



DECHEMA

Gesellschaft für Chemische Technik
und Biotechnologie e.V.

STATUSPAPIER

Blockchain in der Prozessindustrie



IMPRESSUM**Autoren**

Andrei Barascu, Dr. Oliver Hurtig, Dr. Alexander Möller

Herausgeber

DECHEMA e.V.
Theodor-Heuss-Allee 25
60486 Frankfurt am Main

Verantwortlich im Sinne des Presserechts

DECHEMA e.V.
Dr. Andreas Förster
Theodor-Heuss-Allee 25
60486 Frankfurt am Main

Gestaltung/Satz

PM-GrafikDesign
Peter Mück, Wächtersbach

Druck

Seltersdruck & Verlag Lehn GmbH & Co. KG
Selters

Erschienen im Oktober 2020

1. Auflage

ISBN: 978-3-89746-230-4

Inhalt

1	Einleitung	4
2	Was ist eine Blockchain?	5
3	Vorteile und Grenzen von Blockchain	7
	3.1 Manipulationssicherheit	7
	3.2 Verteilung im gesamten Netzwerk	8
	3.3 Ressourcenbedarf	8
	3.4 Abbildung der Realität	9
4	Anwendungsfälle für Blockchain in der Prozessindustrie	10
	4.1 Blockchain für das GxP am Beispiel der pharmazeutischen Industrie	10
	4.2 Blockchain für Logistik und Supply Chain Management – Track and Trace	10
	4.3 Asset Life Cycle Monitoring	12
	4.4 Machine-Controlled-Maintenance	12
	4.5 Smart Contracts und automatisiertes Rechnungswesen	12
5	Fazit	14
	5.1 Wofür ist Blockchain geeignet?	14
	5.2 Blockchain oder klassische Datenbank?	14
	5.3 Blockchain als Enabler im Change Management	14
	5.4 Die Datenbasis nicht aus dem Blick verlieren	14
6	Begriffserklärung zum Thema Blockchain	16

1 Einleitung

Die Blockchain ist im Kontext des digitalen Wandels eines der meist diskutierten Themen. Gleichzeitig besteht vielfach Unsicherheit: Was ist eine Blockchain überhaupt? In welchen Bereichen bietet sie einen Mehrwert gegenüber klassischen Datenbanken? Dieses Statuspapier versucht, bestehende Unsicherheiten aufzulösen und den Mehrwert für die Prozessindustrie darzustellen. Dazu werden zunächst die grundlegenden Eigenschaften von Blockchains erläutert, um anschließend mögliche Nutzungsfelder speziell für die Prozessindustrie zu beleuchten. Auch die Grenzen dieser Technologie werden diskutiert.

Der Entwicklungsursprung von Blockchains liegt im digitalen Zahlungsverkehr und geht auf Satoshi Nakamoto zurück, der im Jahr 2008 die Bitcoin-Blockchain etablierte.¹ Da Blockchains eine Variante der Distributed-Ledger-

Technologie (übersetzt *verteilt Hauptbuch*) sind, eignen sie sich insbesondere für Anwendungsfälle mit einer Hauptbuch-ähnlichen Datenstruktur. Einige der Konzepte lassen sich jedoch auch auf z. B. Logistikanwendungen übertragen. Die Manipulationssicherheit von Blockchains ermöglicht einen Einsatz für kritische Dokumentationsprozesse, zum Beispiel im GxP-Umfeld.² Auch neue, noch in Entwicklung befindliche Geschäftsmodelle wie Machine-as-a-Service können vom Einsatz einer Blockchain profitieren. Ob der Einsatz einer Blockchain oder von Teilaspekten der Technologie sinnvoll ist, hängt vom Einzelfall ab. Konkrete Anwendungsfälle werden in Abschnitt 4 betrachtet. Die Kernaussagen zu Blockchain sind im Anschluss an das Fazit in Abschnitt 5 zusammengefasst. Eine kurze Erklärung zu blockchainspezifischen Begriffen wird in Abschnitt 6 gegeben.

¹ Bitcoin.org, "Bitcoin: A Peer-to-Peer Electronic Cash System", <https://bitcoin.org/en/bitcoin-paper>

² GxP ist ein Sammelbegriff für diverse Qualitätssicherungssysteme, z.B. GMP (Good Manufacturing Practice), GLP (Good Laboratory Practice), etc.

2 Was ist eine Blockchain?

Eine Blockchain ist eine Art der Distributed-Ledger-Technologie, also eine verteilte Datenbank mit Hauptbuch-analoger Struktur, in welcher Datensätze (Transaktionen³) vollständig, chronologisch und unveränderbar abgelegt und gespeichert werden. Die **Verteilung** einer vollständigen und aktuellen Kopie der Blockchain über alle Nutzer des Netzwerks (sog. Knoten) bewirkt ein hohes Maß an Manipulationssicherheit der abgelegten Datensätze. Damit alle Knoten eine immer identische und aktuelle Version der Blockchain vorhalten, besitzt jede Blockchain einen sog. Konsens-Mechanismus, also einen Algorithmus, welcher über die „richtige“ Version der Blockchain entscheidet und diese an alle Knoten verteilt. Weil der Konsens-Mechanismus nicht von einer Partei alleine übernommen werden kann, entsteht so eine gesicherte, fälschungssichere und unstrittige „Single Source of Truth“ (einzige Quelle der Wahrheit). Diese eignet sich gut, Transaktionen und andere kurze, strukturierte Datensätze zwischen Parteien festzuhalten, ohne auf eine zentrale Stelle vertrauen zu müssen.⁴

Im bekannten Fall der öffentlichen Blockchains (Bitcoin, Ethereum, etc.) kann sich jeder Knoten an der Blockerstellung beteiligen. Der Konsens-Mechanismus kann aber auch so ausgestaltet werden, dass nur vorher ausgewählte Knoten die Validierung (Erstellung eines neuen Blocks) durchführen dürfen. In diesem Fall spricht man von genehmigungsbasierten Blockchain-Systemen.⁵

Eine weitere Besonderheit der Blockchain ist, dass die Daten in Blöcken zusammengefasst, neue Blöcke in der Art einer Kette an das Ende des Hauptbuchs angehängt und mit den vorherigen Blöcken über **Kryptografie** verbunden werden. Dazu wird in jedem neuen Block eine verschlüsselte Referenzierung auf die vorherigen Blöcke gespeichert, der so genannte Hashwert. Durch dieses Hashing-Verfahren und die Verteilung über das gesamte Blockchain-Netzwerk ist ein nachträgliches Ändern von

Transaktionen nahezu unmöglich. Eine Transaktion, also ein Datensatz, kann nahezu beliebige Daten enthalten, so dass eine Blockchain-Architektur als Datenablage genutzt werden kann. Die Erzeugung und Nutzung einer digitalen Währung, wie sie in den bekannten FinTech-Blockchains durchgeführt wird, dient mehr als Anreiz zur Erhaltung der Funktionalität und Stabilität dieser Blockchains und ist kein essentiell notwendiger Teil einer Blockchain. Eine Blockchain kann also auch so gestaltet werden, dass die Blöcke keine monetären Transaktionsdaten enthalten, sondern die an die Transaktionen angehängten Daten als Datenbank genutzt werden.

