

MANAGEMENTKOMPASS



Blockchain

03
2017

TREND

Viele kleine Teile ergeben
das große Ganze

THINK TANK

Mehr Vertrauen
und Übersicht

PRAXIS

Dank Blockchain
mit Strom versorgt

4

EXECUTIVE SUMMARY

Nutzen prüfen,
Partner suchen

13

THINK TANK

Mehr Vertrauen
und Übersicht

20

PRAXIS

Die Blockchain
gibt Sicherheit

6

TREND

Viele kleine Teile ergeben
das große Ganze

16

WERKZEUGE

Den Blockchain-
Eignungstest bestehen

22

PRAXIS

Pilotprojekte in der
Finanzindustrie

10

TREND

Hohe Erwartungen
der Unternehmen

18

THINK TANK

Transparenz versus
Datenschutz

24

PRAXIS

Kontoeröffnung per
Gesichtserkennung

**Urs M. Krämer**

CEO
Sopra Steria Consulting

„Die Blockchain ist eine der faszinierendsten Zukunftstechnologien. Sie ist in der Lage, den Austausch von und den Umgang mit Geld, Dokumenten, Identitäten und Sachwerten zu vereinfachen, zu beschleunigen und sicherer zu gestalten – kurz: zu revolutionieren. Für viele Pioniere hat die Blockchain-Gegenwart bereits begonnen. Trotz vieler Unsicherheiten zur Machbarkeit und zu den regulatorischen Anforderungen sehe ich viele spannende praktische Anwendungen. Wer sich jetzt mit den Auswirkungen auseinandersetzt, wird Hürden schneller überwinden und die Möglichkeiten der Blockchain-Technologie für sich nutzen.“



26

PRAXISDank Blockchain
mit Strom versorgt

34

GLOSSAR

30

BLICKWECHSELIdentitätsmanagement
leichtgemacht

35

**STUDIEN
IMPRESSUM**

32

PERSPEKTIVEN

Buch & Web

**VORWORT****Carsten Kengeter**
CEO der Deutsche Börse AG

„Zusammen mit der Deutschen Bundesbank adressieren wir die potenziellen technologischen Chancen für den Finanzsektor. Wir arbeiten mit Hochdruck weiter, um mögliche Effizienzgewinne der Blockchain-Technologie heben zu können und gleichzeitig die damit verbundenen Risiken zu verstehen und zu minimieren.“

**Ginni Rometty**
CEO IBM

„Die Blockchain hat das Potenzial, für Transaktionen das zu werden, was das Internet für den Austausch von Informationen ist.“

Der Einsatz von Blockchain-Technologie ermöglicht es, den Datenaustausch und Transaktionen direkter, schneller und vor allem sicherer durchzuführen. Bei konsequenter Nutzung könnten zentrale Datenbanken, digitale Plattformen, Clearing-Instanzen oder andere Intermediäre weitgehend überflüssig werden. Die Technologie verspricht eine Dynamisierung, mehr Kunden-/Partnernähe sowie höchst individualisierte Leistungen bei geringen Kosten und maximaler Datensicherheit.

Unternehmen, die ihren digitalisierten Waren- und Werteaustausch künftig über chronologisch aneinandergeschaltete, dezentral gespeicherte Datenblöcke betreiben wollen, betreten echtes Neuland. Sie sollten zum einen das Potenzial der Blockchain im eigenen Markt- und Wettbewerbsumfeld erkunden. Zum anderen sollten sie auch die mögliche disruptive Wirkung auf ihre bestehenden Geschäftsmodelle und Strukturen bewerten. Auch der eigene digitale Status quo und bisherige Investitionshorizonte sowie Implikationen für die Mitarbeiter und die betriebliche Organisation sind zu betrachten.

Noch ist offen, wie tiefgreifend der Einfluss der relativ jungen Blockchain-Technologie sein wird. Ob und wie zeitnah ein wirtschaftlicher und gesellschaftlicher Wandel zu Daten-dezentralität und -transparenz erfolgen kann, ist nicht zuletzt eine Frage von Infrastruktur und Gesetzgebung. Welche Veränderungen sich für die Industrie, den Handel oder die öffentliche Verwaltung ergeben könnten, zeigt dieser Managementkompass anhand von Pilotprojekten und Szenarien aus der Finanz- und Energiewirtschaft.

Sopra Steria Consulting

F.A.Z.-Institut

NUTZEN PRÜFEN, PARTNER SUCHEN

Aktuelle Pilotprojekte und Pläne im Anlagenbau, in der Energiewirtschaft oder von Versicherungen zeigen: Blockchains sind wesentlich mehr als die Grundlage für den Zahlungsverkehr und den Handel mit Bitcoins und anderen virtuellen Währungen. Die dezentrale Speicherung und Verifizierung verketteter Datenblöcke nützt überall dort, wo Prozesse, Transaktionen oder Herkunftsnachweise für alle Beteiligten transparent und nachvollziehbar sein sollen, wo die vor Manipulationen geschützte und sichere Datenhaltung erfolgskritisch ist und wo Mittlerinstanzen viel Geld kosten. Nutzen und Erfolg der relativ neuen Technologie hängen von Kooperation und Konsens ab – innerhalb des eigenen Unternehmens, der eigenen Branche und im geschäftlichen Umfeld.

1 | » MANAGEMENTEMPFEHLUNG

Beobachten Sie die aktuellen Entwicklungen rund um das Thema Blockchain in Ruhe. Die Technologie umgibt derzeit ein gewisser Hype, aber es gibt keinen Grund für Hektik und Aktivismus. Bevor Sie Investitionen freigeben, sollten Sie sich kundig machen und gründlich sondieren, welche Nutzenszenarien und Anwendungsbereiche in Ihrem Geschäftsumfeld und für Ihr Unternehmen möglich sind.

Blockchains beziehungsweise die zugrundeliegende Distributed Ledger Technology (DLT) gelten als vielversprechender Ansatz, um Transaktions- und Prozesskosten zu senken und gleichzeitig die Abwicklungsgeschwindigkeit, Transparenz und Sicherheit zu steigern.

Das gilt für finanzielle Transaktionen ebenso wie für Beschaffungs- und Lieferketten, Herkunftsnachweise und vor allem für sogenannte Smart Contracts. Letztere enthalten programmierte Handlungsanweisungen (wenn X, dann Y), mit denen sie Prozesse und Aktionen automatisch auslösen können.

Während es an theoretischen Anwendungsbereichen branchenübergreifend nicht mangelt, ist die Umsetzung bisher weitgehend experimentell. Eine ausreichend hohe technologische Reife und Standards hat die Technologie längst noch nicht erreicht. Glaubt man den aktuellen Prognosen, wird es bis zum flächendeckenden Einsatz von Blockchains in Deutschland und Europa noch bis zu zehn Jahre dauern.

2 | » MANAGEMENTEMPFEHLUNG

Fragen Sie sich, wie Ihr Unternehmen von Blockchains profitieren kann und welche Voraussetzungen dafür nötig sind. Achten Sie dabei nicht nur auf die aktuelle Organisation und Ihre (IT-) Strukturen, sondern behalten Sie auch die Kosten sowie die digitalen Geschäftsmodelle im Blick, die Ihr Unternehmen verfolgt oder plant.

Vorteile können theoretisch überall entstehen, wo ein Austausch von Werten und Daten stattfindet, die vertraglich geregelt sind – also in der Beschaffung, Produktion und Logistik ebenso wie in der Arbeit mit Dienstleistern, im Handel, bei Streitfällen sowie bei der Revision und bei Überprüfungen durch Aufsichtsbehörden.

Egal ob private, öffentliche oder konsortiale Blockchains: Die Grundlagen sind stets ein Konsens, die Kooperation, die unveränderliche Dokumentation jeder einzelnen digitalen Interaktion und damit die komplette Transparenz für alle Beteiligten. Die Evaluierung von Blockchain-Technologien und -Anwendungsbereichen ist also nicht nur eine Frage der technischen Infrastruktur und organisatorischen Machbarkeit, sondern auch eine Grundsatzentscheidung.

Für Entscheider in Branchen, die bereits heute einer starken Regulierung unterliegen und die strengen Transparenzvorgaben entsprechen müssen, dürften die wesentlichen Vorteile in der Automatisierung und Vereinfachung der Prozesse sowie in erheblich niedrigeren Transaktionskosten bestehen.

Zu bedenken ist allerdings, dass es bisher (auch bei den IT-Dienstleistern) nur wenige Blockchain-Fachkräfte gibt.

3 | » MANAGEMENTEMPFEHLUNG

Orientieren Sie sich an Fakten. Wie so oft im Internet der Dinge gibt es eine Vielzahl technischer Plattformen, Anbieter und Start-ups, die in diesem Zukunftsmarkt reüssieren und ihre Claims frühzeitig abstecken wollen. Warten Sie die Entwicklung anerkannter Standards ab.

Bisher fehlen noch belastbare Referenzmodelle, Standards und Normen. Zudem gibt es zurzeit keine fälschungssicheren digitalen Identitäten sowie keinen regulatorischen Rahmen mit internationaler Gültigkeit. Für die Konzeption von Anwendungen und deren Erprobung sind solch offene Fragen kein Hindernis, doch könnten sie im späteren Einsatz zu Problemen führen. Hier gilt es, die Entwicklung zu beobachten und auf dem Laufenden zu bleiben.

Neben der Lösung von Identitäts- und juristischen Fragen (Datenschutz, Vertragsrecht, Haftung etc.) besteht aktuell erheblicher Forschungs- und Entwicklungsbedarf hinsichtlich der Skalierung und Modellierung von Geschäftsprozessen. Zudem müssen Aspekte der IT-, Netzwerk- und Protokoll-sicherheit bedacht werden.

4 | » MANAGEMENTEMPFEHLUNG

Suchen Sie sich Kooperationspartner. Um den Nutzen und die Vorteile von Blockchain- beziehungsweise DLT-Technologie nicht unter Laborbedingungen zu erproben, sondern möglichst im eigenen Geschäftsalltag, brauchen Sie mehrere Akteure, mit denen Sie Werte/Güter und Informationen auf digitalem Wege austauschen. Anwendungen gemeinsam zu entwickeln ist umso wichtiger, da es sich um eine junge Technologie handelt und bislang vor allem Pilotlösungen am Markt sind.

Erfahrungen, die direkt aus der eigenen Praxis gewonnen werden, sind in der Regel nützlicher als mehr oder minder akademische Erkenntnisse.

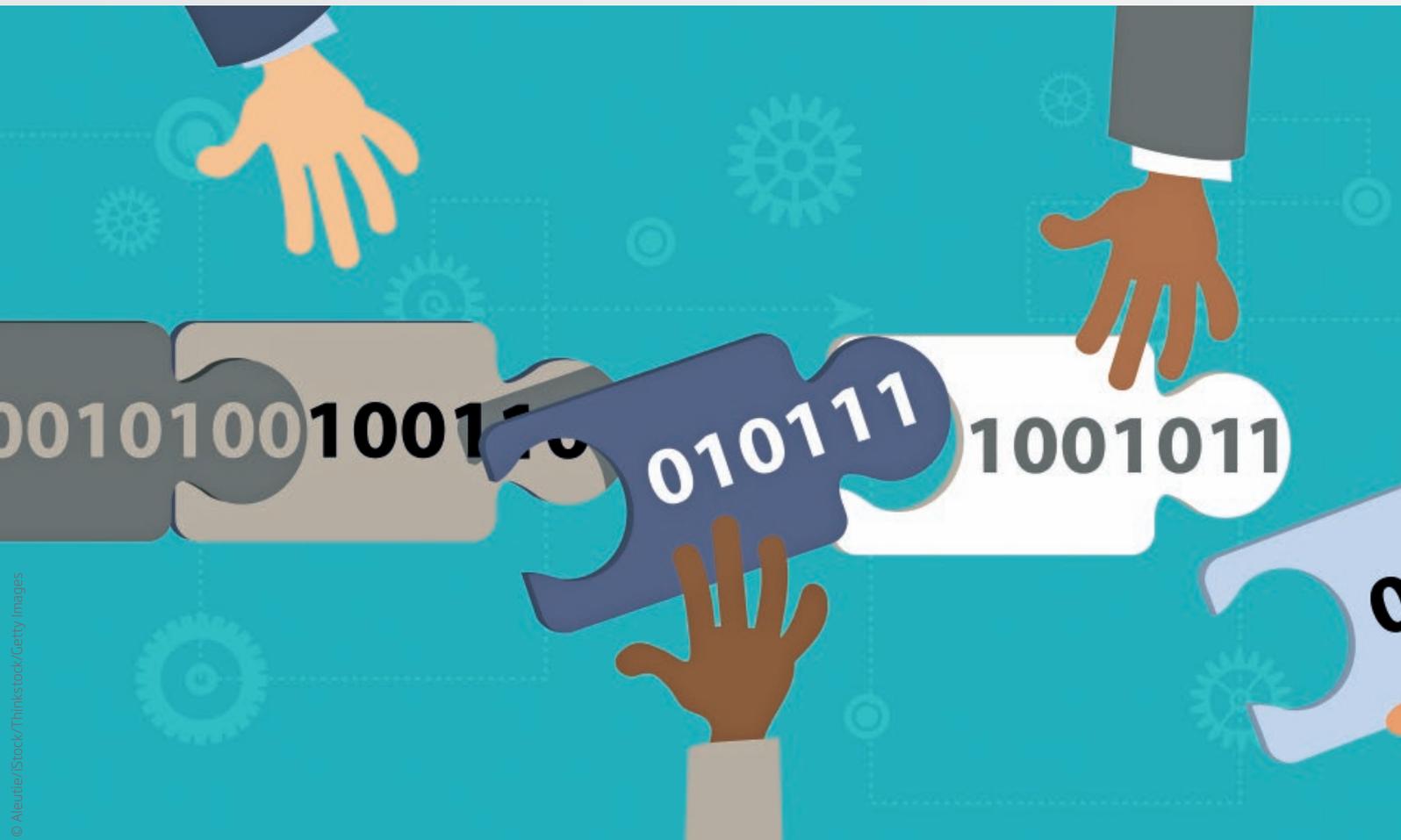
Auch aus Zeit- und Kostengründen raten Experten den Unternehmen dazu, erst einmal gemeinsam einen Prototyp und einfache Anwendungen zu entwickeln, die sich auf Grundfunktionalitäten (etwa für Herkunftsnachweise) konzentrieren. Eine Ausweitung auf andere Einsatzbereiche und Verfeinerungen des Funktionsumfangs können die Partner dann in späteren Iterationen umsetzen. Nicht nur Orientierung und Inspiration, sondern auch Hilfestellung finden Unternehmen möglicherweise in den „Blockchain as a Service“-Angeboten und -Ökosystemen diverser Hersteller.

5 | » MANAGEMENTEMPFEHLUNG

Bringen Sie Kompetenzträger aus verschiedenen Abteilungen Ihres Unternehmens zusammen, und richten Sie Ihre Roadmap auf Flexibilität aus. Um zu ermitteln, welche Use Cases für Ihr Unternehmen in Frage kommen, sollten die Fachabteilungen und IT-Experten zusammenarbeiten und dabei ausreichende kreative Freiräume haben – zum Ausprobieren und, wenn nötig, zum Verwerfen von Ansätzen. Kommunizieren Sie jedoch klar, dass die neuen technischen Möglichkeiten mit den Erfordernissen des Marktumfelds und den Unternehmenszielen in Einklang zu bringen sind.

Interdisziplinäre Zusammenarbeit – sei es im eigenen Unternehmen, in Partnerschaften innerhalb der Branche oder darüber hinaus – ist essenziell, um betriebswirtschaftlich sinnvolle Neuerungen zu schaffen. Das gilt auch für den Einsatz von Blockchain-Technologien – und durchaus auch im Kontext von modernen Analyseverfahren, der wachsenden Verbreitung Künstlicher Intelligenz (siehe Managementkompass 01/2017: Künstliche Intelligenz) und von Automatisierungsverfahren der Generation 4.0 in Industrie, Wirtschaft und öffentlicher Verwaltung. Wichtig ist hier, offen für frische Ideen zu sein und den Willen zum Wandel im eigenen Unternehmen zu kommunizieren.

VIELE KLEINE TEILE ERGEBEN DAS GROSSE GANZE



Mit Blockchain-Technologien können Unternehmen ihre Wertschöpfungsketten und Geschäftsprozesse schneller, transparenter, direkter und kostengünstiger gestalten. Zahlreiche Nutzungsszenarien sind vorstellbar, etliche davon schon auf ihre Machbarkeit untersucht. Erste Anwendungen finden sich bereits im Finanzsektor, und auch in anderen Branchen bietet sich ein weites Feld an Möglichkeiten.

