APRIL 2018

FSBC Working Paper

Blockchain-basierte Abrechnung der IoT-registrierten Stationshalte: ein Proof-of-Concept auf Basis von Ethereum

Michael Kuperberg, Philipp Sandner, Matthias Felder

Mit der Liberalisierung des Marktes für Eisenbahnverkehre ist die Anzahl der Marktteilnehmer und die damit verbundene Komplexität für Abrechnungen zur Nutzung der Eisenbahninfrastruktur rasant gestiegen. Dieser Artikel beschreibt, wie die Blockchain-Technologie mithilfe von Smart Contracts den Anforderungen eines realistischen Einsatzszenarios in einer liberalisierten Eisenbahnindustrie gerecht werden kann. Dabei wird ein Proof-of-Concept näher beleuchtet und diskutiert, der bei dem IT-Dienstleister der Deutschen Bahn intern implementiert wurde und eine automatische Meldung der Stationshalte durch die Technologien des Internet of Things (IoT) zugrunde legt.

Frankfurt School Blockchain Center
www.fs-blockchain.de
contact@fs-blockchain.de

Follow us
www.twitter.com/fsblockchain
www.facebook.de/fsblockchain

Frankfurt School of Finance & Management gGmbH
Adickesallee 32-34
60322 Frankfurt am Main
Germany

Einführung

Nach der Liberalisierung des Marktes für Eisenbahnverkehre in Deutschland steht ein überwiegender Teil der Vollbahn-Infrastruktur den Marktteilnehmern diskriminierungsfrei zur Verfügung, d.h. die Gleise,

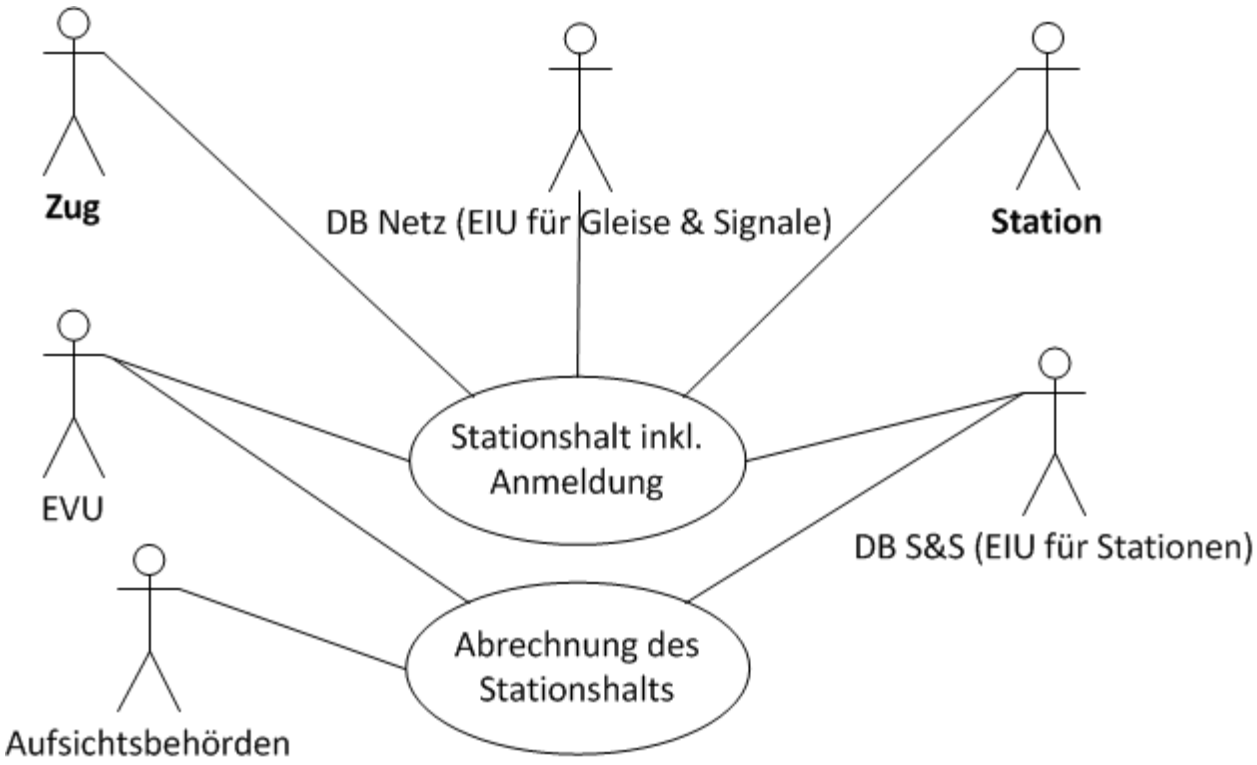
Oberleitungen und die Verkehrsstationen (für den Personenverkehr) werden von den entsprechenden zuständigen Konzerntöchtern der Deutschen Bahn AG gegen Nutzungsentgelte an Dritte überlassen: Wir sprechen von den Rollen Eisenbahninfrastrukturunternehmen (EIU) und Eisenbahnverkehrsunternehmen (EVU). Die Benutzung der Infrastruktur setzt eine **Anmeldung** durch das EVU beim EIU voraus – und zwar so, dass dem EIU jede einzelne Nutzung im Vorfeld (mit zeitlichem Vorlauf) verbindlich schriftlich vorliegt (vgl. Abbildung 1).

In diesem Artikel fokussieren wir uns auf die Abrechnung der Stationshalte; diejenigen Fälle, bei denen ein Marktteilnehmer gleichzeitig ein EVU und ein EIU ist, betrachten wir nicht gesondert, genauso wie die Strecken der Deutschen Bahn auf dem Staatsgebiet der Schweiz (mit separatem Regelwerk[1]). Ebenso wenig beleuchten wir die Abrechnung von Bahntrassen (d.h. die Abrechnung der Gleisnutzung *ohne* die Kosten für Stationshalte), denn diese verfügt über eine dynamische Bepreisung und über einen separaten Bestellprozess. Die Abrechnung von Bahnstrom unterliegt wiederum speziellen Prozessregeln der Energiewirtschaft und wird auch ausgeklammert.

