Blockchains als Herausforderung für das Records Management

Peter Keller-Marxer

Einführung

Die «Blockchain» ist das technologische Herzstück des digitalen Währungs- und Zahlungssystems «Bitcoin»[1]. Der Begriff dient heute als Synonym für Informatik-Anwendungen, die das Grundkonzept der Blockchain – «die Blockchain-Technologie hinter Bitcoin» – in Geschäftsmodellen der Internet-Ökonomie auch jenseits von digitalen Währungen nutzbar machen: Parteien in Handelsbeziehungen sollen untereinander Werte, Besitz oder Rechte auf vertrauenswürdige und verbindliche Weise über das Internet übertragen können, ohne sich dabei auf *vertrauenswürdige Dritte* verlassen zu müssen.

Zu solchen Dritten zählen Banken, Notare, Kreditkarten-Herausgeber, Logistik-Dienstleister, Betreiber von Infrastrukturen zur Telekommunikation und Herausgeber von Zertifikaten für elektronische Signaturen sowie auch die staatlichen Behörden, welche solche Dritte akkreditieren, zertifizieren oder kontrollieren. In herkömmlichen Handelsbeziehungen setzen Parteien ihr Vertrauen in einen solchen vertrauenswürdigen Dritten, damit dieser als Intermediär die Identität der Parteien verbindlich feststellt, als verlässlicher Zeuge ihrer gegenseitigen Willenserklärung auftritt, ihre Transaktion (z.B. die Übertragung von Werten oder die Festschreibung vertraglicher Rechte und Pflichten) authentifiziert und ausführt sowie verbindliche Belege und Nachweise (Records) zu den Sachverhalten der Transaktion erstellt.

Die systematische Führung und Aufbewahrung solcher Records (Records Management) dient der Erfüllung gesetzlicher und regulatorischer Rechenschafts-, Nachweis- und Aufbewahrungspflichten. Sie stellen zudem Urkunden dar, die Rechtsansprüche nachweisen oder begründen und in gerichtlichen Auseinandersetzungen als Beweismittel dienen. Die Parteien tragen die Verantwortung für die gesetzeskonforme Aufbewahrung und die Nachweisbarkeit der Echtheit (Authentizität und Integrität) der von ihnen erstellten und empfangenen Records.

Solche Nachweis- und Aufbewahrungspflichten müssen unabhängig von der Art der geschäftlich genutzten Infrastruktur erfüllt werden. Es stellt sich die Frage, ob dies bei einer Blockchain überhaupt möglich ist, da hier der vertrauenswürdige Dritte und damit auch die im herkömmlichen Sinne vertrauenswürdigen Belege und

1 https://bitcoin.org

Informationswissenschaft: Theorie, Methode und Praxis, Bd. 5 (2018), Nr. 2 — http://dx.doi.org/10.18755/iw.2018.30

Urkunden zum Nachweis der Transaktionen fehlen. Stattdessen übernimmt eine Software, das Blockchain-System, die Rolle des vertrauenswürdigen Dritten: Es identifiziert die Handelspartner, authentifiziert ihre Transaktionen, führt diese aus und weist sie als schriftliche Einträge in einem Journal, der Blockchain, nach. Die Blockchain ist gleichzeitig auch das Behältnis, welches alleine die vertrauenswürdige Aufbewahrung dieser Records zu gewährleisten hat.

Das wesentliche Merkmal eines Blockchain-Systems ist, dass es ein nach festgelegten Regeln *autonom* agierendes System ist, keinen für es haftenden Betreiber hat und durch niemanden oder zumindest nicht durch einzelne Akteure manipulierbar ist, insbesondere auch nicht durch Betreiber der technischen Infrastruktur (Software und Hardware) dieses Systems. (Wäre dieses System das technische Vehikel einer natürlichen oder juristischen Person, welche für sein korrektes Funktionieren verantwortlich zeichnet, so wäre diese Person bereits wieder ein vertrauenswürdiger Dritter und das Blockchain-System bloss ein Surrogat.)

Erreicht wird dies durch eine spezielle System-Architektur, ein sogenanntes *Peer-to-Peer* Verbundnetzwerk aus zahlreichen gleichberechtigten, geografisch verteilten und unabhängig agierenden Computern, die über ein gemeinsames Protokoll Transaktionsdaten untereinander austauschen und sich mit Hilfe von kryptographischen Verfahren und einem sogenannten Konsensalgorithmus selbstständig auf den gültigen Zustand des Gesamtsystems einigen. Dieser Zustand wird zu jedem Zeitpunkt durch die Blockchain als Journal repräsentiert, in dem jede von einem Rechner im Netzwerk authentifizierte und ausgeführte Transaktion aufgezeichnet wird.

Diese Architektur ermöglicht es, dass das System als Ganzes nicht kompromittierbar ist, selbst wenn einige der partizipierenden Rechner manipuliert wurden (also «unehrlich» oder «bösartig» agieren). Mittels kryptografischer Verfahren wird sichergestellt, dass in der Blockchain aufgezeichnete Informationen nachträglich nicht mehr geändert oder gelöscht werden können. Jeder Rechner im Verbundnetzwerk verfügt über eine eigene Kopie der Blockchain und kann jederzeit deren Gültigkeit und ihre exakte Übereinstimmung mit allen anderen im Netzwerk gespeicherten gültigen Blockchain-Kopien überprüfen. Die Blockchain garantiert somit zu jedem Zeitpunkt die Integrität (Unveränderheit) aller jemals in ihr festgehaltenen Informationen. Sie ist durch alle Handelspartner jederzeit und ortsunabhängig einsehbar und dient ihnen als dauerhafter Beleg über die von ihnen im Netzwerk getätigten Transaktionen.

Eine Blockchain lässt sich mit tausenden, weltweit verteilten Kopien eines Buchungsjournals (*distributed ledger*) oder Registerbuchs vergleichen. Für jede Kopie ist ein einzelner, unabhängiger Buchhalter zuständig, der darin immer nur solche Buchungen nachführt, die durch eine Mehrheit aller anderen Buchhalter als

gültig bestätigt werden.[2] Solange sich eine Mehrheit der Buchhalter «ehrlich» (regelkonform) verhält, können einzelne «unehrliche» Buchhalter ihre eigene Kopie des Journals zwar manipulieren, machen sie dadurch aber für alle anderen Buchhalter und partizipierenden Handelspartner sofort sichtbar ungültig.

Das Wesen dieses Konstrukts liegt nicht im Vertrauen der Handelspartner in die «Vertrauensmaschine»[3] Blockchain: Das Vertrauen in Handelspartner, vertrauenswürdige Dritte oder Maschinen basiert schlussendlich immer auf einer Risikoabwägung, ob die gegenseitigen Rechte und Pflichten, welche die Handelspartner in der von ihnen gewählten Form als Willenserklärung festschreiben, im Streitfall auch gerichtlich durchsetzbar sind. Gemäss Zivilprozessordnung gelten auch elektronische Dateien als Beweisurkunden, wenn sie dazu geeignet sind, rechtserhebliche Tatsachen zu beweisen (Art. 177 ZPO), und das Obligationenrecht sieht grundsätzlich die Formfreiheit von Verträgen vor (Art. 11 Abs. 1 OR): Ein Vertrag kann unabhängig von einer bestimmten Form zustande kommen, wenn übereinstimmende gegenseitige Willensäusserungen der Parteien vorliegen und das Gesetz keine speziellen Formerfordernisse vorschreibt (wie zum Beispiel bei Schenkungen) oder eine hoheitliche notarielle Beglaubigung verlangt (wie zum Beispiel bei der Übertragung von Grundeigentum).

Die grundsätzliche Problematik einer zu geschäftlichen Zwecken genutzten Blockchain liegt vielmehr in der fehlenden Verantwortlichkeit für die in ihr aufgezeichneten Informationen als vertrauenswürdige Belege und Nachweise der Transaktionen. Weder die Handelspartner noch Dritte sind für die Vertrauenswürdigkeit und die dauerhafte Verfügbarkeit dieser Records verantwortlich. Dies soll vielmehr das autonom agierende Blockchain-System leisten, also ein Techniksystem, für dessen Funktionieren keine natürliche oder juristische Person haftbar gemacht werden kann (und dessen Betreiber und Nutzer unter Umständen nicht einmal identifizierbar sind, wie im Fall der Bitcoin-Blockchain).

Blockchain-Evangelisten führen unterschiedlichste Gründe für die Umgehung von vertrauenswürdigen Dritten in digitalen Handels- und Kommunikationsbeziehungen an.[4] Anfänglich waren Techno-Libertäre und Krypto-Anarchisten[5] tonangebend, die darin ein probates Mittel zur Befreiung von staatlicher Kontrolle, Unterdrückung oder Zensur sehen. Sie wurden abgelöst von Akteuren der *Sharing*

2 Hier zeigt sich eine Ähnlichkeit zu dem im Bibliotheksbereich bekannten System LOCKSS (Lots of Copies Keep Stuff Safe, https://www.lockss.org). Auch LOCKSS ist ein Peer-to-Peer-Netzwerk und nutzt einen Konsensalgorithmus. Dieser funktioniert jedoch prinzipiell anders als bei Blockchains.

3 Die Zeitschrift «The Economist» widmete der Blockchain-Technologie eine Frontseite unter dem Titel «The Trust Machine» (The Economist 2015)

4 Eine Darstellung der Vielfalt des Blockchain-Ökosystems bietet zum Beispiel Swan (2015).

5 Siehe dazu zum Beispiel das «Crypto Anarchist Manifesto» von May (1992) und die «Declaration of the Independence of Cyberspace» von Barlow (1996).

Economy, denen es Blockchain-Anwendungen wie Bitcoin ermöglichen, die Gebühren und Restriktionen zu umgehen, die ihnen Intermediäre (zum Beispiel Kreditkarten-Institute und Zahlplattformen wie PayPal) zur Vermittlung von Transaktionen auferlegen. Heute dominieren allerdings die grundsätzlichen Zweifel an den etablierten Vertrauensmodellen, die Vertrauenswürdigkeit in der digitalen Kommunikation fast ausschliesslich über vertrauenswürdige Dritte definieren.[6] Viele Anbieter von Internet-Technologien erachten dieses *mittelbare* Vertrauen angesichts einer zunehmenden Kompromittierung der Internet-Infrastrukturen durch geheimdienstliche, militärische und kriminelle Akteure nicht mehr als taugliche Grundlage für die Digitalisierung der Wirtschaft und das «Internet der Dinge». Das «Internet of Things» (IoT) meint die selbständige Interaktion zwischen Geräten unterschiedlichster Art, Hersteller und Besitzer über das Internet. (Man denke zum Beispiel an selbstfahrende Automobile, die mit den Fahrzeugen und Verkehrsinfrastrukturen in ihrer Umgebung kommunizieren und autonom Entscheidungen fällen.) Dazu sei hier exemplarisch IBM (Pureswaran 2015, pp. 5,11) zitiert:

> *The Internet was originally built on trust. In the post-Snowden era, it is evident that trust in the Internet is over. The notion of IoT [Internet of Things] solutions built as centralized systems with trusted partners is now something of a fantasy. Most solutions today provide the ability for centralized authorities, whether governments, manufacturers or service providers to gain unauthorized access to and control devices by collecting and analyzing user data. […] In our vision of a decentralized IoT, the blockchain is the framework facilitating transaction processing and coordination among interacting devices. Each manages its own roles and behavior, resulting in an "Internet of Decentralized, Autonomous Things" – and thus the democratization of the digital world.*

Von der Blockchain-Technologie wird behauptet, sie werde die Nutzung des Internets grundlegend verändern und bedeute den Übergang vom «Internet der Informationen» zum «Internet der Werte und Rechte» (Tapscott & Tapscott, 2016). So schreibt zum Beispiel das britische Government Office for Science zu Handen der Regierung (Walport 2016):

> *Distributed ledger technology has the potential to transform the delivery of public and private services […] to redefine the relationship between government and the citizen in terms of data sharing, transparency and trust […] and] the potential to disrupt the whole economy, and society […] and generally ensure the integrity of government records and services.*

6 Public Key Infrastrukturen, z.B. qualifizierte elektronische Signaturen. Darstellungen von Vertrauensmodellen der digitalen Kommunikation finden sich zum Beispiel bei Cofta (2007) und Sel (2015).

