Spezifikationsbericht

Blockchain-Technologie-Anwendungen für AVIK

Stand der Forschung, Herleitung und Beschreibung relevanter Use Cases

Version 08/2023

Fred Steinmetz & Friedrich-Philipp Wazinski
Blockchain Research Lab gGmbH

Gefördert durch:

Bundesministerium
für Digitales
und Verkehr

aufgrund eines Beschlusses
des Deutschen Bundestages

Inhalt

Abbildungsverzeichnis ..... **II**

Tabellenverzeichnis ..... **III**

Abkürzungsverzeichnis ..... **IV**

1 Stand der Forschung zu Blockchain-Technologie im Kontext von UAVs **1**

Bibliometrische Analyse: Blockchain & Drohnen 1

Forschungsstrom I: Sicherheits- und Authentifizierungsschemata im Internet of Drones 2

Forschungsstrom II: Sicherheit und Datenschutz in aufstrebenden Technologien 4

Forschungsstrom III: Federated Learning 6

Forschungsstrom IV: Ressourcen- und Datenmanagement (in IoT) 8

Forschungsstrom V: Optimierung von UAV-MEC: Sicherheit und Anwendungsfälle 9

Forschungsstrom VI: Blockchain-gestützter Datenaustausch im Internet of Drones 10

Framework zur Blockchain-Anwendung im IoD 11

Zusammenfassung: Mehrwerte der Blockchain-Technologie in UAV-Systemen 15

2 Identifikation und Beschreibung relevanter Anwendungen in AVIK **16**

Warum Blockchain-Technologie? 16

Private und öffentliche Blockchain-Netzwerke im Kontext von AVIK 20

Öffentliche Netzwerke 20

Private Netzwerke 21

Zweckdienliche Eigenschaften der Blockchain-Technologie für AVIK 22

Innovationskapazität der Zusammenführung von unterschiedlichen Datenquellen 22

Incentivierung kontinuierlicher Datensammlung durch Verwertungsperspektive 23

Beschreibung relevanter Use Cases 24

I. Identifizierungs- und Authentifizierungssystem für UAVs und Fahrzeuge 24

II. Protokollierung von Metadaten zu Datenerhebungen 27

III. Dezentraler Marktplatz: Zugriffsmanagement und Handelsabwicklung 30

Literaturverzeichnis **34**

Abbildungsverzeichnis

Abbildung 1: Überblick über die wissenschaftliche Forschungslandschaft im Bereich Blockchain und Drohnen 1

Abbildung 2: Blockchain-basiertes Netzwerkmodell zur Erkennung nicht autorisierter UAVs in IoD 3

Abbildung 3: Architektur eines blockchain-basierten föderierten Lernsystems für UAV-gestütztes mobiles Crowdsensing 7

Abbildung 4: Framework zur Blockchain-Anwendung im IoD 14

Abbildung 5: Strukturelle Chancen von Blockchain-Systeme 16

Abbildung 6: Sechs-Schichten-Modell der Blockchain-Architektur 17

Abbildung 7: Schema zur Visualisierung eines DLT-basierten ID- und Authentifizierungssystems 26

Abbildung 8:Schematische Darstellung des Ablaufs einer ID-Zuordnung und Authentifizierung 27

Abbildung 9: Vereinfachte Visualisierung eines Blockchain-basierten Systems zur Protokollierung von Metadaten über Datenerhebungen 29

Abbildung 10: Vereinfachte Darstellung eines Blockchain-Systems mit Marktplatzlogik 32

Tabellenverzeichnis

Tabelle 1: Einsatzgebiete der Blockchain-Technologie in unbemannten Luftfahrzeugen.....15

Tabelle 2: Vor- und Nachteile öffentlicher Blockchain-Netzwerke.....20

Tabelle 3: Vor- und Nachteile privater Blockchain-Netzwerk.....21

Abkürzungsverzeichnis

CPU	Central Processing Unit
DAO	Decentralized Autonomous Organization
DLT	Distributed-Ledger-Technology
GSS	Ground Server Station
GUI	Graphical User Interface
IIoT	Industrial Internet of Things
IoD	Internet of Drones
IoT	Internet of Things
KI	Künstliche Intelligenz
MCS	Mobile Crowd Sensing
MEC	Mobile Edge Computing
UAV	Unmanned Aerial Vehicles
P2P	Peer-to-Peer

1 Stand der Forschung zu Blockchain-Technologie im Kontext von UAVs

Bibliometrische Analyse: Blockchain & Drohnen

Die Aufrüstung und Ausstattung von Geräten und Gegenständen mit Sensoren hin zu internet- und kommunikationsfähigen Objekten, die Informationen erheben, verarbeiten und austauschen können, bezeichnet man gemeinhin als das Internet der Dinge (IoT; internet of things). Die Anwendung der Blockchain-Technologie im Kontext des IoT ist in den letzten Jahren zu einem umfassenden Forschungsfeld herangewachsen. Hierbei erweisen sich insbesondere die inhärenten Eigenschaften der Blockchain - wie ihre Dezentralität, Transparenz und Sicherheit - als vielversprechend für die Adressierung einer Vielzahl von Herausforderungen im Bereich des IoT. Dies gilt insbesondere in Hinblick auf Themen wie Datenintegrität, -sicherheit und -privatsphäre, aber auch für die Realisierung von automatisierten Transaktionen und Interaktionen zwischen den einzelnen Geräten und Objekten im IoT. In der vorliegenden Untersuchung wurde eine explorative Faktorenanalyse genutzt, um dieses umfangreiche Forschungsgebiet zu sondieren.

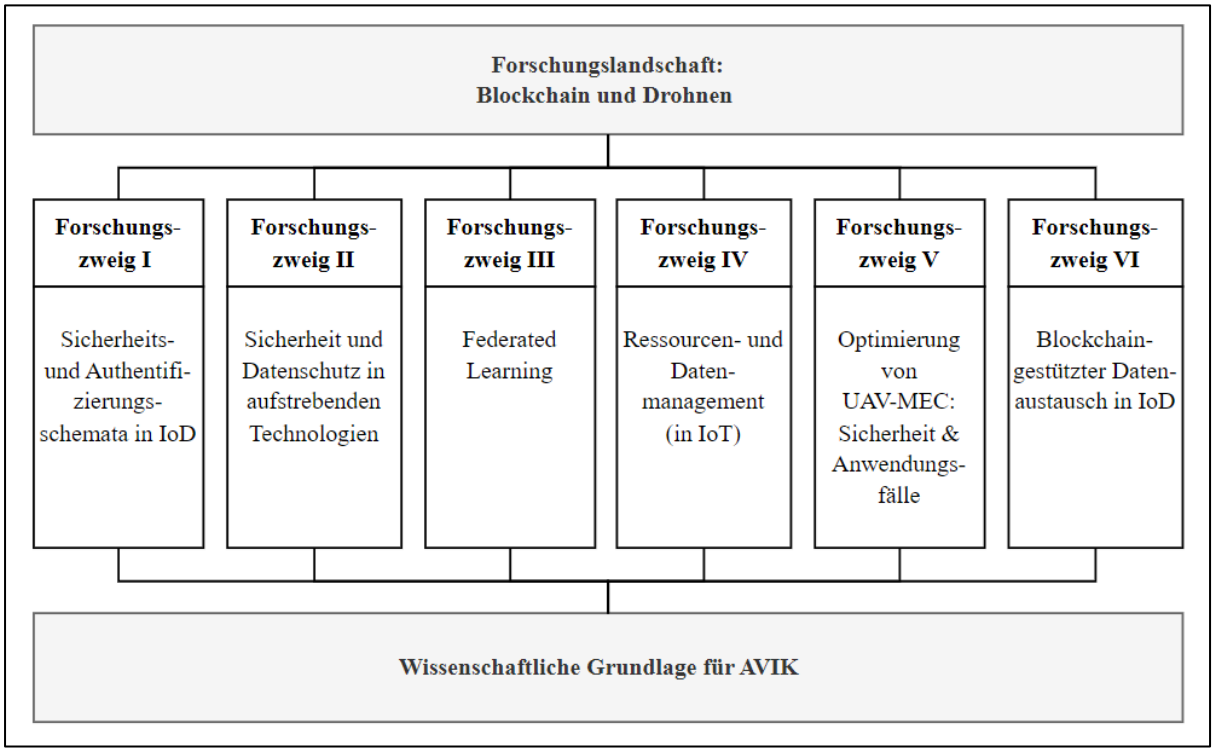

Abbildung 1: Überblick über die wissenschaftliche Forschungslandschaft im Bereich Blockchain und Drohnen
Quelle: Eigene Darstellung

Der primäre Fokus dieser Analyse lag auf der Exploration der Intersektion zwischen den zwei Technologiebereichen - der Blockchain-Technologie und der Drohnentechnik. Dabei galt es,

die Verbindungsstellen und Überschneidungspunkte dieser beiden Technologien zu identifizieren und zu erforschen. Diese Analysetechnik ermöglicht durch die Anwendung statistischer Methoden eine Reduktion der Forschungsdimensionen und die Kategorisierung verschiedener Forschungszweige. Im Zuge dieser Untersuchung wurden sechs Forschungsbereiche ermittelt, die eng mit der aktuellen Forschung im Bereich Blockchain und Drohnen verknüpft sind. Abbildung 1 veranschaulicht die identifizierten Forschungsstränge I bis VI, welche in den nachfolgenden Unterkapiteln näher erläutert werden.

Forschungsstrom I: Sicherheits- und Authentifizierungsschemata im Internet of Drones

Der Forschungszweig I konzentriert sich auf die Entwicklung von Datenschutz- und Sicherheitsrahmenschemata im Kontext des Internet der Drohnen (IoD; Internet of Drones). Im Mittelpunkt stehen Sicherheitsaspekte der Kommunikation und Datenübertragung zwischen unbemannten Luftfahrzeugen (UAVs; unmanned aerial vehicles), zwischen UAVs und terrestrischen Fahrzeugen sowie zwischen UAVs und bodengestützten Serverstationen (GSS; ground server stations). Wesentliche Problemfelder umfassen Schwachstellen in Bezug auf Authentifizierung, Offenlegung von Positions- und Flugdaten, Drohnenentführung und Identitätsverstöße.

Innerhalb des betrachteten Forschungsstroms bieten eine Vielzahl von wissenschaftlichen Publikationen Blockchain-basierte Lösungsvorschläge für die genannten Problemfelder an. Allen voran sind dabei die Publikationen von Bera et al. (2021), Bera, Chattaraj et al. (2020) und Bera, Saha, et al. (2020) hervorzuheben, welche die Blockchain-Technologie für die Konzeptionalisierung von Authentifizierungs- und Datenaustauschschemata nutzen, um Transparenz, Sicherheit, den Automatisierungsgrad und die Interoperabilität in drohnengestützten Peer-to-Peer-Netzwerken zu erhöhen.

Die Blockchain bildet dabei einen Teil eines komplexen Netzwerks, welches beispielhaft im Systemmodell in Abbildung zwei dargestellt ist (Bera et al. 2021). Innerhalb dieses Netzwerks registriert eine vertrauenswürdige Registrierungsstelle alle Netzwerkakteure wie Drohnen und Server. Die Kommunikation innerhalb des Netzwerks erfolgt auf Basis eines Sitzungsschlüssels, sowie auf zertifikat- und signaturbasierten Mechanismen. Dies ermöglicht sowohl die sichere Kommunikation von Echtzeitdaten von Drohnen an die Bodenstation als auch die Identifizierung von nicht autorisierten Drohnen innerhalb einer definierten Flugzone (Bera et al. 2021). Die Bodenstation sendet nachfolgend die Transaktion an ein Peer-to-Peer Cloud-Server-Netzwerk, welches für die Blockgenerierung, die Verifizierung mittels Konsensus-

Mechanismus und die Aufnahme in die private Blockchain verantwortlich ist (Bera et al. 2021). Durch die Datenspeicherung in der privaten Blockchain sind die Daten nicht nur vor Fälschungsversuchen geschützt, sondern die Authentizität ist ebenfalls garantiert, wodurch die Daten nachfolgend mittels maschinellem Lernen für die Vorhersage von Analysen verwendet werden können (Bera et al. 2021).

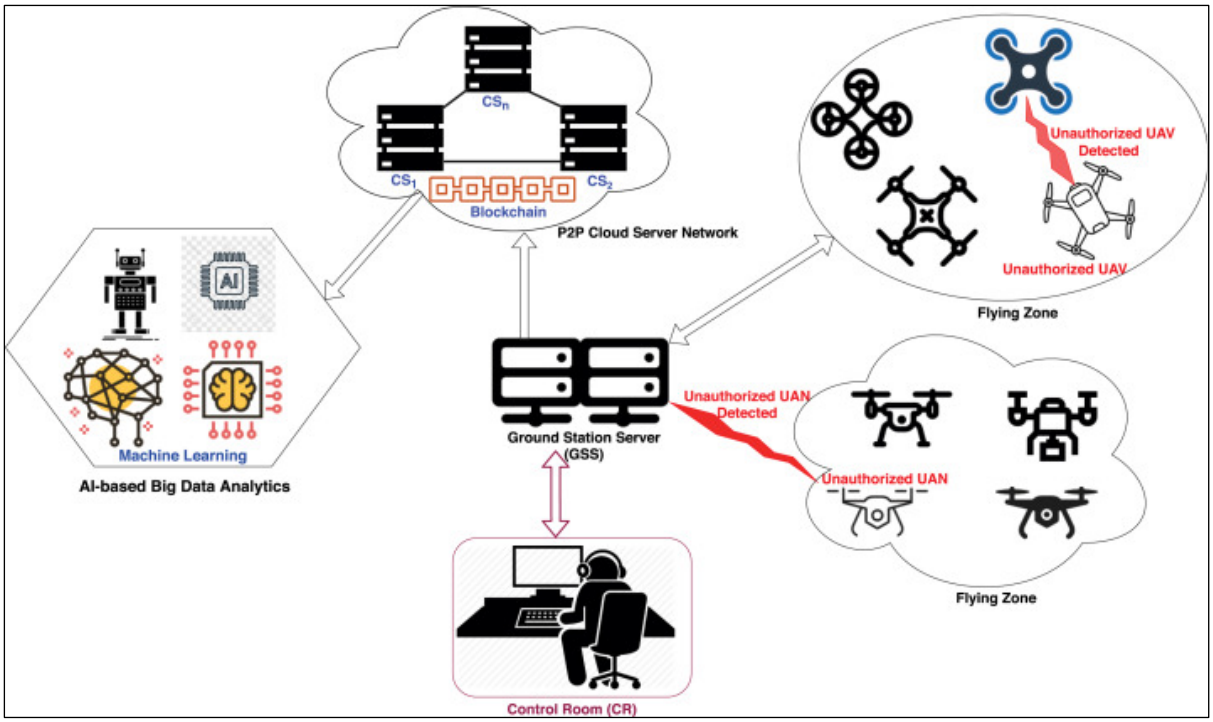

Abbildung 2: Blockchain-basiertes Netzwerkmodell zur Erkennung nicht autorisierter UAVs in IoD
Quelle: Bera et al. (2021)

Insgesamt eröffnet die Anwendung der Blockchain-Technologie erhebliche Potenziale und Vorteile im Kontext der IoD-Authentifizierung und des Datenaustauschs. Durch die dezentralisierte Natur der Technologie kann sie nicht nur zur Robustheit des Gesamtsystems beitragen, indem einzelne zentrale Ausfallpunkte (single-points-of-failure) umgangen werden können, sondern auch eine höhere Transparenz und Nachverfolgbarkeit aller Transaktionen ermöglichen, wodurch alle Zugriffsaktivitäten im Authentifizierungsprozess lückenlos verfolgt werden können. Darüber hinaus bietet die Blockchain-Technologie durch den Einsatz kryptographischer Algorithmen eine erhöhte Datenintegrität. Durch den Einsatz von Smart Contracts, die als automatisierte Verträge verstanden werden können, kann die Blockchain dazu beitragen, Authentifizierungsprozesse in IoD-Netzwerken zu automatisieren. Weiterhin kann Blockchain-Technologie den Schlüssel für die Schaffung von Interoperabilität zwischen diversen Hard-

und Softwarevarianten unterschiedlicher Hersteller und Anbieter darstellen, wenn sie als offene Schnittstelle gestaltet wird und dabei gesetzliche Standards implementiert.