» Eigenschaften wie Offenheit, Transparenz und die Minimierung des Datenfälschungsrisikos machen die Blockchain-Technologie für Unternehmen und Aufsichtsbehörden höchst attraktiv. Die verbundenen Parteien tauschen ihre Daten nach dem Peer-to-Peer(P2P)-Prinzip stets direkt miteinander aus. Dadurch werden zentrale Datenbanken und regelnde Zwischeninstanzen überflüssig, was Manipulationen extrem erschwert, denn dafür müssten Datenblöcke nebst ihrer Historie auf allen beteiligten Systemen ausgetauscht werden – und zwar zur selben Zeit. Das Prinzip der Nichtmanipulierbarkeit gilt für öffentliche Blockchains, wie sie im weitgehend anonymisierten Handel mit Bitcoins und anderen Kryptowährungen üblich sind. Es gilt aber auch für die privaten, geschlossenen Distributed-Ledger-Technologie(DLT)-Netze zwischen bekannten, vertrauenswürdigen Unternehmen in der Privatwirtschaft und Individuen, die in der Privatwirtschaft entstehen.

Aktuelle Szenarien, Experimente und erste Pilotprojekte beschäftigen sich vor allem mit zugangsbeschränkten Blockchains und der Möglichkeit, sogenannte Smart Contracts zwischen bekannten Akteuren aufzusetzen. Dabei handelt es sich um mit einem Regelwerk und Konsensmechanismen hinterlegte, automatisch ausführbare Programme, die greifen und Prozesse anstoßen, wenn zuvor festgelegte Bedingungen erfüllt sind (beispielsweise der Einkauf, sobald eine Herkunftsbestätigung verifiziert ist). Dadurch werden nicht nur Transaktionskosten eingespart, auch die Fehlerrate sinkt.

Der ursprüngliche Leitgedanke der Blockchain-Technologie – dezentrale Organisation ohne Mittelsmänner – tritt bei manchen aktuellen Forschungen, Experimenten

und Pilotprojekten der Privatwirtschaft jedoch in den Hintergrund: Blockchain-Projekte sollen in diesen Fällen die traditionellen Geschäftsmodelle und Vermittler-tätigkeiten (beispielsweise Kredite, Investments oder Clearing) mit moderner Technik erhalten, effizienter und kostengünstiger machen – was den eigentlichen Ansatz der Blockchain-Technologie eher konterkariert. Dies zeigen insbesondere manche Bemühungen um eigene Varianten einer Kryptowährung.

Finanzsektor als Vorreiter

Mit ihren eigenen Projekten reagieren die Banken auf den Trend, denn weltweit sehen sie sich durch Blockchain-Anwendungen in ihrer Rolle als Intermediär unter Druck: Unternehmen und Einzelpersonen können ihre Transaktionen über hochgradig fälschungssichere Datenblöcke und unter Zuhilfenahme von Kryptowährungen direkt miteinander abwickeln. Traditionelle Vermittler- und Vertrauensinstanzen, die für ihre Leistungen (etwa bei Aktiengeschäften, aber auch bei Bezahl-systemen wie Paypal) Gebühren und Provision verlangen, sind dann nicht mehr notwendig.

Dabei bietet die Blockchain-Technologie auch Chancen: Selbst ohne eine Umstellung der Geschäftsmodelle könnten Banken allein durch die Umstellung auf DLT-Verfahren und Smart Contracts erhebliche Effizienzgewinne und Kosteneinsparungen in Milliardenhöhe erzielen. Die Euro Banking Association (EBA) sieht Potenziale für Blockchain-Anwendungen vor allem im Devisenhandel, bei grenzüberschreitenden Transaktionen, Echtzeit-Überweisungen sowie der Abwicklung „komplexerer“ Finanzprodukte.

UNTERSCHIEDE ZWISCHEN ÖFFENTLICHEN UND PRIVATEN BLOCKCHAINS

	Öffentliche Blockchain	Private Blockchain
Zugriff	offener Schreib- und Lesezugriff	Schreib- und Lesezugriff nur nach Berechtigung
Geschwindigkeit	langsamer	schneller
Sicherheit	Proof of Work/Proof of Stake	vorab festgelegte Nutzer
Identität	anonym/Pseudonym	bekannte Identitäten
Beispiele	Finanzsektor: Bitcoin; allgemein: Ethereum	Finanzsektor: Corda; allgemein: Hyperledger

Quellen: Crisp Research, eigene Recherchen

Welche Services Versicherungsgesellschaften und Rückversicherer auf der Grundlage von Blockchain-Technologie entwickeln können, erkundet die 2016 gegründete Blockchain Insurance Industry Initiative B3i. So ließen sich Konditionen individuell gestalten und Prozesse derart definieren, dass mögliche Ansprüche automatisch geprüft werden und Versicherte sofort Entschädigung/Unterstützung erhalten, zum Beispiel bei Betriebsunterbrechungen aufgrund von Strom-/Internetausfall oder bei Wetterschäden in der Landwirtschaft.

Auf der Basis von dokumentierbaren und damit nachvollziehbaren Informationen können auch Reiseunternehmen die Blockchain-Technologie nutzen: „Sobald ein Flug mehr als 30 Minuten Verspätung hat, könnte ein Versicherter Entschädigung bekommen – und das automatisch, denn das Blockchain-Netzwerk erhält die Fluginformationen in Echtzeit und triggert sogleich die Auszahlung, wenn die Kriterien des Vertrags erfüllt sind“, berichtet der Blog zum „Blockchain Bootcamp“ der SAP AG. Das Unternehmen geht wie viele Experten davon aus, dass Blockchains zu einer sinnvollen Ergänzung von ERP-Systemen (etwa im Vertragsmanagement) und parallel zu ihnen laufen werden, während gleichzeitig neue Systeme auf der Grundlage von DLT entstehen.

„Im Prinzip kann die Blockchain wie eine Datenbank genutzt werden – interessant ist das beispielsweise in der Logistik oder im Supply Chain Management, aber auch in der Fertigung oder im 3-D-Druck bei der sicheren Übertragung von Produktionsplänen. Die Blockchain ist überall dort interessant, wo es um die Nachvollziehbarkeit und Rückverfolgbarkeit von Produkten und Dienstleistungen geht“, so die Einschätzung von Marco Liesenjohn, Referent Blockchain beim Digitalverband Bitkom.

Außerhalb des Finanzsektors und des klassischen Vertragswesens finden sich vorstellbare Nutzungsbereiche und experimentelle Blockchain-Anwendungen vor allem in folgenden Bereichen:

- » **Verwaltung:** Datenaustausch zwischen Behörden; Registerführung; Eigentumsrechte (Immobilien, Marken- und Urheberrechte etc.); revisions sichere Archivierung, digitaler Pass/Fingerabdruck
- » **Produktion/IoT (Internet of Things):** manipulations sichere Kommunikation/Datenübertragung in vernetzten Systemen; Rückverfolgbarkeit, Fehlerana-

lyse und Optimierung von Herstellungsprozessen; Smart Contracts/Automatisierung; Zertifikate; Echtzeit-Information

- » **Handel und Logistik:** lückenlose Verfolgbarkeit von Lieferketten; transparente Warenströme; Betrugserkennung (Zoll, gefälschte Produkte, bewusste Fehldeklarationen etc.); Echtheitszertifikate; nachvollziehbarer Online-Handel; sichere Zahlssysteme
- » **Telekommunikation:** Betrugs-/Cybercrime-Aufdeckung; Identitätsmanagement; individualisierte Tarife; Leistungstransparenz; Rechnungstellung
- » **Lebensmittel und Pharmaindustrie:** Nachweis von Inhaltsstoffen und Herkunft; Smart Contracts für Lagerung, Produktion und Logistik; transparente Liefer- und Leistungsketten
- » **medizinische Versorgung:** Austausch und Abgleich von Gesundheitsdaten; Patientenzugriff (Stichwort: Datenhoheit); Transparenz der Leistungsträger und Abrechnungen
- » **Energiewirtschaft:** vereinfachtes Einbinden kleiner, dezentraler Stromerzeugungsanlagen; transparentes Verteilsystem (Angebot/Nachfrage); transparente Verbrauchs-/Rechnungsläufe

Anwendungsszenarien und Erprobungen finden sich auch in der Touristik, in der Luftfahrt und im militärischen Bereich.

Erfolgsfaktor Kooperationen

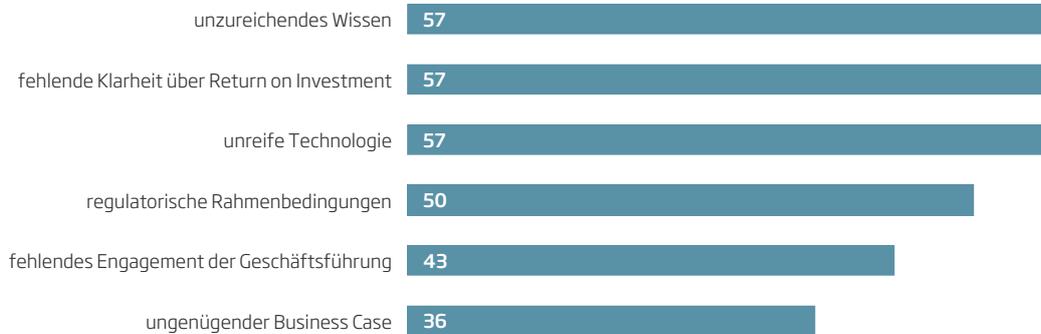
Noch stellen sich viele Fragen rund um die Praxistauglichkeit der Blockchain-Technologie: Es geht um die Risikobegrenzung, die Einhaltung gesetzlicher und regulatorischer Vorgaben, Sicherheits- und Kosteneffizienzaspekte sowie darum, Standards zu setzen.

Mit all diesen Fragen beschäftigen sich aktuell gleich drei internationale Konsortien mit massiver deutscher Beteiligung und unterschiedlichem Ansatz:

- » Die Hyperledger Alliance, der 120 Unternehmen angehören, will Blockchain-Projekte auf der Grundlage von Linux-Software entwickeln.
- » Die R3-Allianz, ein wachsender Verbund von deutschen und internationalen Banken, entwickelt eine

DURCHBRUCH STEHT NOCH AUS

Aktuelle Hindernisse für die Einführung von Blockchain-Technologien im Finanzsektor; Angaben in Prozent der Befragten¹⁾



1) Befragung unter 200 Finanzinstituten aus 16 Ländern (Mehrfachnennungen)

Quelle: IBM Institute for Business Value (2016)

geschlossene DLT-Lösung namens Corda für finanzielle Transaktionen zwischen regulierten Finanzinstituten.

- » Die Enterprise Ethereum Alliance (EEA) betreibt Grundlagen- und Anwendungsforschung auf Basis der Open-Source-Blockchain Ethereum und vereint Unternehmen wie JP Morgan, Microsoft und Intel.

Kein Anlass für Aktionismus

Aktuell kommen die Analysten von Gartner zu der Einschätzung, dass der Hype um Blockchains den Zenit bereits überschritten hat. Bevor DLT-Technologien das „Tal der enttäuschten Erwartungen“ (eine Phase des Hype-Zyklus von Gartner) durchschreiten und Produktionsreife erlangen, könnten noch fünf bis zehn Jahre vergehen. Verschiedene Befragungen zu konkreten Projekten und der mittelfristigen Investitionsplanung in Unternehmen bestätigen diese These.

Laut Untersuchungen von Marktforschungs- und Beratungsunternehmen wie Crisp Research entwickeln sich DLT-Technologien derzeit extrem dynamisch. Das Feld der Anbieter und Anwendungsmöglichkeiten könnte sich in den kommenden sechs bis 18 Monaten also recht deutlich vom heutigen unterscheiden. Die vielversprechende Kombination von Blockchains mit modernen Analytics-Verfahren und maschinellem Lernen (Künst-

liche Intelligenz) könnte noch einmal deutlich breitere Nutzenszenarien ergeben.

Vollkommen offen aber ist, welche der zahlreichen Blockchain-Ansätze sich mittelfristig durchsetzen werden. Für die verschiedenen Branchen und den öffentlichen Bereich müssen sich erst noch Standards durchsetzen, auf die Entscheider aufsetzen können, wenn sie konkrete Use Cases entwickeln.

Machbarkeitsstudien zeigen, dass etliche der theoretisch möglichen Vorteile von Blockchains in der Praxis noch nicht zu erzielen sind. Dies liegt an ungelösten rechtlichen und regulatorischen Fragen, fehlenden technischen und prozessualen Standards oder Aspekten der digitalen Infrastruktur, ihrer Skalierbarkeit und Geschwindigkeit. «



Jacqueline Preußer
ist Redakteurin
im F.A.Z.-Institut.

HOHE ERWARTUNGEN DER UNTERNEHMEN

Sopra Steria Consulting hat im Rahmen der „Potenzialanalyse Blockchain-Technologie“ Fach- und Führungskräfte aus Unternehmen ab 500 Mitarbeitern befragt, wie sie die Chancen und Möglichkeiten einschätzen, die diese neue Technologie für ihr Unternehmen sowie ihre Branche bietet, und wie es um den Status der Einführung steht.

» Die Blockchain-Technologie ist nicht nur ein Thema für Spezialisten und Insider. Sie ist Fach- und Führungskräften in Deutschland durchaus ein Begriff. Das ist ein zentrales Ergebnis der „Potenzialanalyse Blockchain-Technologie“, für die Sopra Steria Consulting im Juli und August 2017 in einer Online-Erhebung 204 Fach- und Führungskräfte befragt hat.

Teilgenommen haben Vorstände und Geschäftsführer (10 Prozent), leitende Angestellte (66 Prozent) und Fachkräfte beziehungsweise Spezialisten (24 Prozent) überwiegend aus der IT, aber auch aus den Bereichen Finanzen/Controlling, Business Development und Vertrieb. Jeweils ein Drittel der Befragten kam aus den Branchen Finanzdienstleistungen und verarbeitendes Gewerbe.

Knapp acht von zehn Befragten haben bereits von Blockchain gehört, knapp die Hälfte gibt sogar an, genau zu wissen, um was es sich dabei handelt. 39 Prozent dieser Befragtengruppe – in der Befragung als „Blockchain-Kenner“ bezeichnet – haben bereits mit mindestens einer Blockchain-Plattform gearbeitet. Vergleicht man die Aussagen und Einschätzungen der Kenner mit denen

der restlichen Befragten, zeigt sich, dass es in weiten Teilen noch an Verständnis und Wissen über die Blockchain-Technologie mangelt.

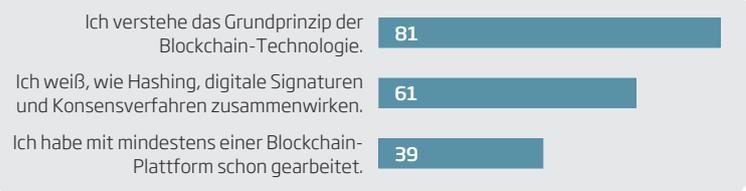
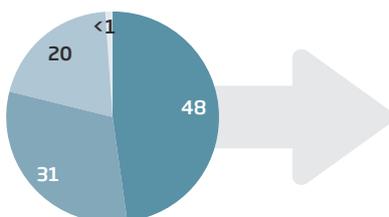
Erste Blockchain-basierte Systeme sind im Einsatz

Die Unternehmen sind mit dem Einsatz der Blockchain überwiegend noch in der Informations- und Entscheidungsphase. 47 Prozent der Blockchain-Kenner geben an, dass ihr Unternehmen mögliche Anwendungsfälle prüft, 45 Prozent sagen, dass die Technologie beobachtet wird. Immerhin 22 Prozent haben in ihrem Unternehmen bereits ein Blockchain-basiertes System im Einsatz, und fast ebenso viele entwickeln derzeit einen Prototypen.

