die Authentizität von Daten wird anhand von digitalen Signaturen verifiziert. Die Erstellung und Validierung von signierten Daten erhöht den Energieverbrauch aufgrund rechenintensiver Operationen. Zur Dimensionierung des PMS wurden unterschiedliche Signaturalgorithmen untersucht, die sich hinsichtlich ihres Ressourcenbedarfs und Sicherheitsniveaus unterscheiden. Fünf verschiedene Signaturalgorithmen wurden unter Berücksichtigung der folgenden Faktoren untersucht; benötigte Berechnungsdauer für das Signieren von Daten, Speicher und

Energieverbrauch, einmalige Verwendung der Signatur und Quantensicherheit (vgl. Tabelle 5.3). Mit Hilfe eines USB-6216-Modul des Unternehmens National Instruments wurde der Energieverbrauch des Mikrocontrollers zur Erstellung der digitalen Signatur bestimmt. Hierzu wurden Spannungsänderungen des Mikrocontrollers während des digitalen Signieren von Daten gemessen (siehe Abbildung 5.3) Die gemessene Spannungsänderungen wurden genutzt, um den Energieverbrauch unterschiedlicher Signaturalgorithmen zu bestimmen. Von allen untersuchten digitalen Signaturalgorithmus lassen sich vor allem die ECDSA und EdDSA Algorithmen zum digitalen Signieren von Sensornachrichten nutzen. Alle anderen digitalen Signaturen führen zu einer Überschreitung der maximal zulässigen Nachrichtengröße von 243 Bytes. Messungen zum Energieverbrauch der ECDSA und EdDSA Algorithmen belegen, dass eine kürzere Dauer der Signaturerstellung, mit einem geringeren Energieverbrauch korreliert. Der EdDSA Algorithmus ist am besten geeignet für das digitale Signieren von Nachrichten portabler Sensormodule.

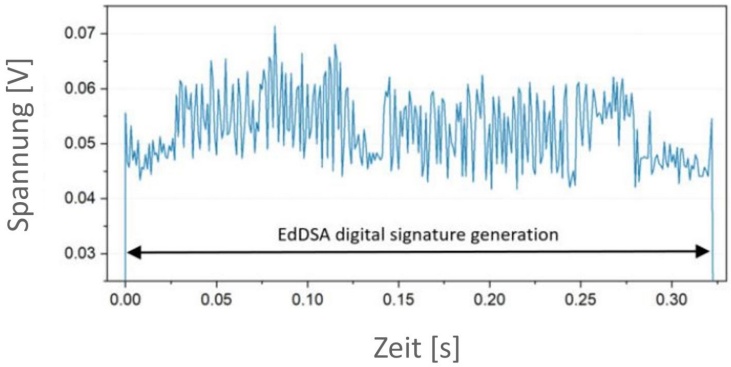

Abbildung 5.3: Spannungsverlauf des MCUs während der EdDSA-Signaturerstellung.

5.3.3 Distributed Ledger

Basierend auf den identifizierten Anforderungen eines PMS (vgl. Tabelle 5.1) wurde ein Distributed Ledger ausgewählt. Anforderungen der Nichtabstreitbarkeit und Transparenz des PMS erfordern, dass sich alle Konsortiumsmitglieder eindeutig identifizieren lassen. Ausschließlich Messwerte von verifizierte Konsortiumsmitglieder sollen im Distributed Ledger gespeichert werden. Basierend auf diesen Anforderungen wurde ein permissoned Distributed Ledger zum Aufbau eines PMS gewählt. In einem private-permissoned Distributed Ledger betreiben ausschließlich registrierte Mitglieder DLT-Knoten und speichern die Replikationen des Ledgers. Verglichen mit public-permissionless Distributed Ledgern, zeichnen sich private-permissioned Distributed Ledger durch ein hohes Maß an Flexibilität, Transparenz und Leistung aus [48]. Innerhalb eines private-permissioned Distributed Ledger lassen sich Identitäten aller Konsortiumsmitglieder mittels einer PKI verwalten. Anhand digitaler Signaturen, gespeicherter Transaktionen und bekannten öffentlichen Schlüssel der Konsortiumsmitglieder, ist transparent nachzuvollziehen welche gespeicherten Messwerte von welchen Mitgliedern stammen. Anders als in public-permissionless Distributed Ledgern, ist in private-permissioned Distributed Ledgern zudem mit geringeren Betriebskosten für die Ausführung von Smart Contracts zu rechnen [48]. Für den Aufbau eines PMS wird das Hyperledger Fabric (HLF) Framework zur Implementierung einer private-permissioned Blockchain genutzt [201].

Hyperledger Fabric (HLF) ist ein Blockchain-Framework der Linux Foundation [202]. Die Unabhängigkeit der Linux Foundation und Zugriffsmöglichkeiten auf den Quellcode der HLF gewährleisten eine freie Nutzung des Frameworks. Das HLF hat mit vielen Hunderten von Implementierungen weltweit eine enorme Popularität erlangt und zählt zu den am häufigsten eingesetzten Frameworks. HLF besteht im Wesentlichen aus drei Softwarekomponenten: Clients, Peer-Knoten und Orderer-Knoten. Die Ausgabe von Transaktionen und die Interaktion mit beispielsweise Browser-Anwendungen erfolgen durch Clients des Distributed Ledger. Clients stellen eine Schnittstelle zwischen dem Distributed Ledger und weiteren Anwendungen dar. Peer-Knoten prüfen Transaktionen, verwalten Replikationen

des Distributed Ledgers und können Smart Contract ausführen. In HFL werden Smart Contracts als Chaincode bezeichnet und können in bekannten Programmiersprachen wie Java oder Go geschrieben werden. Orderer-Knoten generieren und teilen neue Blöcken über das gesamte Netzwerk des Distributed Ledgers. Hierzu nehmen die Orderer-Knoten am Konsensmechanismus teil.

Alle Komponenten des HLF, wie Clients, Peer-Knoten und Orderer-Knoten, müssen sich über ein digitales Zertifikat bei einem Membership Service Provider authentifizieren, um mit der HLF-Blockchain zu interagieren. Der Membership Service Provider repräsentiert die PKI der HLF Blockchain [201]. Innerhalb der PKI werden Zertifikate für alle Clients und Knoten ausgestellt. Diese Zertifikate ermöglichen die Überprüfung der Identitäten und Rollen aller Teilnehmer. Beispielsweise werden Transaktionen von Peer-Knoten mit Hilfe ihres privaten Schlüssels signiert. Anschließend werden digitale Signatur aller Transaktionen durch die in der PKI gespeicherten öffentlichen Schlüssel der Peer-Knoten validiert. Auf diese Weise ermöglicht die PKI nur registrieren Identitäten die Teilnahme am Distributed Ledger.

Eine große Besonderheit des HLF Frameworks besteht in der Möglichkeit unterschiedlicher Konsensusmechanismen zu nutzen. HLF (v 1.4.1) bietet die Wahl zwischen drei Konsensmechanismen: Solo, Kafka und Raft. Zusätzlich zu diesen Konsensmechanismen wurde von Sousa et al. [203] ein fehlertoleranter und byzantinischer Konsensmechanismus BFT-SMaRt für die HLF (v 1.3) entwickelt. Konsensmechanismen haben einen großen Einfluss auf die Leistungsfähigkeit eines Distributed Ledgers. Alle verfügbaren Konsensmechanismen des HLF Frameworks wurden hinsichtlich ihrer Eignung für den Aufbau eines PMS untersucht. Hierzu wurde für verschiedene Konfigurationen, wie die Anzahl der Peer-Knoten, ein Vergleich aller in HLF verfügbaren Konsensmechanismen durchgeführt.

Bei **Solo** handelt es sich um einen zentralisierten Konsensmechanismus. Solo benötigt nur einen einzigen Orderer-Knoten, um eingehende Transaktionen zu empfangen, ordnen und neue Blöcke an alle Peer-Knoten zu senden. Unter allen von der HLF bereitgestellten Konsensmechanismen erzielt Solo den höchsten Transaktionsdurchsatz [204]. Solo wird häufig zu Testzwecken implementiert, da

dieser Mechanismus nicht fehlertolerant ist. Zusätzlich führt die Nutzung des Solo Konsensmechanismus zur Schaffung eines Single-Point-of-Failure (SPoF). Fällt der Orderer-Knoten aus, können keine Transaktionen mehr verarbeitet werden. Aufgrund seines zentralisierten Designs erfüllt Solo nicht die Anforderungen der Zensurresistenz und ist damit ungeeignet für den Aufbau eines dezentralen PMS.

Kafka gehört zu den dezentralen Konsensmechanismen im HLF und verfügt über keinen SPoF. Kafka verwendet zusätzlich zu den Orderer- und Peer-Knoten, ein weiteres Cluster bestehend aus Kafka-Knoten. Das Cluster wählt einen Leader zur Bestätigung von Transaktionen [205]. Durch das zusätzliche Cluster verfügt Kafka über eine hohe Nachrichtenkomplexität. Eine hohe Nachrichtenkomplexität führt zu einer geringen Skalierbarkeit. Kommt es beispielsweise zu einer Aufnahme neuer Konsortiumsmitglieder und die Anzahl der Peer-Knoten wächst von vier auf zwölf, sinkt gleichzeitig der Transaktionsdurchsatz von 200 tx/s auf 50 tx/s. Obwohl verschiedene Organisationen Orderer-Knoten unabhängig voneinander betreiben, kontrolliert eine einzige Organisation das gesamte Kafka-Cluster [206]. Alle Orderer-Knoten kommunizieren mit dem gleichen, zentralisierten Leader des Kafka-Clusters. Die Anforderungen einer hohen Skalierbarkeit und Zensurresistenz des PMS (vgl. Tabelle 5.1) werden vom Kafka Konsensmechanismus nicht erfüllt.

Der **Raft** Konsensmechanismus nutzt ebenfalls einen Leader-Knoten zur Konsensfindung. Einem Orderer-Knoten können drei unterschiedliche Rollen zugewiesen werden: die Leader, Follower und Kandidaten Rolle. Ohne einen Leader-Knoten wird allen Orderer Knoten die Rolle eines Kandidaten zugewiesen. Anschließend wird nach einem Mehrheitsprinzip aus allen Kandidaten ein Leader-Knoten gewählt, dessen Aufgabe es ist mit Clients zu interagieren und Einträge an seinen synchronisierten Follower-Knoten zu replizieren. Zur Synchronisation sendet der Leader-Knoten regelmäßig einen Heartbeat an alle Follower-Knoten. Können Follow-Knoten innerhalb einer bestimmten Zeitspanne kein Heartbeat vom gewählten Leader-Knoten empfangen, ändern sie ihren Status, werden zu Kandidaten-Knoten und es beginnt eine neue Wahl des Leader-Knoten [207].

Verglichen mit Kafka besitzt Raft über eine verbesserte Skalierbarkeit. Messungen (vgl. Anhang A) haben zeigen können, dass durch den Einsatz von Raft eine höhere Anzahl von Peer-Knoten, zu einem geringeren Rückgang des Transaktionsdurchsatzes führt. Bei Raft handelt es sich um einen fehlertoleranten Konsensmechanismus. Dennoch kann ein Leader-Knoten ausfallen und somit Transaktionen solange blockieren, bis wieder ein neuer Leader gewählt wurde [208]. Ein solch böswilliges Verhalten einzelner Knoten kann die Zensurresistenz des Ledgers beeinträchtigen. Raft erfüllt nicht die Anforderungen der Zuverlässigkeit; Zensurresistenz und Verfügbarkeit eines PMS, aufgrund der bestehenden Schwachstelle für byzantinische Fehler.

Der **BFT-SMaRt** Konsensmechanismus verfügt über eine verbesserte Zuverlässigkeit und eine höhere Skalierbarkeit in Bezug auf die Anzahl der Order-Knoten [209]. Ein Leader-Knoten senden eine bestimmte Anzahl an Transaktionen an alle Follower Knoten. Diese Follower-Knoten stimmen darüber ab, ob sie die Transaktionen im Distributed Ledger speichern möchten. Damit eine Anfrage vom Leader-Knoten erfolgreich gespeichert werden kann, müssen mehr als zwei Drittel aller Follower-Knoten die neue Anfrage in ihre lokale Replikation des Distributed Ledger aufnehmen.

BFT-SMaRt erzielt eine geringe durchschnittliche Latenzzeit und eine gute Skalierbarkeit (siehe Abbildung 5.5). Unterschiedliche Latenzzeit sind im Wesentlichen auf die Speicherung von Transaktionen bzw. Blöcke zurückzuführen. Beim BFT-SMaRt werden Transaktionen im Arbeitsspeicher (RAM) gespeichert, wohingegen die HLF-unterstützten Konsensmechanismen Transaktionen in einem langsameren Festplattenspeicher verwalten [210]. Anders als die von der HLF-unterstützten Konsensmechanismen, ist BFT-SMaRt byzantinisch fehlertolerant. Eine Mehrheit der Follow-Knoten kann über die Legitimität des Leader-Knoten abstimmen und diesen ersetzen [209]. Unter den evaluierten Konsensmechanismen ist der BFT-SMaRt am besten für den Aufbau eines PMS geeignet, aufgrund der byzantinisch Fehlertoleranz.

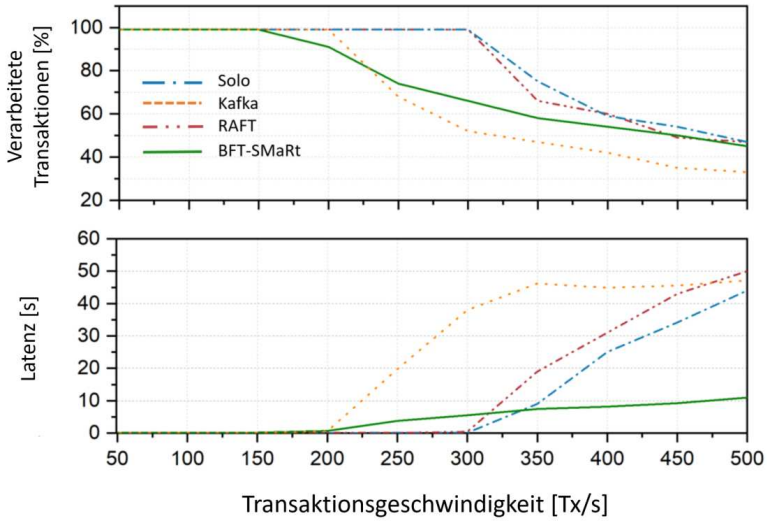

Abbildung 5.4: Transaktionsdurchsatz und Latenz verschiedener Konsensmechanismen (Solo, Kafka, Raft und BFT-SMaRt) für unterschiedliche Transaktionsgeschwindigkeiten

5.3.4 Workflow

Aktive Konsortiumsmitglieder stellen dem PMS Ressourcen bereit, um einen Client, eine Zertifizierungsstelle als Teil der PKI, einen Peer und einen Orderer-Knoten zu betreiben. Eingehende Anfragen werden vom einem Node.js-Server als Client verarbeitet. Der Node.js-Server verwaltet zusätzlich als Zertifizierungsstelle die öffentlichen Schlüssel und Rollen aller Knoten. Möchten Konsortiumsmitglieder ein Sensormodul beim PMS registrieren, wird ein kryptografisches Schlüsselpaar und eine eindeutige Sensormodul-ID für das Sensormodul erstellt. Private Schlüssel aller Sensormodule werden geschützt auf dem Sensormodul gespeichert, wohingegen öffentliche Schlüssel einer Sensormodul-ID zugeordnet und allen Konsortiumsmitgliedern zugänglich in einer PKI gespeichert werden. Jedes Konsortiumsmitglied kann über ein eigens LoRa Netzwerk Sensornachrichten an einen Distributed Ledger senden. Bestehende öffentliche LPWANs können zum Senden von Sensordaten ebenfalls genutzt werden, sofern sichergestellt ist, dass signierte Sensorwerte von öffentlichen LPWAN-Servern an den

Distributed Ledger weitergeleitet werden. Die Mitglieder des Konsortiums können innerhalb eines LoRa Netzwerks ihre Sensormodule an beliebigen Standorten platziert. Nach einer erfolgreichen Platzierung, liefern die sich im Betrieb befindlichen Sensormodule ihre aktuellen GPS-Koordinaten, sowie Messwerte zur relativen Luftfeuchtigkeit, Temperatur und der PM10 Feinstaubkonzentration. Allen Messwerten wird eine eindeutige Bezeichnung (universally unique identifier, UUID) zugewiesen. Gemäß den Empfehlungen der Internet Engineering Task Force (IETF) [211] besitzt die UUID jeweils eine Länge von 16 Bytes und wird von einem Zufallszahlgenerator erstellt. Die ID des Sensormoduls und der Messwerte (UUID) werden anschließend digital signiert und an alle umliegenden LoRa Gateways gesendet. Anschließend schalten die Sensormodule in einen Energiesparmodus und deaktivieren hierzu ihre Sensoren und ihr GPS-Modul.

LoRa Gateways die Sensorwerte empfangen, senden diese über TCP/IP Verbindungen weiter an die Clients der DLT-Knoten. Empfangene Sensornachrichten werden von Clients mit Hilfe von Smart Contract verarbeitet. Zunächst wird die Sensormodul-ID der empfangenen Sensornachricht extrahiert, um den öffentlichen Schlüssel des Sensormoduls aus der PKI zu lesen. Anhand des öffentlichen Schlüssels eines Sensormoduls wird die digitale Signatur der empfangenen Sensornachricht geprüft. Kann kein öffentlicher Schlüssel einer erhaltenden Sensornachricht zugeordnet werden, wird die Sensornachricht verworfen. Erfolgreich verifizierte Sensornachricht werden in einen neuen Block aufgenommen und dem Distributed Ledger hinzugefügt. Die im Distributed Ledger gespeicherte Sensordaten sind über eine öffentlich zugängliche API auch außerhalb des Konsortiums verfügbar und können in verschiedene Anwendungen integriert werden.

5.4 24 Stunden Feldtest

Die Bewertung des dezentralen PMS erfolgt anhand eines Konsortiums bestehend aus vier Mitgliedern, die zusammen in einem städtischen Gebiet fünf Sensormodule, drei LoRa Gateways, vier Clients, vier Peer-Knoten und vier Orderer-Knoten bereitstellen. Die verteilten Sensormodule senden während der Evaluierung alle

fünf Minuten Messungen der Temperatur, relativen Luftfeuchtigkeit und Feinstaubkonzentration (PM10) an umliegende Gateways. Ähnlich anderer Studien [212, 213] wurde das portable PMS anhand eines 24 Stunden Feldtest evaluiert. Im welchem Umfang der entworfene Prototyp die in genannten Anforderungen (vgl., Abschnitt 5.1) erfüllt, soll im Folgenden erörtert werden.

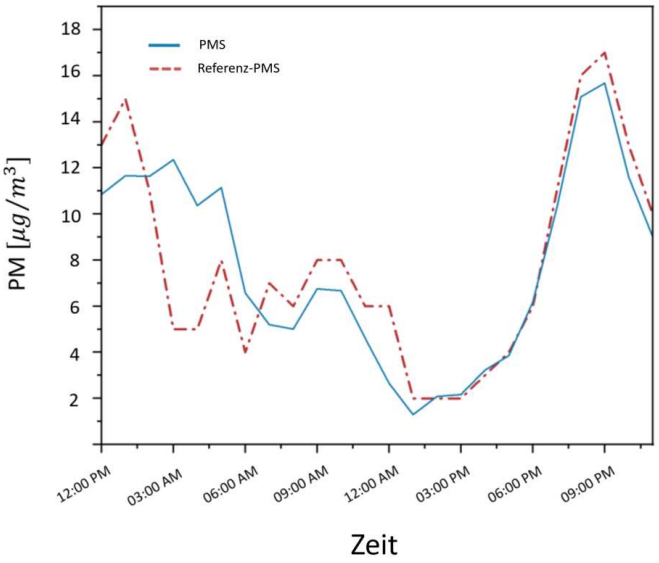

Abbildung 5.5: Vergleich der mit dem vorgeschlagenen PMS gemessenen PM10 Schadstoffkonzentration (rot) und Referenzmessungen einer vom Bayerischen Landesamt für Umwelt (LfU) in Deutschland betriebenen stationären Luftqualitätsstation (gestrichelte Linie) [164]. Alle Messungen wurden am gleichen Standort in Augsburg durchgeführt

Genauigkeit

Basierend auf einer gängigen Feldkalibrierungsmethode [214] wurde die Messgenauigkeit der verteilten Sensormodule untersucht. Hierzu wurden Messungen einer stationären Referenz-PMS [164] mit den Messungen eines portablen Sensormoduls verglichen. Der zeitliche Verlauf der vom portablen PMS (durchgezogene

Linie) gemessen Schadstoffkonzentrationen, ähneln dem Verlauf der Referenzmessung. Während der durchgeführten 24-Stunden Evaluierung, erreichte das portable PMS einen mittleren absoluten Fehler (engl., Mean absolute error, MAE), von 1,7 mg/m^3 [215, 216]. Zwischen beiden Sensoren wurden die geringsten Abweichungen am späten Nachmittag (3:00-6:00 pm); Uhr; MAE = 0,2 mg/m^3 und die höchsten Abweichungen in der Nacht (3:00-6:00 am); MAE = 6,1 mg/m^3 beobachtet. Änderungen der Lufttemperatur und der relativen Luftfeuchte können Messgenauigkeit portabler Low Cost Sensoren beeinflusst [217]. Bezogen auf die ermittelten Abweichungen zwischen der stationären Referenz-PMS und dem Sensormodul, gilt die Anforderungen an die Genauigkeit des PMS zur Bestimmung signifikanter und kurzfristigen Änderungen der PM10 Schadstoffkonzentationsänderung als erfüllt.

Verfügbarkeit

Während des gesamten Evaluierungszeitraums wurden keine Störungen durch beispielsweise temporär nicht verfügbare Sensormodule beobachtet. Im Vergleich zu einem zentralisierten System, verfügt das dezentrale PMS über eine hohe Verfügbarkeit. Verteilte Sensormodule senden simultan Nachrichten an mehrere LoRa Gateways. Trotz eines fehlerhaften Gateways können Sensornachrichten erfolgreich an DLT Knoten weitergeleitet werden. Das vorgestellte PMS erfüllt die Anforderung einer hohen Verfügbarkeit.

Bandbreite

Der von LoRa Protokoll genutzte maximale Duty-Cycle des EU-868-ISM-Bandes beträgt 1 % [218]. Dies führt zu einer maximalen, täglichen Gesamtübertragungszeit der Sensormodule von täglich 864 s pro Kanal. Basierend auf den genutzten LoRa Standardkonfigurationen mit einer Bandbreite von 250 kH, einem Spreizfaktor von neun, einer Coderate von eins und einer Nutzlastgröße von 121 byte pro Übertragung, betrug die verfügbare Sendedauer zur Übertragung von Nachrichten etwa 328 ms. Bezüglich des gewählten Messintervalls, von einer Messung alle fünf Minuten und einer Evaluierungsdauer von 24 h, betrug die gesamte täglich Sendezeit aller fünf Sensormodule täglich etwa 472 s. Die Anforderung der Bandbreite wird vom PMS erfüllt.

Zensurresistenz

Jedes Konsortiumsmitglied betreibt eigenständig LoRa Netzwerke und kann die von Gateways empfangenen Daten an den Distributed Ledger senden. Aufgrund diese Unabhängigkeit verfügt das PMS über eine hohe Zensurresistenz. Eine steigende Anzahl an DLT-Knoten, erhöht die Zensurresistenz des PMS. Die Anzahl der von Konsortiumsmitglieder betriebenen DLT-Knoten ist durch den gewählten BFT-SMaRt Konsensmechanismus begrenzt (siehe Abbildung 5.5). Eine steigende Anzahl an DLT-Knoten führt zu einem abnehmenden Transaktionsdurchsatz. Obwohl das PMS die Anforderung an die Zensurresistenz hinsichtlich der Netzwerkkommunikation erfüllt, wird bezüglich des gewählten Distributed Ledgers lediglich eine begrenzte Zensurresistenz erzielt.

Energieverbrauch

Der durchschnittliche Energieverbrauch des Sensormoduls betrug etwa 60 mA/h. Eine temporäre Deaktivierung des GPS Moduls hat zu einem geringeren Energieverbrauch von 19 mA/h geführt. Lediglich zur synchronisieren und zur Standortprüfung des Sensormoduls, wurde das GPS-Modul einmal täglich genutzt. Ohne permanente Verwendung des GPS-Moduls, lassen sich die portablen Sensormodule mit einer Batteriekapazität von 10 Ah für etwa 22 Tage betreiben. Damit wird das PMS der Anforderung eines geringen Energieverbrauchs gerecht.

Unabhängigkeit

Sensormodule bestehen ausschließlich aus frei erhältlichen Hardwarekomponenten. Einzelne Hardwarekomponenten lassen sich jederzeit austauschen. Ebenfalls sind alle Softwarekomponenten frei verfügbar, wie beispielsweise das genutzte drahtlose Kommunikationsprotokoll (LoRa), die Distributed Ledger Technologie (HLF Blockchain) oder die Signaturalgorithmen. Durch das Vermeiden von Abhängigkeiten von proprietärer Hardware und Software, erfüllt das PMS die Anforderung der Unabhängigkeit.

Integrität

Die Integrität der Sensornachrichten ist aufgrund digitaler Signaturen nachweisbar. Digitale Signaturen aller eingehenden Nachrichten werden automatisch von Smart Contracts überprüft. Eine Manipulation digitale Signaturen kann erfolgen, wenn im Distributed Ledger gespeicherte öffentliche Schlüssel durch eine Mehrheit der Konsortiumsmitglieder manipuliert werden. Ein solches Szenario ist unwahrscheinlich, da meisten Mitglieder eines Konsortiums kein Interesse an einer Datenmanipulation haben sollten. Die Anforderung der Datenintegrität wird vom PMS erfüllt.

Nachweisbarkeit

Alle Sensormodule sind eindeutig identifizierbar und signieren Nachrichten mit Hilfe eines privaten Schlüssels [219]. Verschiedene Sicherheitsprüfungen des Sensormoduls schützen private Schlüssel vor einem unautorisierten Zugriff. Im Distributed Ledger ermöglichen digital signierte Identifier des Sensormoduls und der Sensornachrichten (UUID) zudem eine eindeutige Zuordnung aller Sensormodule und Nachrichten. Zusätzlich ist es aufgrund der Manipulationssicherheit des Distributed Ledger schwer, das PMS hinsichtlich der Nachweisbarkeit zu korrumpieren. Potenziellen Angreifern ist kaum möglich [162] EdDSA-generierte, private Schlüssel zu reproduzieren. Das PMS erfüllt die Anforderung der Nachweisbarkeit.

Portabilität

In einer 13x7x5 cm großen, wetterfesten Box (siehe Abbildung 5.2) sind alle Hardwarekomponenten eines Sensormoduls untergebracht. Ohne auf besondere Umweltbedingungen oder eine permanente Energieversorgung achten zu müssen, können alle Konsortiumsmitglieder ihre registrierten Sensormodule frei im urbanen Raum aufstellen. Lediglich die Portabilität der LoRa Gateways ist aufgrund einer notwendigen permanenten Energieversorgung eingeschränkt. Im Vergleich zu stationären PMS, ist der Energieverbrauch eines dezentralen PMS bestehenden aus verteilten Sensormodulen und Gateways sehr gering, wodurch das PMS die Anforderungen einer hohen Portabilität erfüllt.

