WHITEPAPER

Der digitale Frachtbrief

das eCMR-Protokoll und eine beispielhafte Implementierung

Dieses Projekt wurde aus Mitteln des Bundesministeriums für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (BMK) gefördert und im Rahmen des Programms Logistikförderung durch die Schieneninfrastruktur-Dienstleistungsgesellschaft mbH (SCHIG mbH) abgewickelt.

1 Einleitung

Jährlich werden in der Europäischen Union geschätzte 300 Millionen Frachtbriefe (CMR) erstellt, von denen 99% auf Papier basieren. Diese papierbasierten Dokumente, oft handgeschrieben in verschiedenen Sprachen und manchmal schwer lesbar oder werden sogar während der Fahrt vom LKW-Fahrer ausgefüllt, sind anfällig für Fehler und Manipulationen. Trotz der gelegentlich unprofessionellen Handhabung sind CMR-Dokumente entscheidende Elemente in der Abwicklung von Angelegenheiten im Steuer-, Zoll- und Rechnungswesen.

Die Vorteile einer Digitalisierung dieser Prozesse sind offensichtlich. Sowohl Frächter als auch Spediteure beklagen den hohen manuellen Aufwand, die schlechte Datenqualität und signifikante Verzögerungen, die nicht nur die Rechnungsstellung, sondern auch die Einhaltung bestimmter rechtlicher Vorgaben erschweren.

Hier setzt das eCMR-Protokoll an, welches eine digitale Alternative zum traditionellen CMR-Frachtbrief bietet und in der internationalen Straßengüterbeförderung Anwendung findet. Es soll die Logistikbranche durch die Förderung der Digitalisierung und Modernisierung, sowie durch umweltfreundlichere Prozesse aufgrund des reduzierten Papierverbrauchs voranbringen. Mit eCMR-Dokumenten können Unternehmen ihre Frachtinformationen in Echtzeit verfolgen, wodurch sich Transparenz und Effizienz der Lieferkette steigern lassen. Dies führt nicht nur zu einer vereinfachten Einhaltung der Compliance, sondern auch zu einer schnelleren Abwicklung der Frachtbriefe, was widerum Zeit und Kosten spart.

Dieses Whitepaper erörtert die technische Realisierung des digitalen Frachtbriefs auf Basis des eCMR-Protokolls und beleuchtet, inwieweit Blockchain-Technologie in diesem Kontext einen Mehrwert schaffen kann. Die Erkenntnisse der vorgestellten Implementierung entstanden in Zusammenarbeit mit renommierten österreichischen Spediteuren und Transportunternehmen, mit dem Ziel, einen Prototyp für die Digitalisierung des CMR im Kontext logistischer Prozesse zu entwickeln.

Das Hauptanliegen dieses Whitepapers ist nicht die Bewerbung eines Produkts, sondern die Verbreitung von Wissen. Es zielt darauf ab, Außenstehenden einen verständlichen Zugang zum Thema zu bieten und potenzielle Lösungsansätze aufzuzeigen.

1.1 eCMR-Protokoll

Das eCMR-Protokoll [1] ermöglicht eine vollständig digitalisierte und automatisierte Verwaltung von Frachtpapieren, was die Effizienz und Transparenz in der Logistik signifikant steigert. Es kann traditionelle Papierdokumente ersetzen und adressiert die Hauptziele der Prozessoptimierung:

- **Effizienzsteigerung**: Digitalisierung minimiert Bearbeitungszeiten und erhöht die Produktivität.
- **Fehlerreduktion**: Automatisierte Datenerfassung und -verarbeitung reduzieren das Risiko menschlicher Fehler.
- **Verbesserte Transparenz**: Echtzeit-Zugriff auf Lieferinformationen verbessert die Nachverfolgbarkeit.
- **Umweltschutz**: Der geringere Papierverbrauch unterstützt nachhaltigere Betriebsabläufe.
- **Sicherheit**: Elektronische Speicherung von Dokumenten verringert das Risiko von Verlust und Beschädigung.

Das Protokoll deckt umfangreiche Informationen ab, einschließlich:

- **Kontaktdaten** von Absender und Empfänger,
- **Transportinformationen** wie Fahrzeugdaten und Start-/Zielorte,
- **Details zur Ladung**, inklusive Verpackung, Gewicht und speziellen Anweisungen,
- **Kostenangaben** zum Transport.

Zusätzlich erfordert das eCMR-Protokoll die elektronische Unterschrift der beteiligten Parteien – Absender, Beförderer und Empfänger – um den Transportvorgang zu validieren.

Weitere Anforderungen umfassen:

- **Lesbarkeit und Aufbewahrung:** eCMR-Dokumente müssen klar lesbar sein und über einen vorgegebenen Zeitraum aufbewahrt werden.
- **Datenschutz und Sicherheit:** Die Verarbeitung und Speicherung der Daten muss datenschutzkonform erfolgen und das System sicher vor unbefugtem Zugriff sein.
- **Zugänglichkeit:** Gewährleistung, dass alle Beteiligten auf die Dokumente zugreifen und Informationen zeitnah austauschen können.

Bisher haben 30 Länder, darunter 17 EU-Mitgliedstaaten, das eCMR-Protokoll ratifiziert; Österreich hat diesen Prozess vor kurzem eingeleitet [3]. Zur Unterstützung der Standardisierung und zur Bewältigung der Herausforderungen wurde 2021 die Open Logistics Foundation [2] ins Leben gerufen, die einen schnelleren Markteinstieg für interessierte Parteien ermöglicht. Die in diesem Whitepaper beschriebene Implementierung war jedoch nicht Gegenstand der von der Open Logistics Foundation bearbeiteten Themen.

2 Blockchain-Technologie

2.1 Kurzeinführung

Die Blockchain-Technologie lässt sich als eine dezentralisierte und verteilte digitale Datenbank beschreiben, die Transaktionen auf eine transparente und sichere Weise aufzeichnet. Grundlegend besteht sie aus einer Abfolge von Blöcken, wobei jeder Block eine Reihe von Transaktionen umfasst. Diese Blöcke sind miteinander verbunden und bilden eine chronologische Kette.

Wesentliche Sicherheitsmerkmale der Blockchain umfassen:

1. **Dezentralisierung:** Die herausragende Eigenschaft der Blockchain ist ihr dezentraler Charakter. Sie setzt sich aus zahlreichen Knotenpunkten zusammen, von denen jeder einzelne befugt ist, Daten (Transaktionen) zu validieren und in Form eines neues Blocks zu der Kette, der eigentlichen Blockchain, hinzuzufügen. Diese Struktur erfordert komplexe Verwaltungsprozesse zur Gewährleistung der Datensicherheit und Datenkonsistenz über alle beteiligten Knoten hinweg. Der entscheidende Vorteil liegt darin, dass keine zentrale Instanz existiert, welche die Daten manipulieren könnte oder ein einfaches Ziel für Angriffe darstellen würde.
2. **Kryptographie:** Die Blockchain nutzt fortschrittliche kryptographische Verfahren, um die Datensicherheit zu gewährleisten. Mithilfe asymmetrischer Kryptographie werden Transaktionen digital signiert, was deren Echtheit bestätigt. Weiterhin sind die Blöcke mittels kryptographischer Hash-Funktionen miteinander verknüpft, was die Unversehrtheit der gesamten Kette sicherstellt. Eine nachträgliche Modifikation eines Blocks würde folglich die Invalidität nachfolgender Blöcke und Transaktionen bedeuten.
3. **Unveränderlichkeit:** In die Blockchain eingetragene Daten lassen sich nur schwer modifizieren oder löschen. Die kryptographische Sicherung der Blöcke und ihre Verknüpfung untereinander erfordern für eine nachträgliche Änderung erhebliche Rechenleistungen. Mit zunehmender Dauer der Speicherung in der Blockchain steigt die Sicherheit der Daten.
4. **Transparenz und Integrität:** Jeder Knotenpunkt der Blockchain besitzt eine komplette Kopie der Kette. Alle Transaktionen werden von den Knoten geprüft und müssen von der Mehrheit bestätigt werden, bevor sie hinzugefügt werden. Dies gewährleistet die Korrektheit und Unverfälschtheit der Daten und erschwert es zugleich potentiellen Angreifern manipulierte Daten der Kette hinzuzufügen, da diese durch die Mehrheit der Knoten im Zuge der Datenvalidierung vor dem Hinzufügen eines neuen Blocks aufgedeckt werden würde.

2.2 Permissioned und Public Blockchains

Es gibt unterschiedliche Ansätze im Bereich der Blockchain-Technologie, die jeweils ihre eigenen spezifischen Vorteile, Einschränkungen und Anwendungsfälle bieten. Der Hauptunterschied zwischen diesen beiden Typen liegt in ihrem Zugangskonzept und ihrer Kontrollstruktur.

Public Blockchains (öffentliche Blockchains), sind für jeden zugänglich. Sie ermöglichen es jedem Nutzer dem Netzwerk ohne vorherige Genehmigung oder Identitätsprüfung beizutreten, Transaktionen durchzuführen oder sogar als Knoten im Netzwerk zu agieren. Prominente Beispiele für öffentliche Blockchains sind Bitcoin und Ethereum. Diese Offenheit sorgt für ein hohes Maß an Transparenz und Sicherheit, da die Daten auf tausenden von Computern verteilt gespeichert werden und Manipulationen durch die breite Verteilung und den Einsatz kryptografischer Techniken praktisch unmöglich sind. Der Nachteil dabei ist jedoch, dass diese Offenheit zu Problemen hinsichtlich Skalierbarkeit, Geschwindigkeit und Energieverbrauch führen kann. Transaktionen können langsamer und teuer sein, insbesondere bei hoher Netzwerkauslastung.

Permissioned Blockchains (private Blockchains) beschränken den Zugang zum Netzwerk. Die Besitzer bzw. die Betreiber einer Permissioned Blockchain kontrollieren wer dem Netzwerk beitreten und somit auch wer Transaktionen durchführen oder einen Knoten betreiben darf. Ebenso kontrollieren sie wie die Konsensfindung organisiert ist, welche die Datenintegrität sicherstellt. Solche Blockchains bieten zumeist eine effizientere Transaktionsverarbeitung und eine bessere Skalierbarkeit, da die Teilnehmer bekannt und die Netzwerkgröße begrenzt ist. Dies führt zu schnelleren Transaktionszeiten und geringerem Energieverbrauch im Vergleich zu öffentlichen Blockchains. Permissioned Blockchains sind ideal für Anwendungsfälle, bei denen Datenschutz, Compliance und Geschwindigkeit von entscheidender Bedeutung sind, wie beispielsweise im Bankwesen, Gesundheitswesen und bei Supply-Chain-Management-Systemen. Der offensichtliche Nachteil ist jedoch, dass sie nicht so hochgradig dezentralisiert und transparent wie Public Blockchains sind, da die Kontrolle in den Händen einer begrenzten Anzahl von Akteuren liegt.

2.3 Blockchain-Anwendungen im Kontext eCMR-Protokolls

Die spezifischen Merkmale der Blockchain-Technologie eröffnen vielfältige Anwendungsmöglichkeiten im Rahmen des eCMR-Protokolls.

2.3.1 Speicherung von eCMR-Dokumenten

Die eigentliche digitale Speicherung von eCMR-Dokumenten bietet sich anstelle konventioneller IT-Systeme an. Durch die Nutzung der Blockchain-Technologie können diese Daten sicher und direkt allen relevanten Parteien zugänglich gemacht werden. Allerdings erfordert der Schutz persönlicher Daten und die Wahrung der Vertraulichkeit, dass diese Informationen nicht offen und lesbar auf der Blockchain abgelegt werden, besonders bei öffentlichen Blockchains. Eine Verschlüsselung der Daten ist daher unerlässlich, um den Zugang ausschließlich berechtigten Parteien zu ermöglichen. Zudem ist bei der Entscheidung für eine bestimmte Blockchain-Technologie das Verhältnis von Datenvolumen zu Transaktionskosten zu berücksichtigen.