Ein Fünftel der Befragten insgesamt stellt klar: Ihr Unternehmen tut sich mit dem Identifizieren von sinnvollen Einsatzmöglichkeiten für die Blockchain noch schwer. Immerhin ein Drittel attestiert dem eigenen Unternehmen, dass man zumindest ein grobes Verständnis für die Anwendbarkeit der Blockchain hat. In der Finanzbranche

BEKANNT UND GENUTZT

Bekanntheit der Blockchain und persönlicher Kenntnisstand; in Prozent der Befragten



- Ja, ich habe bereits davon gehört und weiß, was die Blockchain-Technologie ist.
- Ja, ich habe bereits davon gehört, weiß aber nicht genau, was die Blockchain-Technologie ist.
- Nein, ich habe noch nie davon gehört.
- weiß nicht/keine Angabe

Basis: alle Befragten, n = 204

Basis: Befragte, die wissen was Blockchain ist, n = 98 (Mehrfachnennungen)

Quelle: Potenzialanalyse Blockchain-Technologie (Sopra Steria Consulting)

ist die neue Technologie bereits angekommen: Dort sind es immerhin 18 Prozent der Befragten, die angeben, dass ihr Unternehmen genau weiß, wo die Blockchain sinnvoll einzusetzen ist.

Viele Vorteile

Auch wenn sich das Gros der Unternehmen hinsichtlich der Blockchain derzeit noch in der Informations- und Entscheidungsphase befindet: Aus Sicht der Befragten spricht viel für den zukünftigen Einsatz der Technologie. Die gute Hälfte der Befragten sieht darin Chancen für völlig neue Geschäftsmodelle.

Wichtige Argumente für die Blockchain sind aus Sicht der Fach- und Führungskräfte die hohe Transaktions- und Dokumentensicherheit. Vier von zehn Befragten erwarten, dass ihr bestehendes Geschäft durch den Einsatz der Technologie effizienter, schneller oder günstiger werden wird. Damit lassen sich auch Wettbewerbsvorteile in engen Märkten sichern.

Allgemein sieht die Gesamtheit der Befragten einen Verbesserungsbedarf bei der Integrierbarkeit der Technologie (79 Prozent), der Standardisierung (79 Prozent) und der Vertraulichkeit der Daten (76 Prozent). Die Blockchain-Kenner hingegen sehen Verbesserungsbedarf eher bei der Latenz (63 Prozent), dem Durchsatz (61 Prozent) und der Standardisierung (53 Prozent).

Marktreife noch nicht ganz erreicht

Knapp die Hälfte der Unternehmen sieht die Blockchain derzeit noch auf einer experimentellen Entwicklungsstufe. Diese dient derzeit eher dazu, wichtige Erfahrungen für die Zukunft zu sammeln. Marktreife attestieren entsprechend auch nur 7 Prozent der Befragten, und

DEFINITION BLOCKCHAIN

Um auch Befragungsteilnehmern, die zwar von Blockchain gehört haben, aber nicht genau wissen, was sie sich darunter vorstellen sollen, eine sinnvolle Beantwortung der Befragung zu ermöglichen, wurde den Teilnehmern folgende Definition an die Hand gegeben:

Die Blockchain-Technologie, auch als Distributed Ledger Technology bezeichnet, ermöglicht es, Daten dezentral abzuspeichern und Programme dezentral auszuführen. Die technischen Eigenschaften garantieren allen Teilnehmern, dass dabei streng nach gemeinsam festgelegten Regeln vorgegangen wird, so dass niemand den Ablauf manipulieren kann.

Das bekannteste Beispiel ist das Bitcoin-Netzwerk, in dem alle Teilnehmer über die Guthaben aller anderen Teilnehmer anonymisiert Buch führen. Das ermöglicht Zahlungsverkehr ohne eine Bank, und auch allgemein ermöglicht die Blockchain-Technologie, Netzwerke ohne zentrale Vermittlungsinstanz einzurichten. Deswegen schreibt man der Technologie disruptives Potenzial zu.

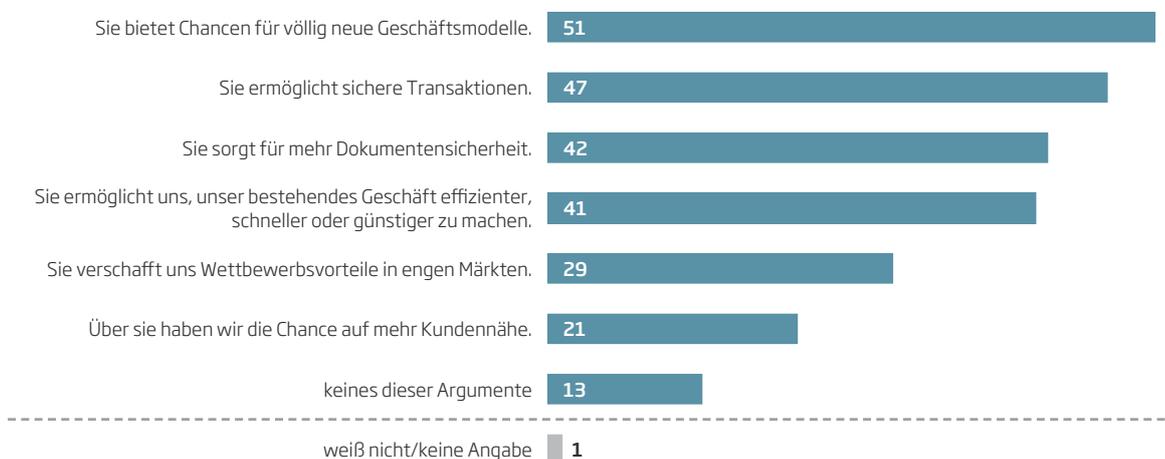
etwas mehr als ein Viertel der Befragten hält die neue Technologie schon für reif genug, um in Randbereichen der Geschäftstätigkeit probeweise eingesetzt zu werden. Nur jeder zehnte Befragte hält die Technologie für nicht praxistauglich. Diese Einschätzung hinsichtlich der Marktfähigkeit ähnelt sich über alle befragten Branchen hinweg.

Denkbare Einsatzbereiche

Es sind vor allem vier Bereiche, in denen sich die Befragten, deren Unternehmen die Blockchain noch nicht einsetzen, den Einsatz vorstellen können: Payments, Supply Chain (jeweils 37 Prozent), Identity Management (31 Prozent) sowie am Kapitalmarkt, zum Beispiel zur Abwicklung von Wertpapiergeschäften ohne eine zen-

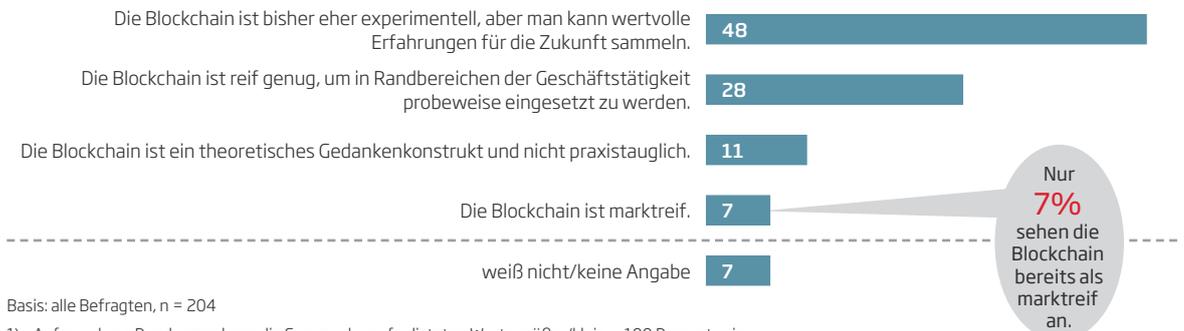
BLOCKCHAIN: CHANCE AUF NEUE GESCHÄFTSMODELLE UND HÖHERE SICHERHEIT

Argumente für die Blockchain; in Prozent der Befragten



DIE BLOCKCHAIN IST NOCH EXPERIMENTELL

Einschätzung des aktuellen Entwicklungsstands der Blockchain; in Prozent der Befragten¹⁾



Basis: alle Befragten, n = 204

1) Aufgrund von Rundungen kann die Summe der aufgelisteten Werte größer/kleiner 100 Prozent sein

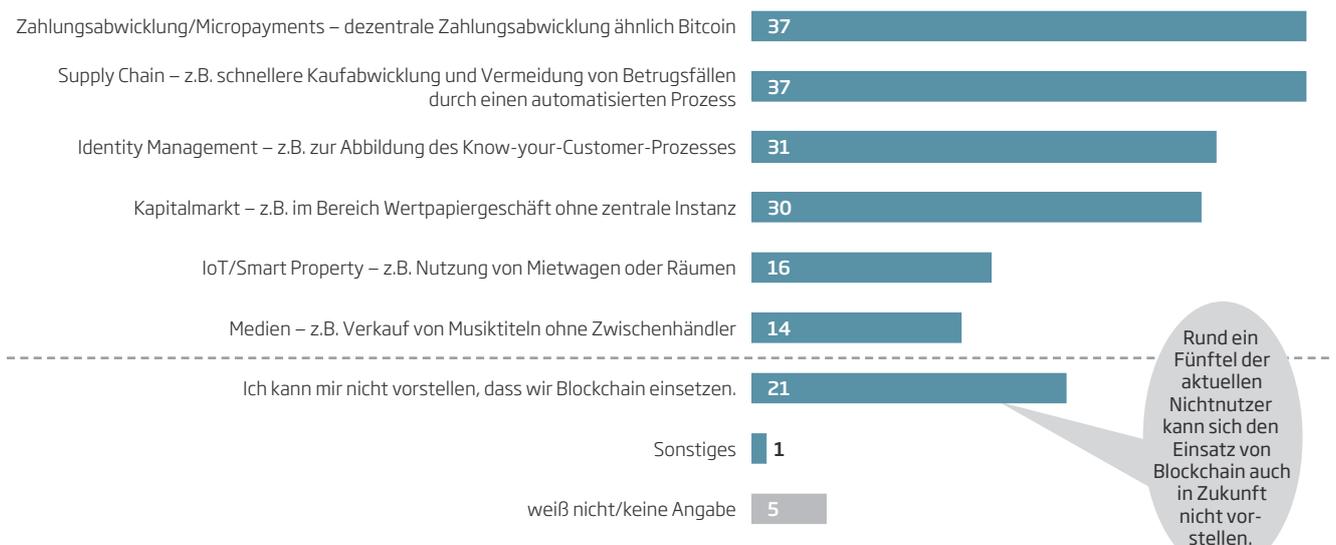
Quelle: Potenzialanalyse Blockchain-Technologie (Sopra Steria Consulting)

trale Instanz (30 Prozent). Bei der Zahlungsabwicklung und bei Micropayments steht die dezentrale Zahlungsabwicklung, wie sie bereits bei Bitcoin praktiziert wird, im Vordergrund. Bei der Identifizierung könnte beispielsweise der komplette Know-your-Customer-Prozess durch die neue Technologie abgebildet werden. Finanzdienstleister und verarbeitendes Gewerbe sehen die Einsatzbereiche für die Blockchain sehr ähnlich. Nur rund ein Fünftel der Befragten, die bislang die Blockchain nicht nutzen, sieht in seinem Unternehmen auch für die Zukunft keine Einsatzmöglichkeit.

Das Gros der Befragten, in deren Unternehmen bereits die Blockchain zum Einsatz kommt oder die sich den Einsatz vorstellen können, sieht hier auch die Möglichkeit der Kooperation mit anderen Unternehmen. Dabei schließen sie auch den gemeinsamen Betrieb mit einem direkten Konkurrenten nicht aus. Die Nutzung von „Blockchain as a Service“ ist der am ehesten für die Befragten vorstellbare Weg der Blockchain-Teilnahme. «

PAYMENTS, IDENTITY MANAGEMENT UND SUPPLY CHAIN ALS EINSATZBEREICHE DENKBAR

Bereiche, in denen ein Einsatz der Blockchain vorstellbar ist; in Prozent der Befragten



Basis: Befragte, in deren Unternehmen die Blockchain noch nicht eingesetzt wird, n = 182 (Mehrfachnennungen)

Quelle: Potenzialanalyse Blockchain-Technologie (Sopra Steria Consulting)

MEHR VERTRAUEN UND ÜBERSICHT

Für die fortschreitende Digitalisierung bietet die Blockchain-Technologie das ideale Gerüst. Mit ihrer Hilfe lassen sich Prozesse optimieren und vereinfachen, Transaktionen werden beschleunigt und nachvollziehbar.

» Die Grundidee hinter der Blockchain-Technologie besteht darin, Transaktionen und Verträge ohne eine zentrale Instanz abzuwickeln. Stattdessen übernimmt ein dezentrales System die Steuerung: ein verteiltes Register (Distributed Ledger), das sämtliche Transaktionen erfasst, in einem Peer-to-Peer(P2P)-Netzwerk speichert und laufend aktualisiert. Die Transaktionen werden in exakt chronologischer Reihenfolge erfasst und können nicht mehr gelöscht werden. Die Blockchain macht es somit möglich, durch ein Protokoll, das betrügerische Intentionen verhindert, Vertrauen zu schaffen. Vergangene Transaktionen könnten nicht mehr korrigiert oder, im Falle von Geldtransfers, ein bereits übermittelter Betrag nicht nochmals ausgegeben werden.

Wie alles begann: Kryptowährungen und Smart Contracts

Als im Jahr 2008 unter dem Pseudonym Satoshi Nakamoto die Funktionsweise der Blockchain-Technologie veröffentlicht wurde, stellte der Autor in diesem Zusammenhang die Kryptowährung Bitcoin vor. Mit der Bitcoin-Währung war der erste konkrete Anwendungsfall geschaffen. Obwohl zahlreiche neue digitale Währungen folgten (Ether, Ripple, Litecoin etc.), ist Bitcoin auch heute noch die bekannteste und bedeutendste unter den Kryptowährungen, deren gesamte Marktkapitalisierung Mitte August 2017 etwa 140 Milliarden US-Dollar betrug, allein 70 Milliarden US-Dollar entfielen auf Bit-

coin. Zum Vergleich: Die Marktkapitalisierung aller 30 Dax-Konzerne betrug zu dieser Zeit 1.140 Milliarden Euro, also umgerechnet über 1.300 Milliarden US-Dollar.

Kryptowährungen in Verbindung mit der Blockchain bieten, verglichen mit herkömmlichen Bezahlmethoden, einige Vorteile. So wird ein reibungsloser, internationaler Transfer gewährleistet, der mit Transaktionszeiten von nur wenigen Minuten und geringen Kosten verbunden ist. Transfers können jederzeit mit einer Internetverbindung, einer Wallet-Software und einem Computer beziehungsweise einem mobilen Endgerät ausgeführt werden.

“

Die Blockchain kann Probleme der Datensicherheit, des Konsumentenschutzes oder der Sicherung geistigen Eigentums lösen.

”

Mit Hilfe der Blockchain-Technologie können sowohl einander unbekannte Organisationen als auch Einzelpersonen ein vertrauenswürdigeres, dezentrales Netzwerk aufbauen. Die Blockchain bietet das Potenzial, Probleme der Datensicherheit, des Konsumentenschutzes oder der Sicherung geistigen Eigentums zu lösen.

Die Technologie ist der Wegbereiter für digitale Verträge, die Smart Contracts. Mit Hilfe von Computerprotokollen lassen sich sämtliche Verträge vollständig digital abbilden,

so dass eine Schriftform überflüssig wird. Durch die Blockchain können smarte Verträge überprüft, verhandelt und abgewickelt werden, seien es Kaufverträge, Mietverträge oder Leasingverträge. Interessant kann hier die Überwachung von Zahlungstransaktionen sein. Wird beispielsweise im Falle eines Leasingfahrzeugs eine fällige Rate nicht bezahlt, so kann der fehlende Zahlungseingang in der Blockchain nachvollzogen wer-

den. Wenn das Fahrzeug mit dem System gekoppelt ist, wäre es außerdem möglich, bei fehlenden Zahlungen die Funktionalität des Kfz abzustellen, bis die fälligen Beträge eingegangen sind.

Die zunehmende Bedeutung von dezentralen Systemen

Während heute nahezu alle Institutionen, egal ob Banken, Behörden, Geschäfte oder Ähnliches, zentral gesteuert werden, könnte sich dies mit der Blockchain-Technologie grundlegend ändern. So müssen bis dato Prozesse von einer zentralen Behörde oder Institution kontrolliert und freigegeben werden. Meistens ist damit ein hoher Zeitaufwand verbunden, was die Einfachheit und den Nutzen vieler Services einschränkt. Mit der Blockchain-Technologie kann all dies effizienter erfolgen. Die dezentrale Verteilung auf unterschiedlichen Rechnern erlaubt eine Abwicklung rund um die Uhr. Damit steigt nicht nur die Flexibilität, sondern auch die Geschwindigkeit, mit der Prozesse ablaufen.