Szenarien wie die oben zitierten stellen auch herkömmliche Prinzipien in Frage, nach denen die Vertrauenswürdigkeit von Records heute beurteilt wird, insbesondere jenes der Verantwortung für die Obhut (custody) über Records durch eine natürliche oder juristische Person (custodian). Das Vertrauensmodell, welches dem Records Management nach heutigem Verständnis zugrunde liegt, basiert wesentlich auf drei Prinzipien (vgl. z.B. Couture & Lajeunesse, 2014; Gilliland 2000):

- *Nachvollziehbarkeit:* Records werden über ihren ganzen Lebenszyklus (von der Erzeugung über die Aufbewahrung bis zur Vernichtung oder Archivierung) in kontrollierten, geeigneten organisatorischen und technischen Umgebungen (Prozesse, Regeln und Infrastrukturen) geführt und aufbewahrt.
- *Verantwortlichkeit:* Records befinden sich in der Obhut (*custody*) einer zuständigen Organisation (*custodian*), die die Aufsicht über die Records wahrnimmt und die uneingeschränkte Verantwortung für ihre Aufbewahrung trägt.
- *Kontinuität:* Eine Übertragung der Verantwortlichkeit für Records im Verlaufe des Lebenszyklus, zum Beispiel an eine Folgeorganisation, muss lückenlos und nachvollziehbar geschehen (*unbroken chain of custody*).

Das Prinzip der lückenlosen Aufsicht über Records bzw. die *unbroken chain of custody* ist eines der ältesten Paradigmen der modernen Archivwissenschaft (vgl. z.B. bei Jenkinson (1922)) und hat angesichts der hohen Volatilität und leichten Veränderbarkeit digitaler Daten stark an Bedeutung gewonnen. Insbesondere das Prinzip der Verantwortlichkeit setzt voraus, dass der Eigner der Records genügend Verfügungsgewalt über die zu ihrer Erstellung und Aufbewahrung verwendeten Umgebungen hat: Ein Unternehmen kann zur Aufbewahrung der Records zwar die Dienstleistungen und Infrastrukturen von Dritten nutzen, jedoch an diese nicht die Verantwortung und Haftbarkeit für die Erfüllung gesetzlicher Rechenschafts-, Nachweis- und Sorgfaltspflichten mit Hilfe authentischer und integerer Records delegieren. Den Mangel an Verfügungsgewalt über die Umgebungen des Dritten muss der Eigner der Records im Sinne einer Risikoabwägung durch vertragliche Vereinbarungen kompensieren.

Im Falle einer Blockchain haben die am Netzwerk teilnehmenden Handelspartner und Betreiber grundsätzlich *keinerlei* Verfügungsgewalt über die technische Umgebung, in welcher die Records erzeugt und aufbewahrt werden (also das Blockchain-System). Das oben skizzierte, klassische Vertrauensmodell der Archivtheorie lässt sich auf die in einer Blockchain aufgezeichneten Records nur anwenden, wenn dabei akzeptiert wird, dass der *custodian* ohne Einschränkungen ein technischer Automat sein kann, der kein Surrogat einer natürlichen oder juristischen Person ist.

Ein solches Verständnis dürfte in der archivwissenschaftlichen Diskussion auf erheblichen Widerspruch stossen. Allerdings waren die unterschiedlichen Sichtweisen auf die Vertrauenswürdigkeit von Urkunden und die Regeln zum angemessenen Umgang mit ihnen in den vergangenen Jahrhunderten immer Produkte ihrer Zeit und wurden durch technologische Veränderungen stark beeinflusst. So könnte auch diese neue Technologie zu einer Änderung der Sichtweise auf Vertrauenswürdigkeit im Records Management führen. Bisher findet die Blockchain-Technologie in der Fachliteratur zu Records Management jedoch kaum Niederschlag.[7]

Vertrauenswürdigkeit im Records Management

Schriftliche Aufzeichnungen sind seit Jahrtausenden ein fundamentales Vehikel zur Begründung und Bezeugung von Eigentum, Macht, Ansprüchen und Pflichten von Individuen und Körperschaften, zum Nachweis von Rechtsverhältnissen, zur Übertragung von Rechten und zur Legitimation von Besitz sowie als Mittel und Quelle der Geschichtsschreibung. Die Beurteilung der Vertrauenswürdigkeit von Urkunden ist deshalb seit jeher ein zentraler Aspekt der Rechtsprechung, des Handels und der historischen Forschung. Die Vorstellungen darüber, was die Vertrauenswürdigkeit einer Urkunde ausmacht und wie diese zu beurteilen ist, haben sich dagegen über die Jahrhunderte stark verändert. Die systematische Unterscheidung zwischen der Authentizität (Echtheit und Integrität) einer Urkunde und ihrer Zuverlässigkeit (Wahrheit der in ihr festgehaltenen Sachverhalte) etablierte sich erst nach dem 15. Jahrhundert (MacNeil 2000). Vorher war Vertrauenswürdigkeit im Wesentlichen an die Authentizität der Urkunde gebunden, also den Nachweis ihrer Echtheit (Identität und Autorität des Erstellers, Zeitpunkt und Ort ihrer Erstellung, formale und inhaltliche Merkmale) und ihrer Integrität (Unverändertheit seit der Erstellung).

Das älteste Konzept der Authentifizierung (Nachweis der Echtheit) von Urkunden ist ihre Aufbewahrung an einem *besonderen Ort*. Im Staatsverständnis des antiken Griechenland hatte es sich dabei nicht nur um einen zweckmässigen, sondern auch um einen *öffentlichen* Ort zu handeln (Tschan 2015). Spätestens in der römischen Urkundenwirtschaft des *Corpus Iuris Civilis* im 6. Jahrhundert wurde die authentifizierende Wirkung des öffentlichen Ortes (Archiv oder Tempel) durch kodifizierte Regeln und Formvorschriften (Floskeln) ergänzt, mit denen vertrauenswürdige Urkunden erstellt und von dazu autorisierten Personen bezeugt werden mussten, um dem Deponieren von Fälschungen vorzubeugen. (Duranti 1996; MacNeil 2000) Im Mittelalter verlor die authentifizierende Wirkung des Aufbewah-

7 Dem Autor ist nur eine Fachpublikation zum eigentlichen Thema bekannt: Lemieux (2016) untersucht mit denselben methodischen Grundlagen wie diese Arbeit die *«limitations, risks and opportunities presented by this new technology»*.

rungsortes jedoch rasch an Bedeutung: Die Siegelwirtschaft und das Notariatswesen verliehen den Urkunden Mobilität durch das Anbringen von hoheitlichen Siegeln oder die eigenhändige Ausfertigung und Beglaubigung der Urkunde durch einen autorisierten Notar nach komplizierten Formvorschriften, die durch Laien nur schwer nachzuahmen waren. Die Urkunden konnten fortan leichter ihren Besitzer wechseln, was die Unterscheidung zwischen Besitzer, Eigentümer und Aussteller einer Urkunde erschwerte und Fälschungen beliebt machte. Die Siegelverfahren und Kanzleiregeln waren an ihre Zeit und lokale Gepflogenheiten gebunden, was die Beurteilung der Echtheit einer älteren Urkunde weiter erschwerte.

Im 16. und 17. Jahrhundert entwickelte sich eine eigentliche Urkundenlehre zur Beurteilung der Authentizität von alten (Rechts-)Urkunden mit Hilfe ihrer Typisierung und Überlieferungsgeschichte, der Prüfung ihrer materiellen, formalen, strukturellen und inhaltlichen Merkmale und dem Wissen über die gebräuchlichen Abläufe bei ihrer Herstellung und den dabei beteiligten Personen und benutzten Hilfsmitteln. Mit dieser mittelalterlichen Urkundenlehre, auch als «Diplomatik»[8] bezeichnet, etablierte sich das Verständnis, dass die Authentizität von Urkunden nur durch eine systematische Untersuchung (Authentifizierung) an Hand von Kriterien *geschlussfolgert* werden kann. Im Rationalismus des 17. und 18. Jahrhunderts setzte sich zudem die Ansicht durch, dass das Resultat dieser Schlussfolgerungen nur als Aussage über eine *Wahrscheinlichkeit* verstanden werden kann, dass die Urkunde authentisch ist.

Im kontinentaleuropäischen Kontext hat sich die Weiterentwicklung des Records Management unter der Bezeichnung «Schriftgutverwaltung» an der Überlieferungsbildung durch staatliche Archive orientiert, welche Unterlagen der Verwaltung archivieren, das heisst bewerten, übernehmen, erschliessen und dauerhaft erhalten und zugänglich machen. Unter diesem Aspekt wurde die mittelalterliche Diplomatik in der Neuzeit unter anderem in den Arbeiten von Duranti (1991) zur *archivischen* Diplomatik (*archival diplomatics*) weiterentwickelt. Nach Menne-Haritz (2011, S. 47) untersucht die Archivwissenschaft mit Hilfe der archivischen Diplomatik *«die Funktionen der verschiedenen Schriftgutformen in den Entscheidungsprozessen der Verwaltung in verschiedenen Zeiten und Staatsformen und wird damit zu einer Verwaltungswissenschaft»*.

Für die Entwicklung des Records Management war das Entstehen der Massenproduktion von Dokumenten in staatlichen Bürokratien entscheidend: Während eine mittelalterliche Urkunde als Einzelstück autonom für den in ihr nachgewiesenen, beurkundeten Akt oder Sachverhalt stand, produziert das Verwaltungshandeln in Bürokratien grosse Mengen an Dokumenten, von denen das einzelne nur

8 Zur klassischen Diplomatik als historische Hilfswissenschaft siehe zum Beispiel Rohr (2015).

Teile eines Verwaltungsakts oder eines Sachverhalts dokumentiert. Erst das Kollektiv mehrerer Dokumente im gemeinsamen Entstehungs- und Nutzungszusammenhang ermöglicht die Nachweisbarkeit des Sachverhalts. Dieser gemeinsame *Geschäftskontext* bildet das «archivische Band» (*archival bond*), das die Dokumente als Kollektiv zusammenhält. In den Worten von Duranti (1997, S. 216):

> *The archival bond is originary, because it comes into existence when a record is created (i.e., when, after being made or received, it is set aside in the fonds of the physical or juridical person who made or received it for action or reference), necessary, because it exists for every record (i.e., a document can be considered a record only if it acquires an archival bond), and determined, because it is qualified by the function of the record in the documentary aggregation in which it belongs. […] The archival bond can be revealed by either the physical order of the records, their classification code or their registration number.*

Erst das archivische Band macht ein Dokument zu einem Record. Damit verschiebt sich der Fokus der Vertrauenswürdigkeit von den *Eigenschaften* des einzelnen Dokuments auf die *Tätigkeit* des Registrierens bzw. die Zuordnung des Dokuments zu einem Geschäftskontext und die dauerhafte Bewahrung desselben. Der Bergiff der vertrauenswürdigen Urkunde, die ganz bestimmte Eigenschaften aufweisen muss und nach ganz bestimmten Regeln erstellt werden muss, verliert somit weitgehend seine Bedeutung. Die Authentizität und Zuverlässigkeit (d.h. Vertrauenswürdigkeit) eines einzelnen Dokuments ergibt sich vielmehr aus dem Kontext aller anderen, im selben Geschäftskontext stehenden Dokumente.