2.3.2 Automatisierung von Prozessabläufen

Das eCMR-Protokoll beschreibt nicht nur die Inhalte digitaler Dokumente, sondern legt auch fest, welche Prozesse und Abläufe diese Dokumente durchlaufen. Ein wesentlicher Aspekt dabei ist die digitale Unterschrift durch die beteiligten Parteien, welche den Versand oder den Erhalt der Waren offiziell bestätigt.

Eine Schlüsseltechnologie zur Automatisierung dieser Abläufe sind Smart Contracts. Diese in der Blockchain gespeicherten Programme führen definierte Aktionen automatisch aus, sobald vorher festgelegte Bedingungen erfüllt sind. Im Anwendungsbereich des eCMR-Protokolls ermöglichen Smart Contracts beispielsweise die automatische Aktualisierung des Dokumentenstatus, sobald die Fracht von einer Partei zur nächsten übergeht. Dies eliminiert die Notwendigkeit für manuelle Eingriffe oder den Einsatz externer IT-Systeme und sorgt für eine effiziente und fehlerfreie Prozessabwicklung.

2.3.3 Integritätsprüfung von Dokumenten

Das eCMR-Protokoll betont die Bedeutung der Dokumentenintegrität, die besagt, dass einmal erstellte Dokumentendaten nicht mehr verändert werden dürfen. Die Unveränderlichkeit, als eine Kernfunktion der Blockchain-Technologie, spielt hier eine entscheidende Rolle bei der Gewährleistung der Dokumentenintegrität, die auf zweifache Weise sichergestellt werden kann.

Direkte Speicherung auf der Blockchain (siehe auch Kapitel 2.3.1): Indem die Daten direkt in der Blockchain abgelegt werden, profitieren sie von deren Unveränderlichkeit. Jegliche nachträgliche Manipulation der Daten wird somit effektiv unterbunden.

Speicherung eines digitalen Fingerabdrucks: Alternativ kann die Integrität eines Dokuments durch die Berechnung und Speicherung seines digitalen Fingerabdrucks (Hash-Wert) auf der Blockchain gesichert werden. Dieser Fingerabdruck, der aus dem Originaldokument generiert wird, ist für Menschen nicht lesbar. Um die Unverfälschtheit eines Dokuments zu überprüfen, kann jederzeit ein neuer Fingerabdruck vom Originaldokument erstellt und mit dem auf der Blockchain gespeicherten Erstfingerabdruck abgeglichen werden. Bei einer Übereinstimmung der beiden Fingerabdrücke wird das Dokument als unverändert und authentisch verifiziert. In diesem Szenario bleibt das eigentliche Dokument außerhalb der Blockchain, lediglich der Fingerabdruck wird in der Blockchain verewigt.

Für die Durchführung einer Integritätsprüfung sind somit das originale Dokument, der Zugang zum initial gespeicherten Fingerabdruck sowie der Einsatz des identischen Algorithmus für die Fingerabdruckerstellung erforderlich.

2.3.4 Transparenz durch Daten

Die Transparenz von Blockchain-Netzwerken stellt einen wesentlichen Vorteil dar. Da Daten auf der Blockchain für alle Teilnehmer öffentlich einsehbar sind, ermöglicht dies einen breiten Zugriff und die Möglichkeit zur unabhängigen Verifizierung. Diese Offenheit fördert das Vertrauen in die Echtheit und Richtigkeit der gespeicherten Informationen, was besonders in der Logistikbranche von großer Bedeutung ist.

2.3.5 Dezentralisierte IT-Infrastruktur

In der vielfältigen Logistikbranche bietet die dezentrale Natur der Blockchain besondere Vorteile. Daten werden nicht zentral, sondern auf vielen verschiedenen Knotenpunkten der Blockchain gespeichert und untereinander repliziert. Dies garantiert die Unabhängigkeit von einzelnen dritten Parteien, sowohl im Betrieb der IT-Infrastruktur als auch bei der Datenspeicherung und -integrität, und stärkt die Resilienz des Systems gegenüber Ausfällen und Manipulationen.

2.4 Risiken

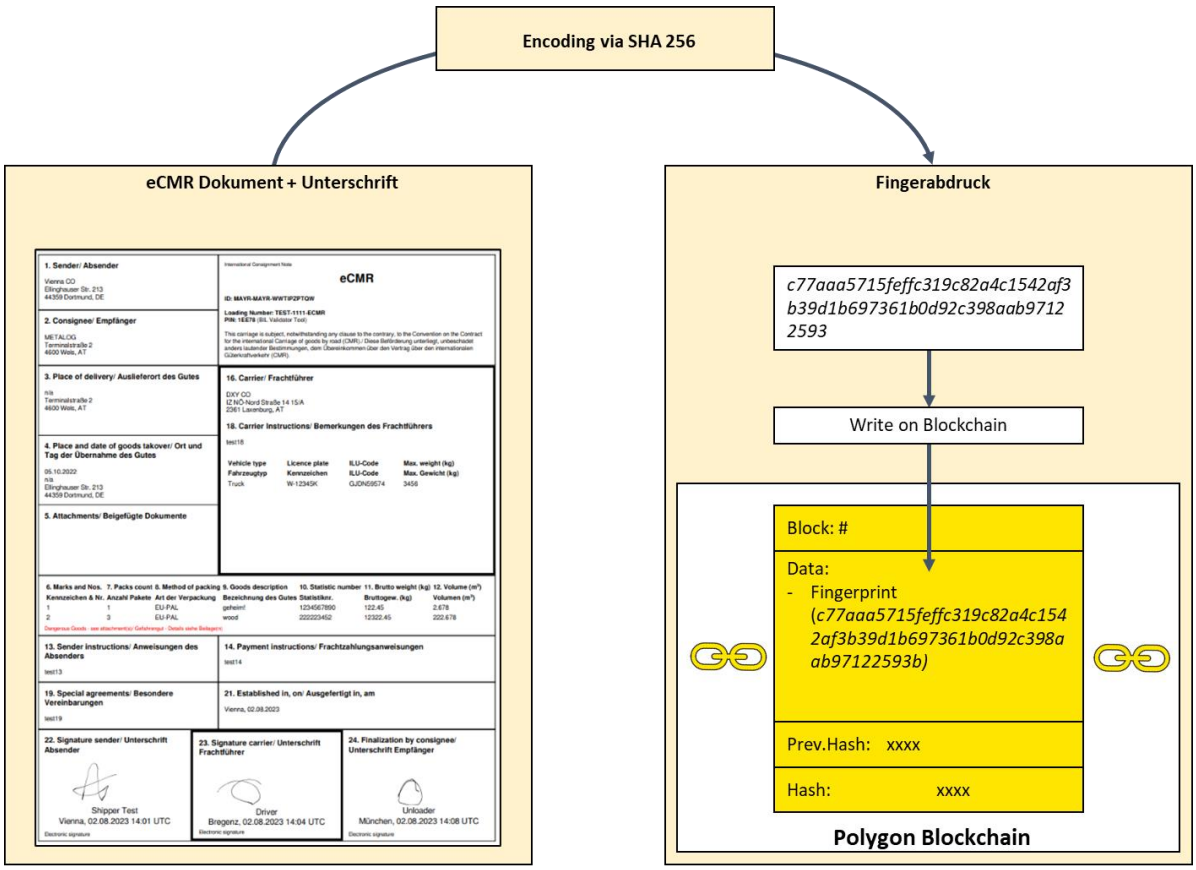
Trotz der vielfältigen Vorteile birgt die Anwendung der Blockchain-Technologie gewisse Risiken, vor allem in Bezug auf Datenschutz und Datensicherheit. Da alle auf der Blockchain gespeicherten Daten prinzipiell einsehbar sind, müssen sensible Informationen verschlüsselt oder durch andere kryptografische Methoden geschützt werden. Zudem könnte die Transparenz der Blockchain ungewollte Rückschlüsse auf Marktbewegungen oder die Aktivitäten einzelner Teilnehmer zulassen. Eine sorgfältige und datenschutzkonforme Speicherung der Daten ist daher essentiell, um einerseits die Anonymität zu wahren und andererseits die Verbindung von Daten zu spezifischen Teilnehmern zu verhindern.

2.5 Implementierte Anwendungen

2.5.1 Dokumentenintegrität mittels Notarization

Eine zentrale Anforderung des eCMR-Protokolls ist die Gewährleistung, dass einmal festgelegte Daten und Angaben innerhalb eines Dokuments, durch die Verknüpfung mit einer digitalen Unterschrift, unveränderbar und sicher sind. Dies stellt nicht nur eine eindeutige Verbindung zwischen Unterschrift und Dokument her, sondern sichert auch langfristig die Integrität der Daten, was für deren Archivierung von besonderem Wert ist.

Zur Erfüllung dieser Anforderung wurde ein Notarisierungsverfahren implementiert, dessen Ergebnisse fälschungssicher und transparent auf einer Blockchain gespeichert werden. Die Notarization transformiert die Dokumentendaten mittels eines speziellen Algorithmus in ein Format, das zwei wesentliche Eigenschaften aufweist. Zum einen ist das resultierende Format für Menschen nicht direkt lesbar, wodurch Rückschlüsse auf die Ursprungsdaten verhindert werden. Zum anderen ist das Verfahren unumkehrbar, was bedeutet, dass die originalen Daten nicht aus dem notarisierten Format rekonstruiert werden können.



In der Praxis wird bei der digitalen Unterschrift eines eCMR-Dokuments ein spezieller Prozess angewendet: Ein digitaler Fingerabdruck, generiert aus den Daten des Dokuments und der Unterschrift (als Bild festgehalten), wird sicher auf der Blockchain gespeichert (on-chain). Das eigentliche Dokument sowie jegliche Änderungshistorie oder Anhänge verbleiben außerhalb der Blockchain (off-chain). Als Algorithmus für die Generierung des Fingeabdrucks wird SHA 256 angewendet.

Durch diesen Fingerabdruck kann das Originaldokument nicht rekonstruiert werden. Er dient jedoch als robustes Werkzeug, um die Echtheit und Unversehrtheit einer Dokumentenkopie zu jedem Zeitpunkt zu verifizieren. Zur Überprüfung wird eine neue Berechnung des Fingerabdrucks aus der Dokumentenkopie und der vorhandenen Unterschrift vorgenommen. Stimmen der neu erzeugte und der bereits gespeicherte Fingerabdruck überein, wird das Dokument als authentisch und unverändert angesehen. Diskrepanzen zwischen den Fingerabdrücken deuten hingegen auf eine Modifikation des Dokuments oder der Unterschrift hin. Dieses Verfahren ermöglicht zwar die Feststellung von Änderungen, zeigt jedoch nicht die spezifischen Modifikationen auf.

Zusätzlich werden alle Anhänge, wie Schadensberichte, Fotos oder Kommentare, als Appendix gespeichert. Jede Version des Anhangs wird zusammen mit der Unterschrift notarisiert, um deren Integrität zusätzlich zum eigentlichen eCMR-Dokument zu gewährleisten und den Zustand zum Zeitpunkt der Notarisierung festzuhalten.

2.6 Zukünftige Innovationen in der Blockchain-Technologie

Die Entwicklungen in der Blockchain-Technologie schreiten rasch voran, was zu spannenden neuen Möglichkeiten führt. Obwohl diese Ansätze im Rahmen des aktuellen Projekts nicht direkt untersucht oder implementiert wurden, bieten sie vielversprechende Perspektiven für die Zukunft.

2.6.1 Zero-Knowledge-Proofs

Zero-Knowledge-Proofs (ZKPs) ermöglichen die Verifizierung der Authentizität von Informationen, ohne die Inhalte selbst offenlegen zu müssen. Im eCMR-Kontext könnten ZKPs dazu genutzt werden, die Existenz und Gültigkeit eines Dokuments zu bestätigen, ohne sensible Daten preiszugeben. Dies stärkt den Datenschutz und die Datensicherheit, indem es nur um die Validierung geht und nicht um den Inhalt. Damit unterstützen ZKPs die Einhaltung von Compliance-Anforderungen, während die Vertraulichkeit der Informationen geschützt bleibt.