Die in der Blockchain gespeicherten Daten sind prinzipiell von allen Beteiligten lesbar, aber nicht unbedingt verständlich, denn sie können verschlüsselt abgelegt werden.

Dieses Statuspapier weicht in einem wesentlichen Aspekt von der gängigen Herangehensweise ab. Es betrachtet die zwei o.g. Hauptcharakteristika der Blockchain-Technologien

- 1) die kryptographische Verkettung von Blöcken und
- 2) die Verteilung der Datenbank im Benutzer-Netzwerk

getrennt voneinander. Diese beiden Eigenschaften werden meist als untrennbare Einheit angesehen. Bei genauerer Betrachtung führen sie jedoch zu unterschiedlichen Möglichkeiten und Restriktionen. Daher ist es hilfreich, beide Merkmale getrennt voneinander zu diskutieren. So ist es grundsätzlich auch möglich, die Blockchain-typische kryptografische Verkettung von Blöcken als (nicht verteilte) Datenbank zu nutzen (siehe Abbildung 1). Das erschwert ebenfalls ein nachträgliches Ändern einzelner Informationen.⁶

Der Begriff Blockchain wird hier also synonym mit allen Varianten von Distributed-Ledger-Technologie (DLT) und hashverknüpften Datenbanken verwendet.⁷

³ Der Begriff "Transaktion" bezeichnet in der IT die Änderung oder Erstellung eines Datensatzes in einer Datenbank. Daher sollte eine „Transaktion“ nicht im üblichen Sinne als Übertragung von Gütern verstanden werden.

⁴ <https://www.accenture.com/us-en/insights/chemicals/ai-blockchain-chemical-industry>

⁵ https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Blockchain_WhitePaper_Grundlagen-Anwendungen-Potentiale.pdf Seite 11

⁶ ORACLE bietet z.B. eine nicht-verteilte SQL-Datenbank mit kryptographisch verknüpften und signierten Zeilen an <https://www.oracle.com/corporate/blog/oracle-database-innovations-021320.html>

⁷ In Diskussionen zu diesem Paper wurde manchmal eingewendet, dass es sich bei nicht verteilten kryptographisch verketteten Datenbanken nicht um Blockchains handelt, sondern um Hashverknüpfungen, die schon seit langem bekannt sind. Für einen möglichen Nutzen ist es jedoch irrelevant, wo die genaue Grenze für die Bezeichnung Blockchain liegt. Vielmehr kommt es darauf an, welche Ausprägungen der Eigenschaften einen Mehrwert generieren. Daher vermeiden wir an dieser Stelle die semantische Differenzierung und konzentrieren uns auf die verfügbaren Bestandteile der Technologie und deren Kombinationsmöglichkeiten.

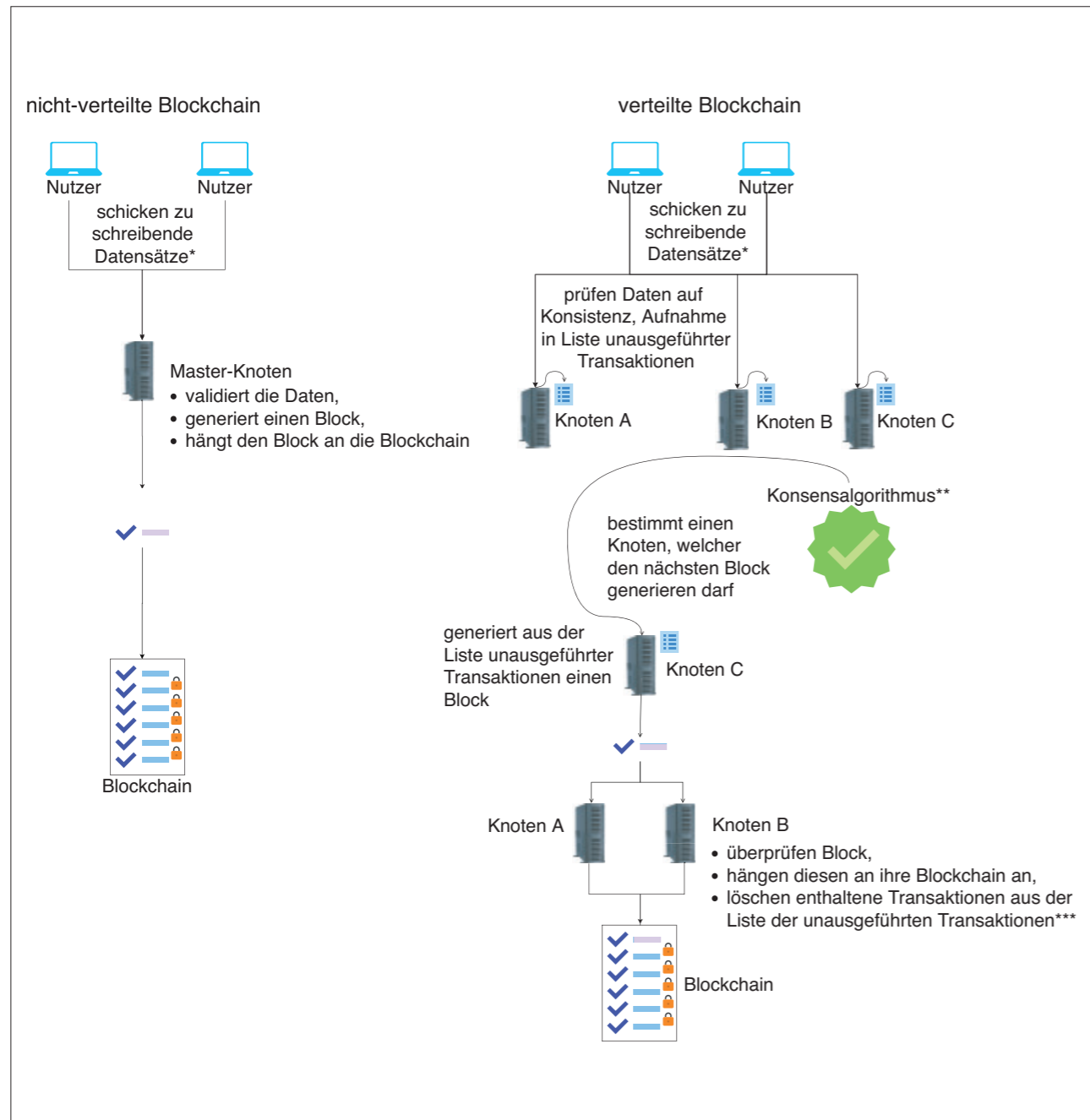


Abbildung 1: Grafische Darstellung der Prozesse in einer hypothetischen, nicht-verteilten Blockchain im Vergleich zu einer verteilten Blockchain.