Digitale Diplomatik

Digital erstellte, aufbewahrte und übermittelte Dokumente haben Eigenschaften, die für die archivische Diplomatik eine neue Herausforderung darstellen. Dazu gehören

- die beliebig häufige, bit-identische Replikation,
- die Unabhängigkeit der Information vom Informationsträger,
- das Auseinanderfallen von Aufzeichnungsform (Speicherung) und Darstellungsform (*rendering*) einerseits sowie von Inhalt (*content*) und Kontext (Metadaten) andererseits,
- die fragile technische Integrität, die durch die Änderung eines einzelnen Bits zerstört wird,
- die Erzeugung von Records durch Softwaresysteme (wie zum Beispiel in einer Blockchain-Anwendung) anstelle von Menschen sowie
- das Fehlen fixer Darstellungsformen zum Beispiel für Daten in Datenbanken.

Insbesondere das Fehlen einer fixen (oder eindeutigen) Darstellungsform digitaler Informationen führt dazu, dass sich das «Archivische Band» häufig nicht mehr bilden lässt. So stellt sich zum Beispiel die Frage, was bei einer durch Eingabemasken oder Formulare gesteuerten Datenbank-Anwendung die vertrauenswürdigen Records sind. Sind es die in der Datenbank gespeicherten Datensätze, die auf der Maske zum Zeitpunkt der Eingabe sichtbaren Informationen, die Eingabemaske selber oder die Definition des Formulars, das die Daten nach den immer gleichen Regeln darstellt? Oder eine Kombination dieser Elemente?

Duranti (2005, 2007, 2009) und das von ihr geleitete Projekt «The International Research on Permanent Authentic Records in Electronic Systems»[9] InterPARES (InterPARES 2001) haben die spezifischen Merkmale und Problemstellungen digitaler Dokumente basierend auf der von Duranti (1991) formulierten archivischen Diplomatik untersucht. Duranti ist der Meinung, dass deren Prinzipien und Vorgehen auch bei *digitalen* Unterlagen noch Bestand haben, wenn dabei die technischen und prozeduralen Besonderheiten digital aufgezeichneter Informationen berücksichtigt werden. Die *Digitale Diplomatik* hat dazu das analytische Instrumentarium zur Analyse der zentralen Begriffe der Vertrauenswürdigkeit – Authentizität und Zuverlässigkeit – erweitert und geschärft, damit es auf die besonderen Umstände digitaler Informationen systematisch angewendet werden kann. Zu den Schwerpunkten dieser Erweiterung gehört der kritische Einbezug der technischen (speicherbezogenen) Integrität in das archivtheoretische Verständnis der Vollständigkeit und Unveränderthеit von Dokumenten: Die Verwendung digitaler «Fingerabdrücke» (kryptografische Hashwerte) als strenges Merkmal der Integrität scheitert etwa bei Formatkonversionen von Dokumenten und bei der in digitalen Informationssystemen allgegenwärtigen Trennung zwischen der technischen Speicherform und der durch Menschen wahrnehmbaren Darstellungsform (*rendering*) der Daten.

Ein Schwerpunktthema der Digitalen Diplomatik ist insbesondere auch die Rolle von Metadaten. Digitale Dokumente und Informationen lassen in der Regel nur noch eine attributierte Authentizität zu, also in Form von Merkmalen, die nicht mehr in das Dokument selber integriert oder mit diesem fest verbunden sind, sondern als separate und vom Dokument leicht lösbare Speicherobjekte (Metadaten) existieren. Das erwähnte archivische Band, das Dokumente erst zu Records macht, kann im Gegensatz zu den Schachteln und Ordnern der Papierwelt nun nur noch virtuell dargestellt, geführt und erhalten werden.

9 http://www.interpares.org. InterPARES hatte bisher vier Projektzyklen (1998 – 2001, 2002 – 2007, 2007 – 2012 und 2013 – 2018).

Grundsätzlich sind zur Beurteilung der Vertrauenswürdigkeit von Records jedoch dieselben Kontexte zu betrachten, die bereits von der archivischen Diplomatik formuliert wurden, nun allerdings mit einer stärkeren Betonung des technologischen Kontexts. Jeder Kontext setzt entsprechendes Wissen über die Organisationen und Prozesse voraus, die an der Erstellung (Erzeugung, Empfang, Bearbeitung, Aufbewahrung) der Records beteiligt waren (Duranti & Rogers, 2012; InterPARES 2001; MacNeil 2000):

- **Rechtlich-administrativer Kontext**: rechtliches und organisatorisches System, in dem die Organisation existiert(e).
- **Provenienz-Kontext**: Verfassung und Aufbau der Organisation sowie ihre Funktionen und Aufgaben während der Lebenszeit der Records.
- **Prozeduraler Kontext**: Geschäftsprozesse und Arbeitsabläufe, in bzw. mit denen die Records erstellt und empfangen bzw. aufbewahrt wurden.
- **Dokumentarischer Kontext**: Art und Weise der Identifikation der Records sowie ihre innere Ordnung, d.h. die Darstellung von strukturellen Abhängigkeiten zwischen den Records, zum Beispiel in Form eines Registratur- oder Aktenplanes (*records filing system*).
- **Technologischer Kontext**: Infrastrukturen (Hilfsmittel und Materialien), mit denen die Records erstellt, geführt und aufbewahrt wurden, z.B. Hardware- und Software-Umgebungen.

Records Management

Das Augenmerk des modernen Records Management gilt der korrekten Bildung des archivischen Bandes und der Vollständigkeit des dadurch zusammen gehaltenen Kollektivs von Dokumenten im gemeinsamen Geschäftskontext. Diese *Tätigkeit* hängt von Fähigkeiten, Möglichkeiten und Verhaltensweisen der Personen ab, die sie ausführen. Records Management verfolgt deshalb vor allem das Ziel, die Korrektheit dieser Tätigkeit zu regeln und soweit möglich durch technische Hilfsmittel zu erzwingen und zu kontrollieren.

> *Contemporary archival diplomatics aims primarily to control concrete manifestations of recordkeeping reality, while the legal and historical principles and rules of evidence aim to evaluate those manifestations. […] The computer has become the perfect observer, with its capacity to witness and capture the actions and interactions of recordkeepers on a microscopic scale. (MacNeil 2000, Seiten 112, 116)*

Das praktische Records Management versteht Duranti (2010) denn auch ausdrücklich als die Pragmatik der archivischen Diplomatik (*«[…] records management theory is archival diplomatics»*). Diese regelnde, führende und kontrollierende Natur des praktischen Records Management (Schriftgutverwaltung, Aktenführung)

kommt in der internationalen und Schweizer Norm SN ISO 15489 «Records Management» (ISO 2001) klar zum Ausdruck:[10]

> *Als Führungsaufgabe wahrzunehmende effiziente und systematische Kontrolle und Durchführung der Erstellung, Entgegennahme, Aufbewahrung, Nutzung und Aussonderung von Schriftgut einschließlich der Vorgänge zur Erfassung und Aufbewahrung von Nachweisen und Informationen über Geschäftsabläufe und Transaktionen in Form von Akten.*

Tatsächlich ist die Begrifflichkeit dieser Norm weitgehend identisch mit jener der Digitalen Diplomatik, da sich die Autorinnen und Autoren bewusst an diesen archivwissenschaftlichen Grundlagen orientiert haben. Danach gilt ein Record *unabhängig von Form und Datenträger* als vertrauenswürdig, wenn er fünf überprüfbare Eigenschaften erfüllt (ISO 2001):

- **Authentizität**: Der Record muss echt sein, also nachweislich das darstellen, was er zu sein vorgibt (z.B. ein Vertrag zwischen den genannten Parteien über den genannten Vertragsinhalt). Echtheit ist das Gegenteil von Fälschung und bedingt prüfbare Angaben zur Provenienz (Herkunft), zu den Identitäten der an seiner Erstellung, Verteilung und Aufbewahrung beteiligten Personen sowie zu Zeitpunkten seiner Erstellung und seines Versands bzw. Empfangs.
- **Integrität**: Der Record muss bezüglich seiner ursprünglich vorhandenen Inhalte und Komponenten nachweislich unverändert und vollständig sein. Nachträglich angebrachte Zusätze müssen als solche erkennbar sein. Dieser Begriff geht somit über die rein technische Integrität eines einzelnen Dokuments hinaus.
- **Zuverlässigkeit**: Der Record muss eine glaubwürdige, vollständige, genaue Wiedergabe der darin nachgewiesenen Transaktionen, Aktivitäten und Tatsachen sein und als verlässliche Grundlage für folgende Aktivitäten und Entscheidungen dienen können.
- **Benutzbarkeit**: Der Record muss inventarisiert (d.h. eindeutig identifizierbar), auffindbar, darstellbar und verstehbar sein, und in seiner Darstellungsform soll die direkte Verbindung mit den geschäftlichen Aktivitäten oder Transaktionen erkennbar sein, in denen er erzeugt wurde.
- **Statische Dokumentationsform**: Der Record muss eine oder mehrere bekannte, statische Darstellungen haben, die seine ursprüngliche Nutzung in Geschäftsprozessen adäquat wiedergeben. Dies betrifft seine Struktur (Beziehungen zwischen Bestandteilen), sein Format, seinen Geschäftskontext

10 Deutsche Fassung zitiert nach DIN ISO 15489 Schriftgutverwaltung (DIN 2002).

(Erzeugung, Nutzung) sowie Verweise auf zugehörige, gesondert aufbewahrte Records.

