Blockchain und Privacy

Problemstellung und Lösungen aus Perspektive des HANSEBLOC-Projekts

Thomas Twenhöven, Kühne Logistics University, Björn Engelmann, itemis AG, Julian Kakarott, HAW Hamburg, Kevin Westphal, Consider IT GmbH und Moritz Petersen, Kühne Logistics University

Blockchain ist als Plattform für den Austausch von Daten nach wie vor in aller Munde. Entscheidend für die Akzeptanz der Technologie im geschäftlichen Kontext ist allerdings die Wahrung von Geschäftsgeheimnissen bzw. die Einhaltung gesetzlicher Vorgaben wie der Datenschutzgrundverordnung. Die Blockchain-inhärente Sichtbarkeit aller gespeicherten Daten für alle Teilnehmer, wegen der die Plattform letztlich eingesetzt wird, kann dabei zum Problem werden. In der Praxis werden deshalb verschiedene Verfahren eingesetzt, um Daten vor unbefugtem Zugriff zu schützen, ohne dabei die Vorteile einer verteilten Datenbankstruktur einzubüßen. In diesem Beitrag stellen wir entsprechende Verfahren vor und berichten von den Erfahrungen des HANSEBLOC-Projekts, das die Nutzung von Blockchain für den Datenaustausch im Logistikbereich untersucht.

Blockchain and Privacy: Problems and Solutions from the HANSEBLOC Project

Blockchain holds high potential for various applications. In the business context, one of its key features – the availability of data to various parties – is a liability as business secrets shouldn't be exposed and GDPR compliance has to be ensured. In this paper, we discuss solutions for these privacy problems. Also, we present the HANSEBLOC project, a blockchain-powered platform for data exchange in logistics, and the chosen privacy solutions.

Keywords:
blockchain, privacy, confidentiality, logistics, GDPR

Die Blockchain ist eine vergleichsweise junge Technologie, die gegenwärtig als Lösung für zahlreiche Probleme in verschiedenen Branchen erprobt wird [1]. Sie verspricht, eine Vielzahl von Akteuren auf einer für alle Teilnehmer offenen Plattform zu verbinden und eine vertrauenswürdige Datenbasis für deren Interaktion bereitzustellen. Durch die Nutzung dieser dezentralen Plattform entfällt – soweit die Theorie – der Bedarf für digitale Schnittstellen und analogen Informationsaustausch. Aus diesem Grund erscheint Blockchain besonders attraktiv für die Logistikbranche, die sich heute vielfach durch analoge Interaktionen einer Vielzahl von kleinen und mittleren Unternehmen auszeichnet [1]. Beim Informationsaustausch geht es hier sowohl um allgemeine Daten zum Transport und zu den transportierten Gütern, als auch um den Status des Transportprozesses: An welchem Ort und in wessen Besitz sich die Fracht gegenwärtig befindet, ist heute in vielen Logistikketten nicht in Echtzeit feststellbar. Die Erhebung und vor allem Weitergabe dieser Informationen ist im Umfeld komplexer Lieferketten und zahlreicher beteiligter Unternehmen eine herausfordernde Aufgabe. Die Logistikbranche erscheint darum prädestiniert für den Einsatz der Blockchain [2].

Privacy-Anforderungen als Problemstellung

Für eine sichere und zuverlässige Datenspeicherung nutzt die Blockchain zum einen die namensgebende Verkettung der Datenblöcke zu einer „Chain" und zum anderen die redundante Speicherung der Daten. Jeder Knoten eines Netzwerks hält eine eigene Kopie der Daten vor und kann jederzeit auf sie zugreifen. Dieses Konzept stellt die Unverfälschbarkeit der Daten sicher [3]. Durch den verteilten Zugang ist es von großer Wichtigkeit, nur solche Daten auf der Blockchain zu speichern, die öffentlich einsehbar sein dürfen. Zu beachten sind neben der Wahrung geschäftlicher Interessen auch juristische Beschränkungen wie beispielsweise die Datenschutzgrundverordnung (DSGVO) für personenbezogene Daten [2]. Es besteht also ein Zielkonflikt zwischen der sicheren (verteilten) und der geheimen Speicherung der Daten [4].

In logistischen Prozessen besitzen vor allem die Transportdaten eine hohe Relevanz, weil Transportaufträge aus verschiedenen Gründen fremdvergeben werden und an einem gebuchten Transportvorgang zwischen Quelle und Senke teilweise fünf oder sechs selbstständige Unternehmen beteiligt sind. Im Interesse aller Beteiligten sollte der Zugang zu den Transportdaten nur denjenigen Parteien möglich sein, die diesen Zugang auch benötigen. Eine Datenspeicherung auf der Blockchain ist im Klartext deswegen ausgeschlossen. Damit verbietet sich allerdings auch die Verwendung von Smart Contracts, die auf Basis der zu schützenden Daten bestimmte Aktionen ausführen

M. Sc. Thomas Twenhöven arbeitet als wissenschaftlicher Mitarbeiter im Department of Logistics der Kühne Logistics University in Hamburg.

