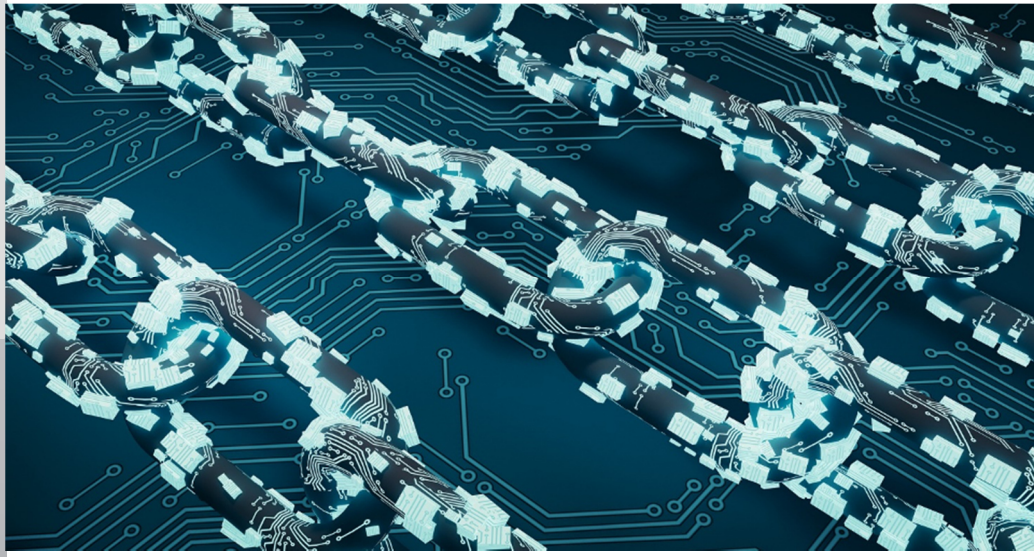
BLOCKCHAIN UND IHRE ANWENDUNGEN IN DER MOBILITÄT

Martin Stabauer



Teil 8 von Digital Business für Verkehr und Mobilität
Ist die Zukunft autonom und digital?

Institut für Digital Business

2020

INSTITUT FÜR
DIGITAL BUSINESS

Digital Business für Verkehr und Mobilität
Ist die Zukunft autonom und digital?

Herausgeber: Johann Höller; Tanja Illetits-Motta; Stefan Küll;
Ursula Niederländer; Martin Stabauer

ISBN: 978-3-9504630-4-0 (eBook)
2020

Johannes Kepler Universität
Institut für Digital Business
A-4040 Linz, Altenberger Straße 69
https://www.idb.edu/

Detailliertere bibliographische Daten, weitere Beiträge,
sowie alternative Formate finden Sie unter
https://www.idb.edu/publications/

Bildquelle Titelbild: https://pixabay.com/illustrations/blockchain-block-chain-bitcoin-3750157/

Inhaltsverzeichnis

BLOCKCHAIN UND IHRE ANWENDUNGEN IN DER MOBILITÄT

Martin Stabauer

Dieser Beitrag beschäftigt sich mit einer der größten Hype-Technologien der letzten Jahre, der Blockchain. Zunächst wird eine praxisnahe Einführung in die Technologie der Blockchain, ihre populärste Anwendung – Kryptowährungen – und ihre kryptografischen Grundlagen geboten, um dann potenzielle Anwendungsbereiche in der Mobilität beleuchten zu können. Neben bereits stark erforschten Bereichen wie der Logistik werden auch weniger populäre Implementierungen wie automatische Updates der Fahrzeugsoftware betrachtet und hinsichtlich ihrer Umsetzungspotenziale analysiert.

1 Einleitung

In der IT, der Logistik, der Finanzwirtschaft und etlichen anderen Bereichen kommt man in den letzten Jahren um ein Schlagwort nur schwer herum: Blockchain. Diese Technologie und die eng mit ihr im Zusammenhang stehenden Anwendungen der Kryptowährungen erfahren eine äußerst breite Aufmerksamkeit. Im jährlich erscheinenden Gartner Hype Cycle wird die Blockchain schon seit 2016 gelistet, in der Ausgabe von 2018 wird ihr bescheinigt, den Gipfel des Hypes bereits überschritten zu haben und sich langsam einer etwas

gefestigteren Position anzunähern. Weiters wird als einer der fünf wichtigsten Trends das Thema „digitalisierte Ökosysteme" gesehen: Viele andere aktuelle Technologien benötigen starke, dynamische Plattformen, die ausreichende Sicherheit und Performance bieten – die Blockchain wird hier als möglicher Enabler für andere Systeme aufgeführt (Panetta 2018). Auch die EU-Kommission befasst sich im Zuge ihrer Digital Single Market Strategie intensiv mit dieser Thematik (EC 2019), ebenso die deutsche Bundesregierung, die das Feld nicht Privatunternehmen wie Facebook überlassen möchte (Schäfers 2019).

Ob die Blockchain tatsächlich in allen kolportierten Anwendungsbereichen effektiv und effizient eingesetzt und allen – teilweise stark überzogenen – Ansprüchen gerecht werden kann, bleibt zum heutigen Zeitpunkt offen. Auch ob sich nachhaltige Geschäftsmodelle entwickeln lassen, ist noch nicht abschließend geklärt. Während skeptische Stimmen von einer „*Lösung, die nach ihrem Problem sucht*" sprechen (Bloomberg 2017), ruft die Association for Information Systems zu einem starken Fokus in der Forschung auf, insbesondere in den Bereichen der Verhaltensforschung, Design Science und der Wirtschaftswissenschaften (Rossi et al. 2019).

