Langfristige Beweiswerterhaltung und Datenschutz in der Blockchain

Tomasz Kusber[1] · Steffen Schwalm[1]
Christian Berghoff[2] · Ulrike Korte[2]

[1]Fraunhofer Institut für Offene Kommunikationssysteme (FOKUS)
{tomasz.kusber | steffen.schwalm}@fokus.fraunhofer.de

[2]Bundesamt für Sicherheit in der Informationstechnik (BSI)
{christian.berghoff | ulrike.korte}@bsi.bund.de

Zusammenfassung

Die Blockchain-Technologie ([Lem16], [WEKJ17]) findet zunehmend branchenübergreifend Beachtung und Verwendung. Dabei sind Blockchains integritätsgeschützte Datenstrukturen, in denen Transaktionen als verteilte elektronische Journale ohne zentrale Instanzen realisiert werden. Zur vertrauenswürdigen Abwicklung und Nachweis elektronischer Geschäftsprozesse sind im Rahmen der Anwendung der Blockchain-Technologie insbesondere Anforderungen hinsichtlich der geltenden gesetzlichen Nachweispflichten, der beweiswerterhaltenden Aufbewahrung gemäß Artikel 34 [eIDAS-VO] und Artikel 15 [VDG] sowie der EU-Datenschutzgrundverordnung (EU-DSGVO) zu erfüllen. Ausgehend von diesen juristischen und technischen Vorgaben werden die vorgenannten Anforderungen erläutert und Lösungen für den Einsatz von Blockchain-Technologien insbesondere im Zusammenhang mit dem Beweiswerterhalt abgeleitet. Dabei werden drei Lösungsvarianten, zusätzliche dedizierte Blöcke in Blockchain, Blockchain und der Einsatz von Evidence Records gemäß [RFC4998] und logische Blockchain auf Basis von [RFC4998], vorgestellt, miteinander vergleichen, und es wird eine Bewertung mit Ausblick gegeben.

1 Einführung

Die Blockchain-Technologie mit ihrem prominentesten Vertreter Bitcoin [Na08] erlebt seit einiger Zeit einen regelrechten Hype. Ihr wird in verschiedenen Branchen, so z.B. der Finanzindustrie, der Energiewirtschaft oder der öffentlichen Verwaltung, großes Potenzial zugeschrieben [WEKJ17]. Blockchains realisieren faktisch eine Technologie für verteilte elektronische Journale. Dabei werden neue Datenblöcke an eine stetig wachsende Kette angehängt und mit ihrem Vorgänger kryptographisch sicher verkettet. Die so entstehende Blockchain wird in einem dezentralen Peer-to-Peer-Netzwerk verteilt. Ein sogenannter Konsensmechanismus sorgt dafür, die Daten auf allen Netzwerkknoten konsistent zu halten. Als wesentliche Neuerung von Blockchains wird ihr Vertrauensmodell angesehen. Im Unterschied zu bestehenden, zentralisierten Technologien wie Datenbanken gibt es in einer Blockchain keine zentrale Instanz, über die die Kommunikation abläuft sowie gesteuert und verwaltet wird und der alle Nutzer vollumfänglich vertrauen müssen. Das Vertrauen in den korrekten Zustand der Blockchain entsteht vielmehr aus der dezentralen Speicherung und Prüfung der Daten durch die übrigen Netzwerkknoten, wobei das Ausmaß der tatsächlichen Dezentralität je nach konkreter Ausgestaltung va-

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 177-191.

riiert. Mittels des Verzichts auf eine zentrale Instanz soll es möglich sein, in Blockchain-Anwendungen Kosten zu sparen, wobei gleichzeitig eine hohe Verfügbarkeit der abgelegten Daten erreicht wird. Nachteile im Vergleich zu Datenbanken ergeben sich wegen der verteilten Speicherung in den Punkten Effizienz und Vertraulichkeit.

Die Aufnahme von Daten (in diesem Kontext meist als Transaktionen bezeichnet[1] [WEKJ17]) in eine Blockchain läuft folgendermaßen ab: Der Netzwerkknoten, der eine Transaktion in die Blockchain integrieren möchte, verteilt diese zunächst an die übrigen Knoten im zugrundeliegenden Peer-to-Peer-Netzwerk. Transaktionen werden gesammelt und in einer festgelegten Frequenz von speziellen Knoten, den Minern, zu Blöcken zusammengefasst. Neben einer Liste von Transaktionen enthält ein Block stets einen Verweis auf seinen Vorgängerblock, der durch eine Hashfunktion realisiert ist und nachträgliche Manipulationen früherer Blöcke verhindert bzw. nachweisbar gestalten soll. Der Anfang der so entstehenden Kette von Blöcken, der „Blockchain", wird als Genesis-Block bezeichnet. Da es im Allgemeinen mehrere Miner gibt, die Blöcke erzeugen können, wird ein sogenannter Konsensmechanismus verwendet, um unter allen Teilnehmern des Netzwerks Einigkeit über den jeweiligen Zustand der Blockchain herzustellen und die Daten konsistent zu halten [Na08, WEKJ17]. Für die konkrete Ausgestaltung des Konsensmechanismus gibt es verschiedene Möglichkeiten, die von der Art der verwendeten Blockchain abhängen. Am bekanntesten ist das von Bitcoin genutzte Proof-of-Work-Verfahren, bei dem der Konsens mithilfe eines rechenintensiven mathematischen Puzzles hergestellt wird. Ein großer Nachteil dieser Methode besteht in ihrem exorbitanten Energieverbrauch und dem niedrigen Datendurchsatz, den sie erlaubt [Di18]. Weiterhin tritt der Konsens nicht unmittelbar, sondern erst nach einer gewissen Zeitspanne ein. Wesentlich effizientere nachrichtenbasierte Konsensverfahren, die auf langjährigen Forschungsarbeiten im Bereich der Verteilten Systeme basieren, können jedoch auf sogenannten privaten (permissioned) Blockchains eingesetzt werden [CGR11]. Anders als beispielsweise bei Bitcoin ist aufgrund des vernachlässigbaren Energie- und Rechenaufwands für diese Konsensmechanismen auf privaten Blockchains ein sogenanntes Anreizsystem für die Mitarbeit der Miner nicht erforderlich.