Diese Eigenschaften muss ein Record *über seine ganze Lebenszeit* behalten, von der Erzeugung (Erstellung oder Empfang) bis zum Ende der Aufbewahrungszeit. Ein Record kann durch seine Authentifizierung nicht zuverlässiger werden, als er es bereits zum Zeitpunkt seiner Erstellung war. Der Nachweis (‹Beweisführung›) der Authentizität wird Authentifizierung (des Records) genannt. Wie dieser Nachweis zu führen ist und was die anzuwendenden, konkreten ‹Messkriterien› zu den oben genannten Qualitätsmerkmalen sind, lässt der Standard offen. Er besagt jedoch, dass jede Organisation diese Kriterien bei der Einführung des Records Management festlegen muss, ausgehend von den für sie relevanten rechtlichen und betrieblichen Anforderungen. Rechenschafts-, Nachweis- und Aufbewahrungspflichten finden sich in den am Geschäftsort des Unternehmens geltenden nationalen Rechtsnormen zum Beispiel im Steuer-, Handels-, Datenschutz-, Haftpflicht-, Produktesicherheits-, Sozial-, Versicherungs- und Arbeitsrecht, aber auch im internationalen Recht und in branchenspezifischen Regulierungen. Für archivwürdige Geschäftsunterlagen staatlicher Institutionen verlangen Archivgesetze deren dauerhafte Archivierung in staatlichen Archiven zur Gewährleistung der Rechtssicherheit und der Nachvollziehbarkeit staatlichen Handelns sowie als Voraussetzungen für die historische und sozialwissenschaftliche Forschung.[11]

Wesensmerkmale und Typologie von Blockchains

Bevor die Vertrauenswürdigkeit von Blockchains an Hand der bisher diskutierten Kriterien beurteilt werden kann, müssen die wesentlichen Merkmale einer Blockchain bekannt sein. Der Begriff «Blockchain» wurde erstmals im Konzeptpapier *«Bitcoin: A Peer-to-Peer Electronic Cash System»* (Nakamoto 2008) eingeführt[12], um einen Teil des Bitcoin-Systems zu definieren. Dieses Konzept nutzt ausschliesslich Technologien, die bereits vorher bekannt und gebräuchlich waren. Das innovative Element war vielmehr die geschickte Auswahl und Kombination solcher Technologien zur konsistenten Propagierung von Zuständen in einem verteilten System. Der Versuch etwa von Swan (2015), den Begriff «Blockchain-Technologie» *ohne* Rückgriff auf Bitcoin zu fassen, führt zu eher pauschalen Aussagen. Demnach ist eine Blockchain

11 In der Schweiz ist dies für Bundesbehörden im Bundesgesetz über die Archivierung (BGA, SR 152.1) geregelt: «Rechtlich, politisch, wirtschaftlich, historisch, sozial oder kulturell wertvolle Unterlagen des Bundes werden archiviert.» (Art. 2 Abs. 1 BGA) Analoge gesetzliche Grundlagen regeln die Archivierung auf kantonaler und kommunaler Ebene.

12 Dieses Konzept wurde von einer bis heute nicht identifizierten Person oder Personengruppe unter dem Pseudonym «Satoshi Nakamoto» 2008 an eine Kryptografie-Mailingliste geschickt.

— ein unveränderliches, permanentes Buchungsjournal (*ledger*),
— das als identische Kopie auf vielen, in einem Netzwerk lose und mehr oder weniger zufällig verbundenen Rechnern existiert,
— öffentlich oder mindestens von allen am Netzwerk beteiligten Rechnern eingesehen werden kann und
— durch kryptografische Verfahren so abgesichert ist, dass
— die darin aufgezeichneten Transaktionen für alle oder zumindest die am Netzwerk Beteiligten als vertrauenswürdig gelten können,
— ohne dass dazu eine natürliche oder juristische Person als vertrauenswürdiger Dritter zur Authentifizierung der Transaktionen benötigt wird.

Das ist weitgehend eine Formulierung von *Systemzielen* statt die Beschreibung einer Technologie[13] (Systemkonzept und Verfahren) zur Realisierung dieser Ziele. Tatsächlich wird in der Literatur überwiegend auf die Beschreibung der Bitcoin-Blockchain und des Bitcoin-Systems zurückgegriffen, um die technische Funktionsweise einer Blockchain-Anwendung zu erläutern.[14] Die Floskel *«Blockchain-Technologie ist die Technologie hinter Bitcoin»* muss deshalb weitgehend als Tautologie gesehen werden: Die Spezifikation der Bitcoin-Blockchain *ist* die Technologie oder stellt zumindest den Archetyp der Blockchain dar. Gewisse Elemente dieser Technologie sind allerdings austauschbar (zum Beispiel die verwendeten kryptografischen Methoden), erweiterbar (etwa zur Beseitigung der für Bitcoin typischen Anonymität der am Netzwerk beteiligten Personen) und analog einsetzbar (insbesondere zur Übertragung von Werten und Rechten jenseits einer digitalen Währung). Die möglichen Abweichungen vom technischen Konzept der Bitcoin-Blockchain scheinen aber gering. Dies zeigt auch ein Vergleich der Bitcoin-Blockchain mit anderen Blockchains wie zum Beispiel «Ethereum»[15] oder dem Projekt «Hyperledger»[16] der Linux Foundation. Die Ankündigung eines ISO-Standards zur Blockchain-Technologie kann hier die nötige begriffliche Klärung bringen.[17]

Nach einem Vergleich der Bitcoin-Blockchain mit anderen Blockchains schlägt der Autor[18] die folgende Konkretisierung der wesensbestimmenden Merkmale des Begriffs «Blockchain» vor.

13 Man vergleiche dies zum Beispiel mit präzisen Beschreibungen der «Datenbank-Technologie».

14 Technisch präzise und umfassende sprachliche Beschreibungen einer Blockchain am Beispiel der Bitcoin-Blockchain finden sich zum Beispiel bei Antonopoulos (2015) und Franco (2015). Eine algorithmische Definition findet sich bei Wattenhofer (2016). Vollständig und unzweideutig ist das Bitcoin-System jedoch nur durch seinen offenen Software-Quellcode definiert, der unter der Adresse https://github.com/bitcoin/bitcoin einsehbar ist.

15 https://ethereum.org

16 Eine Kooperation von über 60 Industriepartnern, um die Entwicklung der Blockchain-Technologie als OpenSource-Projekt zu etablieren (https://www.hyperledger.org).

17 https://www.iso.org/news/Ref2188.htm (24.05.2017)

18 Dieser Aufsatz basiert auf der Masterarbeit «Blockchains als Herausforderung und Instrument des Records Management – Kritische Würdigung verteilter, kryptographisch gesicherter Transaktions-

— **Verfügbarkeit:** Die Verwendung eines Verbundnetzwerkes unabhängiger, verteilter und direkt miteinander kommunizierender Computersysteme ermöglicht, dass die Blockchain auch beim Ausfall zahlreicher Computersysteme im Netzwerk jederzeit und von jedem Ort aus erreichbar bleibt. Jeder Rechner verfügt über eine vollständige lokale Kopie der gesamten, aktuellen Blockchain, die er selber komplett validiert hat.
— **Eindeutiger Transaktionskontext:** Die Authentifizierung der Transaktionspartner (die selber auch technische Systeme sein können), die Unveränderlichkeit der aufgezeichneten Informationen und deren Identifikation durch kryptografische «digitale Fingerabrücke» (Hashwerte) liefern für jede Transaktion einen universell eindeutigen, nach der Authentifizierung unveränderlichen Kontext.
— **Identität:** Urheber von Transaktionen verfügen über einen oder mehrere asymmetrische kryptografische Schlüsselpaare. Die öffentlichen Schlüssel dienen als Identitäten der Transaktionspartner.
— **Authentifizierung:** Einige oder alle Rechner im Netzwerk können als Prüfer agieren, die Transaktionen authentifizieren. Die Authentifizierung einer Transaktion besteht aus der Prüfung ihrer Gültigkeit (Form, Struktur, Inhalt). Die Resultate der Prüfmerkmale zur Gültigkeit einer oder gleichzeitig mehrerer Transaktionen, insbesondere der Zeitpunkt der Prüfung, bilden zusammen als Metadaten eine Einheit bzw. «Block», den der Prüfer mit dem privaten Schlüssel seines asymmetrischen Schlüsselpaars signiert und ins Netzwerk propagiert, damit er an die Blockchain angefügt werden kann.
— **Homogenität und zeitliche Ordnung:** Eine Blockchain ist eine chronologische Aneinanderreihung von solchen einheitlich strukturierten und serialisierten Blöcken. Die Reihenfolge, in welcher die Blöcke verkettet werden, ist eindeutig und unveränderlich, weshalb jede Blockchain ein Journal ist.
— **Block-Integrität:** Die Identität eines Blocks ist sein kryptografischer Hashwert. Jeder von einem Prüfer signierte Block enthält auch die Identität (den Hashwert) des aktuell letzten Blocks in der Blockchain. Diese Verkettung der Identitäten (woraus sich der Name Blockchain ableitet) gewährleistet die Integrität der Blockchain als Ganzes.
— **Transaktionalität:** Die in einem Block der Blockchain aufgezeichneten «Transaktionen» sind Transitionen einer Zustandsmaschine: Die Ausführung einer Transaktion (Authentifizierung und Einschreibung in die Blockchain)

journale in Bezug auf die Vertrauenswürdigkeit digitaler Records» (31.6.16) im Studiengang Master of Advanced Studies in Archiv-, Bibliotheks- und Informationswissenschaften der Universitäten Bern und Lausanne.

erfüllt die ACID-Eigenschaften[19] und überführt die Blockchain von einem konsistenten (gültigen) Zustand in den nächsten. Dabei kann die C-Eigenschaft (*consistency*) auch asymptotisch erfüllt werden, also mit einer an Sicherheit grenzenden Wahrscheinlichkeit erst nach probabilistisch abschätzbarer Zeit (*eventual consistency*).

— **Logische Ordnung:** Jede Transaktion bezieht sich auf eine oder mehrere Vorläufer-Transaktionen, und jede Transaktion enthält das selbe Attribut oder *Token*, welches den Inhalt bzw. Sachverhalt der Transaktion bestimmt. Der Zustand der Blockchain besteht aus den Attributwerten aller Transaktionen sowie allen logischen Bezügen der Transaktionen untereinander.
— **Verlässlichkeit:** Nachdem eine Transaktion durch einen Prüfer erfolgreich validiert und in die Blockchain eingeschrieben wurde, so muss sie mit Hilfe ihres Nachweises in der Blockchain auch später erfolgreich validierbar sein.
— **Authentizität:** Die dauerhafte Nachweisbarkeit der Authentizität der Blockchain hängt nicht davon ab, dass alle Prüfer, die Transaktionen authentifizieren (Merkmal 3), allesamt ehrlich und fehlerfrei agieren, sondern auf der Bildung eines Konsens unter allen Rechnern des Netzwerks über die Gültigkeit jedes neuen Blocks, wozu alle Rechner demselben, geeigneten Verfahren (Konsensalgorithmus) folgen. Erst nachdem dieser Konsens als erreicht gilt, betrachten die Rechner den neuen Block als Teil der Blockchain.
— **Blockchain-Integrität:** Die dauerhafte Integrität der Blockchain wird einerseits durch die Verkettung der Identitäten (Hashwerte) der Blöcke (Merkmal 6) gewährleistet, andererseits durch den Konsensalgorithmus (Merkmal 10), der bewirkt, dass Aufwand und/oder Zeit zur Erzeugung und Bestätigung eines neuen Blocks (Merkmale 4 und 9) zu gross sind, um die Blockchain nachträglich neu (in anderer Form) zu erzeugen.

Nicht wesensbestimmende Merkmale einer Blockchain, jedoch von grosser *praktischer* Bedeutung sind die Art des verwendeten Konsensalgorithmus', die Art der kryptografischen Schlüsselpaare der Transaktionspartner im Merkmal 3 (insbesondere, ob sie nur technische Identitäten sind oder Rückschlüsse auf Personen zulassen) sowie die Art des Anreizes für Prüfer im Merkmal 11, Transaktionen zu au-

19 Über den Begriff Transaktion im Rahmen von Informatiksystemen herrscht seit seiner Einführung in den 1960er-Jahren weitgehend Einigkeit. Es handelt sich um eine Interaktion zwischen einem Client und einem Server, bei dem der Client eine Sequenz von Befehlen an den Server sendet, dessen Systemzustand durch die Ausführung dieser Befehle von einem konsistenten (gültigen) Datenzustand in einen neuen, ebenfalls konsistenten Zustand versetzt wird, den der Server dem Client anschliessend bestätigt. Dabei gelten vier grundlegende Eigenschaften, welche die Transaktion erfüllen muss (vgl. z.B. Tanenbaum & van Steen, 2002): *atomic* (atomar), *consistent* (konsistent), *isolated* (isoliert) und *durable* (dauerhaft), abgekürzt ACID.

thentifizieren und somit den damit verbundenen Rechenaufwand in Kauf zu nehmen, der erheblich sein kann.