Hinzu kommt, dass es im Bereich des E-Commerce in den letzten Jahren enorme Steigerungsraten gegeben hat. Der Anteil der Personen in Europa, die in den letzten drei Monaten für private Zwecke Waren oder Dienstleistungen über das Internet bestellt haben, verdoppelte sich in den letzten 10 Jahren von 23% auf 48% (Eurostat 2017). Diese Entwicklung lässt Kryptowährungen als potenzielle neue Zahlungsweisen attraktiv erscheinen. Zudem ergeben sich auch neue Herausforderungen im Bereich der Paketlogistik und des Supply Chain Management. Dass es hier großes Potenzial zur Effizienzsteigerung gibt, zeigt eine Studie der dänischen Reederei Maersk, die besagt, dass Blumen am Weg von Kenia in die Niederlande durch die Hände von knapp 30 Personen und Organisationen gehen und dabei über 200 Interaktionen entstehen (IBM 2017).

Dieser Beitrag bietet zunächst eine praxisnahe Einführung in die zugrunde liegende Technologie der Blockchain und zeigt dann potenzielle Anwendungsfelder im Bereich der Verkehrsmobilität auf.

2 Technologische Grundlagen

Da die Fälschungssicherheit aller Blockchain-basierten Anwendungen auf den Grundprinzipien asymmetrischer Verschlüsselung und Hash-Funktionen basiert, soll an dieser Stelle zunächst mit einem kurzen Exkurs in die Verschlüsselungstechnik gestartet werden, darauf folgen die Prinzipien der Blockchain und ausgewählter Kryptowährungen.

2.1 Kryptographie

Zwei kryptographische Grundlagen sollen im Folgenden kurz skizziert werden, da ohne entsprechende Grundkenntnisse die Blockchain-Technologie nur schwer verstanden werden kann: Asymmetrische Verfahren und Hash-Verfahren.

Asymmetrische Verschlüsselung basiert auf der Grundidee, dass zum Ver- und zum Entschlüsseln eines Klartexts zwei unterschiedliche Schlüssel verwendet werden: der Private Key und der Public Key. Beide Schlüssel werden auf Basis einer gemeinsamen Zufallszahl gleichzeitig erzeugt, es ist aber extrem schwierig, von einem auf den anderen Schlüssel zu schließen. Wie die Namen vermuten lassen, wird der Public Key öffentlich zugänglich gemacht, während der Private Key geheim gehalten werden muss.

Wenn nun A eine verschlüsselte Nachricht an B schicken möchte, wird zur Verschlüsselung der Public Key von B verwendet, der ja öffentlich und somit auch A zugänglich ist. B kann dann den eigenen Private Key verwenden, um die Nachricht zu entschlüsseln.

Die zweite Anwendungsmöglichkeit der asymmetrischen Verschlüsselung ist die digitale Signatur: Um eine Nachricht fälschungssicher zu veröffentlichen und ihre Herkunft eindeutig zu kennzeichnen, kann A den eigenen Private Key auf die Nachricht anwenden. B (und jeder andere) kann dann den Public Key des A verwenden, um nachzuvollziehen, dass die Nachricht tatsächlich von A stammt.

Hash-Verfahren dienen ebenfalls der Verschlüsselung eines Klartexts, allerdings soll und kann die ursprüngliche Nachricht nicht mehr rekonstruiert werden. Der entstandene Hash hat eine konstante Länge, unabhängig vom Umfang der Nachricht. Dies wird beispielsweise benötigt, um Passwörter von Benutzern sicher abzuspeichern. Gute Hash-Verfahren stellen sicher, dass

- gleiche Nachrichten immer den gleichen Hash ergeben,
- unterschiedliche Nachrichten immer unterschiedliche Hashes ergeben (mit der Limitation, dass es wegen der konstanten Länge nur eine begrenzte Anzahl unterschiedlicher Hashes, aber unendlich viele unterschiedliche Nachrichten gibt),
- kleine Änderungen in der Nachricht große Änderungen im Hash bewirken („Lawinen-Effekt"), und
- die Hashes leicht zu berechnen sind, aber keine Rückschlüsse auf die Ausgangswerte zulassen.

Wendet man beispielsweise das weit verbreitete und als sicher geltende SHA-256-Verfahren – das übrigens auch bei Bitcoin zum Einsatz kommt – auf die Nachricht „Mobilität" an, ergibt dies den Hashwert:

```
68E4C99AF7B0AA81152864DC38622E06AD643467A590E13CA6137A80AC43
A0B0
```

Schon eine geringe Änderung der Nachricht auf „Mobilität0" ergibt:

```
2689F5BA30285C02B6D8D81F58CE6A1FC81C2E8670FB64C7F675F6457039
E47A
```

Und der Hashwert dieses gesamten Beitrags vor dem Lektorat lautet:

```
CFA47FD1E51906FC5CE87AAFC7F87C86334A13549C29669F8D442B0ACA24
119F
```

Daraus lässt sich gut erkennen, wie sich kleine und große Änderungen am Input auf den Output auswirken.

2.2 Blockchain

Die Blockchain und ihr Umfeld können wohl kaum diskutiert werden ohne Bezug auf Bitcoin zu nehmen, die erste und bis heute bekannteste Anwendung dieser Technologie. Bereits 2008 vorgestellt, erlangte das entsprechende Whitepaper (Nakamoto 2008) in den folgenden Jahren enorme Verbreitung. Das System wird auch als „Distributed-Ledger-Technologie" bezeichnet und basiert einfach gesagt darauf, dass spätere Transaktionen auf früheren aufbauen und es so unmöglich gemacht wird, die früheren Transaktionen zu manipulieren oder abzustreiten. Im Folgenden soll die Blockchain-Technologie anhand des Beispiels von Bitcoin erklärt werden.