Die Entgelte für die Stationsnutzung werden von der staatlichen Bundesnetzagentur[2] genehmigt und sind für alle Marktteilnehmer, also für alle EVUs, gleich und öffentlich einsehbar.[3] Die Entgelte sind nach Stationstyp, regionaler Differenzierung und Verkehrsart gestaffelt. So sind Halte von Fernverkehrszügen an derselben Station im Allgemeinen teurer als von Nahverkehrszügen. Für Stationshalte sind nicht nur die klassischen Personenzüge im normalen Fahrplan relevant: so ist es etwa möglich, eine touristische Fahrt kurzfristig anzumelden. Vor einer Genehmigung im Sinne einer Trassenfreigabe muss aber geprüft werden, ob sie sich mit der jeweiligen Situation vereinbaren lässt – man spricht dabei von „Trassen“ im Sinne von Fahrmöglichkeiten. Der Wegfall von Zugfahrten stellt zudem häufig bei Baustellen und Streckensperrungen eine eingeplante Veränderung des Fahrplanes dar.

Abbildung 1

Stakeholder (Use-Case-Diagramm / Anwendungsfalldiagramm)



Anmeldung und Abrechnung der Stationshalte: Situation im Februar 2018

Lange Zeit wurde die *Anmeldung* „traditionell“ mithilfe von Excel-Formblättern und Fax (später zusätzlich E-Mail) bewerkstelligt. Dies war ausreichend, solange die Beinahe-Monopole der vertikal integrierten Staatsbahnen beim Personen- und Güterverkehr existierten. Damit einhergehend gab es auch nur eine kleine Menge von kurz- und mittelfristigen Sonderverkehren. Für den größeren Teil der Verkehre war also die Trennung in Infrastruktur und Betrieb nicht relevant, da es sich um „Eigenleistung“ innerhalb der Deutschen Bahn handelte.

Die Situation änderte sich mit der Liberalisierung des Marktes. So waren 2017 bereits mehr als 400 EVUs als Marktteilnehmer tätig, davon eine hohe zweistellige Anzahl mit Personenverkehren, u.a. Abellio, die Hessische Landesbahn (HLB) und die Ostdeutsche Eisenbahngesellschaft (ODEG).

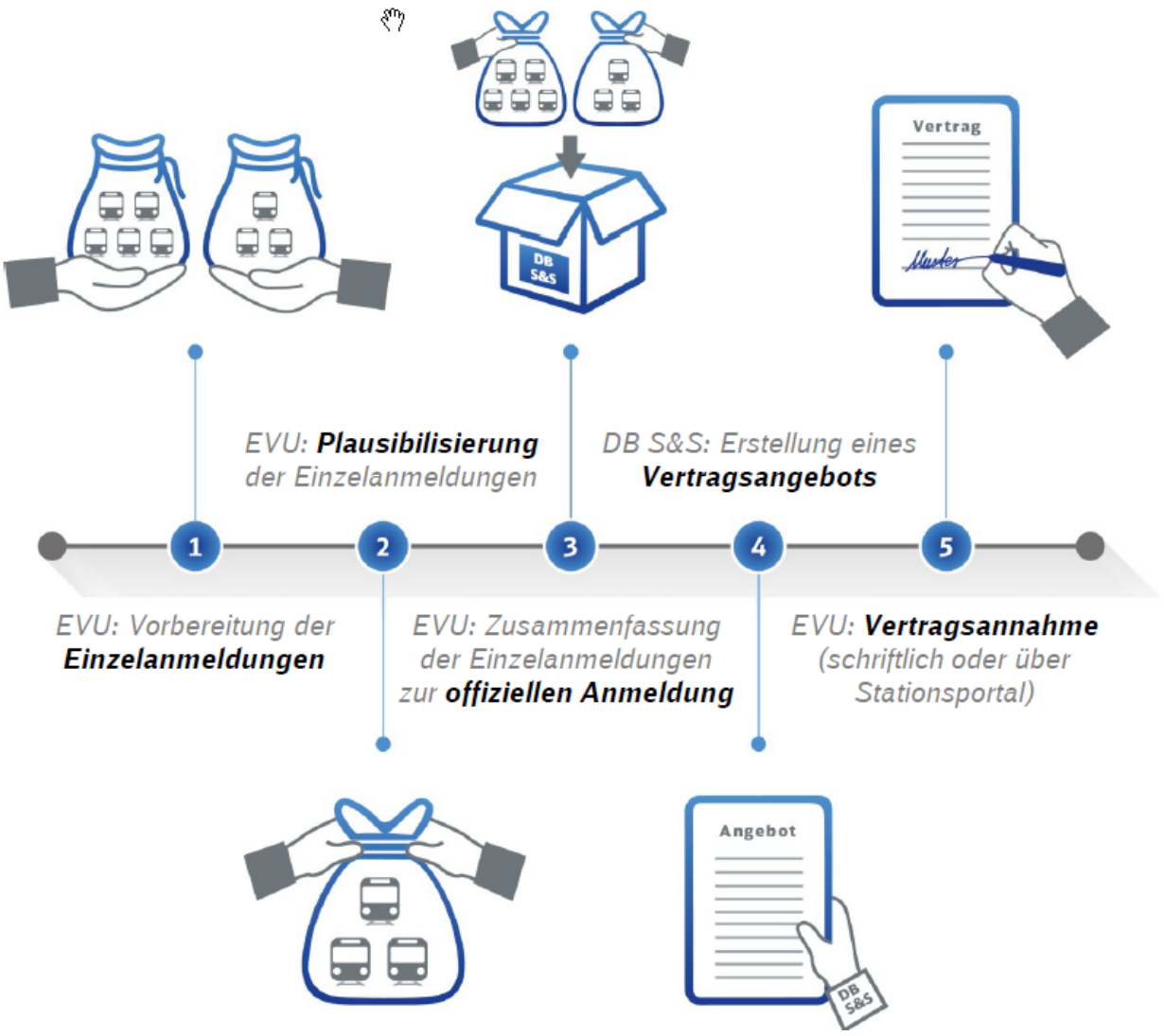
Nach schrittweisen Verbesserungen nahm die DB Station&Service AG das webbasierte, öffentliche Stationsportal[4,5] in Betrieb. Dort lassen sich Fahrten anmelden und Stationsnutzungsverträge abschließen. Damit erreicht man in der Marktkommunikation ein hohes Maß an Transparenz und gleichzeitig eine neue Ebene der Digitalisierung. Zudem greift das Stationsportal auf Daten von anderen IT-Diensten zu, etwa auf die Trassenverwaltungsdaten (DB Netz AG) und auf die Systeme zur Identitätsverwaltung (IdM/IAM).