Das Merkmal 8 (Logische Ordnung der Transaktionen) bestimmt das fachliche Ziel der Blockchain. In Bitcoin ist dies einfach zu verstehen: Der Zweck ist, einen bestimmten Bitcoin-Wert an eine Empfänger-Adresse zu überwiesen, zum Beispiel 0.5 BTC. «Überweisen» heisst in Bitcoin jedoch nur, dass der Sender seinen *Besitz* an einem oder mehreren Bitcoin-Werten, die zusammen mindestens 0.5 BTC ausmachen, an eine neue Bitcoin-Adresse überträgt. Den Besitz an diesen Werten hat der aktuelle Besitzer seinerseits früher von einem Vorbesitzer bereits übertragen erhalten und so weiter, bis zurück zum Bitcoin-Miner, der diesen Wert erzeugt hat. Dies ist die (bisherige) Transaktionskette des Bitcoin-Wertes. Der bei einer Transaktion übertragene Bitcoin-Wert ist der Wert des 8 Bytes langen Attributs «*Amount*» in einer Transaktion (Antonopoulos 2015) und stellt bei Bitcoin das in Merkmal 8 gemeinte Attribut dar. Es bestimmt, was die Transaktion mit dem Systemzustand «tut», nämlich die Übertragung des Besitzes an einem Bitcoin-Wert. Sämtliche in der Bitcoin-Blockchain aufgezeichneten Transaktionsketten bilden den aktuellen Systemzustand (Besitzzustand aller Bitcoin-Werte), der durch neue Transaktionen (bzw. deren Einschreiben in die Blockchain) von einem konsistenten Zustand in den nächsten überführt wird.

Allgemein bedeutet dies, dass jede Blockchain ein Zustandsautomat ist und Transaktionen somit nur eine endliche Menge von Sachverhalten betreffen können, die vorher definiert wurden und den Anwendungsfall der Blockchain bestimmen. Somit können darin nicht *beliebige* Informationen festgehalten werden, da sich dafür weder ein Systemzustand noch Kriterien für dessen Konsistenz definieren liessen. Die logische Ordnung von Transaktionen (Merkmal 8) ist somit eine Voraussetzung für die Transaktionalität (Merkmal 7) des Gesamtsystems. In einer Transaktion überträgt der Urheber dem Adressaten einen Wert, ein Recht oder ein anderes «Beweiszeichen» (*token*), das für den Adressaten von Bedeutung oder Nutzen ist. Zum Beispiel könnte ein Autovermieter den Besitz an einem virtuellen Schlüssel an einen Kunden (Mieter) übertragen, der damit an einem bestimmten Tag den Motor eines bestimmten Mietwagens starten kann. Die Übertragung des Besitzes am Schlüssel vom Kunden zurück an den Vermieter ermöglicht es diesem, den Wagen an neue Kunden zu vermieten.

Typologie von Blockchains

Aus den im vorangehenden Abschnitt genannten Merkmalen einer Blockchain lassen sich die folgenden fünf Rollen ableiten, die im Gesamtsystem von einzelnen Rechnersystemen eingenommen werden.

— **Prüfer** (in Bitcoin «Miner» genannt) validieren und authentifizieren Transaktionen, indem sie diese in die von ihnen digital signierten Blöcke einbinden, welche sie dann zur Fortschreibung der Blockchain ins Netzwerk propagieren. Sie tun dies, weil sie dazu einen Anreiz haben oder daraus einen Nutzen ziehen (z.B. werden die Bitcoin-«Miner» durch neue Bitcoins belohnt).
— **Validierer** (Router) empfangen Transaktionen, validieren diese und propagieren gültige Transaktionen ins Netzwerk, damit sie von Prüfern authentifiziert und Teil der Blockchain werden können. Jeder Validierer speichert eine volle Kopie der aktuell gültigen Blockchain.
— **Benutzer** sind Auslöser einer Transaktion, die sie an benachbarte Validierer schicken, damit diese sie validieren und weiter ins Netzwerk propagieren. Begünstigte einer Transaktion werden zu Benutzern, wenn sie den ihnen in der Blockchain übertragenen Wert selber in Transaktionen nutzen.
— **Wallets** speichern die Identität(en) eines Benutzers, d.h. seine kryptografischen Schlüsselpaare, und ermöglichen die Erzeugung von Transaktionen.
— **Entwickler** programmieren und unterhalten den Software-Code, der das Blockchain-System technisch vollständig definiert.

Diese Rollen werden durch Computer als Akteure wahrgenommen. Sie können jederzeit ihre Rolle aufgeben oder wechseln, das System verlassen, ihre Identität verschleiern oder auch unehrlich agieren oder das System böswillig attackieren. Das *technische* System funktioniert der Architektur einer Blockchain gemäss autonom und ist nicht beeinflussbar und kompromittierbar. Aus diesem Grund ist die Identität der natürlichen oder juristischen Personen, welche diese Computer besitzen und betreiben, grundsätzlich unerheblich. Sie haben eine dienende, aber keine bestimmende Bedeutung für das Funktionieren des Gesamtsystems. (Das heisst, sie führen den Computern Strom zu und wechseln defekte Teile der Hardware aus.) Das Prinzip der Verantwortlichkeit, welches organisatorische Modelle bestimmt, wird durch die Reduktion von Vertrauenswürdigkeit auf ein autonomes technisches System somit obsolet.

In dieser absoluten Form wird sich eine Blockchain jedoch aus rechtlichen Gründen kaum geschäftlich einsetzen lassen, da schlussendlich jemand Verantwortung für Folgen übernehmen muss, die Transaktionen in der Blockchain ausserhalb der Systemgrenzen für Dritte haben können. Ein offensichtliches Beispiel dafür ist die rechtliche Haftung im «Internet der Dinge», in dem autonom agierende Geräte sich durch eine Blockchain gegenseitig vertrauen. Es macht somit Sinn, Blockchains auch nach *organisatorischen* Betriebsmodellen zu typisieren, also nach den juristischen Personen, welche die Rechnersysteme kontrollieren, die eine bestimmte Rolle im System einnehmen. Dazu wird die strikte Systemautonomie gelo-

ckert, indem den Personen entgegen der «reinen» Blockchain-Theorie mehr Verfügungsgewalt und mehr Möglichkeiten zur Einflussnahme auf das Gesamtsystem zugestanden werden. Dies ist eine Bedingung für die Übernahme von Verantwortung und betrifft zum Beispiel die Möglichkeiten, das Gesamtsystem abzuschalten oder zu bestimmen, welche anderen Personen mit ihren Rechnern am System teilnehmen dürfen und wie sie diese identifizieren müssen.

Diese Einflussmöglichkeiten machen das Gesamtsystem unsicherer, was durch eine Verkleinerung der Systemgrenzen des Netzwerks und die Authentifizierung der Teilnehmenden kompensiert werden soll. Dadurch entstehen im Gegensatz zum komplett offenen und anonymen Blockchain-Modell von Bitcoin mehr oder weniger geschlossene Kooperationsmodelle. In der Literatur wird zwischen «öffentlichen», «privaten» und «hybriden» Blockchains unterschieden. Die folgenden fünf Betriebsmodelle orientieren sich an den Unterscheidungen von Walport (2016) und Pilkington (2015):

	Betriebsmodell	**Beschreibung**
I	**offene öffentliche Blockchain** (public shared ledger) zum Beispiel Bitcoin	Offene Teilnahme beliebiger Rechnersysteme in beliebigen Rollen, ohne Zulassung und Identifizierung der Betreiber. Quellcode ist offengelegt und lizenzfrei nutzbar, die Blockchain-Inhalte sind frei zugänglich.
II	**geschlossene öffentliche Blockchain** (public permissioned shared ledger)	Wie I, jedoch mit zwingender Zulassung und Identifizierung der Besitzer von Rechnersystemen für die Rollen Prüfer oder Validierer. Der Quellcode ist offengelegt.
III	**geschlossene private Blockchain** (private permissioned shared ledger)	Alle Rechnersysteme in allen Rollen haben ein und denselben Betreiber, der zudem auch den Quellcode besitzt.
IV	**geschlossene gemeinschaftliche Blockchain** (community permissioned shared ledger)	Vertraglich gebundene Gemeinschaft unterschiedlicher juristischer Personen, von denen jede einen Teil der Rechnersysteme zu allen oder nur bestimmten Rollen eigenständig betreibt und den Quellcode besitzt.
V	**Dienstleister-Blockchain** (Blockchain-as-a-Service)	Alle Rechnersysteme mit Ausnahme jener in der Rolle Benutzer haben ein und denselben Betreiber. Dieser wie auch die Benutzer besitzen den Quellcode.

Weitere Varianten sind denkbar, vor allem in Bezug auf Offenlegung, Besitz und Eigentum des Quellcodes der Software, der die Blockchain definiert. Der Autor ist der Meinung, dass mindestens die Einsehbarkeit und Prüfbarkeit des Quellcodes durch alle *Betreiber* der Rechnersysteme zwingend ist. Denn ein Ziel einer Blockchain ist die Vermeidung von vertrauenswürdigen Dritten bei der Authentifizierung und Bestätigung von Transaktionen. Dies soll durch Algorithmen, also durch die Software der Blockchain gewährleistet werden. Ist diese Software nicht prüfbar, erschöpft sich die Vertrauenswürdigkeit der Blockchain in einem wie auch immer

gearteten Vertrauen der Benutzer in den Entwickler der Software, der dadurch zu einem solchen vertrauenswürdigen Dritten erhoben würde. Von der Vertrauenswürdigkeit der Blockchain zu unterscheiden ist dagegen die Frage der Haftbarkeit: Sind der Entwickler und der Betreiber einerseits oder der Betreiber und Benutzer andererseits nicht dieselbe juristische Person, so wird der Entwickler gegenüber dem Betreiber bzw. der Betreiber gegenüber dem Benutzer jede Haftung für geschäftlichen Schaden ablehnen, der dem Betreiber bzw. dem Benutzer aus der Nutzung der Blockchain entsteht. Dies gilt jedoch grundsätzlich bei jeder Software.

Eine Blockchain als Gefäss für Records

Nachdem die wesentlichen Eigenschaften einer Blockchain identifiziert wurden, lassen sich die dargestellten wissenschaftlich-methodischen Grundlagen der Digitalen Diplomatik und des Records Management anwenden, um die Vertrauenswürdigkeit von Records in einer Blockchain zu bewerten und die Frage zu beantworten, ob sich eine Blockchain grundsätzlich als Träger von und Aufbewahrungsort für vertrauenswürdige Records eignet. Dabei wird die im letzten Abschnitt vorgestellte Typologie von Betriebsmodellen berücksichtigt.