Eine Blockchain besteht, wie der Name bereits andeutet, aus einer Kette von Blöcken. Jeder Block beinhaltet einen Verweis auf den vorhergehenden Block. Eine Besonderheit stellt der allererste Block der Kette dar, der „Genesis-Block", der Anfang 2009 geschürft wurde und natürlich keinen Vorgänger aufweist. Inzwischen beinhaltet die Bitcoin-Blockchain gut 630.000 Blöcke und ist auf 277 GB angewachsen (Blockchain 2020a).

Bitcoin verwendet ein asymmetrisches Verschlüsselungsverfahren zur Sicherstellung der grundlegenden Funktionsweise. Der Public Key eines Benutzers kann dabei als „Kontonummer" gesehen werden, an die andere Benutzer Münzen senden können, während der Private Key als Zugangscode zu diesem Konto dient und so garantiert, dass nur der berechtigte Benutzer auf das Konto zugreifen kann. Zudem werden die Münzen beim Versenden mit dem Private Key digital signiert und so die Herkunft eindeutig identifiziert.

Zum weiteren Verständnis muss klargestellt werden, dass es sich bei Bitcoin um keine Münzen im herkömmlichen Sinn handelt, auch um keine digitale Repräsentation solcher. Vielmehr werden die Kontostände der Beteiligten (die sogenannten Wallets) aus der gegebenen und in sich geschlossenen Menge von Transaktionen berechnet. Der Kontostand eines bestimmten Wallets ergibt sich aus dem Saldo aller Transaktionen von und zu diesem Wallet.

Jeder Block der Blockchain besteht aus einer Menge von Transaktionen. Eine Transaktion ist nichts anderes als eine Bewegung einer Anzahl von Münzen von Konto A zu Konto B. Von jeder Transaktion wird ein Hash gebildet, hierzu kommt das SHA-256 Verfahren zum Einsatz. Die Hashes der einzelnen Transaktionen innerhalb eines Blocks – zurzeit sind dies etwa 2.000 bis 2.500 Transaktionen pro Block (Blockchain 2020b) – werden in weiterer Folge in einer Baumstruktur („Merkle Tree“) zu einem Wurzel-Hash kombiniert. Mit diesem Hashwert, gemeinsam mit dem Hashwert des Vorgängerblocks und einer sogenannten „Nonce“ (=Number used once), wird nun der Hash des aktuellen Blocks berechnet, dieser wird auch „Proof of Work“ genannt. Dabei ist eine Schwierigkeit eingebaut, der Hashwert muss eine bestimmte Anzahl führender Nullen beinhalten. Um diese zu erreichen, wird die Nonce solange verändert, bis sich ein gewünschter Hashwert ergibt. Abhängig von der Gesamtrechenleistung des Systems wird der Schwierigkeitsgrad, also die benötigte Anzahl Nullen, dynamisch verändert, sodass sich immer eine konstante Zeit von etwa 10 Minuten für die Berechnung eines neuen Blocks ergibt.

Abbildung 8-1 zeigt die Zusammenhänge.

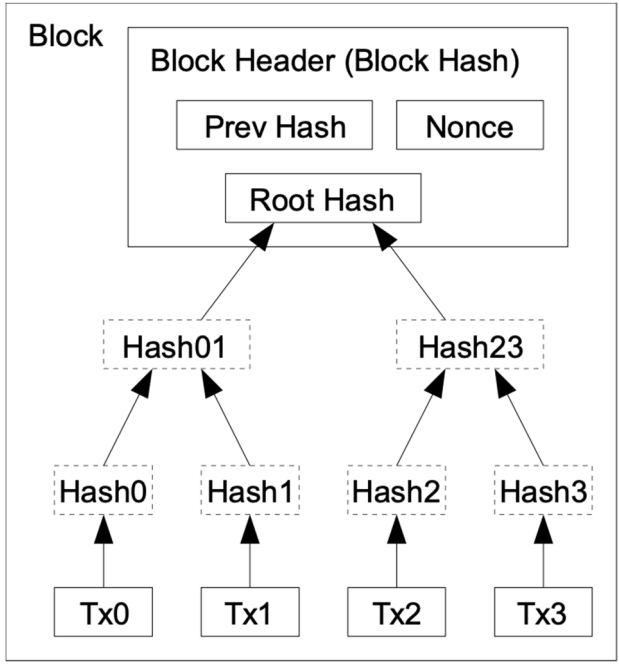


Abbildung 8-1: Merkle Tree in der Bitcoin Blockchain (Nakamoto 2008, S.4)

Die Berechnung dieser Hashes kann (zumindest theoretisch) jeder Benutzer durchführen, ist dies der Fall, wird dieser auch „Miner" genannt – er schürft sozusagen nach Münzen. Der Benutzer, der als erster einen gültigen Hash mit der geforderten Schwierigkeit findet, erhält als Belohnung eine definierte und stetig sinkende Anzahl Münzen. Bis zuletzt waren dies 12,5 Bitcoin, im Mai 2020 wurde die Belohnung jedoch auf 6,25 Bitcoin halbiert – eine Halbierung passiert alle 210.000 Blöcke. Diese durchaus lukrative Belohnung muss aber durch enorme Rechenleistung erkauft werden, weswegen das Schürfen für Privatanwender nicht mehr vernünftig darstellbar ist. Die Kontrolle eines gegebenen Hashs ist gemeinsam mit der gegebenen Nonce hingegen sehr einfach und von jedem Benutzer durchführbar – genau darauf basiert auch die Sicherheit und Überprüfbarkeit des Gesamtsystems.