Verlässlichkeit

Während der gesamten Evaluierung wurden zuverlässig alle 1.440 Messungen der Sensormodule verarbeitet. Messungen gleicher UUID werden nicht im Distributed Ledger gespeichert. Alle gespeicherten Messungen sind über die von den einzelnen Konsortiumsmitgliedern bereitgestellte API öffentlich zugänglich. Die Verlässlichkeit des evaluierten PMS basiert auf einer redundanten Datenverarbeitung, wodurch ein Ausfall einzelner Gateways oder DLT-Knoten nicht zwangsläufig zu einem Datenverlust führt. Sensormodule senden simultan an alle umliegenden Gateways ihre Sensornachrichten. Nachrichten eines Sensormoduls werden somit von mehreren Gateways an den Distributed Ledger gesendet. Der genutzte BFT-SMaRt Konsensusmechanismus toleriert böswillige Order-Knoten im Distributed Ledger. Aufgrund dieser Fähigkeiten des PMS, mit beschädigten Gateways und böswilligen Konsortiumsmitgliedern umzugehen, erfüllt das PMS Anforderungen der Verlässichkeit.

Skalierbarkeit

Die Skalierbarkeit des PMS wird zum einen durch die Duty-Cycle des LoRa Kommunikationsprotokolls und zum anderen durch die Mesh-Netzwerktopologie der Sensormodule und Gateways beinflusst. Vor allem eine steigende Anzahl von Gateways führt zu einer starken Erhöhung der zu verarbeitenden Sensornachrichten. Während der Evaluierung wurden in einem Messintervall von fünf Sensormodulen und drei Gateways, insgesamt 15 Sensornachrichten an den Distributed Ledger weitergeleitet. Wird eines solches Cluster erweitert, steigt die Anzahl der vom Distributed Ledger zu verarbeiten Sensornachrichten. Messungen des Distributed Ledger haben gezeigt, dass sich durch die Integration von zwölf Peer-Knoten in das PMS unter Nutzung des BFT-SMaRt-Konsensmechanismus, der Transaktionsdurchsatz von 150 tx/s auf 100 tx/s verringert. Aufgrund der Vielzahl möglicher Konsortiumsmitglieder einer Stadt, die weit über die evaluierte Anzahl hinausgehen kann, wird die Anforderungen der Skalierbarkeit von dem evaluierten PMS Prototypen nicht erfüllt.

Durchsatz

Während der Evaluierung wurden keine Leistungsengpässe des implementieren PMS Prototypen beobachtet und alle Transaktionen wurden erfolgreich verarbeitet. Mit einer verfügbaren Sendezeit von 864 s/d für jeden öffentlichen LoRa Kanal wäre es theoretisch jedem Sensormodul möglich, 21 msg/h an umliegende Gateways zu übertragen. Werden alle Sensornachrichten gleichzeitig an die umliegenden Gateways gesendet, so muss für einen Messintervall der Distributed Ledger 15 tx/s verarbeiten. Die Evaluierung verschiedener Konsensmechanismen (siehe Anhang A) zeigt, dass der Distributed Ledger bestehend aus vier Peer und vier Orderer-Knoten, bis zu 100 tx/s zuverlässig verarbeiten kann. Das PMS erfüllt damit die Anforderung eines hohen Durchsatzes.

Transparenz

Das vorgestellte PMS basiert auf einem Distributed Ledger dessen Teilnahme ausschließlich registrierten Mitgliedern gewährt wird. Sensorwerte gespeichert im Distributed Ledger sind allen Konsortiumsmitgliedern bekannt und über eine bereitgestellte API auch öffentlich zugänglich. Die einzelnen APIs können von Konsortiumsmitglieder manipuliert werden und somit Leserechte auf die im Ledger gespeicherten Messwerte zu modifizieren. Nicht registrierte Mitglieder können APIs aller Konsortiumsmitglieder abfragen und die abgerufenen Sensordaten auf Inkonsistenzen vergleichen. Auf diese Weise können manipulierte APIs erkannt werden. Aufgrund der Entscheidung die Zugangsrechte des Distributed Ledgers zu beschränken, um einen hohen Ressourcenbedarf durch das Mininig von Blöcken in public-permissionless Distributed Ledgern zu verringern, ist die Anforderungen an die Transparenz des PMS nur teilweise erfüllt, zumal Außenstehende keinen freien Zugriff auf Informationen des Distributed Ledgers haben.

6 Dezentrale Datenverwaltung

Das folgende Kapitel geht der Fragestellung nach, wie sich IoT Datenströme mit Hilfe einer innovativen Datenverwaltung in dezentralen Netzwerken verlässlich teilen lassen. Hierzu befasst sich der erste Abschnitt dieses Kapitels mit aktuellen Herausforderungen, die einen Datentransfer zwischen unterschiedlichen Entitäten erschweren. Im zweiten Abschnitt wird ein innovatives Konzept zur Datenverwaltung vorgestellt. Es wird beschrieben, wie sich Entitäten verlässlich identifizieren, authentifizieren und autorisieren können. Diese Kapitel endet mit der Evaluierung der vorgestellten Konzepte.

Die in diesem Kapitel vorgestellten Ergebnisse stammen aus Veröffentlichungen des Autors in Zusammenarbeit mit verschiedenen Co-Autoren [K2, K3].

6.1 Herausforderungen

Im IoT sind riesige Datenmengen unterschiedlicher Sensornetzwerke verfügbar. Der Transfer dieser enormen Datenmengen zwischen unterschiedlichen Dateneigentümer, wird durch unzureichend erfüllte Sicherheitsanforderungen stark limitiert. Geräten unterschiedlicher Eigentümer ist es nicht möglich, verlässlich miteinander zu interagieren. Es fehlt an digitalen Identitäten, mit denen sich eigenständig Vertrauens- und Reputationsmechanismen zwischen Entitäten etablieren und verifizierbare Transaktionen durchzuführen lassen. Eine sichere Interaktion zwischen unterschiedlichen Sensormodulen und Netzwerken, ist ohne digitale Identitäten kaum möglich [5].

Zur Identifikation von Entitäten werden PKIs genutzt, die es ermöglichen in einer nicht vertrauensvollen Umgebung, wie beispielsweise dem Internet, sicher miteinander zu kommunizieren bzw. Daten auszutauschen. Hierzu nutzen PKIs digitale Zertifikate, die der Identifizierung einer Entität dienen. In konventionellen PKIs werden digitale Zertifikate von Zertifizierungsautoritäten (engl. Certificate Autorities, CAs) erstellt und verwaltet. Das Vertrauen in digitale Zertifikate beruht auf dem Vertrauen in die Zertifikate ausstellende Autorität. Entitäten die einer bestimmten Autorität vertrauen möchten, vertrauen damit auch allen von dieser Autorität verifizierten Identitäten. Hierdurch entstehen hierarchische Strukturen mit einer Zertifizierungsautorität (Root-CA) an der Spitze einer PKI. Diese hierarchischen Strukturen bzw. Vertrauensmodelle gehören zu den größten Schwächen konventioneller PKIs, zumal sie einen SPoF in eine PKI einführen. Wird beispielsweise eine Root-CA kompromittiert oder wird die Root-CA nicht mehr als vertrauenswürdig eingestuft, so lässt sich die gesamte PKI nicht für einen sicheren Datenaustausch nutzen.

Neben Sicherheitsrisiken die primär auf einem SPoF einer einzelnen Autorität beruhen, verfügen Entitäten in einzelnen PKIs über eine geringe Privatsphäre und Datenkontrolle. Einzelne Zertifizierungsautoritäten definieren welche Attribute zum Erstellen und Nutzen einer digitalen Identität notwendig sind. Entitäten ist es nicht möglich, eigenständig ihre digitale Identität zu definieren. Zusätzlich führt eine zentrale Verwaltung digitale Identitäten durch einzelne Zertifizierungsautoritäten zu einer stark limitierten Interoperabilität. Digitale Identitäten lassen sich nur innerhalb einer bestimmten Anwendungsdomäne nutzen. Eine solche Identitätsisolierung innerhalb eines Systems bzw. einer Domäne führt dazu, dass sich mit Identitäten verbundene Eigenschaften, wie beispielsweise Reputationen, nicht über verschiedene Systeme hinweg übertragen oder verfolgen lassen [220].

Alternativ zur zentralisierten PKIs, können Daten einer digitalen Identität sowie deren Zertifikate, dezentral verwaltet werden. In den letzten Jahren wurde vor allem der Einsatz von DLTs zum Aufbau dezentraler PKIs (DPKIs) untersucht. In vielen DPKIs ersetzen Distributed Ledger eine zentrale Datenspeicherung. Das

Einbinden eines Distributed Ledgers innerhalb einer DPKI kann zu einer größeren Datenkontrolle, höheren Ausfallsicherheit sowie einer manipulationsgeschützten Datenspeicherung führen und damit bestehende Limitierungen zentralisierter PKIs kompensieren. In einem Distributed Ledger gespeicherte Daten können von Identitäten eigenständig kontrolliert werden. Einzelne Zertifizierungsautoritäten können gespeicherte Daten anderer Entitäten nicht modifizierte oder weiterleiten. Operationen einer DPKI, wie beispielsweise die Aktualisierung von Identitätsinformationen, werden meistens durch Smart Contracts durchgeführt. Transaktionsgebühren zum Ausführen von Smart Contracts führen beim Verwalten von Millionen von digitalen Identitäten zu sehr hohen Kosten und Verarbeitungszeiten.

Mit Hilfe der DLTs können Informationen über digitale Identitäten in frei zugänglichen und nicht vertrauenswürdigen Umgebungen sicher verwaltet werden. Der Einsatz von DLTs führt jedoch nicht zwangsläufig zu einem verlässlichen Datenaustausch zwischen Identitäten. In einem nicht durch zentrale Autoritäten kontrollierten System, ist es einzelnen Entitäten nur schwer möglich, die Vertrauenswürdigkeit unbekannter Identitäten zu bewerten. Infolgedessen gibt es einen starken Bedarf an quantifizierbaren Vertrauensbeziehungen zwischen digitalen Identitäten [221].

Bisherige Veröffentlichungen zum Aufbau einer DPKI nutzen Distributed Ledger als öffentliche Datenspeicher und verwenden zur Authentifizierung der Identitäten hierarchische Vertrauensmodelle [222, 223, 224, 225]. Beispielsweise werden von einer Autorität signierte Zertifikate und ihr Widerrufsstatus, als Transaktion in einem public permissionless Distributed Ledger gespeichert, um Signierungs- und -sperrvorgänge einer einzelnen Zertifizierungsautorität zu überwachen [222]. Der Ledger dient damit hauptsächlich als manipulationssichere Quelle für die Registrierung und das Nachschlagen eines Zertifikatsstatus. In einem solchen Aufbau ist eine DPKI von einer traditionellen CA-Rolle abhängig.

Eine Alternative zu hierarchischen Vertrauensmodellen bieten sogenannte Web of Trust (WoT) Modelle [226]. WoT Modelle beschreiben dezentrale Vertrauensstrukturen die zwischen Identitäten aufgebaut werden, um öffentliche Schlüssels und damit digitale Identitäten zu verifizieren. Durch ein gegenseitiges Verifizieren

öffentlicher Schlüssel können digitale Identitäten eigenständig Vertrauensstrukturen aufbauen und einander authentifizieren, ohne auf eine zentrale Zertifizierungsautorität angewiesen zu sein. Beispielsweise kann die Identität Alice durch eine digitale Signatur, den öffentlichen Schlüssel einer anderen Identität Bob erfolgreich verifizieren. Eine solche Signatur wird von anderen Identitäten als eine Vertrauensbeziehung interpretiert. Andere Identitäten können eigenständig entscheiden, ob sie einem öffentlichen Schlüssel und damit einer anderen digitalen Identität vertrauen möchten. Im Wesentlichen wird zwischen direkten und indirekten Vertrauensbeziehung unterschieden. Bei einer direkten Vertrauensbeziehung wird der öffentliche Schlüssel einer zu verifizierenden Identität von einer bereits bekannten Identität bestätigt. Wohingegen es bei einer indirekten Vertrauensbeziehung, eine Kette bzw. Beziehung vertrauenswürdiger Signaturen vom eigenen Schlüssel, hin zum Zielschlüssel der zu verifizierenden Identität existiert. Beispielsweise könnte eine Identität John über seine direkte Vertrauensbeziehung zu Alice, eine indirekte Vertrauensbeziehung zu Bob aufbauen.

Der Aufbau dezentraler Vertrauensstrukturen anhand von WoT Modellen war Gegenstand vieler Untersuchungen [227, 228, 221]. Smart Contracts wurden genutzt um Attribute, Signaturen und Widerrufsrechte einer Identität in einem Distributed Ledger zu speichern. Zugleich verfügen Identitäten über die Möglichkeit, diese im Distributed Ledger gespeicherten Identitätsangaben mit Hilfe eines WoT Modells zu verifizieren [227]. Quantifizierbare WoT Vertrauensmodelle, beschreiben den Vertrauensfluss von einer Identität zu einer anderen Identität als gerichteten Graphen und können somit zur Authentifizierung von Identitäten genutzt werden [221].

WoT Modelle haben im Gegensatz zu einzelnen PKIs und hierarchischen Vertrauensmodellen zwar keinen SpoF, leiden aber dennoch unter diversen Herausforderungen, die einer erfolgreichen Nutzung in nicht vertrauensvollen Umgebungen entgegenstehen. Zum einen bieten viele WoT Modelle keine ausreichende Sicherheit, dass angegebene Informationen korrekt sind. Fehlende Anreize führen dazu, dass Angaben zur Identität nicht sorgfältig überprüfen werden [229]. Böswilligen Identitäten ist es möglich eigenständig eine Vielzahl an digitalen Identitäten (Sybil-Identitäten) zu generieren und sich selbst mit Hilfe dieser eigens

erstellten Sybil-Identitäten, ein großes Netzwerk an Vertrauensbeziehungen aufzubauen. Diese nicht realen Vertrauensbeziehungen können genutzt werden, um gegenüber realen Identitäten vertrauensvoll zu wirken. Fehlende Mechanismen die eine böswillige Entität daran hindert, eine beliebige Anzahl an Sybil-Identitäten zu erzeugen, können erfolgreiche Sybil Angriffe ermöglichen [230].

Neben Herausforderungen in den Bereichen der Identifikation und Authentifikation, wird ein freier Datentransfer durch limitierte Möglichkeiten der Autorisierung beschränkt. Vor allem die im IoT typischen Echtzeitdatenströme lassen sich kaum mit unterschiedlichen Entitäten teilen. Datenströme können als eine Folge zeitgestempelter Datenpunkte beschrieben werden und gehören zu den am häufigsten genutzten IoT Datentypen. Das Gewährleisten eines Zugriffs auf kontinuierliche Datenströmen ist durch eine Nutzung bestehender Cloud-Plattform mit vielen Limitierungen verbunden, die auf einer zentralisierten und intransparenten Datenverarbeitung beruhen. Die Nutzer zentral verwalteter Datenplattformen verlieren die Kontrolle über ihre eigenen Daten. Ihnen ist nicht bekannt mit wem ihre Daten geteilt werden oder wie ihre Daten gegen einen unerlaubten Zugriff geschützt werden [231].

Viele Plattformanbieter stellen ihren Nutzern verschiedene Möglichkeiten der Datenverschlüsselung bereit, um einen verbesserten Datenschutz zu gewährleisten [232]. Clientseitige Verschlüsselung werden genutzt, um die innerhalb einer Cloud-Plattform gespeicherte Daten effizient zu schützen. Bei einer clientseitigen Verschlüsselung werden alle Daten vor dem Senden verschlüsselt und erst beim Empfänger wieder entschlüsselt. Eine solche Ende-zu-Ende Verschlüsselung funktioniert plattformübergreifend und speichert zu keinem Zeitpunkt Daten unverschlüsselt auf einer Plattform. Durch eine Ende-zu-Ende Verschlüsselung können beispielsweise die Risiken eines möglichen Datenmissbrauchs reduziert werden. Zu möglichen Schäden zählt beispielsweise ein unbefugter Datenhandel aufgrund einer Systemkompromittierung.

Eine clientseitige Verschlüsselung verstärkt den Datenschutz, schränkt jedoch gleichzeitig das Teilen von Daten bzw. eine Interoperabilität zwischen Systemen stark ein [233]. Verschiedene kryptografische Verfahren können genutzt werden,

um Einschränkungen hinsichtlich der Interoperabilität von verschlüsselten Daten zu überwinden. Attributbasierte Verschlüsselung (engl. attribute based encryption, ABE) gehören zu den häufig genutzten Verfahren zum Teilen verschlüsselter Daten [69]. Anders als bei herkömmlichen Verschlüsselungen, werden bei der ABE Verschlüsselung die Daten mit Attributen verschlüsselt, die mit Zugriffsrichtlinie verknüpft sind. Nur Datenempfänger die über einen spezifischen kryptografischen Schlüssel verfügen und gleichzeitig die Zugriffsrichtlinie erfüllen, können die empfangenen Daten entschlüsseln. Für ABE Verschlüsselungen sind aufgrund der zugrundeliegenden Kopplung der kryptografischen Schlüssel und Attribute, aufwändige Verschlüsselungsoperationen notwendig. Die zur Verschlüsselung notwendigen Ressourcen steigen linear mit der Anzahl der Attribute, wodurch die Granularität des Datenzugriffs stark limitiert wird [234].

Hybride Verschlüsselungsverfahren [235, 236] bei denen zunächst große Datenmengen mit effizienten Verschlüsselungsverfahren verschlüsselt werden, um die hierzu genutzten kryptografischen Schlüssel anschließend mit einem ABE Verfahren zu verschlüsseln, eignen sich ebenfalls nicht für ein effizientes Teilen von IoT Datenströmen. Bereits für zwei Attributen können hybride Verschlüsselungsverfahren eine Verarbeitungszeit von 100 ms für die Ver- und Entschlüsselung der Daten benötigen. Werden für die Ver- und Entschlüsselung IoT Geräte mit stark limitierten Rechenressourcen genutzt, beträgt die Verarbeitungszeit solcher hybrider Verschlüsselungsverfahren bereits einige Sekunden [237].

6.2 Zugriffsmanagement

Eine modernes Datenzugriffsmanagement (engl., identity and access-management, IAM) fördert einen Datenaustausch im IoT durch eine verlässliche Identifikation, Authentifikation und Autorisierung von Entitäten. Zur Konzeptionierung einer modernen Datenverwaltung wird von einem urbanen IoT Ökosystem ausgegangen, in der eine große Anzahl von unterschiedlichen Sensormodule (Datenproduzenten), Dateneigentümern und Datenkonsumenten miteinander interagieren. In

bestehenden IoT Ökosystem existieren proprietäre IAM Anwendungen und unterschiedlichen Kommunikationsstandards, wodurch Entwicklungen hin zu Kollaborationen zwischen Geräten bzw. einem freien Datentransfer verzögert werden. Eine moderne Datenzugriffsverwaltung, die das Teilen von Daten in dezentralen Netzwerken fördert, berücksichtigt folgende Anforderungen;

- Skalierbarkeit: Das IoT möchte viele Millionen von Geräten in einer cyberphysischen Welt miteinander verbinden. Hierzu müssen Millionen von digitalen Identitäten, sowie deren Beziehungen zueinander effizient verwalten werden. Mechanismen zur Identifikation und Authentifikation sind notwendig, mit denen sich große Informationsmengen effektiv verarbeiten lassen.
- Portabilität: Vielfalt und Heterogenität im IoT erschweren es, Informationen zwischen unterschiedlichen Systemen auszutauschen. Zur Förderungen systemübergreifender Anwendungen sollten digitale Identitäten portabel sein, um in unterschiedlicher Netzwerken und Anwendungen genutzt zu werden.
- Privatsphäre: Identitäten sollten die Möglichkeit haben zu entscheiden, welche Informationen sie teilen oder veröffentlichen wollen. Die Privatsphäre einzelner Identitäten gilt es zu schützen.
- Vertrauen: In zugangsfreien und nicht kontrollierten Netzwerken muss berücksichtigt werden, wie sich gegenseitige Vertrauensbeziehungen zwischen Identitäten aufbauen lassen.
- Sicherheit: Digitale Identitäten sind Grundpfeiler vieler Anwendungen und die Basis diverser Sicherheitsmechanismen. Digitale Identitäten und Vertrauensbeziehungen zwischen Identitäten sollten sich nicht unautorisiert modifizieren lassen.

6.2.1 Identifizierung

Zu den Aufgaben eines Identitätsmanagements gehört die Darstellung von Entitäten als digitale Identität in virtuellen Netzwerken [238]. Im Rahmen dieser Dissertation ist eine digitale Identität definiert als eine Repräsentation einer Entität innerhalb einer bestimmten Anwendungsdomäne [239]. Diese Repräsentation erfolgt in Form eines dezentralen Identitätsdokuments (engl., DID Document) in Anlehnung an die DID Spezifikation des World Wide Web Consortium (W3C) [240]. Eine einzelne Entität kann je nach Anwendungsbereich über unterschiedliche Identitäten verfügen. Zur eindeutigen Identifizierung einer Entität sind Identifikatoren notwendig. Die zum Aufbau von selbst-verwalteten Identitäten genutzten Identifikatoren werden Decentralized Identifiers (DIDs) genannt [75]. DIDs ermöglichen eine Auffindbarkeit und eindeutige Identifizierung einer Identität und sind vergleichbar, mit dem im Internet genutzten Uniform Resource Locators (URLs). DIDs sind unabhängig von zentralen Identitätsanbietern bzw. Systemen und können von Entität eigenständig erstellt und verwaltet werden, wodurch selbst-verwaltete Identitäten (SSI) entstehen [78].

Die Charakterisierung digitaler Identität erfolgen anhand von Identifikationsmerkmale (claims). Identitäten können sich selbst oder anderen Identitäten bestimmte Claims zuschreiben. Eine Identität wird repräsentiert durch die Summe ihrer Claims (siehe Abbbildung 6.3). Damit Identitäten den Identifikationsmerkmalen anderer Identitäten vertrauen können, müssen diese Merkmale verifiziert werden. Diese Verifizierung erfolgt durch Bestätigungen (engl. Attestations), mit denen Identitäten ihre persönliche Einschätzung über die Vertrauenswürdigkeit eines bestimmten Claims belegen können. Bei den Attestations handelt es sich um ein elektronisches Äquivalent zu physischen Nachweisen bzw. Bestätigungen, wie beispielsweise einem Personalausweis oder Führerschein.

Eine Attestation eines Claims gilt als vertrauenswürdig, wenn die Attestation ausstellende Identität selbst als vertrauenswürdig eingestuft wird. Welche Identitäten als vertrauenswürdig eingestuft werden, wird stark von dem Vertrauensverhältnis der Attestation gebende und prüfende Identität bestimmt. Vertrauensmodelle können Entitäten unterstützen, einen Vertrauenswert einer unbekannten Identität zu

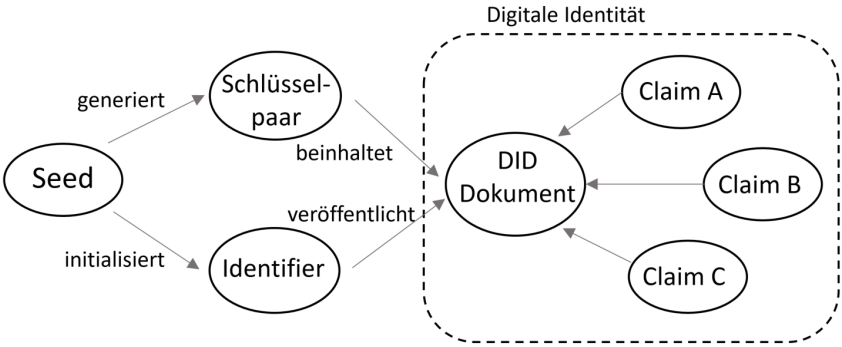

Abbildung 6.1: Aufbau einer digitalen Identität bestehend auf unterschiedlichen Claims [2]

bestimmen [221]. Basierend auf Vertrauenswerten und abhängig von definierten Vertrauensschwellenwerten, kann ein Datenaustausch zwischen zwei Identitäten zustande kommen oder abgelehnt werden.

IAM Anwendungen müssen CRUD Operationen ermöglichen, um den gesamten Lebenszyklus einer digitalen Identität abzubilden. Zu diesen Operationen gehört das Erstellen (Create), Lesen (Read), Ändern (Update) und Löschen (Delete) einer digitalen Identität. Entitäten sollten alle CRUD Operationen ihrer digitalen Identität eigenständig durchführen, ohne von einem einzelnen Identitätsanbieter abhängig zu sein. Zur vollständigen Kontrolle digitaler Identitäten, werden alle Daten einer Entität in einem public permissionless Distributed Ledger gespeichert. Hierzu wird der IOTA Tangle zur eigenständigen Verwaltung digitaler Identitäten genutzt. Der IOTA Tangle ist für skalierbare Anwendungen im IoT konzeptioniert, zumal ein hoher Transaktionsdurchsatz über den IOTA Tangle erzielt werden kann, keine Transaktionsgebühren fällig werden und das Versenden von ausschließlich Datennachrichten möglich ist (vgl. Abschnitt 2.3).

Erstellen einer Identität

Die Generierung einer digitalen Identität beginnt mit der Erzeugung eines Seeds, zur Erstellung eines kryptografischen Schlüsselpaars. Mit Hilfe der generierten Schlüssel wird einen MAM-Stream für die Veröffentlichung eines DID Dokuments erzeugt. Seed Eigentümer nutzen ihren privaten Schlüssel um ein DID

Dokument in Form einer MAM-Nachricht an den erstellten MAM-Kanal zu senden. Die Zugehörigkeit zwischen einen MAM-Kanal und DID Dokumenten wird durch die ID des MAM-Kanals definiert, die im DID Dokument enthalten ist. Das DID Dokument wird als erste Nachricht auf der Root Adresse eines MAM-Kanals gespeichert. Das Format des DID Dokuments entspricht den DID Spezifikation des W3C und enthält den öffentlichen Schlüssel eines DID Dokuments sowie den dazugehörigen dezentraler Identifikator (DID). Eine DID repräsentiert eine ID eines DID Dokument und ist aus drei unterschiedlichen Teilen zusammengesetzt, die durch Doppelpunkte getrennt voneinander getrennt sind. Der erste Teil definiert, dass es sich um ein DID Dokument handel, der zweite Teil beschreibt eine Methode mit der die Identität im dezentralen Netzwerk lokalisiert werden kann. Der dritte Teil repräsentiert die methodenspezifische digitale Identität. Eine DID kann beispielsweise wie folgt aussehen;

did:iota:H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV

Auf der zweiten Adresse eines MAM-Kanals wird eine MAM Nachricht gespeichert, die eine Liste aller als vertrauenswürdig eingestufter Identitäten enthält. Diese Nachricht enthält die IDs vertrauenswürdiger Identitäten, dazugehörige frei wählbare Vertrauenswerte und die digitale Signatur der Identität eines DID Dokuments. Optional enthält diese MAM Nachricht noch einen Transaktionbundelhash, um auf vorherige Nachrichten zu verweisen.

Damit ein DID Dokument zur Identifikation genutzt werden kann, sind verifizierbare Claims notwendig. Ein Claim über eine Identität kann von jeder Entität, zu jederzeit erstellt werden. Ein Claim enthält Informationen über einen *Claim-type*, *Claim-Description*, *Claim-target*, *Claim-issuer*, *Claim-signature*. Der *Claim-type* folgt eine externen Standard, wie beispielsweise dem eCl@ss-Standard. Die *Claim-Description* enthält dem gewählten Standard folgend, eine Beschreibung des Claims zur Charakterisierung bzw. Beschreibung einer digitalen Identität. *Claim-issuer* und *Claim-target* beschreiben, wer einen Claim über wen erstellt hat. Damit ein Claim für die Bewertung von Vertrauensbeziehungen berücksichtigt werden kann, ist jeder gültige Claim vom *Claim-issuer* digital signiert. Dabei ist es möglich, dass eine Entität sich selbst einen Claim über ihre eigene digitale

Identität ausstellt. Erzeugt Claims werden als Transaktion auf einer einer spezifischen Transaktionsadresse im IOTA Tangle gespeichert. Zur Generierung einer claim-spezifischen Transaktionsadresse werden die ID einer Identität (ID Target) ,sowie die Art des Claims (Claim-type) miteinander gehasht. Damit setzten sich Claim-Adressen wie folgt zusammen;

Claim-Adr. = Hash(Id Target + Claim-Typ)

Claims über eine digitale Identität werden für eine Authentifizierung berücksichtigt, sofern diese von digitalen Identitäten bestätigt wurden. Bei den hierzu genutzten Attestations handelt es ebenfalls um IOTA Transaktionen, mit denen sich das Vertrauen einer Entität in einen Claim einer digitalen Identität abbilden lässt. Zunächst wird anhand der ID einer Identität und des Claim Typs, die Claim Transaktionsadresse im IOTA Tangle bestimmt und der gespeicherte Claim gelesen. Soll dieser Claim bestätigt werden, erstellt die bestätigende Entität eine neue IOTA Transaktion. Diese Transaktion bezieht sich auf den gelesenen Claim, enthält einen frei wählbaren Vertrauenswerte, ist von der attestierenden Entität digital signiert und auf einer Attestationsadresse im IOTA Tangle veröffentlicht. Die Transaktionsadresse zur Speicherung einer Attestation setzt sich aus dem Hash zweier Eingabegrößen zusammen.