Private Blockchains unterscheiden sich von öffentlichen Blockchains wie Bitcoin in ihrem Rechtemanagement. Während öffentliche Blockchains für beliebige Nutzer zugänglich und einsehbar sind, trifft dies bei privaten Blockchains nur für einen autorisierten Kreis zu. Zusätzlich geben die Begriffe „permissionless" und „permissioned" an, ob alle Nutzer über die gleichen Berechtigungen verfügen. Bei Bitcoin ist beispielsweise jeder Nutzer a priori ein Miner, wohingegen dies bei permissioned Blockchains nur für eine berechtigte Teilmenge der Fall ist [WEKJ17]. Aus diesem Grund sind private permissioned Blockchains in Bezug auf das Vertrauensmodell klassischen Lösungen ähnlicher, ohne aber die Eigenschaft der Dezentralität völlig aufzugeben. Die Identität der Teilnehmer ist, anders als bei öffentlichen Blockchains, in der Regel bekannt, was die angesprochenen Vorteile durch effizientere Algorithmen ermöglicht.

Die Ideen für den Einsatz von Blockchains in der Wirtschaft sind vielfältig. In Anlehnung an Bitcoin und andere Kryptowährungen können Blockchains eingesetzt werden, um allgemein den Transfer von Gütern, z. B. im Energiehandel, zu dokumentieren. Andere Anwendungen nutzen die Technologie in ausgewählten Fällen, wo dies möglich ist, zur Integritätssicherung von Dokumenten, indem deren Hashwerte in einer Blockchain gespeichert und so vor Manipulationen geschützt werden. Weitere Vorschläge betreffen die Kontrolle von Geschäftsprozessen sowie beispielsweise die Lieferketten- oder Vertragsinhaltsüberwachung durch sog. Smart

[1] Die zuerst auf der Bitcoin-Blockchain (BTC) verwendeten Begriffe haben sich allgemein etabliert.

Contracts [WEKJ17]. In den meisten dieser Fälle ist aus rechtlichen (z.B. Datenschutz, Nachweispflichten (vgl. Kapitel 2) und Effizienzgründen zu erwarten, dass sie mithilfe privater Blockchains realisiert werden. Da die Lebensdauer einer Blockchain potenziell unbegrenzt ist, ist insofern ein umfassendes Konzept zur Archivierung der in Blockchain abgelegten Daten inklusive der Wahl und Aktualisierung geeigneter Kryptoalgorithmen nötig, um die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit auch langfristig zu erreichen [BSIGS]. Diese sind nicht nur aus Gründen der Informationssicherheit erforderlich, sondern ebenso Grundlage zur Erfüllung bestehender Dokumentations- und Nachweispflichten, sofern Blockchain für geschäftsrelevante Prozesse verwendet werden soll. Diese Anforderungen und Herausforderungen sowie mögliche Lösungsansätze werden im Folgenden näher beschrieben.

2 Anforderungen an Blockchain

Im Folgenden werden Anforderungen an Blockchain zur Nutzung für vertrauenswürdige digitale Prozesse aufgezeigt.

2.1 Nachweis- und Aufbewahrungspflichten

Sofern blockchainbasierte Verfahren zur Abbildung vertrauenswürdiger elektronischer Prozesse in Behörden und Unternehmen dienen sollen und damit innerhalb dieser Verfahren oder in Verbund mit angrenzenden Lösungen (z.B. Cloud zur Ablage der Daten selbst und nur Verbleib von Hashwerten in der Blockchain) geschäftsrelevante Unterlagen entstehen und abgelegt werden, so sind, wie in jedem IT-Verfahren, das zur Umsetzung elektronischer Geschäftsprozesse Anwendung findet, die einschlägigen Nachweis- und Aufbewahrungspflichten zu beachten [Ko13], [ISO15489], [Wi15], [We18]. Elektronische Unterlagen geben jedoch aus sich selbst heraus keine Hinweise zu deren Integrität und Authentizität, ebenso wenig können sie ohne technische Hilfsmittel wie Soft- und Hardware wahrgenommen oder gelesen werden. Gleichzeitig bestehen jedoch umfassende Dokumentations- und Aufbewahrungspflichten, deren Dauer zwischen zwei und 110 Jahre[2] oder dauernd[3] umfasst. Innerhalb dieser Zeit ist der eindeutige wie verlustfreie Nachweis von Authentizität, Integrität und Nachvollziehbarkeit der Unterlagen gegenüber Prüfbehörden, Gerichten, Dritten zu erbringen [To07], [Ko14], [KuSc16]. Teilweise beginnen diese Fristen erst zu einem Zeitpunkt in der Zukunft, so z.B., wenn das Produkt, auf das sich die Unterlagen beziehen, vom Markt genommen wird, wie dies im Bereich europäischer Zulassungsverfahren in Luftfahrt, Pharma oder Pflanzenschutzmittel der Fall ist. Um die erforderlichen Nachweise führen zu können, sind die Unterlagen inklusive Meta- und Prozessdaten dem Gericht resp. der Prüfbehörde vorzulegen, was deren Verkehrsfähigkeit erfordert. Die zum Nachweis notwendigen Informationen sind also inhärente Bestandteile der Unterlagen selbst [Ko13], [KuSc16], [Ro07]. Neben dem Nachweis der Authentizität und Integrität ist im Kontext elektronischer Unterlagen sowie der technischen Entwicklung über die o.g. teilweise jahrzehntelangen Aufbewahrungsfristen vor allem deren Verfügbarkeit, also Lesbarkeit zu gewährleisten. Branchenspezifisch kommen, neben der reinen, originären Visualisierung der Daten, spezifische technische Vorgaben hinzu wie deren maschinelle Auswertbarkeit oder die Reproduzierung in den Unterlagen dokumentierter Analyseergebnisse etc.

