iit perspektive

Working Paper of the Institute for Innovation and Technology | Nr. 39

Vertrauen und Transparenz – Blockchain-Technologie als digitaler Vertrauenskatalysator

Silvia Palka, Volker Wittpahl

i4c perspektive

Working Paper of the Institute for Innovation and Technology | Nr. 39

Silvia Palka, Volker Wittpahl

Vertrauen und Transparenz – Blockchain-Technologie als digitaler Vertrauenskatalysator

Ich spreche nicht über Bitcoin oder andere Cyberwährungen, aber über die [zugrundeliegende] Technologie, die Vertrauen und Effizienz bei einem Tausch jeglicher Art mit sich bringt. Das wird eine tiefgreifende Änderung in der Funktionsweise der Welt haben. […] Die Blockchain wird das für Transaktionen sein, was das Internet für Informationen tat."

Ginni Rometty, IBM

1. Vertrauen als Basis für Transaktionsprozesse

In der Ökonomie spielen Transaktionen eine zentrale Rolle. Nahezu jede Art des wirtschaftlichen Handels ist an einen Leistungstransfer gekoppelt, dessen Grundbedingung Vertrauen ist, ob im Verhältnis zwischen den Unternehmen, von Unternehmen zu Endkunden oder ausschließlich im Endkundenbereich; Vertrauen stellt die Basis für jedwede Art wirtschaftlicher Zusammenarbeit. Es ist eine elementare Vorbedingung, ein essenzieller Schlüssel für kollaborative Kooperation. Besonders deutlich äußert sich die Korrelation aus Vertrauen und Transaktionen in Verbindung zur Bonität. Hier werden in der Abhängigkeit zum Vertrauen unterschiedliche Risikoprämien gefordert. Ein zentrales Element in diesem Kontext ist die Einbettung von vertrauensstiftenden Institutionen, wie Notare, externe Prüfende oder Bürgen. Diese Institutionen ermöglichen allen Wirtschaftsteilnehmern einen möglichen Vertrauensbruch zu sanktionieren. Innerhalb der virtuellen Welt erhält das Konstrukt Vertrauen durch eine fehlende persönliche Interaktion sowie die zum Teil mangelnde Prüfung gegebener Informationen zur Durchführung von Transaktionen einen signifikanten Stellenwert. Aber auch die Unsicherheit in Bezug auf objektive Vertrauensintermediäre führt aufgrund verstärkt bekanntwerdender Beeinflussung – wie Softwaremanipulation, Zertifizierungsbetrug etc. – zur Verunsicherung der Wirtschaftsakteure. Selbst etablierte und seriöse Unternehmen unterliegen infolge des mangelnden Vertrauens schnell einem Generalverdacht (Düring, T./Fisbeck, H. 2017).

Basierend hierauf ist es kaum verwunderlich, dass die Blockchain-Technologie in der Wirtschaft, in Institutionen des Staates und im Finanzmarkt immer mehr Anklang erfährt. Sie steht für sichere, direkte sowie transparente Durchführung von Transaktionen. Infolge ihrer architektonischen Struktur „verringert die Blockchain die Notwendigkeit von Vertrauen […] beziehungsweise eliminiert sie komplett. Die Technologie ermöglicht es, Gleichrangigen eine überprüfbare, robuste und kryptographisch sichere Identität zu etablieren und bei Bedarf Vertrauen zu begründen" (Tapscott und Tapscott 2016).

Vor diesem Hintergrund wird am Beispiel von Smart Contracts dargestellt, dass das notwendige Vertrauen, welches derzeit durch Vertrauensintermediäre oder andere Institutionen impliziert wird, in einer Blockchain im Zuge einer digital transparenten Darstellung der Transaktionen substituiert werden kann. Diskutiert wird hierbei, inwiefern die Blockchain-Technologie das Vertrauen bei Transaktionen unterstützen kann.

2. Glaubwürdigkeit in Vertrauensintermediäre und andere Institutionen

Um Transaktionen sowohl in der analogen als auch der digitalen Welt zu sichern und Vertrauen zu erzeugen, haben sich mit der Zeit zahlreiche vertrauensbildende Vertrauensintermediäre etabliert. Diese sind in personelle sowie in institutionelle Vertrauensformen zu differenzieren. Während personales Vertrauen im Allgemeinen auf Akteure abzielt, richtet sich das institutionelle Vertrauen auf Organisationen im Bereich „Regulierungen oder Zertifikate und deren Funktionsfähigkeit. Institutionelles Vertrauen korrespondiert dabei mit dem Begriff Systemvertrauen („confidence") bei Luhmann bzw. mit Vertrauen in abstrakte Systeme" (Möller 2004).

Vertrauensintermediäre stellen u. a. Personen dar, die zwischen zwei Parteien als Vermittler fungieren. Sie beleuchten Leistung und Vertrauenswürdigkeit der jeweils anderen Partei. Zu sol-

chen Intermediären zählen Beratende, Bürgen oder auch Organisationen wie öffentliche Einrichtungen, Unternehmen, Notare und Banken (Richter 2017). In Handelsbeziehungen bewirkt diese Schaltfunktion durch Zeit-, Orts-, Mengen- und Eigentumstransformation eine Senkung der Kosten von Informationen, Vereinbarungen sowie Abwicklungen (Biegel 2001). Zu beachten ist allerdings, dass der Bedarf an Vertrauen hierdurch keinesfalls eliminiert, sondern lediglich auf eine höhere Ebene verlagert wird; der Treugeber vertraut bei der Durchführung der Transaktion auf die gültige Rechtsordnung (Hoßfeld 2006). Intermediäre implizieren so das integre Verhalten der Geschäftspartner.

Ein weiteres Indiz für Vertrauen in einen Kooperationspartner ist Reputation. Diese stützt sich neben eigenen Erfahrungen auch auf die Dritter. Sie ist ein Indikator für die Kenntnis eines Dritten und signalisiert Erfahrungen mit einem potentiellen Kooperationspartner. Reputation stellt eine öffentliche Information über die ex-post Vertrauenswürdigkeit eines Akteurs dar (Koch et al. 2000). Eine signifikante Rolle im Rahmen der Reputation spielt die Evolution des Brandings und der Markenkommunikation. Bei beiden Aspekten besteht ein starker korrelativer Zusammenhang zwischen Marke und Vertrauen. Treiber des Marken-/Brandingvertrauens sind Qualität der Produkte sowie Dienstleistungen, Verlässlichkeit, Ethik und Alter der Organisation, Erfahrungswerte aber auch Werbung (Kindel und Munzinger 2014). Das heutige Markenbild und dessen Implikation in Vertrauen stammen überwiegend aus der Industriezeit, in der „Marken über ihren Markenkern ein Markenversprechen abgegeben haben" (Düring, T./Fisbeck, H. 2017).

Ein gewisses Maß an Verletzlichkeit, bezogen auf die Seriosität und Integrität des Gegenübers, ist somit Voraussetzung für Vertrauensbildung; dies gilt analog auch für die digitalen Märkte. (Nissenbaum 2001) Die Divergenz zwischen Vertrauen in digitale und nicht-digitale Dienste besteht besonders darin, dass das Vertrauensobjekt im Gegensatz zu Individuen, Gruppen oder Intuitionen primär im Zuge einer Website dargestellt wird (Nissenbaum 2001).

Auch in der digitalen Welt bedienen sich die Institutionen einer Reputation. Exemplarisch seien hier der Einsatz von Werbemitteln, das Markenversprechen aber auch Kommunikationswege im Rahmen von sozialen Medien genannt. Im Gegensatz zum klassischen, linearen Modell streben Organisationen im Zuge der sozialen Medien eine interaktive und dynamische Kommunikation an. Die Kommunikationskanäle sind hier durch eine Vielzahl an Kommunikationspartnern geprägt, in denen sich jeder adäquat äußern kann. Persönlichkeit, Authentizität und Vertrauen bilden elementare Faktoren in diesem Kommunikationsprozess (Riedel und Sonntag 2012).

Einen weiteren wesentlichen Aspekt bilden Nutzerratings[1]. Diese Art von Rezensionen erzeugen einen komparativen Vorteil und somit Vertrauen (Heckersbruch et al. 2013). Umfragen zeigen, dass Nutzermeinungen im Internet hohen Stellenwert haben; sie beeinflussen sowohl die Markenbilder als auch die konkrete Produktwahl erheblich (Fittkau & Maaß Consulting 2009). Eine Studie von Brinkmann[2] et al. weist auf, dass sich die Anzahl von Transaktionen bei schlechten Bewertungen verringert (Brinkmann und Seifert 2001).