Att.-Adr. = Hash(Id Certifier + Claim Bundle Hash)

Zum einen der ID der Identität die eine Bestätigung eines Claims erstellen möchte und zum anderen dem Hash eines Transaktionsbündels, der sich auf den zu verifizierenden Claim bezieht. Mit dem Hash lassen sich all Transaktionen eines Bündels identifizieren, die sich auf ein zu verifizierendes Claim beziehen und ermöglichen eine Zuordnung zwischen Attestation und Claim.

Lesen einer Identität

DID Dokumente und Listen vertrauenswürdiger Identitäten werden in einem MAM-Kanal (public mode) unverschlüsselt gespeichert. Zum Lesen von DID Dokumenten und Listen vertrauenswürdiger Identitäten muss lediglich die Adresse des genutzten MAM-Kanals bekannt sein. Da die ID einer Identität auf der MAM-Wurzel (erste Nachricht eines MAM-Kanals) gespeichert wird, besteht das

Lesen von DID Dokumenten im Abrufen der ersten MAM Nachricht. Neben der DID und den Listen sind weitere Informationen notwendig, um Claims und Attestations im IOTA Tangle zu lesen. Um einen Claim zu lesen, muss die zu prüfende ID und der Claim Type bekannt sein. Der Hash beider Informationen ergibt die Transaktionsadresse des Claims, von der die unverschlüsselten Daten gelesen werden können. Ein ähnliches Vorgehen ist für das Lesen von Attestations notwendig. Prinzipiell wird beim Lesen von Attestations von zwei Situationen ausgegangen. In der ersten Situation ist die Identität (Certifier) bekannt, die eine Attestation zu einem Claim ausgestellt hat und die Transaktionsadresse einer Attestation wird direkt ermittelt. Wohingegen in einer zweiten Situation, die verifizierende Identität (Certifier) einer zu lesenden Attestation unbekannt ist. In dieser Situation, wird die in einem MAM-Kanal gespeicherte Liste vertrauenswürdiger Identitäten genutzt, um für alle gelisteten Identitäten eine Transaktionsadresse zu generieren und zu prüfen. Lassen sich durch die gespeicherte Liste vertrauenswürdiger Identitäten keine gültigen Transaktionsadressen bilden und keine Attestation zu einem bestimmten Claim lesen (direkt Vertrauensbeziehung), ist es möglich weitere Prüfungen durch die Listen bekannter Identitäten durchzuführen (indirekte Vertrauensbeziehungen).

Ändern einer Identität

Vertrauenswürdige Identitäten werden durch öffentliche Schlüssel und einen frei wählbaren Vertrauenswert repräsentiert. Ändern sich Vertrauensbeziehungen zwischen Identitäten, erfolgt eine Aktualisierung der Vertrauenswerte. Hierzu wird eine neue MAM Nachricht erstellt und einem MAM-Kanal einer Identität hinzugefügt. Jede gültige Aktualisierung wird durch eine Entität digital signiert. Aktualisierungen enthalten einen Verweis auf eine vorangegangene Aktualisierung bzw. MAM Nachrichten, um eine korrekte Aktualisierungsreihenfolge zu gewährleisten. Anderen Entitäten ist es somit möglichen, stets eine aktuelle Liste vertrauenswürdigen Identitäten zu erhalten. Die Aktualisierung eines Claims oder einer Attestation ist gleichbedeutend mit der Veröffentlichung eines Claims. Die chronologische Reihenfolge der Aktualisierungen wird sichergestellt, indem alle Aktualisierungen auf den vorherige Transaktionsbundelhash referenziert werden.

Löschung einer Identität

Eine Löschung ist gleichbedeutend mit Aktualisierungen von Attestations. Eine Attestation kann als widerrufen bzw. nicht mehr gültig betrachtet werden, wenn der ursprüngliche Vertrauenswert auf Null aktualisiert wird. Eine Identität kann als widerrufen betrachtet werden, wenn alle Ansprüche über sie widerrufen wurden.

6.2.2 Authentifizierung

Zur Authentifizierung einer Identität sind verlässliche Identitätsinformationen notwendig. Die Abschätzung der Verlässlichkeit von Identitätsinformationen repräsentiert ein wichtiges Kernelement vieler IAM Anwendungen. In frei zugänglichen und dezentralen Systemen, in denen Identitätsinformationen nicht mehr durch eine einzelne Autorität selbst verwaltet werden, sind Mechanismen zur Bewertung von Identitätsinformationen erforderlich. Im Rahmen dieser Arbeit wird ein WoT Modell genutzt, um die Bewertung von Identitätsinformationen zu ermöglichen. Mit Hilfe einer vereinfachten Funktion lässt sich das Vertrauen in unbekannte Identitäten bzw. in Identitätsinformationen quantifizieren. Hierzu wird zunächst ein Intervall definiert, mit dem sich Vertrauensbeziehungen zwischen Identitäten beschreiben lassen. Beispielsweise lassen sich Vertrauensbeziehungen durch Werte innerhalb eines Intervalls von null bis fünf beschreiben. Der Wert null repräsentiert ein Misstrauen bzw. den niedrigsten Vertrauenswert, wohingegen der Wert fünf den höchsten Vertrauenswert darstellt.

Zur Quantifizierung von Vertrauensbeziehungen ist es zudem notwendig, Informationen bestehender WoT Graphen zu berücksichtigen. Direkte und Indirekte Vertrauensbeziehungen die über ein WoT Graphen abgebildet werden, sollten in der Bewertung von Identitätsinformationen unterschiedlich gewichtet werden. Durch die Veröffentlichung von Listen vertrauenswürdigen Identitäten in einem frei zugänglichen MAM-Kanal (public mode), lässt sich für jede Identität ein WoT Graph mit vertrauenswürdigen Identitäten bilden. Selbstorganisierte Systeme, die auf solchen WoT basierten Zertifikatsgraphen basieren, weisen Ähnlichkeiten zu sozialen Netzwerken auf und folgen dem Small-World-Phänomen [241]. Diesem

Phänomen nach ist jeder Mensch (sozialer Akteur) mit jedem anderen Menschen auf der Welt über eine Kette von maximal sechs Bekanntschaftsbeziehungen miteinander verbunden. Übertragen auf das IoT in dem hauptsächlich Sensormodule und Netzwerke miteinander kommunizieren, ist es Identitäten ebenfalls möglich ihre WoT Graphen automatisiert zu durchsuchen, um Identitäten zu finden, die einen zu prüfenden Claim attestiert haben. Je nach Vertrauensbeziehung (direkt oder indirekt) bzw. der Tiefe des WoT Graphen, kann die Vertrauenswürdigkeit einer Identität evaluiert werden.

Zur kumulativen Quantifizierung der Verlässlichkeit von Identitätsinformationen werden indirekte Vertrauensbeziehungen geringer gewichtet als direkte Vertrauensbeziehungen. Hierdurch wird einer direkten Vertrauensbeziehung zwischen zwei Identitäten, eine höhere Verlässlichkeit zugeordnet. Möchte beispielsweise ein Sensormodul der Identität X die Verlässlichkeit eines Claims C1 prüfen, können hierzu WoT Graphen genutzt werden (vgl., Abbildung 6.2). Die Identität X bezieht hierzu eine Attestation (A1) des zu verifizierenden Claim C1 über eine direkte Vertrauensbeziehung zur bekannten Identität Y, sowie eine weitere Attestation (A3) über eine indirekte Vertrauensbeziehung zur Identität Z. Zur Quantifizierung der Verlässlichkeit wird vom Claim C1 die direkte Vertrauensbeziehung zwischen den Identitäten X und Y anders gewichtet, als die indirekte Vertrauensbeziehung zur Identität Z. Die Verlässlichkeit in den Claim C1 wird durch das persönliche Vertrauen der Identität X in die verifizierenden Identitäten Y und Z bestimmt.

6.2.3 Autorisierung

Nach einer erfolgreichen Prüfung von Identitätsinformationen erfolgt die Autorisierung bzw. die Freigabe von Zugangsrechten. Für den Entwurf eines dezentralen Autorisierungskonzepts werden im Wesentlichen Interaktionen zwischen drei Entitäten berücksichtigt. Zu diesen Entitäten gehören Datenproduzenten wie Sensormodule, die von Dateneigentümer kontrolliert werden und ihre Daten mit Datenkonsumenten teilen.

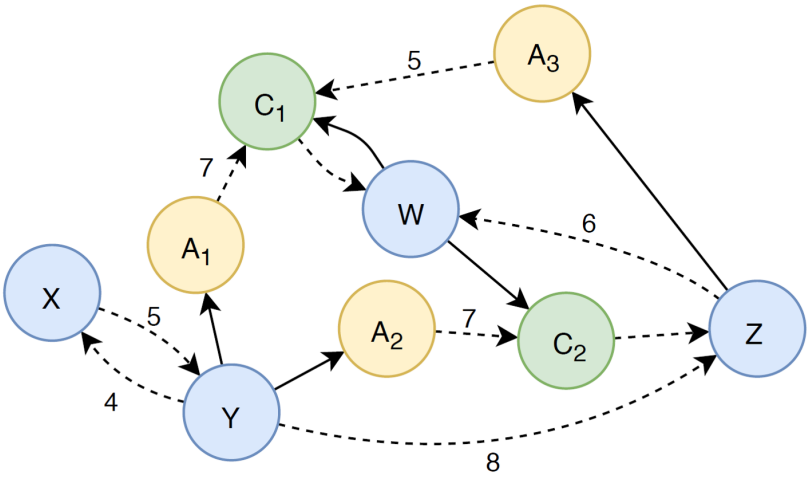

Abbildung 6.2: Skizze eines WoT Graph bestehend aus Identitäten (X;Y;Z;W), Claims (Ci) und Attestations (Ai). Pfeile zwischen Identitäten repräsentieren Vertrauensbeziehungen und können sowohl unilateral als auch bilateral sein [2]

Interaktionen zwischen Entitäten starten mit einer initialen Kopplung (Paring) zwischen einem Datenproduzenten und einem Dateneigentümer zum Austausch kryptografischer Schlüssel. Nach einer erfolgreichen Kopplung sendet der Datenproduzenten verschlüsselte Datenpakete an den IOTA Tangle. Anschließend können Datenkonsumenten einem Dateneigentümern Datenanfragen senden, um einen Zugriff auf einzelne Datenpakete eines Datenstroms zu erhalten. Werden Datenanfragen vom Dateneigentümer akzeptiert, werden den Datenkonsumenten alle zur Entschlüsselung der gespeicherten Datenpakete notwendigen Informationen übermittelt. Mit den erhaltenden Informationen können Datenkonsumenten eigenständig alle zur Entschlüsselung notwendigen Schlüssel bzw. Zugriffsrechte erstellen und die angefragten Datenpakete entschlüsseln. Die unterschiedlichen einzelnen Phasen der initialen Kopplung, Verschlüsselung, Speicherung und Entschlüsselung der Datenpakete werden im Folgenden beschrieben.

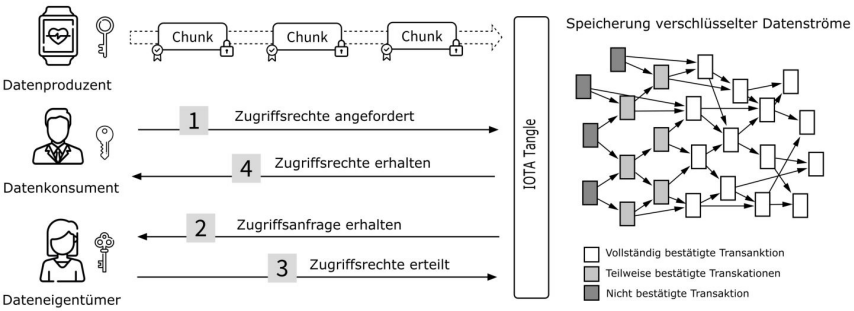

Abbildung 6.3: Skizze einer dezentrale Datenverwaltung von IoT-Datenströme

Kopplung

Während einer initialen Kopplung zwischen Dateneigentümer und Datenproduzenten, wird eine IOTA Seed auf einem Sensormodul gespeichert. Mit Hilfe eines IOTA Seeds werden kryptografische Schlüssel erstellt, um MAM Nachrichten zu verschlüsseln. Seeds sollten auf einem vertrauenswürdigen Hardware-Modul des genutzten Sensormoduls gespeichert werden, um IOTA Seeds vor einem unerlaubten Zugriff zu schützen. Mikrocontroller vieler Sensormodule, wie beispielsweise der ESP32, verfügen über Secure Boot und Flash Encryption Funktionen [242], mit denen sich ein IOTA Seed vor einem unerlaubten Zugriff schützen lässt.

Verschlüsselung

MAM-Kanäle erlauben es Dateneigentümern ihre Datenströme über MAM Nachrichten im IOTA Tangle zu verwalten. Im eingeschränkten (restricted) Modus werden einzelne Datenpakete eines MAM-Kanals mit Sidekeys (SK) verschlüsselt (vgl. Abbildung 6.4). Eigentümer eines MAM-Kanals müssen zur Generierung von Sidekeys keine besonderen Spezifikationen berücksichtigen, wie beispielsweise einer bestimmten Schlüssellänge. Eine schematische Darstellung eines eingeschränkten MAM-Kanals ist in Abbildung 6.4 dargestellt.

Vielen Studien [243, 244, 245] haben eingeschränkte MAM-Kanäle genutzt, um einen feingranularen Datenzugriff auf Datenströme zu ermöglichen. Die Verwaltung von Datenzugriffsberechtigungen durch Sidekeys ist dadurch limitiert,

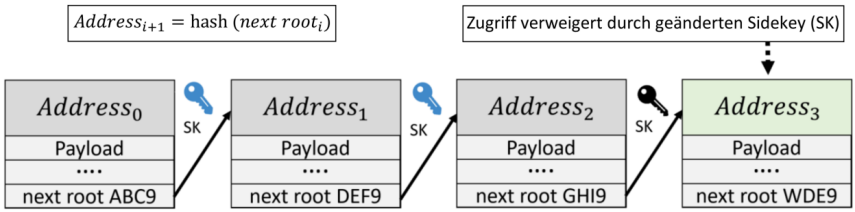

Abbildung 6.4: Eingeschränkter (restricted) MAM-Kanal

dass für die Aktualisierung von Zugriffsberechtigungen neue Sidekeys an alle Datenkonsumenten eines Datenstroms gesendet werden müssen. Unterschiedliche Zugriffsberichtungen eines Datenstroms sind nicht möglich. Die Granularität, mit der Datenpakete eines Datenstroms mit unterschiedlichen Konsumenten bzw. Anwendungen geteilt werden können, ist nicht individuell wählbar. Effiziente Methoden zur Verwaltung der Sidekeys sind notwendig, um einen hohen Kommunikationsaufwand für die Aktualisierung der Sidekeys an unterschiedliche Datenkonsumenten zu reduzieren und die Definition beliebige Granularitätsstufen zu ermöglichen.

Zur effizienten Verwaltung genutzter Sidekeys wird ein graph-basiertes Schema genutzt, mit dem sich effizient Sidekeys für beliebige Granularitätsstufen generieren und an unterschiedliche Datenkonsumenten verteilen lassen. Zur Generierung der Sidekeys erhalten zunächst alle Datenpakete eines von Sensormodulen erzeugten Datenstroms einen Zeitstempel. Die Zeitstempel eines jeden Datenpakets können in einer unterschiedlichen Granularität wie Jahr, Monat, Tag, Stunde und Minute erstellt werden. Je nach der Granularität der erstellten Zeitstempel, variiert die Anzahl der zur Verschlüsselung genutzten Sidekeys einzelner Datenpakete. Sollen beispielsweise Zeitstempel mit einer Granularität von Stunden genutzt werden, so werden alle Daten die vom Sensormodul innerhalb einer Stunde erstellt werden, in einem Datenpaket zusammengefasst und mit einem Sidekey verschlüsselt. Eine selektive Freigabe der Daten mit einer Granularität von Minuten ist anschließend nicht mehr möglich. Stündlich generierte Datenpakete können zu einer höheren Granularität zusammengefasst und freigegeben werden.

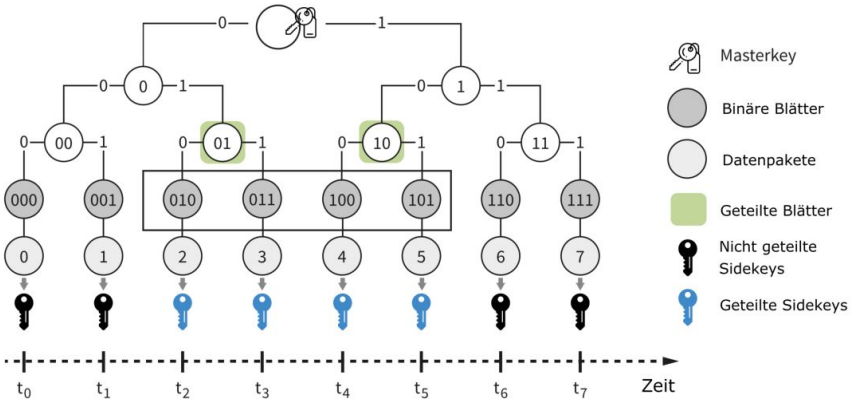

Abbildung 6.5: Hashbaum-basiertes Schema zur effizienten Verwaltung von SideKeys (SKs).

Nachdem die Granularität der Datenverschlüsselung definiert wurde, werden alle Zeitstempel in eine binäre Darstellung konvertiert. Beispielsweise beträgt für den Monat Mai (05), die binäre Darstellung 101. Eine Konvertierung der numerischen in binäre Werte führt zur Erstellung eines Binärbaums. Damit sich diese zum Verwalten von Sidekeys nutzen lässt, erfolgt eine Normalisierung des Binärbaums. Hierzu werden alle Binärzahlen normalisiert, um für jede einzelne Stufe eines Binärbaums einen minimal- und maximal Wert festzulegen. Somit wird für eine Granularität auf Monatsebene ein Binärbaum mit insgesamt 16 Blättern (unterste Stufe des Baums) statt 12 Blätter benötigt (vgl. Abbildung 6.5). Nur durch das Hinzufügen von vier weiteren Blättern, lässt sich ein ausgeglichener Binärbaum erstellen, mit dem es Datenkonsumenten möglich ist, aus einem empfangenen Sidekey einer Stufe, alle dieser Stufe zugehörigen Sidekeys eigenständig zu erstellen.

Durch die selektive Freigabe von Sidekeys und zusätzlichen Informationen zum genutzten Binärbaum, kann ein Dateneigentümer mehreren Datenkonsumenten Datenpakete unterschiedlicher Granularität zur Verfügung zu stellen. Diese Verfahren ermöglicht es, Dateneigentümern sowohl bereits vergangene als auch zukünftige Zeitspannen freizugeben.

Nach der Festlegung der Datengranularität und der Generierung eines ausgeglichenen Binärbaums, werden vom Datenproduzenten (Sensormodul) alle Sidekeys erstellt. Ein Mastersecret wird sequentielle mit allen binären und normalisierten Zeitstempeln aller Stufen des Binärbaums mit einem SHA256 Hashing Algorithmus gehasht. Die Hashwerte der letzten Stufen bzw. Blätter des Baumes, ergeben die zur Verschlüsselung der Datenpakete genutzten Sidekeys.

Speicherung

Für eine verteilte Datenspeicherung wird der IOTA Tangle als Distributed Ledger genutzt. Die Datenspeicherung im IOTA Tangle erfolgt auf Full Nodes, die gültige Transaktionen von Light Nodes empfangen und diese zu ihrer Kopie des gesamten Ledgers hinzufügen, alle betroffenen Transaktionsadressen aktualisieren und diese Aktualisierungen an weitere Full Nodes senden. Light Nodes speichern nicht die gesamten Daten eines Distributed Ledgers und werden zum Erstellen von Transaktionsadressen und zum Signieren von Transaktionen genutzt. Ein Sensormodul, das nicht über die notwendigen Ressourcen verfügt, den jeweils aktuellen Zustand des gesamten Distributed Ledgers zu speichern, kann als Light Node direkt Daten über das MAM-Protokoll an Full Nodes übertragen. Light Nodes müssen keinem spezifischen Full Node vertrauen, um verschlüsselte MAM Nachrichten an den Distributed Ledger zu übertragen und können Nachrichten über unterschiedliche Full Nodes an den Distributed Ledger senden.

Entschlüsselung

Für die Entschlüsselung einzelner Datenpakete eines Datenstroms erhält der Dateneigentümer eine Zugriffsanfrage vom Datenkonsumenten, mit Informationen zur Zeitspanne (Start- und Endzeitpunkt) der angeforderten Daten. Diese Anfrage kann vom Dateneigentümer akzeptiert oder ablehnt werden. Wird die Anfrage vom Dateneigentümer akzeptiert, müssen für die Entschlüsselung einzelner Datenpakete notwendigen Sidekeys (SKs) ausgetauscht werden. Dateneigentümer berechnen den Teilbaum ihres Hash-Baums, der nur Knoten enthält, die zur Berechnung der Sidekeys für den angeforderte Zeitspanne benötigt werden. Soll beispielsweise Datenpakete mit dem Zeitstempel von t2 bis t4 geteilt werden,

so müssen die in Abbildung 6.5 grün markierten Sidekeys zwischen dem Dateneigentümer und Datenkonsumenten ausgetauscht werden. Die Sidekeys werden zusammen mit einer MAM-Nachrichtenadresse an den Datenkonsumenten gesendet. Hat der Datenkonsument die Nachricht des Dateneigentümer erhalten, kann er mit dem Lesen des Datenstroms beginnen. Der Datenkonsument nutzt die erste MAM-Nachrichtenadresse des angefragten Datenabschnitts und überprüft das unverschlüsselte, lesbare Tag-Feld der MAM-Nachricht. Aus diesem Tag-Feld enthält er einen Zeitstempel, der zunächst vom Datenkonsumenten in eine binäre Darstellung umgewandelt wird. Anhand dieser binären Darstellung werden die benötigte Sidekeys der einzelnen Knoten des Binärbaums berechnet. Schließlich werden die MAM-Nachricht mit Hilfe der berechneten Sidekeys entschlüsselt und der Datenkonsument kann auf die angeforderten Datenpakete zugreifen.

6.3 Evaluierung

Basierend auf den vorgestellten Anforderungen, folgt die Evaluierung der entwickelten Konzepte zur gegenseitigen Identifikation, Authentifizierung und Autorisierung in dezentralen Netzwerken.

Skalierbarkeit

Die Evaluierung der Skalierbarkeit erfolgt durch eine Abschätzung der Operationskomplexität. Die Verifizierung eines unbekannten Claims repräsentiert die aufwändigste Operation des vorgestellten Konzepts zur Identifikation und Authentifikation. Zur Verifizierung eines Claims müssen Nachrichten von MAM Kanälen (Request MAM; RMAM) und von Transaktionsadressen (Request Adresse; RA) gelesen werden. Für jede einzelne Verifizierung ist eine RMAM Abfrage zur Bestimmung des DID auf der Root Adresse eines MAM Kanals und eine RA Abfrage zur Bestimmung der Liste vertrauenswürdiger Identität notwendig. Für eine Tiefe D eines WoT Graphen und einer durchschnittlichen Anzahl n an Identitäten je Liste, ergibt sich;

$$\Big(\sum_{d=1}^{D-1} (n_t)^d (RMAM + RA) \Big) + (n_t)^D RMAM \tag{6.1}$$

Für die letzte Stufe eines WoT Graphen entfällt eine Transaktionsabfrage (RA) zur Ermittlung vertrauenswürdiger Identitäten. Sofern WoT Graphen gebildet wurden und die öffentlichen Schlüssel vertrauenswürdiger Identitäten bekannt sind, erfolgt die Verifizierung eines Claims. Hierzu wird geprüft, ob es Attestations des zu verifizierenden Claims von einer direkt oder indirekt bekannten Identität gibt. Hierzu ist je Identität eine weitere Transaktionsabfrage notwendig.

$$\Big(\big(\sum_{d=1}^{D-1} (n_t)^d (RMAM + RA) \big) + (n_t)^D RMAM) \Big) RA \tag{6.2}$$

WoT Graphen mit bekannten Identitäten wachsen stetig und nicht abrupt. Die Listen vertrauenswürdiger Identitäten können daher lokal von Entitäten zwischengespeichert werden, zumal nicht für jede Verifizierung ein komplett neuer WoT Graphen erzeugt werden muss. Speichern Entitäten ihre WoT Graphen lokal, reduziert sich die Anzahl notwendiger Anfragen dramatisch auf,

$$n * RA \tag{6.3}$$

Basierend auf einem proportionalen Anstieg nicht interaktiver Transaktionsabfragen, erfolgt eine skalierbare Authentifizierung, die in einem IoT Ökosystem mit vielen Millionen von Sensormodulen bzw. Entitäten genutzt werden kann.

Portabilität

Digitale Identitäten und quantifizierbare WoT Graphen werden vollständig innerhalb eines public permissionless Distributed Ledgers verwaltet. Voraussetzungen, wie beispielsweise der Besitz von Bitcoin Token zum Bezahlen von Mininggebühren, müssen nicht erfüllt werden. Zudem wurden bekannte Standards zum Aufbau selbstverwalteter Identitäten genutzt. Frei von Restriktionen und einem

internationalen Standard zum Aufbau von selbstverwalteten Identitäten folgend, lassen sich die vorstellten Konzepte zur Identifikation und Authentifikation von digitalen Identitäten für viele Anwendungen nutzen.

Privatsphäre

Informationen zu digitalen Identitäten und Vertrauensbeziehungen sind frei zugänglich im Distributed Ledger gespeichert. Es steht allen Entitäten offen, sich eigenständig über andere Identitäten zu informieren. Die Privatsphäre einer Entität wird durch die vorgestellten Konzepte nicht vollständig geschützt. Ein Schutz der Privatsphäre einer Entität wird lediglich dadurch erzielt, dass Transaktionsadressen eines Claims oder einer Attestations sich ohne Informationen über eine Identität im IOTA Tangle kaum finden lassen. Kennt ein potenzieller Angreifer lediglich das DID Dokument einer Identität, so ist es ihm ohne weitere Informationen kaum möglich die Transaktionsadressen aller Claims und Attestations einer Identität im IOTA Tangle zu lesen. Hierzu müssen Claim Typ und die Claim verifizierende Identität bekannt sein. Die Anforderungen die Privatsphäre einer Entität zu schützen wird nicht vollständig erfüllt.

Vertrauen

Die quantifizierbare Bestimmung der Verlässlichkeit von Identitätsinformationen und der damit einhergehende Vertrauensaufbau zwischen Entitäten gehört zu den wichtigsten Merkmalen vernetzter Anwendungen im IoT. Durch quantifizierbare WoT Graphen, die innerhalb eines public permissionless Ledgers verwaltet werden, ist es allen Entitäten möglich Vertrauensbeziehungen aufzubauen und zu bewerten. Anders als in vielen bisherigen Studien, erfolgt die vorgestellte Authentifizierung nicht interaktiv. Entitäten müssen keine Smart Contracts zu hohen Gebühren ausführen lassen oder auf Aktion bzw. Freigaben anderer Entitäten warten. Entitäten können zudem Funktionen zur Quantifizierung der Verlässlichkeit von Identitätsdaten frei und flexible gestalten. Die Anforderungen der Generierung gegenseitiger Vertrauensbeziehung wird als erfüllt bewertet.