[2] 110 Jahre gelten z.B. im Personenstandswesen für die Registerdaten, siehe https://www.gesetze-im-internet.de/pstg/BJNR012210007.html, § 5

[3] ´Dauernd gilt z.B. für Bauakten oder im Kontext Endlagerung

[ISO14721], [KuSc16], [Ro07], [Gia11]. Der Einsatz kryptographischer Mittel wie fortgeschrittener bzw. qualifizierter elektronischer Signaturen, Siegel sowie qualifizierter Zeitstempel (QZS) ermöglicht nach aktueller Rechtslage die Erhaltung des Beweiswerts geschäftsrelevanter digitaler Unterlagen, der für die Nachweisführung notwendig ist. Die Signaturen, Siegel und Zeitstempel werden direkt an den Unterlagen angebracht oder fälschungssicher verknüpft und gewährleisten so die Beweiswerterhaltung in verkehrsfähiger Form [F06], [Ro07], [eIDAS]. Insofern setzen Maßnahmen zur Beweiswerterhaltung an den Unterlagen selbst an [Ko14], [DIN 31647], [Ro07].

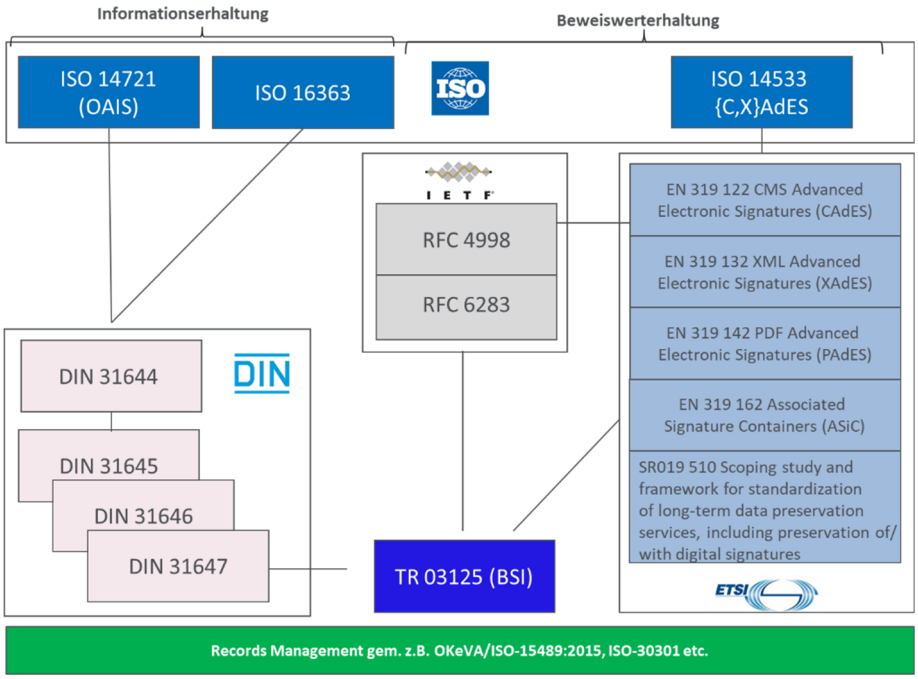

Abb. 1: Relevante Standards zur Informations- und Beweiswerterhaltung

Die wesentlichen internationalen und nationalen technischen Standards für die Umsetzung gem. dem Stand der Technik zeigt die vorstehende Grafik im Überblick. Die Erfüllung dieser Maßgaben, also zusammengefasst der Erhaltung und Nachweis von Authentizität, Integrität, Nachvollziehbarkeit, Verkehrsfähigkeit und Verfügbarkeit durch Beweis- und Informationserhaltung[4] der geschäftsrelevanten Unterlagen, sichert so die Vertrauenswürdigkeit zum einen der Unterlagen, die gem. OAIS in sog. selbsttragenden Archivinformationspaketen, kurz AIP[5] aufbewahrt werden, zum anderen der betroffenen digitalen Transaktionen [ISO14721], [ISO15489], [Ko14]. Wie die in Abbildung 1 dargestellten Standards [RFC4998], [RFC6283], [TR03125] so setzt auch Blockchain Merkle-Hashbäume [Merkle] zur Integritätssicherung der in den Blöcken verarbeiteten resp. gespeicherten Daten ein. Der technische Nachweis der Integrität[6] der in Blockchain enthaltenen resp. der zu den in Blockchain befindlichen Transaktionsdaten in Beziehung stehenden extern gespeicherten Daten erfordert insofern auch hier die Neuverhashung vor Ablauf der Sicherheitseignung der zugrundeliegenden Algorithmen.