Neben der Reputation durch Marke sowie Branding haben auch in der digitalen Welt Vertrauensintermediäre eine essenzielle Rolle. Als vertrauensbildende Institutionen fungieren hier Siegel sowie Zertifikate. Hierbei handelt es sich um Auszeichnungen, welche von einem „unabhängigen Dritten ausgestellt werden, einen gewissen Sicherheitsstandard aufweisen und somit Vertrauenswürdigkeit suggerieren" (Heckersbruch et al. 2013). Studien (Statista 2017, Gütesiegel für Online-Shops) legen den Beweis dar, dass Programme von Drittparteien auf das Kundenvertrauen und ihre Transaktionsabsichten einwirken. Webseiten und Online-Shops wie bspw. Öko-Tex, TÜV Service Tested, e-Trusted welche ein Gütesiegel innehaben, projizieren Vertrauenswürdigkeit, Kundenorientierung sowie Seriosität (Heckersbruch et al. 2013). Diese Intermediäre agieren hierbei als Vermittelnde zwischen Online-Anbietern und Online-Nutzern. Weitere relevante Intermediäre, die im elektronischen Geschäftsverkehr eine wesentliche Stellung einnehmen, sind (Online-)Banken, PayPal, Visa, Uber, Google, Apple sowie weitere digitale Unternehmen; sie fungieren ebenfalls als Mittler zwischen Anbietenden und Nachfragenden. Adäquat zu klassischen Vertrauensintermediären transportieren diese ‚Institutionen' Vertrauen bei Transaktionen und projizieren so das integre Verhalten des Geschäftspartners, welcher in der Regel bei digitalen Vorhaben fremd ist, d.h. nur im Zuge einer Website dargestellt wird (Tapscott und Tapscott 2016).

Gleichzeig wird derzeit die vertrauensbildere Wirkung von etablierten Güte- und Prüfsiegeln in Frage gestellt. „Immer wieder werden Manipulationen bekannt, mit denen selbst etablierte Marken vortäuschen, die jeweiligen Kriterien zu erfüllen. Solche in den Medien breit dargestellten Skandale […] führen zu Verunsicherung bei Verbrauchern und selbst etablierte, seriöse Anbieter geraten so unter Generalverdacht" (Düring, T./Fisbeck, H. 2017). Auch wenn keine betrügerische Absicht hinter

1 Unter Nutzerratings werden hier Empfehlungen oder Beurteilungen von Konsumentinnen und Konsumenten verstanden.
2 Ulrich Brinkmann ist ein deutscher Sozialwissenschaftler und Professor für Soziologie mit den Schwerpunkten Organisations- und Arbeitssoziologie an der Technischen Universität Darmstadt.

Abbildung 1: Ebenen der Vertrauensbildung. Quelle: Düring et al. (2017), S. 452.

den Manipulationen steht, so ist die permanente Kontrolle von Zertifizierungen dauerhaft kaum möglich. Bei einem (neuen) Geschäftspartner ist unmöglich nachzuprüfen, ob die Kriterien weiterhin eingehalten werden.

3. Steigender Anspruch auf Transparenz

Die Nachfrage nach Vertrauenswürdigkeit von Personen, Funktionsträgern oder Institutionen ist in der heutigen Zeit mit einem steigenden Anspruch auf Transparenz verbunden (Statista 2018). Dies ist insbesondere auf die Tatsache zurückzuführen, dass Menschen den sich immer schneller verändernden Innovationen skeptisch gegenüber stehen; Korruption, Manipulationen sowie Globalisierung stellen in diesem Kontext zusätzliche signifikante Faktoren dar (Edelmann 2017). Eine Studie von Edelman[3] aus dem Jahr 2017 zeigt, dass das derzeitige Vertrauen in Institutionen wie Wirtschaft, Regierung und Medien sich derzeit in der Krise befindet (Edelmann 2017). Diskrepanz hinsichtlich des Vertrauensgrads und des Wahrheitsgehalts von Informationen zwischen den klassischen und sozialen Medien steigert den Anspruch auf Transparenz auch bei journalistischen Angeboten. Diese Anforderung ist besonders der Tatsache geschuldet, dass sog. Fake News[4] sowie Social Bots[5] Medien als Informationsverteiler instrumentalisieren (Wollschläger 2017).

Dementsprechend ist Vertrauen auf höchster Ebene nur dann erreichbar, wenn sich der Geschäftspartner „durch erworbenes Wissen und persönliche Kontrolle selbst ein Bild über die Qualität oder die Einhaltung bestimmter Kriterien machen kann" (Düring, T./Fisbeck, H. 2017, siehe Abb. 1). Dies belegt auch eine Studie von Klenk & Hoursch[6]. Sie zeigt, dass für die Gewinnung, Festigung oder Wiederherstellung von Vertrauen Transparenz und sicheres Wissen wesentliche Faktoren sind (Greven und Lahme 2014).

4. Blockchain – die Peer-to-Peer-Lösung

Um Transparenz bei Transaktionen zu erlangen ist eine lückenlose, unveränderbare Historie notwendig. Dies kann z.B. durch die entwickelte Blockchain-Architektur, welche für den sichereren Transfer der Kryptowährung Bitcoin konzeptualisiert wurde, gelöst werden (Düring, T./Fisbeck, H. 2017).

Die Blockchain-Technologie ist eine dezentrale Datenbank, die sowohl eine synchronisierte als auch eine kontinuierlich wach-

3 Das Edelman Trust Barometer ist eine jährliche Studie der PR-Agentur Edelman zu Vertrauen in und Glaubwürdigkeit von Regierungen, Nichtregierungsorganisationen (NGOs), Wirtschaft und Medien, die im Jahr 2017 zum 17. Mal durchgeführt wurde. Für diese Studie wurden rund 33.000 Menschen in 28 Ländern befragt.
4 Fake News stehen für absichtlich verbreitete Falschmeldungen.
5 Social Bots sind Computerprogramme, die in sozialen Medien Nachrichten verbreiten, z. B. um die öffentliche Meinung zu manipulieren.
6 Die Klenk & Hoursch AG gehört zu den führenden inhabergeführten Beratungen für methodische Unternehmens- und Markenkommunikation.

sende Liste von Transaktionsdatensätzen vorhält. Da die Blockchain chronologisch linear erweitert wird, wird hier bildlich von einer Blockkette gesprochen. Erst wenn ein Block vollumfänglich geschaffen wurde, wird der nächste erstellt (Iansiti und Lakhani 2017).

„Als elektronisches Register für digitale Datensätze, Ereignisse oder Transaktionen, die in einem verteilten Rechnernetz verwaltet werden, liegt der Blockchain das Konzept eines sogenannten „Distributed Ledger" (verteiltes Register) zugrunde" (Scherk und Pöchhacker-Tröscher 2017). Hierunter wird ein öffentliches dezentral geführtes Kontobuch verstanden, das von allen Teilnehmern über das Netzwerk geteilt wird und in dem jeder in der Blockchain über eine identische, synchronisierte Kopie des Verzeichnisses verfügt. Diese Art der Netzwerktechnologie wird als P2P-Netzwerke bezeichnet (Hileman und Rauchs 2017). „Im P2P-Netzwerk haben alle Teilnehmer (oft als Knoten oder „nodes" bezeichnet) dieselben Rechte und können auf die gleichen Informationen zugreifen sowie dem Ledger Informationen zufügen" (Scherk und Pöchhacker-Tröscher 2017). Zudem ermöglicht diese Technologie Transaktionen bis zum Ursprung zurückzuverfolgen (Nakamoto 2008).

Die Blockchain hat sich seit ihrer Bekanntheit durch Nakamoto im Jahr 2008 weiterentwickelt. Richtete sich die Blockchain 1.0 ausschließlich auf monetäre Anwendung, „[so] sind mit der Blockchain 2.0 […] im Gegensatz zu Bitcoin auch nichtmonetäre Anwendungen möglich. Beispiele hierfür sind der Handel mit Daten und Waren" (Neumann et al. 2017). Die Blockchain 3.0 umfasst die Nutzung der Technologie über den Finanzbereich hinaus bspw. in der öffentlichen Verwaltung, im öffentlichen Kulturbereich oder im Gesundheitswesen (Sixt 2017). Die bekanntesten Blockchain-Systeme sind u.a. Bitcoin, Ethereum, Ripple, Hyperledger oder Eris (Torvekar 2017).