Sicherheit

In zugangsfreien Systemen, wie dem IOTA Tangle, sind Sybil-Angriff möglich. Bekannte Mechanismen zum Schutz vor Sybil-Angriffe beruhen auf Überprüfung digitaler Identitäten durch eine Autorität, wie beispielsweise einer Zertifizierungsauthorität. In dem vorgestellten Konzept wird ein negativer Einfluss durch Sybil-Angriffen dadurch begrenzt, dass neu generierte Identitäten über keine Vertrauenswerte verfügen und damit von anderen realen Identitäten als nicht verlässlich eingestuft werden. Sybil-Angriffe können dennoch erfolgreich sein, sofern es einer Sybil-Identität gelingt, Vertrauensbeziehungen zu realen Identitäten aufzubauen.

Zusätzlich zur Evaluierung der identifizierten Anforderungen, wurden Messungen einer prototypischen Implementierung durchgeführt. Ziel dieser experimentellen Messungen ist es, für unterschiedliche Granularitätsstufen die Rechenzeit unterschiedlicher Operationen zu bestimmen. Zu den evaluierten Operationen gehören die Generierung von Sidekeys, das Publizieren verschlüsselter Datenpakete, sowie das Entschlüsseln von Datenpaketen aus dem IOTA Tangle. Die Messungen wurden auf einem Full Node und einen Light Node durchgeführt. Der Full Node wird repräsentiert durch einen Ubuntu-Desktop-Computer mit Intel(R) Xeon(R) Gold 6140 CPU, 2,30 GHz mit 16 GB Speicher und der Light Node durch einem Raspberry Pi 3B.

Generierung von Sidekeys

Aus der Perspektive des Datenproduzenten wurde die Berechnungsdauer für die Generierung von Sidekeys (engl. Side Key Creation, SKC) bestimmt. Mit Hilfe der zwei Nodes wurde für unterschiedliche Granularitätsstufen die durchschnittliche Berechnungsdauer zur Generierung von Sidkeys bestimmt (vgl., Tabelle 6.1). Für jeden Node und jede Granularitätsstufe wurden jeweils insgesamt 1000 Berechnungen durchgeführt. Datenpakete mit der Bezeichnung YMDHM repräsentieren Granularitätsstufen mit einem Zeitstempel bestehend aus Angaben des Jahres (Y), Monats (M), Tages (D), Stunde (H) und Minute (M).

Für diese Berechnungen wird von einem Full Node (Desktop-Computer) eine durchschnittliche Berechnungsdauer von 13,1 ms für die Verschlüsselung von Datenpaketen mit einer YMDH Granularitätsstufe benötigt. Verglichen mit dem

Hardwaremodul		YMD	YMDH	YMDHM
Desktop computer	Avg	10.1	13.1	16.5
	Max	18.5	29.5	43.6
	Min	8.5	8.6	10.7
Raspberry Pi 3	Avg	119.3	142.4	174.3
	Max	166.7	194.1	278.7
	Min	109.8	109.8	133.2

Tabelle 6.1: Rechenzeit zur Generierung von SideKey (SKC) in Millisekunden, unter Verwendung verschiedener Hardwaremodule und Granularitätsstufen

genutzten Light Node (Raspberry Pi) ist die Berechnungsdauer für die Generierung von Sidekeys etwa 11 mal kürzer. Da Sidekeys nur einmal während einer anfänglichen Initialisierung generiert werden, beeinflusst die Berechnungsdauer zur Generierung von Sidekeys nicht zwangsläufig die benötigte Dauer zum Teilen bzw. Freigeben von Datenpaketen. Sidekeys können zunächst auf einem Desktop-Computer generiert und anschließend auf ein vertrauenswürdiges Hardware-Modul eines Sensormoduls bzw. eines Light Nodes übertragen werden. Sollen alle Sidekeys auf einem Raspberry Pi generiert werden, beträgt für die feinste Granularitätsstufen die maximale Berechnungsdauer 278 ms.

Datenspeicherung

Aus der Perspektive des Dateneigentümers wurde die benötigte Zeit für die verschlüsselte Speicherung von Datenpaketen unterschiedliche Granularitätsstufen evaluiert. Im Gegensatz zu anderen Distributed Ledgern erlaubt der IOTA Tangle die Auslagerung von PoW-Berechnung. Light Nodes können signierte und verschlüsselte Nachrichten an Full Nodes senden, um PoW Berechnungen durchzuführen. Es wurden Messungen durchgeführt, in denen PoW Operationen lokal (L) auf dem Raspberry Pi, als auch remote (R) mit Hilfe eines Hardwarebeschleunigers (Field Programmable Gate Array, FPGA) eines externen PoW Dienstes [246] durchgeführt wurden.

Konfiguration	AVG (ms)	%-SKC	%-MC	%-ATT
Local-YMDHM	183.5	0.61%	10.40%	88.99%
Remote-YMDHM	183.8	0.68%	11.59%	87.73%
Local-YMDH	154.6	0.52%	10.66%	88.81%
Remote-YMDH	159.9	1.87%	36.96%	61.17%
Local-YMD	120.2	0.39%	10.08%	89.53%
Remote-YMD	151.4	1.54%	32.23%	66.22%

Tabelle 6.2: Rechenzeit eines IoT Geräts (Raspberry Pi) für den SKC in Millisekunden. Prozentuale Angaben beziehen sich auf die gesamte Dauer der SKC, MC und ATT Operationen.

Alle Messungen wurden mit einem lokalen IOTA Tangle TestNet mit einer Mindestgewichtsgröße (MWM) von 14 durchgeführt, um Netzwerkverzögerungen zwischen dem IOTA Tangle und dem Raspberry Pi auszuschließen und reproduzierbare Ergebnisse zu erzielen. Die gewählte MWM entspricht den Sicherheitsanforderungen des IOTA Tangle MainNets und repräsentiert die Mindestanzahl an Nullen, mit denen ein gültiger PoW-Transaktions-Hash einer Nachricht enden muss.

Diese gesamte Berechnungsdauer setzt sich zusammen aus der Generierung von Sidekeys (Sidekey Creation, SKC), der Nachrichtenerstellung (Message Creation, MC) und dem Anhängen (Attachment, ATT) der Nachrichten an das TestNet. Die erzielten Ergebnisse zeigen, dass die Berechnungsdauer maßgeblich durch PoW Operationen für das Anhängen verschlüsselte Nachrichten an den IOTA Tangle bestimmt wird (siehe Tabelle 6.2). Bezogen auf die gesamte Berechnungsdauer, beansprucht die Generierung von Sidekeys prozentual zwischen 0,5% und 1,6%. Die Geschwindigkeit mit der verschlüsselte Nachrichten sich über einen IOTA Tangle teilen lassen, wird wesentlich durch die genutzten Hardwaremodule bestimmt, mit denen PoW Operationen ausgeführt werden und nicht von der gewählten Granularität, mit der Datenpakete eines kontinuierlichen Datenstroms verschlüsselt werden.

Konfiguration	AVG (ms)	%-SKC	Total (ms)
YMDHM	10.3	21.11%	48.9
YMDH	10.7	20.67%	51.9
YMD	10.2	21.70%	47.0

Tabelle 6.3: Rechenzeit eines IoT Geräts (Raspberry Pi) für die SKC in Millisekunden zur Entschlüsselung von MAM Nachrichten bezogen auf die Gesamtzeit zur Datenabfrage aus dem IOTA Tangle.

Empfangen und Entschlüsseln von Datenpaketen

Aus Sicht der Datenkonsumenten wurde die vom Raspberry Pi benötigte Zeit zum Empfangen und Entschlüsseln der Datenpaketen bestimmt. Die notwendige Zeit zur Generierung von Sidekeys um Datenpakete zu entschlüsseln, ist kaum abhängig von den gewählten Granularitätsstufen und beträgt zwischen 10,2 bis 10,7 ms (vgl., Tabelle 6.3). Im Vergleich zur Datenspeicherung, hat damit die Zeit zur Generierung von Sidekeys einen prozentualen Anteil von etwa 20% an der Gesamtdauer des Datenzugriffs. Das Herunterladen verschlüsselter Datenpaketen vom TestNet, die Generierung von Sidekeys und die Entschlüsselung der Datenpakete kann innerhalb vom etwa 50 ms erfolgen, wodurch ein schneller und feingranularer Datenzugriff auf verschlüsselte Datenpakete möglich ist.

7 Datenmonetarisierung

Dieses Kapitel befasst sich mit der letzten Fragestellung dieser Arbeit und soll darstellen, wie sich Daten von Sensormodulen bzw. IoT-Geräten monetarisieren lassen. Hierzu wird zunächst beschrieben, mit welchen aktuellen Herausforderungen die Monetarisierung von Daten verbunden ist. Anschließend wird ein System zur Datenmonetarisierung vorgestellt und evaluiert. Die Evaluierung basiert auf einer durchgeführten Sicherheitsanalyse sowie experimentellen Messungen. In einem exemplarischen V2X Anwendungsszenario wurden anhand experimenteller Messungen die zur Datenmonetarisierung erforderlichen Kosten und Kommunikationsdauern bestimmt.

Ergebnisse diese Kapitels wurden in einer wissenschaftlichen Veröffentlichungen [J2] des Autors in Zusammenarbeit mit weiteren Co-Autoren publiziert.

7.1 Bestehende Limitierungen

Fehlende Anreizmechanismen schränken die Bereitschaft zum Teilen von Daten stark ein. Die Gestaltung von Anreizmechanismen zum Teilen von Daten scheitert an wirtschaftlichen Herausforderungen, die Eigentümer von Sensormodulen oder Fahrzeugen nicht ausreichend zu motivieren, ihre Daten mit anderen Entitäten zu teilen. Durch die Integration eines Zahlungsdienstes in bestehende Systeme, lassen sich monetäre Anreize zum Teilen von Daten schaffen, wodurch es zu einem Wechsel vom kostenlosen Datenaustausch hin zum Datenhandel kommen [247, 248].

Die durch einen Datenmonetarisierung erzielten Zahlungen sollten mindestens die mit dem Datentransfer verbundenen Monetarisierungskosten decken, sowie weitere Anreize für einen Datentransfer bieten. Die im IoT bzw. in einer Smart City gehandelten Datenpakete haben einen geringen Wert von lediglich einigen Mikro-Cents [249] und liegt damit weit unter den Vermittlungsgebühren vieler Zahlungsdienstleister. Hohe Transaktionsgebühren verhindern eine wirtschaftliche Datenmonetarisierung zwischen unterschiedlichen Entitäten [250, 251]. Ein System zur Datenmonetarisierung im IoT sollte dezentralisiert allen Entitäten frei zugänglich sein, um Vermittlungsgebühren und Abhängigkeiten von externen Zahlungsdienstleistern zu vermeiden.

Eine Dezentralisierung von Zahlungssystemen ist mit vielen technischen Herausforderungen verbunden. Dateneigentümer und Datenkonsumenten müssen in einem dezentralen und frei zugänglichen System darauf vertrauen können, dass Zahlungen verlässlich durchgeführt werden. Außerdem sind Mechanismen notwendig, mit denen sich die Zuverlässigkeit anderer Entitäten hinsichtlich gemachter Datenangebote und der bisherigen Zahlungsmoral bewerten lassen. Reputationsmechansimen vieler zentralisierter Datenhandelsplattformen lassen sich in frei zugänglichen und dezentralen Systemen zum Handeln von Daten nicht nutzen.

Eine Vielzahl an mobilen und portablen Sensormodulen innerhalb einer Smart City, erschwert durch limitierte Kommunikationsdauern zum Datentransfer, eine direkte Datenmonetarisierung zwischen Entitäten. Beispielsweise beträgt die Kommunikationsdauer zwischen zwei mobilen Fahrzeugen, die Daten über ein gemeinsames VANET miteinander austauschen möchten und sich mit 50 km/h aufeinander zu bewegen, lediglich 35 s [252][1]. Ob sich innerhalb einer stark limitierten Kommunikationsdauer alle Operationen einer erfolgreiche Datenmonetarisierung verlässlich bewältigen lassen, ist unklar.

[1] maximale Kommunikationsreichweite von 500 m

Diverse Forschungsarbeiten [249, 253] versuchten durch einen Einsatz der DLTs bestehende Herausforderungen der Datenmonetarisierung zu adressieren. Beispielsweise wurden DLT eingesetzt, um eine Unabhängigkeit von zentralen Instanzen zu erreichen [254, 255] und Zahlungen mit geringen Transaktionsgebühren zu ermöglichen [256, 257]. Bestehende Studien [258, 259] kamen zu dem Ergebnis, dass trotz vorteilhafter Eigenschaften vieler DLTs zur Datenmonetarisierung, mehrere DLT-Eigenschaften im Widerspruch zu den Eigenschaften einer direkten drahtlosen Ad-hoc Kommunikation in VANETs stehen. Beispielsweise übersteigt die notwendige Transaktionsbestätigungsdauer vieler DLTs, die verfügbare Kommunikationsdauer zwischen Entitäten in einem gemeinsamen VANET. Damit ist ungewiss, inwieweit sich DLTs nutzen lassen, um die vielfältigen Herausforderungen eines offenen Datenhandels in dynamischen Netzwerken zu bewältigen.

7.2 Systementwurf

Das entworfene System zur Monetarisierung von kleinen Datenmengen besteht aus sogenannten X-Nodes (d.h. Fahrzeugen und Road-Side-Units) und einem Distributed Ledger (siehe Abbildung 7.1). Road-Side-Units (RSUs) repräsentieren Sensormodule, die in Straßennähe positioniert werden. X-Nodes können sowohl die Rolle eines Datenanbieters, als auch Datenkonsumenten annehmen. Als Datenanbieter bieten sie ihre Daten, wie beispielsweise Angaben zu CO2-Emissionen [260], anderen X-Nodes zum Datenhandel an. Die Rolle eines Datenkonsumenten wird von X-Nodes angenommen, die ein Angebot eines Datenanbieters akzeptieren.

Der Austausch gehandelter Daten erfolgt in VANETs über die DSRC Kommunikation (vgl. Abschnitt 2.1). X-Nodes nutzen zum Datenhandel einen Distributed Ledger, um sich zu gegenseitig zu Authentifizieren, Reputationen zu empfangen bzw. abzugeben und gehandelte Daten zu vergüten. Zur Authentifizierung prüfen X-Nodes die auf dem Distributed Ledger gespeicherten Identitätsinformationen

potenzieller Datenhandelspartners. X-Nodes nutzen im Distributed Ledger gespeicherte Reputationen, um die Zuverlässigkeit eines potenziellen Datenhandelspartners zu bewerten. Kleinstbeträge für empfangene Daten werden von X-Nodes durch einen Transfer der Kryptowährungen (IOTA Token) vergütet. Funktechnologien werden für die Kommunikation zwischen X-Nodes und dem Distributed Ledger genutzt. Stationäre X-Nodes kommunizieren mit dem Distributed Ledger über stationäre Netzwerke, wohingegen mobile X-Nodes Mobilfunknetze nutzen. Stationäre Netzwerke ermöglichen hohe Datenraten und geringen Netznutzungskosten, verglichen mit Mobilfunknetzen. Dennoch haben stationäre Netzwerke eine begrenzte Kommunikationsreichweite und können keine permanente Kommunikation zu mobilen X-Nodes gewährleisten. Zur vollständigen Netzwerkabdeckung und permanenten Konnektivität zwischen mobilen X-Nodes und dem Distributed Ledger, werden Mobilfunknetze benötigt. Anders als bei stationären Netzwerken, ist die Datenübertragungsgeschwindigkeit mobiler Netzwerke stark begrenzt, wodurch es bei zu hohen Datenübertragungsgeschwindigkeit zu längeren Datenübertragungszeit kommen kann [261].

Der zum Aufbau eines Datenhandelssystems erforderliche Distributed Ledger, besteht aus einem IOTA Tangle. Der IOTA Tangle ermöglicht eine hohe Skalierbarkeit, einen hohen Transaktionsdurchsatz und Kleinstzahlungen zwischen X-Nodes. Zudem ist der IOTA Tangle für alle X-Nodes frei zugänglich, erhebt keine Mininggebühren und ermöglicht X-Nodes durch vereinfachten PoW-Operationen einen freien Daten und Tokentransfer (vgl. Abschnitt 2.3).

7.2.1 Datenhandelsphasen

Der Datenhandel zwischen X-Nodes kann in eine Abfolge von drei Phasen (siehe Abbildung 7.1) unterteilt werden; der Kaufentscheidung, dem Datenaustausch und der Bewertungsphase. Jeder Datenhandel beginnt mit einer Kaufentscheidungsphase, in der sich die X-Nodes authentifizieren. Im Anschluss einer erfolgreichen

Authentifizierung, entscheiden X-Nodes auf Basis der Reputation ihres Handelspartners, ob sie Daten miteinander handeln möchten. Soll es zu einem Datenaustausch kommen, beginnen beide X-Nodes in der Datenaustauschphase mit der Eröffnung eines Zahlungskanals. Sind alle zu monetarisierenden Daten zwischen X-Nodes ausgetauscht, wird der Zahlungskanal geschlossen und es startet die letzte Phase der gegenseitigen Bewertung. In dieser letzten Phase übermitteln beide X-Nodes ihre Bewertungen des Datenhandels dem Distributed Ledger bzw. dem IOTA Tangle.

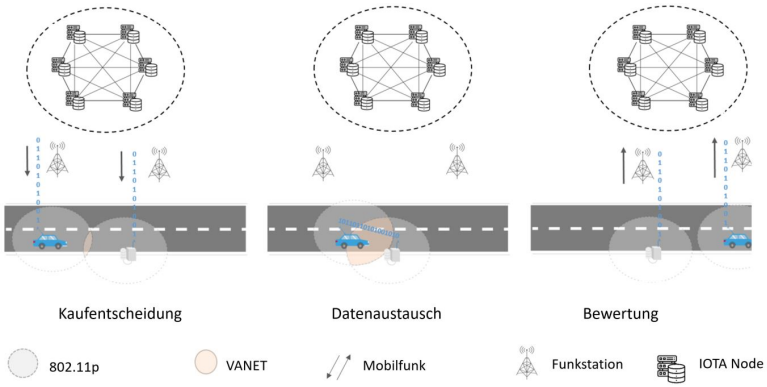

Abbildung 7.1: Schematischer Überblick des entworfenen Datenhandelssystems. Zur besseren Lesbarkeit wurde die Kommunikation mit dem Distributed Ledger für die Erstellung der Multi-Signature-Adresse während der Austauschphase weggelassen

Werbephase

X-Nodes informieren potenzielle Datenhandelspartner über Daten, die sie monetarisieren möchten. Zu diesem Zweck erstellt ein Datenanbieter ein Angebot. Dieses Angebot wird digital signiert und als Werbenachricht versendet. Alle X-Nodes im Umfeld bzw. im gleichen VANET des Datenanbieters, empfangen dessen Werbenachricht. In Form eines DID-Dokuments enthält die Werbenachricht Informationen über die Identität des Datenanbieters (vgl. Abschnitt 6.2.1). Zudem enthält die Werbenachricht Informationen zum angebotenen Datensatz, wie beispielsweise dem Fahrzeugtyp oder Emissionsstandard und dem Datenpreis.

Entspricht das Angebot einer Werbenachricht den individuellen Kriterien eines X-Nodes, kann der Angebotsempfänger (Datenkonsument) mit dem Datenanbieter über ein gemeinsames VANET einen Datenhandel beginnen.

Kaufentscheidung

Der Datenkonsument kann anhand der empfangenden Werbenachricht, die Identität des Datenanbieters prüfen. Hierzu nutzt er den in der Nachricht bzw. dem DID Dokument enthaltenden öffentlichen Schlüssel des DID Dokuments eines X-Nodes. Mit Hilfe eines öffentlichen Schlüssels können überprüfbare Angaben, die mit einer Identitätsadresse des Datenanbieters verbunden sind, aus dem Distributed Ledger geladen werden. Dabei repräsentiert eine Identitätsadresse eine Transaktionsadresse in IOTA Tangle, auf der ein DID Dokument eines X-Nodes gespeichert ist (vgl. Abschnitt 6.2.1). Datenkonsumenten betrachten zur Authentifizierung einer digitalen Identität ausschließlich verifizierbare Claims eines Datenanbieters, die vertrauenswürdigen X-Nodes ausgestellt wurden. Ein X-Node gilt als vertrauenswürdig und wird zur Authentifizierung berücksichtigt, sofern eine Identität verifizierbare Claims des Datenkonsumenten sowie des Datenanbieters ausgestellt hat (direkte Vertrauensbeziehung) [262].

X-Nodes die Daten zum ersten Mal monetarisieren wollen, beginnen mit dem niedrigsten Vertrauenslevel, zumal ihrer Identitätsadresse keine verifizierbaren Claims zugeordnet sind. X-Node Eigentümer haben ein Interesse daran, die Identitätsangaben ihre X-Nodes durch vertrauenswürdige Dritte oder öffentliche Institutionen verifizieren zu lassen, um Vertrauen zu anderen X-Nodes aufzubauen. Zusätzlich zu verifizierbaren Claims, die sich auf Angaben einer Identität beziehen, werden verifizierbare Claims bisheriger Datenmonetarisierungen des Datenanbieters auf einer Reputationsadresse im Distributed Ledger gespeichert. Ähnlich den Identitätsadressen stellen Reputationsadressen im IOTA Tangle ein Dokument dar, mit dem sich die Reputation eines X-Nodes bewerten lässt.

Der Datenkonsument erzeugt eine Antwortnachricht, sofern er die Identität des Datenanbieters erfolgreich authentifizieren konnte und dessen Reputation den Anforderungen des Datenkonsumenten entspricht. Die gesendete Antwortnachricht enthält den öffentlichen Schlüssel des Datenkonsumenten und eine Bestätigung

der bestehenden Handelsbedingungen oder ein Gegenangebot mit neuen Bedingungen. Der Datenkonsument signiert die Antwortnachricht und verschlüsselt diese mit dem öffentlichen Schlüssel des Datenanbieters, noch bevor er diese ins gemeinsame VANET sendet. Zusätzlich enthält die Antwortnachricht noch einen Zeitstempel und eine Zufallszahl, um Replay Attacken zu vermeiden. Hat der Datenanbieter eine Antwortnachricht erhalten, authentifiziert auch dieser den Datenkonsumenten und prüft dessen Reputation nach dem beschriebenen Verfahren.

Datenaustausch

Diese Phase beschreibt den Austausch und die Vergütung gehandelter Daten. Hierzu sind im Wesentlichen drei Teilphasen notwendig, bestehend aus dem Öffnen eines Zahlungskanals, dem eigentlichen Austausch monetarisierter Daten und Token, sowie dem Schließen des genutzten Zahlungskanals. Für das Öffnen eines Zahlungskanals benötigen beide X-Nodes einen gemeinsamem Schlüssel. Hierzu beginnen beide X-Nodes mit der Berechnung und dem Austausch eines AES-Schlüsselfragments (Advanced Encryption Standard). Durch die Addition der zwei AES-Schlüsselfragmente bilden beide X-Nodes einen gemeinsamen Schlüssel zum Öffnen eines Zahlungskanals. AES-Schlüsselfragmente werden in einer Nachricht mit dem öffentlichen Schlüssel des Handelspartners verschlüsselt, um einen sicheren Austausch zu gewährleisten. Anderen X-Nodes im VANET bleiben somit die ausgetauschten AES-Schlüsselfragmente verborgen.

Im weiteren Verlauf des Datenhandels werden die zwischen beiden Datenhandelspartnern ausgetauschten Nachrichten mit Hilfe des gemeinsamen AES Schlüssels geschützt. Eine symmetrische Verschlüsselung der Nachrichten durch nur einen gemeinsamen Schlüssel, ist aufgrund einer geringere Verschlüsselungsdauer, effizienter als eine asymmetrische Verschlüsselung [263]. Konnten beide X-Nodes einen gemeinsamen AES Schlüssel erzeugen, erfolgt die Öffnung eines Zahlungskanals im IOTA Tangle (vgl. Abschnitt 2.3).

In der nächsten Teilphase tauschen Datenkonsument und Datenanbieter Kleinstzahlungen und Datensätze aus. Der Datenkonsument erstellt und signiert ein Transaktionsbündel, um einen Datensatz zu bezahlen. Diese Transaktionsbündel wird als verschlüsselte Zahlungsnachricht ins VANET gesendet, um vom Datenanbieter

empfangen zu werden. Der Datenanbieter kann mit Hilfe des gemeinsamen AES Schlüssels, die durch das VANET empfangene Zahlungsnachricht entschlüsseln und das Transaktionsbündel anhand eines Bündel-Hash prüfen. Gültige Transaktionsbündel werden vom Datenanbieter digital signiert und lokal gespeichert. Der Datenanbieter sendet anschließend eine weitere Zahlungsnachricht zurück an den Datenkonsumenten. Diese Nachricht enthält eine gültige Signatur des Transaktionsbündel-Hash, um Token der IOTA Kryptowährung von einer gemeinsamen Multi-signature IOTA Adresse übertragen zu können. Zusätzlich zu dieser Bestätigung einer ersten Kleinstzahlung durch das Transferieren von Token, enthält diese Nachricht den bezahlten Datensatz. Auch diese Zahlungsnachricht wird verschlüsselt und über das VANET zwischen beiden Handelspartnern ausgetauscht. Dieser Vorgang der Bezahlung getauschter Daten wiederholt sich solange, bis alle zu monetarisierten Datensätze übertragen und bezahlt worden sind, oder die Kommunikation zwischen beiden X-Nodes vorläufig stoppt.

In der letzten Teilphase, dem Schließen des Zahlungskanals, beenden Datenkonsument und Datenanbieter den Datenhandel. Beide X-Nodes verifizieren, ob alle IOTA Token erfolgreich auf ihre gemeinsame Multi-Signatur-Adresse übertragen wurden. Erhalten die X-Nodes eine Bestätigung vom IOTA Tangle, können die X-Nodes jederzeit unabhängig voneinander den Zahlungskanal schließen. Hierzu senden beide X-Nodes ihre signierten Transaktionen an den IOTA Tangle, wodurch der Tokentransfer von der gemeinsamen Multi-signature IOTA Adresse beginnen kann. Im Gegensatz zu den beiden vorangegangenen Teilphasen ist für die Schließung des Zahlungskanals keine DSRC-Kommunikation zwischen den X-Nodes in einem gemeinsamen VANET mehr erforderlich.

Bewertung

Nach der Datenmonetarisierug folgt die gegenseitige Bewertung. Hierzu werden reputationsbezogene, verifizierbare Claims im IOTA Tangle gespeichert. Ein verifizierbarer Claim kann beispielsweise belegen oder widerlegen, ob die gehandelten Daten mit dem Datenangebot aus der Werbenachricht übereinstimmten. X-Node

senden zur gegenseitigen Bewertung eine IOTA-Transaktion an die Reputationsadresse ihres entsprechenden Handelspartners. Diese Transaktionen repräsentieren verifizierbare Claims und enthalten eine Bewertung zwischen null und fünf, um der Aussagen im DID-Dokument des jeweiligen Datenhandelspartners nicht zuzustimmen (null) oder vollkommen zuzustimmen (fünf). Die Aggregation dieser Bewertungen repräsentiert die Reputation eines X-Nodes.