[4] Der vorliegende Aufsatz konzentriert sich auf die Beweiswerterhaltung.

[5] Die AIP beinhalten Content, Metadaten, beweisrelevante Daten und technische Beweisdaten in standardisierten und damit langfristig aufbewahrbaren Formaten.

[6] Aus Sicht der Informationssicherheit beinhaltet die Integrität die Authentizität.

Ebenso gilt es, neben einer vertrauenswürdigen Zeitinformation in Form eines QZS zum Nachweis der rechtzeitigen Neusignierung bzw. -verhashung resp. zwecks Proof of Existence (PoE) auch die Hashwerte selbst durch einen QZS zu schützen [F06], [Ro07], [SR019510], [RFC4998/6283], [TR03125]. Ebenso ist die Frage nach Verkehrsfähigkeit und Nachvollziehbarkeit gegenüber Prüfbehörden, Gerichten, Dritten zu beantworten, die eine Vorlage der geschäftsrelevanten Unterlagen in verkehrsfähiger Form, also unabhängig vom Ausgangsverfahren (hier: Blockchain) erfordert [Ro07], [Ko14], [eIDAS], [DIN31647], [TR03125]. Darüber hinaus wäre die Verfügbarkeit und damit Lesbarkeit sowie ggf. langfristige Auswertbarkeit des Contents einschl. der Meta- und Prozessdaten auch in der Blockchain und damit die Vertrauenswürdigkeit von Prozess und Unterlagen zu gewährleisten [KuSc16], [Gia11]. Angesichts möglicher Anwendungsfelder wie Energiewirtschaft, Börsenhandel oder Zulassungsverfahren, die erfahrungsgemäß mit umfangreichen Nachweispflichten sowie langen Aufbewahrungsfristen verbunden sind, ist die Erfüllung dieser Vorgaben als ein kritischer Erfolgsfaktor blockchainbasierter Verfahren zu bewerten [KuSc16], [Ko14].

2.2 Digitale Identitäten und Datenschutz

Sofern Blockchain für vertrauenswürdige digitale Transaktionen verwendet werden soll, gilt es, neben der Erfüllung geltender Aufbewahrungs- und Nachweispflichten die nichtabstreitbare Zuweisbarkeit von Transaktionen zur zugehörigen natürlichen oder juristischen Entität zu gewährleisten. Dies erfordert deren eindeutige Identifizierung in digitaler Form in einem hinreichend sicheren wie zugelassenen Identifizierungsverfahren, resp. unter Verwendung eines anerkannten Identifizierungssystems [BuBa15], [Sc17] und eine geeignete Zugriffskontrolle, z.B. verbunden mit der Verwendung einer privaten Blockchain (vgl. Kapitel 1). Als Beispiele können hier eID-Systeme gem. [eIDAS] wie der neue Personalausweis oder PostIdent, VideoIdent oder BankID gelten, die z.B. zur Identifizierung gegenüber qualifizierten elektronischen Vertrauensdiensten nach [eIDAS] zugelassen sind. In einem geschäftsrelevanten IT-Verfahren stellen die hierfür verwendeten oder hierin entstandenen digitalen Identitäten, bei natürlichen Entitäten, ebenso personenbezogene Daten (pbD) gem. [EUDSGVO] dar. Im Falle juristischer Entitäten greifen zwar nicht die Vorgaben des Datenschutzes, wohl aber Maßgaben zur Vertraulichkeit der geschäftlichen Handlungen zur Wahrung des Betriebs- und Geschäftsgeheimnisses, die durch Maßnahmen zur Gewährleistung des Schutzziels Vertraulichkeit zu erfüllen sind [ISO27001], [BSIGS]. Die Vorgaben des Datenschutzes resp. der Vertraulichkeit sind zudem für die in Blockchain erzeugten oder gespeicherten geschäftsrelevanten Unterlagen incl. Meta-/Prozessdaten relevant. Im Kontext der im Fokus des vorliegenden Aufsatzes stehenden langfristigen Nachweisfähigkeit elektronischer Transaktionen sind besonders der Nachweis der Einwilligung des Betroffenen zur Erhebung und Verarbeitung seiner personenbezogenen Daten (Art. 6 [EUDSGVO]), die Informationspflicht gegenüber dem Betroffenen (Art. 13 und 14) sowie die Rechte des Betroffenen [EUDSGVO] ins Blickfeld zu rücken [Zi17][7]. Hierzu zählen gemäß [EUDSGVO] unter anderem:

- Recht auf Auskunft (Art. 15),
- Recht auf Berichtigung (Art 16),

[7] Aus Sicht des Datenschutzes wären noch z.B. Fragen zur Auftragsdatenverarbeitung oder Betrieb in der Cloud interessant. Diese sind hier, aufgrund des Schwerpunkts Beweiswerterhaltung, jedoch nicht im Scope des Aufsatzes.

- Recht auf Datenübertragbarkeit in einem strukturierten, gängigen, maschinenlesbaren Format (Art. 20),
- Recht auf Löschung bzw. Recht auf „Vergessenwerden“ (Art. 17).