* Die Datensätze beinhalten die ID (Adresse) des Senders, die Transaktionsdaten (Tokens, Empfänger, Zusatzinformationen), einen öffentlichen Schlüssel zur Prüfung des Hashwertes sowie einen Hash, der in der Regel aus der ID, der Transaktion sowie dem aktuellen Stand der Blockchain erstellt wird.

** Siehe Abschnitt „Validierungsalgorithmus“.

*** Je nach Verfahren können hierbei mehrere akzeptierte Versionen der Blockchain entstehen. Meistens werden diese so lange parallel geführt, bis eine Kette länger ist, und dann nur diese behalten.

3 Vorteile und Grenzen von Blockchain

Aus den zwei grundlegenden Eigenschaften von Blockchains, also der kryptografischen Verkettung sowie der Verteilung identischer Kopien über alle Knoten, ergeben sich diverse Möglichkeiten, aber auch Grenzen. Je nach Blockchain-Typ sind sie unterschiedlich stark ausgeprägt. Der große Vorteil einer Blockchain ist die Manipulationssicherheit, welche sich aus den genannten Eigenschaften ergibt. Dem stehen jedoch Nachteile bei Speicherbedarf, Geschwindigkeit und Datensicherheit gegenüber, wie im Folgenden dargestellt. Gerade im industriellen Umfeld sind nicht alle Eigenschaften im vollen Umfang erforderlich, zumal ihre vollständige Umsetzung zum Teil mit erheblichen Belastungen der IT-Infrastruktur verbunden ist.

Daher sollten für jeden einzelnen Anwendungsfall Vor- und Nachteile abgewogen werden, um zu entscheiden, ob eine Blockchain-Lösung einer klassischen Datenbank überlegen ist.⁸

3.1 Manipulationssicherheit

Die Manipulationssicherheit ist der zentrale Vorteil einer Datenbank, die als Blockchain aufgesetzt wird. Für die konkrete Anwendung ist ausschlaggebend, welcher Grad der Manipulationssicherheit erreicht werden soll. Eine einmal geschriebene Blockchain kann aufgrund der kryptografischen Verkettung der Blöcke nicht mehr ver-

Exkurs: Validierungsverfahren

Die gängigsten Verfahren sind im Folgenden kurz zusammengefasst. Die verschiedenen Verfahren sind ausführlicher z.B. auf <https://101blockchains.com/consensus-algorithms-blockchain> beschrieben.

Proof of work

Bezeichnungen: Prozess der Knoten-Auswahl: „Mining“, Full Node: „Miner“

Beschreibung: Alle Miner lösen ein mathematisches Rätsel mit hohem Rechenaufwand. Der erste mit der richtigen Lösung erhält eine Belohnung und generiert den nächsten Block.

Nachteil: Energieintensiv. Potenziell angreifbar durch node farms (51%-attack)

Beispiel: Bitcoin

Proof of stake

Bezeichnungen: Prozess: „Minting“ oder „Forging“, Full Node: „Validator“

Beschreibung: Es muss eine Mindesteinlage an Tokens (stake) getätigt und gehalten werden. Je höher die Einlage, desto höher die Wahrscheinlichkeit, als Rechner bestimmt zu werden. Der gewählte Knoten erstellt den nächsten Block und erhält eine Belohnung oder einen penalty bei Betrugsversuch.

Vorteil: wesentlich weniger Energieverbrauch. Praktisch unanfällig gegen 51%-attack, da nicht 51% der Knoten gehalten werden müssen, sondern 51% der Token-Menge.

Nachteil: Je nach Ausführung können Knoten mit hohem Anteil an tokens mehr Einfluss auf Entscheidungen nehmen. In einfachen PoS-Ausführungen sind auch bribe-Attacken möglich, bei denen eine parallel aufgebaute Kette die aktuell akzeptierte Kette verdrängt.

Beispiel: Viele Ethereum-basierte Blockchains nutzen Proof of Stake

Proof of authority

Beschreibung: Im Vergleich zu PoS wird auch die Vertrauenswürdigkeit eines Knoten mit berücksichtigt. In der Regel wird hierfür eine zentrale Autorität nötig, die die Vertrauenswürdigkeit prüft und verwaltet.

Beispiel: IBM Hyperledger

⁸ Die Sicherheitsaspekte können in der Kürze dieses Papiers nur oberflächlich wiedergegeben werden. Eine ausführliche Betrachtung ist z.B. vom Bundesamt für Sicherheit in der Informationstechnik (BSI) verfügbar: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf?__blob=publicationFile&v=5

ändert werden. Allerdings kann durch Schwachstellen im Validierungsalgorithmus eine Blockchain auch im Nachhinein gegen eine andere Version getauscht werden. Daher ist das Validierungsverfahren essenziell für den Grad der Manipulationssicherheit (siehe Exkurs Validierungsverfahren). Unabhängig vom Validierungsverfahren führt eine Manipulation eines einzelnen Blockes aufgrund der kryptographischen Verkettung jedoch immer zur Zerstörung aller späteren Blöcke einer Blockchain, da die vorherige Information nicht mehr mit den Hashwerten dieser Blöcke übereinstimmt. Durch den Validierungsprozess wird im gesamten Netzwerk eine Einigung auf die aktuell korrekte Version der Kette erreicht. Bei großen Netzwerken kann es zur Aufspaltung in mehrere Zweige kommen (sog. Forking). Durch festgelegte Mechanismen muss dann eine Entscheidung für einen Zweig getroffen werden. Der andere Zweig und alle Blöcke ab der Abspaltung werden verworfen. Die meisten Manipulationsstrategien zielen auf die absichtliche Erzeugung eines stabilen und vom gesamten Netzwerk akzeptierten Zweiges ab. Um dies zu bewerkstelligen, muss der Angreifer mehr als 50 % der Blockerstellungskapazität bzw. Validierungsressourcen im Blockchain-Netzwerk zur Verfügung haben. Daher wird diese Art der Manipulation als „51%-Attacke“ bezeichnet. Bei diesen Strategien sind Daten nur ab dem Punkt der Zweigerzeugung manipulierbar. Hierdurch ergibt sich auch die höhere Manipulationssicherheit für Blöcke, die weiter vorne in der Blockchain stehen.

3.2 Verteilung im gesamten Netzwerk

Ein Blockchain-Netzwerk besteht aus allen Rechnern (Knoten), die die entsprechende Software installiert haben und im Netzwerk angemeldet sind. Bei privaten Blockchains kann die Anmeldung im Netzwerk durch Genehmigungsinstanzen beschränkt werden, während öffentliche Blockchains für jeden Teilnehmer zugänglich sind. Die gesamte Blockchain ist bei allen Teilnehmern gespeichert, wodurch der Grad der Manipulationssicherheit erhöht wird und eine Datensicherung im Fall von Ausfällen im Netzwerk sichergestellt ist. Sollte es zu einem Korruptionsversuch in einer Blockchain-Kopie kommen, wird dies von den anderen Knoten erkannt und die korrumpierte Version durch die mehrheitlich anerkannte Blockchain restauriert (siehe 3.1 Manipulationssicherheit).