7.2.2 Prototypische Implementierung

Zur Implementierung und Evaluierung des konzeptionierten Systems zum Monetarisieren geringer Datenmengen, wurde ein mobiler (Pkw) und ein stationären (RSU) X-Node genutzt. Die RSU wird repräsentiert durch das entwickelte Multisensormodul SCN (siehe Kapitel 4). Vom Pkw werden zum Verkauf stehende Fahrzeugparametern von einer On-Board-Unit (OBU) und einem GPS-Modul extrahiert. Zusätzlich sind beide X-Nodes mit kleinen Mikrocontrollern und Kommunikationsmodulen ausgestattet. Ein LTE/UMTS-Modul des Pkw und ein herkömmlicher WiFi-Router (Speedport Smart 3) der RSU werden zur Kommunikation zwischen den X-Nodes und dem IOTA Tangle eingesetzt. Für eine Ad-hoc Kommunikation gemäß den DSRC-Standards, wurde ein WiFi-Router (TP-Link WDR 3600) genutzt. Zur standardisierten Kommunikation im VANET, wurde die Open-Source Prototyping-Plattform OpenC2X auf dem Router implementiert [264]. Beiden X-Nodes ist es somit möglich, in einem gemeinsamen VANET über das IEEE 802.11p Protokoll miteinander zu kommunizieren [265]. Das IEEE 802.11p Protokoll überträgt Daten zwischen X-Nodes schneller als andere drahtlose Kommunikationsprotokolle, wie beispielsweise Bluetooth [266], nutzt ein kostenloses Frequenzspektrum (ITS-G5) um Übertragungskosten zu reduzieren [267] und ist nicht auf feste Funkstationen angewiesen [268].

Kooperative Awareness-Nachrichten (engl. Cooperative Awareness Messages, CAMs) wurden genutzt, um Daten zwischen X-Nodes im VANET zu übertragen [269]. Spezifische Nachrichten, wie beispielsweise Zahlungsnachrichten, können durch Änderungen des Headers und des Textfelds einer standardisierten CAM

übertragen werden. Eine einzelne IOTA-Transaktion hat eine Größe von 1590 Bytes [270] und lässt sich nicht durch eine einzelne CAM mit einer maximalen Größe von 1300 Bytes [271] übertragen. Mehrere CAMs müssen versendet werden, um eine einzige IOTA-Transaktion zwischen X-Nodes zu übertragen. Hierzu wird jede CAM mit einem Attribut versehen. Dieses Attribut kann Informationen der individuellen Nummer einer CAM, sowie der Gesamtzahl auszutauschender CAMs enthalten. Auf diese Weise können X-Nodes prüfen, ob alle CAM erfolgreich übertragen wurden.

Das Speichern von Transaktionen in dem IOTA Tangle sollte möglichst effizient erfolgen. Lange Berechnungszeiten limitierten die zum Datenhandel verfügbare Zeit zwischen mobilen X-Nodes. Durch eine Parallelisierung von PoW-Operationen lassen sich Transaktionen innerhalb kurzer Zeit im IOTA Tangle speichern. Field Programmable Gate Arrays (FPGAs) können zur Parallelisierung eingesetzt werden, um Berechnungszeiten für PoW-Operationen zu reduzieren. Verglichen mit Single-Core-Prozessoren, wie einem Raspberry Pi 3B, lässt sich die Berechnungszeiten für PoW-Operationen um einen Faktor von bis 300 verringern [272]. Durch den Einsatz eines Zynq Z-7020 FPGA-Boards [273] wurden PoW Operationen zur Bestimmung gültiger Nonce innerhalb von 400 ms durchgeführt. In dem evaluierten Szenario eines Datenhandels zwischen zwei X-Nodes, verfügt der Pkw als mobiler X-Node über ein FPGA Board zur beschleunigten PoW Berechnung. PoW Operationen die zeitnah durchgeführt werden müssen, um beispielsweise eine gemeinsamen Multi-Signature-Adresse zu erstellen, werden mit Hilfe des FPGA Boards vom Pkw durchgeführt.

Zwei separate Transaktionsadressen, eine Identitäts- und eine Reputationsadresse, werden zum Handeln von Daten genutzt. Auf diesen Adressen werden Informationen über die Identität des X-Nodes und bisherigen Datenhandel öffentlich zugänglich und unverschlüsselt gespeichert. X-Nodes senden verifizierbare Claims an beide Adressen, um Identitätsangaben zu bestätigen bzw. einen abgeschlossenen Datenhandel zu bewerten. IOTA-Transaktionen in denen der öffentliche Schlüssel eines X-Nodes, dessen digitale Signatur und Identitätsbestätigung oder Rating-Score bezüglich des Datenhandels enthalten sind, repräsentieren verifizierbare Claims. Während der Phase einer Kaufentscheidung werden ausschließlich

verifizierbare Claims berücksichtigt, dessen öffentliche Schlüssel von bekannten X-Nodes stammen.

7.3 Sicherheitsanalyse

7.3.1 Netzwerkkommunikation

Anhand des Dolev-Yao-Angreifermodells [274] wurde die Sicherheit des entwickelten Systems zum Monetarisieren geringer Datenmengen aus der Netzwerkperspektive erörtert. Dieses Angreifermodell berücksichtigt einen unsicheren Kommunikationskanal zwischen zwei X-Nodes und einen Angreifer als aktiven Saboteur. Der Angreifer verfügt im Wesentlichen über sechs Fähigkeiten zur Handhabung von Nachrichten [275]: Abhören, Fälschen, Wiedergeben, Verzögern und Beschleunigen, Neuordnung und Löschung.

Abhören (engl., Eavesdropping); Ein Angreifer hört im Netzwerk übertragene Nachrichten ab.

X-Nodes senden Nachrichten ins VANET, die alle sich im VANET befindlichen X-Nodes empfangen können. Von allen empfangenen Nachrichten, sind ausschließlich Werbenachrichten unverschlüsselt und damit für alle X-Nodes im gemeinsamen VANET lesbar. Mit dem öffentlichen Schlüssel eines X-Nodes oder einem generierten AES-Schlüssel werden alle weiteren Nachrichten, wie beispielsweise Zahlungsnachrichten, verschlüsselt. Ohne diese Schlüssel ist es einem Angreifer nur schwer möglich vertrauliche Nachrichten zwischen zwei X-Nodes zu entschlüsseln bzw. zu lesen. Der Angreifer muss einen sehr hohen Aufwand in Form von vielen Rechenressourcen aufbringen, um die Datenverschlüsselung zu brechen. Die mit diesem Aufwand verbundenen Kosten übersteigen den tatsächlichen Wert gehandelter Daten. Das Lesen von ausgetauschten und gehandelten Daten durch einen Angreifer ist daher unwahrscheinlich.

Daten werden nicht nur zwischen X-Nodes, sondern ebenfalls zwischen einzelnen X-Nodes und dem IOTA Tangle ausgetauscht. Das hierzu genutzt Hypertext-Transfer-Protokoll (HTTPS) verhindert, dass ein Angreifer zwischen X-Nodes und dem IOTA Tangle ausgetauschte Nachrichten lesen kann. Auch wenn es einem Angreifer nicht möglich ist, Daten zwischen X-Nodes untereinander bzw. dem IOTA Tangle zu lesen, so ist es ihm dennoch möglich Analysen zum Datentransfer durchführen. Sofern ein X-Nodes ausschließlich ein einzigen IOTA Node für seine gesamte Interaktion mit dem IOTA Tangle nutzt, wie beispielsweise dem Verschieben von IOTA Token, ist es einem Angreifer möglich über eine Kontrolle dieses einen IOTA Node, den öffentlichen Schlüssel eines X-Nodes mit Zahlungsinformationen in Verbindung zu bringen.

Fälschung (engl., Forging); Neue Nachrichten werden vom Angreifer erstellt und in eine Sequenz von Nachrichten eingefügt.

Bis auf Werbenachrichten sind alle Nachrichten die zwischen X-Nodes via DSRC übertragen werden, digital signiert und mit einem RSA (1024-Bit-Schlüssellänge) oder mit AES Schlüssel (128-Bit-Schlüssellänge) verschlüsselt. Signierte und verschlüsselte Nachrichten können vom Angreifer nicht manipuliert werden. X-Nodes erkennen durch Überprüfungen digitaler Signatur manipulierte Nachrichten und ignorieren diese.
Aufgrund der Verwendung des HTTPS und von IOTA genutzten digitalen Signaturschemas, kann ein Angreifer keine Nachrichten fälschen. Sollte es einem Angreifer gelingen einen IOTA Node zu kompromittieren, kann dieser Anfragen der X-Nodes an den IOTA Node ignorieren und gefälschte Nachrichten an X-Nodes zurücksenden. Gefälschte Nachrichten eines IOTA-Nodes können anhand von kompromittierten Signaturen von X-Nodes erkannt werden. X-Nodes könnten auch Daten von mehrere IOTA-Nodes anfragen und erhaltene Nachrichten miteinander vergleichen. Für einen Angreifer ist es mit sehr hohen Rechenressourcen verbunden eine ausreichende Anzahl von IOTA-Nodes zu kompromittierten und zu betreiben. Diese Kosten übersteigen die durch einen Datenhandel im IoT erzielten Gewinne. Ein Angreifer der Nachrichten fälscht, indem er eine ausreichende Anzahl von IOTA-Node kontrolliert, ist unwahrscheinlich.

Wiederholung (engl., Replaying); Bereits gesendete Nachrichten werden vom Angreifer abgefangen und erneut versendet.

Von einem Angreifer können während eines Datenhandels ausgetauschten Nachrichten zwischengespeichert und zu einem späteren Zeitpunkt erneut versendet werden. Zwischen X-Nodes ausgetauschte Nachrichten enthalten Attribute, die eine Sequenznummer und einen Zeitstempel enthalten, um sich wiederholende Nachrichten zu identifizieren.
Von X-Nodes an den IOTA Tangle gesendete Transaktionen führen häufig zu einem Transfer von IOTA Token. Das Senden von wiederholte IOTA-Transaktionen ist ungültig, da die IOTA Token sich nicht mehr auf einer nur einmal zu nutzenden Adresse befinden. Das wiederholte Versenden von Transaktionen zur Bewertung eines X-Nodes führt dazu, dass einer Reputationsadresse eines X-Nodes mehrere identische verifizierbare Claims zugewiesen werden. Diese sich wiederholenden, verifizierbaren Claims haben identische Transaktionshashwerte und können von X-Nodes erkannt und ignoriert werden. Wiederholungsangriffe eines Angreifers sind daher entweder ungültig, weil sich beispielsweise keine Token mehr auf einer Adresse befinden, oder werden von X-Nodes ignoriert. Das vorgestellte System ist damit nicht anfällig für Wiederholungsangriffe.

Verzögern und Beschleunigen (engl., delaying and rushing); Die Zustellung von Nachrichten wird von einem Angreifer verzögert oder beschleunigt.

Eine Verzögerung beim Datenaustausch kann die verfügbare Zeit zur Datenmonetarisierung reduzieren. Einem Angreifer ist es schwer möglich Nachrichten (CAMs) zu verzögern, zumal im VANET alle Nachrichten zwischen X-Nodes direkt (single-hop) ausgetauscht werden.
Während der Kaufentscheidungsphase kann eine Verzögerung von Anfragen an den IOTA Tangle, die verfügbare Zeit zur Kommunikation im VANET reduzieren. Anfragen an den IOTA Tangle in nicht zeitkritisch Phasen, wie beispielsweise der Bewertungsphase, beeinträchtigen nicht den Datenhandel, zumal sich Verzögerung nicht auf die verfügbare Zeit zum Austausch von Datensätzen durch eine Ad-hoc DSRC Kommunikation auswirken.

Umordnung (engl., Reordering); Die Zustellungsreihenfolge von Nachrichten wird vom Angreifer geändert.

In VANETs kommunizieren X-Nodes direkt miteinander, wodurch es einem Angreifer nicht möglich ist die Zustellungsreihenfolge von Nachrichten zu ändern.
Ein Angreifer kann darauf abzielen, einzelnen Anfrage an einen IOTA-Node umzuordnen. Eine Umordnung von Nachrichten wird durch das genutzte HTTPS, Transport Layer Security (TLS) und das Transmission Control Protocol (TCP) erschwert [276]. Ein Angreifer kann durch ein Umordnen von Nachrichten die Kommunikation zwischen X-Nodes und IOTA-Nodes nicht stören.

Löschen (engl., Deleting); Nachrichten werden von einem Angreifer gelöscht.

Datenkonsument und Datenanbieter kommunizieren direkt miteinander. Das Löschen von Nachrichten, die von einem Angreifer empfangen werden, hat keine Auswirkungen auf den Datenhandel.
Ein Angreifer kann darauf abzielen, Anfragen von X-Nodes durch kompromittierten IOTA-Node zu löschen oder Nachrichten in der Kommunikation zwischen den X-Nodes und dem IOTA Tangle zu verwerfen, wie beispielsweise durch eine Kompromittierung des lokalen Routings. X-Nodes können jedoch ihre Anfrage an den IOTA Tangle stets wiederholen, wenn sie innerhalb einer bestimmten Zeitspanne keine Antwort erhalten. Erneute Anfragen von X-Nodes reduzieren jedoch die verfügbare Dauer zur Datenmonetarisierung und somit die Anzahl der zwischen X-Nodes gehandelten Datensätze.

7.3.2 Konzepte der Datenmonetarisierung

Neben einer Sicherheitsanalyse auf Netzwerkebene, soll zusätzlich berücksichtigt werden, wie sicher die zum Datenhandel bereitgestellten Konzepte sind. Es wird angenommen, dass ein Angreifer sich auf die vorgestellten Konzepte zur Authentifizierung und Bewertungen fokussiert. Cyber-physikalische Angriffe durch die Errichtung von physischen Barrieren oder Funkstörung, um die Nachrichtenübertragung im VANET zu behindern, wurden nicht berücksichtigt. Ebenfalls

wurde ein unehrliches Verhalten von X-Nodes beim Erstellen von verifizierbaren Claims nicht berücksichtigt. Beispielsweise werden von X-Node Eigentümern keine negative Bewertung über einen zufriedenstellenden, positiven Datenhandel abgegeben.

Abbruch (engl., Aborting); Der Datentransfer wird von einem X-Node abgebrochen, noch bevor der Datenhandel abgeschlossen ist.

Datenanbieter oder Datenkonsumenten können jederzeit die Übertragung von Daten abbrechen. Token beider Handelspartner verbleiben bei einem vorzeitigen Abbruch auf der gemeinsamen Multi-Signature-Adresse, zumal nur ausgetauschte Datensätze direkt bezahlt wurden. Es ist unwahrscheinlich, dass X-Nodes einen Datenhandel freiwillig abbrechen und somit das Risiko eingehen, gesperrte IOTA Token auf einer gemeinsamen Multi-Signature-Adresse zu verlieren.

Schlechtreden (engl., bad mouthing); Ein Angreifer bewertet mehrfach andere X-Nodes, um dessen Reputation zu manipulieren.

Mit Hilfe des öffentlichen Schlüssels eines X-Nodes, ist es einem Angreifer möglich negative Bewertungen abzugeben. Öffentliche Schlüssel von X-Nodes kann der Angreifer beispielsweise aus Werbenachrichten extrahieren. X-Nodes berücksichtigen nur verifizierbare Claims, die von bekannten X-Nodes ausgegeben wurden (direkte Vertrauensbeziehung). Einem Angreifer muss es gelingen vertrauensvolle Beziehungen, beispielsweise durch einen erfolgreichen Datenhandel, zu zahlreichen anderen X-Nodes aufbauen. Ohne solche Beziehungen zu realen X-Nodes, haben seine Bewertungen keinen Einfluss auf die Reputation eines spezifischen X-Nodes. Bei der Berechnung der Reputation eines X-Nodes wird zudem nur der aktuellste Claim berücksichtigt. Eine mehrfache Bewertung eines einzigen X-Nodes hat daher keinen Einfluss auf die Reputation eines X-Nodes.

Verhaltensanalyse (engl., behavior inferring); Das Verhalten eines X-Nodes wird von einem Angreifer analysieren.

Ein Angreifer kann im IOTA Tangle gespeicherte und zugängliche zahlungsbezogene sowie reputationsbezogene Daten nutzen, um X-Nodes zu analysieren. Zahlungsbezogene Daten über einen IOTA Token Transfer geben Aufschluss über

die Uhrzeit und das Datum, an dem eine IOTA-Transaktion ausgestellt wurde. Aus diesen Informationen kann ein Angreifer kann Rückschlüsse auf den Datenhandel zwischen X-Nodes ziehen. Es ist einem Angreifer nicht möglich, die Identität eines X-Node mit IOTA-Transaktion zu verknüpfen, zumal IOTA-Transaktionen zum Transfer von IOTA Token keine öffentlichen Schlüssel eines X-Nodes beinhalten. Einem Angreifer ist es nicht möglich, den öffentlichen Schlüssel eines X-Nodes aus dessen Identitäts- oder Reputationsadresse zu extrahieren, zumal diese durch das Hashing von öffentlichen Schlüsseln und Identitätsattributen bzw. Reputationsansprüchen erzeugt werden (vgl. Abschnitt 6.2.1).

Ausgabe gefälschter Claims (engl., Fake claim issuing); Durch die Erstellung von mehreren verifizierbaren Claims, möchte ein Angreifer die Reputation eines X-Nodes zu manipulieren.

Die Identität eines X-Nodes und dessen Reputation wird durch verifizierbare Claims andere X-Nodes oder Entitäten bestimmt. Neu erstellte Identitäten sind anderen X-Nodes nicht bekannt und beginnen mit dem geringsten Vertrauensniveau im IOTA Tangle. Einem Angreifer wird es nicht gelingen, die Reputation eines X-Nodes zu manipulieren, indem er verifizierbare Claims von neu erstellten Identitäten zur Manipulation seiner eigenen Reputation nutzt, da diese Claims von anderen X-Nodes nicht in Reputationsberechnung berücksichtigt werden.

7.4 Experimentelle Messungen

Wenige Studien [247, 277] analysierten eine kombinierte Nutzung von DLT und VANETs für den Datenhandel zwischen X-Nodes. Ergebnisse bisherigen Forschungsarbeiten basieren hauptsächlich auf Simulationen bzw. vereinfachter Modellannahmen und spiegeln damit das tatsächliche Systemverhalten in realen Verkehrsszenarien nicht wider [278]. In vereinfachten VANET Simulationen werden beispielsweise komplexe Signalinterferenzen nicht berücksichtigt [279].

Experimentelle Messungen diese Arbeit sollen bisherige simulationsbasierten Erkenntnisse durch empirische Einblicke in das Verhalten eines Systems zur Datenmonetarisierung unter realen Bedingungen erweitern. Während der Evaluierung wurden Messungen der verfügbaren Kommunikationszeit und den entstehenden Kosten durchgeführt. In dem evaluierten Anwendungsszenario wurden drei Datensätze zwischen zwei X-Nodes gehandelt (siehe Abbildung 7.2). Bei den X-Nodes handelt es sich um einen mobilen X-Node (Pkw) als Datenproduzent und einen stationären X-Node (RSU) als Datenkonsument. Während der Messungen fuhr der Pkw mit einer konstanten Geschwindigkeit von 30 km/h an der RSU vorbei, die in Straßennähe an einer festen Position installiert wurde.

Abbildung 7.2: Szenario der Evaluierungsmessungen einschließlich des Pkws (a), der befahrenen Straße (b) und der entlang der Straße montierten RSU (c)

Zu Beginn versenden beide X-Nodes in ihrem VANET alle 0,1 s eine Werbenachricht. Wird eine Werbenachricht von einem der beiden X-Nodes empfangen, beginnt die erste Datenhandelsphase der Kaufentscheidung. In dieser Phase werden von beiden X-Nodes jeweils zehn identitätsbezogene Claims von einer Identitätsadresse und 37 reputationsbezogene Claims von einer Reputationsadresse ihres Datenhandelspartners heruntergeladen. Während der Phase des Datenaustausches wurden drei Datensätze mit einer Größe von jeweils 300 Byte gehandelt. Die in dieser Phase zum Datenhandel erforderlichen PoW Operationen aller IOTA-Transaktionen wurden vom Pkw durchgeführt.

Insgesamt wurden zur Evaluierung des offenen Datenhandels zwischen X-Nodes 42 Messungen durchgeführt. Anhand der durchgeführten Messungen konnte ein

Konfidenzintervallbreite von etwa 1s (Konfidenzintervalle auf dem 95 % - Konfidenzniveau: [14.24;15.28] s für die RSU und [13.72;14.78] s für den Pkw) bezüglich der verfügbaren DSRC basierten Kommunikationsdauer bestimmt werden. Eine Erhöhung der Anzahl durchgeführter Messungen hätte sich nicht signifikant auf die Konfidenzintervallbreite der verfügbaren Kommunikationsdauer ausgewirkt.

7.4.1 Kommunikationsdauer

Messung der Kommunikationsdauer beginnen mit dem Zeitpunkt des Erhaltens einer Werbenachricht und enden mit dem Übermitteln einer Bewertung des durchgeführten Datenhandels an den IOTA Tangle. Zur Evaluierung wurden die Kommunikationszeiten aller Phasen eines Datenhandels gemessen (siehe Abbildung 7.3).

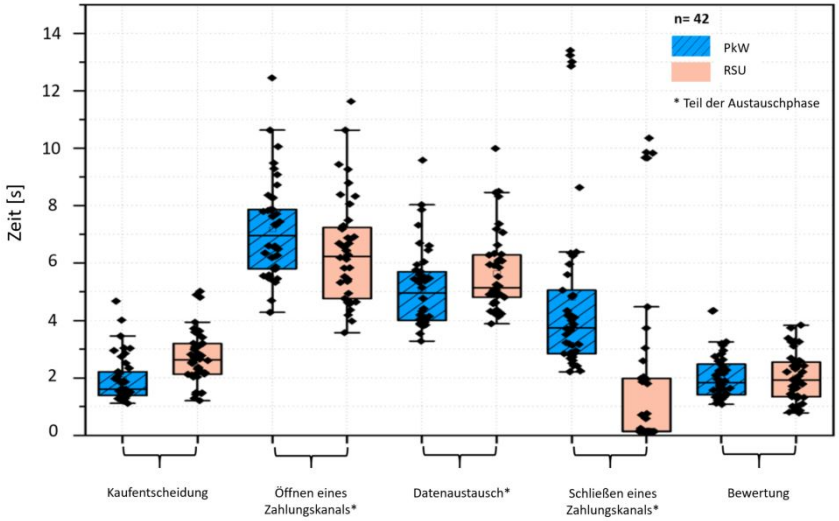

Abbildung 7.3: Kommunikationszeiten aller Datenhandelsphasen die während der Evaluierung zwischen einem stationären und mobilen X-Nodes gemessen wurden

Messungen der Kaufentscheidungsphase beginnen mit dem Erhalten einer Werbenachricht und enden mit der Authentifizierung des Datenhandelspartners sowie der Verifizierung seiner Reputation. Für diese erste Datenhandelsphase benötigte der Pkw durchschnittlich 1,6 s und die RSU 2,8 s (siehe Abbildung 7.3). Die Verlässlichkeit der DSRC basierten Nachrichtenübertragung kann zwischen beiden X-Nodes variieren und zu unterschiedlichen Kommunikationszeiten führen.

Erst unterhalb einer Entfernung von 140 m wurden Nachrichten zwischen X-Nodes verlässlich übertragen. Eine Verschlechterung der Nachrichtenübertragung bei einer zunehmenden Entfernung zwischen X-Nodes, war nicht für beide X-Nodes identisch. Die RSU konnte bei gleicher Entfernung mehr Nachrichten erfolgreich empfangen als der Pkw. Unterschiedliche Übertragungsqualitäten der CAMs im VANET können mit unterschiedlichen Signalabschwächungen zusammenhängen. Die Ausrichtungen und Höhe der für die DSRC verwendeten Antennen können zu unterschiedlichen Abstrahlungsmustern und damit zu unterschiedlichen Erfolgsquoten versendeter Nachrichten führen [280]. Weitere X-Nodes, wie beispielsweise Fahrzeuge, die sich während einer durchgeführten Messung zwischen dem evaluierten Pkw und der RSU befinden, können zusätzlich die Nachrichtenübertragung beeinflussen [281, 279].

Für die Austauschphase wurden Messungen für alle drei Teilphasen (Öffnen des Zahlungskanals, Datenaustausch und Schließen des Zahlungskanals) durchgeführt. Messungen der Kommunikationsdauer der ersten Teilphase beginnen direkt nach der Kaufentscheidungsphase und beendeten mit dem Übermitteln einer Transaktion vom Pkw an den IOTA Tangle. Für diese Teilphase wurde eine mittlere Zeit von 6,2 s für die RSU und 6,9 s für den Pkw bestimmt. Unterschiedliche Kommunikationszeiten der X-Nodes sind darauf zurückzuführen, dass die RSU in dieser Teilphase keine PoW-Operationen durchführt.

Die anschließende Teilphase (Datentransfer) endete mit dem Austausch aller zu handelnden Datensätzen zwischen den beiden X-Nodes, dessen mittlere Dauer 5,1 s für die RSU und 4,9 s für den Pkw betrug. Die Dauer dieser Teilphase wird bestimmt durch die Anzahl der zur Übertragung und Bezahlung der Datensätze ausgetauschten CAMs. Die limitierte Datengröße einer CAM macht es notwendig,

dass insgesamt neun CAMs zwischen X-Nodes ausgetauscht werden müssen, um einen einzigen Datensatz zu monetarisieren. Kann aufgrund von Signalstörungen eine einzelne CAM nicht erfolgreich zugestellt werden, ist die gesamte Zahlungsnachricht unvollständig und zusätzliche Kommunikationszeit wird benötigt, um fehlende CAMs erneut zu versenden.

Die nächste Teilphase (Schließen des Zahlungskanals) endet mit dem Übermitteln eines Transaktionsbündels vom Pkw an den IOTA Tangle und erforderte eine mittlere Zeit von 0,1 s für die RSU und 3,7 s für den Pkw. Die RSU ist nicht mit einem FPGA ausgestattet und führt daher keine Transaktionen zum Schließen eines gemeinsamen Zahlungskanals aus. Von allen Teilphasen der Austauschphase benötigten X-Nodes für das Öffnen eines Zahlungskanals die meiste Zeit (Vergleich Abbildung 7.3), zumal hierzu eine hohe Anzahl an CAMs zwischen den X-Nodes ausgetauscht werden muss und alle PoW-Operationen ausschließlich vom Pkw durchgeführt werden.

Die Phase der gegenseitigen Bewertung beginnt nachdem Transaktionen zum Schließen des Zahlungskanals vom Pkw versendet wurden. Für das Übermitteln von Bewertungen an den IOTA Tangle wurde eine mittlere Kommunikationszeit von 1,9 s für die RSU und 1,8 s für den Pkw gemessen. Die gemessenen Zeiten zwischen den X-Nodes unterscheiden sich nicht signifikant voneinander, zumal beide X-Nodes PoW Operationen mit einem Mikrocontroller ausführen, um Transaktionen auf einer Reputationsadresse zu speichern. Bewertungen eines Datenhandels können jederzeit an den IOTA Tangle übermittelt werden und unterliegen keinen zeitlichen Beschränkungen aufgrund einer limitierten DSRC Reichweite. Beschleunigte PoW-Operationen wurden in dieser zeit-unkritischen Phase nicht durchgeführt.

Alle zeitkritischen Phasen eines Datenhandels (d.h., Kaufentscheidung, Öffnen eines Zahlungskanals, Datentransfer) benötigten insgesamt eine mittlere Kommunikationszeit von 14,6 s. Für eine DSRC-Distanz zwischen den X-Nodes von 140 m (siehe Abbildung 7.2) und einer konstanten Geschwindigkeit des Pkws von 30 km/h, beträgt die verfügbare DSRC-Zeit in einem gemeinsamen VANET

etwa 16,5 s. In allen 42 Messungen wurden alle drei Datensätze erfolgreich zwischen beiden X-Nodes gehandelt. Zwischen beiden X-Nodes könnten wahrscheinlich noch weitere Datensätze gehandelt werden, wird eine DSRC-Reichweite von 280 m aufgrund einer punktsymmetrischen DSRC-Distanz von 140 m zwischen beiden X-Nodes berücksichtigt.