2.6.2 Self-Souvereign-Identity

Self-Sovereign Identity (SSI) bietet Individuen und Organisationen die Möglichkeit, ihre Identitäten digital und unabhängig von zentralen Autoritäten zu verwalten. Im eCMR-Protokoll kann SSI zur sicheren und effizienten Verifizierung der Identität von Transportbeteiligten beitragen, den Übergabeprozess von Frachtbriefen vereinfachen und die Authentizität der Dokumentation verstärken. SSI hat das Potenzial, traditionelle elektronische Signaturen zu ersetzen und so einen staatenübergreifenden Standard zu schaffen.

2.6.3 Alternativen zur Ethereum-Blockchain

Neben Ethereum existieren weitere Blockchain-Plattformen wie Solana, Polkadot und Hyperledger, die spezifische Vorteile hinsichtlich Skalierbarkeit, Transaktionskosten und Funktionalität bieten. Diese könnten für die Speicherung von eCMR-Dokumenten und -Hashes, insbesondere bei hohen Datenvolumen oder speziellen industriellen Anforderungen, eine effizientere oder kostengünstigere Lösung darstellen. Die Auswahl der passenden Blockchain-Technologie hängt von den individuellen Bedürfnissen des eCMR-Systems ab.

2.6.4 EU-konforme Blockchains

Die Konformität mit EU-Gesetzen, insbesondere der Datenschutz-Grundverordnung (DSGVO), ist für eCMR-Systeme essentiell. Blockchain-Lösungen, die den europäischen Datenschutz- und Sicherheitsstandards entsprechen, können die rechtskonforme Verarbeitung und Speicherung von eCMR-Daten gewährleisten. Der Einsatz von EU-konformen Blockchains kann das Vertrauen in das eCMR-System erhöhen und seine Akzeptanz bei den Nutzern verbessern, indem die Sicherheit ihrer Daten und die Einhaltung der gesetzlichen Vorschriften sichergestellt wird.

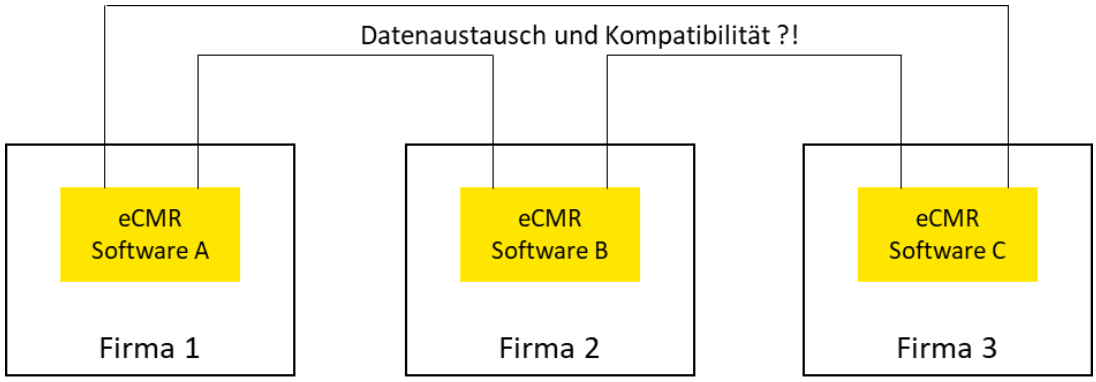
3 Geschäftsmodell

Im Kontext des eCMR-Protokolls können unterschiedliche Geschäftsmodelle zum Einsatz kommen, von denen die folgenden Beispiele lediglich einen Auszug darstellen und keinen Anspruch auf Vollständigkeit erheben.

3.1 Geschäftsmodelle im Kontext eCMR-Protokolls

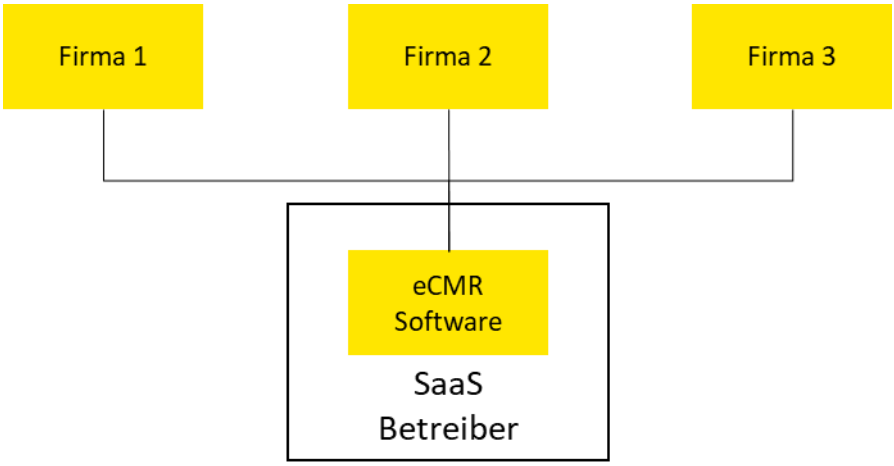
3.1.1 Traditionelle Software

Bei diesem Ansatz erwerben oder lizenzieren Kunden eine Software, die innerhalb ihrer eigenen IT-Infrastruktur implementiert wird. Angesichts der Heterogenität des Logistikmarktes kann dies zu einer breiten Palette kundenspezifischer Implementierungen führen. Obwohl das eCMR-Protokoll theoretisch die Datenkompatibilität zwischen unterschiedlichen Systemen gewährleistet, ist die Kompatibilität der verschiedenen Softwarelösungen hinsichtlich der Schnittstellen für den Datenaustausch nicht immer sichergestellt. Dieses Modell erfordert daher eine sorgfältige Planung und Abstimmung, um die reibungslose Kommunikation zwischen den Systemen verschiedener Kunden zu ermöglichen.



3.1.2 Software-as-a-Service

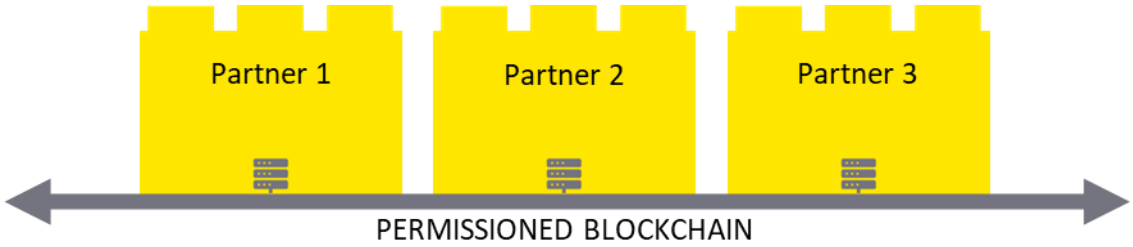
Beim SaaS-Modell ist es für Kunden nicht notwendig, eine eigene IT-Infrastruktur zu unterhalten. Stattdessen werden die vorhandenen IT-Systeme und Logistikprozesse in eine Cloud-basierte Lösung integriert, die von einem externen Dienstleister verwaltet und kontinuierlich weiterentwickelt wird. Dies ermöglicht es den Kunden, von Skaleneffekten zu profitieren, da sie sich entweder eine gemeinsame Plattform mit anderen Nutzern teilen oder eine dedizierte private Lösung erhalten können. Unabhängig von der gewählten Konfiguration ist der effiziente Datenaustausch mit Systemen anderer Teilnehmer ein kritischer Aspekt dieses Modells. Es bietet eine flexible und kosteneffiziente Möglichkeit, ohne die Notwendigkeit, in Hardware oder Software-Lizenzen zu investieren, auf das eCMR-Protokoll zuzugreifen und dieses zu nutzen.



3.1.3 Permissioned Blockchain (Privates Netzwerk)

In diesem Modell werden alle Anwender einer spezifischen technischen Lösung zu Teilnehmern eines exklusiven, privaten Blockchain-Netzwerks. Dies gewährleistet, dass ausschließlich autorisierte Netzwerkmitglieder Zugang zu den sensiblen Daten erhalten. Darüber hinaus bietet das Modell die Möglichkeit für jeden Kunden, entweder selbst einen Knotenpunkt im Netzwerk zu betreiben oder diese Aufgabe an einen spezialisierten IT-Dienstleister zu übergeben.

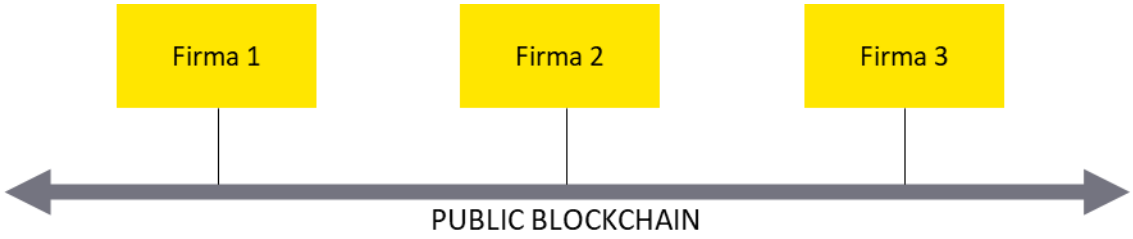
Die besondere Stärke dieses Ansatzes liegt in der dezentralen Natur der Blockchain. Sie bietet einen robusten Schutz gegen Datenmanipulation, da die Daten über das gesamte Netzwerk verteilt gespeichert werden und jede Veränderung von der Mehrheit der Knoten validiert werden muss. So entsteht ein hohes Maß an Datensicherheit und Vertrauen zwischen den Teilnehmern, ohne dass eine einzelne zentrale Instanz benötigt wird. Dieses Modell eignet sich besonders für Anwendungen, bei denen Datenschutz, Sicherheit und Authentizität der Daten von höchster Bedeutung sind.



3.1.4 Public Blockchain (Öffentliches Netzwerk)

Dieses Modell basiert auf der Nutzung einer öffentlichen Blockchain, wodurch der Aufbau und Betrieb eines separaten, privaten Netzwerks überflüssig wird. Die Nutzung einer öffentlichen Blockchain ermöglicht es allen Teilnehmern, auf eine gemeinsame Plattform zuzugreifen. Allerdings ist bei diesem Ansatz besondere Vorsicht geboten, welche Daten in die Blockchain eingetragen werden, da sämtliche Informationen öffentlich einsehbar sind.

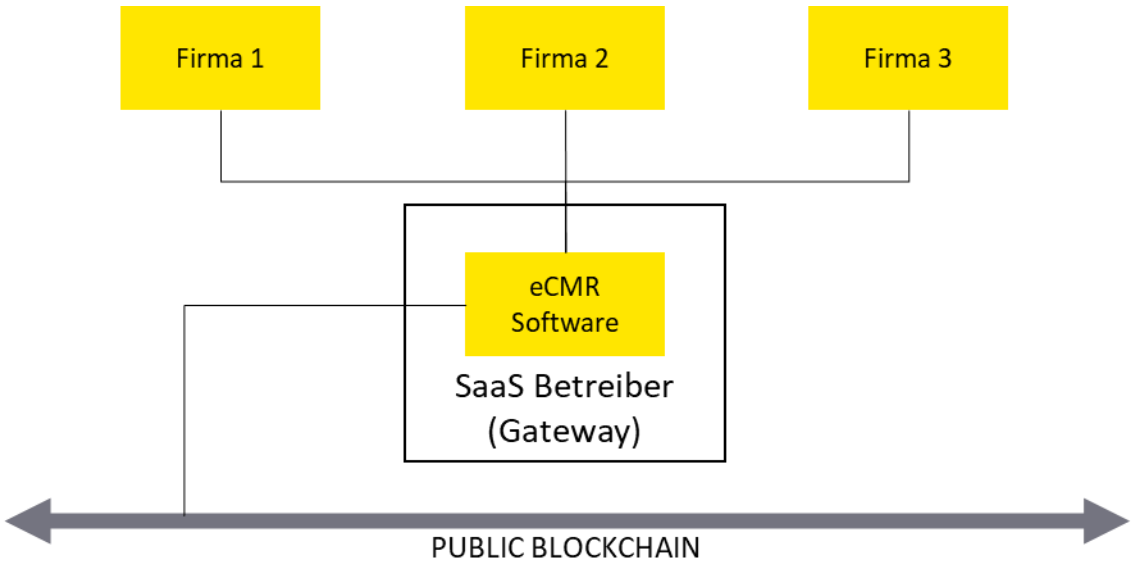
Zusätzlich müssen potenzielle Schwankungen der Transaktionsgebühren berücksichtigt werden, die finanzielle Auswirkungen haben können. Ein wesentlicher Nachteil dieses Modells ist aktuell das Fehlen eines einheitlichen Token-Standards für eCMR-Dokumente sowie spezifischer Smart Contracts für die Automatisierung gemäß dem eCMR-Protokoll. Dies schränkt die Interoperabilität zwischen verschiedenen Parteien, wie Unternehmen innerhalb der Logistikbranche, ein und kann die nahtlose Integration und den universellen Einsatz des eCMR-Protokolls erschweren.