Die EVUs melden zwar ihre geplanten Halte im Voraus über das webbasierte Stationsportal[6] (vgl. Abbildung 2) an, die *Abrechnung* erfolgt aber über separate Systeme (u.a. Standard-Software). Sowohl bei fahrplanmäßigen als auch bei kurzfristig angemeldeten Fahrten wird dabei in der Regel nach der Ist-Leistung abgerechnet. Fällt jedoch eine Fahrt durch Eigenverschulden des EVUs aus, so ist für die ausgefallenen Halte dennoch ein Stationsentgelt zu entrichten. Fällt dagegen aber ein Halt durch ein Verschulden des EIUs (hier DB Station&Service AG) aus, so ist für den ausgefallenen Halt kein Stationsentgelt zu entrichten. Über die Ist-Informationen, die für die Abrechnung maßgeblich sind (also über die tatsächlich stattgefundenen Fahrten und Halte) muss auf *beiden* Seiten (EVUs und EIUs) ein konsistentes gemeinsames Verständnis erzeugt werden.

Die *Abrechnung* der Stationshalte erfolgt nicht über das Stationsportal (Soll-Daten), sondern über separate IT-Systeme, welche die Ist-Daten zugrunde legen und die Soll-Daten nur zum Abgleich heranziehen (teilweise müssen die Daten für die Abrechnung manuell nachkorrigiert werden). Die Abrechnung der Stationshalte findet im sogenannten Postpaid-Verfahren statt. „Postpaid“ bedeutet, dass die DB Station&Service AG (als EIU) eine monatliche Rechnung nach erfolgter Leistungserbringung ausstellt. Das EIU kann Abschläge im Voraus verlangen (aktuell werden 85 % der monatlichen Kosten für die angemeldeten Halte im Voraus verlangt) – es bleibt aber beim grundsätzlichen Prinzip der *nachträglichen* Abrechnung. Naturgemäß sind damit auch verspätete Zahlungen, Mahnungen, etc. möglich, allerdings bleiben diese in der Realität in einem recht kleinen Rahmen.

Abbildung 2

Ausschnitt zur Stationshalt-Anmeldung im Stationsportal[7]



Eine der verbleibenden Herausforderungen ist aber das Claim Management – gerade in den Fällen, in welchen es verschiedene Auffassungen über das Stattfinden eines Haltes gibt, z.B. wenn sich die angemeldeten Halte und die Angaben aus den Aufzeichnungssystemen widersprechen. Solche Fälle müssen manuell bearbeitet werden und verursachen verhältnismäßig hohe Kosten. Hintergrund ist, dass es kein zentrales automatisiertes System gibt, welches die Halte und den Zug (mitsamt abrechnungsrelevanten Eigenschaften) verlässlich „in Echtzeit“

meldet und die zugseitigen Informationen mit den stationsseitigen Informationen abgleicht.

Mit einem solchen System könnte automatisch festgestellt werden, ob es sich bei einem Halt nur um einen technischen Halt handelt oder um einen echten fahrplanmäßigen Halt. Ein technischer Halt findet ohne Aus- bzw. Zustieg statt und kann signalbedingt entstehen. Außerdem können Halte unplanmäßig stattfinden oder übersprungen werden, wenn zum Beispiel Züge umgeleitet werden.

Eine weitere Herausforderung besteht darin, dass es perspektivisch und unter bestimmten Umständen Rabatte auf Stationsentgelte geben kann, etwa bei Minderleistung (z.B. „Bahnsteig nicht von Schnee geräumt“) oder bei Änderung von Fahrtattributen („IRE 1234 verkehrt als Ersatzzug für ICE 5678 in der Fahrlage des ICE mit dessen Halten“).

Das EIU ist also auf der einen Seite daran interessiert, seine Leistungen möglichst zeitnah abzurechnen – auf der anderen Seite ist an eine Einführung einer guthabenbasierten Prepaid-Abrechnung nicht zu denken, da die EVUs diesem Verfahren nicht zustimmen würden. Vergleichbar mit anderen Branchen fallen also auch im Eisenbahnverkehr das Clearing und Settlement auseinander. EIUs wollen jedoch, wie dargelegt, ein möglichst zügiges – oder im Idealfall ein zeitgleiches – Settlement erreichen.

Der Interaktion zwischen dem EIU und den EVUs fußt auf schriftlichen, bilateral *durch Menschen abgeschlossenen* Verträgen. Die Abwicklung dieser Verträge ist nicht in einer automatischen Weise möglich, denn dazu müssten die Vorbedingungen, wie etwa die Erfassung der zustande gekommenen, abrechenbaren Ist-Stationshalte, verlässlich und automatisiert dokumentiert worden sein. Erst wenn dies der Fall wäre, könnte auch die Rechnungsstellung und der Zahlungsvorgang automatisiert werden.

Wir beschreiben nachfolgend einen bei dem IT-Dienstleister der Deutschen Bahn intern implementierten *Proof-of-Concept* (PoC), der eine automatische Meldung der Stationshalte durch die Technologien des *Internet of Things* (IoT) zugrunde legt. Die Zahlungsverpflichtungen, die

sich aus den Verträgen ergeben, bilden wir durch prototypische Smart Contracts auf einer Ethereum-Blockchain ab. Bei der Zahlungsabwicklung beschränken wir uns auf entsprechende Abrechnungspositionen im EVU-Kundenkonto.