2.3 Kryptowährungen und andere Anwendungen

Die Idee der meisten Blockchain-basierten Kryptowährungen ist, dass sie keine zentrale Steuerungseinheit und Kontrolle benötigen, sondern völlig autark von ihren Nutzern betrieben werden können. Es kann argumentiert werden, dass sich dadurch kein völliger Verzicht auf Vertrauen ergibt, sondern dass sich dieses lediglich von einer Gruppe der Stakeholder auf andere verschiebt und traditionelle Grundwerte von Vertrauen bestehen bleiben (Auinger & Riedl 2018, 7f.).

Der kryptographische Mechanismus von Bitcoin wird „Proof-of-Work" genannt, er ist für den inzwischen enormen Stromverbrauch des Systems verantwortlich. Proof-of-Work ist immer noch der am weitesten verbreitete Mechanismus, inzwischen wurden einige Alternativen entwickelt, die den Stromverbrauch des Gesamtsystems deutlich reduzieren können, ohne die Sicherheit oder Anonymität zu beeinträchtigen. Hierzu zählen „Proof-of-Stake", das das Recht auf Validierung von Blöcken an die Menge der Kryptowährung bindet, die ein bestimmter Teilnehmer besitzt, sowie an die Dauer, die diese Menge im Besitz des Teilnehmers ist (z. B. King & Nadal 2012). Es gibt Überlegungen, Ethereum – das in die Kategorie der Applikationsplattformen fällt (Herbert & Stabauer 2017, 34) und für einige Anwendungen in diesem Beitrag verwendet wird – auf einen Proof-of-Stake-Mechanismus umzustellen. Ein weiterer Mechanismus insbesondere für permissioned Blockchains, also solche mit eingebauter Autorisierung, ist „delegated Proof-of-Stake". Hierbei werden von den Teilnehmern Delegierte gewählt, von denen ausgegangen wird, dass sie sich im Sinne des Netzwerks verhalten, und die dann die Validierung von Blöcken übernehmen (Zheng et al. 2017, 560f.).

Eine weitere Einschränkung von Bitcoin ist die Beschränkung der Blockgröße auf 1MB. Diese hat eine Limitierung der maximal bearbeitbaren Transaktionen pro Zeiteinheit zur Folge. Diese Kapazität der Zahlungsplattform liegt weit unterhalb der herkömmlichen Netzwerke wie jene der großen Kreditkartenunternehmen. Die Limitierung der Transaktionen führt auch dazu, dass die eigentlich sehr geringen Transaktionsgebühren übermäßig steigen. Miner erhalten die Möglichkeit, Transaktionen mit hohem Aufschlag gegenüber anderen zu bevorzugen.

2.4 Verbindung zur realen Welt

Die Blockchain wurde ursprünglich ausschließlich für digitale Werte und Nachrichten konzipiert. Viele der Applikationen im folgenden Abschnitt basieren aber auf Daten aus der realen Welt. Diese Kombination ist Gegenstand eigener Forschungen.

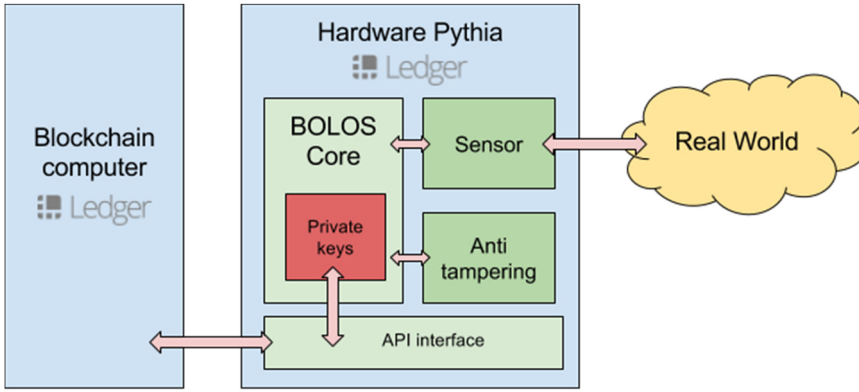


Abbildung 8-2: Verbindung zur realen Welt mit Pythis (Larchevêque 2016)

Ledger, ein Unternehmen, das vornehmlich Hardware Wallets herstellt und vertreibt, hat beispielsweise das Konzept der Hardware Pythia entwickelt, das fälschungssichere und digital signierte Sensordaten an die Blockchain weitergibt. Abbildung 8-2 zeigt die Zusammenhänge,

BOLOS steht hierbei für „Blockchain Open Ledger Operating System“, jenes Open Source Betriebssystem, das bei vielen Geräten des Unternehmens zum Einsatz kommt.

3 Anwendungsbereiche

Die Technologie der Blockchain bietet im Bereich der Mobilität eine große Menge von potenziellen Einsatzmöglichkeiten. Die wenigsten davon sind bisher tatsächlich produktiv im Einsatz oder umgesetzt, es handelt sich zumeist um Visionen, Konzepte und erste Prototypen. Die Frage, die sich bei den meisten Anwendungsbereichen stellt und die grundsätzlich mit Blockchain-basierten Implementierungen beantwortet werden kann, lautet:

Wer wusste wann was?

Eine beispielhafte Auswahl der in der Literatur vorgestellten Anwendungsbereiche soll nun im Folgenden diskutiert werden.