Im Kontext von Aufbewahrungsfristen bis zu 110 Jahren oder dauernd widerspiegeln sie die Forderungen nach Integrität, Authentizität und Nachvollziehbarkeit (Informationspflicht, Auskunft, Übertragbarkeit), Verfügbarkeit (Berichtigung, Löschung, Übertragbarkeit) der Unterlagen sowie deren Verkehrsfähigkeit (Übertragbarkeit) – also die Informations- und Beweiswerterhaltung elektronischer Unterlagen. Die Gewährleistung der datenschutzrechtlichen Vorgaben kann, vor allem mit Blick auf die Bußgeldvorschriften der [EUDSGVO] neben der Erfüllung geltender Dokumentations- und Aufbewahrungspflichten als ein zweiter kritischer Erfolgsfaktor einer privaten Blockchain bezeichnet werden [Zi17], [DEO17], [GOS16]. Im Folgenden werden Lösungsansätze mit Fokus sowohl auf die Beweiswerterhaltung in als auch der o.g. Maßgaben des Datenschutzes vorgestellt, und Handlungsempfehlungen sowie mögliche Bedarfe für weitere Forschungs- und Standardisierungsarbeiten abgeleitet.

3 Herausforderungen und Lösungsansätze

Im Folgenden werden wesentliche Herausforderungen und daraus abgeleitete Lösungsansätze im jeweiligen Kontext betrachtet. Zudem wird eine kurze Bewertung der Lösungsvorschläge vorgenommen.

3.1 Herausforderungen

Integritätsschutz, Beweiserhaltung und die Einhaltung der EU-Datenschutzgrundverordnung sind wesentliche Anforderungen, die zwingend zu berücksichtigen sind.

3.1.1 Integritätsschutz

Eine typische Anwendung einer Blockchain, in der alle Daten (Content, Meta- und Prozessdaten) je Transaktion[8] in der Kette abgelegt werden, wird in der nachfolgenden Grafik dargestellt. Der Block B1 besteht aus einem Header B1H und einem Merkle-Baum, in dem die einzelnen Transaktionen (Tx01 bis Tx04) geschützt werden[9] (vgl. [NA08]). Die Wurzel des Baumes HR1 wird in dem Header mitabgelegt. Es wird der Hashalgorithmus H verwendet. Analog wird der nachfolgende Block B2 mit Transaktionen Tx05 bis Tx08 aufgebaut. In diesem Falle wird aber der Hashalgorithmus H‘ verwendet. Sollte die Sicherheitseignung von H ablaufen und es wurden keine zusätzlichen Maßnahmen getroffen, so wird insbesondere der darunter hängende Merkle-Baum also auch die Transaktionsdaten, d.h. alle rot gekennzeichnete Elemente die Möglichkeit des Integritätsnachweises verlieren. Daher kann die Unversehrtheit der – indirekt durch Blockchain geschützte – Daten nicht mehr zugesichert werden. Die direkt durch Blockchain geschützte Daten, d.h. die Block-Headers inkl. der Wurzel des Merkle-Baums bleiben dagegen davon unberührt.

[8] Der Umfang der in der Transaktion gespeicherten Daten hängt von der Art der mit der Blockchain-Technologie implementierten Anwendung ab. Hier betrachtete Daten sind als die Mindestmenge, die für die Betrachtung der beschriebenen Herausforderungen notwendig ist, anzusehen.

[9] Die hier abgebildeten Daten können als eine Teilmenge angesehen werden, die für die dargestellte Betrachtung von Bedeutung ist. Selbstverständlich können die einzelnen Elemente auch weitere Daten beinhalten, was durchaus auch üblich ist, die aber i.d.R. keinen unmittelbaren Einfluss auf die dargestellte Betrachtung haben werden.