Dr. Björn Engelmann arbeitet als IT-Consultant für die itemis AG am Standort Hamburg.

B. Sc. Julian Kakarott arbeitet als wissenschaftlicher Mitarbeiter in der Arbeitsgruppe DLT³ der Hochschule für Angewandte Wissenschaften in Hamburg.

B. A. Kevin Westphal arbeitet als IT-Consultant für die Consider IT GmbH in Hamburg.

Dr.-Ing. Moritz Petersen arbeitet als Senior Researcher im Department of Logistics der Kühne Logistics University in Hamburg und ist Habilitand an der Technischer Universität Hamburg.

thomas.twenhoeven@the-klu.org
www.the-klu.org

https://doi.org/10.30844/I40M_20-1_S45-48

können. Ohne die Daten sind die Verträge nicht lauffähig.

Doch auch ohne das direkte Abspeichern von Daten auf der Blockchain entstehen durch Transaktionen sogenannte Metadaten, die Rückschlüsse auf geschäftliche Aktivitäten der Unternehmen zulassen [2]. Hierbei geht es vor allem (aber keinesfalls ausschließlich) um die Blockchain-Kontonummern und alle anderen kryptografischen Schlüssel der jeweiligen Unternehmen, von denen alle Transaktionen auf der Blockchain ausgehen [5]. Aus der Analyse dieser Kontonummern lassen sich Geschäftsbeziehungen, Wertschöpfungsketten, Auftragszahlen und andere relevante Informationen ableiten. Entscheidend ist dafür allerdings die Zuordnung des Kontos zu einem konkreten Unternehmen – so lange diese Zuordnung nicht möglich ist, bleibt das Unternehmen geschützt. Mithilfe einer Analyse der zahlreichen Transaktionen zwischen Unternehmen lässt sich allerdings durchaus ableiten, welches Unternehmen zu welchem Konto gehört [2].

Lösungsansätze

Verschiedene Lösungsansätze können zur Geheimhaltung der Informationen verfolgt werden. Zu unterscheiden ist hierbei zwischen der Speicherung der Daten selbst, dem daraus resultierenden Problem mit der Ausführung von Smart Contracts und schlussendlich den anfallenden Metadaten. Bild 1 gibt vorab einen Überblick über Lösungen und mögliche Folgeprobleme.

Lösungsansätze für vertrauliche Datenspeicherung

Der erste und technisch einfachste Lösungsansatz ist die Speicherung relevanter Daten außerhalb der Blockchain. Statt der Daten wird ein digitaler Fingerabdruck, ein sogenannter Hash, auf der Blockchain gespeichert. Dieser Fingerabdruck lässt keine Rückschlüsse auf die tatsächlichen Daten zu. Wenn die Daten außerhalb der Blockchain an die berechtigten Parteien übertragen werden, können alle beteiligten Parteien nun eigenständig den Hash der Daten berechnen und mit dem Hash auf der Blockchain abgleichen. Sie stimmen aber nur dann überein, wenn keine Veränderung der Daten stattgefunden hat. Denkbar wäre beispielsweise, dass nur der Fingerabdruck eines Vertrags und die zugehörigen „Unterschriften" auf der Blockchain gespeichert werden. So kann die Blockchain die Vertragsabwicklung unterstützen, ohne die Inhalte öffentlich zu machen [6]. Metadaten werden hiermit allerdings nicht geschützt, da die jeweiligen Akteure und ihre Interaktionen als solche einsehbar bleiben. Dieser Ansatz verhindert außerdem die automatisierte Vertragsabwicklung im Rahmen von Smart Contracts, da weder die Vertragsbestimmungen noch die Informationen über den Transport selbst auf der Blockchain abgelegt sind.

Ein weiterer, ähnlicher Ansatz ist die Speicherung von verschlüsselten Inhalten auf der Blockchain. Im Unterschied zum Hash werden hier die tatsächlichen Inhalte gespeichert. Die verschlüsselten Inhalte sind damit öffentlich, aber nur für diejenigen Parteien zu entschlüsseln, die die entsprechenden Passwörter kennen. Somit werden Systeme zum Management der Passwörter nötig, was die Komplexität der Speicherung von Blockchain-Passwörtern („private keys") weiter steigert. Im Vergleich zur ersten Lösung wird der Datenaustausch außerhalb der Blockchain durch die Nutzung der Blockchain selbst ersetzt. Die Probleme mit Metadaten und der Ausführung von Smart Contracts bleiben allerdings bestehen.