Datensicherung und Systemredundanz

Durch die Verteilung im gesamten Netzwerk ist die Blockchain je nach Netzwerkgröße sehr gut gegen Datenverluste gesichert, da auf allen Knoten eine vollständige Kopie vorliegt. Die Verteilung sorgt auch für eine sehr hohe Verfügbarkeit, da selbst bei mehreren Ausfällen im Netzwerk die Funktionalität uneingeschränkt erhalten bleibt, solange eine ausreichende Zahl an Knoten zur Validierung der Transaktionen verfügbar ist.

Zugriffssicherheit der Daten

Daten können auf verschiedene Arten vor unbefugtem Zugriff geschützt werden. Zum einen kann bei „klassischen“ Datenbanken vermieden werden, dass kritische Daten das firmeninterne Netzwerk verlassen (Datenzugänglichkeit). Sollte dies dennoch passieren, kann Verschlüsselung den Zugriff auf die Daten erschweren (Datenlesbarkeit). In verteilten Datenbanken wird die erste Ebene aufgegeben, da alle Teilnehmer auf die Daten in der Blockchain zugreifen können. Somit beruht die Datensicherheit ausschließlich auf der Qualität der Verschlüsselung kritischer Daten. Die Ver- und Entschlüsselung läuft allerdings außerhalb der Blockchain und bedarf somit einer parallelen Schlüsselverwaltung. Durch die Nutzung einer genehmigungsbasierten Blockchain lässt sich jedoch auch die erste Ebene der Datensicherheit, nämlich die Datenzugänglichkeit, zum Teil bewerkstelligen, da hier nur ausgewählten Personen/Instanzen die Teilnahme am Blockchain-Netzwerk, und somit der Zugriff, erlaubt wird.

3.3 Ressourcenbedarf

Speicherplatz

Da bei Blockchains neue Daten immer an die bestehende Kette angehängt werden und nichts gelöscht wird, erreichen Blockchains schnell eine signifikante Dateigröße. Die Verteilung von vollständigen Kopien auf alle Knoten führt in Summe zu einem erheblichen Speicherbedarf. Das limitiert die Datenmengen, die sinnvoll in Blockchains abgelegt werden können. In Anwendungsfällen, bei denen allein die Manipulationssicherheit relevant ist (wie z.B. in GxP-Anwendungen), kann die Datenmenge in der Blockchain jedoch deutlich reduziert werden, indem lediglich

ein kryptographisch verkürzter Hashwert abgelegt wird. Mit diesem Hashwert kann dann eine an anderer Stelle abgelegte Datei auf ihre Authentizität geprüft werden. In der Blockchain sind in diesem Fall keine Daten abgelegt, sondern lediglich die Prüfwerte und je nach Anwendungsfall weitere kurz gefasste Informationen wie z.B. ein Zeitstempel. Dieses Vorgehen führt wiederum zu einer verbesserten Datensicherheit, da nicht-zugängliche Speicherorte für die eigentlichen Daten verwendet werden können.

Rechenleistung

Die von der Bitcoin-Blockchain genutzte Validierung durch den Proof-of-Work-Algorithmus erfordert erhebliche Rechenleistung, welche eine künstliche Verzögerung zwischen dem Übermitteln und dem Schreiben der Daten erzeugen soll. Das ist in anonymisierten, öffentlichen Systemen nötig, um die Daten gegen Manipulation zu schützen.⁹ Im industriellen Umfeld mit bekannten Teilnehmern (genehmigungsbasierte Blockchains) können weniger ressourcenintensive Konsensverfahren eingesetzt werden. Trotzdem führt der Validierungsprozess zu einer Verzögerung zwischen dem Absenden der Daten und der Eintragung in die von allen akzeptierte Version der Blockchain.

Alle in der Blockchain zu speichernden Daten werden an die Blockchain angehängt. Die Struktur ist dementsprechend grundlegend anders als in einer klassischen Datenbank und führt zu einer geringen Effizienz beim Auslesen und Auswerten der Daten sowie zu einem hohen Speicher- und Netzwerkbedarf. Die Blockchain sollte daher nicht als Ersatz für klassische Datenbanken angesehen werden, insbesondere wenn es darum geht, große Datenmengen zu speichern.

3.4 Abbildung der Realität

Die Daten in Blockchains bilden – wie jede andere Datenbank – die Realität nur dann ab, wenn die Eintragungen korrekt erfolgt sind. Im Zuge der Konsensverfahren kann zwar eine Übereinkunft über eine einheitliche Version der Blockchain getroffen werden, weshalb dieser die Bezeichnung „single source of truth“ zugesprochen wird. Allerdings handelt es sich hier um die Bestätigung der beteiligten Netzwerkknoten, dass die Berechtigung zur Einstellung der Information besteht und dass die Information den gesetzten Plausibilitätskriterien entspricht. Ob diese Information jedoch auch den tatsächlichen physischen Gegebenheiten entspricht, ist nicht Bestandteil der Datenprüfung. Somit bildet die Blockchain zwar eine allgemein akzeptierte digitale Realität ab, die jedoch mit der physischen Realität nicht zwingend übereinstimmt.

⁹ Zum Schutz vor Angriffen, die auf Forking basieren, enthalten viele Blockchainalgorithmen einen fest eingebauten Abstand zwischen der Erstellung der Blöcke. Hierdurch müssen die notwendigen Ressourcen für den Angriff sehr lange bereitgehalten werden, um größere Manipulationen zu erreichen. Im Bitcoin-Netzwerk beträgt die vorgesehene Zeit zwischen zwei Blöcken 10 Minuten. Zur Erreichung dieses Wertes wird die Schwierigkeit der Aufgabe im Validierungsalgorithmus kontinuierlich an die vorhandene Rechenleistung angepasst.

4 Anwendungsfälle für Blockchain in der Prozessindustrie

Im Kern sind Blockchains Datenbanken mit den beschriebenen besonderen Eigenschaften. Für den Einsatz in den operativen Abläufen der Prozessindustrie eignen sich hauptsächlich private oder von Drittanbietern administrierte Blockchains, da nur diese das geforderte Maß an Datensicherheit abbilden können. Gerade in Anwendungsfällen mit eingebundenem Zahlungsverkehr werden Drittanbieter schon aus regulatorischen Gründen (insbesondere Steuergesetzgebung) notwendig sein. Speziell könnte ein Mehrwert in den Bereichen, welche in den Abschnitten 4.1 bis 4.5 beschrieben sind, erreicht werden.