Aus technischer Sicht liegen die Vorteile ganz klar in der Sicherheit. Zentrale Institutionen bedienen sich in der Regel auch eines zentral gesteuerten IT-Systems, das stets überwacht und gewartet werden muss, was mit enormen Kosten und teils auch Vertrauen in die jeweiligen Mitarbeiter verbunden ist. Die Gefahr, Opfer einer Cyber-Attacke zu werden, ist bei zentral gesteuerten IT-Systemen höher als bei dezentralen. Das Blockchain-System ist nahezu immun gegen Cyber-Angriffe, da keine zentrale Datenbank existiert, die gehackt werden könnte. Stattdessen sind alle Daten auf verschiedenen Rechnern weltweit verteilt gespeichert. Ein weiterer Vorteil dieses Netzwerks: Die Blockchain ist für die Öffentlichkeit zugänglich. So kann prinzipiell jeder zu jeder Zeit Transaktionen nachvollziehen. Eine hochleis-



tungsfähige Verschlüsselung mit Public und Private Keys (benötigt für Transaktionen) etabliert einen hohen Sicherheitsstandard.

Schneller, besser, transparenter

Eine der vielversprechendsten Innovationen durch die Blockchain-Technologie ist die Verbesserung der Infrastruktur. Komplexe Abläufe können mit Hilfe der Technologie miteinander verschmolzen werden, um die Kosten zu senken und die Geschwindigkeit zu verbessern.

Dies bringt beispielsweise Vorteile für das Abwickeln von Zahlungsprozessen und Kapitalbewegungen. Existierende Prozesse im Finanzsektor beruhen großteils auf veralteten Technologien und involvieren eine Vielzahl an Intermediären, die ihrerseits Transaktionsgebühren erheben. Dies gilt nicht nur für Auslandsüberweisungen. Während das Clearing einer Kreditkartenzahlung nur wenige Sekunden in Anspruch nimmt, kann es Tage oder Wochen dauern, bis alle Intermediärsinstanzen durchlaufen sind und das finale Settlement der Forderung erfolgt ist. Zum Vergleich: Bei einer Transaktion auf der Bitcoin-Blockchain beträgt die durchschnittliche Bestätigungsdauer derzeit etwa zehn Minuten.

Auf einer Blockchain werden Zahlungen fortlaufend und integriert abgewickelt (Clearing und Settlement), so dass das Register jederzeit aktuell ist. Intermediäre sind dabei nicht mehr Teil des Prozesses. Internationale Transaktionen werden agiler, günstiger und mögliche Ausfallrisiken minimiert. Durch den Einsatz von Distributed-Ledger-Technologien können Banken bei Zahlungstransaktionen sowie bei der Erfüllung gesetzlicher Anforderungen bis zum Jahr 2022 zwischen 15 und 20 Milliarden US-Dollar pro Jahr sparen, zeigt eine Studie, die Santander InnoVentures mit weiteren Partnern erarbeitet hat.

Compliance im Internet of Things

Die Blockchain kann die Vernetzung und Anwendung von Smart Devices aktiv unterstützen. Eine Konvergenz von Internet of Things (IoT) und Blockchain liegt allein schon wegen ihrer Grundcharakteristika nahe. Das IoT ist per Definition dezentral. Bis zum Jahr 2020 werden laut Gartner Research rund 20 Milliarden Geräte Teil des Netzwerks sein. Eine Integration all dieser dezentral verteilten Geräte zu einem zentral organisierten Netzwerk wäre extrem komplex, kostenintensiv und wenn überhaupt, dann nur mit hohem Aufwand zu sichern. Auf Grundlage der Bitcoin-Blockchain ließe sich sicherstel-

len, dass die von den Smart Devices gelieferten Daten vertrauenswürdig und unveränderbar sind, allerdings ist Bitcoin hierfür nicht ideal geeignet. Besonders relevant ist daher eine Weiterentwicklung: Ethereum. Während die Bitcoin-Blockchain lediglich Transaktionen von Werten abwickelt und ablegt, lassen sich mittels Ethereum Smart Contracts programmieren, mit deren Hilfe Compliance im IoT manifestiert werden kann.

Ein Beispiel: Ein Container mit Medikamenten, der von Schweden nach Indonesien verschifft wird, erhält eine digitale Identität. Smart Devices liefern Daten über den Standort des Containers sowie die Temperatur und Luftfeuchtigkeit innerhalb des Containers. Alle Akteure des Prozesses (Banken im Ursprungs- und Zielland, Spediteure, Häfen, Zoll, Versicherer, Empfänger) sind Teil der privaten Blockchain für diesen Prozess. Über einen Smart Contract wird der Auftrag inklusive gewisser Anforderungen an die Einhaltung bestimmter Temperaturgrenzen erstellt, und im Laufe des Prozesses werden – basierend auf dem Standort des Containers oder durch Barcode-Scans – Zahlungen freigegeben. Verstöße gegen die Temperaturentwicklungen werden aufgenommen und können direkt zugeordnet werden.

Ausblick

Die Blockchain-Technologie erlangt eine immer größere Bedeutung, sei es für die Verarbeitung von Transaktionen, die Abstimmung zwischen vernetzten Maschinen oder „Mikrozahlungen“ ohne den Einbezug von Zahlungsdienstleistern. Intermediäre, die ihr Geschäftsmodell angegriffen sehen, können ihre Zukunftsfähigkeit verbessern, indem sie die durch die Blockchain gebotenen Chancen ergreifen.

Die Technologie erlaubt die Optimierung bestehender Prozesse und vor allem die Umsetzung innovativer Geschäftsmodelle – und zwar nicht nur für den hiesigen Markt, sondern vor allem im internationalen Kontext. Denn insbesondere bei grenzüberschreitenden Leistungen und im internationalen Zahlungsverkehr entfaltet die Blockchain-Technologie ihr gesamtes Potenzial. «



Prof. Dr. Philipp Sandner
leitet das Frankfurt School Blockchain Center an der Frankfurt School of Finance & Management.



Martin Röchow
studiert International Business Administration an der Frankfurt School of Finance & Management.



Patrick Breckner
studierte Biologie und Wirtschaftswissenschaften an der TU München und schreibt derzeit seine Masterarbeit zum Thema Blockchain und Connected Cars.

DEN BLOCKCHAIN- EIGNUNGSTEST BESTEHEN

Szenarien für den Einsatz der Blockchain-Technologie gibt es mittlerweile für viele Branchen. Um Anwendungsfälle zu prüfen, empfiehlt sich ein methodisches Vorgehen.

» Bevor eine konkrete Blockchain-Anwendung implementiert werden kann, muss in einem methodisch aufgebauten Bewertungsprozess ein geeigneter Anwendungsfall gefunden werden. Als Analogie dient ein Trichter, in den alle Ideen für einen Blockchain-Use-Case hineinkommen. Je enger der Trichter, umso feinschziger ist das Sieb, so dass am Ende nur Use Cases herauskommen, mit denen eine Blockchain-Anwendung umsetzbar ist.

Rahmenbedingungen prüfen

Damit eine Idee überhaupt mit Hilfe der Blockchain-Technologie realisiert werden kann, müssen vier grundlegende Voraussetzungen erfüllt sein:

- 1) Assets, also Güter materieller oder immaterieller Art, müssen zwischen zwei oder mehreren Parteien transferiert werden, zum Beispiel Autos, Immobilien, Geld, Patente oder Kunstwerke.
- 2) Alle am Projekt Beteiligten sind über ein Netzwerk miteinander verbunden.
- 3) Es existiert keine zentrale Instanz, alle Transaktionen zwischen den Teilnehmern erfolgen über eine dezentrale Kommunikation.
- 4) Die Anzahl an Transaktionen pro Sekunde ist begrenzt. Zurzeit ist die Blockchain-Technologie für sehr hohe Transaktionsvolumen (> 50 Transaktionen pro Sekunde) nur schwer zu implementieren.

Zur Illustration soll das Beispiel Grundbuchamt dienen: Das Asset wäre der Grundbucheintrag. Ein Netzwerk, an dem alle Teilnehmer miteinander verbunden sind, existiert aktuell nicht, wäre aber in einer Blockchain-Lösung möglich. Das Grundbuchamt wäre als zentrale Instanz nicht zwingend erforderlich, denn durch die Blockchain-Technologie und das dezentrale Netzwerk von Teilnehmern wird Vertrauen gewährleistet. Je nach Größe der Stadt, für die das Grundbuchamt verantwortlich ist, fal-

PROZESS ZUR ERMITTLUNG EINES BLOCKCHAIN-USE-CASES



Quelle: Sopra Steria Consulting

len nicht mehr als zehn Transaktionen pro Sekunde an. Damit erfüllt dieser Use Case die vier Bedingungen.

Ziele definieren

Die Blockchain ist zwar kein Allheilmittel, sie kann aber dazu dienen, bestimmte Ziele zu erreichen. Von den fünf folgenden Zielen sollte mindestens eines mit dem Business-Use-Case verfolgt werden:

- » **weniger Kosten:** Mit der Blockchain lassen sich Kosten reduzieren, indem bestehende Prozesse automatisiert werden oder eine zentrale Instanz obsolet wird.
- » **mehr Sicherheit:** Durch die Verschlüsselung von Daten und die redundante Speicherung der Register (Ledger) erhöht die Blockchain die Sicherheit und erschwert Betrugsversuche.

- » **schnellere Transaktionen:** Die dezentrale Struktur und automatisierte Prozesse verbessern die Abwicklung von Transaktionen, wie etwa die Überweisung von Geld in Minuten anstatt in Tagen.
- » **Vertrauen schaffen:** Die Blockchain protokolliert alle Transaktionen und Zustandsänderungen chronologisch. Dies gewährleistet eine lückenlose Nachvollziehbarkeit. So können Reparaturen und Ersatzteile, die ein Auto seit der Herstellung erhalten hat, aufgezeichnet und die Qualität eines Gebrauchtwagens besser beurteilt werden.
- » **Vernetzung:** Die Blockchain basiert auf der Vernetzung von Teilnehmern. Durch ein solches Netzwerk könnte zum Beispiel ein Logistikunternehmen seinen Kundenstamm vergrößern.

Inwieweit sich die mit einem Blockchain-Use-Case verbundenen Ziele mit der Blockchain-Technologie realisieren lassen, hängt immer vom Einzelfall ab. Ist beispielsweise der Wertpapierhandel heute schon maximal automatisiert und maximal performant, wird eine Bank durch eine Blockchain-Anwendung für dieses konkrete Ziel keine weitere Verbesserung mehr erzielen.

Eigenschaften bestimmen und Komponenten ermitteln

In einem weiteren Schritt geht es darum einzugrenzen, was die Blockchain-Anwendung können soll und welche Blockchain-Komponenten wichtig für die Umsetzung sind. Die Frage ist, ob die Eigenschaften des Use Cases mit einer bestehenden Blockchain-Plattform abgebildet werden können.

Müssen für den konkreten Anwendungsfall Rollen und Rechte in Form von Geschäftsregeln (Business Rules) definiert werden, kommen nur Blockchain-Plattformen in Frage, die Smart Contracts unterstützen.

Als Nächstes ist zu verifizieren, welcher Consensus-Typ für den ausgewählten Use Case am besten passt. Die Consensus-Verfahren Proof of Work (PoW) und Proof of Stake (PoS) eignen sich sehr gut für Public Blockchains, in denen alle Teilnehmer größtenteils anonym sind. Bei diesen Verfahren ist die Sicherheit am höchsten, aber die mögliche Anzahl an Transaktionen pro Sekunde am geringsten. Zudem wird die Verwendung einer Kryptowährung vorausgesetzt. Das Consensus-Verfahren Practical Byzantine Fault Tolerance (PBFT) hat im Vergleich zu PoW/PoS eine geringere Sicherheit, dafür können mehr Transaktionen pro Sekunde erfolgen. Es eignet sich besonders für zugriffsbeschränkte Blockchains.

Sodann interessiert, ob der gewählte Use Case eine Kryptowährung notwendig macht. Nur weil eine Bezahlmethode erforderlich ist, muss nicht automatisch eine Kryptowährung eingesetzt werden. Der Bezahlvorgang in einem Use Case kann – wie auch bei Online-Shops – separat erfolgen. Schließlich gehen mit einer eigenen Kryptowährung auch Verpflichtungen einher, wie die

Bereitstellung eines Umrechnungskurses, die Limitierung der Kryptowährungseinheiten und der Umgang mit Betrugsfällen. Und nicht alle Blockchain-Plattformen unterstützen eine Kryptowährung.

Umsetzbarkeit prüfen

Nicht jeder Use Case, der mit einer Blockchain technisch oder theoretisch umsetzbar ist, kann auch wirklich implementiert werden. Daher gilt es, folgende Aspekte und damit verbundene Fragen zu bedenken:

- » **Recht:** Bestehen rechtliche Hürden? Verhindern strenge Haftungsregelungen eine Umsetzung, oder ist es erforderlich, Gesetze zu ändern oder zu erlassen?
- » **Organisation:** Muss für die Umsetzung des Business-Use-Cases die Organisation im Unternehmen verändert werden, und ist diese Änderung im Unternehmen überhaupt durchführbar? Werden spezielle Blockchain-Entwickler benötigt, und sind dafür Ressourcen vorhanden/ingeplant?
- » **Technik:** Erfüllt die technische Infrastruktur die notwendigen Anforderungen? Sind spezielle Programmiersprachen und Datenbanken vorhanden? Wie lässt sich die Blockchain-Anwendung in die heterogene Anwendungslandschaft integrieren?
- » **Finanzen:** Wie hoch sind die Entwicklungskosten und wie hoch die Betriebskosten für die Blockchain? Nur wenn die Blockchain-Lösung langfristig für Effizienzsteigerungen sorgt, amortisieren sich die Anfangsinvestitionen.
- » **Zeit:** Kann für die erfolgreiche Umsetzung einer Blockchain-Lösung eine kritische Masse an Teilnehmern zeitnah aktiviert werden? Eine Blockchain-Lösung wird nicht im Alleingang implementiert, sondern in der Regel durch eine Community gesteuert, weshalb die Umsetzung nicht nur viel Zeit kostet, sondern auch Absprachen zu neuen Funktionalitäten und die Koordination der Teilnehmer erforderlich macht.



Mustafa Cavus
ist Senior IT-Architect und
Technology Consultant bei
Sopra Steria Consulting.



Marcel Proffert
ist Consultant im Team
Digital Banking bei Sopra
Steria Consulting.

Von der Theorie zur Praxis

Ergibt die Analyse, dass für den ausgewählten Use Case die Blockchain die passende Technologie ist, folgt das konkrete Umsetzungsprojekt. Dafür sollte eine Governance aufgestellt werden, die Rollen und Verantwortlichkeiten in der Blockchain regelt und Lösungen für Konflikte enthält, die auf dem Weg zu einer Plattform auftreten können. «



TRANSPARENZ VERSUS DATENSCHUTZ

Ein zentrales Blockchain-Prinzip ist Kontrolle durch Transparenz. Alle Beteiligten eines offenen Netzwerks haben Einblick in eine Transaktion und segnen sie gemeinsam ab. Dieses Prinzip läuft in Teilen konträr zum Datenschutz. Dieses Dilemma lösen die Betreiber einzelner Blockchain-Plattformen auf ganz unterschiedliche Weise.

» Mit Hilfe der Blockchain-Technologie werden Transaktionen dezentral und fälschungssicher ausgeführt. Die Authentizität wird durch Transparenz gewährleistet, denn alle Teilnehmer eines Netzwerks (der Blockchain) haben Zugriff auf alle Transaktionen. Dieser sogenannte Konsensmechanismus gewährleistet auf der einen Seite die Validität von Transaktionen, stellt auf der anderen Seite jedoch ein Problem für den Datenschutz dar.

Wenn es auf den strengen Schutz von Daten und Anwendungen ankommt, eignet sich nicht jede Blockchain-Plattform gleichermaßen. Einige Plattformbetreiber haben deshalb geschlossene Bereiche

geschaffen, um derzeitige Anforderungen an den Datenschutz besser mit den Prinzipien der Blockchain zu vereinbaren.

Der unbestechliche Weltcomputer

Ethereum zählt zu den ersten Blockchain-Plattformen und bietet, anders als Bitcoin, nicht nur eine Kryptowährung, sondern auch eine Plattform, um Applikationen in Form von Smart Contracts auszuführen. Es lassen sich beispielsweise Verträge abbilden, validieren und abwickeln, wobei eine schriftliche Fixierung überflüssig wird.