Grundsätzlich lässt sich der Blockchain-Ansatz in drei Arten unterteilen: Private Blockchain, Consortium Blockchain und Public Blockchain. Alle Arten sind Peer-to-Peer(P2P)-Netzwerke, bei denen alle Teilnehmenden ein Duplikat des Transaktionsprotokolls besitzt und die Blöcke der Blockchain bis zum Genesis Block[7] zurückverfolgen kann. Der Unterschied der Blockchain-Ansätze liegt in dem Zugriff auf die Daten. Während bei der Private Blockchain alle Schreibrechte zentral gesteuert werden, können hier die Leserechte sowohl beliebig reglementiert werden als auch öffentlich zugänglich sein. In Rahmen der Consortium Blockchain wird hingegen „der Konsistenz-Prozess durch vorselektierte Knoten kontrolliert. Das Leserecht kann hier öffentlich oder auf einzelne Teilnehmer eingeschränkt sein" (Düring, T./Fisbeck, H. 2017). Kennzeichnend für eine Public Blockchain ist, dass alle Teilnehmenden die gleichen Rechte haben sowie dass alle Transaktionen gleichwertig auf jedem Server verzeichnet werden.

4.1 Bestandteile der Blockchain

Blockchain stellt keinesfalls eine neue Technologie dar, sie basiert auf verschiedenen Technologien, die zu einem neuen System integriert wurden. Wesentliche Elemente stammen aus den Bereichen Kryptografie, P2P-Netzwerke und Transaktionen (Voshmgir 2016).

4.1.1 Kryptografie

Die Komponente Kryptografie transportiert Transparenz und Privatsphäre und basiert auf zwei kryptografischen Grundbestandteilen, zum einem den Hash-Funktionen und zum anderen den digitalen Signaturen sog. Public-Key-Kryptografien.

Hash-Funktionen leiten Transaktionen ein, wodurch mittels digitaler Signaturen ein integrer Informationsaustausch zwischen zwei Parteien befähigt wird (Narayanan et al. 2016). Das Konzept der Public-Key-Kryptografie beruht auf einem Algorithmus, der „aus einem privaten (persönlicher Geheimzahl) und einem öffentlichen Schlüssel (Adresse)" (Schlatt et al. 2016), besteht. Hierdurch wird eine (digitale) Unterschrift suggeriert.

Bei der Ausführung einer Transaktion errichtet der Absender eine digitale Signatur des Datensatzes, der Empfänger – alle Knoten im Netzwerk – verwendet zur Dekodierung der Transaktion den öffentlichen Schlüssel; dieser ist ebenfalls zur Validierung des Blockchain-Protokolls notwendig. Auf diese Weise werden drei Sicherheitsaspekte verifiziert: Identifikation des Absenders, Authentizität der Nachricht sowie durch asymmetrische Kodierung des Datensatzes die inhaltliche Integrität (Condos et al. 2016).

Ebenfalls die Hashfunktion ist ein Algorithmus, der eine Zahlenfolge von unbestimmter Länge in eine feste Zahlenreihe (Hashwert) umwandelt. „Eine Hashfunktion ist deterministisch, d.h. dieselben Eingangsdaten ergeben immer denselben Hashwert" (Schlatt et al. 2016).

Überdies führt eine Veränderung an einem Parameter innerhalb der Transaktion zur Veränderung des Hashwerts. Aufgrund der Transparenz im Netzwerk wird ihre Gültigkeit validiert. Grundsätzlich weisen Hashfunktionen drei Merkmale auf: Kollisionssicherheit, Einwegfunktion, Schnelligkeit (Czernik 2016). Hashwerte dienen durch die Berechnung eines digitalen Fingerabdrucks zum Integritätsschutz. Hierdurch wird in einem öffent-

7 Der Genesis-Block ist der aller erste Block innerhalb der Blockkette.

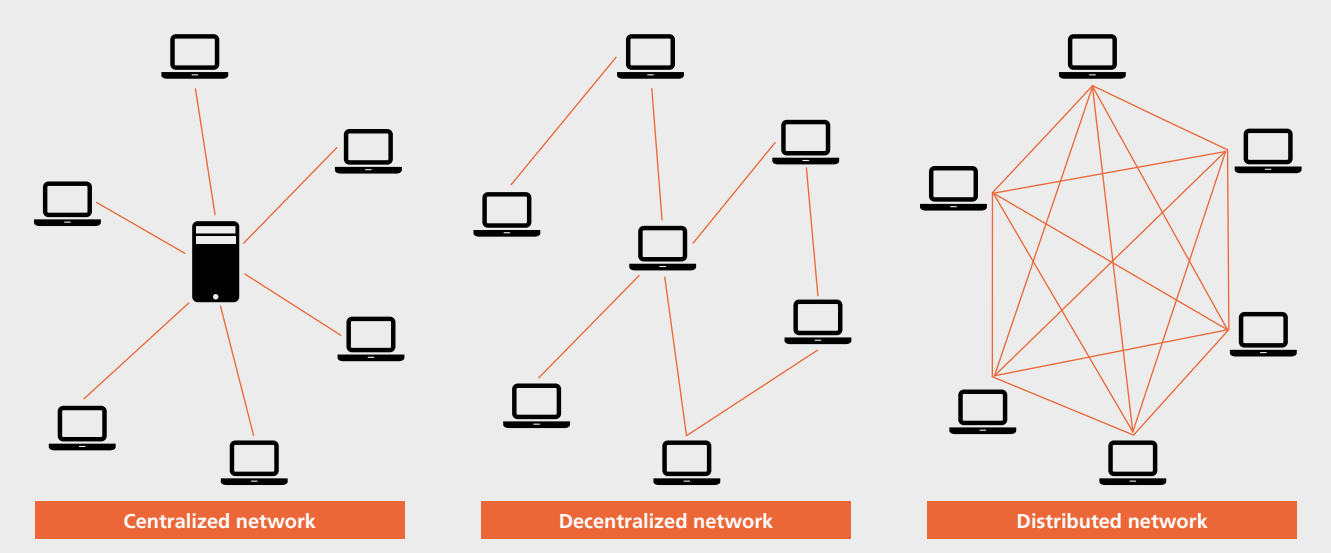

Abbildung 2: Netzwerkarchitekturen. Quelle: Ethereum-Base (2018).

lichen Netzwerke der Aspekt Anonymität und Sicherheit von Sender und Empfänger gewährleistet (Neumann et al. 2017).

4.1.2 Peer-to-Peer Netzwerkarchitektur – Dezentralität des Systems

Grundsätzlich sind P2P-Netzwerke als eine Sammlung von heterogen verteilten Ressourcen, verbunden durch ein Netzwerk, zu verstehen. Kennzeichnend für dieses Netzwerk ist das Konzept einer Entität, d. h. das System als Ganzes agiert autonom (Schollmeier 2001) sowie „vorzugsweise ohne Nutzung zentraler Dienste mit dem Ziel der gegenseitigen Nutzung von Ressourcen" (Dinger 2009). Alle Teilnehmer in einem Blockchain-Netzwerk kommunizieren direkt miteinander. Durch das Konzept Distributed Ledger [8] werden alle Transaktionen erfasst und über das P2P-Netzwerk verteilt. Da Daten wie z. B. Konten bei der Bitcoin-Blockchain mittels eines Zahlencodes verschlüsselt werden, wird trotz der Transparenz die Sensibilität gewahrt, d.h. die Kontowerte sind zwar für jeden im Ecosystem sichtbar, anonymisiert werden hingegen die Besitzerdaten (Ghosh et al. 2017). Eine herbeigeführte Veränderung eines Blocks, bspw. im Zuge eines Hackangriffs, würde von anderen Teilnehmern unmittelbar registriert und überschrieben werden. Da die Sicherheit in einem P2P-Netzwerk nicht wie klassischerweise über eine zentrale Instanz gesteuert wird, sondern hier über das Netzwerk geleitet wird (Düring, T./Fisbeck, H. 2017).

Abb. 2 zeigt schematisch die unterschiedlichen Netzwerkarchitekturen zentral, dezentral sowie das System des Distributed Ledger.

4.1.3 Transaktionen

Die Blockchainarchitektur ist so konzipiert, dass Transaktionen dezentral erstellt gespeichert, verteilt sowie validiert werden. In Blockchain-Netzwerken werden kryptografische Währungen oder Informationen an eine Adresse transferiert, welche den Hashwert des spezifischen öffentlichen Schlüssels repräsentiert (Bonneau et al.).