3.1 Schutz vor Tachomanipulation

Ein sehr einfaches und plakatives Beispiel für Einsatzmöglichkeiten der Blockchain in der Mobilität soll an erster Stelle genannt werden: Die Sicherung diverser Fahrzeugdaten wie beispielsweise des Kilometerstands. Wie im vorigen Abschnitt angeführt, kann ein einmal in die Blockchain gespeicherter Wert nicht mehr getilgt werden. Dies kann für einen digitalen Tacho bestens genutzt werden, indem der Kilometerstand eines Fahrzeugs – bzw. dessen Hashwert – regelmäßig in die Blockchain geschrieben wird. Wenn also beispielsweise ein Kilometerstand von 100.000 abgespeichert wurde, kann ein böswilliger Autoverkäufer das Fahrzeug nicht mehr mit 90.000 Kilometern anpreisen, bzw. könnte ein solcher Betrugsversuch leicht aufgedeckt werden.

Ein Konsortium rund um den Autozulieferer Bosch und den deutschen TÜV hat hierzu eine Lösung vorgestellt, siehe hierzu Abbildung 8-3.

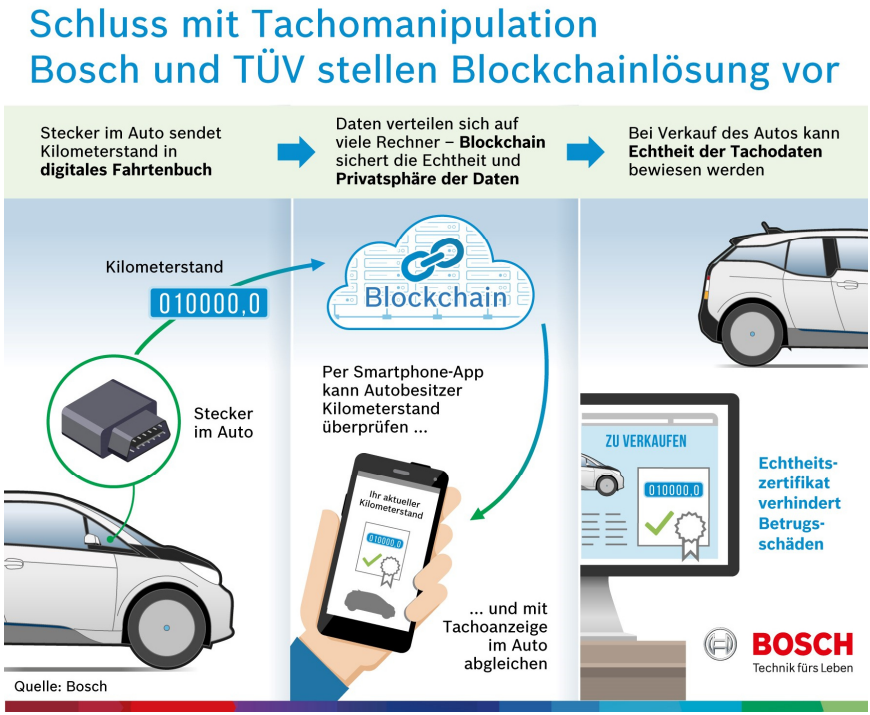


Abbildung 8-3: Tachomanipulation (Bosch 2017)

3.2 Logistik und Supply Chain

Ein weiteres Paradebeispiel für den Einsatz von Blockchains ist die Logistik. In Supply Chains werden zumeist eine oder mehrere von drei Arten von Gütern (Waren, Geld, Informationen) von einer Organisation bzw. Person zur anderen verschoben. Die Koordination dieser drei Güterflüsse erfolgt heute noch fast immer händisch. Eine Automatisierung könnte enormes Einsparungs-, Fehlervermeidungs- und Vereinfachungspotenzial mit sich bringen.

Große Player setzen auf die Blockchain und versprechen nicht weniger als eine Revolution, ähnlich entscheidend wie EDI vor über 30 Jahren. Ein Beispiel ist das Projekt „Hyperledger“ (Hyperledger 2020a), das seit 2016 von der Linux Foundation und über 270 Partnern wie IBM, Intel, Oracle, SAP, Airbus, Daimler, Swift und J.P.Morgan betrieben und weiterentwickelt wird. Dieses bietet mit Hyperledger Fabric ein Framework für die Entwicklung öffentlicher und geschlossener Blockchain-Applikationen und wird auch bereits im Umfeld der Supply Chain eingesetzt (Hyperledger 2020b).

Verschiedene Forschungs- bzw. potenzielle Anwendungsbereiche lassen sich hierbei identifizieren (z. B. Korpela et al. 2017, 4188f.):

- Smart Contracts zur teil- oder vollautomatischen Abwicklung der Lieferprozesse
- Einführung eines eigenen Zahlungsmittels innerhalb der Supply Chain
- Authentifizierung der Teilnehmer
- Erhöhung der Verbindlichkeit aller Prozesse und Dokumente
- Umgang mit unterschiedlichen Rechtslagen
- Standardisierung vs. Einzelfalllösungen in unterschiedlichen Supply Chains

Als Vorteile der Blockchain in diesen Bereichen werden häufig genannt (Chavanne & Pires 2017):

- Verkürzung der Liquiditätszyklen
- Verbesserung der Effizienz durch Verringerung von durch Zwischenhändler entstehenden Kosten
- Beschleunigung von Authentifizierung und Dokumentduplizierung
- Erhöhte Transparenz führt zu Verringerung von Fälschungen und Betrug
- Synchronisation der Entscheidungen in nahezu Echtzeit