3.1.5 Public Blockchain Gateway (Öffentliches Netzwerk)

In Ermangelung eines standardisierten Token-Systems für eCMR-Dokumente bietet sich die Nutzung einer speziell entwickelten Software als Gateway zu einer öffentlichen Blockchain an. Diese Software dient als Schnittstelle, die das eCMR-Protokoll integriert und so den Zugang zur Blockchain für alle Beteiligten ermöglicht. Durch diese Konstruktion interagieren die teilnehmenden Parteien mittelbar mit der Blockchain über das Gateway, wodurch die technologischen Vorteile der Blockchain, insbesondere in Bezug auf Unveränderlichkeit und Transparenz der Daten, erhalten bleiben.

Dieses Modell nutzt somit die Kernfunktionalitäten der Blockchain-Technologie, ohne dass für die eCMR-Dokumente ein eigener Token-Standard existieren muss. Es stellt eine praktikable Lösung dar, die die Einführung und Nutzung des eCMR-Protokolls in einem breiteren Rahmen ermöglicht, indem es die Vorteile der Blockchain zugänglich macht und gleichzeitig die Herausforderungen der Standardisierung und Interoperabilität adressiert.



3.2 Evolution des Geschäftsmodells

Die Implementierung des Projekts durchlief mehrere Entwicklungsphasen, beginnend mit der Idee, ein Konsortium aus unterschiedlichen Unternehmenspartnern zu gründen. Dieses Konsortium sollte ein privates Netzwerk (Permissioned Blockchain) betreiben, um eCMR-Dokumente zu verarbeiten und zu speichern. Der Plan sah vor, dass weitere Partner leicht an das System angeschlossen werden könnten und optional durch den Betrieb eigener Blockchain-Knoten zum Netzwerk beitragen, was das Vertrauen in die verarbeiteten Daten gestärkt hätte. Aufgrund unterschiedlicher Interessen und Zielsetzungen der beteiligten Partner wurde diese Idee jedoch verworfen.

Als Alternative wurde ein hybrides Modell entwickelt, das eine klassische Software-Anwendung für die Verwaltung und Speicherung von Daten außerhalb der Blockchain (off-chain) nutzt, während entscheidende Daten wie der digitale Fingerabdruck eines Dokuments auf einer öffentlichen Blockchain (on-chain) gesichert werden. Dieses Modell erfordert eine eigene IT-Infrastruktur für die Off-Chain-Komponenten und deren Betrieb.

In der Testphase wurde das hybride Modell in zwei Varianten erprobt: einer direkten Integration in die IT-Umgebung des Kunden und einer Betreibung durch einen neutralen Dritten, um Vertrauensprobleme zwischen den Teilnehmern zu adressieren. Letztlich fand sich kein Kunde für den produktiven Einsatz, was eine finale Entscheidung über das Geschäfts- und Preismodell verhinderte. Trotzdem wird für die Zukunft ein Basispreismodell mit zusätzlichen volumenabhängigen Gebühren, basierend auf der Anzahl der eCMR-Dokumente und der beteiligten Parteien, empfohlen.

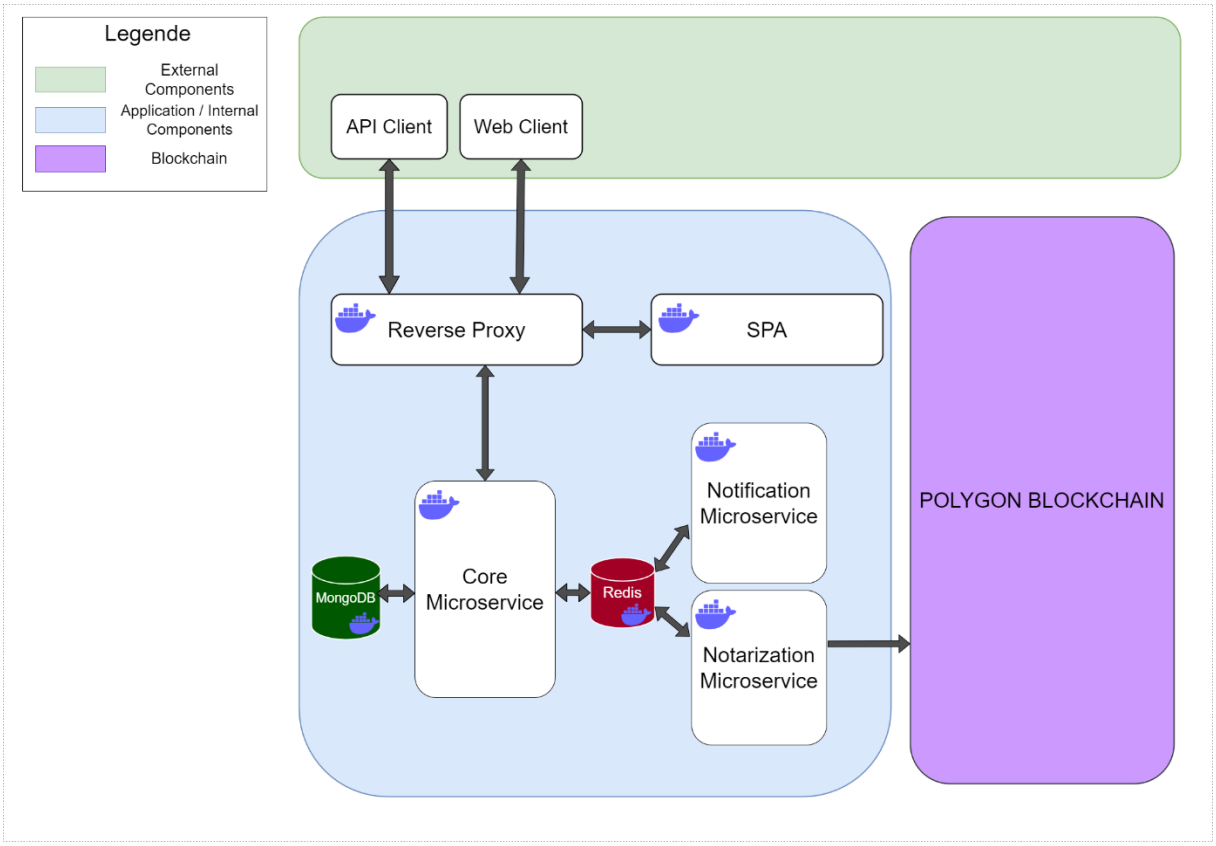
4 Systembeschreibung

4.1 Systemarchitektur

Das Projekt realisiert eine beispielhafte Umsetzung des eCMR-Protokolls durch eine hybride Lösung. Diese speichert kritische Daten wie eCMR-Dokumente und deren Anhänge in einer Softwarelösung, die auf jeglicher IT-Infrastruktur betrieben werden kann. Für die Cloud-Infrastruktur wurde Microsoft Azure gewählt. Zusätzlich werden bestimmte Daten, insbesondere solche, die nicht direkt lesbar sein sollen, auf einer öffentlichen Blockchain gesichert. Diese Maßnahme schützt die originalen, möglicherweise sensiblen Daten vor Rekonstruktion und nutzt gleichzeitig die Stärken der Blockchain-Technologie – vor allem die Unveränderlichkeit der Daten – zur Sicherstellung der Dokumentenintegrität.

Die Architektur der Lösung teilt sich in zwei Bereiche. Off-Chain (außerhalb der Blockchain) für die Speicherung und Verwaltung der eCMR-Dokumente und On-Chain (auf der Blockchain) für die Sicherung der Datenintegrität durch die Unveränderlichkeit der Blockchain. Der Off-Chain-Bereich basiert auf einer Microservice-Architektur, welche die Anwendung in kleinste, unabhängige Dienste gliedert, die über definierte Schnittstellen miteinander kommunizieren. Diese Struktur fördert die Modularität und Flexibilität der Lösung, ermöglicht eine einfache Skalierbarkeit und gewährleistet, dass Änderungen oder Erweiterungen an einem Service die Funktionalität anderer Services nicht beeinträchtigen. Die Entscheidung für diese Architektur beruht auf der Notwendigkeit, eine wachsende Menge an eCMR-Dokumenten effizient zu verarbeiten und dabei eine hohe Systemleistung und Flexibilität zu gewährleisten.

Weitere Einzelheiten zur technischen Infrastruktur und deren Komponenten werden in Kapitel 4.5 näher erläutert.



4.2 Systemarchitektur: Die Microservices im Detail

Die Systemarchitektur der eCMR-Protokollimplementierung basiert auf einer Microservices-Architektur, die sich durch Modularität und Flexibilität auszeichnet. Im Folgenden werden die Schlüsselkomponenten dieser Architektur vorgestellt:

Core Microservice

Dieser zentrale Dienst beinhaltet die Hauptlogik der Anwendung. Er empfängt eCMR-Dokumente über REST-APIs, einer Technologie, die den Austausch von Daten über das Internet mittels standardisierter HTTP-Methoden ermöglicht. Diese Schnittstellen zeichnen sich durch Einfachheit und Flexibilität aus, was die Integration in diverse Systeme vereinfacht. Der Core Microservice ist verantwortlich für die Verwaltung, Validierung und Verarbeitung der eCMR-Dokumente, einschließlich der Erstellung von PDF-Versionen für den Benutzer. Zudem übernimmt er wichtige Funktionen wie die Authentifizierung externer Anwendungen, die Autorisierung von Nutzern und die Verwaltung von Benutzerrollen und Rechten.

Notification Microservice

Dieser Dienst kümmert sich um die Benachrichtigung von Benutzern, die in den Prozess des eCMR-Dokuments involviert sind, z.B. wenn eine digitale Unterschrift erforderlich ist. Durch den Versand von Benachrichtigungen via E-Mail und SMS, die einen direkten Link zum Dokument enthalten, ermöglicht dieser Service eine zeitnahe Kommunikation mit den Stakeholdern.

Notarization Microservice

Er schafft eine Verbindung zur öffentlichen Blockchain und ist spezialisiert auf das Schreiben von digitalen Fingerabdrücken (Hashwerten) der eCMR-Dokumente in die Blockchain. Diese Hashwerte, die im Core Microservice generiert werden, garantieren die Unveränderlichkeit und Authentizität der Dokumente und stärken das Vertrauen in die dokumentierte Lieferkette.

Single Page Application (SPA)

Die SPA bildet die Benutzeroberfläche, über die Nutzer auf alle eCMR-Dokumente zugreifen, einzelne Dokumente verwalten und administrative Aufgaben wie die Benutzerverwaltung durchführen können. Ihre Fähigkeit, ein konsistentes und reaktionsschnelles Nutzererlebnis auf unterschiedlichen Geräten zu bieten, resultiert aus der dynamischen Aktualisierung von Inhalten auf einer einzigen Webseite.