Grundsätzlich werden Transaktionen in Blöcken erfasst. Der Block stellt den zentralen sowie gleichzeitig den kleinsten Bestandteil einer Blockchain dar, der durch die Aneinanderreihung von nicht veränderbaren Richtigbefundanzeigen entsteht (Düring, T./Fisbeck, H. 2017). In der Regel setzt sich ein Block aus vier Komponenten zusammen: erstens aus einem vorangegangenen Block, der aufgrund seines Hashwertes eindeutig identifiziert wird, zweitens einem Zeitstempel (Timestamp) zum Existenz-Nachweis eines bestimmten Termins, drittens der laufenden, noch unbestätigten Transaktion, heruntergebrochen in einem kryptografischen Code (root Hash), sowie viertens einem Index, „einer Einmalnummer, welche über Versuch und Irrtum gefunden werden muss" (Düring, T./Fisbeck, H. 2017), der sogenannte Nonce. Dieser sogenannte Proof of Work stellt sicher, dass eine neue Richtigbefundanzeige nur gebildet wird, wenn diese am neusten Block andockt (Neumann et al. 2017). Dieser Vorgang wird in der Abb. 3 veranschaulicht.

Im Zuge von Mining[9] erfolgt die Generierung eines validen Blocks. Hierbei wird durch (rechnerische) Ermittlung von Nonce ein Block generiert und anschließend samt der Nonce der

8 Distributed Ledger = dezentral geführten Kontobüchern
9 Mining ist ein Rechenprozess, bei dem neue Blöcke der Blockchain durch kryptografische Hashberechnung generiert werden.

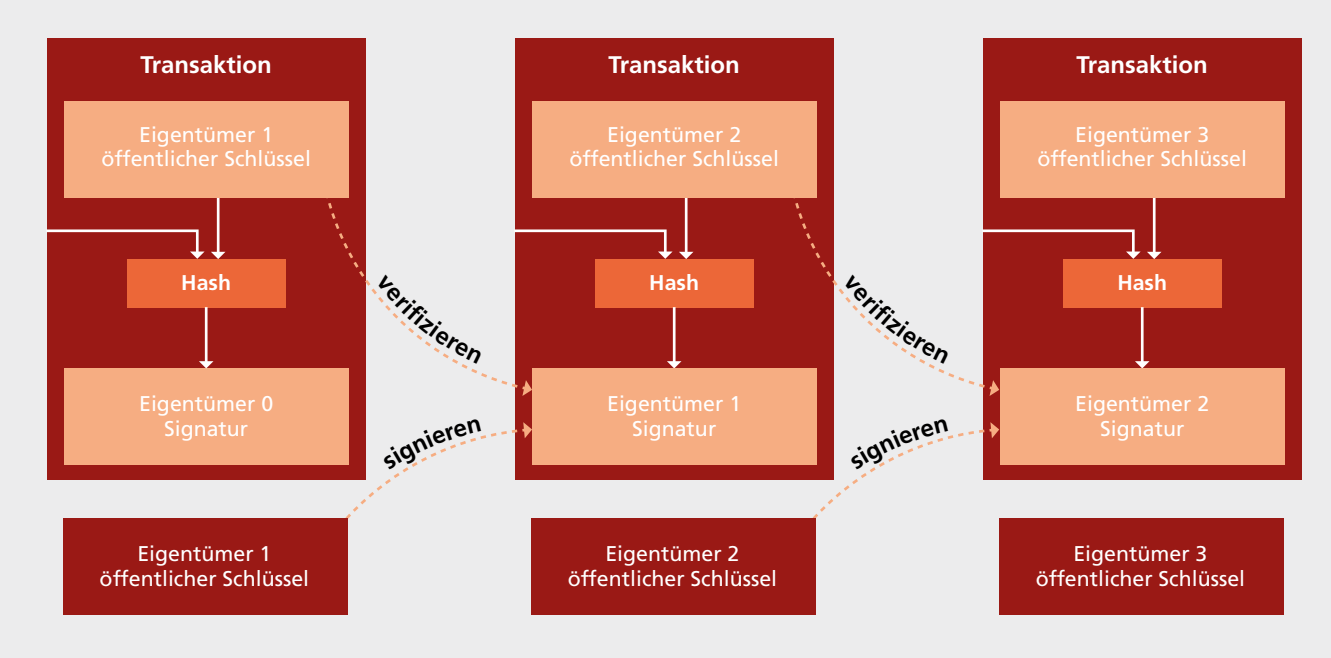

Abbildung 3: Bildung einer Transaktionskette zu einem Block. Quelle: Neumann et al. (2017), S. 22.

Hashwert gebildet (Sixt 2017). Wurde ein Block entsprechend des Protokolls verifiziert, erhält der Teilnehmer, der Miner[10], eine Belohnung (Block Reward). Diese „Incentivierung führt im Zusammenspiel mit dem P2P-Charakter der Blockchain dazu, dass der Aufwand für Manipulationen des Gesamtsystems dann enorm groß wird, wenn die Zahl der beteiligten Nutzer groß ist" (Voshmgir 2016). Zudem erhält jeder Netzknoten neben der Kopie der Blockchain einen Cachespeicher, welcher „Transaktionsoutputs der Blockchain enthält, die noch nicht für neue Transaktionen weiterverwendet wurden, und eine Datenbank mit unbestätigten Transaktionen" (Schlatt et al. 2016).

4.2 Funktion der Blockchain

Aufgrund der architektonischen Struktur bietet die Blockchain eine End-to-End-Transparenz, sowohl im Finanzdienstleistungs- als auch im technisch-konzeptionellen Bereich. Jede Information, jeder Produktionsschritt wird im Rahmen der architektonischen Struktur der Blockchain abgebildet sowie individuell mit jedem einzelnen Produkt verknüpft. Auf diese Weise bietet die Blockchain eine Plattform für globale digitale Transaktionen – ohne Partizipation einer dritten Instanz, eines Vertrauensintermediärs.

In einer Blockchain werden Daten anonym gespeichert, dezentral registriert und übermittelt. Diese Kombination gewährleistet ein hohes Maß an Sicherheit, „die auf sicherer Authentifizierung, Kennzeichnung und Schutz der Daten basiert. Über Sicherheitsaspekte hinaus ergeben sich jedoch auch Möglichkeiten zur Optimierung der Prozesse und zur Reduzierung der Kosten im Unternehmen" (Neumann et al. 2017). Bei einem Produktlebenszyklus können Prozesse bei Verbindung mit Internet of Things[11] bspw. bei Wiederverwertung jedem einzelnen Rohstoff zugeordnet werden. Verbraucher können anstatt autokratischer Entscheidungsprozesse und Vertrauen in Institutionen neue ethische Standards aufgrund der Transparenz in dezentrale Marktordnung setzen (Swan 2015). Die Problematik des derzeitigen geringen Vertrauens in Institutionen kann auf Basis von Transparenz durch sicheres Wissen ausgehebelt werden. Weil jede Transaktion mit einem Zeitstempel versehen und chronologisch mit anderen Blöcken verknüpft ist, wird Vertrauen durch Transparenz in Prozesse generiert.

10 Miner verifizieren Block für Block die hinterlegten Informationen und teilen sie im Blockchain-Netzwerk.
11 Das Internet of Things (IoT) besteht aus Gegenständen, die durch den Einbau von Mikrochips „smart" werden und sich so direkt und über das Internet mit anderen Gegenständen und Computern, jedoch ohne menschlichen Eingriff untereinander koordinieren. Jedes smarte Objekt erhält dabei eine eindeutige Kennung, über die es im Netzwerk identifiziert werden kann.

5. Blockchain als Lösung für manipulationssichere Transaktionen in Wertschöpfungsketten und Smart Contracts

5.1 Wertschöpfungsketten

Das Konzept Blockchain umfasst beispielsweise die Möglichkeit der Abbildung einer kompletten Wertschöpfungskette, von Rohfertigung bis zur Auslieferung eines Produkts. Jeder Prozessschritt kann mittels seiner Architektur abgebildet werden. Die Technologie bietet demnach unterschiedlichen „Systemen der im Prozess beteiligten Unternehmen" (Düring, T./Fisbeck, H. 2017) aber auch überwachenden Institutionen oder Konsumenten eine Plattform zum standardisierten Austauschformat. Im Mittelpunkt der Blockchain steht der sogenannte Shared Ledger, ein gemeinsames Register, zu welchem alle Akteure Zugang haben. Einzelnen Blocks werden hingegen individuelle Zugriffsrechte zugewiesen. Diese Systematik schafft Transparenz und transportiert Vertrauen entlang der ganzen Wertschöpfungskette (Rogaischus 2017). Klassischerweise werden derzeit Daten individuell auf unternehmensinternen Servern gespeichert, wie in Abb. 4 grafisch präsentiert.