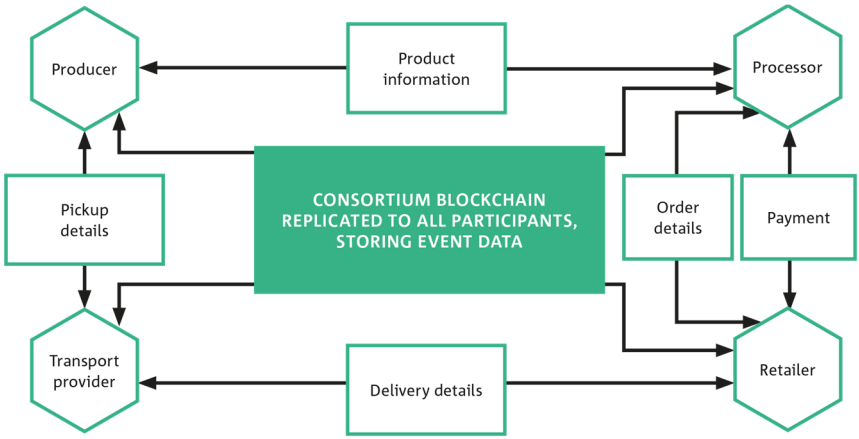


Abbildung 8-4: Blockchain in der Supply Chain (Staples et al. 2017, 14)

3.3 Mobility-as-a-Service (MaaS)

Mobility-as-a-Service wird als Überbegriff für verschiedenste Dienstleistungen im Bereich der Mobilität verwendet, beispielsweise werden On-Demand Fahrzeugservices, selbstfahrende Autos und Technologien im Bereich von Vehicle-to-Everything-Verbindungen umfasst. In der Literatur sind sehr unterschiedliche Definitionen getroffen worden, an dieser Stelle soll folgende Definition Berücksichtigung finden (Kamargianni & Matyas 2017, 4):

> *"Mobility as a Service is a user-centric, intelligent mobility distribution model in which all mobility service providers' offerings are aggregated by a sole mobility provider, the MaaS provider, and supplied to users through a single digital platform."*

Auch hier können Blockchain-basierte Implementierungen helfen, die entstehenden Sicherheits- und Kommunikationsprobleme zu lösen.

Als ein Beispiel sei „TravelToken" genannt, eine Ethereum-basierte Implementierung, die bei Buchung im Vorfeld Tickets in Form von QR-Codes generiert, welche dann im Zuge der Reise bei verschiedenen Mobilitätsdienstleistern eingelöst werden können (Karinsalo & Halunen 2018, 136f.). Smart Contracts sorgen hier für eine automatische Abrechnung beim Einlösen der Tickets oder bei Eintreten anderer vordefinierter Zustände.

3.4 Private E-Tankstellen

Die Zahl der Elektroautos ist im Steigen begriffen. Somit steigt auch die Zahl der benötigten Elektro-„Tankstellen" und die an ihnen ausgeführten Transaktionen. Allerdings findet sich zur Zeit das bekannte Problem von zweiseitigen Märkten: Viele Konsumenten lassen sich von der geringen Anzahl von Ladestationen vom Kauf eines Elektroautos abhalten, und umgekehrt ist der Betrieb von Ladestationen bei der aktuell geringen Marktdurchdringung von Elektroautos wirtschaftlich nicht darstellbar.

Eine Lösung dieses Henne-Ei-Problems könnte die P2P-Abrechnung privater Ladestationen bieten. Diese ermöglicht es privaten Anbietern verhältnismäßig einfach, ihre Ladeinfrastruktur anderen Autofahrern zur Verfügung zu stellen und die Ladevorgänge abzurechnen. Eine Variante wird in Abbildung 8-5 beschrieben: Elektroautos (Electric Vehicles, EV) und Ladestationen (Charging Stations, CS) kommunizieren hierfür verschlüsselt mit dem Smart Contract „ChargingPayment" auf einer Ethereum-basierten Blockchain (BC).

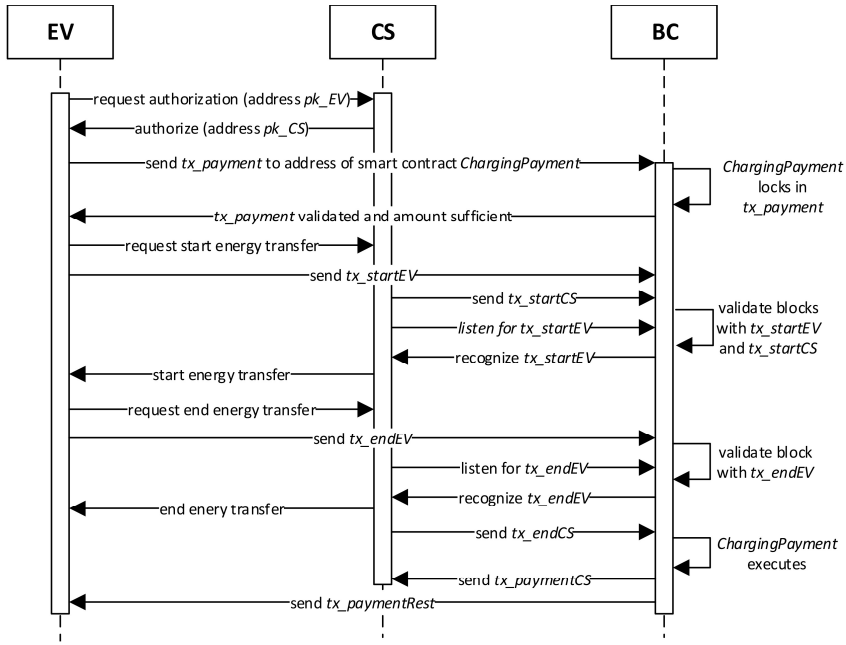


Abbildung 8-5: Laden bei E-Tankstellen (Kirpes & Becker 2018, 4)

Auch das rein private Laden könnte von Blockchain-basierten Techniken profitieren. Wenn etwa Informationen aus dem Smart Home oder dem Kalender des Benutzers mit einbezogen werden, kann der Ladezyklus dahingehend optimiert werden, dass der notwendige Akkustand für die Fahrten des nächsten Tages erreicht wird und gleichzeitig Spitzenlasten im Stromnetz vermieden werden. Durch eine vorausschauende Routenführung kann der Fahrzeugnutzer dann auch ggf. zu induktiven Ladepunkten an Ampeln oder ähnlichen Stellen geleitet werden (z.B. Share&Charge 2020).