Zusammenfassend lässt sich feststellen, dass die Forschung im Bereich der Authentifizierung und des Datenaustauschs in IoD, insbesondere Blockchain-basierte Ansätze, sich in einem initialen und entwicklungsfähigen Stadium befindet, in dem besondere Herausforderungen hinsichtlich Skalierbarkeit, Latenzzeiten, Kosten- und Energieeffizienz bestehen. Dennoch ist die Anwendung eines dezentralen Systems für die Authentifizierung und Datenaustausch im IoD ein sinnvoller Ansatzpunkt, vor allem im Hinblick auf die Abbildung von zukünftig erwartbar steigender Anzahl von automatisierter und autonomer Interaktion zwischen Drohnen. Die Technologie kann in der adäquaten Ausgestaltung durch die redundante Speicherung von Informationen, die erhöhte System-Resilienz durch die Reduktion des Single-Points-of-Failure, sowie die Schaffung notwendiger selektiver Transparenz und Nachvollziehbarkeit und die forcierte Anwendung von Standards einer zentralen Lösung in Performance- und Sicherheitsaspekten überlegen sein.

Forschungsstrom II: Sicherheit und Datenschutz in aufstrebenden Technologien

Der zweite Forschungszweig, der insgesamt 46 Publikationen umfasst, konzentriert sich überwiegend auf hochaktuelle Themen wie Künstliche Intelligenz (KI), Blockchain, Tactile Internet und intelligente Fahrzeugnetzwerke. Im Mittelpunkt des wissenschaftlichen Diskurses stehen dabei vorrangig Fragen der Sicherheit und des Datenschutzes im Kontext dieser aufstrebenden Technologien.

Innerhalb dieses Forschungszweigs kann die Arbeit von Gupta et al. (2020) als die Publikation mit der besten thematischen Übereinstimmung angesehen werden und somit als repräsentativ für den Forschungszweig betrachtet werden. Die Studie behandelt systematisch die komplexen Fragestellungen bezüglich Datenschutz- und Sicherheitsschwachstellen, die sich aus der Anwendung von Smart Contracts ergeben. Gupta, Tanwar und Al-Turjman et al. (2020) widmen sich insbesondere den logischen Schwachstellen, die beispielsweise durch Transaction Ordering, Zero Division Risk oder Stack Size Limit entstehen können, sowie den strukturellen Schwachstellen wie Immutable Bugs, „Ether Lost or Transfer“ oder der Verwendung von Blockhashes. Sheth et al. (2020) thematisieren potentielle Einsatzbereiche der KI und beleuchten dabei verschiedene Anwendungsfelder, mit einem besonderen Fokus auf den Schutz und die Privatsphäre in Kommunikationstechnologien, die durch Netzwerke der sechsten Generation (6G) ermöglicht werden. Bhattacharya et al. (2021) und Hathaliya et al. (2019)

untersuchen die Bedeutung und Potentiale von Blockchain und maschinellem Lernen im Gesundheitswesen. Während Bhattacharya et al. (2021) ein Rahmenwerk für die gemeinsame Nutzung elektronischer Gesundheitsdaten vorstellen, das auf Blockchain- und Deep-Learning-Technologien beruht, schlagen Hathaliya et al. (2019) eine dezentrale KI-gestützte Blockchain-Architektur für die Fernüberwachung von Patienten vor.

Die Sicherheit in intelligenten Fahrzeugnetzwerken stellt einen weiteren Schwerpunkt des zweiten Forschungsstranges dar. Tanwar et al. (2018) präsentieren eine Taxonomie zur Klassifizierung von technischen Angriffsvektoren und entsprechenden Gegenmaßnahmen im Bereich von Ad-hoc-Fahrzeugnetzwerken. Gupta, Tanwar und Kumar (2020) hingegen untersuchen ein System für autonome Fahrzeuge, welches die Blockchain-Technologie verwendet, und bewerten die Sicherheitsresistenz im Vergleich zu herkömmlichen Sicherheitsmaßnahmen. Allen voran betonen die Autoren die potenziellen Verbesserung des Datenschutzes und der Sicherheit in autonomen Fahrzeugnetzwerken durch den Einsatz von Blockchain-Technologie. Gleichzeitig verweisen sie jedoch simultan auf die bestehende Herausforderungen in Bezug auf die Skalierbarkeit, das eingeschränkte Transaktionsvolumen und die Auswahl der passenden Netzwerkstruktur. Weiterhin untersuchen Alladi et al. (2020) die möglichen Anwendungen und die Rolle der Blockchain-Technologie in verschiedenen Szenarien, wie beispielsweise dem automatisierten Management von Lieferketten, der Verwendung von unbemannten Luftfahrzeugen und der dezentralen Speicherung von Daten und Informationen. Die Autoren kommen zu dem Schluss, dass die Implementierung der Blockchain-Technologie das Potenzial hat, wichtige Probleme in Bezug auf Datenschutz, Koordination, Sicherheit und Entscheidungsfindung bei unbemannten Luftfahrzeugen effektiv zu lösen. In einer anderen relevanten Studie stellen Rana et al. (2019) einen Blockchain-basierten Sicherheitsmechanismus vor, der auf Hashing- und digitalen Signaturtechniken zur Verschlüsselung der gesammelten Daten basiert. Weiterhin entwerfen García-Magariño et al. (2019) ein Blockchain-basiertes System zur Überwachung von unbemannten Luftfahrzeugen.

Der wissenschaftliche Diskurs im Rahmen des Forschungsfeldes II beleuchtet vielschichtig aktuelle Themen im Bereich der aufstrebenden Technologien, wobei der Schwerpunkt vorrangig auf Sicherheit und Datenschutz liegt. Die analysierten Studien veranschaulichen die vielfältigen Möglichkeiten und Herausforderungen, die mit der Anwendung und Integration fortschrittlicher Technologien wie Blockchain einhergehen.

Forschungsstrom III: Federated Learning

Der dritte Forschungsstrom, der durch die explorative Faktorenanalyse zur Dimensionsreduktion identifiziert wurde, fokussiert sich auf das Thema des federated learning (föderierten Lernens) und beinhaltet 37 Publikationen. Die wissenschaftliche Literatur innerhalb dieses Forschungsstroms ist durch eine thematisch verknüpfte Zweiteilung charakterisiert. Eine Gruppe von Publikationen befasst sich mit den Grundlagen und fundamentalen Charakteristiken des föderierten Lernens, während eine zweite Gruppe die Schnittstelle und Anwendungsmöglichkeiten von Blockchain-Technologie und föderierten Lernen thematisiert. Zudem beziehen sich die Publikationen auf verschiedene Anwendungsfelder, wie zum Beispiel das Internet der Dinge, das industrielle Internet der Dinge (IIoT) und Smart-Home-Anwendungen. Der wissenschaftliche Diskurs innerhalb dieses Forschungsfeldes verdeutlicht das erhebliche Potenzial der Verknüpfung von Blockchain-Technologie und föderiertem Lernen. Aus der kombinierten Anwendung dieser Technologien ergeben sich vielfältige Vorteile, insbesondere in Bezug auf Verbesserungen in der Datenerfassung, der Datensicherheit, der Nachvollziehbarkeit sowie im Energieverbrauch und der Möglichkeit für automatisierte Kompensation.

Das föderierte Lernen ermöglicht den Austausch von Modelldaten über eine Vielzahl von Geräten, ohne dass dabei sensible Daten zentral gespeichert werden müssen. Dieser Prozess kann über Blockchain-Technologie erfolgen, die eine dezentrale Datenbank bietet und Transaktionen transparent, unveränderlich und sicher macht. Beispielsweise wird die Kombination dieser Technologien in der IoT-Geräteherstellung genutzt, um Authentizität, Transparenz und Rückverfolgbarkeit von elektronischen Geräten und deren Fertigungsprozessen zu gewährleisten (Zhao et al. 2021). Darüber hinaus ermöglicht sie ein effizientes On-Device-Machine-Learning ohne zentrale Koordination (Kim et al. 2020). Die nachfolgende Abbildung 3 illustriert dabei, in vereinfachter Form, ein föderiertes Lernmodel ohne den Einsatz einer zentralen Entität nach Wang et al. (2021).

Im Rahmen des IIoT wurden ebenfalls ganzheitliche Ansätze vorgeschlagen, die auf der Verknüpfung von Blockchain-Technologie und maschinellem Lernen beruhen. Ein Beispiel hierfür ist der Vorschlag von Liu et al. (2019), die ein Ethereum-basiertes Deep Reinforcement Learning System präsentieren. Dieses System zielt darauf ab, eine energieeffiziente Datenerfassung und einen sicheren Datentransfer von intelligenten mobilen Endgeräten wie

Mobiles Crowdsensing stellt ein innovatives Erfassungsparadigma im Bereich des vernetzten Computing dar, bei dem eine Vielzahl von mobilen Geräten kooperieren, um sensorische Daten aus ihrer unmittelbaren Umgebung wie beispielsweise Standorte, Lärmpegel und Verkehrsbedingungen zu erfassen und auszutauschen (Guo et al. 2014).

beispielsweise UAVs oder Smartphones im Kontext des sogenannten "mobile crowdsensing" (MSC) zu gewährleisten. Weiterhin untersuchen die Autoren Lu et al. (2020) in ihrer Studie die sicherheitsoptimierte Datenfreigabe zwischen mehreren Parteien im IIoT. Dabei nutzen sie ein privates Blockchain-Netzwerk und setzen das Konzept des föderierten Lernens ein, um Datenlecks zu minimieren.

Im Bereich des IoD bietet die Verknüpfung von Blockchain und föderiertem Lernen sichere Mechanismen für den Austausch und die Validierung von lokalen Modellupdates. Wang et al. (2021) und Pokhrel (2020) verwenden eine Konsortium-Blockchain und mobile föderierte Lernsysteme, um einen sicheren Rahmen für mobiles Crowdsensing, sowie eine sichere und effiziente Zusammenarbeit und Notfallmanagement in 6G-Edge-Umgebungen zu schaffen.

Die analysierten Studien illustrieren die multiplen Anwendungsmöglichkeiten und Vorteile, die sich aus der Kombination von Blockchain-Technologie und föderiertem Lernen ergeben, insbesondere im Kontext des Internet of Things und des Industrial Internet of Things. Dabei unterstreichen sie das Potenzial dieser Technologiekombination, den Datenaustausch zwischen mobilen Einheiten zu erleichtern und gleichzeitig Sicherheit und Datenschutz zu gewährleisten, während die Notwendigkeit einer zentralen Autorität entfällt.

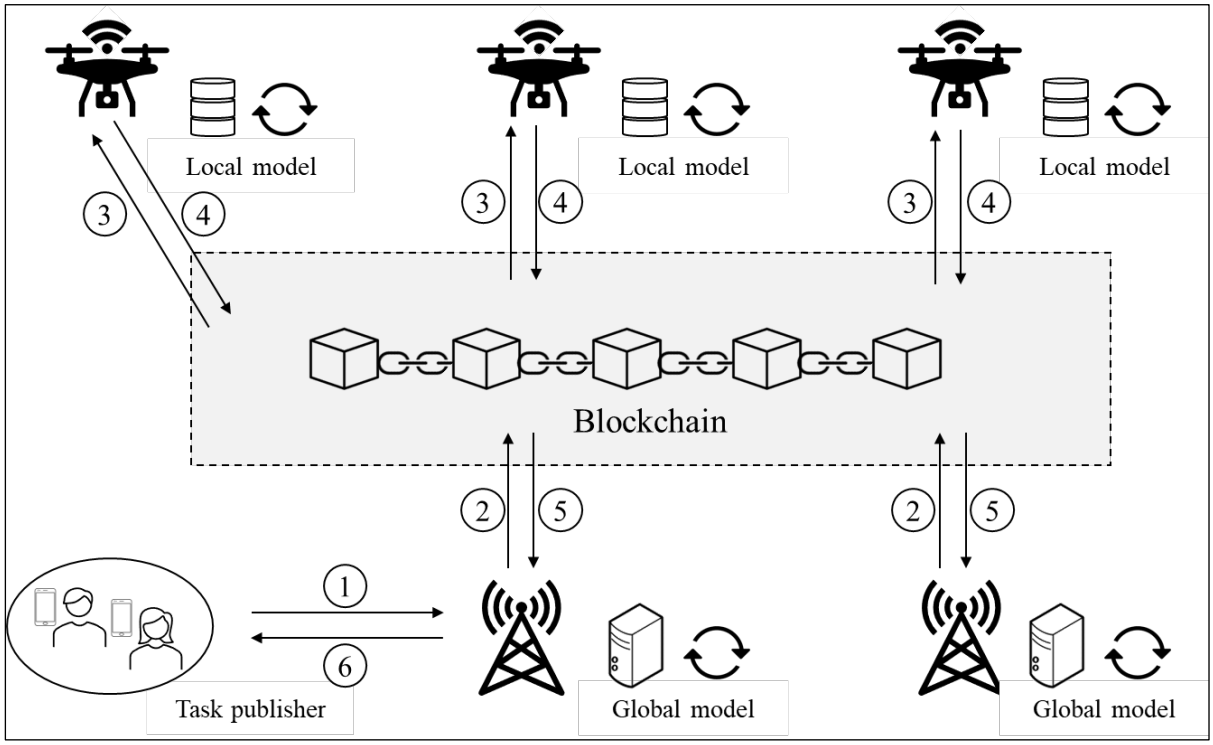

Abbildung 3: Architektur eines Blockchain-basierten föderierten Lernsystems für UAV-gestütztes mobiles Crowdsensing
Quelle: In Anlehnung an Wang et al. (2021)

Zusammenfassend lässt sich feststellen, dass die Verknüpfung von föderiertem Lernen und Blockchain-Technologie eine vielversprechende technologische Konvergenz darstellt. Vergleichbar mit den Forschungsbemühungen im ersten Forschungsstrom, befinden sich die gegenwärtigen Untersuchungen zur Synergie zwischen föderiertem Lernen und Blockchain-Technologie allerdings ebenfalls in einer initialen Entwicklungsphase.

Forschungsstrom IV: Ressourcen- und Datenmanagement (in IoT)

Forschungsstrom IV umfasst 31 Publikationen, was 11% der im Datensatz vorhandenen Veröffentlichungen entspricht. Die betrachteten Publikationen behandeln eine Vielzahl von Themen, die mit der Verwaltung von Ressourcen und Daten im Kontext des IoT zusammenhängen. Vor diesem Hintergrund kann der vierte Forschungszweig als "Ressourcen- und Datenmanagement (in IoT)“ kategorisiert werden.

Im Zentrum des Forschungsstromes steht die Studie von Hayat et al. (2016), die sich mit den Anwendungen von UAVs aus der Perspektive der Kommunikationstechnik befasst. Die Autoren betonen, dass die spezifischen Anforderungen der verschiedenen Einsatzbereiche - Rettungsaktionen, Netzabdeckung, Überwachung und Maintenance im Bauwesen sowie Warenlieferungen - qualitativ und quantitativ variieren, insbesondere im Hinblick auf die Kommunikation und minimalen Datenanforderungen.