Die Teilnehmer an den Netzwerken von Ethereum und Bitcoin sind pseudonym, müssen ihre wahre Identität also nicht preisgeben. Die Inhalte einer Transaktion und der Quellcode der Smart Contracts sind dennoch einsehbar. Vertrauliche Daten sind also bestenfalls mäßig geschützt und darüber hinaus für immer in das kollektive Gedächtnis eingebrannt. Da sich jeder Teilnehmer stets ein neues Pseudonym zulegen kann, muss niemand für seine Schulden und Verpflichtungen einstehen, was die Nutzbarkeit der Plattform aus Sicht eines Finanzunternehmens enorm einschränkt.

Zum Teil sollen diese Probleme und Einschränkungen durch Erweiterungen wie sogenannte Off-Chain-Channels, also private Kommunikationskanäle, behoben werden. Letztlich verfolgt Ethereum aber eigene Regeln – und das mit voller Absicht: Das Netzwerk will kein Medium für etablierte Strukturen sein, sondern ein Gegenentwurf zur bestehenden Finanzindustrie.

Hyperledger Fabric: Blockchains von und für Unternehmen

Hyperledger Fabric ist eine Blockchain-Lösung, die speziell für die Nutzung in Unternehmen entwickelt wurde. Es handelt sich um eine Applikation, um private, zugangsbeschränkte Netzwerke aufzubauen, die eine Prüfung der Teilnehmer erlauben. Für einzelne Unternehmen, Geschäftsbereiche oder andere Interessen können zugangsbeschränkte Netzwerke etabliert werden, in denen die Teilnehmer namentlich bekannt sind und dafür Berechtigungen erhalten (Level of Permission). Dies wird dem Datenschutz und regulatorischen Vorgaben gerecht. Zudem können private Kanäle für bestimmte Teilnehmer eines Netzwerks eingerichtet werden, so dass auch innerhalb eines zugangsbeschränkten Netzwerks weiter differenziert werden kann.

Im Gegensatz zu Bitcoin und Ethereum werden keine Pseudonyme genutzt, so dass den Teilnehmern einer Blockchain die Identitäten der anderen Teilnehmer bekannt sind. Allerdings haben die Teilnehmer keinen vollen Zugriff auf beziehungsweise keine volle Einsicht in die Aktivitäten der anderen Teilnehmer. Dass nicht jeder Teilnehmer alle Transaktionen kontrollieren kann und muss, hat einen guten Grund: die Skalierbarkeit. Bitcoin und Ethereum arbeiten bereits unter Vollast, und eine Erhöhung des Durchsatzes erfordert in beiden Netzwerken Anpassungen, die von den Communities kontrovers diskutiert werden.

Hyperledger bietet hier von vornherein Flexibilität, denn die Betreiber der Blockchain können selbst festlegen, welche Teilnehmer eine Transaktion verifizieren müssen. Je mehr Signaturen nötig sind, desto sicherer ist das Netzwerk gegen Manipulation, aber desto mehr Knoten sehen Informationen ein und müssen sie verarbeiten. Sind umgekehrt weniger Signaturen erforderlich, steigt der mögliche Durchsatz, und Daten sind einfacher geheim zu halten, aber auch weniger vertrauenswürdig. So wird Hyperledger verschiedenen Anforderungen gerecht, wenn auch nicht unbedingt allen gleichzeitig.

Corda: Distributed Ledger für Financial Services

Noch mehr Wert auf Geheimhaltung legt die Corda-Plattform, die vom R3-Konsortium entwickelt wurde. R3 wurde 2015 von namhaften Banken und Finanzinstituten gegründet und arbeitet mittlerweile mit über 80 Banken, Finanzinstituten, Regulatorien, technologieorientierten Unternehmen und weiteren Institutionen zusammen an der Corda-Plattform, die speziell auf Finanzservices ausgerichtet ist. Daten werden nur nach dem Need-to-know-Prinzip weitergegeben. Das bedeutet allerdings auch, dass es keine unbeteiligten Knoten mehr gibt, die Transaktionen prüfen können. Diese Aufgabe wird von sogenannten Notaren übernommen, das sind Netzwerkservices, die Transaktionen auf ihre Konformität mit den vereinbarten Regeln prüfen. Im Gegensatz zu Ethereum und Hyperledger besitzt also kein Teilnehmer eine vollständige Kopie der Blockchain.

Fazit

Der Vergleich von Ethereum, Hyperledger Fabric und Corda zeigt drei verschieden ausgeprägte Lösungen, die jeweils auf Basis ihrer Zielsetzung und Ausrichtung unterschiedliche Schwerpunkte setzen. Die öffentlichen Blockchains funktionieren durch ein gezieltes Zusammenwirken von Pseudonymität, Transparenz und Dezentralität, was sich mit Geschäftsbeziehungen zwischen Unternehmen kaum vereinbaren lässt. Der Schutz vertraulicher Daten (sowohl der eigenen als auch der der Kunden) ist kein Luxus, sondern eine Notwendigkeit – gerade im Finanzsektor und gerade in Deutschland. Um dem Datenschutz entgegenzukommen, entfernen sich Hyperledger und Corda von der ursprünglichen Funktionsweise; Corda bezeichnet sich selbst noch nicht einmal mehr als Blockchain.

Durch Anpassungen der ursprünglichen Blockchain-Funktionsweise können Unternehmen von der Dezentralität profitieren, die mit sensiblen Daten arbeiten. Und grundsätzlich ist eine nachverfolgbare Transaktionshistorie mit Blick auf aufsichtsrechtliche Vorgaben in manchen Bereichen sogar vorteilhaft. Generell gilt jedoch: Keine der Plattformen erfüllt von vornherein alle Datenschutzaufgaben automatisch. In der Anwendung muss genau geprüft werden, wie die jeweiligen Tools konfiguriert werden müssen, um sich im rechtlichen Rahmen zu bewegen.

Einzelne Blockchain-Plattformen unterscheiden sich teilweise sehr stark voneinander, weil die Technologie noch so jung ist. Das macht es umso wichtiger, eine Wahl zu treffen, die den wirtschaftlichen, technischen und Compliance-Anforderungen gerecht wird. «



Lena Pinkerneil
ist Junior Consultant bei
Sopra Steria Consulting.



Dr. Stefan Mehner
ist Junior Consultant bei
Sopra Steria Consulting.

DIE BLOCKCHAIN GIBT SICHERHEIT

Wie das Internet unsere Art zu kommunizieren verändert hat, wird auch die Blockchain viele Bereiche des Lebens verändern, ist Jörg von Minckwitz überzeugt. Der Gründer und CEO von Bitwala, einem Blockchain-Banking-Unternehmen, erwartet, dass vor allem die Sicherheit von Transaktionen steigt.

Herr von Minckwitz, was hat Sie dazu bewogen, Ihre unternehmerischen Tätigkeiten der Blockchain zu widmen?

Das erste Mal mit der Blockchain in Berührung gekommen bin ich bereits 2011. Das Potenzial für gesellschaftliche Veränderungen war für mich offensichtlich, aber nach Recherchen musste ich feststellen, dass es wenig Anwendungen für Blockchain und Bitcoin gab, vor allem in Deutschland und Europa. Aus diesem Grund haben wir eine Cryptocurrency Consultancy gegründet und waren damit recht schnell erfolgreich. 2012 war der erste Cryptocurrency-Hype, und wir haben damit begonnen, Anwendungsfälle in Deutschland aufzubauen, indem

wir Unternehmen, unter anderem eine erfolgreiche E-Commerce-Plattform, gegründet haben. Bitwala ist im Moment unser Hauptprojekt, unser Fokus liegt auf dem Zukunftsthema Blockchain Banking.

Gab es in der Gründungszeit Schwierigkeiten, weil Sie mit der Blockchain arbeiten?

Deutschland ist nicht unbedingt ein einfaches Land für Gründer. Es ist besonders schwierig, wenn man etwas gründet, was tendenziell auf Unverständnis oder mangelndes Wissen stößt. Bei Zukunftsthemen wie der Blockchain muss man Durchhaltevermögen an den Tag



legen. In den vergangenen fünf Jahren hat sich ein Markt entwickelt; das sieht man nicht zuletzt daran, dass Investoren ein steigendes Interesse an Blockchain-Start-ups haben.

Warum wird der Blockchain so viel Innovationspotenzial zugeschrieben?

Die Blockchain bietet durch die dezentrale Struktur mehr Sicherheit als ein zentraler Server, der im Vergleich leicht angreifbar ist. Über die Blockchain können Verträge in jedweder Form schnell, transparent und sicher abgewickelt werden.

Wie innovativ ist Deutschland im internationalen Vergleich in Bezug auf die Blockchain?

Allgemein sind die USA im Technologiemarkt zwar Deutschland voraus. Im Bereich Blockchain gilt dies allerdings nicht. Dadurch, dass die Blockchain, Bitcoin und Ethereum ihre Wurzeln in Berlin haben, nimmt Deutschland eine Vorreiterrolle ein. Berlin ist unser „Crypto Valley“. 80 Prozent der Initial Coin Offerings (ICOs) haben ihre Entwicklerteams in Berlin. Blockchain ist einer der wenigen Märkte, in denen Deutschland und Europa den USA weit voraus sind. Ich sehe hier eine große Chance, eine zukunftssträchtige Branche signifikant mitzuprägen.

Dennoch ist Bitcoin bisher als Zahlungsmittel, zumindest in Europa, wenig verbreitet. Warum?

Gerade in Deutschland ist Bitcoin nicht verbreitet, aber das gilt auch für Visa-Karten. Hierzulande zahlt man hauptsächlich mit Bargeld, deswegen ist die Implementierung neuer Technologien etwas schwieriger. Dieses Phänomen gab es bereits bei der Verbreitung des Internets: Nach dem Senden der ersten E-Mail hat es Jahrzehnte gedauert, bis Internetzugänge in Haushalten selbstverständlich waren. Allerdings ist es nicht zwingend notwendig, dass jedes Geschäft in Deutschland Bitcoin akzeptiert. Auch Bargeld ermöglicht im Alltag schnelle, effiziente Transaktionen. Aber im internationalen Zahlungsverkehr, bei kleineren Überweisungen oder der Überschreibung von Werten wird klar, wie langsam das bestehende System tatsächlich ist. Jede Bank hat eigene Standards und steht in Konkurrenz zu anderen. Die Lösung hier ist etwas Unabhängiges wie Bitcoin, auf das sich alle Akteure einigen können.

Sind etablierte Unternehmen schon bereit für Bitcoin und Blockchain? Welche Rolle spielen Start-ups?

Jedes große deutsche Unternehmen hat mittlerweile ein Blockchain Lab. Es gibt keinen in der Industrie, der nicht mit der Blockchain arbeitet, gerade in Bezug auf das Internet of Things, zum Beispiel im Bereich Mobile Payments zwischen Maschinen. Es gibt auch keine Bank, die

kein Blockchain Lab hat. Alle arbeiten an diesem Thema. Aber große Firmen sind eher langsam, auch im Entscheidungsprozess. Start-ups sind in dieser Hinsicht im Vorteil, da sie flexibel und beweglich sind. Aber klar ist, dass Gründen im Finanzbereich schwieriger ist. Deswegen sind Partner so wichtig. Es gibt beispielsweise Banken, die mit Start-ups kooperieren, um den regulatorischen Part zu übernehmen.

Wie gewährleistet man Sicherheit für die Nutzer bei Blockchain-basierten Anwendungen?

Die Entwicklung verläuft im Moment sehr schnell, und die Einstellung zur Blockchain und zu Kryptowährungen hat sich zuletzt sehr geändert: Was vorher als risikoreich galt, ist jetzt das große Zukunftsthema. Unseren Kunden erklären wir, welche Mechanismen genutzt werden müssen, um Sicherheit zu gewährleisten, aber letztendlich ist jeder Kunde eigenverantwortlich. Jeder hat die volle Kontrolle. Private Keys und Wallets werden auf den privaten Rechnern gespeichert – man agiert als eigene Bank. So ist beispielsweise gewährleistet, dass bei einer Pleite von Bitwala Kunden ihre Bitcoins nicht verlieren.

Wir befinden uns da in einem Spannungsfeld: Mainstream und erhöhte Usability versus Eigenverantwortung und volle Kontrolle des Kunden. In dem Moment, in dem wir unser Konzept benutzerfreundlicher gestalten, übernehmen wir auch mehr Verantwortung.

Ist die Blockchain tatsächlich so disruptiv, wie gesagt wird? Welche Veränderungen erwarten Sie?

Die Blockchain hat großes disruptives Potenzial – ich sehe die Blockchain als durchaus vergleichbar mit dem Internet an: Das Internet hat die Kommunikation grundlegend verändert – und die Blockchain hat das Potenzial, das Gleiche für Werte zu tun. Es wird sich alles ändern, was wir heutzutage kennen. Egal, ob wir über Verträge, Börsenhandel, Wechselkurse oder internationalen Handel sprechen. Die Blockchain wird fast jeden kleinen Teil der Gesellschaft erreichen, den das Internet noch nicht erreicht hat. Der Finanzbereich war der Erste. Als Nächstes sind Aktien dran, dann Vertragswerke. Durch die Blockchain werden Sicherheitslücken geschlossen, Serverangriffe quasi unmöglich – und auch deshalb steht dieser Veränderung nichts mehr im Wege. «

Das Interview führte Annika Scharbert.

“

Die Blockchain wird fast jeden Teil der Gesellschaft erreichen, den das Internet noch nicht erreicht hat.

”



Jörg von Minckwitz
ist Gründer und CEO
von Bitwala.



© Choreograph/Stock/Thinkstock/Getty Images

PILOTPROJEKTE IN DER FINANZINDUSTRIE

Die Finanzbranche wird oft als ein geeigneter Kandidat für den Einsatz der Blockchain-Technologie gehandelt. Denn grundsätzlich ermöglicht die Technologie, Werte sicher und effizient zwischen Teilnehmern zu transferieren. Aktuell existieren vor allem Pilotprojekte.

» 2008 – inmitten der Finanzkrise – entstand unter dem Begriff „Bitcoin“ die erste Kryptowährung, die seitdem eine ständig steigende Bekanntheit in der breiten Öffentlichkeit erreicht hat. Das eigentlich „Revolutionäre“ an Bitcoin ist allerdings nicht die Kryptowährung selbst, deren praktische Verwendung auch durchaus kritisch und skeptisch verfolgt wird. Es ist die technologische Basis – das Konzept der Blockchain.

Die verwendeten kryptographischen Verfahren machen es beim heutigen Stand der Technik de facto sehr schwer, eine Blockchain nachträglich zu manipulieren. Diese Sicherheit ist unter anderem eine Erklärung für die globale Ausbreitung von Bitcoin. Die Unabänderlichkeit von Daten ist eine unverzichtbare Voraussetzung, um genügend Vertrauen aller Anwender in diese Art der dezentralen Buchführung sicherzustellen.

Die Blockchain verspricht eine Reihe weiterer Vorteile: Transaktionen könnten schnell (in Minuten) und kosten-

günstig abgewickelt werden – und zwar vollständig standortunabhängig. Zudem ermöglicht die Blockchain scheinbar, Werte jeglicher Art schnell und sicher zu übertragen. Die Vision des „Internet of Values“ scheint sich zu materialisieren, ohne zentrale Intermediäre und zum Vorteil vieler.

Es drängt sich daher die Frage auf, warum sich fast zehn Jahre nach der Entstehung von Bitcoin die Blockchain-Technologie (noch) nicht großflächig ausgebreitet hat und kaum bedeutende Anwendungen darauf basieren. Einfache Antworten gibt es sicher nicht, und die Begründungen werden abhängig vom Anwendungsbereich vermutlich sehr unterschiedlich ausfallen.

Für den Bereich der Finanzmärkte ist es zunächst hilfreich, sich vor Augen zu führen, dass diese hochgradig reguliert sind – und die Regulierung hat sich in den vergangenen Jahren als Folge der Finanzkrise nochmals deutlich erhöht. Dadurch kollidieren aber manche Eigen-

schaften der Blockchain mit bestehenden Vorschriften. So steht etwa ein einfacher und freier Zugang zu Finanzprodukten, bei dem der Teilnehmer anonym bleibt, im diametralen Gegensatz zu deutlich gestiegenen Transparenzanforderungen (zum Beispiel beim Thema Steuern, dem Know-your-Customer-Prinzip oder bei Compliance-Aspekten).