7.4.2 Kommunikationskosten

Für jeden Datenhandel entstehen den X-Nodes Kosten, die sich im Wesentlichen auf die Bereiche der Kommunikation und des Energieverbrauchs beziehen. Die Kommunikation zwischen X-Nodes über das IEEE 802.11p Protokoll des DSRC verursacht keine Gebühren. Lediglich für die Kommunikation zwischen X-Nodes und dem IOTA Tangle fallen Kosten an. Während der Evaluierung der Datentransfers (Daten Up- und Download) zwischen X-Nodes und dem IOTA Tangle, wurden die Kommunikationskosten aller Datenhandelsphasen bestimmt.

Beide X-Nodes laden zur Kaufentscheidung über 47 verifizierbare Claims von zwei IOTA-Adressen herunter. Mit der Anzahl der verifizierbaren Claims, die von X-Nodes benötigen werden, um die Identität und Reputation ihres Datenhandelspartners zu verifizieren, steigen ebenfalls die Kosten für das Herunterladen der Daten. Je mehr verifizierbare Claims die X-Nodes benötigen, desto höher sind die Kommunikationskosten eines Datenhandels. Das Öffnen und Schließen eines Zahlungskanals benötigt ebenfalls einen über Mobilfunk stattfindenden Datentransfer zwischen X-Nodes und dem IOTA Tangle. Der Daten-Upload wird in erster Linie durch das Versenden von IOTA Tansaktionsbündeln verursacht, wohingegen der Daten-Download durch das Abfrage von Daten über eingereichte Transaktionen und einen erfolgreichen IOTA Token Transfer verursacht wird (siehe Tabelle 7.1).

Jeder X-Node hat pro evaluiertem Datenhandel durchschnittlich 37,3 kB an Daten vom IOTA Tangle heruntergeladen und 62,5 kB an Daten zum IOTA Tangle hochgeladen. Damit belaufen sich die Kommunikationskosten für die Nutzung mobiler drahtloser Netze auf etwa 0,055 cent.

Tabelle 7.1: Durchschnittlicher Datentransfer zwischen dem IOTA Tangle und einem einzelnen X-Node während einer Datenhandelssitzung

Datenhandelsphasen	**Download [kB**	**Upload [kB]**
Kaufentscheidung	10,90	5,73
*Öffnen des Zahlungskanals**	11,43	24,43
*Datentransfer**	0,00	0,00
*Schließen des Zahlungskanals**	11,42	19,04
Bewertung	3,50	13,32
Gesamter Datentransfer per X-Node	37,3	62,5

* Teil der Datenaustauschphase

Die Kostenkalkulation basiert auf Business-to-Customer-Preisen für mobiles Breitband in der Europäischen Union von 0,00277 € pro MB für ein mittleres Datenvolumen von 5 GB [282]. Die Kommunikationskosten variieren nicht mit der Menge der zwischen den X-Nodes gehandelten Daten und beziehen sich ausschließlich auf den Datentransfer zwischen X-Nodes und dem IOTA Tangle.

Neben Kommunikationskosten müssen X-Nodes noch weitere variable Kosten für den Stromverbrauch der genutzten Hardwaremodule aufbringen (siehe Tabelle 7.2). Für einen Datenhandel von drei Datensätzen haben beide X-Nodes eine mittlere Kommunikationszeit von 20,2 s benötigt und einen maximalen Stromverbrauch von 18.4 W. Unter Berücksichtigung des Strompreises in Deutschland von 0,3 € pro kWh [283], ergeben sich Stromkosten von 0,0031 cent.

Tabelle 7.2: Stromverbrauch der verschiedenen Hardwaremodule des PkWs in [W]

Hardwaremodul	**Min. [W]**	**Durschn. [W]**	**Max. [W]**
Recheneinheit	3,9	4,9	5,2
DSRC Modul	3,5	4,3	4,9
PoW Beschleuniger	3,1	3,1	3,1
Mobilfunk Modul	5,2	5,2	5,2
Summe	15,7	17,5	18,4

Während der Evaluierung hat ausschließlich der Pkw als mobiler X-Node einen PoW Hardwarebeschleuniger genutzt. Die RSU hat somit einen geringeren Energieverbrauch als das der Pkw. Für jeden Datenhandel benötigte die RSU eine mittlere Kommunikationszeit von 18 s und einen Energieverbrauch von 15,3 W. Die Energiekosten der RSU lagen somit bei 0,0023 cent. Die Kosten der X-Nodes für die Kommunikation und den Energieverbrauch eines Datenhandels mit drei Datensätzen betrugen 0.0581 cents. Für den Handel von IoT Daten sollten diese Transaktionskosten der Datenmonetarisierung unter 2 % des gesamten Datenpreises liegen [249], wodurch der Pkw für die gehandelten drei Datensätze einen Gesamtpreis von mindestens 2.9 cent von der RSU bekäme. Das vorgestellte System erfüllt die Forderung aus früheren Studien [284, 285] nach niedrigen Datenhandelskosten, und macht eine Datenmonetarisierung im IoT bzw. einer Smart City möglich.

8 Zusammenfassung und Ausblick

In diesem Kapitel wird ein Zusammenfassung der vorgestellten Ergebnisse präsentiert. Im Ausblick werden Themen aufgezeigt, die im Rahmen dieser Arbeit nicht oder nur unvollständig behandelt wurden und Anknüpfungspunkte für zukünftige Forschungsarbeiten darstellen.

8.1 Zusammenfassung

Diese Arbeit leistet im im Wesentlichen vier Beiträge zum Aufbau einer vernetzten Stadt, in der Daten frei zwischen Entitäten monetarisiert werden, um Kollaboration zwischen Intelligenten Geräten zu fördern.

Zunächst wurde zur Datenerhebung ein intelligentes Sensormodul, der Smart City Node (SCN), entworfen und unter realen Bedingungen getestet. Der entwickelte SCN ermöglicht eine effiziente Sammlung unterschiedlichster Messgrößen aus den Bereichen Umwelt und Verkehr. Eine intelligente Datenverarbeitung von Verkehrsvideos auf dem SCN garantiert den Schutz der Privatsphäre gefilmter Verkehrsteilnehmer und macht einen Einsatz in realen Messszenarien möglich. Basierend auf einer Vielzahl an Messgrößen repräsentiert der SCN eine Art "Fitness-Tracker"moderner Städte, mit dem sich zukünftig wichtige Faktoren der urbanen Lebensqualität auf lokaler Ebene bestimmen lassen.

Zudem befasste sich diese Dissertation mit der Entwicklung eines dezentralen PMS, um eine effiziente und sichere End-to-End Datenübertragung zwischen portablen Sensormodulen und einem Distributed Ledger zu ermöglichen. Verschiedene digitale Signaturverfahren und Konsensmechanismen wurden evaluiert, um

ein angemessenes Gleichgewicht hinsichtlich des Kompromisses zwischen der Leistung und Sicherheit eines PMS zu erzielen. Die durchgeführten Messungen haben verdeutlicht, welchen großen Einfluss unterschiedliche Konsensmechanismen auf die Leistungsfähigkeit eines Distributed Ledger haben können. Die erzielten Evaluierungsergebnisse dienen als Leitfaden zur erfolgreichen Koppelung von ressourcen-limitierten IoT Geräten und Distributed Ledgern, um kollaborative Forschungsinitiative zwischen unterschiedlichen Stakeholdern bzw. Entitäten zu fördern.

In einem weiteren Kapitel dieser Arbeit wurden innovative Konzepte einer dezentralen Datenverwaltung vorgestellt. Die entwickelten Konzepte kombinieren Vorzüge selbst-verwalteter Identitäten (SSIs), mit denen eines dezentralen WoT Modells zur nicht interaktiven Quantifizierung von Vertrauensbeziehungen. Ein feingranularer Datenzugriff zur gemeinsame Datennutzung verschlüsselter Datenströme, wird durch ein neuartiges Konzept zur effizienten Schlüsselverwaltung ermöglicht. Frei von jeglichen Kontrollinstanzen und Zugangsbeschränkungen fördern die entwickelten Konzepte zur Identifikation, Authentifikation und Autorisierung kollaborative Anwendungsszenarien im IoT.

Abschließend wurden die entwickelten Konzepte genutzt, um Daten im IoT erfolgreich zu monetarisieren. Für unterschiedliche Phasen einer Datenmonetarisierung zwischen mobilen Entitäten wurden experimentelle Messungen durchgeführt. Entgegen den Erkenntnissen bisheriger Studien [258, 259], belegen die vorgestellten Evaluierungsergebnisse, dass eine Monetarisierung von geringen Datenmengen mit Hilfe von DLTs technisch machbar ist und wirtschaftlich sinnvoll sein kann. Durch empirische Einblicke in das Verhalten des entwickelten Systems wurden wertvolle Erkenntnisse zur Datenmonetarisierung im IoT geliefert.

8.2 Ausblick

Trotz der wertvollen Beiträge dieser Arbeit für Kollaborationen zwischen intelligenten Geräten und vernetzten Städten, gehen aus den erzielten Ergebnissen weitere Anknüpfungspunkte für zukünftige Forschungsarbeiten hervor.

Messungen des vorgestellten SCN haben verdeutlicht, dass eine Ausweitung des Messzeitraums und der Messstandorte notwendig ist, um Korrelationen zwischen den erhobenen Messgrößen verlässlich zu analysieren.

Hinsichtlich der vorgestellten Methoden zur gegenseitigen Identifikation und Authentifikation, sollten sich zukünftig Arbeiten vor allem auf den Schutz der Privatsphäre einer Entität fokussieren. Zwar lassen sich Transaktionsadressen eines Claims oder einer Attestations ohne Informationen über eine Identität im IOTA Tangle kaum finden, dennoch werden identitätsbezogenen Daten unverschlüsselt im IOTA Tangle gespeichert. Weitere Mechanismen zur vollständigen Kontrolle der Privatsphäre sind notwendig, um beispielsweise festzulegen welche Informationen einer Identität öffentlich einsehbar sind. Von besonderem Interesse wären beispielsweise Untersuchungen zum Einsatz von Zero Knowledge Proofs (ZKPs) [286] zum Schutz der Privatsphäre in dezentralen Netzwerken.

Zukünftige Arbeiten der Datenmonetarisierung sollten sich mit Datenkomprimierungstechniken befassen. Es gilt zu ein Optimum zu finden zwischen der erforderlichen Verarbeitungszeit zur Komprimierung der zu übertragenden Nachrichten und einer Reduktion der Datenübertragungsdauer durch eine geringere Nachrichtengröße. Zudem wäre es hilfreich, die verfügbare Datenübertragungszeit bereits vor dem Beginn eines Datenhandels zu ermitteln. Somit wäre es möglich, die Anzahl der einzelnen Datensätze zu bestimmen, die während einer einzelnen Datenhandelssitzung ausgetauscht werden können.

A Anhang

Evaluierungsergebnisse verschiedener Konsensmechanismen (d.h. Solo, Kafka, Raft und BFT-SMaRt) für eine unterschiedliche Anzahl von Peer-Knoten (d.h. 4, 8 und 12; außer zentralisierte Solo) zur Messung des max. Transaktionsdurchsatzes.

	Solo			Kafka			Trans.
Kriterium	4	8	12	4	8	12	
Schreibgeschw.	10.10	10.10	10.10	10.10	10.10	10.01	10
Max. Durchsatz	10.00	10.01	10.01	10.01	10.00	10.00	
Durchschn. Latenz	0.34	0.35	0.30	0.35	0.39	0.41	
Max. Latenz	0.56	0.59	0.64	0.59	0.62	0.70	
Schreibgeschw.	50.10	50.10	50.10	50.01	50.01	50.10	50
Max. Durchsatz	50.00	50.00	50.00	50.00	50.00	50.00	
Durchschn. Latenz	0.12	0.13	0.14	0.14	0.16	0.18	
Max. Latenz	0.22	0.25	0.26	0.48	0.45	0.42	
Schreibgeschw.	100.10	100.10	99.80	100.10	100.10	100.10	100
Max. Durchsatz	100.00	100.00	100.00	99.90	99.90	96.90	
Durchschn. Latenz	0.08	0.09	0.12	0.11	0.13	1.68	
Max. Latenz	0.14	0.27	0.44	0.47	0.42	3.93	
Schreibgeschw.	150.10	150.10	150	150.10	150.10	150.10	150
Max. Durchsatz	150.00	149.90	149.69	149.69	117.60	90.41	
Durchschn. Latenz	0.07	0.08	4.51	0.12	8.73	31.58	
Max. Latenz	0.31	0.26	16.25	0.71	21.24	42.86	

	Solo			Kafka			Trans
Kriterium	4	8	12	4	8	12	
Schreibgeschw.	200.10	200.10	200.10	200.10	200.10	200.00	200
Max. Durchsatz	199.89	199.80	137.91	198.70	114.20	85.84	
Durchschn. Latenz	0.06	0.10	18.19	0.61	30.57	54.63	
Max. Latenz	0.16	0.26	36.90	0.97	42.33	68.99	
Schreibgeschw.	249.2	250.10	250.10	250.10	250.10	250.10	250
Max. Durchsatz	249.71	185.09	139.01	169.99	118.70	92.71	
Durchschn. Latenz	0.07	10.55	26.31	19.75	45.56	71.00	
Max. Latenz	0.22	22.16	49.29	30.69	56.26	88.91	
Schreibgeschw.	300.10	298.00	300.10	300	300	300	300
Max. Durchsatz	299.71	185.09	137.30	155.70	121.59	63.51	
Durchschn. Latenz	0.09	26.11	34.35	38.01	59.67	78.20	
Max. Latenz	0.29	37.08	58.20	48.63	74.83	100	
Schreibgeschw.	350.00	350.00	350.10	350	350.10	350.10	350
Max. Durchsatz	264.50	196.70	122.18	166.60	124.99	39.11	
Durchschn. Latenz	9.02	36.67	40.85	46.21	73.88	82.59	
Max. Latenz	21.78	48.97	68.14	58.19	92.50	100	
Schreibgeschw.	400.00	400.00	400.1	400	400.10	397.50	400
Max. Durchsatz	239.32	192.52	129.19	169.08	127.99	30.01	
Durchschn. Latenz	25.30	46.14	43.53	43.91	63.45	87.97	
Max. Latenz	35.73	65.88	59.25	54.51	81.01	100	
Schreibgeschw.	450.00	447.30	437.10	450	449.20	414.1	450
Max. Durchsatz	245.30	181.29	130.39	161.10	147.57	39.59	
Durchschn. Latenz	34.14	54.19	46.05	45.59	63.99	88.57	
Max. Latenz	46.12	75.10	69.01	60.05	83.29	100.33	
Schreibgeschw.	499.99	494.40	499.2	499.90	498.10	384.8	500
Max. Durchsatz	235.07	182.19	130.89	166.92	127.91	35.71	
Durchschn. Latenz	44.04	60.67	46.01	47.13	67.44	88.57	
Max. Latenz	57.41	82.54	61.86	60.43	89.93	100.30	

	Raft			BFT-SMaRt			Trans
Kriterium	4	8	12	4	8	12	
Schreibgeschw.	10.10	10.10	10.10	10.40	10.40	10.40	10
Max. Durchsatz	9.90	10.00	10.00	10.10	10.3	10.30	
Durchschn. Latenz	0.35	0.36	0.37	0.77	0.51	0.78	
Max. Latenz	0.67	0.60	0.61	2.28	1.80	2.30	
Schreibgeschw.	50.10	50.00	50.10	50.40	50.40	50.40	50
Max. Durchsatz	50.00	50.00	50.00	50.00	50.10	50.10	
Durchschn. Latenz	0.13	0.14	0.15	0.15	0.15	0.16	
Max. Latenz	0.28	0.29	0.24	0.28	0.25	0.28	
Schreibgeschw.	100.10	100.10	100.00	100.40	100.40	100.40	100
Max. Durchsatz	100.00	100.00	99.90	100.10	99.90	99.70	
Durchschn. Latenz	0.10	0.10	0.11	0.11	0.10	0.15	
Max. Latenz	0.16	0.20	0.22	0.24	0.19	0.34	
Schreibgeschw.	150.1	150.1	145.21	150.30	150.30	150.30	150
Max. Durchsatz	149.99	144.47	149.59	99.53	146.80	125.31	
Durchschn. Latenz	0.07	0.09	1.66	0.18	0.28	1.76	
Max. Latenz	0.15	0.28	4.10	0.43	0.69	3.01	
Schreibgeschw.	200.00	200.10	200.10	200.30	200.30	200.40	200
Max. Durchsatz	199.90	127.48	128.20	182.40	163.91	145.39	
Durchschn. Latenz	0.08	2.41	25.56	0.69	1.92	3.47	
Max. Latenz	0.42	4.73	37.55	1.82	3.31	5.03	
Schreibgeschw.	250.1	248.30	250.00	250.40	250.30	250.30	250
Max. Durchsatz	249.80	140.91	134.95	185.40	173.90	149.99	
Durchschn. Latenz	0.09	23.11	42.34	3.77	4.45	6.60	
Max. Latenz	0.63	35.09	54.34	5.30	6.30	7.83	
Schreibgeschw.	300.00	300.10	300.10	300.20	300.20	300.20	300
Max. Durchsatz	299.70	148.25	139.95	198.19	178.71	167.39	
Durchschn. Latenz	0.41	34.88	52.42	5.50	6.72	6.92	
Max. Latenz	1.05	46.13	77.70	7.38	9.54	9.46	

	Raft			BFT-SMaRt			Trans
Kriterium	4	8	12	4	8	12	
Schreibgeschw.	350.00	350.0	348.80	350.20	350.30	350.10	350
Max. Durchsatz	229.50	150.15	136.31	203.99	201.11	172.11	
Durchschn. Latenz	18.48	46.71	65.25	7.45	6.94	8.46	
Max. Latenz	28.84	63.06	85.72	10.78	9.48	15.32	
Schreibgeschw.	396.20	391.4	400.00	400.10	400.20	400.20	400
Max. Durchsatz	236.81	167.91	140.20	219.29	208.58	179.49	
Durchschn. Latenz	18.48	58.92	57.05	8.16	8.43	10.16	
Max. Latenz	28.84	76.67	85.19	11.26	12.35	13.88	
Schreibgeschw.	444.90	443.5	449.20	450.10	450.20	448.2	450
Max. Durchsatz	218.00	173.99	141.00	229.28	210.20	181.40	
Durchschn. Latenz	30.74	67.50	57.05	9.24	10.45	12.14	
Max. Latenz	42.28	88.19	85.19	12.79	13.79	18.05	
Schreibgeschw.	500.10	486.20	456.6	500.2	500.1	500.3	500
Max. Durchsatz	223.39	173.62	142.09	226.89	210.29	179.81	
Durchschn. Latenz	49.92	76.53	58.83	10.98	11.87	13.85	
Max. Latenz	68.56	99.38	82.40	13.94	15.51	19.08	

Schreibgeschw	Die Geschwindigkeit mit der Hyperledger Caliper Transaktionen erstellt [tx/s]
Max. Durchsatz	Die maximale Anzahl der erfolgreich verarbeiteten Transaktionen pro Sekunde [tx/s].
Durchschn. Latenz	Die durchschnittliche Zeitspanne zwischen der Ausgabe einer Transaktion durch einen DLT-Knoten und dem Anhängen der Transaktion an den Distributed Ledger [s].
Max. Latenz	Die maximale Zeitspanne zwischen der Ausgabe einer Transaktion durch einen DLT-Knoten und dem Anhängen der Transaktion an den Distributed Ledger [s].

Messungen für Solo, Kafka und Raft wurden mit Hyperledger Fabric (v 1.4.1) durchgeführt. Aufgrund der eingeschränkten Kompatibilität wurde für BFT-SMaRt Hyperledger Fabric (v 1.3) genutzt. Alle Messungen wurden in Docker-Containern unter Verwendung des Hyperledger Caliper Frameworks durchgeführt.

Abbildungsverzeichnis

Tabellenverzeichnis

Eigene Veröffentlichungen

Journal-Artikel

[J1] M. Lücking, N. Kannengießer, M. Kilgus, T. Riedel, M. Beigl, A. Sunyaev, and W. Stork, "The Merits of a Decentralized Pollution-Monitoring System Based on Distributed Ledger Technology," *IEEE Access*, vol. 8, pp. 189365–189381, 2020.

[J2] M. Lücking, F. Kretzer, N. Kannengießer, M. Beigl, A. Sunyaev, and W. Stork, "When Data Fly: An Open Data Trading System in Vehicular Ad Hoc Networks," *Electronics*, vol. 10, no. 6, 2021.

[J3] B. Farahani, F. Firouzi, and M. Lücking, "The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions," *Journal of Network and Computer Applications*, vol. 177, p. 102936, 2021.

Konferenzbeiträge

[K1] M. Lücking, E. Rivera, L. Kohout, C. Zimmermann, D. Polad, and W. Stork, "A video based vehicle counting system using an embedded device in realistic traffic conditions," *in Proceedings of the 6th World Forum on Internet of Things (WF-IoT)*, pp. 1–6, 2020.

[K2] M. Lücking, C. Fries, R. Lamberti, and W. Stork, "Decentralized Identity and Trust Management Framework for Internet of Thing," *in Proceeding of the*

IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2020, 2020.

[K3] M. Lücking, R. Manke, M. Schinle, L. Kohout, S. Nickel, and W. Stork, "Decentralized patient-centric data management for sharing IoT data streams," *in Proceeding of the International Conference on Omni-Layer Intelligent Systems, COINS 2020*, 2020.

[K4] R. Lamberti, C. Fries, M. Lücking, R. Manke, N. Kannengießer, B. Sturm, M. M. Komarov, W. Stork, and A. Sunyaev, "An open multimodal mobility platform based on Distributed Ledger Technology," *in Proceeding of international Conference on Next Generation Wired/Wireless Networking*, pp. 41–52, 2019.

Literaturverzeichnis

[1] J. E. Kohlhase, "The new urban world 2050: perspectives, prospects and problems," *Regional Science Policy & Practice*, vol. 5, no. 2, pp. 153–165, 2013.

[2] X. Q. Zhang, "The trends, promises and challenges of urbanisation in the world," *Habitat International*, vol. 54, no. 13, pp. 241–252, 2016.

[3] K. Su, J. Li, and H. Fu, "Smart city and the applications," *in Proceedings of the International Conference on Electronics, Communications and Control, ICECC 2011 - Proceedings*, pp. 1028–1031, 2011.

[4] J. Mercille, "Inclusive smart cities: Beyond voluntary corporate data sharing," *Sustainability (Switzerland)*, vol. 13, no. 15, 2021.

[5] X. Zhu, Y. Badr, J. Pacheco, and S. Hariri, "Autonomic Identity Framework for the Internet of Things," *in Proceedings of the IEEE International Conference on Cloud and Autonomic Computing, ICCAC 2017*, pp. 69–79, 2017.

[6] X. Zhu and Y. Badr, "Identity Management Systems for the Internet of Things: A Survey Towards Blockchain Solutions," *Sensors (Basel, Switzerland)*, vol. 18, no. 12, pp. 1–18, 2018.

[7] Visa, "Visa USA Interchange Reimbursement Fees." https://usa.visa.com/content/dam/VCOM/download/merchants/visa-usa-interchange-reimbursement-fees.pdf. besucht am 15.05.2022.

[8] D. Wilusz and J. Rykowski, "The Architecture of Coupon-Based, Semi-off-Line, Anonymous Micropayment System for Internet of Things," in *Technological Innovation for the Internet of Things* (L. M. Camarinha-Matos,

S. Tomic, and P. Graça, eds.), (Berlin, Heidelberg), pp. 125–132, Springer, 2013.

[9] M. S. Ali, M. Vecchio, and F. Antonelli, "A Blockchain-Based Framework for IoT Data Monetization Services," *Computer Journal*, vol. 64, no. 2, pp. 195–210, 2021.

[10] A. Suliman, Z. Husain, M. Abououf, M. Alblooshi, and K. Salah, "Monetization of IoT data using smart contracts," *IET Networks*, vol. 8, no. 1, pp. 32–37, 2019.

[11] C. Manville, G. Cochrane, J. Cave, J. Millard, J. K. Pederson, R. K. Thaarup, A. Liebe, M. Wissner, R. Massink, and B. Kotterink, "Mapping smart cities in the EU," 2014.

[12] M. Batty, K. W. Axhausen, F. Giannotti, A. Pozdnoukhov, A. Bazzani, M. Wachowicz, G. Ouzounis, and Y. Portugali, "Smart cities of the future," *European Physical Journal: Special Topics*, vol. 214, no. 1, pp. 481–518, 2012.

[13] A. Caragliu, C. D. Bo, and P. Nijkamp, "Smart Cities in Europe," *Journal of Urban Technology*, vol. 18, no. 2, pp. 65–82, 2011.

[14] R. Giffinger, "Smart cities ranking: an effective instrument for the positioning of the cities?," *ACE: Architecture, City and Environment*, 2010.

[15] N. B. Aletà, C. M. Alonso, and R. M. Ruiz, "Smart Mobility and Smart Environment in the Spanish cities," *Transportation Research Procedia*, vol. 24, pp. 163–170, 2017.

[16] C. García Fernández and D. Peek, "Smart and Sustainable? Positioning Adaptation to Climate Change in the European Smart City," *Smart Cities*, vol. 3, no. 2, pp. 511–526, 2020.

[17] Y. Shen, T. Zhang, Y. Wang, H. Wang, and X. Jiang, "MicroThings: A Generic IoT Architecture for Flexible Data Aggregation and Scalable Service Cooperation," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 86–93, 2017.

[18] A. Musaddiq, Y. B. Zikria, O. Hahm, H. Yu, A. K. Bashir, and S. W. Kim, "A Survey on Resource Management in IoT Operating Systems," *IEEE Access*, vol. 6, pp. 8459–8482, 2018.

[19] A. Kazmi, Z. Jan, A. Zappa, and M. Serrano, "Overcoming the heterogeneity in the internet of things for smart cities," in *Interoperability and Open-Source Solutions for the Internet of Things*, (Cham), pp. 20–35, Springer International Publishing, 2017.

[20] B. Cheng, M. Wang, S. Zhao, Z. Zhai, D. Zhu, and J. Chen, "Situation-Aware Dynamic Service Coordination in an IoT Environment," *IEEE/ACM Transactions on Networking*, vol. 25, no. 4, pp. 2082–2095, 2017.

[21] J. Jin, J. Gubbi, T. Luo, and M. Palaniswami, "Network architecture and QoS issues in the internet of things for a smart city," *in Proceedings of the International Symposium on Communications and Information Technologies, ISCIT 2012*, pp. 956–961, 2012.

[22] W. Viriyasitavat, T. Anuphaptrirong, and D. Hoonsopon, "When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities," *Journal of Industrial Information Integration*, vol. 15, no. April, pp. 21–28, 2019.

[23] C. Kyriazopoulou, "Smart city technologies and architectures: A literature review," *in Proceedings of the 4th International Conference on Smart Cities and Green ICT Systems, Proceedings*, pp. 5–16, 2015.

[24] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[25] Z. Idrees and L. Zheng, "Low cost air pollution monitoring systems: A review of protocols and enabling technologies," *Journal of Industrial Information Integration*, vol. 17, no. December 2019, p. 100123, 2020.

[26] C. Consortium, "Air Quality Standards." https://ec.europa.eu/environment/air/quality/standards.html. besucht am 25.09.2021.

[27] J. Van den Bossche, J. Theunis, B. Elen, J. Peters, D. Botteldooren, and B. De Baets, "Opportunistic mobile air pollution monitoring: A case study with city wardens in Antwerp," *Atmospheric Environment*, vol. 141, pp. 408–421, 2016.

[28] M. Pavani and P. Rao, "Urban air pollution monitoring using wireless sensor networks: A comprehensive review," *International Journal of Communication Networks and Information Security*, vol. 9, pp. 439–449, 2017.

[29] D. Hasenfratz, *Enabling large-scale urban air quality monitoring with mobile sensor nodes*. PhD thesis, ETH Zurich, 2015.

[30] N. K. Jain, R. K. Saini, and P. Mittal, "A Review on Traffic Monitoring System Techniques," in *Soft Computing: Theories and Applications*, (Singapore), pp. 569–577, Springer Singapore, 2019.