Ein weiterer entscheidender Aspekt in diesem Forschungsstrom ist die Rolle der Blockchain-Technologie bei der Verwaltung von Daten und Ressourcen. Xiong et al. (2018) stellen ein Modell für mobiles Edge-Computing-Ressourcenmanagement speziell für mobile Blockchains vor, das die begrenzten Energie- und CPU-Ressourcen von IoT-Geräten berücksichtigt. Ein ähnliches Konzept wird von Xiong et al. (2019) verfolgt, in dem sie ein ressourcenorientiertes Managementsystem für Proof-of-Work-Blockchain-Netzwerke präsentieren.

Zusätzliche innovative Ansätze zur Ressourcenverwaltung unter Einbeziehung der Blockchain-Technologie werden von Novo (2018), Shen et al. (2019) und Zhu et al. (2019) vorgestellt. Novo (2018) stellt ein Ethereum-basiertes Zugangsverwaltungssystem für das IoT dar, das ohne eine zentrale Instanz operiert. Ebenso implementieren Shen et al. (2019) und Zhu et al. (2019) Blockchain-Technologie zur Steuerung von Datensystemen. Shen et al. (2019) präsentieren eine Blockchain-basierte Plattform, die sicheren Datenaustausch zwischen IoT-Datenanbietern ermöglicht. Diese Plattform beinhaltet ein datenschutzkonformes Trainingsverfahren für Support Vector Machines zur Verarbeitung verschlüsselter IoT-Daten. Ähnlich

verfolgen Zhu et al. (2019) ein Modell für sichere Datenverwaltung, welches ebenfalls auf Blockchain-Technologie beruht.

Zusammenfassend lassen die Forschungsergebnisse des vierten Forschungsstroms erkennen, dass die Blockchain-Technologie zur Optimierung der Ressourcen- und Datenverwaltung in IoT-Umgebungen genutzt werden kann. Dabei lassen die Publikation erkennen, dass Blockchain-Technologie das Potenzial hat, die Effizienz der Geräteverwaltung zu verbessern, sichere Datenübertragungen zu gewährleisten und die Kontrolle in Cloud-Umgebungen zu optimieren. Dies unterstreicht die zentrale Rolle der Blockchain-Technologie als entscheidendes Instrument zur Ressourcen- und Datenverwaltung in IoT-Umgebungen.

Forschungsstrom V: Optimierung von UAV-MEC: Sicherheit und Anwendungsfälle

Der fünfte Forschungsstrom umfasst 25 Veröffentlichungen, die 9% des gesamten Datensatzes repräsentieren. Der zentrale Fokus dieses Forschungszweiges liegt auf der Anwendung von UAVs in Verbindung mit Mobile Edge Computing (MEC) oder Edge Cloud Computing. Die wissenschaftlichen Arbeiten adressieren in diesem Bereich eine Vielzahl von Themen, einschließlich der Auslagerung von Aufgaben, dem sogenannten Offloading, der Optimierung der Recheneffizienz und der Flugbahn sowie der Bewertung der Sicherheitsleistung. Angesichts dieser thematischen Zentralisierung ist es angemessen, den Forschungsstrom als "Optimierung von UAV-MEC: Sicherheit und Anwendungsfälle" zu bezeichnen.

Die Studie von Zhou et al. (2020) steht im Zentrum dieses Forschungszweiges und stellt ein MEC-System vor, das UAVs zur Auslagerung rechenintensiver Aufgaben von Bodennutzern auf nahegelegene UAVs verwendet. Die Studie stellt einen Algorithmus vor, der den Datenschutz optimiert, während gleichzeitig der UAV-Standort, das Entlastungsverhältnis und die jeweiligen Energieleistungsbeschränkungen der beteiligten UAVs berücksichtigt werden.

Zudem wurde die Thematik der UAV-gestützten MEC-Systeme von anderen Forschern ebenfalls ausführlich thematisiert. Dabei liegt ein besonderer Schwerpunkt auf Aspekten wie dem gemeinsamem Offloading, der Maximierung der Rechenleistung sowie der Optimierung der Flugbahn. Zum Beispiel stellen Zhou et al. (2018) einen zweistufigen Algorithmus zur partiellen Berechnungsauslagerung und einen dreistufigen Algorithmus zur binären Berechnungsauslagerung in UAV-gestützten MEC-Systemen vor. Guo und Liu (2020) schlagen einen Ansatz vor, der Berechnungsauslagerung, Flugbahn-Optimierung und Bit-Zuteilung sowohl im Uplink als auch im Downlink zur Reduzierung des Energieverbrauchs in UAV-basierten mobilen Edge-Umgebungen einbezieht. Weiterhin geben Mach und Becvar (2017) einen Überblick über

MEC-Anwendungsszenarien und klassifizieren die Forschung zur Berechnungsauslagerung in drei Kategorien: Entscheidungen zur Berechnungsauslagerung, Ressourcenzuteilung und Mobilitätsmanagement. Darüber hinaus illustriert die Studie von Motlagh et al. (2017) die Anwendung von Video-Daten-Auslagerung zu MEC-Knoten im Bereich der Menschenmengen-Überwachung, was den Autoren eine gesteigerte Effizienz bei der Datenanalyse und Energieeinsparung zur Folge hat.

Zusammenfassend lässt sich konstatieren, dass die Forschungsarbeiten innerhalb dieses fünften Streams signifikante Fortschritte und Innovationen in der Nutzung von UAV-gestützten mobilen Edge-Computing-Systemen aufzeigen. Die Publikationen decken ein breites Spektrum von Optimierungsstrategien und Anwendungsfällen ab, von der Auslagerung von Berechnungen und Flugbahnoptimierung bis hin zur Verbesserung der Sicherheitsleistung. Darüber hinaus wird die Bedeutung der effektiven Ressourcenallokation und des effizienten Energiemanagements in diesem Kontext betont. Dieser Forschungsstrang stellt somit einen wichtigen Beitrag zur Entwicklung und Verbesserung von UAV-gestützten mobilen Edge-Computing-Systemen dar, jedoch ohne expliziten Bezug zur Anwendung von Blockchain-Technology zu nehmen.

Forschungsstrom VI: Blockchain-gestützter Datenaustausch im Internet of Drones

Insgesamt lassen sich 15 Publikationen dem Forschungsstrom VI zuordnen, was 5% der Publikationen im Datensatz entspricht. Die Publikationen in diesem Bereich zeigen thematische Kohärenz in ihrer Untersuchung der potenziellen Anwendungsmöglichkeiten der Blockchain-Technologie innerhalb des IoD. Insbesondere befassen sich die wissenschaftlichen Publikationen mit der Nutzung der Blockchain-Technologie, um sichere Datenübertragungen zu ermöglichen, automatisierte Prozesse durch Smart Contracts auszuführen und die Identität von Drohnen innerhalb von Drohnennetzwerken zu verifizieren. Dies soll dazu beitragen, wesentliche Sicherheits- und Datenschutzbedenken zu adressieren. Vor diesem Hintergrund kann Forschungszweig VI als "Blockchain-gestützter Datenaustausch im Internet of Drones (IoD)" bezeichnet werden.

Basierend auf der statistischen Auswertung kann die Arbeit von Yazdinejad et al. (2021) als die Publikation mit der besten thematischen Kohärenz innerhalb des betrachteten Forschungsstrangs bezeichnet werden. Diese Studie stellt einen Ansatz für die Schaffung eines sicheren und effizienten Drohnennetzwerks in Smart Cities vor. Das evaluierte System nutzt eine zonenbasierte Netzwerkarchitektur und integriert Blockchain-Technologie. Das Systemdesign stützt sich auf einen dezentralisierten Konsensmechanismus, den sogenannten "Drone-based

Delegated Proof of Stake". Dieser Konsensmechanismus ist Teil eines Authentifizierungsprozess, der keine erneute Authentifizierung beim Wechsel der Flugzone erfordert.

In weiteren Fachpublikationen wird künstliche Intelligenz in Verbindung mit der Blockchain-Technologie verwendet. Khan et al. (2021) schlagen ein auf Blockchain-basierendes dezentrales maschinelle Lernsystem vor, um die Sicherheit in IoD-Umgebungen zu erhöhen, indem sie betrügerisches Verhalten von Netzwerkteilnehmern durch prädiktive Analytik erkennen. Weiterhin stellt Singh et al. (2020) ein Framework vor, welches neurale Netze, das sogenannte „Boltzmann Machine“ und Blockchain-Technologie verwendet, um sichere Datenübertragung und Informationsaustausch in cyber-physischen Systemen, insbesondere in IoD-Umgebungen, zu ermöglichen.

Zusammenfassend lässt sich feststellen, dass die gegenwärtige Forschungsrichtung darauf hinweist, dass die Integration der Blockchain-Technologie in Drohnennetzwerke bedeutende Potenziale zur Verbesserung der Sicherheits- und Datenschutzparadigmen aufweist. Die Anwendung von Blockchain ermöglicht nicht nur eine sichere Datenübertragung, sondern auch die automatisierte Ausführung von Prozessen und die Verifizierung der Drohnenidentität. Infolgedessen stellen die vorliegenden wissenschaftlichen Fachpublikationen einen signifikanten Beitrag zur Weiterentwicklung von sicheren und effizienten Drohnennetzwerken dar.

Framework zur Blockchain-Anwendung im IoD

Der nachfolgende Abschnitt liefert einen Überblick über das konzeptuelle Rahmenwerk (Framework), welches den Forschungsbereich der Blockchain- und Drohnentechnologien im Kontext von AVIK skizziert. Es ist wichtig zu beachten, dass dieses Framework einen generellen Überblick ohne hohen Detailgrad bietet und als Orientierungshilfe im Kontext der genannten Thematik dient. Das Framework unterteilt sich in sechs Ebenen und zielt darauf ab, basierend auf der vorangegangenen explorativen Faktorenanalyse und identifizierten Forschungszweigen, einen ganzheitlichen Überblick der möglichen Integration von Blockchain-Technologie im IoD auf Basis des vorliegenden Forschungsgegenstandes zu skizzieren.

Die erste Ebene des Frameworks stellt einen direkten Bezug zur Anwendung von UAVs her und integriert die übergeordneten Schritte und Maßnahmen, die zum Betrieb eines UAV-Netzwerks oder einer Flugzone erforderlich sind. Aufgrund der Auswertung relevanter Literatur wurden vielfältige Anwendungsmöglichkeiten der Blockchain-Technologie identifiziert, darunter beispielsweise die sichere Authentifizierung von Netzwerkakteuren in UAV-

Netzwerken, sichere Kommunikation und Datenübertragung von Drohne zu Drohne und von Drohne zu Bodenstation. Zudem umfassen die Anwendungsfelder der Blockchain-Technologie auf dieser Ebene die Planung und Durchsetzung von Flugpfaden, das Energiemanagement sowie das Schwarmmonitoring und die Koordination von UAVs.

Die zweite Ebene des konzeptualisierten Frameworks adressiert die Anwendungen des Fernerkundungsverfahrens, auch bekannt als Remote Sensing. Hierbei kann angeführt werden, dass unbemannte Luftfahrzeuge, ausgestattet mit einer breiten Palette von Sensoren, darunter bildgebende Sensoren, aktive Fernsensoren, thermische Sensoren und Gassensoren, ein erhebliches Volumen von Datenpunkten generieren können. Diese gesammelten Daten sind von erheblichem Wert für drei Hauptanwendungsbereiche. Erstens können sie zur Optimierung der Operationen und Netzwerke der UAVs selbst beitragen. Zweitens stellen diese Daten eine potenzielle Ressource für Drittparteien dar, die auf spezialisierte Daten angewiesen sind. Drittens können die erfassten Daten kommerziell auf einem speziell dafür vorgesehenen Drohnendatenmarkt verwertet werden. Im Kontext dieser vielschichtigen Nutzungspotenziale ist die Rolle von UAVs in der Datenerfassung und -analyse von entscheidender Bedeutung.

Die dritte Ebene bezieht sich auf die Datenspeicherung. Hier kann die Blockchain-Technologie aufgrund ihrer inhärenten Eigenschaften erheblich zur sicheren und manipulationssicheren Datenverarbeitung und -speicherung beitragen. Die Blockchain-Technologie bietet verschiedene Vorteile in der Datensicherheit, wie die Unveränderlichkeit der Daten oder die Sicherstellung der Daten-Integrität durch kryptographische Hash-Funktionen. Es ist allerdings zu unterstreichen, dass die Blockchain-Technologie lediglich eine unter mehreren existierenden Lösungen für die Datenspeicherung und -verarbeitung darstellt. Alternativ können etwa auch Cloud-Dienste oder Mobile Edge-Server in Betracht gezogen werden. Die Implementierung einer Blockchain-Lösung geht mit der Berücksichtigung einer Vielzahl von möglichen Ausprägungen bezüglich ökonomischer Anreizsysteme, Governance und Maintenance sowie des Zugriffs auf Daten (öffentlich versus privat) sowie der Möglichkeit der Partizipation and Validierungsvorgängen (permissioned versus permissionless) einher. Kapitel 2 widmet sich einer detaillierten Untersuchung dieser Aspekte sowie der Vorzüge einer auf Blockchain basierenden Lösung. Eine hervorzuhebende Eigenschaft, die durch ein auf Blockchain basierendes System realisiert werden könnte, besteht in der strukturierten und standardisierten Erfassung von Metadaten im Zusammenhang mit von UAV erhobenen Daten und Informationen. Mittels einer detaillierten Dokumentation, die Aufschluss über die Zeitpunkte und verantwortlichen Instanzen der Datenerhebung gibt, könnte ein nachvollziehbarer Pfad zur Herkunft und Verarbeitung der Daten

entstehen. Dieser Pfad würde über die nachfolgenden Prozesse der Datenverarbeitung und -vermarktung hinwegreichen und die zugehörigen Verantwortlichkeiten bezüglich der erfassten Daten transparent abbilden. Die vierte Ebene unseres konzeptualisierten Frameworks ist eng mit der dritten Ebene der Datenspeicherung verknüpft und konzentriert sich auf die weiterführende Verarbeitung der erfassten Daten durch Technologien wie KI, maschinelles Lernen und föderiertes Lernen. Durch den Einsatz dieser Technologien werden die gesammelten Daten verarbeitet und analysiert, um aussagekräftige Informationen zu extrahieren und Muster zu identifizieren. In diesem Kontext kann maschinelles Lernen zum Beispiel genutzt werden, um aus den gesammelten Daten Muster und Zusammenhänge zu ermitteln, die wiederum in der Optimierung des Drohnenbetriebs und der Netzwerkverwaltung Anwendung finden können. Künstliche Intelligenz kann zur Identifizierung und Vorhersage von betrügerischem Verhalten oder potenziellen Sicherheitsbedrohungen eingesetzt werden, was zur Stärkung der Integrität und Sicherheit des gesamten UAV-Netzwerks beitragen kann. Angesichts der wachsenden gesellschaftlichen Relevanz des Internet der Dinge (IoD) sowie der Vielzahl von Anbietern, UAVs und Anwendungsfeldern gewinnt das föderierte Lernen in diesem Kontext besondere Bedeutung. Dies resultiert aus seiner Fähigkeit, Modelle auf Grundlage disparater Datensätze zu erstellen, die nicht zentral verwaltet werden und nicht zentral zugänglich sind.