Eine pilotmäßige Realisierung mitsamt einer Ausweitung auf echte Zahlungsprozesse unter Einbindung echter Abrechnungssysteme (*Immediate Asset Transfer*) wären machbar, standen für uns bisher aber nicht im Vordergrund. Auch die Möglichkeit, Rabatte aufgrund von mängelbehafteten Leistungen anzusetzen, haben wir zunächst nicht in unsere Betrachtung/Implementierung miteinbezogen.

Die Bestandssysteme für Anmeldung und Abrechnung unterstützen über die beschriebenen Aspekte hinaus weitere unternehmerische Aufgaben, z.B. Ressourcen- und Kapazitätsplanung. Diese Aspekte werden durch den PoC nicht adressiert – wir fokussieren uns nur auf die Abrechnung der Halte.

Blockchain-basierte Umsetzung als Proof-of-Concept

Warum Blockchain?

Die IT-technische Umsetzung eines *Proof-of-Concept* für Stationshalte muss natürlich nicht zwingend auf einer Blockchain implementiert werden. Dennoch bietet sich eine Umsetzung mittels Blockchain-Technologie in unserem Falle aus den folgenden Gründen an:

Nichtabstreitbarkeit: Durch die Überprüfbarkeit der Konsistenz anhand von Hashes lässt sich mithilfe der Datenreplikate nachweisen und überprüfen, dass Daten (z.B. Haltereignisse) angefallen sind; die Nichtabstreitbarkeit ist eine Out-of-the-Box-Fähigkeit des Blockchain-Prinzips, die sich u.a. aus der Verteilung/Dezentralität ergibt.

Datenoffenheit: Da die Stationshalt-Tarife für alle Marktteilnehmer gleich sind (keine EVU-spezifischen Rabatte, vollständig öffentlich und transparent) und auch die Haltereignisse öffentlich einsehbar sind (vgl. Fahrplan-Echtzeitinformationen), liegen damit alle Grunddaten öffentlich vor.

Smart Contracts: Verträge und Vertrauensbeziehungen bilden die Grundlage und somit lässt sich die IT-Entsprechung angemessen konstruieren (man beachte, dass es je nach Blockchain-Produkt möglich ist, bestimmte bilaterale Details vor den anderen zu verbergen und andere Details wiederum öffentlich bereitzustellen).

Auto-Replikation: Die Aufsichtsbehörden (z.B. das Eisenbahnbundesamt[8] bzw. die Bundesnetzagentur) oder andere Berechtigte können als Blockchain-Teilnehmer dynamisch hinzugefügt werden und damit die vorgehaltenen Daten replizieren, ohne dass die Grundstruktur der IT-Lösung geändert werden muss (diese Teilnehmer können z.B. einen eigenen Node aufsetzen).

Dezentralisierung: Die Replikation verhindert, dass es eine zentrale Instanz der Datenhaltung gibt, die beschädigt oder sabotiert werden kann – auch dies ist eine Out-of-the-Box-Fähigkeit.

Disziplinierung: Die Blockchain-Mechanismen halten die Marktteilnehmer dazu an, regelkonform und ressourcenschonend zu interagieren.

Mangel an COTS-Alternativen (COTS steht für *Completely-off-the-shelf*, d.h. direkt einsetzbar): Es existieren keine marktgängigen *Append-only*-Datenbanken mit kryptografischer Konsistenz als COTS-Produkt und ebenso wenig ein COTS-System mit den obigen Eigenschaften, ob nun Blockchain-basiert oder nicht.

Bewährte Implementierungen: Öffentliche Blockchain-Plattformen sind voll funktionsfähig und schon jahrelang im Einsatz, vgl. z.B. die Währung Ethereum[9], welche bisherigen öffentlichen Angriffen standgehalten hat (der bekannte Angriff[10] auf eine DAO/DApp nutzte eine Schwachstelle innerhalb eines konkreten *Smart Contracts* aus; Ethereum-Protokolle/-Stacks waren nicht betroffen).

Normierung: Ethereum ist die am weitesten verbreitete Blockchain-Plattform für fachlich spezifische Lösungen (*Custom Solutions*).

Kein *Right to be forgotten*: Anders als bei Individuen haben Firmen (juristische Personen) kein Recht auf eine „Löschung der Daten auf Zuruf" – der jeweilige Geschäftspartner hat ein fristbegrenztes Recht, die Daten aufzubewahren – und teilweise sogar eine rechtliche Pflicht zur revisionskonformen Archivierung. Letzteres lässt sich auch ohne Blockchain-Einsatz lösen, indem die Blockchain-Inhalte zusätzlich in ein Archivierungssystem eingespeist werden.