3.5 Sensordaten von selbstfahrenden Autos

Noch über das automatische Abspeichern von Kilometerständen (siehe Abschnitt 3.1) hinaus geht der Versuch, weitere Sensordaten

sicher in die Blockchain zu speichern. „CertifiCar“ (Chanson et al. 2019, 1280ff.) ist ein Beispiel für ein solches Sensor Data Protection System (SDPS). Abbildung 8-6 zeigt die Architektur des Systems. Das System wurde in einem an Design Science orientierten Prozess implementiert und in 100 Autos über mehrere Wochen im Realbetrieb getestet. Ebenso wurden im Nachhinein Evaluations-Interviews geführt, die vielversprechende Ergebnisse brachten.

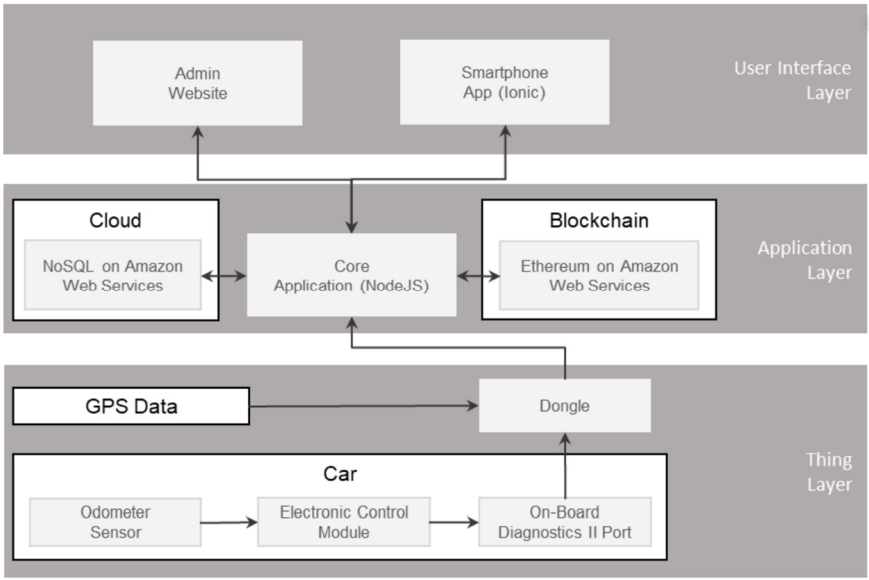


Abbildung 8-6: Architektur von CertifiCar (Chanson et al. 2019, 1288)

3.6 Remote Software Updates

Moderne PKWs können schon beinahe als Computer mit vier Rädern gesehen werden. Die Software des PKWs ist daher von essenzieller Bedeutung für dessen Funktionsweise. Dies gilt insbesondere im Hinblick auf die steigende Anzahl selbstfahrender Autos. Wenn sich in der Software ein sicherheitsrelevanter Fehler eingeschlichen hat, sollte dieser schnellstmöglich behoben werden. Mit dem Auto in die

Werkstatt zu fahren, kann aber einige Zeit in Anspruch nehmen, weshalb das Einspielen von Updates – nicht nur zum Bug Fixing, sondern auch zum Erweitern und Verbessern der Funktionalität – über eine drahtlose Verbindung eine durchaus sinnvolle Alternative ist. Da hierbei aber voller Zugriff auf die Fahrzeugsteuerung benötigt wird, stellt diese Art des Updates ein erhebliches Sicherheitsrisiko dar.

Das Durchführen der Softwareupdates über eine eigene Blockchain kann eine Lösung für diese Authentifizierungs- und Sicherheitsthemen sein, Abbildung 8-7 zeigt die Zusammenhänge: Die Updates werden sowohl vom Software Provider als auch vom Fahrzeughersteller (OEM) signiert (PK1 und PK2), die Fahrzeuge über die Blockchain bzw. deren Overlay Block Managers (OBM) vom Update verständigt und diese laden die Updates nach deren Verifizierung dann direkt herunter (Dorri et al. 2017, 122f.).

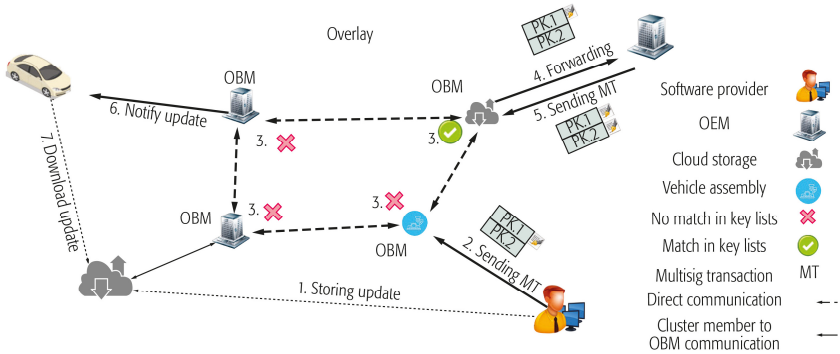


Abbildung 8-7: Softwareupdates bei Fahrzeugen (Dorri et al. 2017, 123)

4 Fazit

Das Potenzial der Blockchain wird – wie in den meisten Forschungsbereichen – auch im Gebiet der Mobilität bisher nur sehr bedingt ausgeschöpft. Ob sich in naher Zukunft zu einigen der angeführten Anwendungsfeldern tatsächlich praxistaugliche Implementierungen zeigen werden, ist noch nicht absehbar. Es ist möglich, dass die Blockchain ganze Industrien wie die Logistik revolutionieren kann, oder aber sie bleibt eine „Lösung auf der Suche nach ihrem Problem". Dies wird nicht zuletzt von der Unterstützung durch größere Organisationen und die globale und lokale Gesetzgebung abhängen. Auch wird die Frage sein, wie die nächste Generation der Kryptowährungen mit den bekannten Problemen der aktuellen Generation umgeht. Hier zeigen sich erste Tendenzen und unterschiedliche Entwicklungsrichtungen – es bleibt spannend.