Eine Vielzahl an Datenerhebungen durch UAVs haben einen kommerziellen Hintergrund. Die fünfte Ebene des Frameworks umfasst entsprechend den wichtigen Aspekt der wirtschaftlichen Verwertung von erhobenen und (weiter)verarbeiteten Daten. Im Rahmen des Handels mit Daten und Datenprodukten kann die Blockchain-Technologie eine technische Infrastruktur für die Abwicklung solcher Transaktionen darstellen, insbesondere in den Bereichen der Kompensation, Reputationssysteme, Bereitstellung einer Funktionalität zur Nachverfolgung der Datenherkunft sowie Automation des Handels. In Anlehnung an das Konzept von sogenannten „Decentralized Exchanges“ (dt. dezentrale Börsen), kann eine marktplatzorientierte Infrastruktur technologisch derart gestaltet sein, dass die gehandelten digitalen Objekte, etwa Kompensationsmittel in Form von kryptografischen Euro-Derivaten, sowie Session-Token zur Erlangung von Zugangsberechtigungen zu extern gespeicherten Daten, nicht notwendigerweise auf ein individuelles "Börsenaccount" des Nutzers übertragen werden müssen. Ein solcher Ansatz impliziert eine Minimierung von Abhängigkeiten und inhärenten Risiken, die ansonsten für die involvierten Nutzer von zentralen Marktplatzlösungen entstehen können.

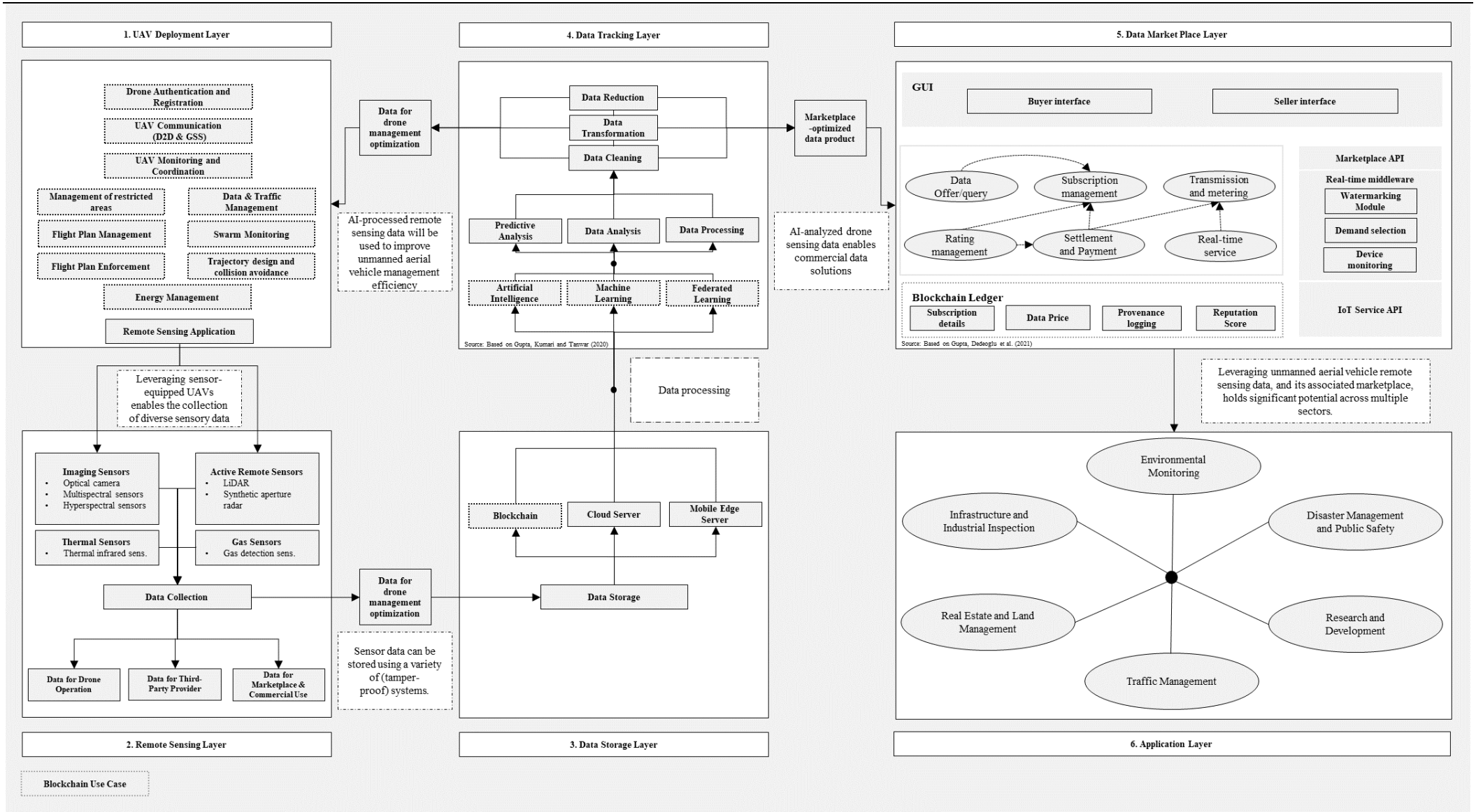

Abbildung 4: Framework zur Blockchain-Anwendung im IoD
Quelle: Eigene Darstellung (P. Gupta et al., 2021; R. Gupta et al., 2021)

Die sechste Ebene beschreibt die Anwendungsfelder, die mittels der Drohnendaten und einem entsprechenden Drohnendatenmarkt profitieren könnten. Die Nennung der Anwendungen und Intention der Darstellung besteht darin, das Potenzial und die Vielfalt der Drohnendaten im Kontext verschiedener industrieller und kommerzieller Anwendungen hervorzuheben. Applikationen auf Basis von Drohnendaten sind nach aktuellem Kenntnisstand kommerziell begrenzt verbreitet.

Zusammenfassung: Mehrwerte der Blockchain-Technologie in UAV-Systemen

Komplementär zu den in den vorangegangenen Unterkapiteln beleuchteten Analyseergebnissen listet Tabelle 1 unterschiedliche Anwendungsfelder für die Technologie auf und beschreibt ihre Rolle im Rahmen der jeweiligen Anwendung.

Anwendung	Rolle der Blockchain
I. Automatisierung von UAV-Systemen	- Automatisierung von Datenspeicherung und -überprüfung - Automatisierung von Transaktionen - Automatisierte Entscheidungsfindung
II. UAV-Dienstleistungen	- Schaffung neuer Geschäftsmodelle - Kollisionsfreie Bewegung von UAVs - Einheitliche Lastverteilung - Daten- und Entitätsauthentifizierung - Zusammenarbeit und schnelle Synchronisierung
III. Dezentrale Speicherung in UAV-Netzwerken	- Ermöglichung von Transaktionen zum gegenseitigen Nutzen zwischen heterogenen IoT-Agenten - Erhöhung der Sicherheit von Flugdaten - Bewältigung der Problematik begrenzter On-Board Speicher- und Verarbeitungskapazitäten von UAVs
IV. Sicherheit in UAV-Netzwerken	- Minderung der Beeinträchtigung von UAV-Signalen - Erkennung von UAV-Entführungen, manipulierten Daten und Sicherstellung der Datenintegrität - Verhinderung von Luftkollisionen - Sicherung der Kommunikation - Schutz von UAV-Daten - Gewährleistung der Datenverteilung
V. UAV-Überwachungsanwendungen	- Aufrechterhaltung des Vertrauens in Alarmmeldesysteme - Absicherung von Überwachungsdaten - Minimierung der Systemvulnerabilität hinsichtlich Cyberattacken und physischen Barrieren - Dynamische Visualisierung weitläufiger Regionen - Implementierung eines effizienten und sicheren Datenübertragungsprotokolls
VI. UAV-Netzwerke für Edge Computing	- Erhöhung der Zuverlässigkeit mobiler Edge-Computing-Netzwerke bezüglich Konnektivität, Verfügbarkeit und Resilienz

Tabelle 1: Einsatzgebiete der Blockchain-Technologie in unbemannten Luftfahrzeugen
Quelle: In Anlehnung an Alladi et al. (2020)

2 Identifikation und Beschreibung relevanter Anwendungen in AVIK

Warum Blockchain-Technologie?

Die Blockchain-Technologie, ursprünglich als Infrastruktur für die Kryptowährung Bitcoin konzipiert, ist mittlerweile weit über diese Anwendung im Finanzwesen hinaus in den Fokus der wissenschaftlichen Gemeinschaft und des gesellschaftlichen Diskurses gerückt. Besonders die strukturellen Chancen (siehe Abbildung 5) und das disruptive Potenzial, etablierte Prozesse und Systeme in Bereichen wie Finanzen, Lieferkettenmanagement und öffentlichen Dienstleistungen tiefgreifend zu verändern, sowie die Erforschung von Synergien und Schnittstellen aufstrebender Technologien wie Blockchain-Nutzung im Kontext von IoT, sind von erheblichem Interesse. Vor diesem Hintergrund skizziert das folgende Unterkapitel anhand der von Alladi et al. (2020) vorgestellten sechs Ebenen (Layer) die Vorteile der Nutzung der Blockchain-Technologie. Abbildung 6 illustriert die von Alladi (2020) skizzierte generische Blockchain-Architektur.

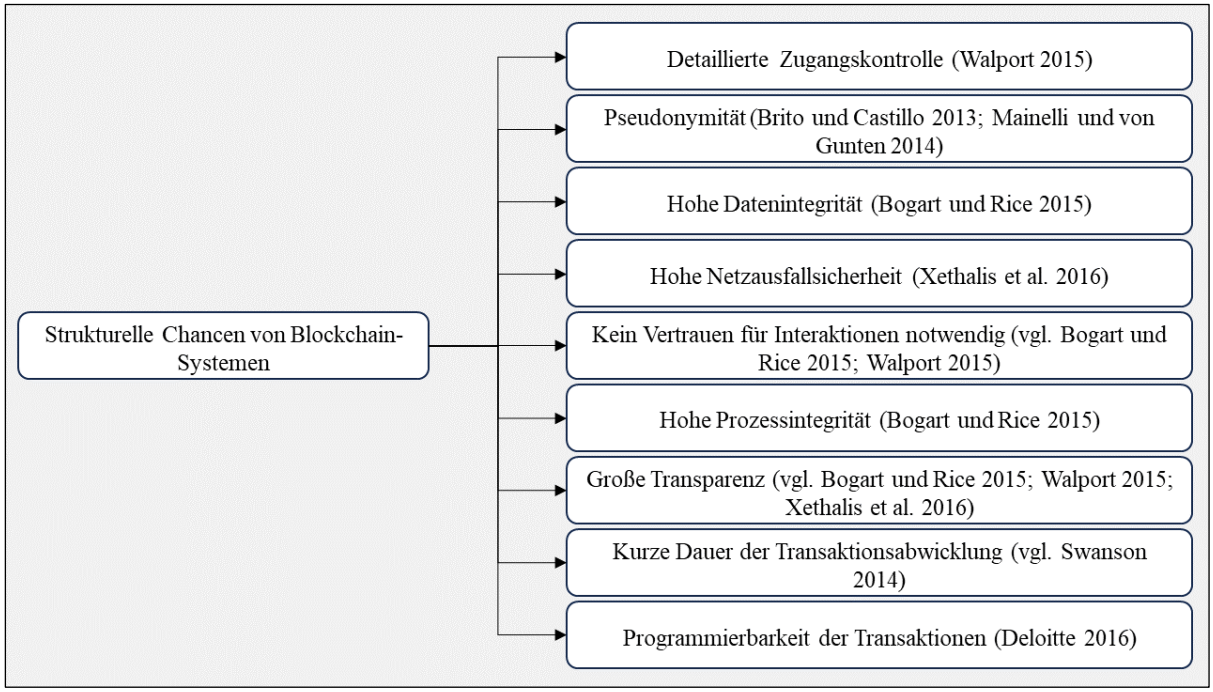

Abbildung 5: Strukturelle Chancen von Blockchain-Systeme
Quelle: In Anlehnung an Schlatt et al., 2016

Die fundamentale Struktur einer Blockchain ergibt sich aus der Datenebene, dem sogenannten Data Layer. Diese gewährleistet eine chronologische Anordnung von Transaktionen, die in Blöcken zusammengefasst und durch kryptographische Verfahren untereinander verknüpft sind. Die aus dieser Struktur resultierende Datenintegrität und die Unveränderlichkeit einmal in die Blockchain eingefügter Daten sind von zentraler Bedeutung für Erreichung der optimierten Datensicherheit als auch der Nachvollziehbarkeit. Dies steht im Gegensatz zu traditionellen,

zentralisierten Datenbanksystemen, in denen nachträgliche Veränderungen oder Löschungen von Daten grundsätzlich möglich sind.

Der Netzwerk-Layer (Network Layer) stellt das Bindeglied zwischen den Teilnehmern des Netzwerkes dar und orchestriert die entsprechenden Interaktion im sogenannten Peer-to-Peer Netzwerk. Die dezentrale Architektur des verteilten Netzwerkes erhöht die Robustheit des Systems, da die Kontrolle nicht bei einer zentralen Instanz liegt, sondern auf verschiedene, unabhängige Knoten verteilt ist. Dies wiederrum mindert das Risiko systemweiter Ausfälle aufgrund zentraler Fehlerquellen und damit das sogenannte "Single Point of Failure-Risiko"(Agrawal et al. 2018; Atlam et al. 2018).

Ein weiterer integraler Bestandteil innerhalb von Blockchain-Netzwerken ist der "Consensus Layer". Dieser regelt, welche Version der Blockchain von den Netzwerkmitgliedern als "valide" anerkannt wird. Dafür werden Konsensmechanismen wie "Proof-of-Work" oder "Proof-of-Stake" angewendet, welche eine Übereinstimmung der beteiligten Knoten über den aktuellen Stand der Blockchain sicherstellen.

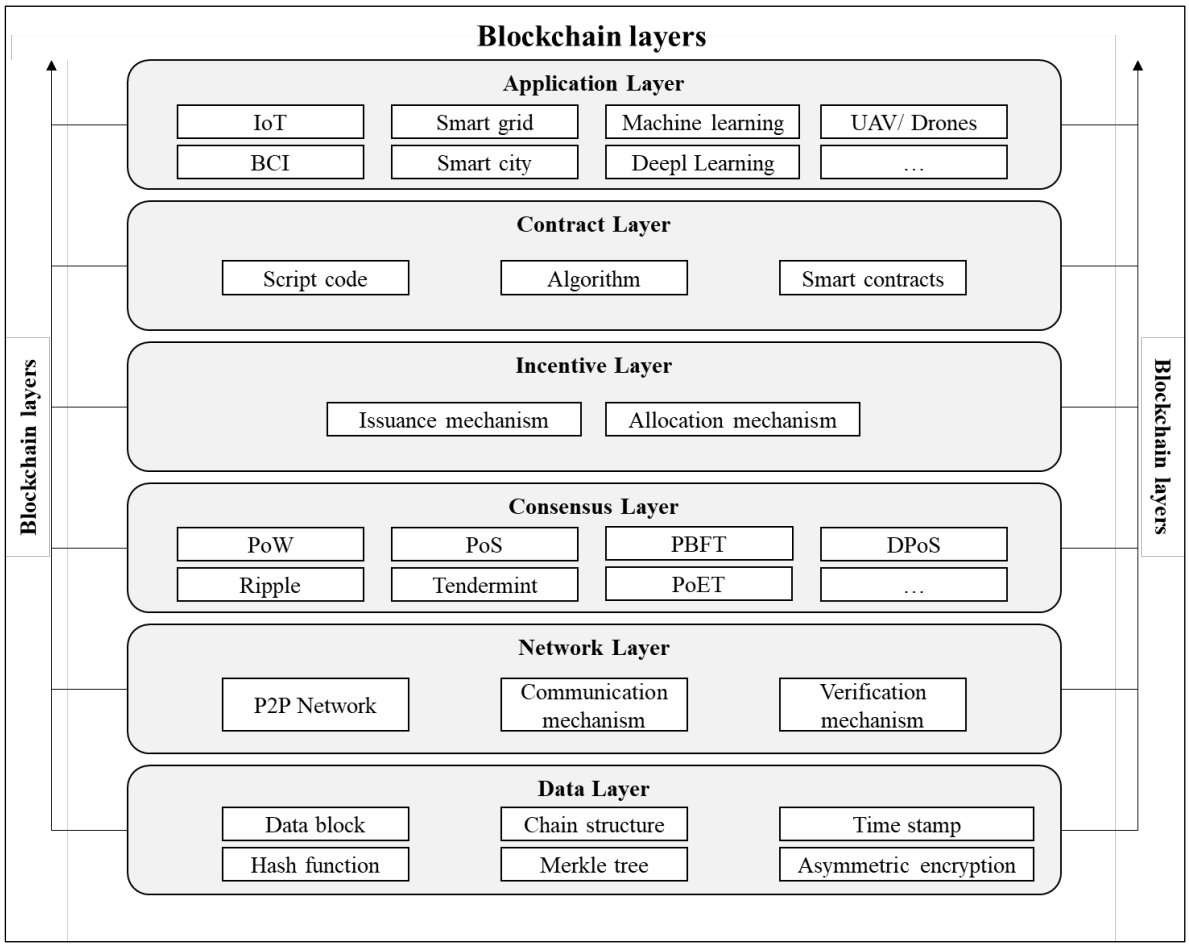

Abbildung 6: Sechs-Schichten-Modell der Blockchain-Architektur
Quelle: In Anlehnung an Alladi et al. (2020)

Hierdurch wird eine hohe Prozessintegrität erreicht, die für das Funktionieren dezentraler Netzwerke unerlässlich ist. Die wohl wichtigste Innovation von Bitcoin ist der sogenannte "Nakamoto Consensus" oder auch "Proof-of-Work Consensus". Dieser Mechanismus ermöglicht es den Teilnehmern im Netzwerk, kontinuierlich einen "aktuellen" Stand der Blockchain zu erreichen, ist robust gegenüber verschiedenen Angriffsvektoren und ermöglicht die quasi-deterministische Validierung von Netzwerktransaktionen (Gervais et al. 2016).