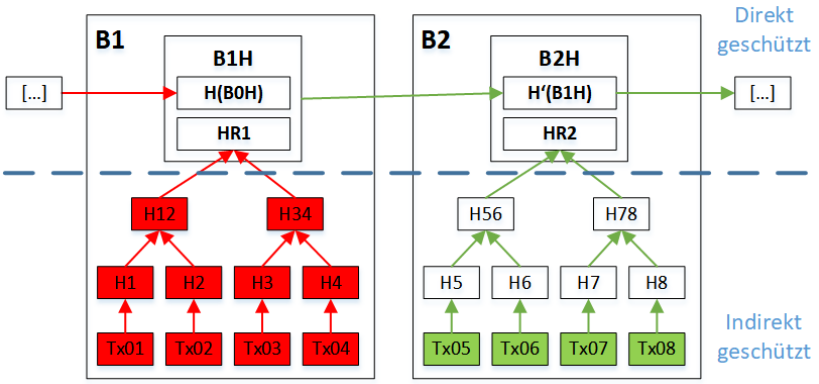

Abb. 2: Blockchain (ähnlich Bitcoin [BTC]) – generelles Problem mit Rehashing

3.1.2 Beweiswerterhaltung

Die Beweiswerterhaltung selbst erfolgt gem. § 15 [VDG] sowie [eIDAS] durch Erneuerung der Signaturen und Siegel durch eine neue qualifizierte elektronische Signatur/Siegel oder einen qualifizierten elektronischen Zeitstempel sowie, sofern notwendig, durch die Neuverhashung der zu schützenden Daten, sobald die bislang verwendeten Signatur-/Siegel-/Hashalgorithmen drohen, ihre Sicherheitseignung zu verlieren. Die Verwendung von Merkle-Hashbäumen [RFC4998], [RFC6283] ermöglicht eine effiziente wie wirtschaftliche Beweiswerterhaltung für eine Vielzahl von Datenobjekten und ist in Abbildung 2 dargestellt. Wesentlich ist dabei auch, dass vor der Neusignierung/Neuverhashung aktuelle Verifikationsdaten, wie z.B. Zertifikate, Status- und Sperrinformationen, etc. der vorausgegangenen Signatur bzw. des vorausgegangenen Siegels/Zeitstempels, eingefügt werden. Es ist zum Nachweis der Existenz zu einem bestimmten Zeitpunkt ([SR019510], siehe „Proof of Existence“) auch eine vertrauenswürdige Zeitinformation – aktuell durch den qualifizierten Zeitstempel eines qualifizierten Vertrauensdiensteanbieters – notwendig [eIDAS], [KSDV15], [KuSc16], [Ko14], [SR019510], [TR03125]. Sofern in Blockchain geschäftsrelevante Unterlagen enthalten sind, ist (vgl. Kapitel 2), auch deren Beweiswert durch entsprechende Maßnahmen gem. dem Stand der Technik zu erhalten. Als solcher gilt das o.g. Verfahren nach [RFC4998] in Verbindung mit [TR03125]. Für Blockchains ist aufgrund mangelnder standardisierter Mechanismen für eine Neuverhashung und das (erneute) Einbringen qualifizierter Zeitstempel die langfristige Erhaltung der Integrität eingeschränkt sowie der Existenznachweis derzeit nicht sichergestellt.

3.1.3 EU-Datenschutzgrundverordnung

Die Gewährleistung der Informationspflicht gegenüber dem Betroffenen sowie des Auskunftsrechts kann in Blockchain vergleichsweise einfach erfüllt werden, allerdings ist, sofern die Erhebung in der Blockchain stattfindet, eine eindeutige Identifizierung des Antragstellers erforderlich. Standardisierte Mechanismen für die Umsetzung der Gewährleistung der Berichtigung, Löschung, standardisierte Übertragbarkeit personenbezogener Daten stehen nicht im ausreichenden Maße zur Verfügung. So können elektronische Unterlagen zwar in der Blockchain gespeichert werden. Es liegt jedoch kein plattformneutrales, selbsttragendes Austauschformat zu anderen IT-Verfahren wie z.B. [ISO13527] oder [TR03125-F] vor, wie es für die langfristige Interpretierbarkeit der Daten sowie deren Verkehrsfähigkeit notwendig wäre [Gia11], [Ro07]. Ebenso können aktuell Daten, die in der Blockchain gespeichert sind, nicht mit standardisierten Mechanismen gelöscht werden. Die Vertraulichkeit sowie Authentizität und Integrität müssen

ggf. mit weiteren Maßnahmen z.B. Nutzung sicherer Verschlüsselung, digitaler Identitäten, Signierung/Siegelung von Transaktionen etc. hergestellt werden.

3.2 Lösungsvorschläge

Im Folgenden werden drei Vorschläge für das Rehashing-Problem diskutiert.

3.2.1 Integrität durch dedizierte Blöcke in Blockchain

Eine potentielle Lösung des Rehashing-Problems könnte darin bestehen, dass unter Anwendung von einem besonderen Block der Merkle-Hashbaum eines vorherigen Blocks abgesichert werden kann (vgl. Abbildung 3).

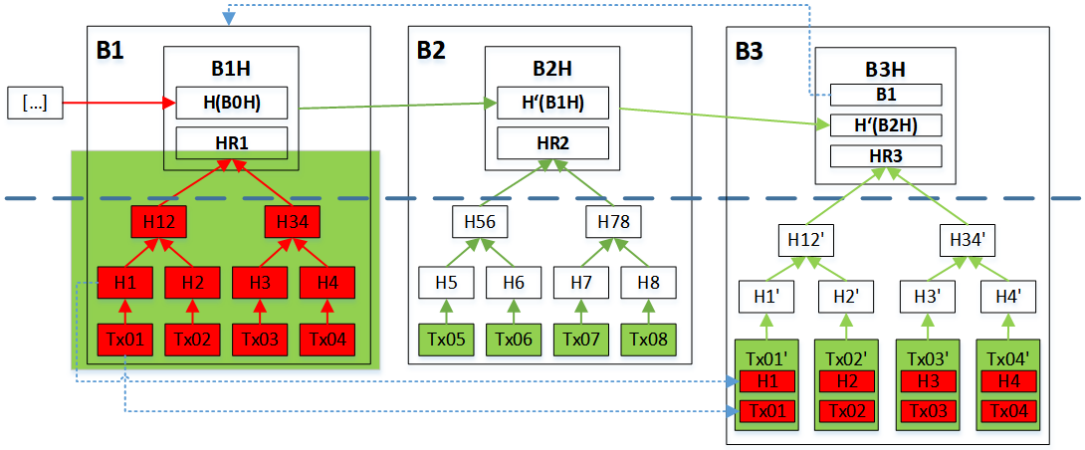

Abb. 3: Blockchain (ähnlich BTC) – Problemlösung mit Rehashing durch Einsatz dedizierter Blöcke