Der eindeutige Transaktionskontext der Eintragung einer Transaktion in der Blockchain (Merkmal 2 der wesentlichen Eigenschaften einer Blockchain) kann in allen genannten Betriebsmodellen als Registrierung im Sinne des Records Management gelten, wenn (und nur wenn) dieser technische Kontext innerhalb oder ausserhalb der Blockchain mit einem Geschäftskontext (*archival bond*) verknüpft wird, der den Entstehungszusammenhang der Transaktion und alle weiteren, vor oder nachher damit verbundenen Records nachweist. Dies ist aus der Sicht der Blockchain ohne weiteres möglich, da der Transaktionskontext eindeutig und seine Form homogen ist und sowohl den Urheber der Transaktion wie auch deren Inhalt eindeutig identifiziert. Umgekehrt enthält dieser Kontext auch alle Informationen, die seine Registrierung in einem separaten Records Management System ermöglichen (Transaktionsnummer, Zeitpunkt, Urheber, Empfänger, Betreff etc.).

A) Lebenszyklus

In allen Betriebsmodellen spielt sich das «Leben» einer Blockchain-Transaktion vollständig in derselben organisatorischen und technischen Umgebung ab. Erstens erfolgt eine Validierung und Authentifizierung jeder Transaktion, bevor sie in der Blockchain festgeschrieben wird (Merkmale 4 und 5), zweitens erfolgt eine Wiederholung der Validierung der Authentizität und Integrität jedes Blocks und jeder darin aufgezeichneten Transaktion auch durch jeden neuen Teilnehmer im Netzwerk (Merkmal 1).

— Als für die Aufbewahrung *geeignet* darf eine Blockchain gelten, weil dazu keine Migration in ein anderes System benötigt und das Original im eigentlichen Sinne aufbewahrt wird.
— Als *ungeeignet* muss sie allerdings gelten, wenn der Urheber von Blockchain-Records diese nur eine beschränkte Zeit (Aufbewahrungsfrist) aufbewahren und danach löschen will oder muss. Eine Löschung von einzelnen Blockchain-Einträgen ist nicht möglich (Merkmal 6), ohne die Integrität der Blockchain zu zerstören. Die Records müssen dauerhaft in der Blockchain verbleiben. Eine Aufbewahrungsplanung (Retention Management) für Blockchain-Records ist somit nicht möglich. Eine Blockchain kann nur als Ganzes vernichtet werden.
— In den geschlossenen Betriebsmodellen III und IV ist die Löschung (Vernichtung) der *gesamten* Blockchain möglich, in den öffentlichen Modellen I und II und im Service-Modell V dagegen aus naheliegenden Gründen nicht.
— Auch die Archivierung von Blockchain-Records in einem *separaten* Archivsystem ist nicht oder nur sehr eingeschränkt möglich, da der Nachweis der Authentizität und Integrität eines einzelnen Records auf derjenigen der gesamten Blockchain beruht.

Allerdings lässt sich die gesamte Blockchain durchaus einfach unter die Kontrolle einer Archivinstitution bringen, da sich die Institution dazu nur einmalig dem Netzwerk anschliessen muss, um eine auf dem eigenen Rechner gültige und validierte Kopie der Blockchain zu erhalten (Merkmal 1). Diese kann mit der Hilfe der Blockchain-Software anschliessend im Archiv unabhängig aufbewahrt und benutzt werden. Ob dies allerdings in den geschlossenen Betriebsmodellen III und IV und im Service-Modell V möglich ist, hängt von der rechtlichen Vereinbarung zwischen dem (nicht beteiligten) Archiv und den Betreibern der Blockchain ab.

B) Zuständigkeit und Verantwortlichkeit für Records (custody)

In einer öffentlich, geschlossen gemeinschaftlich oder als Service betriebenen Blockchain (Modelle I, II, IV und V) vermischen sich Records unterschiedlicher Provenienzen (Herkunft) im selben Speichermedium (der Blockchain). Provenienzen der Transaktionen vermischen sich auch innerhalb eines einzelnen Blocks (Merkmal 7), und die Integrität eines einzelnen Blocks ist von allen Vorgängerblöcken abhängig (Merkmal 6).

— Eine Separierung von Transaktionen nach Provenienzen ist in allen Modellen nicht ohne Verlust der Authentizität möglich. Dadurch ist in allen Modellen auch keine Separierung der Zuständigkeit für die Aufbewahrung bzw. Obhut (*custody*) nach Provenienz möglich.

— Nur im geschlossenen privaten Modell III haben alle Transaktionen (per Definition) dieselbe Provenienz, weshalb nur in diesem Modell eine Zuständigkeit für die Aufbewahrung der Records eindeutig zugewiesen werden kann.

Eine Zuständigkeit bzw. Verantwortlichkeit für Records bedingt, dass die verantwortliche Stelle genügend Verfügungsgewalt über die Verfahren und Systeme hat, die zur Aufbewahrung eingesetzt werden. Ausserdem setzt eine Aussage über die Zuverlässigkeit von Records entsprechendes Wissen über die in der Digitalen Diplomatik ausgezeichneten fünf Kontexte von Records und ihren Erzeugern und ihren Aufbewahrern voraus, darunter auch das Wissen über den rechtlich-administrativen und technologisch-infrastrukturellen Kontext.

— Einige der Computersysteme des verteilten Verbundnetzwerks, in dem die Blockchain betrieben wird, können sich in unterschiedlichen Rechtsräumen befinden, so dass weder im geografischen noch rechtlichen Sinne von einem «Standort der Blockchain» gesprochen werden kann. Somit ist der rechtlich-administrative Kontext von Records und ihren Erzeugern nur im geschlossenen privaten Modell III derselbe und eindeutig identifizierbar.
— Eine öffentliche oder geschlossen gemeinschaftliche Blockchain (Modelle I, II und IV) hat entweder gar keinen identifizierbaren oder aber keinen einzelnen Betreiber, der für den Inhalt und die Aufbewahrung der Blockchain verantwortlich ist oder im rechtlichen Sinne verantwortlich gemacht werden kann. Im Service-Modell V gibt es einen einzelnen Betreiber, der aber kein Custodian ist, sondern nur im vertraglichen Sinne, also «im Auftrag» für die Aufbewahrung zuständig sein kann. Die Eigner der Records sind dagegen die (zahlreichen) Betreiber der Rechnersysteme in der Rolle Benutzer.

Somit kann nur im geschlossenen privaten Modell III von einem eigentlichen Custodian gesprochen werden. Das Dienstleister-Modell V hat grundsätzlich dieselbe rechtliche Konstruktion wie ein Cloud-Anbieter und beinhaltet somit auch dieselbe rechtliche Problematik. Dies allerdings in verschärfter Form: Der Erzeuger der Records (also ein Kunde, der sein Rechnersystem in der Rolle Benutzer betreibt) kann seine Records *prinzipiell* nicht vom Dienstleister «rückholen», wenn dieser den Betrieb einstellt. Denn nur die Rückholung einer *gesamten* Blockchain ist möglich. Doch auch in diesem Modell vermischen sich in der Blockchain des Dienstleisters unterschiedliche Provenienzen der Records untrennbar.

C) Kontinuität (chain of custody)

In jedem der Betriebsmodelle werden die Records in der Blockchain erzeugt, geführt und aufbewahrt. Das heisst, der gesamte Lebenszyklus eines Records läuft innerhalb der Blockchain ab. Eine Übertragung der Verantwortlichkeit für die Records im Verlaufe des Lebenszyklus kann somit nur dadurch stattfinden, dass die

Verantwortlichkeit für den Betrieb der gesamten Blockchain übertragen wird oder ihr Betriebsmodell wechselt.

- Eine nachvollziehbare *Übertragung* der Betriebsverantwortung für eine Blockchain ist nur bei den Modellen III, IV und V (also geschlossenen privaten oder gemeinschaftlichen sowie Dienstleister-Blockchains) möglich.
- Ein nachvollziehbarer *Wechsel* des Betriebsmodells ist nur bei einer geschlossenen privaten Blockchain möglich, da in allen anderen Modellen unterschiedliche Provenienzen der Records in der Blockchain existieren.

Allerdings muss berücksichtigt werden, dass nur bei einer geschlossenen, privaten Blockchain (Modell III) überhaupt von einem klassischen Custodian im Sinne des Records Management gesprochen werden kann. Nur hier lässt sich also eine lückenlose Obhut für Records (*unbroken chain of custody*) erreichen. Allerdings entsprechen die Modelle IV und V weitgehend der Konstellation bei der Nutzung eines Cloud-Service. Somit darf auch bei einer Blockchain in den Modellen IV und V die «Aufbewahrung im Auftrag» als eine pragmatische Form des Custodians gelten, wenn der eigentliche Eigner der Records seine Verantwortung durch entsprechende Abklärungen der Vertrauenswürdigkeit und Zuverlässigkeit des Blockchain-Dienstleisters im Sinne einer Risikoabwägung vorher abklärt und vertraglich absichert.

D) Authentizität

Die Authentifizierung und anschliessende Sicherung der Authentizität ist das erklärte Ziel jeder Blockchain. Die Frage ist, ob die technische Umsetzung von Authentizität in einer Blockchain dem fachlichen Begriff entspricht.

- Die in der Blockchain aufgezeichneten Informationen umfassen prüfbare Angaben zur Identität des Urhebers der Transaktion in Form von dessen digitaler Signatur (Merkmal 3). Er muss als Erzeuger und Übermittler dieser Records gelten, da kein vertrauenswürdiger Dritter existiert. Die Authentizität des Records wird vom Prüfer (Merkmal 4) geprüft und besteht aus der Gültigkeit der Signaturen von Prüfer und Urheber sowie der Gültigkeit von Form, Struktur und Inhalt der Transaktion.
- Diese Authentifizierung und ihr dauerhafter Nachweis ist unabhängig von der Ehrlichkeit des Prüfers (Merkmal 10).
- Der Zeitpunkt der Erstellung des Nachweises (als Record) wird aufgezeichnet (Merkmal 4) und ist ein kryptografisch abgesichertes Attribut der Transaktion. Es handelt sich um den Zeitpunkt der Bestätigung der Transaktion, also den Zeitstempel des Blocks. Dieser Zeitstempel ist somit identisch mit dem Zeitpunkt der Authentifizierung der Transaktion durch den Prüfer.

— Die an der Aufbewahrung beteiligten Personen sind durch das Betriebsmodell gegeben. Im Modell III (geschlossene private Blockchain) ist die Provenienz der Urheber selber, im Modell V ist es der Dienstleister.
— Da bei einer Blockchain die Aufzeichnung der Transaktion gleichzeitig auch wirkenden Charakter hat (also als Beweisurkunde dienen muss), ist dieser Nachweis als Record per se echt und stellt «das dar, was er zu sein vorgibt». Dies wird durch Merkmal 8 (Logische Ordnung) gewährleistet: Die vollständige Kette der Vorgänger-Transaktionen, auf die sich eine Transaktion bezieht, stellt alles dar, was über den Sachverhalt oder den Vertragsinhalt der Transaktion ausgesagt werden kann.

Die Provenienz einer Transaktion, also die Zugehörigkeit ihres Urhebers zur Organisation, welche die Eigentümerin des Records darstellt, ist allerdings nicht per se nachgewiesen. Dies hängt von der Art der verwendeten digitalen Signatur ab. Die Verwendung einer nicht-anonymen (z.B. einer qualifizierten) Signatur wird im Merkmal 3 allerdings nicht ausgeschlossen.

E) Integrität

Das Kriterium der Integrität in ISO 15489 geht über die reine technische Integrität eines einzelnen Datensatzes hinaus: Der Record muss bezüglich seiner ursprünglich vorhandenen Inhalte und Komponenten nachweislich unverändert und vollständig sein. Nachträglich angebrachte Zusätze müssen als solche erkennbar sein.