Reverse Proxy

Diese Komponente spielt eine entscheidende Rolle in der Sicherstellung der reibungslosen Kommunikation zwischen den externen Anwendungen und den Microservices. Sie dient als Zwischenschicht, die für Lastverteilung, Routing, Sicherheit und Übersetzung von Protokollen zuständig ist, und trägt damit zur Leistungsfähigkeit und Sicherheit der gesamten Architektur bei.

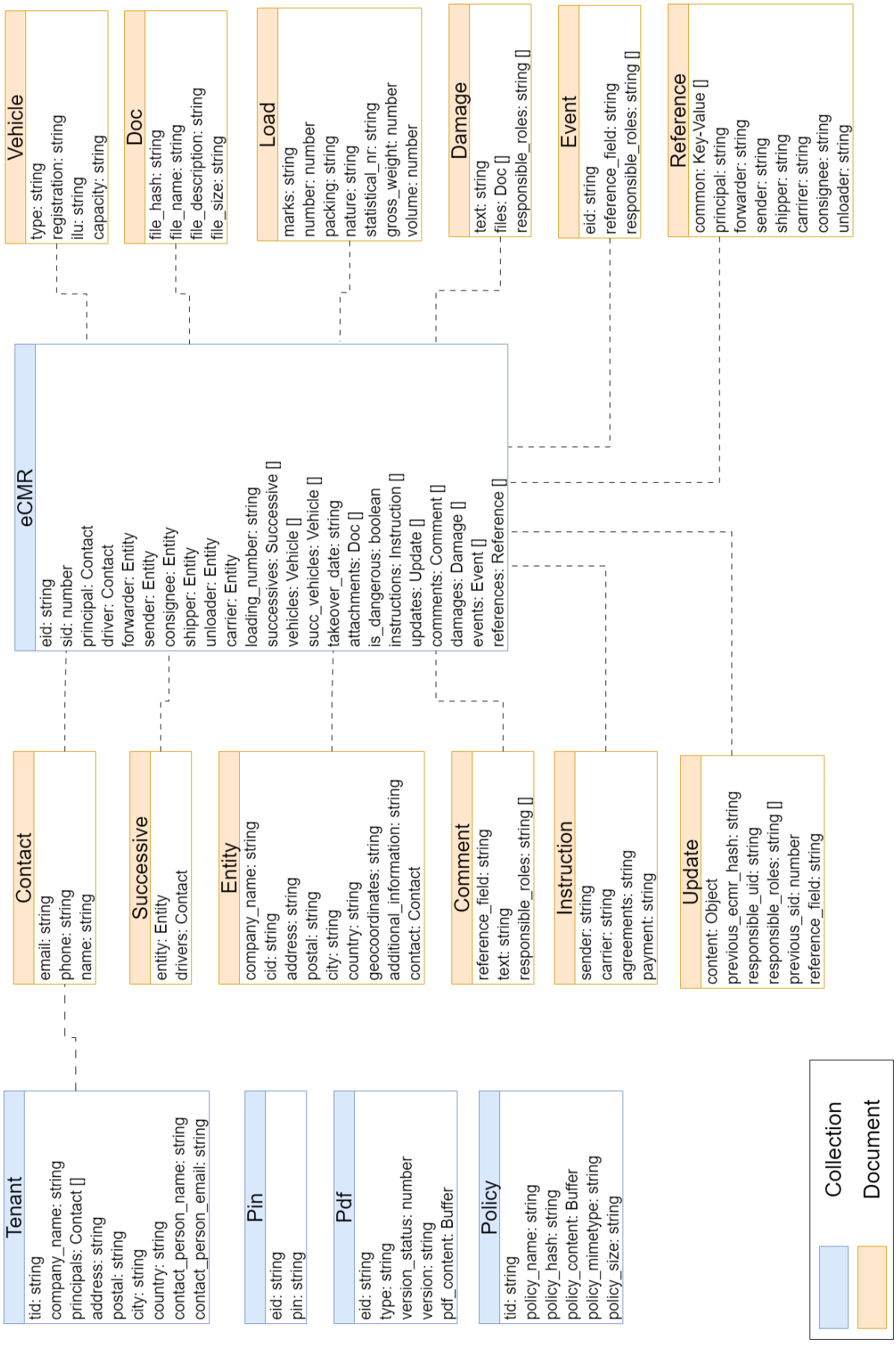
4.3 Datenmodell und Dateninfrastruktur

Das hier vorgestellte eCMR-System setzt auf MongoDB, eine flexible NoSQL-Datenbank, die ein schemaloses Dokumentdatenmodell nutzt. Dieses Modell ist besonders für die Verarbeitung und Speicherung von strukturierten Daten in Form von Dokumenten konzipiert, die in Sammlungen organisiert sind.

Sammlungen: Diese fungieren ähnlich wie Tabellen in relationalen Datenbanken, bieten jedoch mehr Flexibilität. Sie erlauben eine variable Struktur der enthaltenen Dokumente, ohne ein starres Schema vorzuschreiben. Dadurch können Dokumente innerhalb derselben Sammlung unterschiedliche Datenfelder aufweisen.

Dokumente: Als grundlegende Dateneinheiten speichern Dokumente Informationen in Form von Schlüssel-Wert-Paaren. Sie können vielfältige Datentypen enthalten, von Text und Zahlen bis hin zu Arrays und eingebetteten Dokumenten. Die flexiblen Strukturen der Dokumente, typischerweise im JSON-Format, erlauben eine dynamische Anpassung an unterschiedliche Datenanforderungen.

Um die Verarbeitung großer Datenmengen effizient zu bewältigen, ist ein schneller Zugriff auf die Daten entscheidend. Hier kommt Redis ins Spiel, eine In-Memory-Datenbank, die als Caching-Lösung dient. Redis ergänzt MongoDB, indem es die Abfragegeschwindigkeit erhöht und somit die Systemleistung verbessert. Es speichert Indizes und Verknüpfungen, die einen raschen Zugriff auf häufig benötigte eCMR-Dokumente und zugehörige Daten ermöglichen. Die Kombination aus MongoDB für die dauerhafte Datenspeicherung und Redis für das Caching stellt sicher, dass das System auch unter hoher Last schnell und zuverlässig reagiert.


Vehicle
type: string
registration: string
ilu: string
capacity: string
Doc
file_hash: string
file_name: string
file_description: string
file_size: string
Load
marks: string
number: number
packing: string
nature: string
statistical_nr: string
gross_weight: number
volume: number
Damage
text: string
files: Doc []
responsible_roles: string []
Event
eid: string
reference_field: string
responsible_roles: string []
Reference
common: Key-Value []
principal: string
forwarder: string
sender: string
shipper: string
carrier: string
consignee: string
unloader: string
eCMR
eid: string
sid: number
principal: Contact
driver: Contact
forwarder: Entity
sender: Entity
consignee: Entity
shipper: Entity
unloader: Entity
carrier: Entity
loading_number: string
successives: Successive []
vehicles: Vehicle []
succ_vehicles: Vehicle []
takeover_date: string
attachments: Doc []
is_dangerous: boolean
instructions: Instruction []
updates: Update []
comments: Comment []
damages: Damage []
events: Event []
references: Reference []
Contact
email: string
phone: string
name: string
Successive
entity: Entity
drivers: Contact
Entity
company_name: string
cid: string
address: string
postal: string
city: string
country: string
geocoordinates: string
additional_information: string
contact: Contact
Comment
reference_field: string
text: string
responsible_roles: string []
Instruction
sender: string
carrier: string
agreements: string
payment: string
Update
content: Object
previous_ecmr_hash: string
responsible_uid: string
responsible_roles: string []
previous_sid: number
reference_field: string
Tenant
tid: string
company_name: string
principals: Contact []
address: string
postal: string
city: string
country: string
contact_person_name: string
contact_person_email: string
Pin
eid: string
pin: string
Pdf
eid: string
type: string
version_status: number
version: string
pdf_content: Buffer
Policy
tid: string
policy_name: string
policy_hash: string
policy_content: Buffer
policy_mimetype: string
policy_size: string
Collection
Document

4.4 Interfaces (Schnittstellen)

Die eCMR-Lösung wurde mit einigen Programmierschnittstellen (APIs) ausgestattet, welche eine reibungslose Integration in bestehende IT-Systeme wie ERP, TMS und Yard Management ermöglichen. Diese RESTful APIs ermöglichen die effiziente Kommunikation und den Datenaustausch zwischen verschiedenen Systemkomponenten. Nachfolgend eine vereinfachte Übersicht der Schnittstellen.

eCMR-Interface für Administratoren:

- **/v1/admin/ecmr/report**: Ermittlung der Gesamtzahl der eCMRs.
- **/v1/admin/ecmr**: Abruf einer Liste aller eCMRs.
- **/v1/admin/ecmr/{id}/pdf**: Abruf der PDF-Datei eines spezifischen eCMRs.
- **/v1/admin/ecmr/{id}/pdflist**: Auflistung aller PDF-Dateien eines spezifischen eCMRs.
- **/v1/admin/ecmr/{id}**: Löschen eines spezifischen eCMRs.

eCMR-Interface für Principals und weitere Rollen:

- **/v1/ecmr**: Erstellung eines neuen eCMR.
- **/v1/ecmr**: Abruf einer Liste aller eCMRs.
- **/v1/ecmr/{id}**: Bearbeitung eines spezifischen eCMR.
- **/v1/ecmr/{id}**: Abruf eines spezifischen eCMR.
- **/v1/ecmr/{id}/pdf**: Abruf der PDF-Datei eines spezifischen eCMRs.
- **/v1/ecmr/{id}/pdflist**: Auflistung aller PDF-Dateien eines spezifischen eCMRs.

Alle API-Endpunkte unterstützen grundlegende CRUD-Operationen (Create, Read, Update, Delete) für eine effiziente Verwaltung der eCMR-Dokumente. Die Sicherheit dieser Endpunkte wird durch die Vergabe von persönlichen Zugriffstokens (JWTs; Java Web Token) gewährleistet, die eine eindeutige und sichere Identifikation der Benutzer ermöglichen. Diese Tokens haben eine Gültigkeitsdauer von zwei Wochen und können bei Bedarf verlängert werden.

Um die Nutzer über wichtige Prozessschritte zu informieren, nutzt die Lösung einen Notification-Service, der Benachrichtigungen via E-Mail und SMS versendet. Dieser Service ist flexibel konfigurierbar, sodass externe Dienstleister je nach Bedarf ausgewählt und gewechselt werden können.

4.5 IT-Infrastruktur

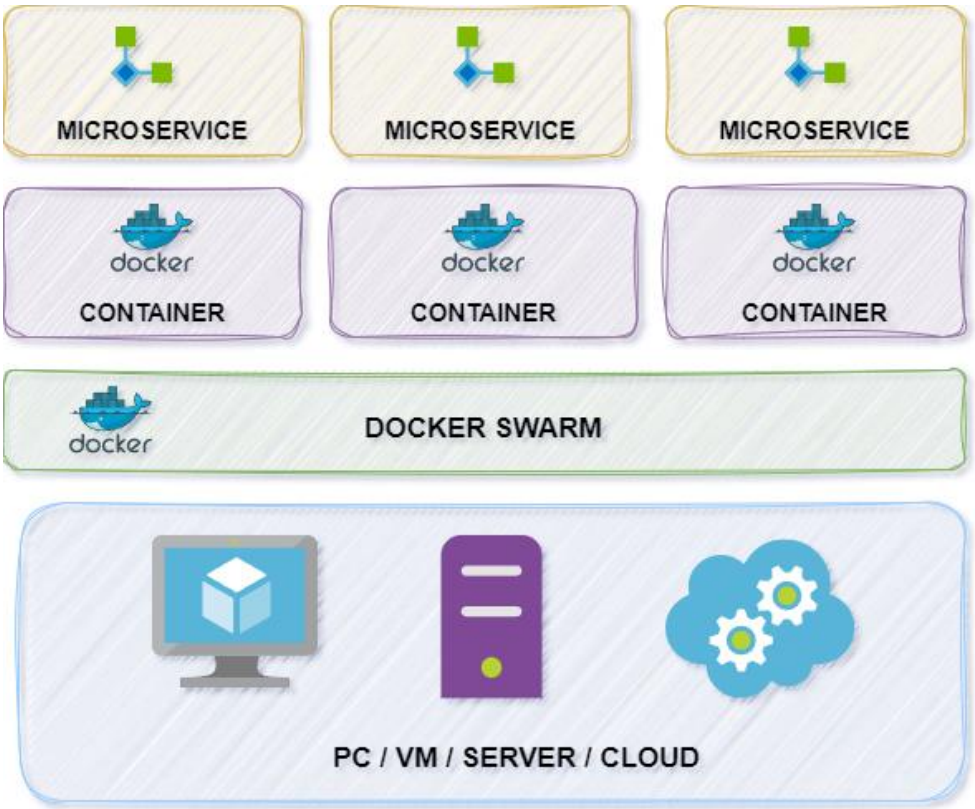
Die technische Umsetzung des Projekts basiert auf einer Microservice-Architektur, wobei sämtliche Microservices mithilfe von Docker containerisiert wurden. Durch die Containerisierung wird jeder Microservice inklusive seines Codes, der benötigten Laufzeitumgebung, Systemtools, Bibliotheken und Konfigurationen in einem eigenständigen Container gekapselt. Dies sorgt für eine einheitliche Ausführungsumgebung und ermöglicht es, die Microservices unabhängig voneinander zu

entwickeln, zu testen und bereitzustellen. Der Einsatz von Containern gewährleistet eine hohe Konsistenz und Portabilität über verschiedene Einsatzumgebungen hinweg, wie zum Beispiel On-Premise Rechenzentren bis hin zu Cloud-Umgebungen.