Solch ein besonderer Block (hier B3) würde im Grunde keine neuen Transaktionsdaten beinhalten, sondern die zuvor stattgefundenen Transaktionen mit Hilfe eines neuen Hashalgorithmus (H‘) absichern[10], und somit den Beweiswert des vorausgegangenen Blocks (hier B1) erhalten. Basierend auf den vorhandenen Transaktionsdaten sowie den zugehörigen alten Hashwerten (z.B. Tx01[11] und H1) würden entsprechend neue Transaktionen gebildet, die diese Daten beinhalten (z.B. Tx01‘) und mit dem neuen Hashalgorithmus abgesichert werden (z.B. H1‘). Das Verfahren müsste entsprechend auch auf alle Blöcke, die mit H verhasht wurden, angewandt werden. Spätestens bevor H‘ seine Sicherheitseignung verliert, muss die Prozedur mit einem neuen Hashalgorithmus mit Bezug auf alle Blöcke, die mit H‘ verhasht wurden, wiederholt werden. Der Ansatz erfüllt die Anforderung gemäß Abschnitt 3.1, ist jedoch mit einer deutlich gestiegenen Komplexität und einer wesentlich längeren Blockkette verbunden. Die Anforderungen gemäß Abschnitt 3.2 werden nicht erfüllt, da kein PoE, z.B. in Form eines qualifizierten Zeitstempels etc. [SR019510], [TR03125], erzeugt und gespeichert wird mit der Zeit (abhängig von der Parametrisierung der zugrundeliegenden Blockchain-Anwendung) kann unter Umständen die Anzahl der Blöcke, die der Beweiswerterhaltung dienen, die Anzahl der

[10] Die dedizierten Blöcke stellen eine solche Absicherung der Transaktionsblöcke dar. Mit der Zeit müssen auch die besonderen Blöcke neu abgesichert werden.

[11] Ausreichend wäre es, auf die „alten“ Transaktionsdaten in geeigneter Weise zu verlinken (z.B. H‘(Tx01)), um die redundante Datenhaltung zu vermeiden.

Blöcke mit neuen Transaktionen deutlich übersteigen[12]. Um die Nachweispflichten zu erfüllen (vgl. Abschnitt 2.1), müsste die vollständige Kette der Blockheader sowie die involvierten Transaktionsdaten vorgelegt werden (vgl. Kapitel 8 [Na08]). Hinsichtlich des Datenschutzes gelten die Einschränkungen aus Abschnitt 3.1.3.

3.2.2 Blockchain und RFC4998

Eine weitere Alternative könnte beispielweise der Einsatz eines RFC4998-basierten Systems z.B. BSI TR-03125 TR-ESOR sein, um die Merkle-Hashbäume zu erzeugen und diese auch beweiswert-technisch mit einem qualifizierten Zeitstempel gemäß Abschnitt 3.1.2 abzusichern (vgl. Abbildung 4).

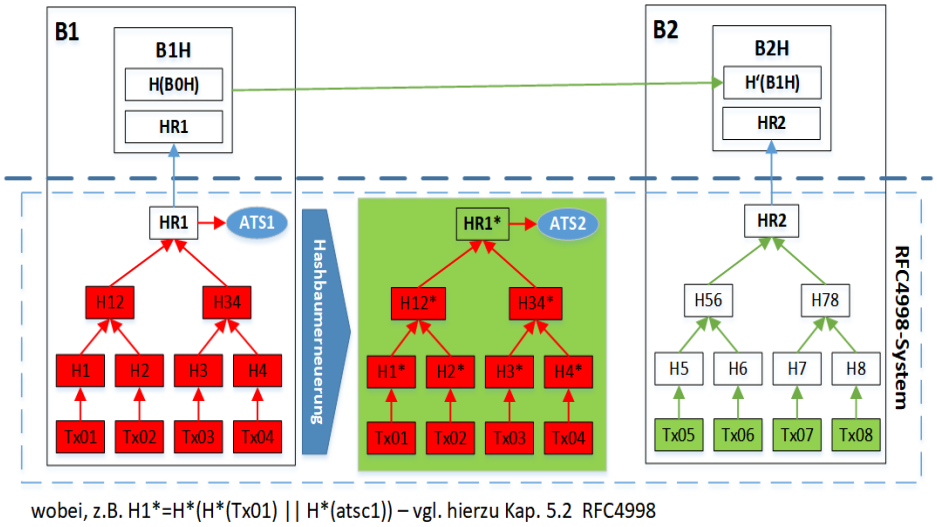

Abb. 4: Blockchain (ähnlich BTC) – Problemlösung mit Rehashing durch Einsatz von RFC4998

Das Erzeugen der Merkle-Bäume übernimmt dabei vollständig das RFC4998-System. Die Wurzel des berechneten Baums kann somit einerseits (wie gewöhnlich) im Header des dazugehörigen Blocks (z.B. HR1 in B1H) abgelegt werden, sowie andererseits durch den Archivzeitstempel des RFC4998-Systems (ATS1) abgesichert werden[13][14]. Die Blockkette an sich bleibt zunächst von dem zusätzlichen System vollumfänglich unberührt. Droht der verwendete Algorithmus die Sicherheitseignung zu verlieren (hier H) so wird innerhalb des RFC4998-Systems eine Hashbaumerneuerung angestoßen (vgl. Abschnitt 5.2 [RFC4998]). Auf diese Weise kann zu jedem Zeitpunkt zu jeder Transaktion ein Evidence Record (ER) vorgelegt werden, der die Unversehrtheit dieser Transaktion garantiert. Beispielweise ergibt sich für die Transaktion Tx01 zunächst ER1={<[{(H1,H2),(H34)},ATS1]>}, mit einer Archivzeitstempelkette und einem Archivzeitstempel. Nach der erfolgten Hashbaumerneuerung wäre es entsprechend ER2={<[{(H1,H2),(H34)},ATS1]>,<[{(H1*,H2*),(H34*)},ATS2]>}, mit zwei Archivzeit-