4.1 Blockchain für das GxP am Beispiel der pharmazeutischen Industrie

Im Bereich der pharmazeutischen Industrie bestehen strenge Regularien und Vorschriften innerhalb aller Entwicklungs- und Herstellungsbereiche. Ein wesentlicher Teil bei allen GxP-Varianten ist die Dokumentation der korrekten Durchführung aller Vorschriften. Diese erstrecken sich von der Konzipierung und Durchführung klinischer Studien (GCP – good clinical practice) über die Dokumentation von Laborergebnissen (GLP – good laboratory practice und GCLP – good clinical laboratory practice) bis hin zum Nachweis der Nutzung zugelassener, valider Rohstoffe und Rezepturen im Herstellungsprozess (GMP – good manufacturing practice).

In allen Fällen muss eine nicht oder nur sehr schwer veränderbare, Audit-sichere Dokumentation erstellt werden (Datenintegrität). Das erfordert derzeit aufwändige Prozesse und große Mengen ausgedruckter Dokumente. Die Eigenschaft der Unveränderbarkeit durch die kryptografische Verknüpfung der Blöcke von Blockchains ist hier von besonderer Bedeutung, da mit wesentlich geringerem Aufwand nahezu nicht veränderbare Daten abgelegt werden können.

Dabei muss die Unveränderbarkeit aber nicht zwingend dadurch erreicht werden, dass die Blockchain auf ver-

schiedene Knotencomputer verteilt ist. Auch ein einzelner Knoten, auf den mehrere Nutzer schreiben, verhindert die Manipulation. Durch die Authentifizierung der schreibberechtigten Nutzer mittels public-private key und die kryptografische Verkettung der Blöcke ist eine Veränderung unmöglich, ohne alle darauf folgenden Daten aller Nutzer ungültig zu machen. Somit führt jede nachträgliche Datenmanipulation zu einer einfach nachweisbaren Verletzung der Integrität einer bestehenden GxP-Dokumentation.

Wie bei bisherigen GxP-Dokumentationsablagensystemen ist hiermit aber lediglich die Unveränderbarkeit der Dokumentation gewährleistet. Wenn beispielsweise ein Sensor in einer GxP-Anwendung einen fehlerhaften (aber plausiblen) Wert liefert, wird dieser Wert trotzdem in der Blockchain akzeptiert. Das Auftreten fehlerhafter Messwerte kann zwar durch Kalibrierungsvorschriften vermieden werden und die Durchführung dieser Kalibration wird auch auf der Blockchain dokumentiert. Die Kontrolle über die korrekte Durchführung dieser Kalibrierung liegt jedoch weiterhin außerhalb der Blockchain.

4.2 Blockchain für Logistik und Supply Chain Management – Track and Trace

Fälschungssicherheit von Produkten

Ein weiterer Anwendungsfall für die Blockchain ist die Nachverfolgbarkeit von Produkten. Wenn einzelne kritische Produkte von deren Herstellern am Produktionsort in die Blockchain geschrieben werden und die Produktidentifikation anschließend entlang der Lieferkette in der Blockchain weitergegeben wird, werden Fälschungen deutlich erschwert. Einträge, die nicht mit tatsächlichen Produktionsmengen übereinstimmen, sind einfach ersichtlich. Dieses Prinzip wurde schon für Diamanten¹⁰ umgesetzt, um deren Herkunft nachvollziehen zu können und „Blutdiamanten“ aus Lieferketten auszuschließen. Auch in der Lebensmittel-Lieferkette gibt es schon Ansätze von IBM und Walmart.¹¹

In der Prozessindustrie wäre eine Umsetzung für kritische Produkte wie Pharmazeutika denkbar, bei denen der Kunde (z.B. über einen QR-Code) die Authentizität prüfen und den Lieferweg nachvollziehen kann. Aufbauend auf IBMs FoodTrust Blockchain führte Merck&Co in den USA bis Ende 2019 ein Pilotprojekt für diese Anwendung durch.¹² Einen deutlich umfassenderen Ansatz zur Bekämpfung von Medikamentenfälschung verfolgt Merck KGaA. Durch eine beliebige Eigenschaft oder die Kombination mehrerer Eigenschaften kann mithilfe von künstlicher Intelligenz ein Hashwert errechnet und verschlüsselt in einer Blockchain abgelegt werden. Misst man die gewählten Fingerprint-Eigenschaften und gleicht sie entsprechend mit dem vorher errechneten Hashwert mithilfe von KI-Methoden ab, kann die Echtheit des Produkts überprüft werden.¹³

Transparenz, Nachhaltigkeit und Rohstoffherkunft

Auch Nachhaltigkeitskriterien könnte man entlang der Lieferkette nachverfolgen, indem aus der Blockchain ersichtlich ist, welche Rohstoffe oder Prozesse für ein Produkt verwendet wurden. Dies ist insbesondere für Drop-in-Stoffe interessant, die vergleichbare Eigenschaften wie Produkte aus fossilen Rohstoffen haben, jedoch CO₂-neutral hergestellt wurden. Die höheren Produktionskosten solcher klimaneutraler Substitutionsstoffe sollen durch einen höheren Verkaufspreis („green premium“) gedeckt werden. Durch die Validierung über eine Blockchain können dieser Mehrwert und dessen korrekte Umsetzung transparent für den Konsumenten dargestellt werden. Dadurch ließe sich der höhere Preis besser durchsetzen. Alternativ können die eingesetzten Mengen auch rechtsicher für eventuelle Steuervorteile oder die Vermeidung von Strafsteuern nachgewiesen werden. Eine analoge Umsetzung für die Lebenszyklusverfolgung von Kunststoffen und den Nachweis von enthaltenen Recyclingmengen wird aktuell durch Covestro entwickelt.¹⁴

Auch für den Herkunftsnachweis für bestimmte Anteile einer Produktion, wie sie in Freihandelsabkommen festgehalten sind, eignet sich eine Blockchain.

Digitalisierung der Lieferkette

Durch den Einsatz smarter Paletten mit automatisierter Dokumentation in eine Blockchain können die Einhaltung von Lager- und Transportbedingungen und der Lieferweg von Waren nachvollzogen werden. Auch das Lagermanagement könnte durch die selbstständige Standortdokumentation deutlich effizienter werden. Die niederländische Logistik-IT-Firma Ahrma Group nutzt solche intelligenten Paletten in der Nachverfolgung von Produkten in der Nahrungsmittellieferkette.¹⁵ Aus öffentlichen Quellen ist jedoch nicht ersichtlich, ob ein expliziter Bezug zur Blockchain-Technologie besteht. Die Speicherung und Abfrage der Daten soll über das proprietäre „Ahrma Supply Chain Big Data System“ erfolgen.¹⁶ Dass die chemische Industrie jedoch ein reales Interesse an solchen smarten Lösungen hat, beweist die 2017 getätigte Investition von BASF in die Ahrma Group.¹⁷ Auch die Telekom hat in Zusammenarbeit mit dem Fraunhofer IML und der EPAL den sogenannten „Low Cost Tracker“ entwickelt und ein Pilotprojekt mit 500 smarten Paletten gestartet.¹⁸ Auch hier kann die Datenverfügbarkeit über eine Blockchain gelöst werden, was jedoch nicht zwingend ist.