Die Anreizebene (Incentive Layer) stellt ein zentrales Element zur Aufrechterhaltung der Blockchain-Infrastruktur dar. Sie umfasst die Kompensation der Netzwerkakteure zur Durchführung bestimmter standardisierter Aufgaben und schafft die Motivation für aktive Netzwerkpartizipation. Im Fall des Bitcoin-Netzwerks werden sogenannten „Minern“ Bitcoin als Belohnung für die Validierung von Transaktionen und das Hinzufügen neuer Blöcke mit neuen Transaktionen gesendet. Anreizsysteme unterscheiden sich auf vielen öffentlichen Blockchain-Netzwerken teils erheblich, und umfassen auch Parameter wie die Inflation oder Deflation der Netzwerk-spezifischen Assets. In privaten Netzwerken kann auch auf Anreizschemata auf infrastruktureller Ebene verzichtet werden, wenn andere Finanzierungswege für die Aufrechterhaltung des Netzwerks erschlossen wurden. So kann ein Konsortial-Netzwerk auch genossenschaftlich organisiert sein, und die Validierung und Maintenance kostendeckend über Beiträge der Nutzer finanziert werden.

Der Vertrags-Layer (Contract Layer) in der Blockchain ermöglicht die Integration von sogenannten "Smart Contracts". Diese selbstausführenden Verträge, die auf programmatischen Regeln basieren, lösen bei Erfüllung bestimmter Bedingungen vordefinierte Aktionen aus. Die Nutzung von Smart Contracts ermöglicht damit eine weitreichende Automatisierung von Prozessen, die von finanziellen Transaktionen bis hin zur Verwaltung und Steuerung dezentralisierter autonomer Organisationen (DAOs) reichen. Diese Automatisierung minimiert nicht nur die Notwendigkeit manueller Eingriffe und die damit verbundenen Fehlermöglichkeiten, sondern birgt ebenfalls das Potenzial die Effizienz und Geschwindigkeit von Transaktionen und Prozessen erheblich zu steigern. Eine dezentrale Börse ist beispielsweise ein Konstrukt aus mehreren Smart Contracts, die es im Resultat ermöglichen, einen Handel durch den programmatischen und automatisierten Austausch auf Basis einer Einigung vorzunehmen, ohne dass ein Mittelsmann als Custody eingesetzt werden muss. Dies spart je nach Umsetzung und Gebührenstruktur Kosten in der Nutzung und reduziert Abhängigkeiten für die Nutzer.

Abschließend fungiert die Anwendungsebene (Application Layer) als Prisma, durch welches sich die vielfältigen Einsatzmöglichkeiten der Blockchain-Technologie in verschiedenen

Bereichen veranschaulichen lassen. So reichen die Einsatzbereiche von Anwendungen im Kontext urbaner Informationsinfrastrukturen - bekannt als Smart Cities - und des Internet of Things, bis hin zu Integrationen im Feld des maschinellen Lernens und der unbenannten Luftfahrzeugsysteme. Innerhalb der als Beispiele genannten Anwendungsdomänen besitzt die Blockchain-Technologie durch ihre einzigartigen Eigenschaften großes Potenzial bei der Optimierung und effizienten Nutzung der jeweiligen digitalen Infrastrukturen. Ihre Kernmerkmale - Dezentralität, Sicherheit, Transparenz und Unveränderlichkeit - ermöglichen dabei neuartige Ansätze zur Gestaltung und Verwaltung digitaler Prozesse und können substanziellen Mehrwert generieren.

Zusammenfassend lässt sich konstatieren, dass die Blockchain-Technologie ein vielversprechendes Werkzeug zur Verbesserung der Datensicherheit, Transparenz und Effizienz digitaler Infrastrukturen darstellt. Ihre Anwendungsmöglichkeiten reichen weit über die ursprüngliche Intention einer digitalen Währung hinaus und bieten ein breites Spektrum an Nutzungsmöglichkeiten. Gleichzeitig erfordert ihre Implementierung eine sorgfältige Abwägung der technischen Ausgestaltung, beispielsweise in Bezug auf Transparenz, vertrauensbildende Kontrollmöglichkeiten und Partizipation von Nutzern in der System-Governance. In den nachfolgenden Unterkapiteln wird dabei die Anwendungsmöglichkeiten und technischen Herausforderungen der Blockchain-Technologie im Kontext von AVIK skizziert und spezifiziert.

Private und öffentliche Blockchain-Netzwerke im Kontext von AVIK

Zu differenzieren sind etwaige Anwendungen anhand der Nutzung existierender öffentlicher Netzwerke und dedizierter privater Netzwerke. Die Auswahl eines geeigneten Netzwerktyps ergibt sich aus der Anwendung, dem Grad der angestrebten Dezentralisierung und daraus, welche Eigenschaften der Blockhain-Technologie für die avisierte Anwendung wichtig sind.

Öffentliche Netzwerke

Eine Vielzahl bestehender Blockchain-Netzwerke, bieten die Möglichkeit, dezentrale Applikationen zu entwickeln. Anwendungen auf Ethereum werden durch Transaktionen ausgelöst; jede Interaktion mit einem Smart contract ist in der Blockchain nachvollziehbar. Dieses Level an Transparenz ist für einige Anwendungen problematisch, da trotz Pseudo-anonymität und kryptografischen Verschlüsselungen, theoretisch Transaktionsmuster identifiziert und Verbindungen von Adressen und Organisationen geknüpft werden können. Im Gegensatz zu privaten Netzwerken, bieten sich auch einige Vorteile: Das Thema Governance und Maintenance ist auf infrastruktureller Ebene für die dezentrale Applikation weniger relevant.

Vor- und Nachteile von öffentlichen Blockchain-Netzwerken

Vorteile	Nachteile
Dezentralisierung: Öffentliche Blockchains sind dezentralisiert und bieten Transparenz und Sicherheit durch ein verteiltes Netzwerk von Nodes.	**Skalierbarkeit:** Öffentliche Blockchains stehen aufgrund der beträchtlichen Anzahl an Knotenpunkten und der angewandten Konsensmechanismen häufig vor Herausforderungen im Bereich der Skalierbarkeit. Diese Schwierigkeiten können sich in Form von verlangsamten Transaktionsraten sowie erhöhten Transaktionskosten manifestieren.
Sicherheit: Öffentliche Blockchains verwenden kryptografische Algorithmen und Konsensmechanismen, um die Integrität von Transaktionen und Daten sicherzustellen.	**Mangelnde Privatsphäre:** Öffentliche Blockchains sind nicht von Natur aus privat, und Transaktionsdetails sind oft für jedermann sichtbar, was für bestimmte Anwendungsfälle ein Problem darstellen kann.
Unveränderlichkeit: Sobald eine Transaktion auf einer öffentlichen Blockchain erfasst ist, ist es äußerst schwer, sie zu ändern, was eine manipulationssichere Aufzeichnung von Ereignissen ermöglicht.	**Regulatorische Herausforderungen:** Öffentliche Blockchains können in einigen Rechtsgebieten regulatorische Unsicherheiten hervorrufen, insbesondere aufgrund von Bedenken hinsichtlich Anonymität und illegalen Aktivitäten.
Zensurresistenz: Öffentliche Blockchains ermöglichen Transaktionen und Datenaustausch ohne die Notwendigkeit von Intermediären, wodurch sie eine inhärente Resistenz gegenüber zensierenden Eingriffen aufweisen.	**Energieverbrauch:** Viele öffentliche Blockchains verwenden energieintensive Konsensmechanismen wie den Proof of Work (PoW), was zu Umweltbedenken führen kann.
Netzwerkeffekte: Öffentliche Blockchains profitieren von starken Netzwerkeffekten, da mehr Teilnehmer dem Netzwerk beitreten und so die Sicherheit und Benutzerfreundlichkeit steigen.	**Begrenzte Kontrolle und Einflussnahme:** Teilnehmer haben begrenzte Kontrolle über die Governance und Upgrades des Blockchain-Protokolls, was zu Konflikten und Netzwerkteilungen führen kann.

Tabelle 2: Vor- und Nachteile öffentlicher Blockchain-Netzwerke; Quelle: Eigene Darstellung

Private Netzwerke

In privaten Netzwerken werden grundlegende Parameter auf infrastruktureller Ebene für den entsprechenden Anwendungsfall definiert. Dies impliziert meist einen höheren späteren Nutzen, aber auch höhere initiale Kosten. Das System muss ökonomische Anreizschemata umfassen, und gleichzeitig die für die Nutzer wichtigen Charakteristika aufrechterhalten. So können private Netzwerke nicht das Vertrauensniveau und die Manipulationssicherheit gewährleisten wie öffentliche Netzwerke, wohl aber adäquatere Performance garantieren, z.B. eine höhere Kapazität der Transaktionsabwicklung, und flexibel an sich ändernde Gegebenheiten angepasst und rekonfiguriert werden.

Vor- und Nachteile von privaten Blockchain-Netzwerken

Vorteile	Nachteile
Skalierbarkeit: Private Blockchains können höhere Transaktionsgeschwindigkeiten und geringere Kosten erreichen, da sie eine geringere Anzahl von bekannten und vertrauenswürdigen Teilnehmern umfassen.	**Zentralisierung:** Private Blockchains sind stärker zentralisiert, da sie auf einer begrenzten Anzahl von berechtigten Nodes basieren, was die Prinzipien der Dezentralisierung beeinträchtigen kann.
Privatsphäre: Private Blockchains ermöglichen eine präzisere Überwachung der Privatsphäre, indem Transaktionsdetails ausschließlich für befugte Teilnehmer sichtbar sind. Diese Eigenschaft qualifiziert sie besonders für den Einsatz in vertraulichen Geschäftsprozessen.	**Sicherheitsbedenken:** In Szenarien, in denen eine Mehrheit der Teilnehmer einer privaten Blockchain gemeinschaftliche Ziele verfolgt oder anfällig für Kompromittierungen ist, könnten diese Blockchains verstärkter Gefahr von Angriffen ausgesetzt sein.
Effizienz: Durch eine geringere Anzahl von Knotenpunkten und die Anwendung eines Konsensmechanismus, der auf die individuellen Bedürfnisse der Teilnehmer zugeschnitten ist, können private Blockchains eine gesteigerte Energieeffizienz aufweisen.	**Begrenzte Akzeptanz:** Private Blockchains könnten die Netzwerkeffekte und Vorteile, die öffentliche Blockchains bieten, aufgrund ihrer geschlossenen Natur vermissen lassen.
Anpassbarkeit: Teilnehmer haben mehr Kontrolle über die Regeln, Governance und Konsensmechanismen, was maßgeschneiderte Lösungen ermöglicht.	**Interoperabilitätsprobleme:** Die Interoperabilität zwischen verschiedenen privaten Blockchain-Netzwerken kann komplex sein und zusätzliche Entwicklungsarbeit erfordern.
Compliance: Private Blockchains ermöglichen es Organisationen, die Kontrolle über Daten zu behalten und gleichzeitig branchenspezifische Vorschriften einzuhalten.	**Verringerte Unveränderlichkeit:** Private Blockchains könnten eine größere Flexibilität bei der Änderung von Transaktionen haben, was Bedenken hinsichtlich Nachvollziehbarkeit und Vertrauen hervorrufen könnte.

Tabelle 3: Vor- und Nachteile privater Blockchain-Netzwerk
Quelle: Eigene Darstellung

Zweckdienliche Eigenschaften der Blockchain-Technologie für AVIK

Das Projekt AVIK untersucht die Innovationskapazität der Zusammenführung von unterschiedlichen Datenquellen, im Speziellen von mit Sensortechnik ausgerüsteten UAVs und Bodenfahrzeugen gesammelte Daten, und die Möglichkeiten der Incentivierung kontinuierlicher Datensammlung durch die Kommerzialisierungsperspektive eines Marktplatzes zur Bündelung des Datenangebots und dessen Zusammenführung mit entsprechenden Nachfragern.

Entsprechend stehen für den Anwendungsbereich die folgenden Eigenschaften der Technologie im Vordergrund:

Innovationskapazität der Zusammenführung von unterschiedlichen Datenquellen

Im Kontext der Nutzung von Daten unterschiedlicher Herkunft und Speicherung zur erweiterten Erkenntnisgewinnung, beispielsweise im Kontext des federated learning, kann Blockchain-Technologie als Infrastruktur für die Koordinierung und Dokumentation von Zugriff und Durchführung auf Datensätze eingesetzt werden. Ein bemerkenswerter Vorteil in diesem Zusammenhang besteht darin, dass das System gleichzeitig als Bezahlinfrastruktur fungieren kann. Dies bedeutet, dass die Vergütung für den Zugang auf automatisierte Weise gemäß vordefinierter Parameter erfolgen kann. Zum Beispiel kann ein zeitlich begrenzter Zugang eingerichtet werden. Dies ermöglicht eine kostengünstige Abwicklung der Zahlungsabwicklung und erleichtert die Verwaltung der Kompensationsmechanismen. Auf dieser digitalen Infrastruktur lassen sich weitere relevante Anwendungen aufbauen, etwa Reputationssysteme und -mechanismen, welche eine Beurteilung der Datenqualität oder Vertrauenswürdigkeit der Gegenpartei im Vorfeld eines Handels zulassen. Darüber hinaus besteht die Möglichkeit, verschlüsselte Metadaten von Datenerhebungen mithilfe der implementierten Blockchain-Technologie derart zu erfassen, dass eine selektive Freigabe seitens eines Verkäufers die rückverfolgbare Dokumentation der Datenerfassung ermöglicht. Hierdurch wird es potenziellen Käufern gestattet, die relevanten Details der Datenerhebung nachzuvollziehen, beispielsweise Informationen über das ausführende Unternehmen, das verwendete UAV, den Zeitpunkt sowie den Ort der Erfassung.