Lösungsansätze für die Ausführung von Smart Contracts

Für die Ausführung von Smart Contracts bzw. der Rechenoperationen auf Basis der unzugänglichen Daten bestehen ebenfalls zwei theoretisch denkbare Lösungsansätze. Auch hier gibt es eine technisch unkomplizierte Lösung – die Daten werden auf einem der oben beschriebenen Wege an eine dritte Partei übertragen, die das Ergebnis entsprechend zur Verfügung stellt. Die dritte Partei hat in diesem Fall Zugriff auf die Daten und die Möglichkeit, das Ergebnis zu verfälschen. Der Rückgriff auf eine solche (hoffentlich vertrauenswürdige) dritte Partei stellt also das Konzept einer Blockchain insgesamt in Frage.

Bild 1: Geheimhaltung von Informationen auf der Blockchain – Probleme, Lösungen und Folgeprobleme.

Problem	Lösungen	Folgeprobleme
Geheimhaltung von Daten	Off-Chain-Speicherung	Ausführung von Smart Contracts nicht möglich
	Verschlüsselte Speicherung	Ausführung von Smart Contracts nicht möglich
Ausführung von Smart Contracts nicht möglich	Dritte Partei	Zentrale Rolle für dritte Partei
	Zero-Knowledge Proof	Technisch nicht ausgereift
Geheimhaltung von Metadaten	Wegwerf-Konten	Transaktionsgebühren verraten Kontoinhaber

Technisch deutlich komplizierter sind die sogenannten zero knowledge proofs (ZKP). Hierbei handelt es sich um ein neuartiges kryptografisches System, mit dessen Hilfe die Gültigkeit einer Behauptung bewiesen werden kann, ohne die für eine Überprüfung eigentlich notwendigen Informationen zu verwenden. Als Beispiel ist vorstellbar, dass ein Unternehmen das Inventar eines bestimmten Produkts mithilfe der Blockchain publiziert. Anstatt der tatsächlichen Zahl X wird nur ihr Hash auf der Blockchain gespeichert. Zusätzlich veröffentlicht das Unternehmen nun die Behauptung „Das Inventar ist größer als 20". Formal betrachtet handelt es sich hierbei um das Ergebnis einer Berechnung („Ist X größer als 20?") auf Basis dieser Zahl. Die Geschäftspartner können sich nun darauf verlassen, dass das veröffentlichte Ergebnis („Ja") dieser Berechnung korrekt ist, ohne den Eingangswert (z. B. 49) zu kennen. Dieser Richtigkeitsbeweis auf Basis von „Null Wissen" ist Namensstifter für ZKP. Damit können auch komplexe Verträge oder die vollständig anonyme Übertragung von Kryptowährungen umgesetzt werden. ZKP ist zwar schon funktionstüchtig, hat aber noch nicht die nötige Stabilität für den produktiven Einsatz [7].

Lösungsansätze für Metadaten

Bezüglich der Metadaten können von den jeweiligen Unternehmen für verschiedene Geschäftsbeziehungen komplett unabhängige „Wegwerf-Konten" verwendet werden, die nur für diesen Zweck genutzt werden. Die Identität des dahinterstehenden Unternehmens muss dem jeweiligen Partner auf vertraulichem Wege mitgeteilt werden. Hierbei werden die Transaktionsgebühren zum Problem – Ethereum basierte Blockchains erfordern üblicherweise die Bezahlung einer geringen Gebühr für jede Transaktion. Die finanzielle Ausstattung der Wegwerf-Konten offenbart jedoch die Identität des Kontoinhabers, da Überweisungen zurückverfolgt werden können.

Vergleichbar mit Smart Contracts können für diese anonymen Überweisungen dritte Parteien (Metatransactions) oder ZKP verwendet werden. Denkbar ist auch, dass ein am Transport beteiligtes Unternehmen die Gebühren für alle anderen übernimmt und nur dieses eine Unternehmen als Teilnehmer identifizierbar wird. Hierbei sind verschiedene Konstellationen möglich – entscheidend ist nur, dass die Gebühr auf irgendeine Art und Weise bezahlt wird und der Einfluss etwaig beteiligter dritter Parteien minimal ist. Bei einer entsprechenden Struktur der zugrundeliegenden Blockchain kann gänzlich auf Transaktionsgebühren verzichtet werden; es entsteht allerdings das Problem von Spam-Transaktionen.