— Der in der Blockchain gespeicherte Nachweis der Transaktion enthält alle ursprünglich vorhandenen Inhalte und Komponenten der Transaktion, da die vollständigen Daten der Transaktion aufgezeichnet werden (Merkmal 4).
— Die nachweisliche Unverändertheit und Vollständigkeit aller Inhalte wird kryptografisch durch Hashwerte über die Daten und Blöcke sowie durch die digitale Signatur des Prüfers gewährleistet (Merkmale 6, 9 und 11). Nachträgliche Zusätze sind somit per Definition nicht möglich.

Damit ist eine Integrität auch im Sinne von ISO 15489 gewährleistet. Diese ist zudem unabhängig vom Betriebsmodell.

F) Zuverlässigkeit

Zuverlässigkeit im Sinne von ISO 15489 verlangt, dass der Record eine glaubwürdige, vollständige und genaue Wiedergabe der darin nachgewiesenen Transaktionen, Aktivitäten und Tatsachen ist und als verlässliche Grundlage für folgende Transaktionen, Aktivitäten und Entscheidungen dienen kann.

— Wie schon bei der Betrachtung der Authentizität gilt: Bei einer Blockchain stellt die Aufzeichnung der Transaktion gleichzeitig ihre Beweisurkunde dar, hat also selber wirkenden Charakter. Wegen ihrer technischen Integrität ist

die Aufzeichnung zudem auch eine vollständige Wiedergabe der Transaktion. Wäre dieser Nachweis nicht glaubwürdig, nicht vollständig oder nicht eine genaue Wiedergabe dessen, was er ja beweisen soll, wäre die Blockchain selber ad absurdum geführt.

— Jede validierte und in der Blockchain aufgezeichnete Transaktion ist eine verlässliche Grundlage für eine weitere, sich darauf beziehende Folgetransaktion. Dies ergibt sich aus der Eindeutigkeit des Transaktionskontexts (Merkmal 2), ihrer zeitlichen Ordnung (Merkmal 5) und ihrer logischen Ordnung in Transaktionsketten (Merkmal 8).

Selbst wenn es sich um Transaktionen, Aktivitäten und Entscheidungen ausserhalb des Blockchain-Systems handeln sollte, kann die Tauglichkeit der Records in der Blockchain dafür nicht bestritten werden, weil sonst die Tauglichkeit der Blockchain selber bestritten werden müsste. (Dies gilt bei jedem Informationssystem, das Informationen zur weiteren Verarbeitung an ein anderes, unabhängiges System liefern soll.) Daraus folgt, dass Records in einer Blockchain auch zuverlässig im Sinne des Records Management sind oder dies zumindest sein können. Auch hier ist das Kriterium unabhängig vom Betriebsmodell erfüllt: Einzelne Betreiber haben keinen Einfluss auf die Authentifizierung von Transaktionen und können die Integrität und damit Vollständigkeit der Blockchain nicht kompromittieren.

Diese Bewertung bezieht sich ausdrücklich nur auf die Merkmale 7 (Transaktionalität) und 8 (Logische Ordnung) der Blockchain, also auf einen definierten Gesamtzustand des Systems. Wie bereits erläutert, kann eine Blockchain nicht dazu dienen, *beliebige* oder willkürliche Informationen über Aktivitäten und Tatsachen nachzuweisen. Das Schreiben von Informationen wie «Hans war heute in Bern» oder «Wir haben heute ein Auto gekauft» in eine Blockchain kann keine Transaktion darstellen, weil sie nicht einen Zustand der Blockchain beschreiben, wenn sie nicht einen vorher bekannten Wert des Attributs oder «Beweiszeichens» (*token*) der Transaktion darstellen. Die Bitcoin-Blockchain liefert dazu ein anschauliches Beispiel: Im Feld `OP_RETURN` können einer Transaktion zwar 80 Bytes beliebige Information eingeschrieben werden, der mit dieser Transaktion verbundene Bitcoin-Wert (also das *token*) ist danach aber automatisch *unspendable* (d.h. er ist verloren), und diese Transaktion kann nicht mehr als Ausgangspunkt einer neuen, darauf basierenden Bitcoin-Transaktion verwendet werden. (Antonopoulos 2015, S. 133)

G) Benutzbarkeit

Benutzbarkeit im Sinne von ISO 15489 verlangt, dass der Record inventarisiert, eindeutig identifizierbar, auffindbar, darstellbar und verstehbar sein muss. Zudem muss in seiner Darstellungsform die direkte Verbindung mit den geschäftlichen Aktivitäten oder Transaktionen erkennbar sein, in denen er erzeugt wurde.

- Der eindeutige Transaktionskontext (Merkmal 2) ist durch die Verwendung kryptografischer Hashfunktionen sogar universell eindeutig und ermöglicht damit eine Inventarisierung. Diese kann nach Provenienz erfolgen, soweit diese bekannt ist, oder chronologisch, oder sachlogisch nach einem Attribut der Transaktion.
- Die Transaktionalität (Merkmal 7), logische Ordnung (Merkmal 8) und Unveränderlichkeit (Merkmal 11) einer Blockchain gewährleisten, dass jeder Record (als Nachweis einer Transaktion) auffindbar und verstehbar ist. Zum Beispiel gewährleistet die logische Ordnung (Merkmal 8) das eindeutige Auffinden aller Vorgänger- und Nachfolger-Transaktionen in einer Transaktionskette.
- Jeder Record ist auf Grund seines eindeutigen Transaktionskontexts (Merkmal 2) und seiner logischen und zeitlichen Ordnung sowie der Homogenität der Records (Merkmale 8 und 5) verstehbar, solange die Bedeutung aller Attribute der Transaktion bzw. das Zustandsmodell der Blockchain bekannt ist.
- Der Record ist einfach darstellbar, da er ein strukturierter Datensatz mit definierter und serialisierbarer Syntax und Semantik ist (Merkmal 5) und dauerhaft, jederzeit und ortsunabhängig abgerufen werden kann (Merkmal 1).
- Jeder Record ist mit der Transaktion verknüpft, die ihn erzeugt hat.

Was eine Blockchain jedoch *nicht* per se gewährleistet, ist die eigene Verknüpfung eines Records der Blockchain mit den geschäftlichen Aktivitäten oder Transaktionen, die *ausserhalb* des Blockchain-Systems stattfinden. Es wird einzig der Urheber über seine digitale Signatur (mit der er die Transaktion signiert) und die Transaktion selber identifiziert.

Allerdings spricht nichts dagegen, dass ein Geschäftskontext (*archival bond*) bewusst im Attributsatz bzw. Token der Transaktionen vorgesehen wird. Dies ist jedoch bereits eine *Anwendung* der Blockchain, die dafür entsprechend ausgelegt sein muss. Allerdings ist eine solche Anwendung nur in den nicht öffentlichen Betriebsmodellen III, IV und V möglich, da die möglichen Arten des Nachweises von Geschäftskontexten vorher bekannt sein müssen. Beim Dienstleister-Modell müsste dazu zudem jeder Kunde seine eigene Blockchain zur Verfügung haben. Die Referenzierung eines Blockchain-Records in einem externen Records Management System (zum Beispiel über seine Transaktionsnummer) ist dagegen immer problemlos möglich. Es lässt sich also schliessen, dass die Benutzbarkeit von Records im Sinne von ISO 15489 gewährleistet werden *kann*.

H) Statische Dokumentationsform

Ein Record muss eine oder mehrere bekannte, statische Darstellungen haben, die seine ursprüngliche Nutzung in Geschäftsprozessen adäquat wiedergeben. Dies

betrifft seine Struktur (Beziehungen zwischen Bestandteilen), sein Format, seinen Geschäftskontext (Erzeugung, Nutzung) sowie Verweise auf zugehörige, aber gesondert aufbewahrte Records.

— Darstellungsformen eines Blockchain-Records, die seine Nutzung im Geschäftsprozess adäquat wiedergeben, basieren alle auf seiner eindeutigen technischen Speicherform in der Blockchain als strukturierter Datensatz mit definierter, serialisierbarer Syntax und Semantik (Merkmal 5).
— In welcher Form diese Daten einem Benutzer in einem anderen System, z.B. einer Geschäftsanwendung oder einem Web-Browser angezeigt wurden, lässt sich allerdings nicht in der Blockchain festhalten.

Die Blockchain alleine kann neben seiner technischen Speicherform keine statische Darstellung seiner Inhalte nachweisen, genau gleich wie dies auch bei allen anderen Formen von strukturierten (also nicht dokumentzentrierten) Daten der Fall ist, zum Beispiel bei Datenbanken.

Übersicht

Die folgende Tabelle stellt die oben diskutierten Beurteilungen als Übersicht pro Betriebsmodell dar.

Kriterium nach ISO 15489 (**E**: Erfüllt, **M**: Möglich, **N**: Nicht erfüllbar) *Begründung in dem unter «siehe» genannten Abschnitt*		**Betriebsmodell**					siehe
		I	II	III	IV	V	
K1	Geeignete organisatorisch-technische Umgebung zur kontrollierten Aufbewahrung über den ganzen Lebenszyklus ohne Vernichtung?	E	E	E	E	E	A)
K2	Geeignet für Retention Management (kontrollierte Vernichtung nach Ablauf von Aufbewahrungsfristen)?	**N**	**N**	**N**	**N**	**N**	A)
K3	Wahrnehmung der Verantwortlichkeit als Custodian möglich?	**N**	**N**	E	**N**	**N**	B)
K4	Durchsetzbarkeit des Prinzips der lückenlosen Obhut (*unbroken chain of custody*)?	**N**	**N**	E	M	M	C)
K5	Authentizität der Records gewährleistet?	M	M	M	M	M	D)
K6	Integrität (inkl. Vollständigkeit) der Records gewährleistet?	E	E	E	E	E	E)
K7	Zuverlässigkeit der Records?	E	E	E	E	E	F)
K8	Benutzbarkeit (Findbarkeit, Darstellbarkeit und Verstehbarkeit der Records sowie Nachweis des Geschäftskontexts) der Records?	**N**	**N**	M	M	M	G)
K9	Statische Dokumentationsform vorhanden?	**N**	**N**	**N**	**N**	**N**	H)

Nach dieser Beurteilung kann eine Blockchain in keinem der fünf definierten Betriebsmodelle *alle* Kriterien der Vertrauenswürdigkeit im Sinne der archivischen

Diplomatik und des Records Management nach ISO 15489 erfüllen. Im Betriebsmodell III (geschlossene private Blockchain) ist die Vertrauenswürdigkeit jedoch grundsätzlich gegeben, wenn ein Löschen von Records nach Ablauf von gesetzlichen Aufbewahrungsfristen nicht zwingend nötig ist. Das Fehlen einer statischen Dokumentationsform ist dagegen ein grundsätzliches Problem bei strukturierten Daten, das zum Beispiel auch bei jedem Datenbanksystem besteht.