Zur Verwaltung dieser Container kommt Docker Swarm zum Einsatz, eine leistungsstarke Orchestrierungsplattform. Docker Swarm erleichtert die Verwaltung von Containern auf einem Cluster von Maschinen, indem es Funktionen wie automatische Verteilung, Skalierung und Fehlerbehandlung bietet. Mit Docker Swarm können Microservices flexibel

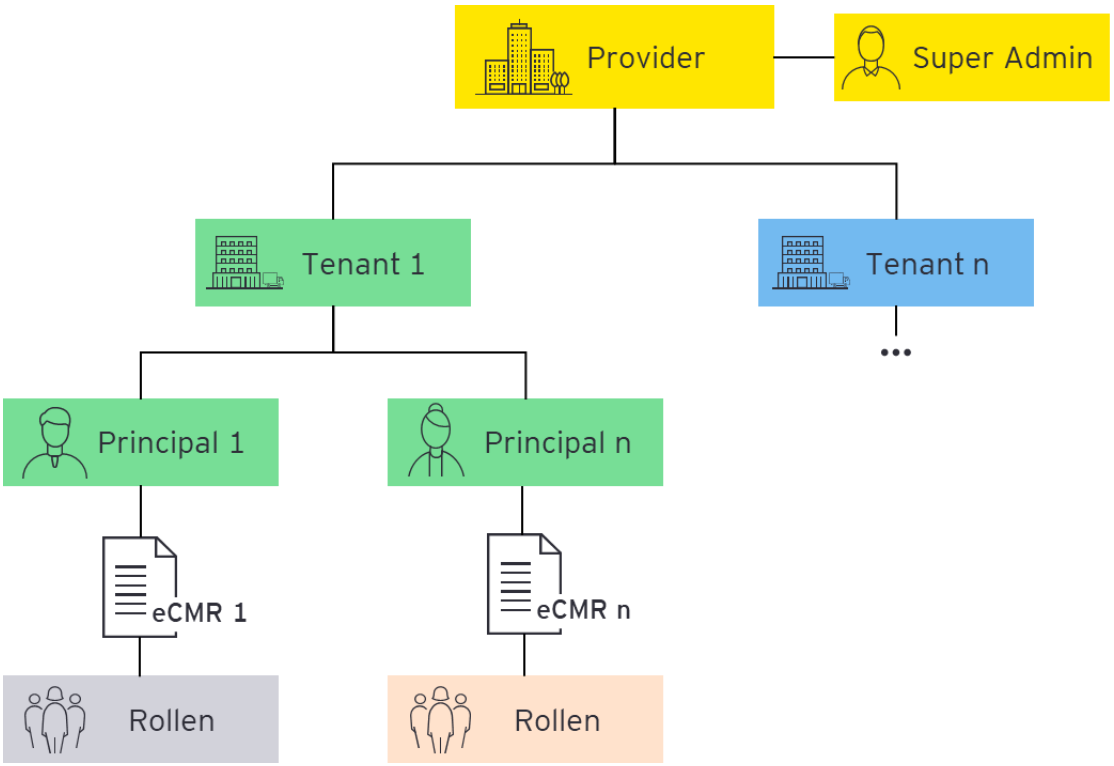
- Über physische oder virtuelle Server, sowohl in privaten Rechenzentren als auch
- in der Cloud, sowie
- in lokalen Entwicklungsumgebungen oder
- in hybriden Konfigurationen bereitgestellt werden.

Die Nutzung von Docker Swarm unterstützt eine effiziente und skalierbare Bereitstellung der Microservices und fördert die Agilität des Entwicklungsprozesses. Diese Technologie stellt sicher, dass die eCMR-Lösung zuverlässig funktioniert, leicht skaliert und nahtlos in bestehende IT-Infrastrukturen integriert werden kann.



2.5 Rollen und Rechte

Ein zentrales Element der Systemarchitektur ist das klar definierte Modell der Rollen und Rechte, das die Organisationsstruktur und die Beziehungen der verschiedenen Stakeholder innerhalb des Systems abbildet. Dieses Modell ist entscheidend für die Sicherstellung einer effizienten und sicheren Datenverarbeitung und -verwaltung.



Das Rollen- und Rechtemodell dient als Grundlage für die Implementierung von Sicherheits- und Zugriffskontrollmechanismen, die sicherstellen, dass jeder Benutzer nur auf die für seine Rolle relevanten Informationen und Funktionen zugreifen kann. Durch die klare Definition und Trennung der Rollen wird zudem die Transparenz innerhalb des Systems erhöht und die Grundlage für eine nachvollziehbare und vertrauenswürdige Datenverarbeitung geschaffen.

5 Technische Innovationsmerkmale

5.1 Blockchain

Die Implementierung innerhalb dieses Projekts setzt auf die Blockchain-Technologie, um die Authentizität von Dokumenten langfristig sicherzustellen. Ein zentrales Element ist die Erstellung und Speicherung eines digitalen Fingerabdrucks – generiert aus den Daten des Dokuments und der dazugehörigen Unterschrift – in der Blockchain. Die Identität dieses Fingerabdrucks zu einem späteren Zeitpunkt erneut zu überprüfen, ermöglicht es die Unverfälschtheit der Originaldaten zu verifizieren.

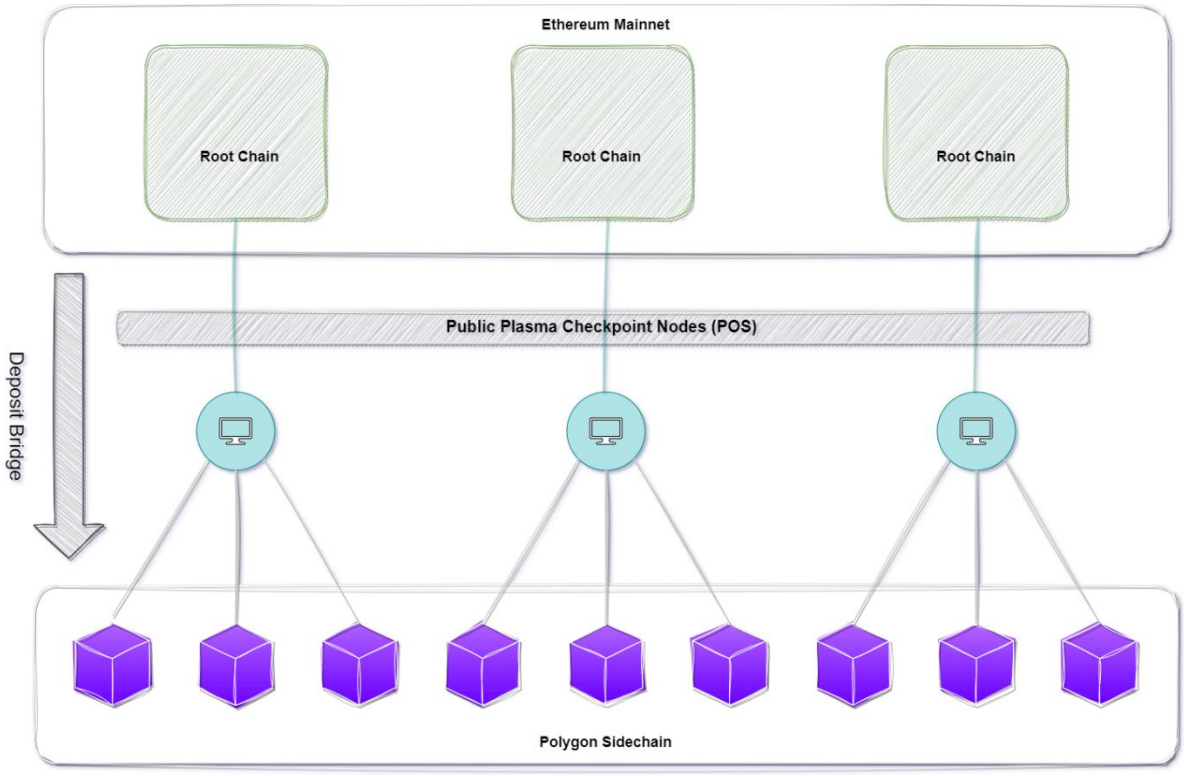


Figure 4: Beziehung zwischen Layer 1 (Ethereum) und Layer 2 (Polygon)

Für die Umsetzung wurde primär Ethereum (Layer 1) als Blockchain-Plattform ausgewählt. Trotz ihrer Vorteile birgt diese Wahl auch Herausforderungen, wie schwankende Transaktionsgebühren und eine geringe Rate an Transaktionen. Um diese Einschränkungen zu umgehen, kommt zusätzlich Polygon (Layer 2) zum Einsatz. Polygon optimiert die Transaktionskosten und -geschwindigkeit und unterstützt somit eine effizientere Durchführung von Blockchain-Transaktionen.

Sicherheit und Konsens durch Proof of Stake (PoS)

Polygon nutzt den Proof of Stake (PoS)-Mechanismus, der eine zentrale Rolle im Netzwerk spielt:

- **Validatoren** sind für das Vorschlagen und Validieren neuer Blöcke verantwortlich. Ihre Auswahl basiert auf dem Anteil der gehaltenen Kryptowährung (MATIC), was einen Anreiz für die Sicherheit und Zuverlässigkeit des Netzwerks schafft.

- **Staking** erfordert, dass Validatoren eine Sicherheitsleistung in MATIC hinterlegen, was deren Engagement für das Netzwerk unterstreicht.

- **Konsensfindung** erfolgt durch die Zustimmung einer Mehrheit der Validatoren zu einem neuen Block, wodurch dessen Gültigkeit bestätigt und in die Blockchain aufgenommen wird.

- **Belohnungen und Strafen** motivieren Validatoren zur korrekten Ausführung ihrer Aufgaben, indem erfolgreiche Blockvalidierungen belohnt und Verstöße bestraft werden.

Dezentralisierung und Nachhaltigkeit

Das PoS-System von Polygon fördert eine energieeffiziente und umweltfreundlichere Alternative zum traditionellen Proof of Work (PoW), erhöht die Transaktionsgeschwindigkeit und garantiert durch eine breite Netzwerkvalidierung die Sicherheit und Unveränderlichkeit der gespeicherten Daten.

Durch die Kombination von Ethereum und Polygon bietet das Projekt eine robuste, skalierbare und sicherheitsorientierte Blockchain-Lösung, die die Integrität und Authentizität von Dokumenten effektiv gewährleistet und gleichzeitig die Herausforderungen hinsichtlich Skalierbarkeit und Kosten adressiert.