Das Format einer Blockchain als Hauptbuch stimmt mit den Anforderungen an die Nachverfolgbarkeit von logistischen Transaktionen überein und eine absichtliche oder versehentliche Korruption der Daten durch den Datenbankmanager wird ausgeschlossen.

¹⁰ <https://www.tracr.com>

¹¹ Walmart nutzt IBM Blockchain (<https://www.ibm.com/blockchain/solutions/food-trust>) zur Nachverfolgbarkeit von Gemüse und Shrimps: <https://corporate.walmart.com/newsroom/2018/09/24/in-wake-of-romaine-e-coli-scare-walmart-deploys-blockchain-to-track-leafy-greens>

¹² <https://www.merck.com/about/featured-stories/from-factory-to-patient-merck-pilots-blockchain-project-to-trace-and-track-drugs.html>

¹³ <https://www.merckgroup.com/de/news/us-patent-blockchain-30-01-2019.html>
Im Patent von Merck KGaA ist auch explizit die Möglichkeit der Ablage in nicht-geblockten DLTs genannt.

¹⁴ <https://www.covestro.com/press/circularise-covestro-und-domo-praesentieren-loesung-zur-rueckverfolgbarkeit-von-kunststoffen-auf-der-ces-2020>

¹⁵ <https://www.rabobank.com/en/raboworld/articles/the-smart-pallet-a-new-platform-for-food-security.html>

¹⁶ <http://ahrmagroup.com/iot>

¹⁷ <https://www.basf.com/global/de/media/news-releases/2017/12/p-17-374.html>

¹⁸ <https://www.telekom.com/de/medien/medieninformationen/detail/telekom-macht-paletten-intelligent-546702>

4.3 Asset Life Cycle Monitoring

Machine-as-a-Service

Vielfach wird als zukünftiges Geschäftsmodell die Bereitstellung von Apparaten als Dienstleistung diskutiert. Anstatt beispielsweise einen Kompressor zu kaufen, wird die Bereitstellung von Druckluft bestellt und nach tatsächlichem Verbrauch abgerechnet. Oder eine Anlage wird über pay-per-use abgerechnet. In beiden Fällen ist die Dokumentation der Nutzungsgeschichte sowohl für den Anbieter als auch für den Servicenutzer entscheidend, insbesondere wenn das Geschäftsmodell auf medienberührende Anlagenteile ausgeweitet wird (z.B. Pumpen). Um Vertrauen in die Korrektheit dieser Nutzungsgeschichte zu erreichen, ist die Erfassung in einer Blockchain geeignet. Auch für die nutzungsorientierte Abrechnung ist eine automatisierte, unveränderbare Dokumentation erforderlich. Erste Anwendungsfälle sind z.B. für Verpackungsmaschinen bekannt.¹⁹

Life Cycle Information Management

Zulieferer von Anlagenteilen haben häufig erweiterte Nachweispflichten für den Fall, dass es zu einem Ausfall oder Schaden kommt. Ohne Informationen über die Nutzungsgeschichte und den Betriebszustand des Bauteils zum Schadenszeitpunkt ist dieser Nachweis jedoch schwierig. Die verschlüsselte Ablage von Lebenszyklusinformationen auf einer Blockchain ermöglicht einen Nachweis über den Zustand des Bauteils, analog zur Blackbox in einem Flugzeug. Die Daten werden sensorbasiert automatisch erzeugt und manipulationssicher abgelegt; das schafft ein hohes Vertrauen der Partner in die Korrektheit der Informationen, was die Abwicklung im Schadensfall deutlich vereinfacht. An einer Umsetzung dieses Konzeptes wird bei Samson gearbeitet.

4.4 Machine-Controlled-Maintenance

Die automatisierte Wartung von Anlagen ist ein häufig angeführter Anwendungsfall für Blockchain im industriellen Umfeld. Die Vision von Machine-Controlled-Maintenance integriert zusätzlich Sensorinformationen, um ungeplante Wartungsfälle frühzeitig zu erkennen und an den zuständigen Servicetechniker zu melden (predictive maintenance). Diesem Techniker wird gleichzeitig die Liste der benötigten Werkzeuge und Ersatzteile zugeschickt und die nicht lagernden Teile werden automatisch bestellt. Hierdurch lassen sich Ausfallzeiten deutlich reduzieren und durch die frühzeitige Erkennung mit ausreichend Vorlaufzeit zur Ersatzteilbestellung könnten Lagerkosten deutlich verringert werden. Durch eine Blockchain ließe sich dieses System gemeinsam mit den Komponentenlieferanten betreiben. Sie können dank der Information über die von ihnen gelieferten Anlagenkomponenten einen Wartungsservice anbieten. Allerdings wird eine Produktionsfirma Daten, die Rückschlüsse auf die Produktionsprozesse zulassen, mit externen Dienstleistern nicht ohne Weiteres teilen. Zudem besteht in dieser Anwendung kein Vertrauensproblem, da der Anlagenbetreiber ein eigenes Interesse an effizienten Wartungsvorgängen hat. Daher ließe sich dieses System ebenso gut mit konventionellen Datenbanken umsetzen. Die externen Dienstleister erhalten in diesem Fall ausschließlich die für sie nötigen Informationen, ohne dass es einer komplizierten Verschlüsselung und Zugriffsverwaltung bedarf. Die Herausforderung bei diesem Anwendungsfall ist nicht die eingesetzte Datenbanktechnik, sondern die Bereitstellung der nötigen Informationen.

4.5 Smart Contracts und automatisiertes Rechnungswesen

Smart Contracts sind automatisierte Geschäftsprozesse, bei denen die Dokumentation einer Leistungserbringung auf der Blockchain unmittelbar eine Gegenleistung, Rech-

nungsstellung oder Folgeaktion auslöst. Damit können sie Teile von Verträgen oder Vereinbarungen als Grundlage für die automatisierten Prozesse abbilden (z.B. Zahlungsanweisungen oder Produktfreigaben), müssen jedoch keine Verträge im rechtlichen Sinne sein. Hierdurch können Prozesse mit bisher hohem manuellem Bearbeitungsaufwand deutlich effizienter und weniger fehleranfällig gestaltet werden. Bei Formelpreisen kann zum Beispiel der aktuelle Energiepreis zum Produktionszeitpunkt automatisch aus der Datenbank der Strombörse abgerufen werden und mit der Preisformel die Rechnung (ebenfalls automatisch) erstellt werden. In der Logistik können durch Zeitstempel und Geofencing (Überschreiten virtueller geographischer Begrenzungen) Standzeiten auf dem Werksgelände dokumentiert und Standgebühren automatisiert abgerechnet werden.