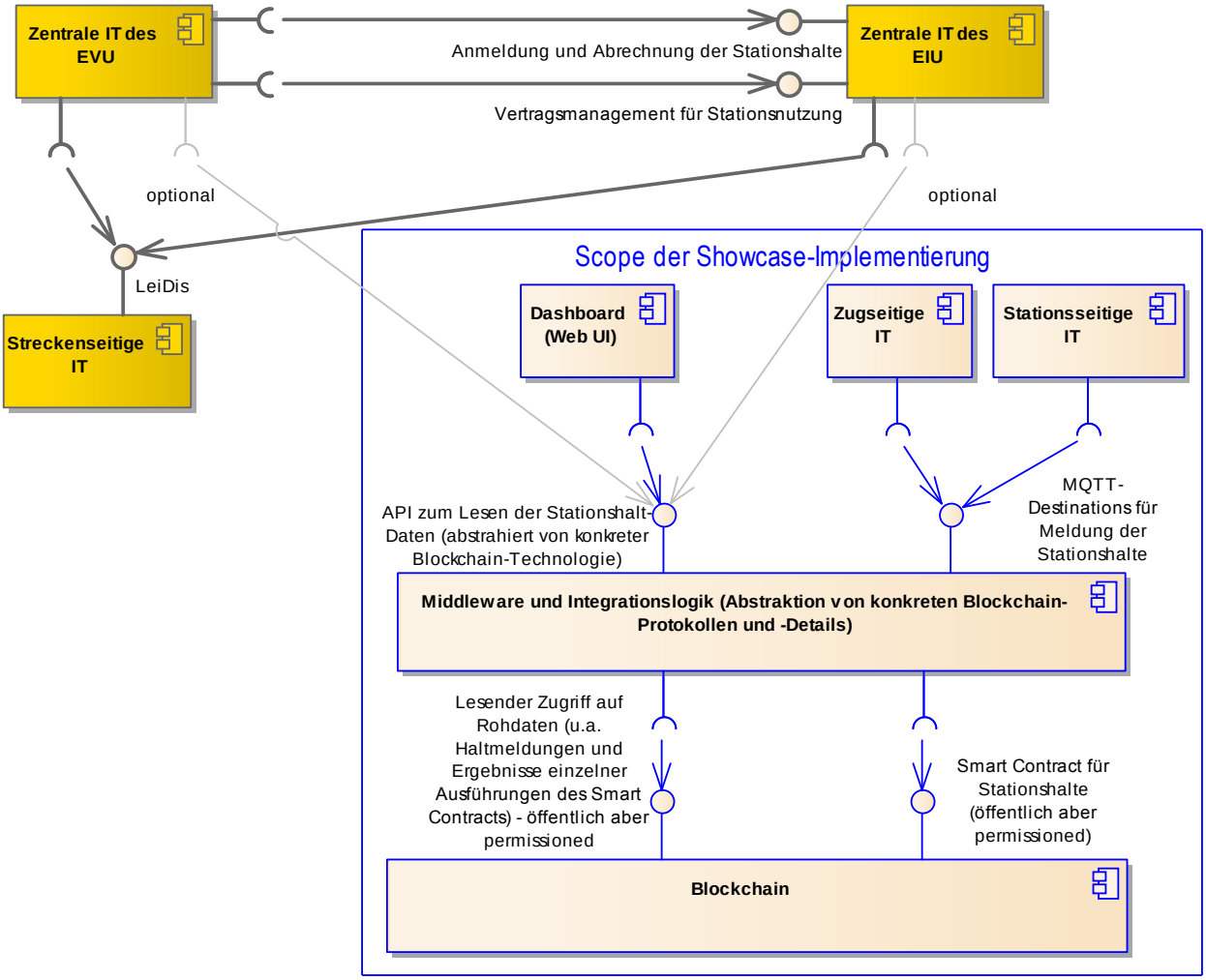
Definierbarkeit des Quorums bzw. des Consensus-Verfahrens, um Blöcke und Transaktionen zu validieren: Normalerweise nimmt man an, dass der Consensus-Schritt, der auf das erfolgreiche *Minen* eines Blockes folgt, derart vonstattengeht, dass alle teilnehmenden Mitspieler konstruktiv agieren und einem korrekten Block zustimmen. Selbst wenn man diese Annahme relativiert und man entweder „faule" oder „bösartige" Mitspieler unterstellt, ist es dennoch möglich, einen Block am Ende positiv zu bescheiden, etwa unter Benutzung des Proof-of-Stake-Verfahrens.

Ausreichende Performance: Anders als bei öffentlichen Blockchains, die auf einem energieverschwendenden Proof-of-Work-Algorithmus basieren, reicht im vorliegenden Fall eine private Blockchain („Konsortium-Blockchain") aus; in dieser können unerwünschte Faktoren ausgeschaltet werden. Man kann die kryptografische Komplexität von Proof-of-Work auf ein Minimalmaß heruntersetzen oder aber das notwendige Quorum (vgl. vorherigen Punkt) minimal auslegen.

Am Ende bleibt festzuhalten, dass wir darauf verzichten, selbst eine Datenbank mit den Eigenschaften der (kryptografisch gesicherten) Nichtabstreitbarkeit und gleichzeitig mit der automatischen Replikation zu entwickeln. Folgende Abbildung 3 zeigt die Architektur und den Scope des Showcases.

Abbildung 3

Architektur und Scope des Showcases



Designoptionen bei Abrechnung der Stationshalte

Es gibt verschiedene Möglichkeiten, einen Stationshalt abzurechnen. Dabei sollte man bedenken, dass ein Stationshalt aus einer Einfahrt und einer Ausfahrt besteht. Die Abrechnungsmöglichkeiten lassen sich anhand folgender Kriterien klassifizieren:

- Toll-Before-Access: Einfahrt erst nach Abrechnung/Zahlung/Kreditierung

- Toll-After-Access: Die Einfahrt wird nicht durch die Abrechnung begrenzt, allerdings kann hierbei die Ausfahrt durch die Bezahlung eingeschränkt sein.
- Toll-After-Departure: Die Abrechnung findet erst nach Ausfahrt statt, was z.B. bei Berücksichtigung der Haltedauer sinnvoll sein kann; die Freigabe der Ausfahrt wird nicht durch den Bezahlvorgang beschränkt und der zeitliche Abstand kann sich unterscheiden.
- Online vs. Offline: d.h. ob bei der Einfahrt und/oder bei der Ausfahrt eine Verbindung zum Infrastrukturbetreiber bestehen muss oder nicht (es sind natürlich auch Kombinationen möglich).
- Guthabenbasiert (Prepaid) vs. kreditbasiert (Postpaid) – auch hier kann eine Mischform gefunden werden.

Während der Einsatz einer Blockchain für alle Kombinationen durchaus sinnvoll erscheint, konzentrieren wir uns im Folgenden auf die Szenarien, die der heutigen realen Marksituation am ehesten nahekommen: Toll-After-Departure, Offline und kreditbasiert. Im einfachsten Fall stellt die Abrechnung des Stationshaltes ein einzelnes Ereignis dar, welches beim EIU registriert wird und in die Abrechnung miteinfließt. Dieses Ereignis kann

- entweder vom Zug (bzw. vom EVU),
- vom EIU selbst (hier vom Stationsbetreiber),
- oder von einer dritten Partei kommen (etwa von den Balisen des Signalsystems, die in der Verantwortung einer anderen Gesellschaft der DB AG stehen).