5.2 Advanced Electronic Signature (AdES)

5.2.1 Voraussetzungen für eine Unterschrift gemäß Art 3 eCMR-Protokoll

Durch den Ministerratsvortrag vom 13. März 2024 [3] ist der Beitritt Österreichs zum eCMR-Protokoll eingeleitet. Es wird daher vermutet, dass die Regelungen des eCMR-Protokolls in naher Zukunft in Österreicht rechtsgültig sind. Gemäß der Anlagen [6] (Seite 6) ist davon auszugehen, dass eine elektronische Signatur als Unterschrift angewendet werden kann.

Artikel 3 des eCMR-Protokoll der deutschen Übersetzung [4] als Anlage zum Ministerratsvortrag [3] definiert folgendes:

(1) „Der elektronische Frachtbrief ist von den Parteien des Beförderungsvertrags mit Hilfe einer zuverlässigen elektronischen Signatur zu authentifizieren, mit der deren Verknüpfung mit dem elektronischen Frachtbrief gewährleistet wird. Bis zum Beweis des Gegenteils wird die Zuverlässigkeit einer Methode zur Erstellung der elektronischen Signatur vermutet, wenn die elektronische Signatur

*a) **ausschließlich** dem Unterzeichner **zugeordnet** ist,*

*b) die **Identifizierung** des Unterzeichners ermöglicht,*

*c) mit **Mitteln** erstellt wird, die der **Unterzeichner unter seiner alleinigen Kontrolle halten kann**, und*

*d) so mit den Daten, auf die sie sich bezieht, verknüpft ist, dass eine **nachträgliche Veränderung der Daten erkannt werden kann**.*

(2) *Der elektronische Frachtbrief kann auch durch jede andere Methode der elektronischen Authentifizierung authentifiziert werden, die nach dem Recht des Staates, in dem der elektronische Frachtbrief ausgestellt worden ist, zulässig ist.*

(3) *Die in dem elektronischen Frachtbrief enthaltenen Angaben sind jeder dazu berechtigten Partei zugänglich*."

Es ist anzumerken, dass im CMR und eCMR-Protokoll nicht geregelt ist, wer zu den in Punkt (3) genannten Parteien gehört. Die offene Formulierung lässt jedenfalls Interpretationsspielraum offen; eine vernünftige Auslegung kann darunter (i) die Parteien des Frachtvertrags, (ii) an der Durchführung Beteiligte (zB Empfänger), oder (iii) weitere Interessierte (zB Behörden) verstehen.[1]

Artikel 3 stellt jedoch eine Vermutung für die Zuverlässigkeit einer elektronischen Signatur auf. Sofern die unter (a) bis (d) dargelegten Kriterien von einer elektronischen Signatur erfüllt sind, gilt eine solche elektronische Signatur laut Artikel 3 eCMR-Protokoll als zuverlässig. Erst ein Beweis des Gegenteils kann diese (Rechts-)Vermutung entkräften.

5.2.2 Vergleich mit fortgeschrittener elektronischer Signatur gem Art 26 eIDAS-VO

In der Anlage [6] (Seite 6) zum Ministerratsvortrag vom 13. März 2024 [3] wird erläutert, dass die Definition der „fortgeschrittenen elektronischen Signatur" im eCMR-Protokoll im Wesentlichen der Signatur-RL entnommen wurden und Art. 3 Nr. 11 iVm Art. 26 der eIDAS-VO, welche die Signatur-RL ersetzt hat, die fortgeschrittene elektronische Signatur abweichend davon definiert. Da die Anforderungen an eine fortgeschrittene elektronische Signatur nach der eIDAS-VO im Wesentlichen aber den früheren Anforderungen nach der Signatur-RL entsprechen, ist davon auszugehen, dass eine fortgeschrittene elektronische Signatur nach der eIDAS-VO die Anforderungen nach Art. 3 Abs. 1 Satz 2 des Zusatzprotokolls erfüllt und dadurch die darin normierte Beweisvermutung eintritt.

5.2.3 Anforderungen nach Art 26 eIDAS-VO

Eine *fortgeschrittene* elektronische Signatur nach Art 26 eIDAS-VO verlangt einen **geheimen**, privaten, nur dieser Person zugeordneten **Schlüssel** des Unterzeichnenden, mit dem er das elektronische Dokument so verschlüsseln kann, dass dessen **nachträgliche Veränderung zu erkennen** ist.[2]

Die elektronische Form basiert auf dem **asymmetrischen Verschlüsselungsverfahren** (kryptografischen Verfahren)[3], das durch den Einsatz von zwei verschiedenen Schlüsseln gekennzeichnet ist, nämlich zum einen dem geheimen privaten und zum anderen dem für jedermann zugänglichen öffentlichen Schlüssel. Der öffentliche Schlüssel (Signaturvalidierungsdaten[4]) stellt eine Art Gegenstück zu dem privaten Schlüssel (Signaturerstellungsdaten[5]) dar, ohne dass sich jedoch (nach derzeitigem Stand der Erkenntnis) aus dem öffentlichen Schlüssel der private Schlüssel berechnen ließe.[6]

Praktisch bedeutet dies, dass aus dem Text des (zu verschlüsselnden) Dokuments nach einem bekannten Algorithmus der sog. Hash-Wert (vergleichbar mit einer Quersumme) errechnet und

---

[1] *Harald Schön,* Deutsches Bundesministerium der Justiz und für Verbraucherschutz, Präsentationsfolien "e-CMR – der elektronische CMR-Frachtbrief, Symposium der Deutschen Gesellschaft für Transportrecht 2021", 8 f; *Saive*, Die Zukunft der Beförderungsdokumente, RdTW 2023, 132 (134).
[2] *MüKoBGB/Einsele*, 9. Aufl. 2021, BGB § 126a Rn 9.
[3] Vgl hierzu auch ErwGr 8 Durchführungsbeschluss (EU) 2016/650 vom 25.4.2016 ABl. EU 2016 L 109, 40.
[4] Signaturvalidierungsdaten sind demnach Daten, die zur Validierung einer elektronischen Signatur (oder eines elektronischen Siegels) verwendet werden (siehe Art 3 Z 40 eIDAS-VO). Unter Validierung vesteht man den Prozess der Überprüfung und Bestätigung der Gültigkeit einer elektronischen Signatur (oder eines elektronischen Siegels) (siehe Art 3 Z 41 eIDAS-VO).
[5] Signaturerstellungsdaten sind eindeutige Daten, die vom Unterzeichner zum Erstellen einer elektronischen Signatur verwendet werden (siehe Art 3 Z 13 eIDAS-VO).
[6] *MüKoBGB/Einsele*, 9. Aufl. 2021, BGB § 126a Rn 10.

dadurch die Nachricht komprimiert wird; der errechnete Hash-Wert wird nun mit dem privaten Schlüssel des "Unterzeichnenden" verschlüsselt. **Der unverschlüsselte Text wird zusammen mit dem verschlüsselten Hash-Wert dem Empfänger übermittelt, der das verschlüsselte Komprimat mit dem Signaturprüfschlüssel öffnen kann.** Den passenden Prüfschlüssel erhält der Empfänger entweder vom Absender oder von Vertrauensdiensteanbietern, bei denen dieser Schlüssel abrufbar gehalten wird. Der Empfänger kann nun mit diesem öffentlichen Schlüssel den verschlüsselten Hash-Wert decodieren. Sodann kann er seinerseits aus dem unverschlüsselten Text nach dem bekannten Algorithmus den Hash-Wert berechnen und diesen Wert mit dem ihm übermittelten decodierten Hash-Wert vergleichen**. Stimmen diese Werte überein, wurde der Text (nach derzeitigem Erkenntnisstand) nachträglich nicht verändert, weil sich ansonsten auch der Hash-Wert geändert hätte.** Jedoch stellt auch die fortgeschrittene elektronische Signatur noch keine bestimmten Sicherheitsanforderungen an die Schlüsselverwaltung und an die Software- und Hardwareeinheiten zur Speicherung und Anwendung des jeweiligen Signaturschlüssels (Signaturerstellungsdaten).[7]

Eine fortgeschrittene elektronische Signatur muss somit jedenfalls folgende vier Voraussetzungen erfüllen:

- **einfache elektronische Signatur**: Es muss sich um Daten in elektronischer Form handen, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet.

- **Identitätsfunktion**: Die elektronische Signatur muss den Unterzeichner eindeutig identifizieren.

- **Authentizitätsfunktion**: die elektronische fortgeschrittene Signatur muss unter Verwendung elektronischer Signaturerstellungsdaten angebracht werden, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann.

- **Integrätitsfunktion**: die elektronische Signatur muss außerdem derart mit dem elektronischen Dokument verbunden werden, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

In der Praxis werden diese Voraussetzungen regelmäßig durch Nutzen einer sog. **Zwei-Faktor-Identifizierung** unter Einsatz einer von einem zertifizierten Trustcenter ausgegebenen Signaturkarte und der zugehörigen persönlichen Identifikationsnummer (PIN) erfüllt. Die fortgeschrittene elektronische Signatur reicht im elektronischen Rechtsverkehr nur dann aus, wenn für die Übermittlung des signierten Dokuments ein **sicherer Übermittlungsweg** gewählt wird.[8]

5.2.4 Ursprüngliche Annahmen

Das primäre Ziel der hier entwickelten eCMR-Lösung war es, eine für den Logistikalltag praktikable und einfach zu bedienende Digitalisierung des traditionell papierbasierten CMR-Frachtbriefs zu ermöglichen. Dabei stand im Vordergrund, den Prozess zu vereinfachen, ohne neue Komplexität einzuführen. Die Lösung sollte für alle Prozessbeteiligten – von Versendern über Spediteure und Fahrer bis hin zu Empfängern – leicht handhabbar sein, und zwar unabhängig vom Standort innerhalb der EU und unter Nutzung gängiger Endgeräte wie Smartphones und Tablets. Um dies zu erreichen, galt es, bestimmte Herausforderungen zu vermeiden.

---

[7] *MüKoBGB/Einsele*, 9. Aufl. 2021, BGB § 126a Rn 10.
[8] *BeckOK IT-Recht/Loos*, 11. Ed. 1.7.2023, ZPO § 130a Rn 21.

- **Registrierung von Benutzern:** Angesichts der vielfältigen Rollen eines Fahrers im Logistiknetzwerk und der potenziellen Interaktion mit unterschiedlichen eCMR-Plattformen sollte die Notwendigkeit einer wiederholten Registrierung vermieden werden. Eine solche Anforderung würde den Prozess unnötig komplizieren und die Nutzerfreundlichkeit beeinträchtigen.

- **Passwörter:** Die Verwaltung unterschiedlicher Passwörter für mehrere Plattformen erhöht das Risiko von Passwortverlusten und -missbrauch, was zusätzliche Sicherheitsbedenken mit sich bringt.

- **Schlüsselverwaltung (Key-Management):** Die Nutzung von Verschlüsselungsverfahren für Unterschriften, Dokumente und Kommunikation setzt ein komplexes Management von Sicherheitsschlüsseln voraus. Dies würde den Prozess für die Anwender erschweren, insbesondere in Bezug auf die Generierung, Verwaltung und Aktualisierung von Schlüsseln.

Um diese Herausforderungen zu umgehen und die Handhabung so einfach wie möglich zu gestalten, wurde eine Lösung entwickelt, bei der der Zugang zu den CMR-Dokumenten über Hyperlinks erfolgt, die per E-Mail und SMS verschickt werden. Diese Zugangsmethode setzt keine Passwörter oder komplizierte Authentifizierungsverfahren voraus und basiert auf der Annahme, dass eine per E-Mail oder SMS übermittelte Nachricht eine ausreichende Verbindung zur berechtigten Person herstellt. Diese Herangehensweise ermöglicht einen reibungslosen und unkomplizierten Prozess für alle Beteiligten.