Das geschlossene gemeinschaftliche Modell (IV) ist weitgehend äquivalent zum Dienstleistermodell V. Gleichermassen ungeeignet als Träger von Records sind die beiden öffentlichen Blockchains (Modelle I und II). Ob bei einer öffentlichen Blockchain die Teilnahme am Netzwerk einer Zulassung (und damit Identifikation) unterliegt oder nicht, erscheint aus Sicht des Records Management somit als unwesentlich. Bezüglich der Erfüllbarkeit der fünf Qualitätsmerkmale von Records (K5 bis K9) sind die Betriebsmodelle III, IV und V dagegen äquivalent, d.h. diese Merkmale können mit Ausnahme der statischen Dokumentationsform in allen Betriebsmodellen realisiert werden. In den öffentlichen Blockchain-Modellen I und II lässt sich dagegen die Benutzbarkeit nicht herstellen, weil dort der Geschäftskontext der Records nicht nachgewiesen werden kann, da die Form dieses Nachweises auf Grund der beliebigen Benutzer nicht vorher bekannt sein kann.

Schlussfolgerungen

Blockchains eignen sich nach den in dieser Arbeit präsentierten Resultaten nur sehr begrenzt und unter bestimmten Randbedingungen als Erzeuger und Träger vertrauenswürdiger Records im Sinne der archivischen Diplomatik und des heutigen Verständnisses von Records Management. Möglich ist dies grundsätzlich nur im Betriebsmodell einer geschlossenen, privaten Blockchains, in der alle beteiligten Rechnersysteme denselben Betreiber haben. Allerdings geht in diesem Betriebsmodell die ‹Magie› einer öffentlichen Blockchain (wie bei Bitcoin) als autonome und unbestechliche «Vertrauensmaschine» verloren, die heute die Medienberichte über Blockchain-Technologie befeuert: Kontrolliert ein Betreiber alle beteiligten Rechnersysteme des Blockchain-Systems, so hat er dadurch auch weitreichende Möglichkeiten, um auf das Gesamtsystem Einfluss zu nehmen. Immerhin verbleiben auch in diesem Modell die Sicherheitsvorteile eines verteilten Systems im Vergleich zu einem zentralisierten Transaktionssystem.

Allerdings kommt die Bewertung auch zum Schluss, dass die auf Records *direkt* bezogenen Merkmale der Vertrauenswürdigkeit – Authentizität, Integrität, Zuverlässigkeit und Benutzbarkeit – auch durch Blockchains in kooperativen Betriebsmodellen durchaus in guter Qualität hergestellt und bewahrt werden können. Nicht erfüllbar ist bei solchen Betriebsmodellen einzig das *herkömmliche* Vertrau-

ensmodell des Records Management. Danach muss der Erzeuger der Transaktionen auch als Erzeuger (Provenienz) der in der Blockchain als Records aufgezeichneten Nachweise gelten können und eine massgebliche Verfügungsgewalt über alle daran beteiligten Rechnersysteme haben, um die Verantwortung für die Obhut (*custody*) seiner Records wahrnehmen zu können. Die Argumentation lässt sich an Hand des Betriebsmodells IV der geschlossenen, gemeinschaftlich betriebenen Blockchain (*community permissioned shared ledger*) illustrieren: Hier vermischen sich die Records unterschiedlicher Provenienzen, namentlich jener Betreiber, die gleichzeitig auch Nutzer der Blockchain sind. Die Verantwortlichkeit für die Aufbewahrung der Records lässt sich nicht nach Provenienz trennen, womit auch nicht von einem Custodian gesprochen werden kann, da die Verantwortlichkeit für die Obhut eigener Records im herkömmlichen Verständnis nicht teilbar ist, weder in archivischer noch rechtlicher Sicht.

Die Partner dieser Betreiber-Gemeinschaft könnten ein Konsortium gründen und diesem den Betrieb der Rechnersysteme (der Blockchain) übertragen. Dadurch würde eine geschlossene Variante des Dienstleister-Modells (*Blockchain-as-a-Service*) entstehen, die sich von diesem nur dadurch unterscheidet, dass der Kundenkreis geschlossen und durch das Konsortium vertraglich gebunden ist. Dies erweckt den Eindruck, als operiere dieses Konsortium als ein vertrauenswürdiger Dritter wie zum Beispiel ein Clearing-Haus. Doch dieser Eindruck täuscht: Ein echter vertrauenswürdiger Dritter würde die Transaktionen seiner Kunden als juristische Person authentifizieren und darüber Nachweise als *eigene* Records führen. Das Wesen einer Blockchain ist aber, dass es Transaktionen ohne Beteiligung eines Dritten authentifiziert. Anders als ein Clearing-Haus, eine Kreditkartenfirma oder ein Notar kann dieses Konsortium also keinen eigenen Beitrag an die Authentifizierung der Transaktionen leisten und auch keine eigenen Nachweise darüber erstellen. Es hält einzig die Rechnersysteme bzw. das Blockchain-System am Laufen.

Von den fünf beschriebenen Betriebsmodellen hat diese geschlossene, von wenigen Partnern gemeinschaftlich betriebene Blockchain jedoch die grösste Relevanz für die Praxis. Sie ermöglicht den höchsten wirtschaftlichen Nutzen bei (im Vergleich zu öffentlichen und privaten Blockchains) erheblich geringeren betrieblichen Aufwänden und rechtlichen Risiken. Nach der Bewertung dieser Arbeit kann eine Blockchain in diesem Betriebsmodell zwar die Qualitätskriterien für vertrauenswürdige Records durchaus erfüllen, nicht jedoch das herkömmliche, an die Rolle des *Custodian* gebundene Vertrauensmodell des Records Management. Es stellt sich deshalb die umgekehrte Frage, ob im Zeitalter der Blockchains nicht dieses Vertrauensmodell zu überdenken ist. Kann die Rolle des *Custodian*, der die Verantwortung für die Vertrauenswürdigkeit von Records trägt, nicht auch an ein autonom agierendes Technik-System delegiert werden, wenn dieser Automat unbeein-

flussbar und nach vordefinierten Regeln funktioniert? Diese Diskussion ist im Bewusstsein zu führen, dass die Sichtweisen auf die Vertrauenswürdigkeit von Urkunden und die Regeln zum angemessenen Umgang mit ihnen in den vergangenen Jahrhunderten immer Produkte ihrer Zeit waren und durch technologische Veränderungen stark beeinflusst wurden.

Literatur

Antonopoulos, A. M. (2015), Mastering Bitcoin: Unlocking Digital Cryptocurrencies. Sebastopol, CA, USA: O'Reilly Media.

Barlow, J. P. (1996), A Declaration of the Independence of Cyberspace. World Economic Forum Davos, Switzerland: Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence

Cofta, P. (2007), Trust, complexity and control confidence in a convergent world. Chichester, England: John Wiley & Sons. https://doi.org/10.1002/9780470517857

Couture, C. & Lajeunesse, M. (2014), L'archivistique à l'ère du numérique: Les éléments fondamentaux de la discipline (Collection Gestion de l'information). Presses de l'Université du Québec.

DIN. (2002), DIN ISO 15489-1:2002-1: Information und Dokumentation - Schriftgutverwaltung - Teil 1: Allgemeines. Berlin: DIN Deutsches Institut für Normung e.V. (Normenausschuss Bibliotheks- und Dokumentationswesen).

Duranti, L. (1991), Diplomatics: New Uses for an Old Science (Parts I–VI). Archivaria, 28 (1989), 29 (1989), 30 (1990), 31 (1990), 32 (1991), 33 (1991).

Duranti, L. (1996), Archives as a Place. Archives & Manuscripts, 24 (2), 242-255.

Duranti, L. (1997), The Archival Bond. Archives and Museum Informatics, 11, 213-218.

Duranti, L. (2005), The InterPARES Project: The Long-term Preservation of Authentic Electronic Records: the Findings of the InterPARES Project. San Miniato (PI), Italia: Archilab. http://interpares.org/book/index.cfm

Duranti, L. (2007), Reflections on InterPARES – The InterPARES 2 Project (2002 – 2007): An Overview. Archivaria, 64, 113-121

Duranti, L. (2009), From Digital Diplomatics to Digital Records Forensics. Archivaria, (68), 39-66

Duranti, L. (2010), Concepts and principles for the management of electronic records, or records management theory is archival diplomatics. Records Management Journal, 20(1), 78-95.

Duranti, L. & Rogers, C. (2012), Trust in digital records: An increasingly cloudy legal area. CLSR Computer Law & Security Review: The International Journal of Technology Law and Practice, 28(5), 522-531.

Franco, P. (2015), Understanding Bitcoin – Cryptography, engineering and economics (Wiley Finance Series). Chichester, West Sussex: John Wiley & Sons. http://public.eblib.com/choice/publicfullrecord.aspx?p=1823060

Gilliland, A. J. (2000), Enduring paradigm, new opportunities: the value of the archival perspective in the digital environment. Washington, D.C.: Council on Library and Information Resources. https://www.clir.org/pubs/reports/pub89/pub89.pdf

InterPARES. (2001), InterPARES 1 Project Book – The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project. http://www.interpares.org/book/index.cfm

ISO. (2001), SN ISO 15489-1:2001 (E): Information and documentation - Records management - Part 1: General. Geneva: International Organization for Standardization (ISO).

Jenkinson, H. (1922), A manual of archive administration including the problems of war archives and archive making. Oxford; London; New York: The Clarendon Press; H. Milford.

MacNeil, H. (2000), The Archivist's Library, Volume 1: Trusting Records : Legal, Historical and Diplomatic Perspectives. Dordrecht: Springer Netherlands.

May, T. C. (1992), The Crypto Anarchist Manifesto. http://www.activism.net/cypherpunk/crypto-anarchy.html

Menne-Haritz. (2011), Veröffentlichungen der Archivschule Marburg: Schlüsselbegriffe der Archivterminologie (3. Auflage). Marburg: Archivschule Marburg, Institut für Archivwissenschaft.

Nakamoto, S. (2008), Bitcoin: A Peer-to-Peer Electronic Cash System. gmane.comp.encryption.general Mailing List. https://bitcoin.org/bitcoin.pdf

Pilkington, M. (2015), Blockchain Technology: Principles and Applications. In Research Handbook on Digital Transformations: Social Science Research Network. http://ssrn.com/abstract=2662660

Pureswaran, V. (2015), Device democracy – Saving the future of the Internet of Things. Executive Report. IBM Institute for Business Value, IBM Corporation. http://www-935.ibm.com/services/us/gbs/thoughtleadership/internetofthings/

Rohr, C. (2015), Diplomatik (Urkundenlehre). In Historische Hilfswissenschaften. Wien, Köln, Weimar: Böhlau Verlag.

Sel, M. (2015), A Comparison of Trust Models. In Information Security Solutions Europe 2015 Conference (pp. 206-215). Springer Fachmedien Wiesbaden. doi:10.1007/978-3-658-10934-9_17

Swan, M. (2015), Blockchain – Blueprint for a New Economy. Sebastopol, CA, USA: O'Reilly Media.

Tanenbaum, A. S. & van Steen, M. V. (2002), Distributed Systems: Principles and Paradigms. Upper Saddle River, New Yersey: Prentice Hall, Pearson.

Tapscott, D. & Tapscott, A. (2016), Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. New York, USA: Penguin Random House.

The Economist. (2015, October 31). The trust machine. Print Edition. http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

Tschan, R. (2015), Archival Custody. In L. Duranti & P. C. Franks (Eds.), Encyclopedia of Archival Science. Lanham, Boulder, New York, London: Rowman & Littlefield.

Walport, M. (2016), Distributed Ledger Technology: beyond block chain – A report by the UK Government Chief Scientific Adviser. London: UK Government Office for Science. https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain

Wattenhofer, R. (2016), The Science of the Blockchain (1 ed.). Zürich: CreateSpace Independent Publishing Platform. http://www.dcg.ethz.ch/lectures/distsys/