Dieser einfachste Fall birgt Fehlerpotentiale, etwa bei unzuverlässiger Datenübermittlung. Zum Beispiel kann es bei einem Zug signalbedingt zu einem außerplanmäßigen Halt *innerhalb einer Station* kommen, ohne dass die Fahrgäste aus- und zusteigen können. Somit wäre dies kein abzurechnender Halt, sondern nur ein Betriebshalt. Daher ist eine Interaktion zwischen Fahrzeug und Infrastruktur sinnvoll, um die Situation abzuklären. Diese minimiert bei sorgfältigem Design der Interaktion auch das Fehlerpotential und berücksichtigt weitergehende Informationen, z.B. den Soll-Fahrplan, Baustelleninformationen, die bereits erwähnten

Trassenbestellungen, etc. Perspektivisch können zudem Ortungsdaten und Signaldaten in diese Interaktion einfließen.

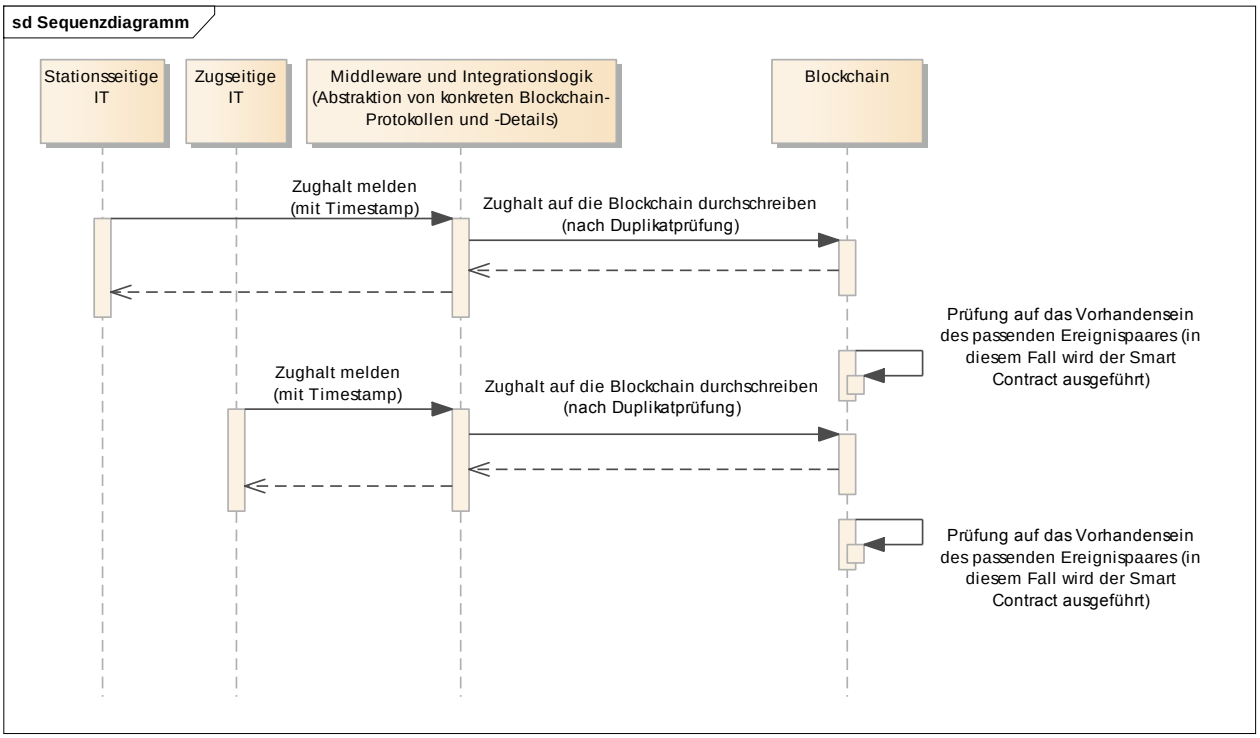
Im vorgestellten PoC wurden zwei Ereignisse (Meldungen) der Interaktion zugrunde gelegt:

- Das Fahrzeug (EVU-Seite) schreibt seinen Halt in die Blockchain, mit Angabe des Haltes, ggf. angereichert mit weiteren Informationen zur Haltedauer, Zugeigenschaften, Anmerkungen des Lokführers, etc.
- Die Station (EIU-Seite) schreibt das *von ihr* detektierte Haltereignis in die Blockchain zusammen mit einem Fahrzeug-Identifikator.

Im *Smart Contract* ist nun hinterlegt, dass bei einem Match zwischen fahrzeugseitigem und haltseitigem Ereignis der Stationshalt als validiert (sogar gegenseitig bestätigt) angesehen wird und abgerechnet werden kann. Die erlaubte(n) Reihenfolge(n) der Ereignisse und das maximale Zeitintervall zwischen diesen sind dabei schon im Vertrag vorgegeben, wir analysieren sowohl den Empfangszeitpunkt des Ereignisses als auch den Zeitstempel im Ereignis (vgl. Abbildung 4).

Abbildung 4

Sequenzdiagramm zum Smart Contract



Außerdem ist eine Logik zur Entdeckung von Duplikaten integriert – diese hilft, Doppelabrechnung zu vermeiden, etwa wenn aufgrund von Übertragungsfehlern sowohl das fahrzeugseitige als auch das haltseitige Ereignis doppelt erzeugt und auch doppelt in die Blockchain geschrieben wurde. Schließlich kann mittels PKI (hier: Signierung von Meldungen) dafür gesorgt werden, dass dem Abrechnungssystem keine gefälschten Inhalte untergeschoben werden.