5.2.5 Technische Umsetzung

In der aktuellen Implementierung erfolgt die allgemeine Benutzeridentifikation über eine angegebene E-Mail-Adresse oder Telefonnummer. Danach wird basierend auf der angegebenen E-Mail-Adresse oder Telefonnummer ein JWT (JSON Web Token)[9] zugewiesen und an den Benutzer gesendet, mit dem der Benutzer auf einen eCMR zugreifen, Daten aktualisieren und schließlich das Dokument signieren könnte. Darüber hinaus kann der Unterzeichnungsprozess des eCMR nur von den folgenden Stakeholdern durchgeführt werden:

- Absender, Spediteur/ Fahrer und Empfänger

Beim Signiervorgang besteht die Benutzereingabe aus Folgendem:

- Ort
- Name
- Unterschrift mittels Finger

Nach dem Signiervorgang wird einerseits eine Prüfsumme (Hashwert) über die händische Signatur (Bild) gebildet, andererseits wird der gesamte eCMR zum Zeitpunkt der Unterschrift gehasht und als eine Version des Dokuments in der Datenbank gespeichert werden. Im Unterschriftsfeld wird neben der Unterschrift der Name des Unterzeichners sowie Datum und Uhrzeit der Unterschrift im Klartext dargestellt. Diese Prüfsumme ist ein digitaler Fingerabdruck, welcher aus den Daten des Dokuments und der digitale Unterschrift (Schriftzug) gebildet wird. Er ist nicht mit dem

[9] JSON Web Token stellt ein kryptographisch erstellter Token dar (948 alphanumerische Zeichen), der für einen begrenzten Zeitraum gültig ist, um in einer gewissen Rolle auf das System zugreifen zu können.

biometrischen Fingerabdruck einer Person zu verwechseln. Es werden keine biometrischen Daten im System verarbeitet oder gespeichert.

Unter Berücksichtigung des vorgenannten Vorgehens lässt sich ableiten, dass die Anforderungen an eine fortgeschrittene elektronische Signatur auf folgende Weise erfüllt sind:

Die Signatur ist eindeutig mit dem Unterzeichner verknüpft

- Nur Personen mit einem gültigen JWT können das Dokument unterschreiben
- JWT (JSON Web Token) wird gespeichert, und es kann nachvollzogen werden an welche Email Adresse/Tel. Nummer er gesendet wurde
- Die Unterschrift mittels Finger ist einem Unterschreiber zuzuordnen (wie eine normale Stift auf Papier Unterschrift)

Die Signatur in der Lage, den Unterzeichner zu identifizieren

- Name des Unterschreibers ist im System abgespeichert und wird beim Unterschreiben in Klartext angezeigt

Die Signatur wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann

- Ein Unterschreiber hält das Handy/Tablet in der Hand und hat die Kontolle was er/sie mit Finger/Stift unterschreibt

Die Signatur ist mit den damit signierten Daten so verknüpft, dass eine spätere Änderung der Daten erkennbar ist

- Technisch gesehen, könnten die Originaldaten eines Dokuments nachträglich geändert und als neue Versionen gespeichert und wiederum mit einer Unterschrift verknüpft werden.
- Da eine Änderung des Dokuments gemäss eCMR-Protokoll jedoch nicht zulässig ist, wird in der Software sichergestellt, dass des eCMR-Dokument nach den Unterschriften nicht mehr verändert werden kann.
- Stattdessen wird je Dokument ein Anhang erzeugt, welcher Kommentare, Vorbehalte, Photos und dergleichen enthalten kann. Von diesem wird bei jeder Erweiterung eine neue Version erstellt und diese als Sicherheitsmaßnahme ebenfalls mit der Unterschrift verknüpft. Somit enthält diese Version das genaue Datum und die Uhrzeit wann die Änderungen eingetreten sind und ist als solche nicht mehr veränderbar.

5.2.6 Bewertung der Umsetzung

Eine nachträgliche Bewertung der technischen Umsetzung hat gezeigt, dass die Vermutungen hinsichtlich der Erfüllung der Anforderungen einer fortgeschrittenen Signatur nicht erfüllt sind, da

- Eine **E-Mail-Adresse** nicht garantiert einer Person zugeordnet werden kann. In der Praxis hat sich gezeigt, dass oft gemeinsam genutzte E-Mail-Postfächer genutzt werden. Der Zugriff auf diese Postfächer erfolgt zudem durch Geräte (Smartphones oder Computer), die wiederum gemeinsam genutzt werden und oftmals ohne Passwörter oder sonstige Sicherheitsmaßnahmen geschützt sind.
- Eine **SMS-Rufnummer** nicht garantiert einer Person zugeordnet werden kann. In der Praxis kommt es vor, dass Firmen s.g. Pool-Handys an Mitarbeiter ausgeben, deren Rufnummer zwar

der Firma, jedoch nicht ohne weitere Maßnahmen einer natürlichen Person zugeornet werden können.

- Der **Schriftzug einer Unterschrift** graphologisch einer Person zuzuordnen wäre, jedoch Firmen in der Praxis oft auf ein gespeichertes Bild einer Unterschrift zurückgreifen und stets dieses verwenden. In diesem Fall wäre die im Bild gespeicherte Unterschrift unter Umständen einer anderen Person zuzuordnen, als jene, die den CMR mit dem Bild bei Übergabe der Waren unterschreibt. Weiters haben in diesem Fall verschiedenen Parteien Zugriff auf die Unterschrift.

Im Vergleich mit einer fortgeschrittenen elektronischen Signatur gem Art 26 eIDAS-VO ist festzuhalten, dass lediglich (d) erfüllt ist; (c) als erfüllt vermutet werden kann und (a) und (b) nicht eindeutig erfüllt sind.

Im Vergleich zu Artikel 3 des eCMR-Protokoll ist festzuahlten, dass

- Absatz 1 (d) erfüllt ist und (c) als erfüllt vermutet werden kann während (a) und (b) nicht eindeutig erfüllt sind.
- Absatz 2 nicht erfüllt ist, da die technische Umsetzung nicht den Anforderungen einer fortgeschrittenen elektronischen Signatur gem Art 26 eIDAS-VO genügt und somit nicht als in Österreich anerkannt angenommen werden kann.
- Absatz 3 als erfüllt gilt.

Aus den o.g. Gründen ist eine Akzeptanz eines eCMR-Dokuments, so wie hier vorgestellt, durch andere EU-Länder oder Behörden nicht garantiert und eine Akzeptanz durch österreichische Gerichte fraglich. Dies gilt umso mehr, da der Beitritt Österreichs zum eCMR-Protokoll durch den Ministerratsvortrag vom 13. März 2024 [3] eingeleitet wurde. Gemäß der Anlage [6] (Seite 6) wird hier vor allem eIDAS als zielführendes Unterschriftsverfahren hervorgehoben.

6 Zusammenfassung und Ausblick

Die Entwicklung und Implementierung des eCMR-Protokolls hat eine Lösung hervorgebracht, die sich effizient in bestehende Logistikprozesse integrieren lässt, mit einem besonderen Fokus auf die Vereinfachung der Dokumentenerstellung, -bearbeitung und des Unterschriftsverfahrens. Während des Projekts stellte sich jedoch heraus, dass die elektronische Unterschrift die größte Herausforderung darstellt, da sie einerseits nutzerfreundlich und andererseits rechtlich konform gestaltet sein muss. Die derzeitige Lösung vereinfacht zwar den Umgang mit eCMR-Dokumenten, erfüllt jedoch nicht alle rechtlichen Anforderungen.

Die notwendige Anpassung des Unterschriftsprozesses würde zusätzliche Investitionen erfordern. Es ist zu erwarten, dass eine an die eIDAS-Verordnung angelehnte elektronische Unterschrift in der Praxis aufgrund der erforderlichen kryptografischen Prozesse und der fehlenden Infrastruktur für eine länderübergreifende Implementierung auf geringe Akzeptanz stoßen könnte.

Angesichts eines fragmentierten Marktes und der bis vor Kurzem fehlenden rechtlichen Grundlagen konnte das Geschäftsmodell nicht abschließend entwickelt und evaluiert werden. Eine abwartende Haltung potenzieller Kunden rechtfertigt derzeit keine weiteren Investitionen. Dennoch wird dem Produkt und dem Geschäftsmodell ein erhebliches zukünftiges Potenzial zugeschrieben.

Vor diesem Hintergrund wurde beschlossen, die weitere Erprobung und Implementierung einer rechtskonformen Unterschrift und damit die Fortentwicklung der vorgestellten Lösung momentan nicht fortzusetzen. Dieser Schritt eröffnet jedoch die Möglichkeit, zukünftige Entwicklungen im rechtlichen und technologischen Bereich zu beobachten und die Lösung zu einem späteren Zeitpunkt entsprechend anzupassen und weiterzuentwickeln.

7 Anhänge

7.1 Quellenverzeichnis und Anlagen

[1] eCMR-Protokoll: https://unece.org/DAM/trans/conventn/e-CMRe.pdf

[2] Open Logistics Foundation: https://openlogisticsfoundation.org/

[3] BMEIA: 2023-0.844.266, Vortrag an den Ministerrat, 8. März 2024 (Anlage: 006_000.pdf)

[4] Zusatzprotokoll zum Übereinkommen über den Beförderungsvertrag im internationalen Straßengüterverkehr (CMR) betreffend den elektronischen Frachtbrief (Übersetzung, Anlage: 006_001.pdf)

[5] Vorblatt Vereinfachte wirkungsorientierte Folgenabschätzung WFA Beitritt zur e-CMR (Anlage: 006_003.pdf)

[6] Erläuterungen zu BMEIA: 2023-0.844.266 [3] (Anlage: 006_004.pdf)

[7] EU-Verordnung 2020/1056 über elektronische Frachtbeförderungsinformationen https://www.bmk.gv.at/themen/mobilitaet/transport/gueterverkehrslogistik/eFTI.html

7.2 Glossar

CMR-Dokument	Frachtbrief auf Basis des CMR-Übereinkommens über den Beförderungsvertrag im internationalen Straßengüterverkehr (Consignment Note for Road Transport).
eCMR	Electronic Consignment Note for Road Transport; Zusatzprotokoll zum Übereinkommen über den Beförderungsvertrag im internationalen Straßengüterverkehr (CMR) betreffend den elektronischen Frachtbrief. Auch eCMR-Protokoll genannt.
eFTI	EU-Verordnung 2020/1056 über elektronische Frachtbeförderungsinformationen [7]
(eCMR)-Dokument	Ein digitales Dokument, welches dem eCMR-Protokoll entspricht. Auch eCMR oder eCMR-Dokument genannt.
API	Eine Anwendungsprogrammierschnittstelle ist eine Schnittstelle zur Kommunikation zwischen verschiedenen Softwareanwendungen.
Rest API	Ein Representational State Transfer Application Programming Interface ist eine Schnittstelle, die die Kommunikation zwischen verschiedenen Softwareanwendungen über das Internet ermöglicht.
Hash	ein einzigartiger digitaler Fingerabdruck, der durch eine mathematische Hashfunktion aus Daten erzeugt wird.
Fingerprint	Siehe Hash
Encoding	Umwandeln (Kodieren) von Daten in ein spezielles Format für die Übertragung oder Speicherung
Decoding	Prozess der Rückumwandlung kodierter Daten in ihr ursprüngliches Format
Private Key	ein geheimer Schlüssel, der in der Kryptografie verwendet wird, um Daten zu verschlüsseln oder zu signieren, wobei nur der Besitzer des Schlüssels Zugriff darauf hat
Public Key	ein öffentlicher Schlüssel in der Kryptografie, der gemeinsam mit einem privaten Schlüssel verwendet wird, um Daten sicher zu verschlüsseln oder Signaturen zu verifizieren
Digitale Signatur	eine elektronische Form der Unterschrift, die die Integrität und Authentizität eines digitalen Dokuments gewährleistet
Blockchain Node (oder auch Knoten)	ein Knotenpunkt in einem Blockchain-Netzwerk, der dazu dient, Transaktionen zu validieren und zu speichern.