[31] Z. Yang and L. S. C. Pun-Cheng, "Vehicle detection in intelligent transportation systems and its applications under varying environments: A review," *Image and Vision Computing*, vol. 69, pp. 143–154, 2018.

[32] E. Barnoviciu, V. Ghenescu, S.-V. Carata, M. Ghenescu, R. Mihaescu, and M. Chindea, "GDPR compliance in Video Surveillance and Video Processing Application," *in Proceedings of the International Conference on Speech Technology and Human-Computer Dialogue (SpeD)*, pp. 1–6, 2019.

[33] A. F. Santamaria and C. Sottile, "Smart traffic management protocol based on VANET architecture," *Advances in Electrical and Electronic Engineering*, vol. 12, no. 4, pp. 279–288, 2014.

[34] S. A. Mohammad, A. Rasheed, and A. Qayyum, "VANET Architectures and Protocol Stacks: A Survey," in *Communication Technologies for Vehicles*, (Berlin, Heidelberg), pp. 95–105, Springer, 2011.

[35] H. T. Mouftah, M. Erol-Kantarci, and S. Sorour, *Connected and Autonomous Vehicles in Smart Cities*. CRC Press, 2020.

[36] Z. Allam and Z. A. Dhunny, "On big data, artificial intelligence and smart cities," *Cities*, vol. 89, pp. 80–91, 2019.

[37] K. H. Nam Bui, H. Yi, and J. Cho, "A multi-class multi-movement vehicle counting framework for traffic analysis in complex areas using CCTV systems," *Energies*, vol. 13, no. 8, 2020.

[38] A. Corovic, V. Ilic, S. Duric, M. Marijan, and B. Pavkovic, "The Real-Time Detection of Traffic Participants Using YOLO Algorithm," *in Proceeding of the 26th Telecommunications Forum, TELFOR 2018*, no. November, 2018.

[39] H. Yi, K.-H. N. Bui, and H. Jung, "Implementing A Deep Learning Framework for Short Term Traffic Flow Prediction," in *Proceedings of the 9th International Conference on Web Intelligence, Mining and Semantics*, WIMS2019, (New York, NY, USA), Association for Computing Machinery, 2019.

[40] N. Bui Khac Hoai, J. Jung, and D. Camacho, "Game theoretic approach on Real-time decision making for IoT-based traffic light control," *Concurrency and Computation: Practice and Experience*, vol. 29, 2017.

[41] M. Naphade, Z. Tang, M. C. Chang, D. C. Anastasiu, A. Sharma, R. Chellappa, S. Wang, P. Chakraborty, T. Huang, J. N. Hwang, and S. Lyu, "The 2019 AI city challenge," *in Proceeding of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, vol. 2019-June, pp. 452–460, 2019.

[42] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You only look once: Unified, real-time object detection," *in Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, vol. 2016-Decem, pp. 779–788, 2016.

[43] W. Liu, D. Anguelov, D. Erhan, C. Szegedy, S. Reed, C.-Y. Fu, and A. Berg, "SSD: Single Shot MultiBox Detector," vol. 9905, pp. 21–37, 2016.

[44] S.-K. Weng, C.-M. Kuo, and S.-K. Tu, "Video object tracking using adaptive Kalman filter," *Journal of Visual Communication and Image Representation*, vol. 17, pp. 1190–1208, 2006.

[45] C. Chang and R. Ansari, "Kernel particle filter for visual tracking," *Signal Processing Letters, IEEE*, vol. 12, pp. 242–245, 2005.

[46] S. Zhang, G. Wu, J. Costeira, and J. Moura, "FCN-rLSTM: Deep Spatio-Temporal Neural Networks for Vehicle Counting in City Cameras," *in Proceedings of the IEEE International Conference on Computer Vision (ICCV)*, pp. 3687–3696, 2017.

[47] Z. Al-Zaydi, B. Vuksanovic, and I. Habeeb, "Image processing based ambient context-aware people detection and counting," *International Journal of Machine Learning and Computing*, vol. 8, no. 3, pp. 268–273, 2018.

[48] N. Kannengießer, S. Lins, T. Dehling, and A. Sunyaev, "Trade-offs between Distributed Ledger Technology Characteristics," *ACM Computing Surveys*, vol. 53, no. 2, 2020.

[49] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, p. 382–401, 1982.

[50] A. Sunyaev, "Distributed Ledger Technology," pp. 265–299, 2 2020.

[51] N. Kannengießer, S. Lins, T. Dehling, and A. Sunyaev, "What Does Not Fit Can be Made to Fit! Trade-Offs in Distributed Ledger Technology Designs," *in Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019.

[52] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[53] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, "Inclusive block chain protocols," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8975, pp. 528–547, 2015.

[54] S. Popov, "IOTA whitepaper v1.4.3." https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf. besucht am 25.05.2022.

[55] P. Zheng, Z. Zheng, X. Luo, X. Chen, and X. Liu, "A detailed and real-time performance monitoring framework for blockchain systems," *in Proceedings of the International Conference on Software Engineering*, pp. 134–143, 2018.

[56] F. Glaser, Florian (Goethe University and F. Bezzenberger, Luis (Goethe University, "Beyond Cryptocurrencies - A Taxonomy Of Decentralized Consensus," *in Proceedings of the 23rd European Conference on Information Systems (ECIS 2015)*, no. Ecis, pp. 1–18, 2015.

[57] L. Ren and P. A. S. Ward, "Distributed consensus and fault tolerance mechanisms," *Essentials of Blockchain Technology*, p. 1, 2019.

[58] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," in *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, OSDI '99, (USA), p. 173–186, USENIX Association, 1999.

[59] M. T. Oliveira, G. R. Carrara, N. C. Fernandes, C. V. Albuquerque, R. C. Carrano, D. S. Medeiros, and D. M. Mattos, "Towards a Performance Evaluation of Private Blockchain Frameworks using a Realistic Workload," *in Proceedings of the 22nd Conference on Innovation in Clouds, Internet and Networks and Workshops, ICIN 2019*, pp. 180–187, 2019.

[60] L. Luu, D. H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," *in Proceedings of the ACM Conference on Computer and Communications Security*, vol. 24-28-Octo, pp. 254–269, 2016.

[61] M. Marescotti, M. Blicha, A. E. J. Hyvärinen, S. Asadi, and N. Sharygina, "Computing Exact Worst-Case Gas Consumption for Smart Contracts," in *Leveraging Applications of Formal Methods, Verification and Validation. Industrial Practice*, (Cham), pp. 450–465, Springer International Publishing, 2018.

[62] I. D. Kotilevets, I. A. Ivanova, I. O. Romanov, S. G. Magomedov, V. V. Nikonov, and S. A. Pavelev, "Implementation of directed acyclic graph in blockchain network to improve security and speed of transactions," *IFAC-PapersOnLine*, vol. 51, no. 30, pp. 693–696, 2018.

[63] W. F. Silvano and R. Marcelino, "Iota Tangle: A cryptocurrency to communicate Internet-of-Things data," *Future Generation Computer Systems*, vol. 112, pp. 307–319, 2020.

[64] Serguei Popov, "On the Tangle, White Papers, Proofs, Airplanes, and Local Modifiers." https://blog.iota.org/on-the-tangle-white-papers-proofs-airplanes-and-local-modifiers-44683aff8fea/, 2018. besucht am 25.05.2022.

[65] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Keccak," in *Advances in Cryptology*, (Berlin, Heidelberg), pp. 313–314, Springer Berlin Heidelberg, 2013.

[66] IOTA Foundation, "Proof of work." https://legacy.docs.iota.works/docs/getting-started/0.1/transactions/proof-of-work. besucht am 25.05.2022.

[67] Coordicide Team of the IOTA Foundation, "The Coordicide." https://files.iota.org/papers/Coordicide_WP.pdf. besucht am 25.05.2022.

[68] IOTA Foundation, "OTA 2.0 DevNet - nectar release." https://v2.iota.org/. besucht am 02.06.2022.

[69] P. K. P, S. K. P, and A. P.J.A., "Attribute based encryption in cloud computing: A survey, gap analysis, and future directions," *Journal of Network and Computer Applications*, vol. 108, pp. 37–52, 2018.

[70] P. Bramhall, M. Hansen, K. Rannenberg, and T. Roessler, "User-centric identity management," in *IEEE Security and Privacy*, vol. 5, pp. 84–87, 2007.

[71] D. Pöhn and W. Hommel, "An overview of limitations and approaches in identity management," *in Proceedings of the ACM International Conference Proceeding Series*, 2020.

[72] J.-M. Seigneur and T. E. Maliki, "Chapter 17 - Identity Management," in *Computer and Information Security Handbook*, pp. 269–292, Boston: Morgan Kaufmann, 2009.

[73] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Computer Science Review*, vol. 30, pp. 80–86, 2018.

[74] Christopher Allen, "The path to self-sovereign identity." http://www.lifewithalacrity.com/previous/. besucht am 25.05.2022.

[75] World Wide Web Consortium, "Verifiable Claims Data Model and Representations." https://www.w3.org/TR/2017/WD-verifiable-claims-data-model-20170803/. besucht am 25.09.2021.

[76] Z. A. Lux, D. Thatmann, S. Zickau, and F. Beierle, "Distributed-Ledger-based Authentication with Decentralized Identifiers and Verifiable Credentials," *in Proceedings of the 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS 2020*, pp. 71–78, 2020.

[77] D. Van Bokkem, R. Hageman, G. Koning, L. Nguyen, and N. Zarin, "Self-sovereign identity solutions: The necessity of blockchain technology," *arXiv*, pp. 1–8, 2019.

[78] Q. Stokkink and J. Pouwelse, "Deployment of a Blockchain-Based Self-Sovereign Identity," *in Proceedings of the 2018 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)*, pp. 1336–1342, 2018.

[79] J. StClair, A. Ingraham, D. King, M. B. Marchant, F. C. McCraw, D. Metcalf, and J. Squeo, "Blockchain, Interoperability, and Self-Sovereign Identity: Trust Me, It's My Data," *Blockchain in Healthcare Today*, pp. 5–7, 2020.

[80] G. Fortino, L. Fotia, F. Messina, D. Rosaci, and G. M. Sarné, "Trust and Reputation in the Internet of Things: State-of-the-Art and Research Challenges," *IEEE Access*, vol. 8, pp. 60117–60125, 2020.

[81] L. Mui, M. Mohtashemi, and A. Halberstadt, "A computational model of trust and reputation," *in Proceedings of the Annual Hawaii International*

Conference on System Sciences, vol. 2002-Janua, no. November, pp. 2431–2439, 2002.

[82] F. Hendrikx, K. Bubendorfer, and R. Chard, "Reputation systems: A survey and taxonomy," *Journal of Parallel and Distributed Computing*, vol. 75, no. September 2018, pp. 184–197, 2015.

[83] E. Bellini, Y. Iraqi, and E. Damiani, "Blockchain-Based Distributed Trust and Reputation Management Systems: A Survey," *IEEE Access*, vol. 8, pp. 21127–21151, 2020.

[84] A. S. Almasoud, F. K. Hussain, and O. K. Hussain, "Smart contracts for blockchain-based reputation systems: A systematic literature review," *Journal of Network and Computer Applications*, vol. 170, no. September 2019, p. 102814, 2020.

[85] R. Dennis and G. Owen, "Rep on the block: A next generation reputation system based on the blockchain," *in Proceedings of the 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015*, pp. 131–138, 2016.

[86] S. Lee, "A Decentralized Reputation System: How Blockchain Can Restore Trust In Online Markets."

[87] C. Dark, D. Emery, J. Ma, C. Noone, and others, "Cryptocurrency: Ten years on| bulletin–june quarter 2019," *Bulletin*, no. June, 2019.

[88] H. S. Galal, M. ElSheikh, and A. M. Youssef, "An Efficient Micropayment Channel on Ethereum," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11737 LNCS, no. September, pp. 211–218, 2019.

[89] N. Khan, T. Ahmad, and R. State, "Blockchain-based Micropayment Systems: Economic impact," *in Proceedings of the ACM International Conference Proceeding Series*, pp. 10–13, 2019.

[90] D. Múnera, V. Diana, J. Aguirre, and N. G. Gómez, "IoT-based air quality monitoring systems for smart cities: A systematic mapping study," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 4, pp. 3470–3482, 2021.

[91] F. Arena and G. Pau, "An overview of vehicular communications," *Future Internet*, vol. 11, no. 2, 2019.

[92] V. A. Natarajan, S. Jothilakshmi, and V. N. Gudivada, "Scalable Traffic Video Analytics using Hadoop MapReduce," *in Proceedings of the first International Conference on Big Data, Small Data, Linked Data and Open Data Scalable*, pp. 11–15, 2015.

[93] A. Senior, "Privacy protection in a video surveillance system," *Protecting Privacy in Video Surveillance*, pp. 35–47, 2009.

[94] H. A. Rashwan, A. Solanas, D. Puig, and A. Martínez-Ballesté, "Understanding trust in privacy-aware video surveillance systems," *International Journal of Information Security*, vol. 15, no. 3, pp. 225–234, 2016.

[95] L. Jiao, F. Zhang, F. Liu, S. Yang, L. Li, Z. Feng, and R. Qu, "A survey of deep learning-based object detection," *IEEE Access*, vol. 7, no. 3, pp. 128837–128868, 2019.

[96] M. Manana, C. Tu, and P. A. Owolawi, "A survey on vehicle detection based on convolution neural networks," *in Proceedings of the 3rd IEEE International Conference on Computer and Communications, ICCC 2017*, pp. 1751–1755, 2018.

[97] R. Girshick, J. Donahue, T. Darrell, and J. Malik, "Region-Based Convolutional Networks for Accurate Object Detection and Segmentation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 38, no. 1, pp. 142–158, 2016.

[98] T. Evgeniou and M. Pontil, "Support vector machines: Theory and applications," in *Advanced Course on Artificial Intelligence*, pp. 249–257, Springer, 1999.

[99] R. Girshick, “Fast R-CNN,” *in Proceedings of the IEEE International Conference on Computer Vision*, vol. 2015 Inter, pp. 1440–1448, 2015.

[100] S. Ren, K. He, R. Girshick, and J. Sun, “Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 39, no. 6, pp. 1137–1149, 2017.

[101] A. Arinaldi, J. A. Pradana, and A. A. Gurusinga, “Detection and classification of vehicles for traffic video analytics,” *Procedia Computer Science*, vol. 144, pp. 259–268, 2018.

[102] J. E. Espinosa, S. A. Velastin, and J. W. Branch, “Vehicle Detection Using Alex Net and Faster R-CNN Deep Learning Models: A Comparative Study,” in *Advances in Visual Informatics*, (Cham), pp. 3–15, Springer International Publishing, 2017.

[103] J. E. Espinosa, S. A. Velastin, and J. W. Branch, “Motorcycle detection and classification in urban scenarios using a model based on faster R-CNN,” *IET Conference Publications*, vol. 2018, no. CP745, pp. 91–96, 2018.

[104] V. Moustaka, Z. Theodosiou, A. Vakali, and A. Kounoudes, “Smart Cities at Risk!: Privacy and Security Borderlines from Social Networking in Cities,” *in Proceedings of The Web Conference 2018 - Companion of the World Wide Web Conference*, pp. 905–910, 2018.

[105] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, “Security and Privacy in Smart City Applications: Challenges and Solutions,” *IEEE Communications Magazine*, vol. 55, no. 1, pp. 122–129, 2017.

[106] H. Lu, S. Zhao, X. Xiong, K. Zheng, P. Chatzimisios, M. S. Hossain, and W. Xiang, “Internet of Things Cloud: Architecture and Implementation,” *IEEE Communications Magazine*, vol. 54, 2016.

[107] L. T. Khrais, “IoT and blockchain in the development of smart cities,” *International Journal of Advanced Computer Science and Applications*, no. 2, pp. 153–159, 2020.

[108] M. Wang, C. Fan, Z. Wen, S. Li, and J. Liu, "Implementation of Internet of Things oriented data sharing platform based on RESTful Web Service," *in Proceedings of the 7th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM 2011*, pp. 26–29, 2011.

[109] B. Balamurugan, P. V. Krishna, M. N. Devi, R. Meenakshi, and V. Ahinaya, "Enhanced framework for verifying user authorization and data correctness using token management system in the cloud," *in Proceedings of the International Conference on Circuits, Power and Computing Technologies, ICCPCT 2014*, pp. 1443–1447, 2014.

[110] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Generation Computer Systems*, vol. 88, no. 2018, pp. 173–190, 2018.

[111] H. Xu, Q. He, X. Li, B. Jiang, and K. Qin, "BDSS-FA: A Blockchain-Based Data Security Sharing Platform with Fine-Grained Access Control," *IEEE Access*, vol. 8, pp. 87552–87561, 2020.

[112] Z. Ma, J. Zhang, Y. Guo, Y. Liu, X. Liu, and W. He, "An Efficient Decentralized Key Management Mechanism for VANET With Blockchain," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5836–5849, 2020.

[113] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. Ogah, and Z. Sun, "Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1832–1843, 2017.

[114] H. A. Pham, T. K. Le, T. N. M. Pham, H. Q. T. Nguyen, and T. V. Le, "Enhanced Security of IoT Data Sharing Management by Smart Contracts and Blockchain," *in Proceedings of the 19th International Symposium on Communications and Information Technologies, ISCIT 2019*, pp. 398–403, 2019.

[115] Y. L. Sun, Z. Han, W. Yu, and K. J. Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks," *in*

Proceedings of the 25th IEEE international conference on computer communications, IEEE INFOCOM 2006, 2006.

[116] M. Toorani and C. Gehrmann, "A decentralized dynamic PKI based on blockchain," *in Proceedings of the ACM Symposium on Applied Computing*, pp. 1646–1655, 2021.

[117] KJ Chugh, "How can cities monetize their data?." https://atos.net/en/blog/how-can-cities-monetize-their-data, 2019. besucht am 25.05.2022.

[118] Gartner, "Data Monetization." https://www.gartner.com/en/information-technology/glossary/data-monetization. besucht am 25.05.2022.

[119] M. S. Najjar and W. J. Kettinger, "Data Monetization: Lessons from a Retailer's Journey.," *MIS Quarterly Executive*, vol. 12, no. 4, 2013.

[120] J. Fred, *Data Monetization-How an Organization Can Generate Revenue with Data?* PhD thesis, Tampere University of Technology, 2017.

[121] G. S. Ramachandran, R. Radhakrishnan, and B. Krishnamachari, "Towards a Decentralized Data Marketplace for Smart Cities," *in Proceedings of the 2018 IEEE International Smart Cities Conference, ISC2 2018*, pp. 1–8, 2019.

[122] S. Bajoudah and P. Missier, "Latency of Trading Transactions in Brokered IoT Data Marketplace in Ethereum," *in Proceedings of the Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation, 2021 IEEE SmartWorld*, pp. 254–263, 2021.

[123] A. S. Mihăiță, L. Dupont, O. Chery, M. Camargo, and C. Cai, "Evaluating air quality by combining stationary, smart mobile pollution monitoring and data-driven modelling," *Journal of cleaner production*, vol. 221, pp. 398–418, 2019.

[124] L. Morawska, P. K. Thai, X. Liu, A. Asumadu-Sakyi, G. Ayoko, A. Bartonova, A. Bedini, F. Chai, B. Christensen, M. Dunbabin, *et al.*, "Applications of low-cost sensing technologies for air quality monitoring and exposure assessment: How far have they gone?," *Environment international*, vol. 116, pp. 286–299, 2018.

[125] P. Saxena and V. Naik, *Air Pollution: Sources, Impacts and Controls*. Oxfort, U.K.: CABI, 2018.

[126] H. K. Elminir, "Dependence of urban air pollutants on meteorology," *Science of the Total Environment*, vol. 350, no. 1-3, pp. 225–237, 2005.

[127] G. Hernandez, T.-A. Berry, S. Wallis, and D. Poyner, "Temperature and humidity effects on particulate matter concentrations in a sub-tropical climate during winters," *Proceedings - International Proceedings of Chemical, Biological and Environmental Engineering*, pp. 41–49, 2017.

[128] J. Xu, F. Zhu, S. Wang, X. Zhao, M. Zhang, X. Ge, J. Wang, W. Tian, L. Wang, L. Yang, L. Ding, X. Lu, X. Chen, Y. Zheng, and Z. Guo, "Impacts of relative humidity on fine aerosol properties via environmental wind tunnel experiments," *Atmospheric Environment*, vol. 206, no. March, pp. 21–29, 2019.

[129] W. Ouyang, Y. Xu, J. Cao, X. Gao, B. Gao, Z. Hao, and C. Lin, "Rainwater characteristics and interaction with atmospheric particle matter transportation analyzed by remote sensing around Beijing," *Science of the Total Environment*, vol. 651, pp. 532–540, 2019.

[130] L. T. Padró-Martínez, A. P. Patton, J. B. Trull, W. Zamore, D. Brugge, and J. L. Durant, "Mobile monitoring of particle number concentration and other traffic-related air pollutants in a near-highway neighborhood over the course of a year," *Atmospheric Environment*, vol. 61, pp. 253–264, 2012.

[131] A. A. Karner, D. S. Eisinger, and D. A. Niemeier, "Near-roadway air quality: Synthesizing the findings from real-world data," *Environmental Science and Technology*, vol. 44, no. 14, pp. 5334–5344, 2010.

[132] M. Pindus, H. Orru, M. Maasikmets, M. Kaasik, and R. Jõgi, "Association Between Health Symptoms and Particulate Matter from Traffic and Residential Heating Results from RHINE III in Tartu," *The Open Respiratory Medicine Journal*, vol. 10, no. 1, pp. 58–69, 2016.

[133] Digital Gipfel, "Neue Nachhaltigkeitsinfrastrukturen Digitale Luftqualitätsmessung für ein umweltsensitives Verkehrsmanagement." https://plattform-digitale-netze.de/neue-nachhaltigkeitsinfrastrukturen-digitale-luftqualitaetsmessung-fuer-ein-umweltsensitives-verkehrsmanagement-veroeffentlicht/. besucht am 25.05.2022.

[134] S. Bezantakos, F. Schmidt-Ott, and G. Biskos, "Performance evaluation of the cost-effective and lightweight Alphasense optical particle counter for use onboard unmanned aerial vehicles," *Aerosol Science and Technology*, vol. 52, no. 4, pp. 385–392, 2018.

[135] S. Sousan, K. Koehler, L. Hallett, and T. M. Peters, "Evaluation of the Alphasense optical particle counter (OPC-N2) and the Grimm portable aerosol spectrometer (PAS-1.108)," *Aerosol Science and Technology*, vol. 50, no. 12, pp. 1352–1365, 2016.

[136] L. R. Crilley, M. Shaw, R. Pound, L. J. Kramer, R. Price, S. Young, A. C. Lewis, and F. D. Pope, "Evaluation of a low-cost optical particle counter (Alphasense OPC-N2) for ambient air monitoring," *Atmospheric Measurement Techniques*, vol. 11, no. 2, pp. 709–720, 2018.

[137] Alphasense, "View by Sensor Technology." https://www.alphasense.com/product_type/sensor-technology/. besucht am 25.05.2022.

[138] P. Kumar, L. Morawska, C. Martani, G. Biskos, M. Neophytou, S. Di Sabatino, M. Bell, L. Norford, and R. Britter, "The rise of low-cost sensing for managing air pollution in cities," *Environment International*, vol. 75, pp. 199–205, 2015.

[139] R. Tanzer, C. Malings, A. Hauryliuk, R. Subramanian, and A. A. Presto, "Demonstration of a low-cost multi-pollutant network to quantify intra-urban spatial variations in air pollutant source impacts and to evaluate environmental justice," *International Journal of Environmental Research and Public Health*, vol. 16, no. 14, 2019.

[140] X. Liu, R. Jayaratne, P. Thai, T. Kuhn, I. Zing, B. Christensen, R. Lamont, M. Dunbabin, S. Zhu, J. Gao, D. Wainwright, D. Neale, R. Kan, J. Kirkwood, and L. Morawska, "Low-cost sensors as an alternative for long-term air quality monitoring," *Environmental Research*, vol. 185, no. December 2019, p. 109438, 2020.

[141] M. I. Mead, O. A. Popoola, G. B. Stewart, P. Landshoff, M. Calleja, M. Hayes, J. J. Baldovi, M. W. McLeod, T. F. Hodgson, J. Dicks, A. Lewis, J. Cohen, R. Baron, J. R. Saffell, and R. L. Jones, "The use of electrochemical sensors for monitoring urban air quality in low-cost, high-density networks," *Atmospheric Environment*, vol. 70, pp. 186–203, 2013.

[142] J. Kim, A. A. Shusterman, K. J. Lieschke, C. Newman, and R. C. Cohen, "The BErkeley Atmospheric CO2 Observation Network: Field Calibration and Evaluation of Low-cost Air Quality Sensors," *Atmospheric Measurement Techniques Discussions*, pp. 1–20, 2017.

[143] M. Liu, K. K. Barkjohn, C. Norris, J. J. Schauer, J. Zhang, Y. Zhang, M. Hu, and M. Bergin, "Using low-cost sensors to monitor indoor, outdoor, and personal ozone concentrations in Beijing, China," *Environmental Science: Processes and Impacts*, vol. 22, no. 1, pp. 131–143, 2020.

[144] J. T. Peterson and E. C. Flowers, "Interactions between air pollution and solar radiation," *Solar Energy*, vol. 19, no. 1, pp. 23–32, 1977.

[145] L. C. Belalcazar, O. Fuhrer, M. D. Ho, E. Zarate, and A. Clappier, "Estimation of road traffic emission factors from a long term tracer study," *Atmospheric Environment*, vol. 43, no. 36, pp. 5830–5837, 2009.

[146] R. Zalakeviciute, A. Buenaño, D. Sannino, and Y. Rybarczyk, *Urban air pollution mapping and traffic intensity: Active transport application*. IntechOpen, 2018.

[147] S. V. Liu, F. L. Chen, and J. Xue, "Evaluation of traffic density parameters as an indicator of vehicle emission-related near-road air pollution: A case study with NEXUS measurement data on black carbon," *International Journal of Environmental Research and Public Health*, vol. 14, no. 12, 2017.

[148] M. André and C. Pronello, "Speed and acceleration impact on pollutant emissions," *SAE Technical Papers*, pp. 1–8, 1996.

[149] V. Mazzia, A. Khaliq, F. Salvetti, and M. Chiaberge, "Real-time apple detection system using embedded systems with hardware accelerators: An edge AI application," *IEEE Access*, vol. 8, pp. 9102–9114, 2020.

[150] D. L. Dinh, H. N. Nguyen, H. T. Thai, and K. H. Le, "Towards AI-Based Traffic Counting System with Edge Computing," *Journal of Advanced Transportation*, vol. 2021, 2021.

[151] Z. Zivkovic, "Improved Adaptive Gaussian Mixture Model for Background Subtraction," *in Proceedings of the 7th International Conference on Pattern Recognition, ICPR 2004*, pp. 28–31, 2004.

[152] W. Liu, D. Anguelov, D. Erhan, C. Szegedy, S. Reed, C.-Y. Fu, and A. C. Berg, "SSD: Single shot MultiBox detector," in *Computer Vision – ECCV 2016*, pp. 21–37, Springer International Publishing, 2016.

[153] M. Sandler, A. Howard, M. Zhu, A. Zhmoginov, and L.-C. Chen, "Mobilenetv2: Inverted residuals and linear bottlenecks," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 4510–4520, 2018.

[154] A. Heredia and G. Barros-Gavilanes, "Video processing inside embedded devices using SSD-Mobilenet to count mobility actors," *in Proceedings of the IEEE Colombian Conference on Applications in Computational Intelligence, ColCACI 2019*, pp. 1–6, 2019.

[155] N. Nishant, A. Maharjan, D. Chutia, P. Raju, and A. Pradhan, "Real-time road monitoring using deep learning algorithm deployed on iot devices," in *Artificial Intelligence*, pp. 137–147, Chapman and Hall/CRC, 2021.