Bei jedem Schreibvorgang in die Blockchain prüft der *Smart Contract*, ob nicht bereits ein passendes „Gegenereignis“ vorliegt, welches noch offen ist (in keiner Abrechnung berücksichtigt) und ob das geschriebene Ereignis nicht per se ein Duplikat ist. Sehr wichtig dabei ist, dass alle übermittelten Ereignisse (Rohdaten) immer in Originalform in die Blockchain durchgeschrieben werden, d.h. Duplikate werden nicht verworfen, sondern beim Durchschreiben als Duplikate markiert. Die beschriebenen Prüfungen finden also innerhalb eines *Smart Contracts* statt, welcher als „Broker“ die

Ereignisse entgegennimmt. Dieser Broker kann perspektivisch auch die Signaturprüfung bei den Rohdaten übernehmen.

Wenn das Gegenereignis zu einem Rohereignis gefunden wurde, wird in einem dritten Schreibvorgang die eigentliche Abrechnung („Vollzug“ der definierten Regel) durchgeführt. Diese nimmt dabei Bezug auf die beiden Transaktionen mit den zugrunde gelegten Ereignissen und vermerkt die aktualisierten „Schulden“ des EVUs gegenüber dem EIU. Somit bleiben die komplette „Konto“-Historie in der Blockchain wie auch die Rohdaten nachvollziehbar. Vorgesehen ist außerdem, dass bestimmte Berechtigte „Storno-Transaktionen“ in die Blockchain schreiben können: Damit wird zwar ein Eintrag in der Blockchain nicht gelöscht, aber fachlich kompensiert. Dies dient dazu, dass die Sachbearbeiter die strittigen (Claim-)Fälle abarbeiten können.

IoT-Anteile des Showcases

Die Signalisierung des Haltereignisses findet im PoC über eine IoT-orientierte Lösung statt. Dabei löst die Zugeinfahrt in die Station zwei MQTT-Ereignisse aus. Über etablierte MoM-Patterns (etwa Message-Duplizierung oder Broadcast) lassen sich also weitere Systeme zur Haltauswertung ergänzen, ohne das eigentliche Abrechnungsszenario zu beeinträchtigen. Die zwei MQTT-Nachrichten sind:

- Das stationsseitige Haltereignis wird durch den Infrastrukturbetreiber verarbeitet und mündet in einem neuen Blockchain-Eintrag (neue Transaktion in einem Block).
- Das zugseitige Haltereignis wird von der EVU-Seite erzeugt und führt ebenso zu einem Blockchain-Eintrag.

Für die physische Demonstration im Brio-Maßstab wurde ein NFC-Ergänzungsmodul an einem Raspberry Pi gewählt (vgl. Abbildung 5). Das Lesegerät reagiert auf NFC-Tags (es kann auch mit neuen, d.h. unbekannten Tags umgehen) und schickt ein Ereignis über ein lokales Netzwerk an einen MQTT-Topic, der von einem MQTT-Gateway persistent vorgehalten wird (d.h. auch beim Gateway-Absturz gehen die MQTT-Messages nicht verloren). Eine weitere Komponente lauscht auf dem MQTT-Topic und holt

die Nachrichten ab (vom Topic entfernt werden sie erst, wenn sie erfolgreich verarbeitet worden sind). Der Inhalt der Nachricht wird geprüft und fallbasiert in die Ethereum-Blockchain durchgeschrieben. Inhaltlich duplizierte Nachrichten werden durchgeschrieben (vgl. oben), auf Transportebene inkorrekte Nachrichten, semantisch oder syntaktisch, werden verworfen. Grundsätzlich lässt sich vom Raspberry Pi auch direkt (ohne MQTT) in die Blockchain schreiben, dabei müsste aber die Komplexität (u.a. die Fehlerbehandlung, PKI, …) dorthin verlagert werden.

Abbildung 5

Foto des Showcase-Aufbaus

Die für die Demo verwendete Ethereum-Blockchain ist privat („Konsortial-Blockchain“). Der Ether-Vorrat ist bei der Initialisierung der Blockchain auf einen maximal hohen Wert gesetzt; die Ether können automatisch und Mining-frei nachgefüllt werden (sie werden ja in Ethereum *by Design* verbraucht, wenn Rechenvorgänge und Transaktionen ausgeführt werden).

Für den PoC-Showcase haben wir darauf verzichtet, Archivierung und Daten-Trunkierung (*Rollover*) für die Ethereum-Blöcke zu implementieren. Vielmehr haben wir uns darauf konzentriert, die Fachlichkeit und den Blockchain-Unterbau über eine klar gegliederte grafische Oberfläche zu visualisieren, die wir im nächsten Abschnitt beschreiben. Hier möchten wir noch anmerken, dass sich Clients an die Ethereum-Blockchain mit den Standard-Werkzeugen von Ethereum ankoppeln können, etwa um Blöcke zu validieren.

UI und Hardware für den Showcase

Das primäre Ziel des Showcases ist die Veranschaulichung des Use-Cases für Stakeholder und Interessierte. Außerdem haben wir damit wertvolle Erfahrungen mit der quelloffenen Java-Implementierung von Ethereum (EthereumJ) sammeln können – es gibt nämlich signifikante Unterschiede bei der Usability der einzelnen Implementierungen von Ethereum.

Die grafische Oberfläche des Showcases ist mit HTML und CSS implementiert und läuft auf einem schlanken Webserver. Es überwiegen die fachlichen Informationen, auch wenn die Blocksignaturen dargestellt sind. Die Oberfläche ist so dimensioniert, dass sie auf einem Microsoft Surface Hub (Full-HD-55“-Display mit eingebautem Windows-Rechner) gut zur Geltung kommt.

Neben den beschriebenen IT-Anteilen besteht der Showcase aus zahlreichen Elementen der stromlosen Brio-Spielzeugeisenbahn, also aus „Schienen“, „Fahrzeugen“ und „Bahnhöfen“. Neuerdings hat Brio auch eine per Bluetooth fernsteuerbare, mit herkömmlichen AA-Batterien betriebene Lok im Programm. Diese kann „ihre Runden drehen“, ohne dass die vorführende Person ständig die (mit dem NFC-Tag versehene) Lok am NFC-Lesegerät (an der Station) von Hand vorbeiführen muss. Die Lok hat keine offene Steuerungs-API.