Literaturverzeichnis

Auinger, A., & Riedl, R. (2018). Blockchain and Trust: Refuting Some Widely-held Misconceptions. In: *Proceedings of the International Conference on Information Systems*.

Blockchain (2020a). https://www.blockchain.com/de/charts/blocks-size [19.12.2020].

Blockchain (2020b). https://www.blockchain.com/de/charts/n-transactions-per-block [19.12.2020].

Bloomberg, J. (2017). Eight Reasons To Be Skeptical About Blockchain. *Forbes*, 31. Mai, 2017. https://www.forbes.com/sites/jasonbloomberg/2017/05/31/eight-reasons-to-be-skeptical-about-blockchain [19.12.2020].

Bosch (2017). Bosch und weitere internationale Unternehmen gründen neues Bündnis zur Nutzung von Blockchain und verwandten Technologien, 19. September, 2017. https://www.bosch-presse.de/pressportal/de/de/bosch-und-weitere-internationale-unternehmen-gruenden-neues-buendnis-zur-nutzung-von-blockchain-und-verwandten-technologien-126592.html [19.12.2020].

Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., & Wortmann, F. (2019). Blockchain for the IoT: Privacy-Preserving Protection of Sensor Data. *Journal of the Association for Information Systems*, 20(9), 1271-1307.

Chavanne, Y., Pires, T. (2017). Die Blockchain entrümpelt die Supply Chain, *Netzwoche*, 1. September, 2017. https://www.netzwoche.ch/news/2017-09-01/die-blockchain-entruempelt-die-supply-chain [19.12.2020].

Dorri, A., Steger, M., Kanhere S., & Jurdak, R. (2017). BlockChain: A Distributed Solution to Automotive Security and Privacy. *IEEE Communications Magazine*, 55(12), 119-125.

European Commission (2019). https://ec.europa.eu/digital-single-market/en/blockchain-technologies [19.12.2020].

Eurostat (2017). Internet-Käufe durch Einzelpersonen [isoc_ec_ibuy].

Schäfers, M. (2019). Gegen Libra, für Blockchain, *FAZ*, 18. September, 2019. https://www.faz.net/aktuell/finanzen/digital-bezahlen/regierung-foerdert-blockchain-und-bekaempft-libra-16391393.html [19.12.2020].

Herbert, J. & Stabauer, M. (2017). Bitcoin & Co: An Ontology for categorising Cryptocurrencies.*International Journal of Multidisciplinarity in Business and Science*, 3(3), 29-37.

Hyperledger (2020a). https://www.hyperledger.org [19.12.2020].

Hyperledger (2020b). https://www.ibm.com/blockchain/hyperledger [19.12.2020].

IBM (2017). Maersk and IBM Unveil First Industry-Wide Cross-Border Supply Chain Solution on Blockchain. http://www-03.ibm.com/press/us/en/pressrelease/51712.wss [19.12.2020].

Kamargianni, M. & Matyas, M. (2017). The Business Ecosystem of Mobility as a Service. In: *Proceedings of the 96th Transportation Research Board (TRB) Annual Meeting.*

Karinsalo, A. & Halunen, K. (2018). Smart Contracts for a Mobility-as-a-Service Ecosystem. In: *Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security Companion.*

King, S. & Nadal, S. (2012). PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, 19. August, 2012. https://bitcoin.peryaudo.org/vendor/peercoin-paper.pdf [19.12.2020].

Kirpes, B. & Becker, C. (2018). Processing Electric Vehicle Charging Transactions in a Blockchain-based Information System. In: *Proceedings of the Twenty-fourth Americas Conference on Information Systems (AMCIS).*

Korpela, K., Hallikas, J., & Dahlberg, T. (2017). Digital Supply Chain Transformation toward Blockchain Integration. In: *Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS)*.

Larchevêque, E. (2016). Hardware Pythias: Bridging the Real World to the Blockchain, 31. August, 2016. https://www.ledger.com/hardware-pythias-bridging-the-real-world-to-the-blockchain [19.12.2020].

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf [19.12.2020].

Panetta, K. (2018). 5 Trends Emerge in the Gartner Hype Cycle for Emerging Technologies 2018, 16. August, 2018. https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018 [19.12.2020].

Rossi, M., Mueller-Bloch, C., Bennett Thatcher, J., & Beck, R. (2019). Blockchain Research in Information Systems: Current Trends and an Inclusive Future Research Agenda. *Journal of the Association for Information Systems*, 20(9), 1388-1403.

Share&Charge (2020). https://shareandcharge.com [19.12.2020].

Staples, M., Chen, S., Falamaki, S., Ponomarev, A., Rimba, P., Tran, A. B., Weber, I., Xu, X., Zhu, J., (2017). Risks and opportunities for systems using blockchain and smart contracts. http://data61.csiro.au/~/media/D61/Files/Blockchain-reports/Blockchain-RisksandOpps-PDF.pdf [19.12.2020].

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In: *Proceedings of the IEEE International Congress on Big Data*, 557-564.