Wie lassen sich die potenziellen Vorteile der Blockchain nutzen, ohne den gültigen regulatorischen Rahmen zu verlassen? Es erfordert zunächst, dass im Gegensatz zu Lösungen im freien Internet mögliche Anwendungsfälle sehr detailliert analysiert und vorab klar geregelte Rollen und Verfahren definiert werden müssen. Stichworte sind hier etwa die Zulassungsregeln (Wer darf wie teilnehmen?), die rechtliche Verbindlichkeit (Wer hat welche Ansprüche?) und die Einhaltung von gesetzlichen und regulatorischen Pflichten (Was muss erfüllt werden?).

Für einen Marktinfrastrukturanbieter wie die Deutsche Börse ist die fortlaufende Auseinandersetzung mit technischen Neuerungen eine unabdingbare strategische Notwendigkeit – und das gilt auch für das Thema Blockchain. Seit annähernd zwei Jahren beschäftigt sich ein eigenes Team mit der Analyse, wo die Blockchain sinnvoll eingesetzt werden kann, und hat erste Prototypen für identifizierte Anwendungsfälle entwickelt.

Aufgrund der starken regulatorischen Einbettung, die die Deutsche Börse beispielsweise von Fintech-Unternehmen deutlich unterscheidet, kennen die Mitarbeiter die existierenden Regelwerke sehr gut und können dieses Know-how bei der Entwicklung solcher Anwendungen zielgerichtet einbringen. Grundsätzlich gilt: Die Deutsche Börse setzt derzeit auf sogenannte Permissioned-Blockchain-Lösungen. Das bedeutet, Zugang wird nur autorisierten Teilnehmern gewährt, die in vordefinierten Rollen agieren.

Aktuell arbeitet die Deutsche Börse an drei konkreten Blockchain-Projekten:

Blockchain-Projekt mit der Deutschen Bundesbank

Gemeinsam mit der Deutschen Bundesbank hat die Deutsche Börse im November 2016 eine Konzeptstudie und einen Prototyp für den Transfer von „digitalen Wertpapieren“ und „digitalen Coins“ vorgestellt, die von zentralen Identitäten erzeugt werden. Gegenwärtig setzt sich das Projekt mit Themen wie Skalierbarkeit und Vergleichbarkeit mit etablierten Verfahren/Systemen auseinander. Die Deutsche Börse ist damit weltweit der erste Finanzmarktinfrastrukturanbieter, der gemeinsam mit einer Zentralbank ein Blockchain-Modell erprobt.

Geschäftlicher Zahlungsverkehr mittels Blockchain

Das Projekt beschäftigt sich mit einem Modell für die risikolose Peer-to-Peer-Übertragung von Geschäftsbankgeld über eine Blockchain-basierte Infrastruktur, die die Funktionalitäten eines zentralen Kontrahenten (CCP) nutzt. Die „Collateralised Colored Coin“-Infrastruktur, kurz „CollCo“, ist ein Instrument zur Durchführung von Zahlungen auf der Blockchain, deren Erfüllung durch ein Clearinghaus sichergestellt wird. Dies reduziert Kreditrisiken deutlich, da die Transaktionen beim Clearinghaus besichert werden. Jeder Teilnehmer kann dabei einen eigenen „Coin“ in Form sogenannter Tokens ausgeben.

“

Die Unabänderlichkeit von Daten ist unverzichtbare Voraussetzung, um genügend Vertrauen aller Anwender in diese Art der dezentralen Buchführung sicherzustellen.

”

Liquidity Alliance – internationaler Transfer von Sicherheiten

Zusammen mit den Zentralverwahrern aus Kanada, Luxemburg, Norwegen und Südafrika hat die Deutsche Börse eine globale Initiative, die Liquidity Alliance Ledger (LA Ledger), in Angriff genommen, die die grenzüberschreitende Bereitstellung von Wertpapiersicherheiten deutlich schneller und einfacher machen würde. Ein Prototyp ist seit Mai 2017 fertiggestellt und wird seither mit den nationalen Aufsichtsbehörden aller Partner im Detail evaluiert. Positiv hierbei ist, dass das LA-Ledger-Projekt im Rahmen von

CPMI-IOSCO, dem globalen Gremium der Zentralbanken und Regulatoren, als Anwendungsfall betrachtet wird. Die in diesen aufsichtsrechtlich ausgerichteten Diskussionen gewonnenen Erkenntnisse sind unverzichtbar für die gegenwärtig stattfindenden Kundenkonsultationen. Ziel ist es, mit Hilfe des Prototyps bis Ende 2017 ein implementierungsfähiges Konzept zu entwickeln, um bei positiver Resonanz eine schrittweise Einführung in Kooperation mit den internationalen Partnern der Deutschen Börse voranzutreiben.

Ausblick

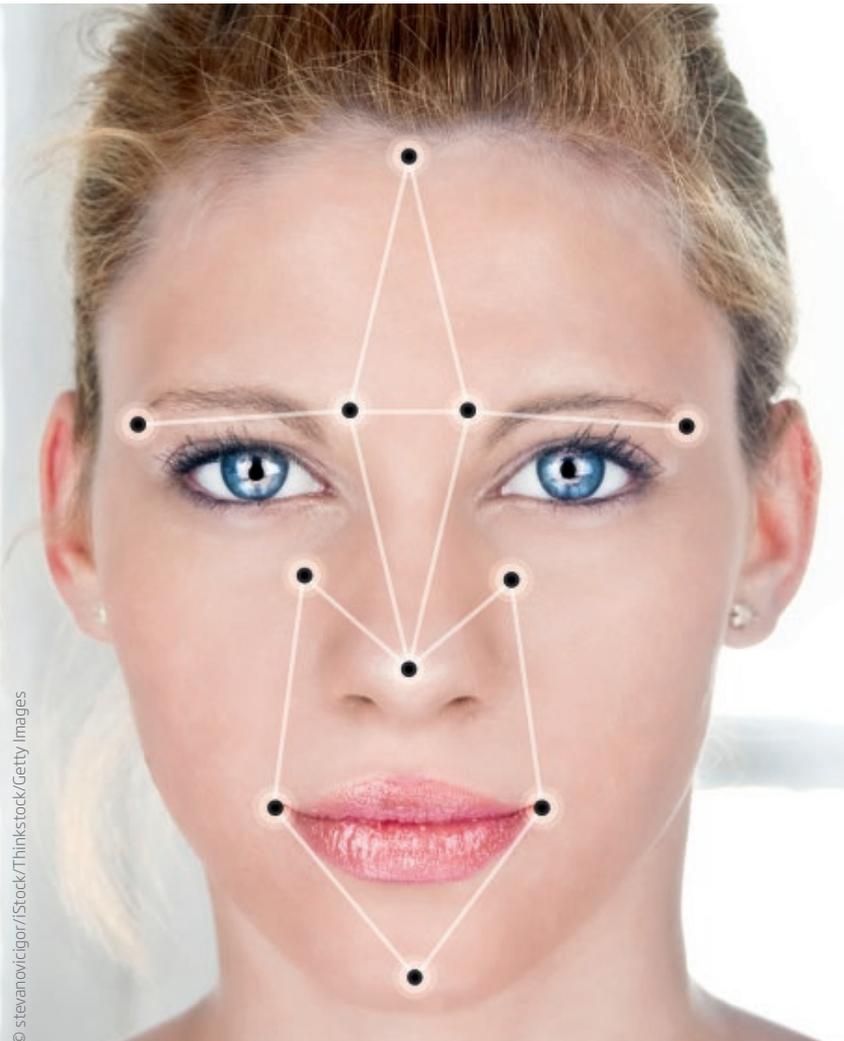
Zusammengefasst: Aufgrund unbestreitbarer Vorteile kann sich die Blockchain langfristig auch im Finanzsektor durchsetzen, wenn die unabdingbare technologische Standardisierung erfolgreich vorangetrieben wird. Die konkrete Umsetzung bedarf darüber hinaus jeweils der angemessenen Einbettung in die bestehende und sich ständig weiterentwickelnde Regulierung. Dies wird nicht schlagartig, sondern eher evolutionär erfolgen. Als Marktinfrastrukturanbieter verfügt die Deutsche Börse über eine hohe regulatorische Kompetenz, diesen Gesamtprozess entscheidend mitzugestalten. «



Gerd Hartung
ist Senior Vice President im Bereich Strategic Execution bei der Deutschen Börse AG.

KONTOERÖFFNUNG PER GESICHTS- ERKENNUNG

Wer Konten bei mehreren Banken unterhält, muss sich gegenüber jeder Bank aufs Neue identifizieren. Mittels Blockchain kann das auch anders gehen. Erste Prototypen werden entwickelt.



» Kreditinstitute sind dazu verpflichtet, vor der Begründung einer Geschäftsbeziehung ihren potenziellen Vertragspartner zu überprüfen. Die Aufnahme und Verifizierung von Personen- und Geschäftsdaten stellt den ersten kritischen Schritt innerhalb des sogenannten Know-your-Customer-Verfahrens dar. Dieses risikobasierte Verfahren dient der Prävention von Geldwäsche und Terrorismusfinanzierung.

In der Praxis werden Daten, die Kreditinstitut A bereits aufgenommen und verifiziert hat, von Kreditinstitut B wiederholt aufgenommen und verifiziert. Dieser Aufwand lässt sich vermeiden.

Vision

Mit Hilfe von einheitlichen Anlaufstellen kann ein standardisierter Identifizierungsprozess von Personen- und Geschäftsdaten etabliert werden. Dabei verlagern sich die Datenaufnahme und die Verifizierung von den verpflichteten Unternehmen zu sogenannten Trusted Parties. Dies können zum Beispiel Behörden sein, die die Authentizität von Identitäten sicherstellen.

Im Zuge der Standardisierung und Verlagerung des Identifizierungsprozesses genügt es zukünftig, den Prozess zur Aufnahme und Verifizierung von Personen- und Geschäftsdaten nur einmal zu durchlaufen. Anschließend kann der Kunde seine beglaubigten Daten an verpflichtete Unternehmen selbstbestimmt übermitteln. Dies hat Vorteile für alle Beteiligten: Der Zeitaufwand zur Erfassung von Identitäten sinkt erheblich, und die verpflichteten Unternehmen können sich stärker auf ihr Kerngeschäft konzentrieren.

FALLBEISPIEL KONTOERÖFFNUNG

- 1 Im ersten Schritt erfasst eine Kamera die Gesichter der anwesenden Personen und hält hinterlegte Informationen bereit.
- 2 Anschließend bestätigt der Kunde seine Identität mit seinem Token (z.B. Fingerabdruck) und genehmigt den Zugang zu seinen Daten.
- 3 Im dritten und letzten Schritt erhält der Bankangestellte die für den Vorgang relevanten Identitätsdaten aus der Blockchain.



© neyro2008/iStock/Thinkstock/Getty Images

Technischer Lösungsansatz

Kernanforderung dieser Vision ist ein hochverfügbarer und integrier Datenbestand von digitalen Assets, der vor Datenmanipulation und unautorisierten Zugriffen geschützt ist. Außerdem sollen alle Interaktionen chronologisch abgespeichert werden, so dass sie auch zu einem späteren Zeitpunkt einsehbar sind. Zusätzlich sollen der Zugriff und die Freigabe der Personen- und Geschäftsdaten durch eine biometrische Authentifizierung der Kunden erfolgen.

Um diesen Kernanforderungen gerecht zu werden, erfolgt die technische Umsetzung anhand einer prototypischen Implementierung mit einer Blockchain-Lösung. Dabei bilden die Trusted Parties ein Konsortium, das ausschließlich das Recht der Blockerzeugung innehat, um einen geregelten Schreibzugriff innerhalb der Blockchain sicherzustellen.

Nachdem eine Trusted Party Identitätsdaten aufgenommen und verifiziert hat, werden diese gespeichert, signiert und verschlüsselt. Durch die Signatur und die Verschlüsselung lässt sich jederzeit nachvollziehen, wer

der Ersteller einer Identität ist und welche nachfolgenden Änderungen es gegeben hat. Damit ist die Authentizität der Identität jederzeit überprüfbar.

Die verschlüsselten Identitätsdaten werden in einem für den Kunden erzeugten Smart Contract festgehalten. So kann ausschließlich der Kunde als Besitzer dieses Smart Contracts seine Daten einsehen, löschen und an von ihm ausgewählte Unternehmen freigeben. Die Interaktion von Kunden, verpflichteten Unternehmen und Trusted Parties wird chronologisch und nachvollziehbar abgespeichert.

Neben der Blockchain-Technologie sollen technische Komponenten in den zu erstellenden Prototyp integriert werden, um biometrische Merkmale zu erfassen und eine für den Kunden einfache und sichere Authentifizierungsmethode zu ermöglichen. Damit kann sich der Kunde sowohl innerhalb der Räumlichkeiten von verpflichteten Unternehmen als auch ganz bequem von Zuhause aus über die eigene Webcam identifizieren. «



Mustafa Cavus
ist Senior IT-Architect und
Technology Consultant bei
Sopra Steria Consulting.



Tobias Lange
ist Werkstudent bei
Sopra Steria Consulting.

“
*Der Kunde ist Besitzer des Smart Contracts
und kann seine Daten einsehen, löschen und
für andere freigeben.*
”



DANK BLOCKCHAIN MIT STROM VERSORGT

Im Energie- und Versorgungsmarkt machen Blockchain-basierte Smart Contracts nicht nur Abrechnungsprozesse und Dokumentationen leichter. Auch dezentrale Stromnetze und Initiativen lassen sich organisieren.

» Smart Contracts auf Basis der Blockchain-Technologie haben für die Energie- und Versorgungswirtschaft großes Potenzial. Mit Smart Contracts lassen sich Verträge teilweise oder vollständig automatisiert abwickeln. So lässt sich die Blockchain-Technologie für Ables- und Abrechnungsprozesse sowie für das Clearing einsetzen. Auch die Dokumentation von Eigentumsverhältnissen, Anlagenzuständen (Asset Management), Herkunftsnachweisen, CO₂- und Ökostromzertifikaten kann effizienter erfolgen.

Vom zentralen Netz zur dezentralen Verteilung

Momentan wird zentral erzeugte Energie über das Verteilnetz der Energieversorgungsunternehmen an industrielle und private Nutzer geliefert. Händler kaufen und verkaufen Energie an Börsen, Banken fungieren als Zahlungsdienstleister, über die die Transaktionen der beteiligten Akteure abgewickelt werden.

Steuert man den Prozess über eine Blockchain, werden diese Intermediäre überflüssig. Es entsteht ein dezentral gesteuertes Transaktions- und Energieliefersystem. Dezentral erzeugte Energie wird über kleinere Netze (sogenannte Microgrids) zum Endverbraucher transportiert. Intelligente Messsysteme messen erzeugte und verbrauchte Energie, der Energiehandel und die Bezahlung mit einer Kryptowährung erfolgen über die Blockchain – automatisch gesteuert mittels Smart Contracts. So erhält der Verbraucher über die Blockchain und darauf aufgesetzte Smart Contracts die Entscheidungsgewalt über Stromlieferverträge und Verbrauchsdaten.

Lokales Microgrid

Im New Yorker Stadtteil Brooklyn entsteht zurzeit ein Peer-to-Peer(P2P)-Netz für lokal erzeugte erneuerbare Energien. Installiert wird das Brooklyn Microgrid von der Siemens-Tochter Siemens Digital Grid. Neben Network-Control-Systemen, Konvertern und Smart Metern gehö-

GESCHÄFTSMODELL DES BROOKLYN MICROGRIDS

In Anlehnung an Business Model Canvas

Schlüsselpartner <ul style="list-style-type: none"> » Start-up-Förderer next47 von Siemens » enger Kontakt zu regulatorischen Gremien und Behörden » nichtspezifizierte Partnerschaften mit Energieversorgern 	Hauptaktivitäten <ul style="list-style-type: none"> » Kommunikation mit Behörden und Kommunen 	Leistungsversprechen <ul style="list-style-type: none"> » P2P-Handel in einem Microgrid » skalierbares Netzwerk » Sicherheit gegen Cyber-Attacken und Umweltkatastrophen » höhere Einspeiserträge für Prosumer » Angebot lokaler grüner Energie 	Kundenbeziehungen <ul style="list-style-type: none"> » intensive Kommunikation in der Gemeinschaft 	Kundensegmente <ul style="list-style-type: none"> » LOHAS (Lifestyles of Health and Sustainability) » Prosumer » auf Sicherheit fokussierte Kunden
Kostenstruktur <ul style="list-style-type: none"> » hauptsächlich Personalkosten 		Einnahmestruktur <ul style="list-style-type: none"> » Transaktionsgebühr im Direktvertrieb » Dienstleister für Energieversorger 		
Blockchain <ul style="list-style-type: none"> » private Blockchain auf Basis der Ethereum Virtual Machine erlaubt hohes Transaktionsvolumen » Privatsphäre durch Exklusivität der Informationen gegeben 				

Quelle: Nicolai Hecht, Bachelorthesis „Die Energy Chain – Blockchain-Geschäftsmodelle im deutschen Strommarkt“

ren zu dem Versorgungssystem auch Lithium-Ionen-Akkus, die auch bei größeren Stromausfällen die Versorgung gewährleisten sollen.