Die Hardware des Showcases ist portabel und kann auch mit einem spontanen WLAN-Netzwerk, etwa von einem Mobil-Hotspot eines Smartphones aus, betrieben werden. Der Raspberry Pi kann über USB mit Strom versorgt werden. Mit einem Laptop oder einem Surface-Tablet ist

eine mehrstündige Vorführung auch ohne Stromanschluss machbar, z.B. auf Messen oder bei Kunden.

Ausfallsicherheit und Schutzmechanismen

Der Charme der Blockchain-Technologie ist an dieser Stelle, dass das Schreiben in die Blockchain auf verschiedenen Nodes stattfinden kann. Vorausgesetzt, es liegt ein korrekt aufgesetzter und funktionierender Konsensus vor, wird dabei von den Blockchain-Teilnehmern ein notwendiges Quorum erzielt, um die „vorgeschlagene“ Transaktion auch tatsächlich durchzuschreiben.

Kryptoassets als Perspektive

Wie beschrieben ist die aktuelle PoC-Implementierung ein Postpaid-Verfahren – die EVUs häufen sozusagen Schulden an. Die Blockchain bietet aber über das Konzept der Kryptoassets, etwa in Gestalt von Kryptowährungen, eine Lösung an, die weder zu einer (Online-)Anbindung an echte Abrechnungssysteme zwingt noch dem EIU das Risiko aufbürdet, auf den Rechnungen sitzen zu bleiben. Konkret könnte man ein Guthaben auf der Blockchain abbilden, ohne dass das EVU sein Geld tatsächlich aus der Hand gibt. Vorstellbar wäre hier eine 1:1-Abbildung von einer Geldeinheit auf ein Kryptoasset (wir nennen das Kryptoasset symbolisch „StationshaltCoin“) und ein EVU würde vor jeder Abrechnungsperiode ein Guthaben aufbauen – Eintausch von Euro gegen StationshaltCoin. Mit anderen Worten, die Blockchain wäre das Notaranderkonto und der *Smart Contract* ein Notar, der eine Auszahlung erst freigibt, wenn sich beide Seiten einig sind. Im September 2017 stellten IBM, ZF und UBS eine auf Hyperledger basierte Lösung[11] vor, die ein Wallet (elektronische Geldbörse) für Autos bereitstellt, mit welchem Dienste bezahlt werden sollen.

Zusammenfassung und Ausblick

Der beschriebene Anwendungsfall zeigt, wie die Vorteile von Blockchains bei der Abrechnung der Stationshalte im Bahnverkehr helfen können, die Prozesse zu verbessern und die manuellen Aufwände zu miniminieren. Die vorgestellte Proof-of-Concept-Implementierung zu diesem Anwendungsfall

zeigt, wie Ethereum und IoT-Aspekte kombiniert werden können, um die physische Welt und die virtuelle Welt der IT zu verbinden.

Für einen großflächigen und produktiven Einsatz muss die Detektion der Halte und der Zugeigenschaften zuverlässig und zeitnah sein. Dann lassen sich mithilfe der Smart Contracts die Geschäftsprozesse der Stationshalt-Abrechnung dynamisieren, die Bezahlung weiter automatisieren, und die Anzahl der strittigen Fälle kann gesenkt werden. Die Blockchain schafft dabei durch die Transparenz der maschinellen Verträge und durch die Verlässlichkeit (Replikation, Nichtabstreitbarkeit) ein höheres Vertrauen zwischen Dienstleistern und Kunden.

Dr. Michael Kuperberg arbeitet als Blockchain Lead Architect bei der DB Systel GmbH in Frankfurt am Main und berät Kunden innerhalb des DB-Konzerns zum Thema Blockchain. Erreicht werden kann er per E-Mail (michael.kuperberg@deutschebahn.com)

Prof. Dr. Philipp Sandner leitet das Frankfurt School Blockchain Center. Er kann über E-Mail (email@philipp-sandner.de) kontaktiert werden, via LinkedIn (https://www.linkedin.com/in/philippsandner/) und ist auch bei Twitter aktiv (@philippsandner).

Matthias Felder verantwortet die Themen Blockchain und IoT im Portfolio-Management der DB Systel GmbH. Er ist Product Owner mehrerer Projekte mit diesen Technologien, darunter ist auch eine Angebotsplattform auf Blockchain-Basis.

[1] Zur Abrechnung in der Schweiz: http://fahrweg.dbnetze.com/fahrweg-de/kunden/nutzungsbedingungen/strecken_in_der_schweiz.html

[2] Bundesnetzagentur: https://www.bundesnetzagentur.de/DE/Sachgebiete/Eisenbahnen/Unternehmen_Institutionen/unternehmen_institutionen-node.html

[3] Stationshalt-Entgelte: http://www.deutschebahn.com/de/geschaefte/infrastruktur/bahnhof/stationsnutzung/11878060/preisliste.html?start=0

[4] Stationsportal: https://www.deutschebahn.com/stationsportal

[5] Informationen zum Stationsportal: http://www.deutschebahn.com/de/geschaefte/infrastruktur/bahnhof/stationsnutzung/11878074/stationsportal.html?start=0

[6] Stationsportal: https://www.deutschebahn.com/stationsportal

[7] Stationsportal Präsentation: www.deutschebahn.com/file/de/11878072/rMsgeQU9pcnFQVTGqZh0yERBtB4/9806628/data/praesentation_allgemeine_infos_stationsportal.pdf (abgerufen am 31.08.2017)

[8] Eisenbahnbundesamt: https://www.eba.bund.de/DE/home_node.html

[9] Ethereum: https://www.ethereum.org/

[10] Angriff auf die DAO: https://www.cryptocoinsnews.com/ex-ethereum-developer-dao-hack-happened-comes-next/ sowie https://medium.com/@MyPaoG/explaining-the-dao-exploit-for-beginners-in-solidity-80ee84f0d470

[11] Hyperledger Wallet für Autos: https://www.ibm.com/blogs/internet-of-things/zf-ubs-ibm-vehicle-payments/