Sowohl die Implementierung der Bezahlinfrastruktur als auch die Ermöglichung der Rückverfolgbarkeit von Datenerhebungen stellen vertrauensbildende Maßnahmen dar, die einen dezentral-konzipierten Marktplatz von bestehenden Ansätzen differenzieren würde. Wesentlich ist hierbei, dass sie auf derselben Infrastruktur prinzipiell automatisiert und standardisiert abgewickelt werden können. Diese Infrastruktur dient somit gleichzeitig der Koordination von

Datenzugriffen sowie der Vergütung. Zusammenfassend lassen sich in diesem Kontext folgende Eigenschaften und Möglichkeiten festhalten:

- Die Koordinierung einer Vielzahl von Akteuren, Datenquellen und Handelsaktivitäten über Netzwerkstruktur und standardisierte Dokumentation und Validierung
- Nachvollziehbarkeit von Datenerhebungen und Datenverarbeitung über kryptografisch verknüpfte Blockstruktur
- Tokenisierung intangibler Werte wie Reputations-Scores sowie automatisierte Zuweisung und Entzug von entsprechenden Accounts

Incentivierung kontinuierlicher Datensammlung durch Verwertungsperspektive

Die Verwertungsperspektive für Akteure die Mittels UAVs und Bodenfahrzeugen Daten erheben ist elementar für den Erfolg des Projektes. In diesem Kontext können Daten-erhebende Akteure solche sein, die für eigene Zwecke Daten erheben und diese zusätzlich kommerzialisieren wollen, wie auch solche, die Daten im Auftrag erheben oder in Antizipation eines Bedarfs der Daten. Neben den Kosten der Ausstattung von UAVs mit entsprechender Sensortechnik, etwaige Genehmigungen sowie Betriebs- und Wartungskosten von UAV und Sensoren sind die Kosten der Verwertung ein weiterer wichtiger Kostenfaktor in der Kalkulation eines Datenerhebenden Akteurs. Hier kann die Blockchain-Technologie als technische Infrastruktur für dezentralisierte Abwicklung von Verwertungsaktivitäten, im Speziellen den Handel von Zugriffsrechten gegen Kompensationen, dienen. Dadurch können für die Nutzer geringe Gebühren sowie die Reduktion von Abhängigkeiten realisiert werden.

Die Realisierung geringer Gebühren im Vergleich zu zentralisierten Datenmarktplätzen könnte aufgrund des erheblichen Maßes an Automatisierung erreicht werden. Ebenso könnten alternative Organisationsstrukturen des Marktplatzes, wie beispielsweise genossenschaftliche Ansätze, oder im Wesentlichen kostendeckende Finanzierungssysteme dazu beitragen. Die Reduktion von Abhängigkeiten könnte im Rahmen der technischen Umsetzung des Marktplatzes so gewährleistet werden, dass die Nutzer der Plattform weder Zugriffsrechte (etwa in Form von kryptografischen Token), noch monetäre Bestände (für Zahlungen; in Form kryptografischer Fiat-Derivate) auf die Plattform übertragen müssen, sondern stattdessen Smart Contracts den Transfer entsprechender Assets (bei Autorisierung) vornehmen. Plattform-Risiken für die Nutzer sowie Counterparty-Risiken werden reduziert. In der abschließenden Betrachtung könnte der traditionelle Intermediär, üblicherweise repräsentiert durch profitorientierte Akteure eines zentralisierten Datenmarktplatzes, seine Relevanz verlieren. Die bislang erhobenen Gebühren

könnten durch eine kollektive Aufbringung der Kosten für den Betrieb der Blockchain-Infrastruktur oder der zugehörigen Blockchain-Applikation substituiert werden. Zusammenfassend lassen sich in diesem Kontext folgende Eigenschaften und Möglichkeiten festhalten:

- Automatisierung mittels Smart Contracts zur Dezentralisierung des Marktplatzes
- Smart-contract-gestützte Automatisierung zur Realisierung von Kostenreduktionen
- Durchführung unterschiedlicher Governance-Modelle für den Betrieb und die Weiterentwicklung der Applikation
- Weitere Anreizschemata: Neben der Möglichkeit Handel zu betreiben, könnten Akteure auch in Form von intangiblen Werten (etwa Reputation) oder tangiblen Werten (Profitbeteiligungen; Empfehlungsprogramme) zur kontinuierlichen Sammlung von Daten und Nutzung des Marktplatzes incentiviert werden, die sich ebenfalls auf der selben Blockchain-Infrastruktur umsetzen ließen.

Basierend auf dem gegenwärtigen Stand der Wissenschaft und Forschung, welcher im vorigen Kapitel ausführlich dargelegt wurde, sowie der Identifikation der zweckdienlichen Eigenschaften der Blockchain-technologie im Kontext des Projekts AVIK, lassen sich drei spezifische Anwendungsfälle identifizieren, die im folgenden Kapitel näher beleuchtet werden.

Beschreibung relevanter Use Cases

I. Identifizierungs- und Authentifizierungssystem für UAVs und Fahrzeuge

Ein Identifikations- (ID) und Authentifizierungssystem, welches sowohl für Bodenfahrzeuge als auch für unbemannte Flugobjekte dienlich ist, oder potenziell für jegliche Objekte oder Geräte, die mit Sensorik zur Datenerhebung ausgerüstet sind, fungiert als wesentliches Instrument zur Kontrolle und Koordination. Dieses Instrument ist insbesondere für Autoritäten von Bedeutung, welche die Nutzung spezifischer Lufträume oder Korridore unter festgelegten Bedingungen überwachen. Gleichfalls von Bedeutung sind spezifische Akteure im Marktumfeld, die beispielsweise verpflichtet sind, nachzuweisen, dass sie die erforderliche Genehmigung besitzen, um in einem bestimmten Luftraum operative Aktivitäten durchzuführen oder Daten zu sammeln. Angesichts der prognostizierten signifikanten kommerziellen Zunahme von UAVs und autonomen Bodenfahrzeugen, die vielfältige Aufgaben und Kapazitäten aufweisen, müssen bestimmte Merkmale in einem Identifikations- und Authentifizierungssystem berücksichtigt werden. Diese umfassen technische Skalierbarkeit zur Bewältigung steigender

Teilnehmerzahlen, Robustheit gegenüber verschiedenen Betriebsbedingungen und Manipulationssicherheit, um gegen potenzielle Sicherheitsbedrohungen gerüstet zu sein.

Ein Blockchain- oder DLT-basiertes System kann diese Voraussetzungen theoretisch erfüllen, wie auch eine Vielzahl zentralisierter Ansätze. Die Implementierung einer Blockchain- oder DLT-Infrastruktur für ein Identifikations- und Authentifizierungssystem präsentiert gegenüber zentralisierten Systemen eine Reihe von Vorteilen. Abhängig von der spezifischen architektonischen Gestaltung ermöglicht die Nutzung von Blockchain-Technologie eine manipulationssichere Speicherung relevanter Daten und Informationen. Zudem bietet es eine eindeutige und nachvollziehbare Zurechnung von Verantwortlichkeiten (Accountability), die ausschließlich verifizierten Teilnehmern vorbehalten ist. Zudem kann ein derartiges System als Open-Source-Plattform fungieren und als Grundlage für die Entwicklung neuer, innovativer Anwendungen und Schnittstellen dienen. Während ein zentrales System ein sogenannten Single-Point-of-Failure darstellt, also ein einzelnes, definiertes Ziel für Angriffe zur Informationsextraktion oder Manipulation, ist die Integrität eines dezentrales Systems durch implementierte Konsensalgorithmen und die redundante Speicherung der Transaktionsinformationen geschützt. Hierbei ist zu berücksichtigen, dass die Informationen über Transaktionen innerhalb des Netzwerks entweder öffentlich einsehbar sein können (öffentliches Netzwerk) oder nur für bestimmte Teilnehmer zugänglich sind (privates Netzwerk) – dies kann auch auf vordefinierte Informationen beschränkt sein. Mit Bezug zur Extraktion von Informationen, kann entsprechend auch in einer Blockchain- oder DLT-Lösung ein Single-Point-of-Failure entstehen, wenn die Validatoren des Systems nicht-öffentliche Daten verwalten. Jedoch wird durch Konsensalgorithmen und die redundante Speicherung der Datenbank eine Manipulation signifikant erschwert.

Ein dezentrales System bietet somit im Vergleich zu einem zentralen System eine erhöhte Datensicherheit, eine effizientere Kostenaufteilung sowie die Reduzierung von Abhängigkeiten von Preisgestaltung und Verfügbarkeit einzelner Anbieter solcher Technologien. Allerdings können dezentrale Systeme Nachteile in Bezug auf ihre Performance aufweisen, da zentralisierte Systeme unter Umständen besser skalierbar sind und damit eine effizienteres und höheres Volumen von Anfragen abwickeln können.

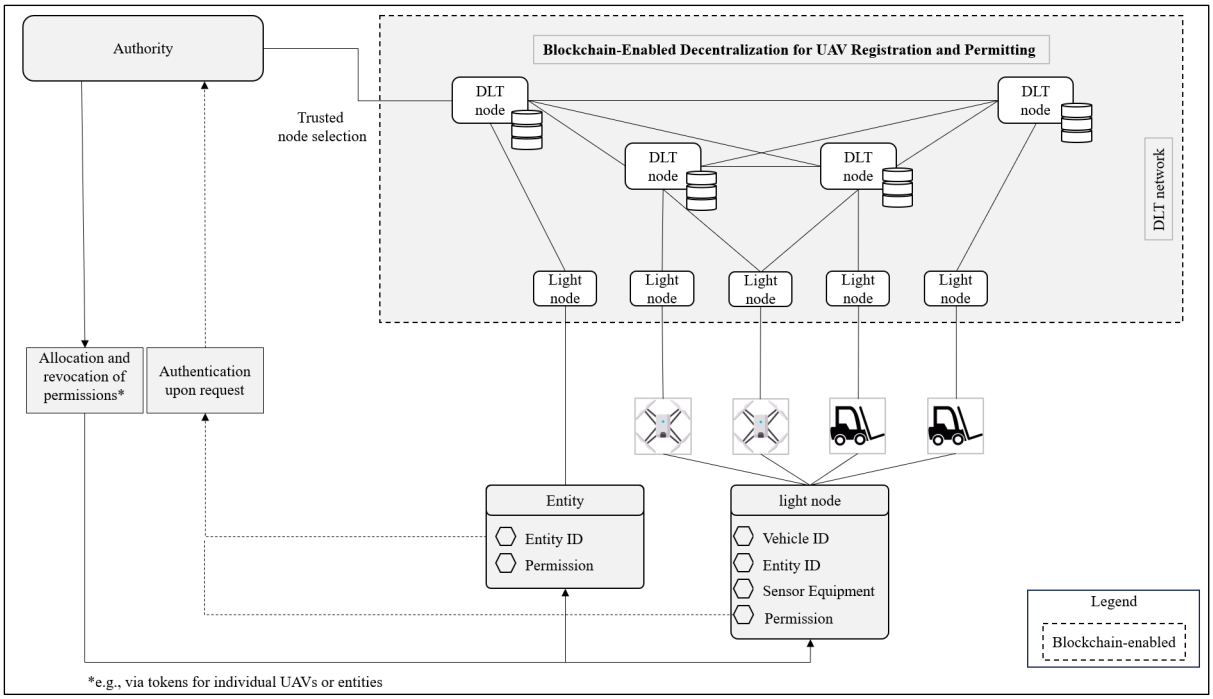

Abbildung 7: Schema zur Visualisierung eines DLT-basierten ID- und Authentifizierungssystems
Quelle: Eigene Darstellung

Abbildung 07 zeigt eine vereinfachte Darstellung eines dezentralen Systems zur Nutzung als ID- und Authentifizierungssystem. Teilnehmer durchlaufen Registrierungs- und Verifikationsprozesse, die von einem autorisierten Dienstleister oder einer Behörde durchgeführt werden, um ihre unbemannten Luftfahrzeuge oder Bodenfahrzeuge in eingeschränktem Luftraum und auf Straßen nutzen zu können. Innerhalb dieses Systems sind Identifikationsnummern entsprechend fahrzeuggebunden und manifestieren somit eine direkte Zuordnung zu spezifischen mobilen Entitäten. Des Weiteren existiert eine übergeordnete Kategorie von Identifikationsnummern, die an bestimmte Anbieter gebunden sind. Diese ermöglichen eine klare Zuweisung von Verantwortlichkeiten innerhalb des Ökosystems und tragen so zu einer effizienten Verwaltung und Kontrolle bei. Basierend auf diesen ID-Ebenen können Authentifizierungen zur Nutzung spezifischer Wege und Korridore implementiert werden, wodurch die vorübergehende und gezielte Gewährung von Berechtigungen ermöglicht wird. Anforderungen für die Erlangung einer Berechtigung, wie beispielsweise eine nachweisbare Wartungshistorie, können dabei berücksichtigt werden. Eine Vielzahl weiterer Prozesse kann mithilfe der Distributed-Ledger-Technologie automatisiert werden. Dazu gehören die Kontrolle von Berechtigungen, die (temporäre) Sperrung von öffentlichen Räumen oder spezifischen Fahrzeugen sowie Transaktionen auf Primär- und Sekundärmärkten.

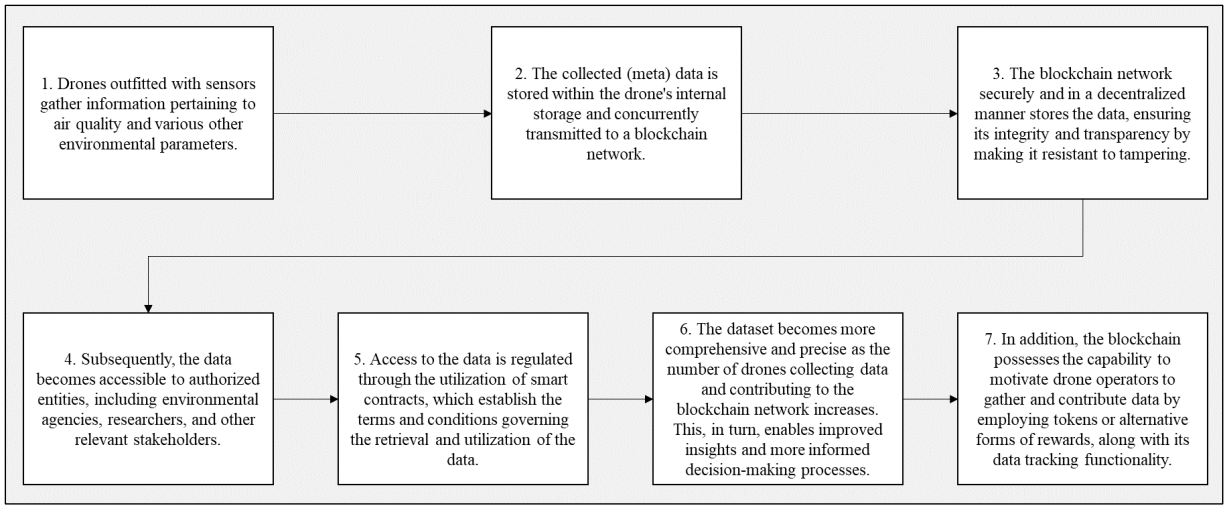

Abbildung 8:Schematische Darstellung des Ablaufs einer ID-Zuordnung und Authentifizierung
Quelle: Eigene Darstellung

Die in der Blockchain abgelegten Daten repräsentieren Transaktionsinformationen, die zwischen verschiedenen Teilnehmern des Systems ausgetauscht werden. Dies beinhaltet die Übertragung von ID-Token und anderen Verifikationsprozessen und der Bestätigung bestimmter Merkmale von Autoritäten oder Dienstleistern (Wartung) an eine ID bzw. deren „Wallet“. Es ist ebenso möglich, bestimmten IDs, Nutzern oder übergeordneten Nutzern temporär eine Berechtigung in Form von standardisierten Tokens auf Blockchain-Basis zuzuweisen oder diese Berechtigungen zu widerrufen bzw. zu revidieren. Abhängig von der Gestaltung der Kontrollmechanismen eröffnen sich unterschiedliche Wege der Authentifizierung von Luft- und Bodenfahrzeugen. Dies kann beispielswiese stichprobenartig oder beim Eintreten in einen spezifizierten Kontrollkorridor geschehen. Mithilfe grundlegender technischer Verfahren ist es möglich, die mit den Fahrzeugen verbundenen digitalen Wallets auszulesen. Zusätzliche Transaktionsdaten könnten beispielsweise die zurückgelegten Routen oder das Betreten spezifischer Luftraumkorridore umfassen, wodurch eine geographische Nachverfolgung ermöglicht werden kann. Die schematische Darstellung des Ablaufs des Authentifizierungsprozesses wird in Abbildung 08 illustriert. Die Implementierung eines ID-Systems bildet eine Grundvoraussetzung für die Realisierung der im folgenden betrachteten Anwendungsfälle.