Im Jahr 2016 wurde hier die weltweit erste Energiehandelstransaktion über eine Blockchain abgewickelt: Der über Solarzellen auf dem Dach eines Hauses erzeugte, überflüssige Strom wurde über einen Smart Contract (Ethereum Blockchain) an Nachbarn verkauft, die keine eigene Solaranlage besitzen. Begleitet wurde der Verkauf durch das Start-up LO3 Energy, das 2012 in New York gegründet wurde und als Pionier von Blockchain-Anwendungen im Strommarkt gilt.

Für das Projekt hat LO3 Energy die energiemarktspezifische Blockchain-Plattform „TransActive Grid“ entwickelt, die den P2P-Handel in einem physisch verbundenen Microgrid ermöglicht. Teilnehmer können Strom, den sie

selbst nicht verbrauchen, direkt an ihre Nachbarn verkaufen. Die Transaktionsdaten stehen dabei ausschließlich den beiden Parteien zur Verfügung. Damit ermöglicht die Technologie den Lastenausgleich von lokaler Produktion und lokalem Verbrauch.

Praktisch kommt aus den Steckdosen der Microgrid-Haushalte ohne eigene Solaranlagen zwar weiterhin Strom aus dem nächstgelegenen Kraftwerk. Das Prinzip ist ähnlich wie bei Stromkunden, die einen Ökostromtarif bei ihrem Energieversorger buchen und diesen somit dafür bezahlen, Strom aus erneuerbaren Energiequellen entsprechend ihrem Verbrauch ins Netz einzuspeisen. Die Teilnehmer am Brooklyn Microgrid überweisen ihr Geld für den ins Netz einfließenden Solarstrom allerdings nicht an den Stromversorger, sondern direkt an ihre Nachbarn. Bis 2018 sollen 1.000 Teilnehmer dem Microgrid angehören.

GESCHÄFTSMODELL VON SHARE&CHARGE

In Anlehnung an Business Model Canvas

Schlüsselpartner <ul style="list-style-type: none"> » Innogy SE und RWE AG » E-Mobility-Start-up Wallbe » Ladestationenhersteller EBG Compleo 	Hauptaktivitäten <ul style="list-style-type: none"> » Aufbau eines flächendeckenden Netzwerks » Weiterentwicklung der Ethereum Chain Schlüsselressourcen <ul style="list-style-type: none"> » bestehendes Ladestationennetzwerk » App » Blockchain-Know-how 	Leistungsversprechen <ul style="list-style-type: none"> » transparentes und verlässliches Protokoll für Mietstrommodelle » Beseitigung von Customer Pain Points » Effizienzgewinn 	Kundenbeziehungen <ul style="list-style-type: none"> » weitestgehend autonome Kunden (Customer Enablement) Kanäle <ul style="list-style-type: none"> » App » Messen und Veranstaltungen 	Kundensegmente <ul style="list-style-type: none"> » private Besitzer von Ladestationen » gewerbliche Betreiber von Ladestationen » Besitzer von Elektroautos
Kostenstruktur <ul style="list-style-type: none"> » Hardware- und Installationskosten » Service- und Instandhaltungskosten 		Einnahmestruktur <ul style="list-style-type: none"> » Transaktionsgebühr (15%) » für Endkunden Flatrate sowie zeit- und quantitätsbasierte Tarife möglich 		
Blockchain <ul style="list-style-type: none"> » Public Ethereum Chain ermöglicht Nutzung positiver Netzwerkeffekte » Risiko der begrenzten Skalierbarkeit; kein exponentielles Wachstum möglich » Privatsphäre von sicherer Verwahrung des Private Keys abhängig 				

© AdventurePicture/iStock/Thinkstock/Getty Images

Quelle: Nicolai Hecht, Bachelorthesis „Die Energy Chain – Blockchain-Geschäftsmodelle im deutschen Strommarkt“

“

Durch Blockchain-Technologie werden Zwischenhändler (fast) überflüssig, und Transaktionskosten sinken.

Privates Netzwerk für Ladestationen

Auf dem deutschen Markt haben sich RWE und das aus dem sächsischen Mittweida stammende Start-up Slock IT zusammengetan, um Zahlverfahren für das Laden von Elektrofahrzeugen auf Basis einer Blockchain-Technologie zu etablieren. RWE stellt die Ladesäulen zur Verfügung, Slock IT hat die App entwickelt. Zu dem Netzwerk „Share&Charge“ gehörten Mitte August 2017 deutschlandweit knapp 1.200 Ladestationen für Elektroautos. Über die Ladestationen von RWE erreicht das Projekt die notwendige Relevanzschwelle. Besitzer/Anbieter von Ladestationen können sich dem Netzwerk anschließen und ihre Stromtankstellen mit anderen teilen. Wer seine eigene Ladestation beispielsweise nur nachts nutzt, kann tagsüber zusätzliche Einnahmen generieren. Die Tarife an den Ladestationen bestimmen die Anbieter selbst.

Für die Abwicklung hat Slock IT eine Smartphone App entwickelt, die auf der Blockchain-Technologie basiert. Die Anmeldung zum Netzwerk, Informationen über verfügbare Ladestationen, das Festsetzen des Tarifs, die Einbindung eines Zahlungsdienstleisters sowie die gesamte Abwicklung erfolgen über die App. Durch den Einsatz der Blockchain-Technologie können Transaktionen mit geringeren Gebühren ausgeführt werden. Nutzer (Lader) und Anbieter der Ladestationen verfügen über ein „Share&Charge“-Konto, das per Kreditkarte, Paypal oder Sofortüberweisung aufgeladen wird und über das Transaktionen abgewickelt werden.

Fazit: Chancen und Risiken der Blockchain im Energiesektor

Einer der grundlegenden Vorteile der Blockchain-Technologie bei Anwendungen im Energiemarkt ist, dass Zwischenhändler (fast) entfallen und Transaktionskosten sinken. Für den Zahlungsverkehr fallen keine Bankgebühren an, Betriebskosten für die Ablesung oder Abrechnung entstehen nicht oder nur in geringem Maß. Mahn- oder Inkassoverfahren entfallen. Zudem erlauben eine bessere Netzsteuerung sowie der Einsatz von Smart Meter und Smart Contracts eine höhere Flexibilität mit Blick auf den Energieverbrauch und -verkauf.

Die Risiken für Blockchain-Geschäftsmodelle (nicht nur im Energiemarkt) liegen vor allem darin, dass sie die aktuellen regulatorischen Anforderungen erfüllen müs-

”

sen. Der Nutzen der dezentralen P2P-Beziehungen geht damit zum Teil verloren. Da es sich bei der Blockchain um eine neue Technologie handelt, sind noch keine Langzeiterfahrungen vorhanden. Zudem fehlt Blockchain-basierten Systemen noch die rechtliche Anerkennung. Die Kernphilosophie besteht in diesen Systemen in der „Intelligenz des Schwarms“. Aktuelle Rechtssysteme

sind jedoch darauf ausgelegt, dass organisatorische und rechtliche Verantwortungen klar definiert sind. Der Mangel an Erfahrungen und das Problem der rechtlichen Anerkennung dürften entscheidend dafür sein, dass es der Blockchain-Technologie noch an einer breiten Akzeptanz seitens der Verbraucher fehlt.

Ausblick

Mit Blick auf den Energiemarkt hat die Blockchain jedoch das Potenzial, die Wettbewerbssituation erheblich zu beeinflussen – positiv wie negativ. Beispielsweise könnten etablierte Energieversorger private Blockchains entwickeln und so kleineren Anbietern den Zugang zum Transaktionsmodell beziehungsweise zum Markt verwehren.

Ein vollständig dezentral organisiertes Stromnetz ist aus heutiger Sicht kein realistisches Szenario – und mit Blick auf die Versorgungssicherheit wohl auch nicht erstrebenswert. Selbst Scott Kessler von LO3 Energy schränkt ein: „There is a reason we have sort of regulated monopolies in electric utilities. It’s a critical resource for people and so it’s not really a sector that I think is going to go to the totally crypto-anarchist mindset where we have no government and no regulation whatsoever.“ Einzelne Untersuchungen zeigen, dass eine autarke Stromversorgung in städtischen Siedlungsstrukturen unmöglich und auch in ländlichen Regionen nur unter günstigen Bedingungen realisierbar ist.

Vorteile bieten sich jedoch mit Blick auf die Netzstabilität. Projekte wie NRG Coin beinhalten erste Ansätze, durch eine entsprechende Programmierung des Smart Contracts zur Netzstabilität beizutragen. «



Sascha Krauskopf
ist Senior Manager Utilities bei Sopra Steria Consulting.

IDENTITÄTSMANAGEMENT LEICHTGEMACHT

Seit dem Jahr 2012 tragen alle Teilnehmer am Finanzmarkt einen Legal Entity Identifier (LEI). Mit dieser Rechtsträgerkennung steht ein globaler und eindeutiger Identifikator zur Verfügung. Mit der Blockchain-Technologie lassen sich die Zertifikate verwalten.

» Allen Blockchain-Ansätzen ist gemein, dass Benutzer – das können natürliche Personen, aber auch Avatare und Algorithmen sein – sich gegenüber der Technik ausweisen müssen. Das kann anonym erfolgen oder auch mit einer Identifizierung der Person oder Organisation. Dazu werden im Allgemeinen Identitäten mittels Private/Public Key Pairs erzeugt. Der Besitzer des privaten Schlüssels kann Transaktionen signieren und durchführen. Für bestimmte Anwendungsfälle

kann es sein, dass man Nutzungsrechte weiter einschränken möchte. Beispielsweise könnte man es einer Gruppe erlauben, Transaktionen durchzuführen, während andere nur lesenden Zugriff auf die Transaktionsdaten haben – auch Permissioned DLT genannt. Auf diese Weise kann man sehr spezifische verteilte Anwendungen bauen, die entweder in öffentlichen Netzen wie dem Internet oder in abgeschirmten privaten Netzen laufen.

Aus diesen Schilderungen wird bereits ein grundsätzliches Problem erkennbar: Werden wir in Zukunft für jede DLT-Anwendung eigene Schlüssel und damit Identitäten erhalten, oder wird sich ein Standard etablieren, sozusagen ein Generalschlüssel? Diese Frage ist derzeit nicht beantwortet. Viele Organisationen und Firmen wetteifern darum, die erste beziehungsweise beste Lösung dafür zu entwickeln.

Die Frage dabei ist, ob man nicht auf bekannte und etablierte Verfahren zurückgreifen kann. Beispielsweise gibt es einen allgemein akzeptierten und sicheren Standard für die Erzeugung und Verwaltung von Private/Public Key Pairs, den Standard ITU X.509/ISO-IEC 9594 für digitale Zertifikate. In vielen Ländern liegt dieser Standard den jeweiligen Signaturgesetzen zugrunde, wie etwa der eIDAS-Verordnung der Europäischen Union. So könnte man fordern, dass nichtanonyme DLT-Anwendungen Zertifikate als Authentifikationsmethode benutzen müssen. Das würde sicherstellen, dass die eigene Identität plattform- und anwendungsübergreifend anwendbar würde. (Zum Vergleich: Warum haben wir eigentlich unterschiedliche Kundennummern bei jeder Firma, mit der wir etwas vereinbaren oder kaufen? Wäre es nicht eine erhebliche Erleichterung, wenn man stattdessen überall eine einheitliche Identitätskennung nutzen könnte?)

Codes in der Finanzbranche vergeben

Ein solches Identitätsmanagement gibt es global mit dem Legal Entity Identifier (LEI). Nach dem Zusammenbruch der Lehman Bank 2008 war schnell klar, dass ein weltweites Unternehmensregister fehlte, das zentral Informationen zu den handelnden Akteuren im Finanzmarkt bereithielt und aufzeigte, wer alles von der Pleite betroffen sein würde. Aus diesem Grund wurden 2012 die LEI aus der Taufe gehoben. Jeder Teilnehmer am Finanzmarkt, wie zum Beispiel Banken, Broker, Fonds, Wertpapier- und Rohstoffhändler, kann über den ihm zugewiesenen LEI eindeutig identifiziert werden und muss auch den LEI seiner Vertragspartner kennen und im regulatorischen Meldewesen nutzen.

Der LEI ist ein 20-stelliger, alphanumerischer Code, der auf der von der Internationalen Organisation für Normung (ISO) entwickelten ISO-Norm 17442 basiert. Er ist mit wesentlichen Referenzdaten verknüpft, die eine klare und eindeutige Identifikation der Rechtsträger, die an Finanztransaktionen beteiligt sind, ermöglichen. Die Ausgabe und die Überprüfung der Richtigkeit der Daten der Rechtsträger erfolgen durch LEI-Vergabestellen. Die Akkreditierung dieser Vergabestellen, die untereinander im Wett-

bewerb stehen, sowie die jährliche Compliance-Prüfung erfolgen durch die Global Legal Entity Identifier Foundation (GLEIF) mit Sitz in der Schweiz. Diese steht unter der Aufsicht von 71 internationalen Regulierungsbehörden, die sich im Auftrag des Financial Stability Boards im Regulatory Oversight Committee (LEI ROC) zusammengefunden haben.

Der so entstandene und weiter anwachsende öffentlich zugängliche LEI-Datenpool lässt sich, vereinfacht ausgedrückt, als ein globales Verzeichnis von überwiegend juristischen Personen sehen, das die Transparenz auf dem globalen Markt-

“

Die Transparenz erlaubt einfachere, billigere und bessere Entscheidungen, mit wem man Geschäfte tätigen möchte.

”

platz stark verbessert. Jede Unternehmung kann ihren eigenen LEI für eine lebenslange Nutzung erhalten, während alle anderen sich kosten- und IP-Rechtfrei auf diesen globalen Datenschatz verlassen können. So entsteht ein globaler Index aller Rechtsträger, auf den jeder frei zugreifen kann.

Während der LEI garantiert einzigartig ist und (unternehmens-)lebenslang gültig bleibt, ist das bei digitalen Identitäten nicht so. Diese laufen nach festen Regeln aus und müssen durch neue ersetzt werden. Außerdem sind sie nicht einzigartig. Jeder Rechtskörper und sogar jede Person kann beliebig viele Zertifikate gleichzeitig führen. Und natürlich ändert sich jedes Mal der öffentliche Schlüssel. Für eine lückenlose Verfolgung von Transaktionen ist das wenig geeignet, und in der Tat stehen bis heute keine Management-Tools zur Verfügung, die einen globalen Überblick gewähren würden.

Und genau hier greift das LEI-Konzept: Wenn man als ein zusätzliches Datenattribut in Zertifikaten den LEI hinzufügt, hat man diese Transparenz, die einfachere, billigere und bessere Entschei-

dungen darüber erlaubt, mit wem man Geschäfte tätigen möchte. So wurde folgerichtig ein XML-Tag für den LEI in der Spezifikation von eIDAS vorgesehen. Technisch ist man damit zukunftssicher gerüstet. Jetzt geht es im nächsten Schritt um die Massenanwendung.

Identitäten über die Blockchain verwalten

Was hat das aber mit DLT beziehungsweise Blockchain zu tun? Einerseits sind – wie bereits ausgeführt – Zertifikate mit eingebautem LEI ideal für DLT-Anwendungen geeignet. Man erfindet nicht das Rad neu, sondern setzt auf moderne Standards zur Authentifizierung. Andererseits kommt aber unweigerlich die Frage auf, ob DLT eine geeignete Technik ist, um den LEI selbst zu erzeugen, zu verwalten und zu verteilen. Da es sich um eine Problematik handelt, bei der sehr viele LEI-Besitzer und noch mehr LEI-Benutzer weltweit immer auf den neuesten Stand zugreifen möchten, bietet sich DLT dann an, wenn man die Alternative eines zentral betriebenen Gateways scheut. Neben vielen technischen Fragen gilt es dabei, das Geschäftsmodell genauer zu untersuchen. Wer bezahlt eigentlich den Betrieb? Wer hat den Nutzen der Anwendungen? Wie wird Qualitätssicherung vorgenommen? Und wie kann das mit behördlichen Auflagen in Einklang gebracht werden?