Zwischen Handelspartnern mit hohem bidirektionalem Handelsvolumen kann auch eine Verrechnung der gegenseitigen Forderungen auf der Blockchain dokumentiert werden und in regelmäßigen Abständen die Differenz beglichen werden, anstatt jede Einzelforderung einzeln abzurechnen.

¹⁹ „Pearson to unveil Machines as a Service – a new way to automate without the capital cost – at Pack Expo 2019“, Pearson Packaging Systems, 30.08.2019, <https://pearsonpkg.com/resources/pearson-to-unveil-machines-as-a-service-a-new-way-to-automate-without-the-capital-cost-at-pack-expo-2019>

5 Fazit

Die Blockchain ist eine komplexe Lösung für spezifische Probleme, für die sie einen großen Mehrwert liefern kann. Wie in allen Innovationsprojekten sollten zunächst ein klares Problem definiert und Lösungen ergebnisoffen bewertet werden. Wenn die Vorteile der Blockchain, Manipulationssicherheit und Verteilung im Netzwerk, im Anwendungsfall die Nachteile des erhöhten Ressourcenbedarfs und der schlechteren Performance überwiegen, kann eine Einrichtung sinnvoll sein. Aufgrund der inhärenten Nachteile ist Blockchain aber nicht die Lösung aller Probleme, als die sie bisweilen beschrieben wird. Insbesondere ist die Technologie aufgrund der fragmentierten Datenablage nicht geeignet für Anwendungen im Bereich Big Data und Data Analytics.

5.1 Wofür ist Blockchain geeignet?

Blockchains können Vertrauensprobleme lösen. Dies kann das Vertrauen eines Auditors in die Integrität einer Dokumentation sein oder das Vertrauen eines Kunden in die Herkunft eines Produktes. Wenn dieses Vertrauen nicht durch eine Datenbank bei einer vertrauenswürdigen Autorität²⁰ hergestellt werden kann, ermöglichen die Eigenschaften einer Blockchain diese Vertrauensbildung. Sie bezieht sich jedoch lediglich auf die Unveränderbarkeit und Transparenz der Daten. Die Korrektheit dieser Daten müssen wiederum ergänzende Prozesse außerhalb der Blockchain gewährleisten. Im Falle von Smart Contracts können vertrauenswürdige Daten durch automatisierte Datenbankabrufe integriert werden, um über einfache Wenn-Dann-Entscheidungen Prozessschritte zu automatisieren und unveränderbar zu dokumentieren.

5.2 Blockchain oder klassische Datenbank?

Die Alternative, mit der Blockchain bei der Bewertung verglichen werden muss, ist die konventionelle Datenbanktechnik: Viele der auch in der Literatur beschriebenen Anwendungsfälle der Blockchain-Technologie lassen sich ebenso mit konventionellen Datenbanken umsetzen. Wenn spezifische Problemstellungen mit Aspekten der Blockchain-Technologie zu lösen sind, sollte dieser Weg

in Betracht gezogen werden. Wenn solche Probleme nicht vorliegen, ist eine klassische Datenbankstruktur vorzuziehen. Daher sollten nicht Probleme für einen Einsatz von Blockchains gesucht werden, sondern bei bestehenden Fragestellungen sollte geklärt werden, ob die Einführung einer Blockchain einen Mehrwert liefert. Damit wird die neue Technologie zu einem nützlichen Werkzeug in der Toolbox der Digitalisierung.

5.3 Blockchain als Enabler im Change Management

Die Umsetzung von inkrementellen Veränderungen in bestehenden Systemen birgt die für Digitalisierungsprojekte typische Gefahr, dass die Nutzer die gewohnten Prozesse nicht ändern und somit die Umsetzung scheitert. Bei der Verlagerung in die Blockchain werden Prozesse nicht einfach in ein anderes Datenbankformat überführt, sondern die Arbeitsabläufe werden grundlegend verändert. Die manuelle Arbeit besteht nicht mehr in der Eingabe einer Buchung, sondern in der Festlegung von Buchungsbedingungen. Dies bedeutet zwar ein größeres Ablehnungsrisiko in der Einführungsphase, dem durch aktives Change Management begegnet werden muss. Andererseits wird die Beibehaltung gewohnter, aber veralteter Prozessabläufe durch die Einführung der neuen Technologie Blockchain vermieden.

5.4 Die Datenbasis nicht aus dem Blick verlieren

Was für die Umsetzung von Digitalisierungsprojekten bisher häufig fehlt, ist die digitale Verfügbarkeit der benötigten Daten. Daher muss der Fokus auf die Entwicklung von einheitlichen Datenmodellen und die Investition in entsprechende Erfassungssysteme (Sensoren, Erfassungsterminals, etc.) gelegt werden, um die Digitalisierung voranzubringen. Diese bilden die Basis, um überhaupt ein digitales Abbild der Realität darstellen zu können. Wenn die Daten der Anlage, des Produktes oder des Prozesses vorliegen, ist erst der nächste Schritt die Entscheidung für die geeignete Datenbankarchitektur.

Folgende Kernaussagen lassen sich zusammenfassen:

- » Eine Blockchain ist grundsätzlich sehr sicher gegen Manipulationsversuche. Die Manipulation eines bestehenden Blocks führt dazu, dass alle darauffolgenden Blöcke ungültig werden, so dass die Manipulation sofort auffällt und rückgängig gemacht wird.
- » Die Manipulation von Datensätzen ist nur möglich, wenn eine Instanz über mindestens 50% der Ressourcen verfügt, die für die Validierung benötigt werden. Dabei werden die manipulierten Daten an eine bestehende Blockchain geschrieben, welche sich dann als die dominante und folglich akzeptierte Version durchsetzt.
- » Eine Blockchain benötigt während ihres Bestehens zunehmend mehr Speicherplatz, da keine Daten gelöscht werden können.
- » Die Rechenleistung zur Blockerstellung ist abhängig vom Validierungsmechanismus und kann in genehmigungsbasierten Blockchains sehr gering sein.
- » Blockchains besitzen im Vergleich zu klassischen Datenbanken eine geringere Effizienz durch reduzierte Schreib- und Lesegeschwindigkeiten. Die Datenverfügbarkeit ist in einem Blockchain-Netzwerk durch die Systemredundanz nahezu immer gegeben.
- » Daten in einer Blockchain sind inhärent weniger sicher vor unberechtigtem Zugriff als in einer klassischen Datenbank, da die Ebene der Datenzugänglichkeit aufgegeben wird.
- » Die Plausibilität (Gültigkeit) einer Transaktion in der Blockchain wird durch den Validierungsmechanismus geprüft, nicht jedoch deren Richtigkeit (Wahrheitsgehalt).
- » Eine versehentliche oder absichtliche Datenkorruption durch einen Datenbankmanager ist ausgeschlossen.