[156] C. Consortium, "Coco common objects in context." https://cocodataset.org/#home. besucht am 25.05.2022.

[157] N. Wojke, A. Bewley, and D. Paulus, "Simple online and realtime tracking with a deep association metric," *In Proceedings of the International Conference on Image Processing, ICIP 2018*, pp. 3645–3649, 2018.

[158] S. Chanthakit and C. Rattanapoka, "Mqtt based air quality monitoring system using node MCU and node-red," *In Proceeding of the 7th ICT International Student Project Conference, ICT-ISPC 2018*, pp. 1–5, 2018.

[159] V. Kumar, G. Sakya, and C. Shankar, "WSN and IoT based smart city model using the MQTT protocol," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, pp. 1423–1434, 2019.

[160] P. G. Krishna, K. S. Ravi, S. Kumar, and S. Kumar, "Implementation of MQTT protocol on low resourced embedded network," *International Journal of Pure and Applied Mathematics*, vol. 116, pp. 161–166, 2017.

[161] Zymbit, "ZYMKEY4 Plug-in hardware security module for Raspberry Pi." https://www.zymbit.com/zymkey/. besucht am 25.05.2022.

[162] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, 2001.

[163] C. E. Catlett, P. H. Beckman, R. Sankaran, and K. K. Galvin, "Array of things: A scientific research instrument in the public way," *In Proceedings of the 2nd International Workshop on Science of Smart City Operations and Platforms Engineering, in partnership with Global City Teams Challenge, SCOPE 2017*, pp. 26–33, 2017.

[164] Bayerisches Landesamt für Umwelt, "Messstation Augsburg Koenigsplatz." https://www.lfu.bayern.de/luft/immissionsmessungen/doc/lueb_dokumentation/aktiv/07_Schwaben/03_augsburg_koenigsplatz.pdf. besucht am 25.05.2022.

[165] D. H. Hagan, G. Isaacman-Vanwertz, J. P. Franklin, L. M. M. Wallace, B. D. Kocar, C. L. Heald, and J. H. Kroll, "Calibration and assessment of electrochemical air quality sensors by co-location with regulatory-grade instruments," *Atmospheric Measurement Techniques*, vol. 11, no. 1, pp. 315–328, 2018.

[166] A. Cavaliere, F. Carotenuto, F. Di Gennaro, B. Gioli, G. Gualtieri, F. Martelli, A. Matese, P. Toscano, C. Vagnoli, and A. Zaldei, "Development of low-cost air quality stations for next generation monitoring networks: Calibration and validation of PM2.5 and PM10 sensors," *Sensors (Switzerland)*, vol. 18, no. 9, pp. 1–20, 2018.

[167] P. Han, H. Mei, D. Liu, N. Zeng, X. Tang, Y. Wang, and Y. Pan, "Calibrations of low-cost air pollution monitoring sensors for co, no2, o3, and so2," *Sensors*, vol. 21, no. 1, p. 256, 2021.

[168] V. Van Zoest, F. Osei, A. Stein, and G. Hoek, "Calibration of low-cost no2 sensors in an urban air quality network," *Atmospheric environment*, vol. 210, pp. 66–75, Aug. 2019.

[169] P. Nowack, L. Konstantinovskiy, H. Gardiner, and J. Cant, "Machine learning calibration of low-cost no 2 and pm 10 sensors: non-linear algorithms and their impact on site transferability," *Atmospheric Measurement Techniques*, vol. 14, no. 8, pp. 5637–5655, 2021.

[170] Y. Xia, X. Shi, G. Song, Q. Geng, and Y. Liu, "Towards improving quality of video-based vehicle counting method for traffic flow estimation," *Signal Processing*, vol. 120, pp. 672–681, 2016.

[171] Y. L. Chen, B. F. Wu, H. Y. Huang, and C. J. Fan, "A real-time vision system for nighttime vehicle detection and traffic surveillance," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 5, pp. 2030–2044, 2011.

[172] I. D. Buldin, M. G. Gorodnichev, S. S. Makhrov, and E. N. Denisova, "Next Generation Industrial Blockchain-Based Wireless Sensor Networks," in *Wave Electronics and its Application in Information and Telecommunication Systems*, p. 1–5, IEEE, 11 2018.

[173] Y. M. Yussoff, H. Hashim, and M. D. Baba, "Identity-based Trusted Authentication in Wireless Sensor Networks," *International Journal of Computer Science Issues*, vol. 9, no. 3, pp. 230–239, 2012.

[174] J. Webster and R. T. Watson, "Analyzing the Past to Prepare for the Future," *MIS Quarterly*, vol. 26, no. 2, p. xiii–xxiii, 2002.

[175] J. M. Corbin and A. L. Strauss, *Basics of qualitative research : techniques and procedures for developing grounded theory*, vol. 2015. Sage Publications, 4 ed., 2015.

[176] A. Durand, P. Gremaud, and J. Pasquier, "Resilient, crowd-sourced LPWAN infrastructure using blockchain," *in Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, pp. 25–29, 2018.

[177] D. H. Shih, P. Y. Shih, and T. W. Wu, "An infrastructure of multi-pollutant air quality deterioration early warning system in spark platform," *in Proceedings of the 3rd IEEE International Conference on Cloud Computing and Big Data Analysis, ICCCBDA 2018*, pp. 648–652, 2018.

[178] S. R. Niya, S. S. Jha, T. Bocek, and B. Stiller, "Design and Implementation of an Automated and Decentralized Pollution Monitoring System with Blockchains, Smart Contracts, and LoRaWAN," *in Proceedings of the IEEE/IFIP Network Operations and Management Symposium, NOMS*, pp. 1–4, 2018.

[179] H. Cheng, R. Guo, and Y. Chen, "Node selection algorithms with data accuracy guarantee in service-oriented wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2013, 2013.

[180] O. Attia, I. Khoufi, A. Laouiti, and C. Adjih, "An IoT-Blockchain Architecture Based on Hyperledger Framework for Healthcare Monitoring Application," *in Proceedings of the 10th IFIP International Conference on New Technologies, Mobility and Security*, pp. 1–5, 2019.

[181] M. T. Hammi, P. Bellot, and A. Serhrouchni, "BCTrust: A decentralized authentication blockchain-based mechanism," *in Proceedings of the IEEE Wireless Communications and Networking Conference*, pp. 1–6, 2018.

[182] X. Zhao, S. Zuo, R. Ghannam, Q. H. Ab-basi, and H. Heidari, "Design and Implementation of Portable Sensory System for Air Pollution Monitoring Monitoring," *in Proceedings of the IEEE Asia Pacific Conference on Postgraduate Research in Microelectronics and Electronics*, pp. 47–50, 2018.

[183] R. T. Tse and Y. Xiao, "A portable Wireless Sensor Network system for real time environmental monitoring," *in Proceedings of the 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks*, pp. 1–6, 2016.

[184] S. Ibba, A. Pinna, M. Seu, and F. E. Pani, "CitySense Blockchain oriented Smart Cities," in *Proceedings of the XP2017 Scientific Workshops*, p. 1–5, ACM, 2017.

[185] W. Stallings, *Cryptography and Network Security: Principles and Practice*. USA: Prentice Hall Press, 5th ed., 2010.

[186] I. Kabashkin and J. Kundler, "Reliability of Sensor Nodes in Wireless Sensor Networks of Cyber Physical Systems," *Procedia Computer Science*, vol. 104, pp. 380–384, 2016.

[187] EEA, "Exceedance of air quality standards in Europe — European Environment Agency," 2019.

[188] B. S. Sarjerao and A. Prakasarao, "A Low Cost Smart Pollution Measurement System Using REST API and ESP32," *in Proceedings of the 3rd International Conference for Convergence in Technology*, p. 1–5, 2018.

[189] B. Pearson, L. Luo, C. Zou, J. Crain, Y. Jin, and X. Fu, "Building a low-cost and state-of-the-art iot security hands-on laboratory," in *Internet of Things. A Confluence of Many Disciplines*, pp. 189–306, Switzerland: Springer, 2020.

[190] K. Sovani, "Understanding ESP32's Security Features." https://medium.com/the-esp-journal/understanding-esp32s-security-features-14483e465724. besucht am 12.12.2021.

[191] E. Systems, "Secure Boot." https://docs.espressif.com/projects/esp-idf/en/latest/esp32/security/secure-boot-v1.html. besucht am 12.04.2022.

[192] Y. Song, J. Lin, M. Tang, and S. Dong, "An Internet of Energy Things Based on Wireless LPWAN," *Engineering*, vol. 3, p. 460–466, 8 2017.

[193] S. Martiradonna, G. Piro, and G. Boggia, "On the evaluation of the NB-IoT random access procedure in monitoring infrastructures," *Sensors (Switzerland)*, vol. 19, no. 14, pp. 1–25, 2019.

[194] A. Khalifeh, K. A. Aldahdouh, K. A. Darabkh, and W. Al-Sit, "A Survey of 5G Emerging Wireless Technologies Featuring LoRaWAN, Sigfox, NB-IoT and LTE-M," *in Proceeding of the International Conference on Wireless Communications Signal Processing and Networking, WiSPNET 2019*, pp. 561–566, 2020.

[195] A. Augustin, J. Yi, T. Clausen, and W. Townsley, "A Study of LoRa: Long Range and Low Power Networks for the Internet of Things," *Sensors*, vol. 16, p. 1466, 9 2016.

[196] L. J. Chen, Y. H. Ho, H. C. Lee, H. C. Wu, H. M. Liu, H. H. Hsieh, Y. T. Huang, and S. C. C. Lung, "An Open Framework for Participatory PM2.5 Monitoring in Smart Cities," *IEEE Access*, vol. 5, no. July, pp. 14441–14454, 2017.

[197] W. Chen, L. Yan, and H. Zhao, "Seasonal variations of atmospheric pollution and air quality in Beijing," *Atmosphere*, vol. 6, no. 11, pp. 1753–1770, 2015.

[198] Y. J. Jung, Y. K. Lee, D. G. Lee, K. H. Ryu, and S. Nittel, "Air pollution monitoring system based on geosensor network," *in Proceeding of the IEEE International Geoscience Remote Sensing Symposium, IGARSS 2008)*, vol. 3, no. 1, 2008.

[199] K. L. Tsai, Y. L. Huang, F. Y. Leu, I. You, Y. L. Huang, and C. H. Tsai, "AES-128 based secure low power communication for LoRaWAN IoT environments," *IEEE Access*, vol. 6, pp. 45325–45334, 2018.

[200] J. Lin, Z. Shen, and C. Miao, "Using Blockchain Technology to Build Trust in Sharing LoRaWAN IoT," in *Proceedings of the 2nd International Conference on Crowd Science and Engineering*, p. 38–43, 2017.

[201] Hyperledger Foundation, "A blockchain platform for the enterprise." https://hyperledger-fabric.readthedocs.io/en/release-1.4/. besucht am 25.05.2022.

[202] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, and E. al, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," *in Proceedings of the 13th EuroSys Conference*, pp. 1–15, 2018.

[203] J. Sousa, A. Bessani, and M. Vukolic, "A byzantine Fault-Tolerant ordering service for the hyperledger fabric blockchain platform," *Proceedings - 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2018*, no. 1, pp. 51–58, 2018.

[204] L. Zanzi, A. Albanese, V. Sciancalepore, and X. Costa-p, "NSBchain : A Secure Blockchain Framework for Network Slicing Brokerage," *ArXiv*, 2020.

[205] K. Christidis, "A Kafka-based Ordering Service for Fabric." https://docs.google.com/document/d/19JihmW-8blTzN99lAubOfseLUZqdrB6sBR0HsRgCAnY/edit, 2016. besucht am 15.03.2022.

[206] "The Ordering Service."

[207] V. Arora, T. Mittal, D. Agrawal, A. E. Abbadi, X. Xue, Zhiyanan, and Zhujianfeng, "Leader or Majority: Why have one when you can have both? Improving Read Scalability in Raft-like consensus protocols," *in Proceeding of the 9th Workshop on Hot Topics in Cloud Computing (HotCloud 17)*, p. 6, 2017.

[208] G. Zhang and C.-Z. Xu, "An Efficient Consensus Protocol for Real-Time Permissioned Blockchains Under Non-Byzantine Conditions," *in Proceeding of the 14th International Conference on Green, Pervasive and Cloud Computing*, pp. 298–311, 2019.

[209] A. Bessani, J. Sousa, and E. E. P. Alchieri, "State machine replication for the masses with BFT-SMART," *in Proceedings of the 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2014*, pp. 355–362, 2014.

[210] C. Berger, F. Sabino, and A. Bessani, "Byzantine Fault-Tolerant (BFT) State Machine Replication (SMaRt) v1.2." https://github.com/bft-smart/library. besucht am 17.03.2022.

[211] P. Leach, M. Mealling, and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace." https://tools.ietf.org/html/rfc4122. besucht am 25.01.2022.

[212] K. K. Johnson, M. H. Bergin, A. G. Russell, and G. S. W. Hagler, "Field test of several low-cost particulate matter sensors in high and low concentration urban environments," *Aerosol and Air Quality Research*, vol. 18, no. 3, pp. 565–578, 2018.

[213] G. Ramachandran, J. Adgate, G. Pratt, and K. Sexton, "Characterizing Indoor and Outdoor 15 Minute Average PM 2.5 Concentrations in Urban Neighborhoods," *Aerosol Science and Technology*, vol. 37, p. 33–45, 2003.

[214] D. H. Hagan, G. Isaacman-Vanwertz, J. P. Franklin, L. M. Wallace, B. D. Kocar, C. L. Heald, and J. H. Kroll, "Calibration and assessment of electrochemical air quality sensors by co-location with regulatory-grade instruments," *Atmospheric Measurement Techniques*, vol. 11, no. 1, pp. 315–328, 2018.

[215] E. Lagerspetz, N. H. Motlagh, M. Arbayani Zaidan, P. L. Fung, J. Mineraud, S. Varjonen, M. Siekkinen, P. Nurmi, Y. Matsumi, S. Tarkoma, and T. Hussein, "MegaSense: Feasibility of Low-Cost Sensors for Pollution Hot-spot Detection," *in Proceeding of the IEEE International Conference on Industrial Informatics (INDIN)*, vol. 2019-July, pp. 1083–1090, 2019.

[216] M. Penza, D. Suriano, V. Pfister, M. Prato, and G. Cassano, "Urban Air Quality Monitoring with Networked Low-Cost Sensor-Systems," *Proceedings*, vol. 1, no. 10, p. 573, 2017.

[217] A. P. K. Tai, L. J. Mickley, and D. J. Jacob, "Correlations between fine particulate matter (PM2.5) and meteorological variables in the United States: Implications for the sensitivity of PM2.5 to climate change," *Atmospheric Environment*, vol. 44, no. 32, pp. 3976–3984, 2010.

[218] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the Limits of LoRaWAN," *IEEE Communications Magazine*, vol. 55, p. 34–40, 9 2017.

[219] D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, and B.-Y. Yang, "High-speed high-security signatures," *Journal of Crypto-graphic Engineering*, vol. 2, p. 77–89, 9 2012.

[220] C. Keutmann and T. Pastoor, "Digital Trust Protocol," *Nature*, vol. 555, no. October, pp. 559–560, 2018.

[221] A. Gruner, A. Muhle, T. Gayvoronskaya, and C. Meinel, "A quantifiable trust model for blockchain-based identity management," *in Proceedings of the IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, iThings/Gree*, pp. 1475–1482, 2018.

[222] Z. Wang, J. Lin, Q. Cai, Q. Wang, D. Zha, and J. Jing, "Blockchain-based Certificate Transparency and Revocation Transparency," *IEEE Transactions on Dependable and Secure Computing*, vol. 5971, no. c, pp. 1–1, 2020.

[223] B. Khieu and M. Moh, "CBPKI: Cloud Blockchain-based Public Key Infrastructure," *in Proceedings of the 2019 ACM Southeast Conference*, pp. 58–63, 2019.

[224] Y. Dong, W. Kim, and R. Boutaba, "Conifer: Centrally-Managed PKI with Blockchain-Rooted Trust," *in Proceedings of the IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, iThings/Gree*, pp. 1092–1099, 2018.

[225] S. Matsumoto and R. M. Reischuk, "IKP: Turning a PKI Around with Blockchains," *Cryptology ePrint Archive*, 2016.

[226] R. Khare and A. Rifkin, "Weaving a web of trust.," *World Wide Web Journal*, vol. 2, no. 3, pp. 77–112, 1997.

[227] M. Al-Bassam, "SCPKI: A smart contract-based PKI and identity system," *in Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, pp. 35–40, 2017.

[228] A. Moinet, B. Darties, and J.-L. Baril, "Blockchain based trust & authentication for decentralized sensor networks," *arXiv preprint arXiv:1706.01730*, pp. 1–7, 2017.

[229] B. Leiding, C. H. Cap, T. Mundt, and S. Rashidibajgan, "Authcoin: Validation and Authentication in Decentralized Networks," *arXiv preprint arXiv:1609.04955*, pp. 1–14, 2016.

[230] J. R. Douceur, "The sybil attack," *in Proceedings of the International workshop on peer-to-peer systems,IPTPS 2002*, pp. 251–260.

[231] P. G. Neumann, "Security and privacy," *Computer Science Handbook, Second Edition*, no. December, pp. 77–1, 2004.

[232] Microsoft, "Azure encryption overview." https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview. besucht am 25.11.2021.

[233] H. Shafagh, L. Burkhalter, S. Duquennoy, A. Hithnawi, and S. Ratnasamy, "Droplet: Decentralized Authorization for IoT Data Streams," *in Proceeding of the 29th USENIX Security Symposium (USENIX Security 20)*, pp. 2469–2486, 2018.

[234] S. Agrawal and M. Chase, "FAME: Fast attribute-based message encryption," *in Proceedings of the ACM Conference on Computer and Communications Security*, pp. 665–682, 2017.

[235] F. Wang, J. Mickens, N. Zeldovich, and V. Vaikuntanathan, "Sieve: Cryptographically enforced access control for user data in untrusted clouds," *in Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2016*, pp. 611–626, 2016.

[236] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," *in Proceedings of the IEEE INFOCOM*, 2010.

[237] X. Wang, J. Zhang, E. M. Schooler, and M. Ion, "Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT," *in Proceedings of the IEEE International Conference on Communications, ICC 2014*, pp. 725–730, 2014.

[238] X. Zhu and Y. Badr, "A survey on blockchain-based identity management systems for the internet of things," *in Proceedings of the IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, iThings/Gree*, pp. 1568–1573, 2018.

[239] J. Chen, Y. Liu, and Y. Chai, "An Identity Management Framework for Internet of Things," *Proceedings - 12th IEEE International Conference on E-Business Engineering, ICEBE 2015*, pp. 360–364, 2015.

[240] M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele, and C. Allen, "Decentralized Identifiers ({DIDs}) v1.0," tech. rep., 2019. besucht am 25.07.2021.

[241] S. Capkun, L. Buttyán, and J.-P. Hubaux, "Small worlds in security systems: an analysis of the PGP certificate graph," in *NSPW '02*, 2002.

[242] Espressif Systems, "ESP32 Series - Datasheet." https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf. besucht am 25.05.2022.

[243] X. Zheng, S. Sun, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Meré, "Accelerating Health Data Sharing: A Solution Based on the Internet of Things and Distributed Ledger Technologies," *Journal of medical Internet research*, vol. 21, no. 6, p. e13583, 2019.

[244] D. Hawig, C. Zhou, S. Fuhrhop, A. S. Fialho, and N. Ramachandran, "Designing a distributed ledger technology system for interoperable and general data protection regulation–compliant health data exchange: A use case in blood glucose data," *Journal of Medical Internet Research*, vol. 21, no. 6, pp. 1–13, 2019.

[245] S. K. Pinjala and K. M. Sivalingam, "DCACI: A decentralized lightweight capability based access control framework using iota for internet of things," *in Proceedings of the 5th World Forum on Internet of Things, WF-IoT 2019*, pp. 13–18, 2019.

[246] Alexander Sporn, Thomas Pototschnig, "Powsrv.io PoW libary." https://gitlab.com/powsrv.io/js/iota.lib.js.powsrvio. besucht am 25.05.2022.

[247] G. S. Ramachandran, X. Ji, P. Navaney, L. Zheng, M. Martinez, and B. Krishnamachari, "MOTIVE: Micropayments for trusted vehicular services," *arXiv:1904.01630 [cs]*, 2019.

[248] Y. Park, C. Sur, H. Kim, and K.-H. Rhee, "A Reliable Incentive Scheme Using Bitcoin on Cooperative Vehicular Ad Hoc Networks," *IT CoNvergence PRActice (INPRA)*, vol. 5, no. 4, pp. 34–41, 2017.

[249] P. Missier, S. Bajoudah, A. Capossele, A. Gaglione, and M. Nati, "Mind My Value: A decentralized infrastructure for fair and trusted IoT data trading," *in Proceedings of the ACM International Conference*, 2017.

[250] F. Rezaeibagha and Y. Mu, "Efficient micropayment of cryptocurrency from blockchains," *Computer Journal*, vol. 62, no. 4, pp. 507–517, 2019.

[251] S. T. Ali, D. Clarke, and P. McCorry, "The nuts and bolts of micropayments: A survey," *Preprint arXiv*, 2017.

[252] S. Demmel, A. Lambert, D. Gruyer, A. Rakotonirainy, and E. Monacelli, "Empirical IEEE 802.11p performance evaluation on test tracks," *in Proceedings of the IEEE Intelligent Vehicles Symposium*, pp. 837–842, 2012.

[253] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new type of blockchain for secure message exchange in VANET," *Digital Communications and Networks*, vol. 6, no. 2, pp. 177–186, 2019.

[254] M. T. Lwin, J. Yim, and Y. B. Ko, "Blockchain-based lightweight trust management in mobile ad-hoc networks," *Sensors (Switzerland)*, vol. 20, no. 3, pp. 1–19, 2020.

[255] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "BARS: A Blockchain-Based Anonymous Reputation System for Trust Management in VANETs," *in Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, pp. 98–103, 2018.

[256] X. Deng and T. Gao, "Electronic Payment Schemes Based on Blockchain in VANETs," *IEEE Access*, vol. 8, pp. 38296–38303, 2020.

[257] Y. Park, C. Sur, and K. H. Rhee, "A Secure Incentive Scheme for Vehicular Delay Tolerant Networks Using Cryptocurrency," *Security and Communication Networks*, vol. 2018, 2018.

[258] M. Wagner and B. McMillin, "Cyber-physical transactions: A method for securing VANETs with Blockchains," *in Proceedings of IEEE Pacific Rim International Symposium on Dependable Computing, PRDC*, vol. 2018-Decem, pp. 64–73, 2019.

[259] S. Kim, "Impacts of Mobility on Performance of Blockchain in VANET," *IEEE Access*, vol. 7, pp. 68646–68655, 2019.

[260] K.-K. Jung and W.-S. Choi, "Estimation of Vehicle's CO2 Emission using OBD-II Interface," *Journal of the Korea Society of Computer and Information*, vol. 16, pp. 167–174, 2011.

[261] Y. Khaled, M. Tsukada, J. Santa, and T. Ernst, "The role of communication technologies in vehicular applications," *Advances in Vehicular Ad-Hoc Networks: Developments and Challenges*, pp. 37–58, 2010.

[262] G. Theodorakopoulos and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 318–328, 2006.

[263] B. Padmavathi and S. R. Kumari, "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique," *International Journal of Science and Research (IJSR)*, vol. 2, no. 4, pp. 170–174, 2013.

[264] Florian Klingler, "OpenC2X-standalone." https://github.com/florianklingler/OpenC2X-standalone/blob/master/config/openc2x_dcc. besucht am 25.05.2022.

[265] F. Klingler, G. S. Pannu, C. Sommer, B. Bloessl, and F. Dressler, "Poster: Field testing vehicular networks using OpenC2X," *in Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services*, p. 178, 2017.

[266] A. Matsumoto, K. Yoshimura, S. Aust, T. Ito, and Y. Kondo, "Performance evaluation of IEEE 802.11n devices for vehicular networks," *in Proceedings of the Conference on Local Computer Networks, LCN*, pp. 669–670, 2009.

[267] ABI research, “V2X System Cost Analysis DSRC+LTE and C-V2X+LTE,” 2018.

[268] A. Festag, “Standards for vehicular communication—from IEEE 802.11p to 5G,” *Elektrotechnik und Informationstechnik*, vol. 132, no. 7, pp. 409–416, 2015.

[269] J. Santa, F. Pereñíguez, A. Moragón, and A. F. Skarmeta, “Experimental evaluation of CAM and DENM messaging services in vehicular communications,” *Transportation Research Part C: Emerging Technologies*, vol. 46, no. September, pp. 98–120, 2014.

[270] Schiener, Dominik, “The Anatomy of a Transaction.” https://domschiener.gitbooks.io/iota-guide/content/chapter1/transactions-and-bundles.html. besucht am 25.05.2022.

[271] Radiocommunication Study Groups, “Intelligent transport systems (ITS) usage in ITU Member States,” tech. rep., 2017.

[272] T. Pototschnig, “PiDiver 1.3 Documentation,” 2019.

[273] Xilinx, “zynq7000.”

[274] D. Dolev and A. C. Yao, “On the Security of Public Key Protocols,” in *Proceedings of the 22nd Annual Symposium on Foundations of Computer Science*, SFCS ’81, (USA), p. 350–357, IEEE Computer Society, 1981.

[275] J. Walker, “Chapter 7 - Internet Security,” in *Computer and Information Security Handbook* (J. R. Vacca, ed.), pp. 93–117, Boston: Morgan Kaufmann, 2009.

[276] S. Bohacek, J. P. Hespanha, Junsoo Lee, C. Lim, and K. Obraczka, “A new TCP for persistent packet reordering,” *IEEE/ACM Transactions on Networking*, vol. 14, no. 2, pp. 369–382, 2006.

[277] A. Sadiq, N. Javaid, O. Samuel, A. Khalid, N. Haider, and M. Imran, "Efficient Data Trading and Storage in Internet of Vehicles using Consortium Blockchain," *2020 International Wireless Communications and Mobile Computing, IWCMC 2020*, pp. 2143–2148, 2020.

[278] H. Ahmed, S. Pierre, and A. Quintero, "A flexible testbed architecture for VANET," *Vehicular Communications*, vol. 9, no. April, pp. 115–126, 2017.

[279] R. K. Schmidt, T. Köllmer, T. Leinmüller, B. Böddeker, and G. Schäfer, "Degradation of Transmission Range in VANETs caused by Interference," *PIK - Praxis der Informationsverarbeitung und Kommunikation*, vol. 32, no. 4, 2010.

[280] R. Miucic, Z. Popovic, and S. Mahmud, "Experimental Characterization of DSRC Signal Strength Drops," *in Proceedings of the 12th International IEEE Conference on Intelligent Transportation Systems, ITSC*, pp. 1–5, 2009.

[281] M. Boban, T. T. V. Vinhoza, M. Ferreira, J. Barros, and O. K. Tonguz, "Impact of Vehicles as Obstacles in Vehicular Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 1, pp. 15–28, 2011.

[282] European Commission DG Communications Networks, "Mobile Broadband Prices in Europe, howpublished = http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50378, note = besucht am 25.05.2022."

[283] Eurostat, "Electricity prices (including taxes) for household consumers, first half 2020." https://ec.europa.eu/eurostat/statistics-explained/index.php/Electricity_price_statistics. besucht am 25.05.2022.

[284] J. Robert, S. Kubler, and S. Ghatpande, "Enhanced Lightning Network (off-chain)-based micropayment in IoT ecosystems," *Future Generation Computer Systems*, vol. 112, pp. 283–296, 2020.

[285] N. Khan and R. State, “Lightning Network: A Comparative Review of Transaction Fees and Data Analysis,” *in Proceedings of the International Congress on Blockchain and Applications*, 2019.

[286] J. Kurmi and A. Sodhi, “A survey of zero-knowledge proof for authentication,” *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, no. 1, 2015.