Fallbeispiel HANSEBLOC

Das Privacy-Problem und die möglichen Lösungsansätze werden im Folgenden anhand des HANSEBLOC-Projekts illustriert. HANSEBLOC ist ein gemeinsames Forschungs- und Entwicklungsprojekt von vier Logistikunternehmen, vier IT-Dienstleistern und zwei Hochschulen aus Norddeutschland unter der Leitung der Logistik-Initiative Hamburg. Das Projekt arbeitet in seiner 30-monatigen Laufzeit an der Blockchain basierten Dokumentation von Transportprozessen.

Im Frachtverkehr spielt eine fälschungssichere Dokumentation von Absprachen, Vertragsbedingungen und Umladungen eine wichtige Rolle. Aufgrund der Vielzahl an beteiligten Unternehmen und des insgesamt stark fragmentierten Marktes ist es bisher nicht gelungen, eine Plattform als Speicherort für derartige Informationen zu etablieren. Zu bedenken ist hier die Machtposition, die eine solche Plattform gegenüber der Logistikbranche insgesamt einnehmen würde. Aus diesem Grund wird solchen Plattformen eher mit Misstrauen begegnet – vor allem, wenn die Plattform durch ein Logistikunternehmen betrieben wird.

HANSEBLOC verfolgt drei Entwicklungsschwerpunkte:

- die Sicherung der Frachtbriefdaten eines Transportvorgangs,
- die Echtzeitdokumentation von Übergängen der Fracht von einer Partei zu einer anderen (sogenannte Gefahrenübergänge) und
- die Einbindung von Daten, die von Sensoren an Ladung oder Fahrzeug gesammelt werden.

Die Verwendung von Smart Contracts im engeren Sinne ist dafür nicht erforderlich. Bild 2 gibt einen Überblick des HANSEBLOC-Systems.

Ein Beispiel aus dem Anwendungsgebiet von HANSEBLOC ist der digitale Frachtbrief. Zu Beginn eines Transportvorgangs definiert der Auftraggeber bestimmte Grunddaten wie Abhol- und Lieferorte, Zeitfenster und Verantwortlichkeiten, die im Frachtbrief festgehalten werden. Weil auch ein digitaler Frachtbrief im Verlauf des Transportprozesses durch viele Hände geht, speichert der Auftraggeber lediglich den Hash der Frachtbriefdaten auf der Blockchain. Die eigentlichen Daten werden über eine herkömmliche Schnittstelle ausge-

https://doi.org/10.30844/I40M_20-1_S45-48

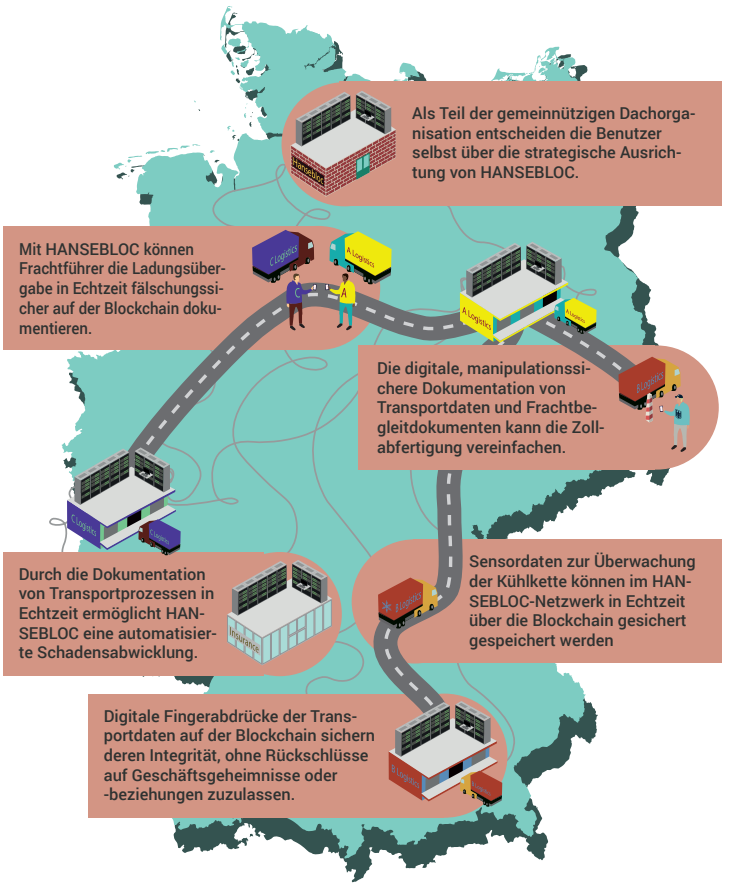

Bild 2: Struktur des HANSEBLOC-Systems.

tauscht, die ebenfalls im Rahmen des Projekts definiert wird.