²⁰Im B2B Umfeld und gerade bei der Abwicklung und Verrechnung von Forderungen wird trotzdem eine dritte Instanz nötig sein. Im Fall von Zahlungsabwicklung ist dies schon aus regulatorischen Gründen erforderlich.

6 Begriffserklärung zum Thema Blockchain

Abkürzung	Begriff	Erläuterung
	Bitcoin	Bitcoin ist die bekannteste virtuelle Kryptowährung (s. „ Kryptowährung “), welche über eine Blockchain abgebildet ist.
	Block	Ein Block ist eine Einheit, die in die Blockchain geschrieben wird. Jeder Block ist durch kryptographische Verknüpfung mit den vorherigen Blöcken verbunden. Je nach Ausgestaltung der Blockchain kann ein Block mehrere Transaktionen enthalten.
DLT	Distributed-Ledger-Technology	Wörtlich übersetzt: „Verteiltes Hauptbuch“ (s. „ Hauptbuch “). Der Begriff bezeichnet eine dezentrale Datenbank, wobei durch einen Konsensmechanismus (s. „ Konsensverfahren “) Einigkeit über die aktuell korrekte Version hergestellt wird. Die Technologie stellt einen Gegensatz zum klassischen Ansatz dar, bei dem ein Hauptbuch in der Regel von einer Instanz verwaltet wird.
DAG	Directed Acyclic Graphs	DAG ist ein DLT-Typ (s. „ Distributed-Ledger-Technology “). Er basiert nicht auf einer linearen Verkettung von Blöcken, die mehrere Daten/Transaktionen zusammenfassen, sondern auf der Speicherung von Daten/Transaktionen in einer Baumstruktur. Dadurch wird die Validierung beschleunigt und der Aufwand verringert. So soll sich DAG insbesondere für Mikrotransaktionen oder Internet of Things (IoT) bzw. Machine-to-Machine (M2M)-Daten eignen. Als Kritikpunkt wird oft angeführt, dass Transaktionen nicht zwangsläufig akzeptiert werden und dass in heutigen Implementierungen oft ein zentraler Koordinator nötig ist. Zusätzlich hängt die Validierungsgeschwindigkeit von der Geschwindigkeit der Erzeugung neuer Blöcke ab.
	Forking	Aufspalten einer Blockchain in zwei Zweige, z.B. wenn zwei Knoten (s. „ Knoten “) gleichzeitig die Validierungsbedingung erfüllen und die unterschiedlichen Blöcke in Teilen des Netzwerkes jeweils zuerst ankommen. Forking ist aber auch durch eine Änderung des Algorithmus möglich, den nur ein Teil des Netzwerkes durch Installation der aktualisierten Software akzeptiert.
	Full Node	Knoten (s. „ Knoten “), welcher Hashes (s. „ Hash “) für Blöcke (s. „ Block “) errechnet und damit die Blockchain fortschreibt. Siehe auch „ Mining/Miner “.
	Hash	Hashes bilden die Grundlage für digitale, kryptografisch verschlüsselte Wertzeugungs- und Werttransferprozesse. Die Funktion wandelt Buchstaben und Zahlen in ein verschlüsseltes Ergebnis fester Länge (Zeichenzahl) um.
	Hauptbuch	Begriff aus dem Rechnungswesen. Das Hauptbuch ist Bestandteil der doppelten Buchführung, in welches alle Geschäftsvorfälle/Transaktionen eingetragen werden. Blockchain ist eine technologische Variante eines „verteilten Hauptbuchs“ (s. „ Distributed-Ledger-Technologie “).

Abkürzung	Begriff	Erläuterung
	Knoten (Node)	Ein Knoten bezeichnet einen Computer, der am Blockchain-Netzwerk teilnimmt. Die Gesamtheit der Knoten (Nodes) bildet das Nutzer-Netzwerk der Blockchain. Jeder Knoten im Netzwerk hat eine Kopie der aktuellen und akzeptierten Blockchain.
	Konsensverfahren	Das Konsensverfahren ist ein Algorithmus, mit dem die Gültigkeit von Transaktionen (s. „ Transaktion “) und Blöcken (s. „ Block “) bestimmt wird. Durch das Konsensverfahren wird sichergestellt, dass alle Knoten (s. „ Knoten “) die gleiche Version einer Blockchain benutzen.
	Kryptographie	Kryptographie ist ein Überbegriff für Verschlüsselungsmethoden. Die Kryptographie in einer Blockchain beruht auf mathematischen Verschlüsselungsverfahren, mit dem Ziel Informationen zu schützen. Bei Blockchains kommen insbesondere asymmetrische kryptographische Verfahren zum Einsatz, bei denen die Erzeugung eines kryptographischen Wertes deutlich schwieriger ist, als die Verifizierung der Korrektheit dieses Wertes.
	Kryptowährung	Kryptowährung bezeichnet virtuelles Geld, bei der ein verteiltes, dezentrales und digitales Zahlungssystem genutzt wird.
	Mining/Miner	In ressourcenbasierten Validierungsalgorithmen sind Miner die Full Nodes (s. „ Full Node “), die entsprechende Ressourcen bereitstellen, um die Berechtigung zum Schreiben eines Blocks (s. „ Block “) zu erhalten. Da diese Knoten für die Aufrechterhaltung des Netzwerkes essentiell sind, werden durch die Aussicht auf eine Belohnung entsprechende Anreize gesetzt (bei Kryptowährungen durch den Erhalt einer bestimmten Menge der Währung). Der Prozess wird „Mining“ genannt.
	Node	s. „ Knoten (Node) “
	Public-private key	Jeder Nutzer hat einen einmaligen privaten Schlüssel (key), mit dem er seine Daten signiert (oder verschlüsselt). Mit dem public key, der allen Teilnehmern zur Verfügung steht, kann diese Signatur verifiziert werden.
	Smart Contracts	Smart Contracts sind intelligente/selbstausführende Prozesse. Die Ausführungsbedingungen bestehen über ein verteiltes, dezentrales Netzwerk, wodurch beispielweise keine zentrale Entscheidungsstelle notwendig ist. Transaktionen (s. „ Transaktion “) sind daher nachvollziehbar, transparent und irreversibel.
	Transaktion	Der Begriff „Transaktion“ bezeichnet in der IT die Änderung oder Erstellung eines Datensatzes in einer Datenbank. Daher sollte eine Transaktion nicht im üblichen Sinne als Übertragung von Gütern verstanden werden. Eine Transaktion muss keinen monetären Gegenwert aufweisen.
	Unveränderbarkeit (immutability)	Die Tatsache, dass einmal geschriebene Daten nicht mehr verändert werden können.
	Validierungsverfahren	s. „ Konsensverfahren “. Die Begriffe werden hier synonym verwendet.

DECHEMA

Gesellschaft für Chemische Technik
und Biotechnologie e.V.
Theodor-Heuss-Allee 25
60486 Frankfurt am Main

Telefon: 069 7564-0
Telefax: 069 7564-117
E-Mail: info@dechema.de