II. Protokollierung von Metadaten zu Datenerhebungen

Ein weiterer signifikanter Anwendungsbereich der Blockchain-Technologie besteht in der Protokollierung von Metadaten im Rahmen der Datenerhebung durch Boden- und Luftfahrzeuge. Diese Vorgehensweise dient der Schaffung der Nachvollziehbarkeit bei der Datenerhebung, wodurch ein (potenzieller) Käufer eines Datensatzes oder Datenprodukts die Möglichkeit

erhält, die Authentizität der Daten zu verifizieren. In diesem Kontext impliziert die Verifikation der "Echtheit" die Nachvollziehbarkeit, welches Fahrzeug (inklusive der entsprechenden Sensorausstattung) zu welchem Zeitpunkt und an welchem Ort (und mit oder ohne Erlaubnis) die Roh- oder Ursprungsdaten erhoben hat. Die manipulationssichere Dokumentation solcher Metadaten durch permanente und redundante Speicherung würde die Verbreitung gefälschter Daten erschweren und die Wahrscheinlichkeit der Entdeckung erhöhen. Dies kann zu einem höheren Vertrauensniveau bezüglich der Integrität der angebotenen Daten führen, was wiederum einen Wettbewerbsvorteil für den angestrebten Marktplatz darstellen kann. Die Nachfrage seitens potenzieller Käufer nach einem solch aufwändigen Vertrauensniveau gilt es zu verifizieren. Abbildung 09 veranschaulicht ein Blockchain-basiertes System zur Protokollierung von Metadaten. Kern dieses Prozesses ist die Kennzeichnung der erhobenen Daten mit einem "Wasserzeichen". Im vorliegenden Fall wären dies ein Zeitstempel, eine Geo-Markierung oder ein simpler Hash des Datensatzes oder einer Kombination unterschiedlicher Informationen, welche mit der ID des Fahrzeugs verknüpft sind. Diese kombinierten oder individuellen Metadaten über die Erhebung werden in verschlüsselter Form über eine Transaktion in der Blockchain gespeichert und können über vordefinierte Prüfmechanismen abgerufen werden. Dabei könnten aufgezeichnete Bewegungsdaten des Fahrzeugs für erste Validierungsprozesse herangezogen werden. Letztlich sollte ein Käufer eines Datenprodukts (z.B. Luftgüte-Stadtkarte Stuttgart, 20-06-2023) in der Lage sein, die Übereinstimmung der in der Blockchain gespeicherten Daten mit den angegebenen zu überprüfen. Idealerweise sollte dieser Prozess nicht vom Käufer initiiert werden müssen, sondern automatisch im Hintergrund ablaufen und in einer entsprechenden Anzeige auf der Benutzeroberfläche des Marktplatzes sichtbar sein. Durch eine solche Kennzeichnung könnte eine klare Unterscheidung zwischen nicht-verifizierten und verifizierten Datensätzen auf dem Marktplatz hergestellt werden. Innerhalb des Datenmarktplatzes kann dieser Differenzierungsfaktor dem Käufer als Qualitätsmerkmal für den Markplatz und die erworbenen Daten dienen. Die Entscheidung, sowohl verifizierte als auch nicht-verifizierte Datenprodukte anzubieten, obliegt dem Betreiber des Marktplatzes.

Entsprechend der Vielseitigkeit unterschiedlicher Daten und Services, die auf einem solchen Datenmarktplatz angeboten werden können, ergibt sich eine beträchtliche Komplexität für den Anwendungsfall. Betrachten wir exemplarisch den Szenariobereich eines Käufers, der eine Luftqualitätskarte einer Stadt erwirbt: Hier könnte nicht nur der aktuelle Tag von Interesse sein, sondern auch eine Zeitreihe über mehrere Wochen oder Monate. Im Kontrast dazu ist für den Erwerb von Echtzeitdaten zum Binnenschifffahrtsverkehr, welche durch Drohnen erfasst

wurden, die zeitnahe Verfügbarkeit von Relevanz. Innerhalb verschiedener Käufergruppierungen manifestieren sich divergente Bedürfnisse, wobei manche eine Präferenz für Rohdaten hegen, während andere bereits aufbereitete Daten oder spezifische Berichtsformate bevorzugen. Im Kontext möglicher Datenverarbeitungen, in dem Änderungen an Rohdaten vorgenommen werden, ist es von zentraler Bedeutung, dass der Ursprung der Daten und deren Erhebungsprozess nachvollziehbar bleiben.

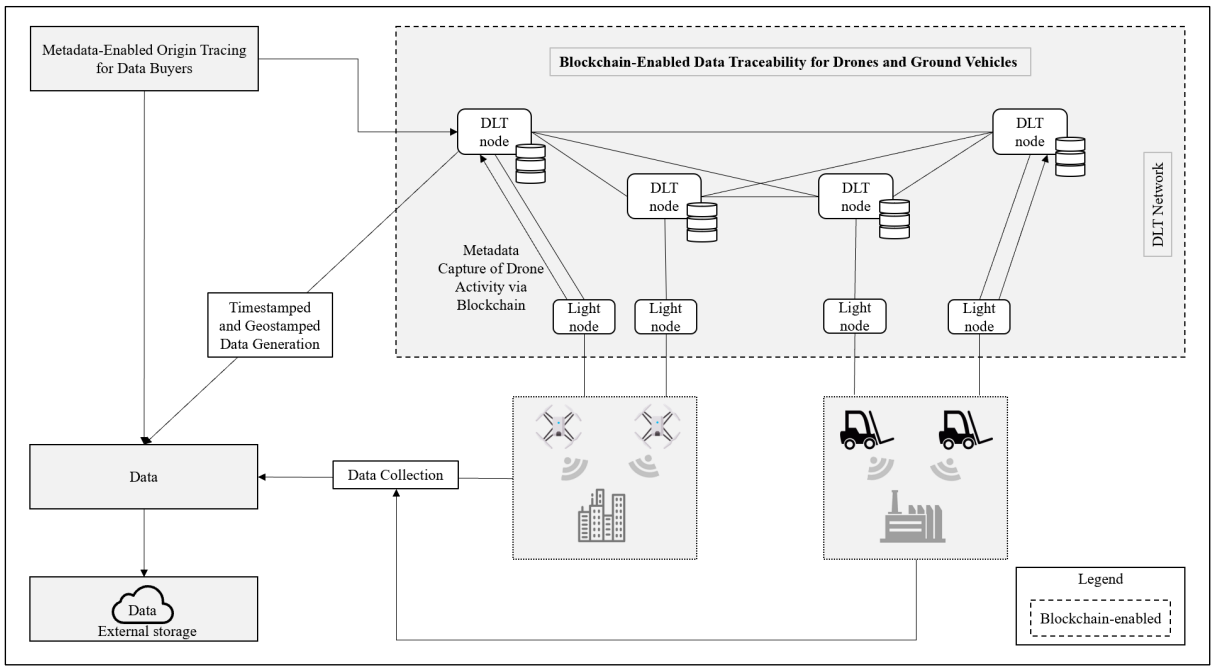

Abbildung 9: Vereinfachte Visualisierung eines Blockchain-basierten Systems zur Protokollierung von Metadaten über Datenerhebungen
Quelle: Eigene Darstellung

Für die Herstellung einer Nachvollziehbarkeit der Herkunft und Verarbeitung von erhobenen Daten gibt es unterschiedliche Ansätze. Der Hash eines Datensatzes ist ein algorithmisch erzeugter einzigartiger alpha-numerischer Code, der sich nicht-nachvollziehbar und grundlegend ändert, wenn sich der betrachtete Datensatz auch nur minimal ändert. Durch den Einbezug von früheren Versionen eines Datensatzes bei der Generierung eines Hashes für einen über/verarbeiteten Datensatz, ließe sich eine Form der Nachvollziehbarkeit über sogenannte „Merkle tree“-Struktur erzeugen. Eine innovativere Lösung würde die Nutzung von sogenannten FaR-Hashes darstellen (Tripathi & Skwarek 2023). Dabei werden algorithmisch alpha-numerische Codes eines zugrundeliegenden Datensatzes erzeugt, die sich teilweise ändern, sodass die Versionierung bei der Bearbeitung von Datensätzen leichter nachvollziehbar wird.

Letztlich bietet der Anwendungsfall der Technologie in dem beschriebenen Kontext einen Mechanismus zur Qualitätssicherung von Daten, die über den Marktplatz angeboten werden. Dieses Szenario lässt ebenfalls die Möglichkeit offen, dass externe Anbieter ebenso nicht-verifizierbare Daten anbieten können, was wiederum für Datensätze und -produkte sinnvoll wäre, für die eine umfassende Nachvollziehbarkeit über die Erhebung nicht kritisch sind.

Durch die Implementierung dieser spezifischen Form der Qualitätssicherung könnte eine Situation entstehen, in der involvierte Akteure – sowohl Käufer als auch Verkäufer – in einer anonymen Kapazität miteinander interagieren können. Diese Strategie verringert die anfänglich erforderliche Vertrauensbereitschaft seitens des Käufers, da monetäre Transaktionen automatisch mittels eines Blockchain-Tokens abgewickelt werden. Diese fortschrittliche Herangehensweise bildet das fundamentale Gerüst für die Schaffung eines dezentralisierten, automatisierten und vertrauenswürdigen Datenmarktplatzes.

Dem gegenüber stehend muss jedoch berücksichtigt werden, dass die Vielfalt und Zugänglichkeit von Daten erheblich variieren können. Aspekte wie Datenzugang, Erhebungsaufwand und Informationsgehaltssensitivität spielen eine entscheidende Rolle bei der Beurteilung der Marktfähigkeit von Daten. Beispielsweise könnte ein dezentraler Marktplatz nicht zwangsläufig geeignet sein, um Aufträge für Wartungsarbeiten mittels Drohnen und Bodenfahrzeugen auszuschreiben. In einem Kontext, der eine spezifische Beauftragung zur Erhebung sensibler Informationen betrifft, könnte es für den Auftraggeber möglicherweise keinen substanziellen Mehrwert haben, den exakten Ablauf der Datenerhebung im Detail nachvollziehen zu können. Es ist daher unerlässlich, genauer zu differenzieren und zu spezifizieren, welche Vorteile in welchem Szenario und für welchen Art von Marktteilnehmer entstehen könnten. Letztendlich ist es von höchster Bedeutung, den Aufwand für die Implementierung und den laufenden Betrieb eines solchen Systems in Relation zu den Zahlungsbereitschaften potenzieller Kunden zu setzen.

III. Dezentraler Marktplatz: Zugriffsmanagement und Handelsabwicklung

Die Anwendung der Blockchain- oder Distributed Ledger-Technologie zur Schaffung eines dezentralen Datenmarktplatzes beschreibt die Idee eine Marktplatzinfrastruktur zu gestalten, die sich durch die automatisierte und dezentrale Handelsabwicklung auszeichnet. Damit verbunden gehen die Vorteile der Reduktion eines Counterparty-Risikos und Plattform-Risikos gegenüber eines zentralen Providers einher, sowie vielseitiger Potentiale für automatisierte Handelsabwicklung und Zugriffsmanagement auf dynamische und statische Daten und Datensätze.

Ein wesentliches Merkmal einer dezentralen Marktplatzinfrastruktur liegt in den Möglichkeiten zur Kostenreduktion für die Handelsabwicklung durch die Nutzung von Smart-Contract-basierter Automatisierung. Diese sollte sich in entsprechend niedrigen Handelsgebühren widerspiegeln. Somit könnten die generierten Gebühren beispielsweise primär zur kostendeckenden Finanzierung der Plattform und Infrastruktur verwendet werden oder die Plattform durch eine genossenschaftsähnliche Besitzstruktur gekennzeichnet sein, in dem Mitglieder Beiträge zu Finanzierungszwecken zahlen. Ebenso kann eine solche Plattform profitorientiert sein.

Die Dezentralität eines solchen Datenmarktplatzes kann je nach technischer Gestaltung unterschiedliche Ausmaße annehmen: Ein hohes Maß and Dezentralität ergibt sich, wenn weite Teile der technischen Infrastruktur Blockchain-basiert sind. Dann handelt es sich um ein Konstrukt aus Smart Contracts auf einer öffentlichen Blockchain, die von Nutzern über ein web-basierte grafische Benutzeroberfläche (GUI) angesteuert werden. Ein Browser-Plugin verknüpft das Wallet eines Nutzers mit der Applikation. Bei Auswahl eines Datenprodukts und Zustimmung zu den durch Smart Contracts ermittelten Transaktionen werden die auszutauschenden Assets vom Wallet des Käufers zum Wallet des Verkäufers und umgekehrt transferiert. Auf diese Weise kann beispielsweise ein Token (im Folgenden: Access-Token) mit spezifischen Merkmalen das Recht auf Datenzugriff repräsentieren (vom Verkäufer zum Käufer), während die Kompensation in Form digitaler kryptografischer Euro-Derivate (vom Käufer zum Verkäufer) erfolgt. Der Besitz des Asset-Token kann im Vorfeld des Datenzugriffs, beispielsweise auf Cloud-basierte Datensätze oder extern gehostete Dashboards, als Legitimation für den Zugriff geprüft und erkannt werden. Die technische Ausgestaltung eines Access-Token kann temporäre oder unterschiedliche Abstufungen des Datenzugriffs beinhalten. Die Zahlungsabwicklung kann komplexere Szenarien wie wiederkehrende Zahlungen, gestaffelte Zahlungen oder Zahlungen nach bestimmten Zeiträumen abbilden.

Es bestehen auch dezentrale Netzwerke zur Datenspeicherung, die ihrerseits eigene technische und ökonomische Anreizsysteme und Netzwerkwährungen aufweisen. In diesen dezentralen Netzwerken werden Datensätze fragmentiert und verschlüsselt auf den Computern der Netzwerkteilnehmer gespeichert, die ihrerseits für die Bereitstellung von Speicherkapazität kompensiert werden. Die Aggregation der Fragmente sowie die Verwaltung des Zugriffs darauf obliegen dem Eigentümer unter Einsatz kryptografischer Methoden. Die Nutzung solcher existierender Netzwerke würde zwar den Grad der Dezentralisierung erhöhen, jedoch auch die Komplexität erhöhen und dadurch möglicherweise die Praktikabilität des Systems verringern.

Die tatsächliche Nachfrage potentieller Datenanbietern für die Verwendung dieser Technologien und deren Implikationen bedarf weiterer Überprüfung.