Bezüglich der Metadaten werden auf der HANSEBLOC-Blockchain für jeden Transportvorgang neue Wegwerf-Konten genutzt. Die Eigentümer dieser Konten identifizieren sich untereinander durch eine herkömmliche Schnittstelle und bleiben gegenüber dritten Parteien anonym; die anfallenden Metadaten erlauben keine Identifikation der beteiligten Parteien. Nicht abschließend geklärt ist der Umgang mit Transaktionsgebühren, die Vorzugsvariante ist die Nutzung von Metatransactions. Eine endgültige Entscheidung steht zum Zeitpunkt der Veröffentlichung dieses Beitrags allerdings noch aus.

Im Gesamtsystem können dritte Parteien zwar einsehen, dass ein Transport stattfindet und dafür mehrere Unternehmen interagieren – nicht aber, was konkret transportiert wird (Off-chain-Datenspeicherung) oder welche Firmen daran beteiligt sind (Metadaten). Dadurch bleiben alle vertraulichen Informationen geheim.

Fazit

Wie dieser Beitrag aufzeigt, bietet die Blockchain neue Möglichkeiten, schafft aber auch neue Probleme. Die verteilte Speicherung von Daten macht sie notwendigerweise öffentlich.

Komplexe technische Systeme sind erforderlich, um das dabei auftretende Problem der Datensicherheit im Geschäftskontext zu lösen. Der Teufel steckt im Detail: Bei der Verarbeitung können anfallende Metadaten ähnlich wichtig sein wie die zugrundeliegenden Daten selbst und die verschiedenen Lösungen ziehen Folgeprobleme nach sich. Dennoch zeigt sich, dass die Probleme der Blockchain prinzipiell nicht unlösbar sind.

Das HANSEBLOC-Projekt beschränkt sich auf spezielle Anwendungsfälle aus der Logistik. Die Erfahrungen aus dem Projekt sind allerdings für zahlreiche Branchen interessant, denn Geschäftsgeheimnisse und -beziehungen sind fast immer ein entscheidender Teil des Wettbewerbs. Die hier dargestellten Probleme beziehen sich auf Business-Blockchains und entstammen nicht dem Ökosystem der Public Blockchains wie Bitcoin und Ethereum, die die Blockchain als Technologie bekannt gemacht haben. Dennoch lässt sich beobachten, dass Lösungen für Probleme der Geschäftswelt, wie beispielsweise ZKP oder Metatransactions, nicht selten zunächst für Public Blockchains entwickelt werden, die ihre technische Vorreiterrolle nach wie vor verteidigen.

Dieser Beitrag entstand im Rahmen des Projekts „HANSEBLOC – Hanseatische Blockchain-Innovationen für Logistik und Supply Chain Management", das durch das Bundesministerium für Bildung und Forschung (BMBF) unter dem Kennzeichen 03VNE2044J gefördert wird. Die Verantwortung für den Inhalt dieses Beitrags liegt bei den Autoren.

Schlüsselwörter:
Blockchain, Vertraulichkeit, Datenschutz, Logistik, DSGVO

Literatur

[1] Petersen, M.; Hackius, N.; von See, B.: Mapping the Sea of Opportunities: Blockchain in Supply Chain and Logistics. In: it – Information Technology 60 (2018) 5-6, S. 263-271.
[2] Hackius, N.; Reimers, S.; Kersten, W.: The Privacy Barrier for Blockchain in Logistics. In: Bierwirth, C., u. a. (Hrsg): Logistics Management. Berlin 2019.
[3] Mougayar, W.: The Business Blockchain, 1. Auflage. Hoboken 2016.
[4] Henry, R.; Herzberg, A.; Kate, A.: Blockchain Access Privacy: Challenges and Directions. In: IEEE Security Privacy 16 (2018) 4, S. 38–45.
[5] Wood, D. G.: Ethereum: A Secure Decentralized Generalized Transaction Ledger. Ethereum Foundation 2014.
[6] Buterin, V.: Zk-SNARKs: Under the Hood. URL: https://medium.com/@VitalikButerin/zk-snarks-under-the-hood-b33151a013f6, Abrufdatum 03.09.2019.
[7] Eberhardt, J.; Tai, S.: On or Off the Blockchain? Insights on Off-Chaining Computation and Data. In: De Paoli, F.; Schulte, S.; Johnsen, E. Broch: Service-Oriented and Cloud Computing. Berlin 2017.