Die dezentrale Architektur bietet eine Reihe von Optionen, mit denen auf branchenspezifische Trends reagiert werden kann. Zentrale Faktoren in diesem Zusammenhang lauten: Kosteneffizienz, durchgängig digitale Abbildung einer unternehmensübergreifenden Lieferkette, Reduzierung von Verzögerungen in der Lieferkette auf ein Minimum sowie finanzielle Werte, welche in Sekundenschnelle und mit geringen Transaktionskosten ausgetauscht werden könnten (Backofen und Klingenburg 2017). Beispielhaft sei hier die Lebensmittelbranche genannt. Das gesamte Ecosystem eines Produkts kann mittels der Blockchain-Technologie adressiert werden, vom Landwirt/Erzeuger über die verarbeitende Industrie bis hin zum Verbraucher – alle Beteiligten haben binnen Sekunden Zugang auf den aktuellen Datensatz. Der Produzent kann zu jedem Zeitpunkt verfolgen, an welchem Standort sich einzelne Zutaten befinden und danach seine Produktion ausrichten. Verbraucher oder Gesundheitsbehörden beispielsweise bekommen Möglichkeiten, digitale Produktinformationen jedes einzelnen Gliedes, wie „Herkunftsbetrieb, Chargennummer, Verarbeitungsdaten, Ablaufdaten und Lieferungsdetails wie die Einhaltung der Kühlkette" (Gahr 2017), sofort einzusehen. Hierdurch erhalten Qualitätsmanagement sowie Kundenanforderung in der Produktion eine höhere Relevanz. Neben der Transparenz, welche eine höhere Lebensmittelsicherheit und Rückverfolgbarkeit schafft, werden ethische Foodprints einzelner Produkte als Nachweis für den Wahrheitsgehalt erzeugt. Dieser Prozess führt aufgrund der Transparenz und Rückverfolgbarkeit innerhalb der gesamten Wertschöpfungskette zur Vertrauenssteigerung.

5.2 Smart Contracts

Bei Verträgen im herkömmlichen Sinn werden Vereinbarungen zwischen zwei oder mehreren Parteien geschlossen. Die Pflichterfüllung beruht in diesem Kontext primär auf einer Vertrauensbasis oder wird auf eine höhere Ebene, in Form von einem Intermediär, verlagert. Smart Contracts beinhalten adäquat zu klassischen Verträgen die gleiche Art von Vereinbarungen, sie eliminieren jedoch, basierend auf ihrer Technologie, die Instanz der Vertrauensintermediäre. Ein Smart Contract wird mittels Codes definiert sowie automatisch durch den Code verwirklicht (Swan 2015).

Smart Contracts sind „programmierte Anwendungen, bei denen der Vertragsgegenstand automatisiert ausgeführt wird, wenn eine definierte Vertragsbedingung erfüllt ist" (Neumann et al. 2017). Sie sind Verträge, die auf einer Wenn-Dann-Beziehung basieren und mit realen Vermögenswerten interagieren (Sixt 2017).

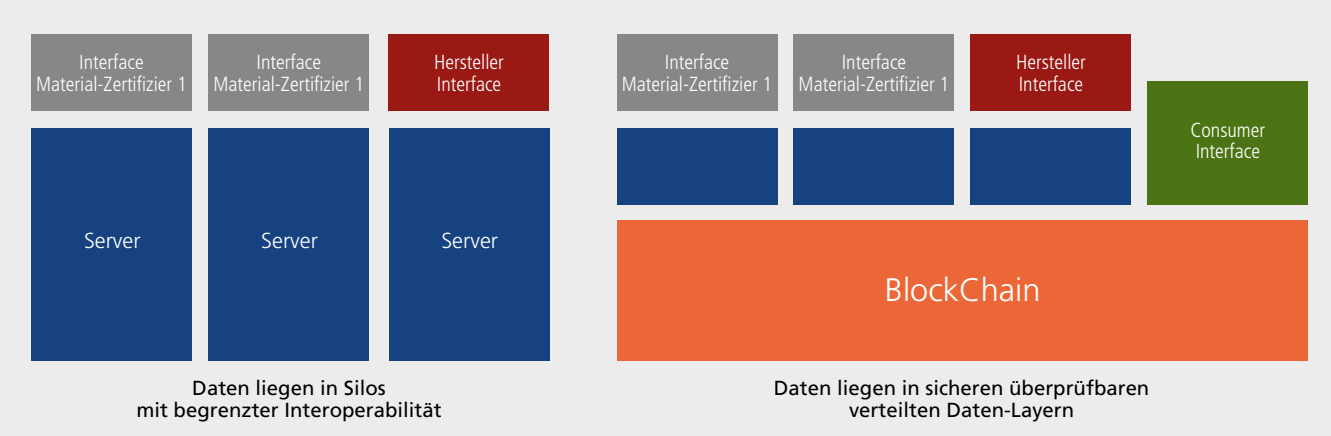

Abbildung 4: Datenhaltung mit und ohne Blockchain in einer Wertschöpfungskette. Quelle: Düring et al. (2017), S. 457.

Klassisches Beispiel für eine Smart Contract-Applikation stellen elektronische Autotürschlösser dar, welche bei Anmietung eines Fahrzeugs automatisch prüfen, ob der Nutzer einerseits in Besitz einer gültigen Legitimation ist, andererseits, ob die Nutzungsgebühr bereits entrichtet wurde. Erst wenn beide Voraussetzungen erfüllt sind, öffnet sich das Schloss (Schlatt et al. 2016).

Signifikant für Smart Contracts sind drei Eigenschaften: Autonomie, Autarkie und Dezentralisierung (Swan 2015). Autonomie in diesem Zusammenhang bedeutet, dass die Ausführung des Vertrags im Rahmen von Algorithmen überwacht und ausgeführt (Buterin 2013). Zwei wesentliche Faktoren wirken sich positiv auf den Vertrag aus: Zum einen reduzieren sich Transaktionskosten durch die Einsparung eines Vermittlers, zum anderen wird mittels der Technologie die Übertragung des Eigentums- oder Nutzungsrechts beschleunigt, das binnen Minuten übertragen werden kann. Wird ein neuer Block erstellt, werden die Daten oder Rechte, die im dem Block transferiert wurden, auf den Empfänger übertragen.

Durch das P2P-Netzwerk werden Smart Contracts dezentral und anonym gespeichert und über die Netzwerkknoten verteilt sowie ausgeführt (Swan 2015). Dieser Umstand erzeugt eine Irreversibilität, d.h. Manipulationen bei Buchungen, wie das Zurückdatieren von Verträgen, sind infolge des Zeitstempels ausgeschlossen, welcher als Nachweis der Existenz einer Transaktion in der Blockchain fungiert. Eine weitere relevante Eigenschaft ist Korrektheit. Ein einmal aufgesetzter Blockchain-Code ist nicht revidierbar und stellt somit Integritäten von in der Blockchain gespeicherten Daten nie in Frage.

Am Beispiel von Smart Contracts lässt sich Disintermediation aufzeigen. Die Blockchain ermöglicht mehreren Parteien eine gemeinsame Datenbank zu verwenden, ohne die Einbindung einer dritten Instanz. Diese Komponente ist besonders für Parteien von Relevanz, die sich nicht kennen und/oder sich nicht vertrauen. Smart Contracts bieten eine Grundlage Prozesse in der Wirtschaft gravierend zu transformieren: Verträge werden in Form von Computerprotokollen ausgefertigt und basierend auf sicherheitstechnischen Systemen neu strukturiert. Sie bieten darüber hinaus die Möglichkeit, komplexe, aber auch stark individualisierte Verträge digital abzubilden und umzusetzen.

6 Potenziale und Risiken der Blockchain

6.1 Potenziale

Grundsätzlich bietet die Blockchain-Technologie vielschichtige Potenziale. Zu den zwei zentralen Eigenschaften gehören die transparente Darstellung der Daten und selbige fast in Echtzeit von der Genese an; Protokolle in einer Blockchain werden fortgeschrieben und alle Änderungen dokumentiert. Mittels dieser beiden Komponenten wird der Faktor Vertrauen transportiert und die Gefahr von manipulativen, betrügerischen Transaktionen durch die Verzahnung dieser beiden Komponenten werden weitestgehend reduziert. Diskrepanzen beim Informationsfluss vom Sender zum Empfänger werden aufgrund der chronologischen Verkettung der Blöcke in der Blockchain eliminiert. Globale Sicherheit sowie Authentizität der Daten werden hierdurch von Beginn an gewährleistet. Dieser Konsens zeichnet sich zudem positiv auf die Transaktionskosten aus. Durch die Offenlegung der Daten hinsichtlich der Herkunft von Rohstoffen, Herstellungsprozessen usw. können Transaktionskosten signifikant gesenkt sowie Vertrauensintermediäre umgangen werden.