Abbildung 10 veranschaulicht in vereinfachter Form die Prozesse innerhalb eines auf Blockchain-basierten Marktplatzsystems. Innerhalb dieses Systems besitzen Käufer und Verkäufer individuelle Wallets im Blockchain-Netzwerk. Die Vorteile eines dezentralen Marktplatzes umfassen potentiell niedrigere Kosten für Nutzer, und eine Minimierung des Counterparty-Risikos. Letzteres bezieht sich auf die potenzielle Gefahr eines Ausfalls seitens des Handelspartners. Gleichzeitig wird das Plattformrisiko verringert, welches die möglichen Gefahren durch die Abhängigkeit von einem Plattformanbieter beschreibt. Ein solches Abhängigkeitsbeispiel könnte die Zugänglichkeit der Dienste oder Veränderungen in der Preisgestaltung darstellen.

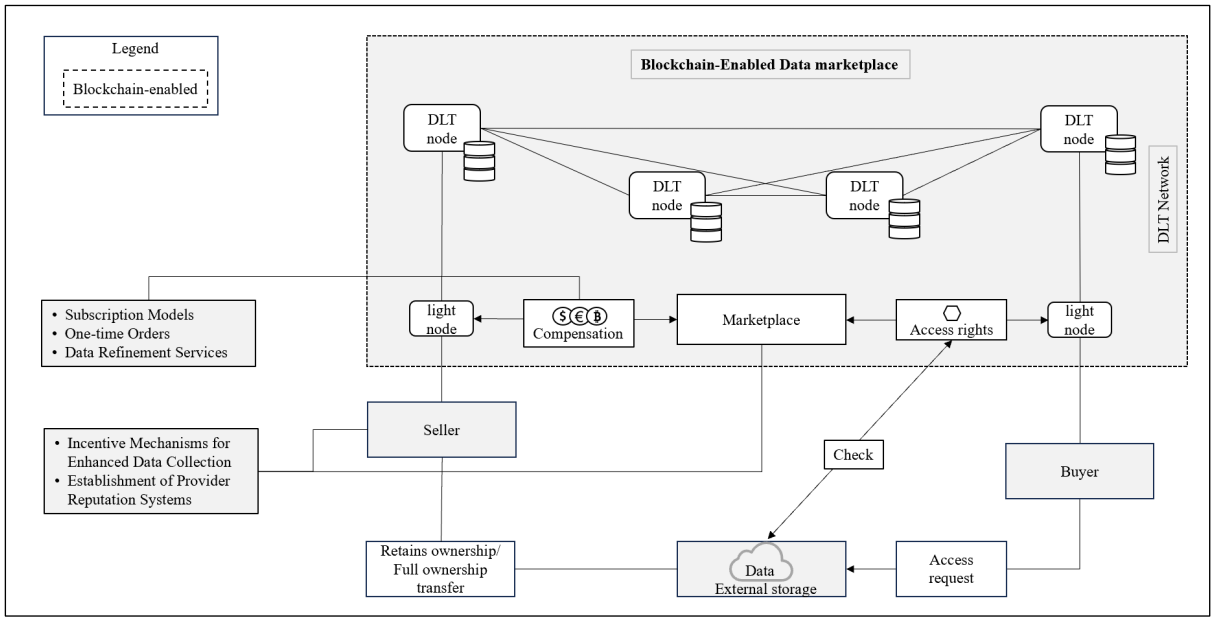

Abbildung 10: Vereinfachte Darstellung eines Blockchain-Systems mit Marktplatzlogik
Quelle: Eigene Darstellung

Wichtige Aspekte für die Realisierung eines Datenmarktplatzes beziehen sich die darzustellende Angebotsstruktur. Konkret betrachtet eröffnet sich ein breites Spektrum möglicher Variationen sowohl in den Angeboten als auch den Gesuchen. Hierbei lassen sich diverse Szenarien konzipieren, die von bereits gesammelten Daten bis hin zu in regelmäßigen Abständen generierten Datenserien reichen, welche durch Abonnementmodelle gestützt sind. Ebenso sind Anfragen für umfassende und langanhaltende Wartungsverträge von Relevanz. Entsprechend muss bei der technischen Ausgestaltung auch berücksichtigt werden, dass die Besitzverhältnisse der erhobenen Daten unterschiedlich ausgestaltet sind: Es ist intuitiv, dass ein Auftraggeber die vom Auftragnehmer erfassten Messdaten oder Daten im Rahmen von

Wartungsaktivitäten besitzt. Gleichzeitig kann ein Anbieter von städtischen Luftqualitätsdaten die Kontrolle über die generierten Informationen behalten und den Zugriff auf diese Daten mehrfach verkaufen. Dies birgt eine gewisse Komplexität, die durch Smart Contracts abgebildet werden muss. Im Rahmen einer Pilotierung wäre es ratsam, Vorlagen für unterschiedliche Angebotstypen und Anfragen zu definieren.

Grundsätzlich könnte der Nutzer mithilfe einer grafischen Benutzeroberfläche die spezifische Konfiguration eines Smart Contracts für sein jeweiliges Angebot entsprechend seinen Präferenzen erstellen. Abschließend ist es erforderlich zu eruieren, inwieweit aufgrund der Vielfalt der zu repräsentierenden Angebotstypen jedes Marktplatzangebot oder -gesuch einen eigenen individuellen Smart Contract erfordert.

Literaturverzeichnis

Agrawal, R., Verma, P., Sonanis, R., Goel, U., De, A., Kondaveeti, S. A., & Shekhar, S. (2018). Continuous security in IoT using blockchain. *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, *2018-April*, 6423–6427. https://doi.org/10.1109/ICASSP.2018.8462513

Alladi, T., Chamola, V., Sahu, N., & Guizani, M. (2020). Applications of blockchain in unmanned aerial vehicles: A review. *Vehicular Communications*, *23*. https://doi.org/10.1016/J.VEHCOM.2020.100249

Atlam, H. F., Alenezi, A., Alassafi, M. O., & Wills, G. B. (2018). Blockchain with Internet of Things: Benefits, challenges, and future directions. *International Journal of Intelligent Systems and Applications*, *10*(6), 40–48. https://doi.org/10.5815/IJISA.2018.06.05

Bera, B., Chattaraj, D., & Das, A. K. (2020). Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment. *Computer Communications*, *153*, 229–249. https://doi.org/10.1016/J.COMCOM.2020.02.011

Bera, B., Das, A. K., & Kumar Sutrala, A. (2021). Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet of Drones environment. *Computer Communications*, *166*, 91–109. https://doi.org/10.1016/j.comcom.2020.12.005

Bera, B., Saha, S., Das, A. K., Kumar, N., Lorenz, P., & Alazab, M. (2020). Blockchain-Envisioned Secure Data Delivery and Collection Scheme for 5G-Based IoT-Enabled Internet of Drones Environment. *IEEE Transactions on Vehicular Technology*, *69*(8), 9097–9111. https://doi.org/10.1109/TVT.2020.3000576

Bhattacharya, P., Tanwar, S., Bodkhe, U., Tyagi, S., Member, S., & Kumar, N. (2021). *BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications; BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications*. https://doi.org/10.1109/TNSE.2019.2961932

García-Magariño, I., Lacuesta, R., Rajarajan, M., & Lloret, J. (2019). Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain. *Ad Hoc Networks*, *86*, 72–82. https://doi.org/10.1016/J.ADHOC.2018.11.010

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Čapkun, S. (2016). On the security and performance of Proof of Work blockchains. *Proceedings of the ACM Conference on Computer and Communications Security*, *24-28-October-2016*, 3–16. https://doi.org/10.1145/2976749.2978341

Guo, B., Yu, Z., Zhou, X., & Zhang, D. (2014). From participatory sensing to Mobile Crowd Sensing. *2014 IEEE International Conference on Pervasive Computing and Communication Workshops, PERCOM WORKSHOPS 2014*, 593–598. https://doi.org/10.1109/PERCOMW.2014.6815273

Guo, H., & Liu, J. (2020). UAV-Enhanced Intelligent Offloading for Internet of Things at the Edge. *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS*, *16*(4). https://doi.org/10.1109/TII.2019.2954944

Gupta, P., Dedeoglu, V., Kanhere, S. S., & Jurdak, R. (2021). Towards a blockchain powered IoT data marketplace. *2021 International Conference on COMmunication Systems and NETworkS, COMSNETS 2021*, 366–368. https://doi.org/10.1109/COMSNETS51098.2021.9352865

Gupta, R., Kumari, A., & Tanwar, S. (2021). Fusion of blockchain and artificial intelligence for secure drone networking underlying 5G communications. *Transactions on Emerging Telecommunications Technologies*, *32*(1). https://doi.org/10.1002/ETT.4176

Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., & Nauman, A. (2020). *Smart Contract Privacy Protection Using AI in Cyber-Physical Systems: Tools,Techniques and Challenges*. https://doi.org/10.1109/ACCESS.2020.2970576

Gupta, R., Tanwar, S., Kumar, N., & Tyagi, S. (2020). Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review R. *Computers and Electrical Engineering*, *86*, 106717. https://doi.org/10.1016/j.compeleceng.2020.106717

Hathaliya, J., Sharma, P., Tanwar, S., & Gupta, R. (2019). *Blockchain-based Remote Patient Monitoring in Healthcare 4.0*.

Hayat, S., Yanmaz, E., & Muzaffar, R. (2016). Survey on Unmanned Aerial Vehicle Networks for Civil Applications: A Communications Viewpoint; Survey on Unmanned Aerial Vehicle Networks for Civil Applications: A Communications Viewpoint. *IEEE Communications Surveys & Tutorials*, *18*(4). https://doi.org/10.1109/COMST.2016.2560343

Khan, A. A., Khan, M. M., Khan, K. M., Arshad, J., & Ahmad, F. (2021). A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs. *Computer Networks*, *196*. https://doi.org/10.1016/J.COMNET.2021.108217

Kim, H., Park, J., Bennis, M., & Kim, S.-L. (2020). Blockchained On-Device Federated Learning; Blockchained On-Device Federated Learning. *IEEE Communications Letters*, *24*(6), 1279. https://doi.org/10.1109/LCOMM.2019.2921755

Lu, Y., Huang, X., Dai, Y., Maharjan, S., & Zhang, Y. (2020). Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT. *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS*, *16*(6), 4177. https://doi.org/10.1109/TII.2019.2942190

Mach, P., & Becvar, Z. (2017). Mobile Edge Computing: A Survey on Architecture and Computation Offloading. *IEEE Communications Surveys and Tutorials*, *19*(3), 1628–1656. https://doi.org/10.1109/COMST.2017.2682318

Motlagh, N. H., Bagaa, M., & Taleb, T. (2017). UAV-Based IoT Platform: A Crowd Surveillance Use Case. *IEEE Communications Magazine*, *55*(2), 128–134. https://doi.org/10.1109/MCOM.2017.1600587CM

Novo, O. (2018). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT; Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE INTERNET OF THINGS JOURNAL*, *5*(2). https://doi.org/10.1109/JIOT.2018.2812239

Pokhrel, S. R. (2020). Federated learning meets blockchain at 6G Edge: A drone-assisted networking for disaster response. *DroneCom 2020 - Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond*, 49–54. https://doi.org/10.1145/3414045.3415949

Rana, T., Shankar, A., Kamran Sultan, M., Patan, R., & Balusamy, B. (2019). *An Intelligent approach for UAV and Drone Privacy Security Using Blockchain Methodology; An Intelligent approach for UAV and Drone Privacy Security Using Blockchain Methodology*.

Schlatt, V., Schweizer, A., Urbach, N., & Fridgen, G. (2016). *Blockchain: Grundlagen, Anwendungen und Potenziale*.

Shen, M., Tang, X., Zhu, L., & Guizani, M. (2019). Privacy-Preserving Support Vector Machine Training Over Blockchain-Based Encrypted IoT Data in Smart Cities. *IEEE INTERNET OF THINGS JOURNAL*, *6*(5). https://doi.org/10.1109/JIOT.2019.2901840

Sheth, K., Patel, K., Shah, H., Tanwar, S., Gupta, R., & Kumar, N. (2020). A taxonomy of AI techniques for 6G communication networks. *Computer Communications*, *161*, 279–303. https://doi.org/10.1016/J.COMCOM.2020.07.035

Singh, M., Singh Aujla, G., & Singh Bali, R. (2020). *ODOB: One Drone One Block-based Lightweight Blockchain Architecture for Internet of Drones; ODOB: One Drone One Block-based Lightweight Blockchain Architecture for Internet of Drones*.

Tanwar, S., Vora, J., Tyagi, S., Kumar, N., & Obaidat, M. S. (2018). A systematic review on security issues in vehicular ad hoc network. *Security and Privacy*, *1*(5), e39. https://doi.org/10.1002/SPY2.39

Tripathi, S., & Skwarek, V. (2023). *Fuzzified advanced robust hashes for identification of digital and physical objects*. https://www.itpro.co.uk/security/22804/hp-70-of-internet-of-things-devices-

Wang, Y., Su, Z., Zhang, N., & Benslimane, A. (2021). Learning in the Air: Secure Federated Learning for UAV-Assisted Crowdsensing. *IEEE Transactions on Network Science and Engineering*. https://doi.org/10.1109/TNSE.2020.3014385

Xiong, Z., Member, S., Feng, S., Wang, W., Niyato, D., Wang, P., Member, S., Han, Z., Wang Xiong, P. Z., Feng, S., Wang, W., & Niyato, D. (2019). Cloud/Fog Computing Resource Management and Pricing for Blockchain Networks; Cloud/Fog Computing Resource Management and Pricing for Blockchain Networks. *IEEE Internet of Things Journal*, *6*(3). https://doi.org/10.1109/JIOT.2018.2871706

Xiong, Z., Zhang, Y., Niyato, D., Wang, P., & Han, Z. (2018). When Mobile Blockchain Meets Edge Computing; When Mobile Blockchain Meets Edge Computing. *IEEE Communications Magazine*, *56*. https://doi.org/10.1109/MCOM.2018.1701095

Yazdinejad, A., Parizi, R. M., Dehghantanha, A., Srivastava, G., & Aledhari, M. (2021). Enabling Drones in the Internet of Things With Decentralized Blockchain-Based Security. *IEEE INTERNET OF THINGS JOURNAL*, *8*(8). https://doi.org/10.1109/JIOT.2020.3015382

Zhao, Y., Student Member, G., Zhao, J., Jiang, L., Tan, R., Member, S., Niyato, D., Li, Z., Lyu, L., Liu, Y., & Zhao Yang Zhao, J. (2021). Privacy-Preserving Blockchain-Based Federated Learning for IoT Devices; Privacy-Preserving Blockchain-Based Federated Learning for IoT Devices. *IEEE Internet of Things Journal*, *8*(3). https://doi.org/10.1109/JIOT.2020.3017377

Zhou, F., Wu, Y., Member, S., Qingyang Hu, R., & Qian, Y. (2018). Computation Rate Maximization in UAV-Enabled Wireless-Powered Mobile-Edge Computing Systems. *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, *36*(9). https://doi.org/10.1109/JSAC.2018.2864426

Zhou, Y., Pan, C., Yeoh, L., Wang, K., Elkashlan, M., Vucetic, B., & Li, Y. (2020). Secure Communications for UAV-Enabled Mobile Edge Computing Systems. *IEEE TRANSACTIONS ON COMMUNICATIONS*, *68*(1). https://doi.org/10.1109/TCOMM.2019.2947921

Zhu, L., Wu, Y., Gai, K., & Choo, K. K. R. (2019). Controllable and trustworthy blockchain-based cloud data management. *Future Generation Computer Systems*, *91*, 527–535. https://doi.org/10.1016/J.FUTURE.2018.09.019