Diese Fragen scheinen gewichtig genug, um sie in einem Pilotprojekt einmal eingehend zu untersuchen. Die GLEIF wird dazu in Kürze eine Dokumentation veröffentlichten und einen Request for Information starten. Man darf gespannt auf die Ergebnisse sein. «

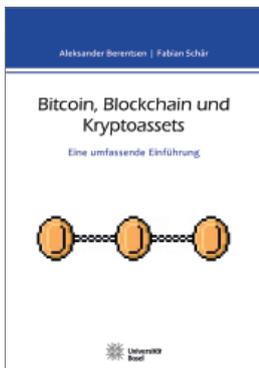


Stephan Wolf

ist CEO der Global Legal Entity Identifier Foundation (GLEIF) und Co-Convenor der FinTech Advisory Group für die International Organization for Standardization (ISO).

BUCH & WEB

FACHLITERATUR



Aleksander Berentsen und Fabian Schär:

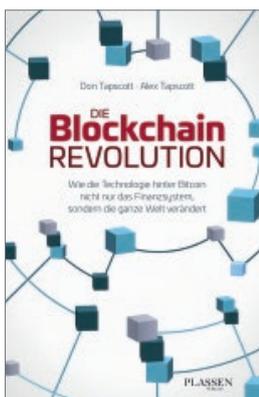
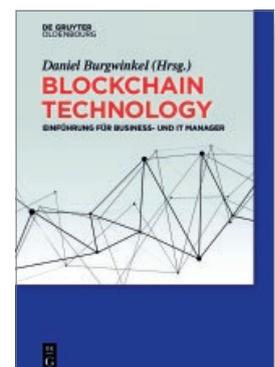
Bitcoin, Blockchain und Kryptoassets. Eine umfassende Einführung.
Books on Demand 2017

Die Blockchain-Experten der Universität Basel bieten in ihrem interdisziplinären Fachbuch eine Einführung in das Thema Blockchain und Kryptowährungen für Einsteiger und Fortgeschrittene. Dabei vereint das Buch die drei Kernbereiche Informatik, Kryptographie und Ökonomie. Das letzte Kapitel bietet einen Praxisleitfaden, der einen leichten Einstieg in die Verwendung von Bitcoin ermöglicht.

Daniel Burgwinkel (Hrsg.):

Blockchain Technology. Einführung für Business- und IT-Manager.
De Gruyter Oldenbourg 2016

Das Buch versteht sich als Handbuch für Entscheider. Nach einer allgemeinen Einführung in die Blockchain-Technologie präsentieren Experten aus Wissenschaft und Wirtschaft konkrete Anwendungsbeispiele. So wird dargestellt, wie sich die Blockchain unter anderem in der Finanzwelt und Energiewirtschaft einsetzen lässt. Anhand von Checklisten kann der Leser erkennen, welches Potenzial und welche Auswirkungen die Blockchain auf das eigene Unternehmen haben kann.



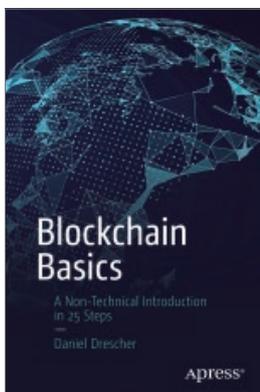
Don Tapscott und Alex Tapscott:

Die Blockchain Revolution. Wie die Technologie hinter Bitcoin nicht nur das Finanzsystem, sondern die ganze Welt verändert.
Plassen Verlag 2016

Blockchain ist mehr als nur Bitcoin – die Technologie, die hinter der Kryptowährung steht, hat das Potenzial, wirtschaftliche Beziehungen grundlegend zu verändern. Die Autoren erläutern, wie ein Blockchain-basiertes Wirtschaftssystem aufgebaut werden könnte und welche Anwendungen und Veränderungen damit verbunden sein könnten – von Finanzdienstleistungen bis hin zu Urheberrechtsregelungen. Auch die Risiken und Herausforderungen werden umrissen.

LINKS

- » www.btc-echo.de
Aktuelle Nachrichten und Hintergrundwissen zum Thema Bitcoin und zur Blockchain-Technologie
- » <https://hbr.org/2017/01/the-truth-about-blockchain>
Artikel in der „Harvard Business Review“ zur Blockchain und ihrem Potenzial
- » www.fit.fraunhofer.de/de/fb/cscw/blockchain.html
Blockchain-Labor des Fraunhofer-Instituts für Angewandte Informationstechnik: multidisziplinäre Konzepte, Entwicklung und Evaluation von Blockchain-Lösungen
- » www.frankfurt-school.de/home/research/centres/blockchain.html
Blockchain Center der Frankfurt School of Finance & Management: Forschungsprojekte sowie Austausch mit und für Unternehmen



Daniel Drescher:

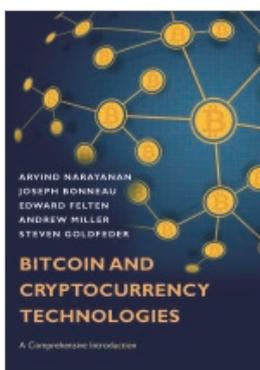
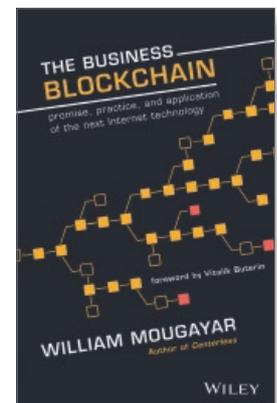
Blockchain Basics. A Non-Technical Introduction in 25 Steps. Apress 2017

Daniel Drescher, der selbst im Security Trading tätig ist, erklärt, warum die Blockchain relevant ist, wie sie funktioniert, welche Hindernisse es gibt und wie die Blockchain eingesetzt werden kann. Ohne Fachjargon und in 25 einfachen Schritten, angefangen von der Terminologie bis hin zur Funktionsweise und Anwendungen von Blockchain, schließt dieses Buch die Lücke zwischen rein technischen Einführungen und Handbüchern für Entscheider.

William Mougayar:

The Business Blockchain: Promise, Practice and Application of the Next Internet Technology. Wiley 2016

Der Autor stellt in seinem Buch zwei zentrale Thesen auf: erstens, dass Blockchain in einer Vielzahl von Gestalten auftritt und deswegen weitreichende und verschiedenste Auswirkungen auf Gesellschaft und Wirtschaft haben wird. Zweitens argumentiert er, dass nicht das Lösen von existierenden Problemen relevant ist, sondern vielmehr die Entwicklung von neuartigen Geschäftsmodellen auf Basis der Blockchain.



Arvind Narayanan et al.:

Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press 2016

Der Hype um die Blockchain ist groß: Doch wie viel davon ist gerechtfertigt, und was ist tatsächlich umsetzbar? Die Autoren bieten einen historischen Überblick und geben praktische Anleitungen zum Entwickeln von Softwarelösungen für die und mit der Blockchain. Das Lehrbuch bietet Antworten auf eine Vielzahl von Fragen: Wie funktioniert die Blockchain? Wie anonym sind die Nutzer? Wie können Kryptowährungen reguliert werden?

GLOSSAR

» Bitcoin

Bekannteste und bedeutendste Kryptowährung. Überweisungen oder andere Transaktionen werden über eine Blockchain abgewickelt, mittels Public Keys ausgeführt und sind so gegen Manipulationen gesichert. Der Umrechnungskurs von Bitcoin in andere Zahlungsmittel ist sehr volatil. Über die Bitcoin-Blockchain lassen sich im Unterschied zu Ethereum nur Zahlungstransaktionen abwickeln.

» Block

Abschnitt der Transaktionshistorie, die aus technischen Gründen in Pakete zerlegt werden muss. Bei öffentlichen Chains erhalten die Miner für das Finden einer Einheit eine Belohnung. Im Fall von Bitcoin zum Beispiel ist ein Block maximal 1 Megabyte groß und enthält bis zu 2.400 Transaktionen.

» Blockchain

Datenbank, in der Transaktionen, Informationen und Werte (Regeln, Verträge und Prozesse) festgehalten und dokumentiert sind. Jeder Datensatz ist durch einen sogenannten Hash-Wert mit dem nächsten Datensatz kryptographisch verkettet, was Manipulationen unmöglich macht. Neue Blöcke werden über ein Konsensverfahren geschaffen und anschließend an die Blockchain angehängt. Änderungen werden ebenso wie die ursprünglichen Transaktionen dokumentiert. Die Blockchain wird nicht zentral, sondern über ein dezentrales Netzwerk von Rechnern über das Internet verwaltet.

» Distributed Ledger

Verteiltes Register, das Transaktionen erfasst, in einem Peer-to-Peer-Netzwerk speichert und laufend aktualisiert. Die Technologie liegt der Blockchain zugrunde.

» Ethereum

Protokoll, Plattform und Netzwerk, um Code dezentral ausführen zu können. Alle Teilnehmer dieses verteilten Systems arbeiten mit einer gemeinsamen

Datenbasis: der Ethereum-Blockchain. Ethereum verwendet die Kryptowährung Ether als Zahlungsmittel für Rechenleistung, die die Teilnehmer zur Verfügung stellen. Ether ist nach Bitcoin die zweitbedeutendste Kryptowährung. Über Ethereum lassen sich im Unterschied zur Bitcoin-Blockchain auch Smart Contracts und der Transfer von anderen Werten abwickeln.

» Hash-Wert

Fingerabdruck eines Datensatzes, damit dieser verifiziert werden kann. In einer Blockchain ist der Hash-Wert eines vorgehenden Datensatzes im jeweils nachfolgenden gesichert.

» Initial Coin Offering (ICO)

Eine Art Crowdfunding über die Blockchain, bei dem ein Start-up sogenannte Token als Gutscheine für Leistungen seines Projekts verkauft, um seine Entwicklung zu finanzieren. Investoren können die ICO-Token in ihrer Ethereum-Wallet speichern. ICO lehnt sich an den Begriff des Initial Public Offerings (IPO) an.

» Mining

Prozess, um die Blöcke (öffentlicher) Blockchains zu bilden und Transaktionen zu validieren. Um eine neue Kontobewegung einem bestehenden Kontobuch hinzuzufügen, braucht es einen ganz bestimmten „Schlüssel“ (Hash). Dafür stellen Miner ihre Rechnerleistung zur Verfügung. Der Miner, der den speziellen Schlüssel findet, erhält eine Belohnung (zum Beispiel Bitcoins).

» Konsens

Verfahren, das die Dezentralität und Sicherheit in der Blockchain gewährleistet. Das populärste Konsensverfahren ist Proof of Work (PoW), bei dem der Nutzer beziehungsweise dessen Computer eine mäßig schwere Aufgabe lösen muss. Andere Konsensverfahren sind Proof of Stake (PoS), Proof of Burn, Proof of Activity. PoW und PoS eignen sich sehr gut für Public Blockchains. Das Konsensverfahren „Practical Byzantine Fault Tole-

rance“ eignet sich besonders für zugriffsbeschränkte private Blockchains.

» Off-Chain-Channel/-Transaktion

Transaktion außerhalb der Blockchain (nicht im Netzwerk), wobei ihre Echtheit dennoch über die Blockchain geprüft werden kann.

» Private vs. Public Blockchain

Unterschieden wird anhand der Teilnehmerrechte: Eine Public Blockchain ist vollkommen öffentlich, und jeder kann sich an dem Netzwerk beteiligen; die einzelnen Teilnehmer bleiben anonym (Beispiel: Bitcoin). Der Zugang zu einer Private Blockchain ist hingegen begrenzt und erfolgt per Einladung beziehungsweise Genehmigung der Netzwerkteilnehmer. Die Teilnehmer nutzen keine Pseudonyme (Beispiel: Hyperledger Fabric).

» Smart Contracts

In Softwareform niedergelegtes, intelligentes Regelwerk sowie Konsensmechanismen, auf die sich alle Beteiligten der Blockchain im Vorfeld verständigt haben. Smart Contracts überwachen ihre Ausführung selbst: Automatisch ausführbare Programme greifen und stoßen Prozesse an, wenn zuvor festgelegte Bedingungen erfüllt sind (Wenn-dann-Bedingungen). Einsatzfelder sind unter anderem E-Voting-Systeme, virtuelle Organisationen, Identity Management und Crowdfunding.

» Token

Mit Hilfe von Token, die meist auf der Ethereum-Blockchain basieren, werden zum Beispiel Blockchain-Start-ups und -Projekte finanziert/unterstützt (siehe ICO). Die so geschaffenen Assets können frei auf den Kryptobörsen gehandelt werden. Token haben nicht nur monetären Wert. Im Fall der DAO (Decentralized Autonomous Organization) erhalten Token-Besitzer über die beim ICO verkauften Token ein Stimmrecht über die Zukunft der Organisation.

AKTUELLE STUDIEN



Managementkompass Cyber Security

Unternehmen müssen ihre IT-basierten Abläufe und Aktionen durchgängig überwachen, um gegen Cyber-Angriffe gewappnet zu sein. Welche Herausforderungen das mit Blick auf Technik, Organisation und Mitarbeiter mit sich bringt, beleuchtet dieser Managementkompass ebenso wie rechtliche Implikationen und wirksame Maßnahmen zur Prävention, Erkennung und Reaktion.

Branchenkompass Banking

Der Branchenkompass Banking steht auf neuen Füßen. Praktiker aus der Finanzbranche haben sich getroffen, um die wichtigsten Herausforderungen und mögliche Lösungen zu diskutieren. Die herausgearbeiteten Themen wurden durch eine Online-Befragung von Führungskräften der Branche quantifiziert. Klares Fazit: Der Anpassungsdruck durch Regulierungsmaßnahmen auf nationaler, europäischer und internationaler Ebene bleibt hoch, und auch Datensicherheit und Datenschutz stehen auf der Agenda weit oben.



Studie Datengetriebene Agilität

Sopra Steria Consulting sowie Wissenschaftler der Universität Hamburg und der Leuphana Universität Lüneburg haben das Phänomen der datengetriebenen Agilität in Unternehmen untersucht und zeigen, dass sich diese Arbeitsweise digital exzellenter Unternehmen auch für Organisationen mit gewachsenen Strukturen und IT-Systemen eignet.

IMPRESSUM

Haftungsausschluss: Alle Angaben wurden sorgfältig recherchiert und zusammengestellt. Für die Richtigkeit und Vollständigkeit des Inhalts sowie für zwischenzeitliche Änderungen übernehmen Redaktion, Verlag und Herausgeber keine Gewähr.

© Oktober 2017

Sopra Steria GmbH
Hans-Henny-Jahnn-Weg 29, 22085 Hamburg

F.A.Z.-Institut für Management-, Markt-
und Medieninformationen GmbH
Frankenallee 68–72, 60327 Frankfurt am Main

Verlag: FRANKFURT BUSINESS MEDIA GmbH – Der F.A.Z.-Fachverlag
Bismarckstraße 24, 61169 Friedberg
Geschäftsführung: Dr. André Hülsbömer, Hannes Ludwig

Alle Rechte vorbehalten, auch die der fotomechanischen
Wiedergabe und der Speicherung in elektronischen Medien.

Titelfoto: © bearcreative/iStock/Thinkstock/Getty Images

ISBN: 978-3-945999-53-0

Redaktion: Jacqueline Preußner (verantwortlich),
Andrea van Baal, Juliane Streicher
Gestaltung und Satz: Christine Lambert
Lektorat: Vera Pfeiffer

Druck und Verarbeitung: Boschen Offsetdruck GmbH
Alpenroder Straße 14, 65936 Frankfurt am Main
www.boschendruck.de

Mit Ökofarben auf umweltfreundlichem Papier gedruckt.
Diese Studie wurde klimaneutral hergestellt. Der CO₂-Ausstoß
wurde durch Klimaschutzprojekte kompensiert.



Ansprechpartner

Sopra Steria GmbH

Corporate Communications
Birgit Eckmüller
Hans-Henny-Jahnn-Weg 29
22085 Hamburg
Telefon: (040) 22703-5219
E-Mail: birgit.eckmueller@soprasteria.com

F.A.Z.-Institut für Management-, Markt- und Medieninformationen GmbH

Jacqueline Preußner
Frankenallee 68–72
60327 Frankfurt am Main
Telefon: (069) 7591-1961
E-Mail: j.preusser@faz-institut.de

ISBN: 978-3-945999-53-0



9 783945 999530 >