Die Kombination eines Konsensmechanismus zur Justierung des Status der Blockchain mit einem verteilten P2P-Netzwerk zollt zusätzliches Vertrauen. Im Zuge dessen, dass „sowohl die Blockchain selbst, als auch einzelne Mechanismen wie die Verifikation digitaler Signaturen […], vielfach bei allen Netzteilnehmern reproduziert wird, gibt es innerhalb des Netzwerks keinen Single Point of Failure" (Schlatt et al. 2016); Datensicherheit sowie Stabilität des Netzwerks wird auf diese Weise sichergestellt. Dieser Konsensmechanismus verhindert überdies beispielsweise bei monetären Transaktionen die Gefahr von Double Spending[12], alle Knotenpunkte prüfen individuell einerseits Konten der einzelnen Transaktionen, andererseits die Gültigkeit der Blöcke. Diese Funktion ersetzt die Rolle eines Vertrauensintermediärs, dritte „Parteien [sind] für Aktionen innerhalb des Netzwerks und die Verwaltung der Blockchain obsolet" (Schlatt et al. 2016). Die Abbildung der Blockchain auf kryptografischen Prinzipien transportiert Sekurität. Durch die Verwendung eines privaten und öffentlichen Schlüssels wird eine detaillierte Zugangskontrolle etabliert. Die Kombination aus beiden Schlüsseln verleiht der Blockchain eine hohe Sicherheit, welche in der analogen Welt in dieser Form selten gegeben ist. Sicherheitsaspekte, wie bspw. Authentizität der Nachricht, Identifikation des Absenders sowie inhaltliche Integrität der Daten, erfüllen die Faktoren einer vertrauenswürdigen Technologie. Einen weiteren Vorteil bildet die Verwendung der Hashfunktion und Erzeugung eines digitalen Zwillings. Diese Komponenten gewährleisten Datensicherheit der in der Blockchain enthalten Informationen. Zwar gibt es außerhalb der Blockchain-Technologie adäquate

12 Double Spending (engl.): Doppelausgabe

Möglichkeiten der Datenspeicherung bspw. über eine Cloud, doch sind diese zentral gebündelt. Zudem fallen für Cloudsysteme Kosten sowohl für die Datenspeicherung als auch Übertragung an, welche hier deutlich höher sind.

Ein wesentlicher Faktor im Hinblick auf Vertrauenssteigerung ist die Nachweisbarkeit der Produkterzeugung. Insbesondere Verbrauchern ist es möglich, infolge der Transparenz in der Blockchain die Lieferkette ganzheitlich zu verfolgen und beispielsweise die Versprechen der Hersteller hinsichtlich einer Produkteigenschaft zu überprüfen. Offengelegte Rückverfolgungen führen zur Wiederherstellung und zur Steigerung von Vertrauen. Eine Folge hiervon wäre, dass Nachweise, wie Produktsiegel oder -zertifikate automatisch auf einer Webseite ein- und ausgeschaltet werden können, wenn bestimmte Kriterien erfüllt sind (Düring, T./Fisbeck, H. 2017). Die Bewertung durch eine dritte, nicht fälschungssichere, Instanz wäre hierdurch hinfällig. Aufgrund der Transparenz sowie Rückverfolgbarkeit werden Verunreinigungen oder Probleme in der Lieferkette besser erkannt und Produkte schneller, gezielter sowie systematischer aus dem Markt entfernt; Verursacherquellen erfahren eine zügige Identifikation. Diese weltweite Nachverfolgbarkeit, begründet durch den gewissen Grad an Kontrolle und führt zur Sicherstellung der Glaubwürdigkeit. Die unveränderbare Historie der Blockchain schafft Beweiskraft; Vertrauen in die Vertragspartner wird durch sicheres Wissen ersetzt (Düring, T./ Fisbeck, H. 2017). Gleichzeitig können Käufe in der Blockchain zurückgespiegelt werden, d.h. für den Käufer/Verbraucher entstehen neue Potenziale, bsph. infolge von personalisierten Kaufempfehlungen. Weil die Daten in einer Blockchain dezentral allen Händlern zur Verfügung stehen, können individuelle Empfehlungen übergreifend durchgeführt sowie personifizierte Vorlieben berücksichtigt werden. Grundsätzlich können durch die Blockchain Prozesse schneller und effizienter gestaltet werden, insbesondere auf globaler Ebene. Papiergebundene und langwierige Prozesse für Transportkosten würden im Zuge der Blockchain entfallen. Kosten für die Qualitätskontrolle angelieferter Ware würden hierdurch deutlich reduziert werden.

Ein signifikanter Vorteil von Smart Contracts liegt in der autonomen Ausführung der Vertragsbedingungen. Die Einhaltung derer erfolgt nicht im Rahmen von menschlicher Interaktion, sondern infolge von automatisierten Algorithmen. Hierdurch können Verträge effizient, schnell sowie mit minimalen Transaktionskosten abgewickelt werden. Werden heute für einen dokumentierten Vertragsabschluss in der Regel zwei bis drei Tage benötigt, erfolgt der Vertragsabschluss im Zuge von Smart Contracts binnen Minuten. Aufgrund von Codierung sowie Dezentralität gelten intelligente Verträge als betrugs- und fälschungssicher. Sollte eine Vertragspartei Veränderungen an Verträgen oder Bedingungen vornehmen, werden die anderen Parteien gewarnt. Die unveränderbare Historie der Blockchain schafft Vertrauen, auch wenn Vertragspartner unbekannt sind. Aufgrund der Zug-um-Zug-Ausführung in fast Echtzeit werden Vollstreckungen der Bedingungen automatisch überprüft und durchgesetzt, der hier entstehende Mehrwert spiegelt sich in Rechtssicherheit wider.

6.2 Risiken

Trotz vieler inhärenter, positiver Aspekte weisen Blockchain-Systeme Risiken auf. Die Irreversibilität von Transaktionen bildet einen wesentlichen Nachteil. Fehlerhaft eingegebene sowie abgesendete Transaktionen sind nicht mehr reversibel, d.h. Rückerstattungen können nur mittels einer neuen Transaktion vorgenommen werden. Erst mit kritischer Masse von Teilnehmern manifestiert die Technologie ihre Sicherheit. „Die Entscheidung, welche Blöcke der Kette hinzugefügt werden, wird bei der Blockchain durch ein Consensus-Modell getroffen. In der Regel muss dafür die Mehrheit des Netzwerks die Korrektheit der Daten verifizieren […]. Ist das Netzwerk relativ klein, ist es umso einfacher für Akteure, die Mehrheit der Rechenleistung im Netzwerk aufzubringen – wodurch eine Manipulation der Daten möglich wäre“ (Scherk und Pöchhacker-Tröscher 2017).

Ein wesentlicher Nachteil im Rahmen von Wertschöpfungsketten folgt aus der Transparenz. Weil derzeit in einer Produktionskette nicht alle Komponenten digitalisiert sind und somit nicht direkt miteinander kommunizieren, müssten die Daten z.T. auch manuell in die Datenbank implementiert werden. Der Faktor Mensch als Fehlerquelle oder als Werkzeug für manipulative Handlungen besteht somit weiterhin. Ein weiteres Risiko basiert auf der kollaborativen Zusammenarbeit des Ecosystems in einer Blockchain. Wird ein gemeinsamer Nutzen nicht erkannt oder aufgrund landestypischer Gesetzeslagen von einem Partner, einer Behörde, bspw. dem Zollamt, nicht akzeptiert, wird ihre Funktion als Kontrollinstanz des gesamten Lebenszyklus eines Produkts hinfällig. Auf der Grundlage der Daten aus Blockchain erfolgt ein transparenter Verlauf vom Kunden zum Hersteller. Die positiv dargestellt personifizierten Angebote, insbesondere im Rahmen der Losgröße 1[13], bieten gleichzeitig die Grundlage für den individuellen und direkten Kontakt zwischen Händler und Kunden; der Verbraucher wird hiermit zu einem gläsernen Kunden. Ein erweiterter Schutz der Privatsphäre müsste daher im Rahmen von Blockchain berücksichtigt werden.

Im Rahmen von Smart Contracts bildet die Ausführung der Verträge im Zuge von Algorithmen die größte Hürde. Der Vertragspartner wird hier nicht aufgrund seiner Persönlichkeit, Vertrautheit oder menschlicher Ebene als vertrauenswürdig einge-

13 Losgröße 1 ist die individuelle Produktion nach Kundenwunsch.

stuft, Transaktionskosten werden aufgrund eines Algorithmus berechnet. Die menschliche Komponente und das Wort eines Geschäftspartners ist infolge von Smart Contracts zu keinem Zeitpunkt von Relevanz. Zur Senkung der Transaktionskosten besteht langfristig ein Risiko in der Raster-Optimierung. Die Höhe der Transaktionskosten wird im Rahmen von Smart Contras individuell bemessen. Wenn ein Vertragspartner das vorgegebene Raster in der Blockchain unterlaufen will, um seine Reputation zu verbessern und auf diese Weise die Berechnung der Transaktionskosten durch den Algorithmus zu minimieren, besteht die Gefahr, dass er sich im Vorfeld, analog zur Google Optimization, bestimmter Werkzeuge bedient. Somit wären die Transaktionskosten in einer Blockchain in einer gewissen Weise anfällig für Manipulationen. Ein weiteres Risiko bildet die Gestaltung der Verträge. Jeder einzelne Aspekt, wie Regressansprüche, Anwartschaften oder Gewährleistungen, müssen im Vorfeld detailliert definiert werden. Der Wegfall von Intermediären reduziert nicht zwingend gleichermaßen das Konfliktpotenzial zwischen den Vertragspartnern. Gleichzeitig, um Rechtssicherheit zu erlangen, muss die Nutzeridentität offengelegt werden. Hierdurch können dieser Person rückwirkend jegliche Transaktionen zugeordnet werden. In einer öffentlichen Blockchain stellt dieser Umstand ein Konfliktpotenzial zwischen Datenschutz und der Irreversibilität von Daten innerhalb eines Blockchain-Netzwerks dar. Die Irreversibilität der Blockchain stellt ein Risiko in Rahmen von Code is Law dar. Einerseits kann ein Fehler im Code nicht einfach revidiert werden. Andererseits stellen Fehler im Code ein erhebliches „Sicherheitsrisiko dar und können von Hackern ausgenutzt werden, um das System zu kompromittieren. In solchen Fällen kann es auch schwierig sein nachzuweisen, ob dabei eine illegale Handlung vorliegt oder das Ausnutzen von Hintertüren quasi ein Feature des Codes ist“ (Scherk und Pöchhacker-Tröscher 2017). Zu beachten ist, dass Smart Contracts keinesfalls die Rechtsordnung der Vertragsbedingungen überprüft, sondern ausschließlich die Erfüllung des Codes, sie sind ein automatisiertes Vertragsausführungswerkzeug. Professionelle Governance-Regeln sowie eine prinzipielle juristische Prüfung entfällt mit Smart Contracts zu keinem Zeitpunkt.

7 Zusammenfassende Bewertung

Durch ihre unveränderbare und lückenlose Historie projiziert die Blockchain Beweiskraft und schafft sicheres Wissen. Dadurch wird Vertrauen in Aussagen von Vertragspartnern oder vertrauensstiftenden Institutionen durch vollkommende Transparenz zu jeder Zeit ersetzt. Gleichzeitig wird durch die Dokumentation sämtlicher Prozessschritte Vertrauen durch Wissen und persönliche Kontrolle wiederhergestellt sowie stabilisiert.

Durch ihr breites Spektrum an Kapazitäten ermöglicht die Blockchain Organisationen, ihre Datensilos zu verlassen und gewährt effiziente sowie nachvollziehbare Prozesse in ihrem Ökosystem. Neben Reduzierung von Papierdokumenten z. B. bei der Digitalisierung von Frachtbriefen in Prozess- oder Wertschöpfungsketten bietet die Blockchain Käufern mehr Informationen über die Herkunft sowie den Produktionsweg eines Produkts, wodurch sich eine Kultur der Transparenz erzeugen lässt. Manipulationsversuche können aufgrund der umfangreichen Verwendung von kryptografischen Signaturen und Hash-Ketten erkannt (und abgelehnt) werden. Im Zentrum der Blockchain stehen der Aufbau einer gemeinsamen und sicheren Wissensbasis sowie die Entstehung von Vertrauen durch Transparenz.

In Kombination mit einer blockchainbasierten Transaktionswährung erzeugt die Blockchain bei ökonomischen Prozessen die größten Veränderungspotenziale; Zug um Zug könnten Transaktionen von Waren, Wissen, etc. saldiert werden. Allerdings fehlt es derzeit hierzu an passenden Regularien oder Standards. Die Etablierung der Blockchain-Technologie innerhalb von traditionellen Institutionen und Prozessen bedeutet einen revolutionären Wandel. Trotz dieser Einschränkung sowie den aufgeführten Risiken hat die Blockchain das Potenzial in diversen Bereichen die bisherigen Standards bei Transaktionen, Datenhaltung, Prozessen sowie Kommunikation zu verändern. Infolge ihrer Stabilität und der direkten (1:1) Kommunikation können sowohl vertragliche Bedingungen als auch Transaktionen automatisiert werden.

Zusammenfassend lässt sich festhalten, dass die Blockchain-Technologie das Potenzial hat, die wirtschaftlichen aber auch sozialen Prozesse zu revolutionieren. Sie bietet infolge ihrer Eigenschaften die Chance innerhalb der digitalen Transformation Vertrauen durch Transparenz zu steigern bzw. wiederherzustellen. Hierfür müssen die dargestellten Schwächen sowie Rechts- und Datenschutzfragen geklärt und offene Sicherheitsaspekte geschlossen werden.

Literaturverzeichnis

Backofen, Dirk; Klingenburg, Peter: Vertrauen und Transparenz in Wertschöpfungsketten – Blockchain offenbart großes Potenzial für Industrie 4.0. In: manage it, Ausgabe 7-8-2017. Online verfügbar unter http://ap-verlag.de/vertrauen-und-transparenz-in-wertschoepfungsketten-blockchain-offenbart-grosses-potenzial-fuer-industrie-4-0/36398/, zuletzt geprüft am 15.04.2018.

Biegel, Thomas (2001): Die rolle von intermediaren (zwischenhandlern) auf elektronischen markten. [Place of publication not identified]: Diplom De.

Bonneau, Joseph; Miller, Andrew; Clark, Jeremy; Narayanan, Arvind; Kroll, Joshua A.; Felten, Edward W.: SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In: 2015 IEEE Symposium on Security and Privacy (SP). San Jose, CA, S. 104–121.

Brinkmann, Ulrich; Seifert, Matthias (2001): „Face to Interface": Zum Problem der Vertrauenskonstitution im Internet am Beispiel von elektronischen Auktionen. In: *Zeitschrift für Soziologie* 30, S. 23–47.

Buterin, Vitalik: A Next Generation Smart Contract and Decentralized Application Platform 2013. Online verfügbar unter http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf, zuletzt geprüft am 15.04.2018.

Condos, James; Sorrbell, William H.; Donegan, Susan L. (2016): Blockchain Technology. Opportunities and Risks. Vermont, 2016. Online verfügbar unter https://legislature.vermont.gov/assets/Legislative-Reports/blockchain-technology-report-final.pdf.

Czernik, Agnieszka (2016): Hashwerte und Hashfunktionen einfach erklärt, 02.09.2016. Online verfügbar unter https://www.datenschutzbeauftragter-info.de/hashwerte-und-hashfunktionen-einfach-erklaert, zuletzt geprüft am 15.04.2018.

Dinger, Jochen (2009): Das Potential von Peer-to-Peer-Netzen und -Systemen. Architekturen, Robustheit und rechtliche Verortung. Zugl.: Karlsruhe, Univ., Diss., 2008. Karlsruhe: Univ.-Verl.

Düring, T./Fisbeck, H. (2017): Einsatz der Blockchain-Technologie für eine transparente Wertschöpfungskette. In: Alexandra Hildebrandt und Werner Landhäußer (Hg.): CSR und Digitalisierung. Der digitale Wandel als Chance und Herausforderung für Wirtschaft und Gesellschaft. Berlin, Heidelberg: Springer Gabler (Management-Reihe Corporate Social Responsibility), S. 449–464.

Edelmann (2017): Edelman trust barometer. Executive summary. Online verfügbar unter http://fipp.s3.amazonaws.com/media/documents/Edelman%20Trust%20Barometer%202017_Executive%20Summary.pdf.

Ethereum-Base: https://ethereum-base.com/blockchain/, zuletzt geprüft am 31.05.2018.

Fittkau & Maaß Consulting (2009): Nutzermeinungen im Internet beeinflussen Kaufverhalten erheblich. Online verfügbar unter http://www.w3b.org/e-commerce/nutzermeinungen-im-internet-beeinflussen-kaufverhalten-erheblich.html, zuletzt geprüft am 15.04.2018.

Gahr, Oliver: Mit Blockchain Lebensmittel sicherer machen – und Leben retten. In: IBM, Think Blog DACH. Online verfügbar unter https://www.ibm.com/de-de/blogs/think/2017/09/14/mit-blockchain-lebensmittel-sicherer-machen/, zuletzt geprüft am 15.04.2018.

Ghosh, Raoul; Ott, Mathias; Sandne, Philipp (2017): Digitalisierung der Versicherungswirtschaft mit Blockchain und Smart Contracts. FSBC Working. Frankfurt am Main. Online verfügbar unter http://explore-ip.com/2017_Digitalisierung-der-Versicherungswirtschaft.pdf.

Greven, Kathrin; Lahme, Georg (2014): Freiwillige Transparenz führt zum Erfolg. In: Riccardo Wagner, Georg Lahme und Tim Breitbarth (Hg.): CSR und Social Media. Unternehmerische Verantwortung in sozialen Medien wirkungsvoll vermitteln. Berlin: Springer Gabler (Management-Reihe Corporate Social Responsibility), S. 99–116.

Heckersbruch, Christina; Öksüz, Nicolai Walter, Jörg Becker, Guido, Ayten Öksüz, Nicolai Walter, Jörg Becker, Guido, Ayten; Walter, Nicolai; Becker, Guido, Jörg; Hertel, Guido (2013): Vertrauen und Risiko in einer digitalen Welt -. Hamburg. Online verfügbar unter https://www.divsi.de/wp-content/uploads/2013/09/DIVSI-Vertrauen-und-Risiko-in-einer-digitalen-Welt.pdf.

Hileman, Garrick; Rauchs, Michel (2017): Global Blockchain Benchmarking Study. Cambridge. Online verfügbar unter https://fsinsights.ey.com/dam/jcr:e9c710a5-1863-45e5-bd93-cae227d808fc/Blockchain%20Benchmarking%20Study%20(Web).pdf, zuletzt geprüft am 15.04.2018.

Hoßfeld, Heiko (2006): Die Erklärung von Vertrauen im ökonomischen Modellbau - zwischen Realitätsnähe und Komplexität. In: *Sozialwissenschaftlicher Fachinformationsdienst soFid*, S. 9–31.

Iansiti, Marco; Lakhani, Karim R.: The Truth About Blockchain. In: *Harvard Business Review* 2017. Online verfügbar unter https://hbr.org/2017/01/the-truth-about-blockchain, zuletzt geprüft am 15.04.2018.

Kindel, Heike; Munzinger, Uwe (2014): Der Schlüssel zum Markenvertrauen. Hamburg. In: *Markenartikel*, S. 100–103.

Koch, Michael; Möslein, Kathrin; Wagner, Michael (2000): Vertrauen und Reputation in Online-Anwendungen und virtuellen Gemeinschaften. In: Martin Engelien und Detlef Neumann (Hg.): Virtuelle Organisation und Neue Medien 2000. Workshop GeNeMe2000, Gemeinschaften in Neuen Medien: TU Dresden, 5. und 6. Oktober 2000. Lohmar, Köln, Dresden: Josef Eul Verlag; Sächsische Landesbibliothek - Staats- und Universitätsbibliothek Dresden (Telekommunikation Mediendienste, Band 10), 69–84.

Möller, Antje (2004): Ökonomische Analyse von Vertrauen in umweltorientierten Innovationskooperationen. Bochum: Fakultät für Wirtschaftswissenschaft, Ruhr-Universität Bochum (Discussion Paper No. 03-04). Online verfügbar unter http://www.ruhr-uni-bochum.de/vwb/paper/vwbrub03-04.pdf.

Nakamoto, Satoshi: A Peer-to-Peer Electronic Cash System. Online verfügbar unter A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, zuletzt geprüft am 15.04.2018.

Narayanan, Arvind; Bonneau, Joseph; Felten, Edward (2016): Bitcoin and Cryptocurrency Technologies. A Comprehensive Introduction // Bitcoin and cryptocurrency technologies. A comprehensive introduction. Princeton.

Neumann, Susanne; Demidova, Ekaterina; Kohlhoff, Mareike (2017): Die Potenziale der Blockchain in der Energiewirtschaft. In: *ew Magazin für die Energiewirtschaft*, S. 20–26.

Nissenbaum, Helen: Securing Trust Online: Wisdom or Oxymoron? In: *Law Review* 2001 (81 (3)), S. 101–131.

Richter, Caroline (2017): Vertrauen innerhalb von Organisationen. Ein soziologisches Modell. Dissertation. Bielefeld (Kultur und soziale Praxis).

Riedel, Jana; Sonntag, Ralph (2012): Kompetenzen für das Online-Reputation-Management. In: Ralph Sonntag, Jana Riedel, Matthias Bernhard Schulten, Artur Mertens und Andreas Horx (Hg.): Kompetenzen für das Online-ReputationManagement // Social Branding. Strategien - Praxisbeispiele - Perspektiven. Wiesbaden: Gabler Verlag, S. 97–108.

Rogaischus, Axel: Blockchain in der Automobilindustrie. In: IBM, Think Blog DACH. Online verfügbar unter https://www.ibm.com/de-de/blogs/think/2017/07/11/blockchain-automobil-industrie, zuletzt geprüft am 15.04.2018.

Scherk, Johannes; Pöchhacker-Tröscher, Gelinde (2017): Die Blockchain – Technologiefeld und wirtschaftliche Anwendungsbereiche. Linz.

Schlatt, Vincent; Schweize, André; Urbach, Nils; Fridgen, Gilbert (2016): Blockchain: Grundlagen, Anwendungen und Potenziale. White Paper. Bayreuth.

Schollmeier, Rüdiger (2001): A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications. In: *Proceedings of the First International Conference on Peer-to-Peer Computing (P2P 2001)*, S. 101–102.

Sixt, Elfriede (2017): Bitcoins und andere dezentrale Transaktionssysteme. Blockchains als Basis einer Kryptoökonomie. Wiesbaden: Springer Gabler.

Statista (2017): Gütesiegel für Online-Shops: Bekanntheit – Vertrauen – Beachtung,. Hamburg.

Statista (2018): Warum müssen Unternehmen transparent sein? Hamburg.

Swan, Melanie (2015): Blockchain. Blueprint for a new economy. 1. Aufl. Beijing: O'Reilly (Safari Tech Books Online).

Tapscott, Don; Tapscott, Alex (2016): Die Blockchain-Revolution. Wie die Technologie hinter Bitcoin nicht nur das Finanzsystem, sondern die ganze Welt verändert. Kulmbach: Plassen Verlag.

Torvekar, Gaurang (2017): 7 blockchain technologies to watch out for in 2017. Online verfügbar unter https://medium.com/@gaurangtorvekar/7-blockchain-technologies-to-watch-out-for-in-2017-4b3fc7a85707.

Voshmgir, Shermin (2016): Blockchains, Smart Contracts und das Dezentrale Web. Berlin.

Wollschläger, Julia (2017): Bevölkerungsbefragung: Social Bots und Fake News, PwC Communications. Düsseldorf. Online verfügbar unter https://www.pwc.de/de/technologie-medien-und-telekommunikation/social-bots-berichtsband.pdf, zuletzt geprüft am 15.04.2018.

Herausgeber
Prof. Dr. Volker Wittpahl
Institut für Innovation und Technik (iit)
in der VDI/VDE Innovation + Technik GmbH
Steinplatz 1, 10623 Berlin

Kontakt
Silvia Palka
Tel.: +49 (0)711 123-3033
E-Mail: silvia.palka@vdivde-it.de

Prof. Dr. Volker Wittpahl
Tel.: +40 (0)30 310078-5507
E-Mail: wittpahl@iit-berlin.de

iit perspektive Nr. 39
Juni 2018

Layout: Poli Quintana
Bildnachweis: Adobe Stock/Sashkin

ISBN: 978-3-89750-193-5

Aus Gründen der besseren Lesbarkeit wird teils auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Ferner wird auf die Verwendung des geschlechterneutralen Gender-Sterns verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für jedes Geschlecht.