[12] Wenn es x_1 Transaktion mit H gibt so gibt es (x_1+x_2) Transaktionen mit H‘ und $(x_1+x_2+x_3)$ Transaktionen mit H‘‘ usw. Somit gäbe es für die Teilkette insgesamt $s=x_1+(x_1+x_2)+(x_1+x_2+x_3)$ Transaktionen, im Normallfall ergäbe eine solche Kette aber nur $s‘=x_1+x_2+x_3$ Transaktionen.

[13] Die Ablage der Beweisdaten muss entsprechend der Anforderungen an die bestimmte Anwendung vorgenommen werden. Diese Daten könnten in einem Drittsystem, oder auch innerhalb der Blockchain gespeichert werden.

[14] Dabei handelt es sich um r einen qualifizierten Zeitstempel, für dessen Erzeugung ein qualifizierter Vertrauensdiensteanbieter gem. eIDAS-VO notwendig ist.

stempelketten, und jeweils einem Archivzeitstempel. Auch in diesem Falle ist mit einer Steigerung der Komplexität des Systems zu rechnen, da ein zweites System (RFC4998) parallel betrieben wird. Der Beweiswert der Transaktion kann standardmäßig mit dem ER nur durch die Vorlage von Artefakten, die aus beiden Systemen stammen, vollumfänglich nachgewiesen werden. Da auf dem Markt verschiedene RFC4998-konforme Systeme angeboten werden, kann der Aufwand einer solchen Implementierung deutlich reduziert werden. Die Beweiswerterhaltung wie auch Verkehrsfähigkeit des ER (Stichwort: Nachweispflichten) ist in diesem Fall gegeben, da die Unversehrtheit der Daten durch den Einsatz von QZS auch außerhalb der Blockchain belegt werden kann. Hinsichtlich des Datenschutzes gelten die Einschränkungen aus Abschnitt 3.1.3.

3.2.3 Logischer Blockchain auf Basis von RFC4998

In den vorausgegangenen Kapiteln wurde eine Blockchain betrachtet, welche die Transaktionsdaten und damit Content, Meta- und Prozessdaten vollständig beinhaltet. Aus Gründen der Performance oder des Datenschutzes kann auch der Fall eintreten, dass die Transaktionsdaten in der Blockchain lediglich den tatsächlichen Content sowie die Metadaten referenzieren, und diese in einem Fremdsystemen (außerhalb der Blockchain) gehalten werden[15]. Dieses führt zur Einführung der dritten Schutzebene in der Betrachtung – doppelt indirekt geschützte Daten (vgl. Abbildung 5).

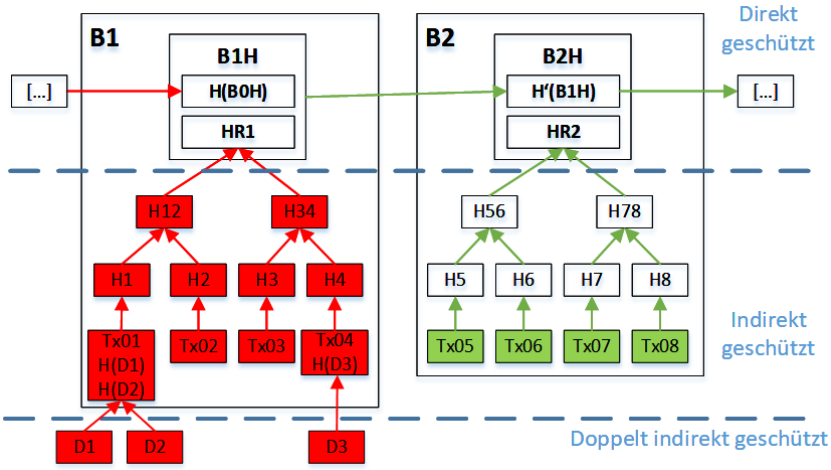

Abb. 5: Blockchain (ähnlich Smart-Contract) – spezielles Problem mit Rehashing von Inhaltsdaten

In einem solchem Fall kommen zu den generellen Fragestellungen bezogen auf Blockchain hinsichtlich Beweiswerterhaltung (vgl. Abschnitt 3.1) zusätzlich noch spezielle Aspekte (doppelt indirekt geschützte Daten) hinzu, die durch die Auslagerung der Inhaltsdaten entstanden sind. Die Ad-hoc-Anwendung der beiden Lösungsansätze aus den Abschnitten 3.2.1 und 3.2.2 würde hier auch keine schnelle Abhilfe schaffen[16]. Eine Idee für eine mögliche Lösung wäre eine geeignete Speicherung der Daten vollständig in einem RFC4998 System und Aufbau einer logischen Blockchain (vgl. Abbildung 6).

---

[15] Vgl. hierzu z.B. Smart-Contracts. Die Daten der Transaktion (Smart-Contract selbst) werden in der Blockchain gehalten, die relevanten Inhaltsdaten werden aber häufig außerhalb der Blockchain abgelegt und nur durch die Hashwerte referenziert.

[16] Die außerhalb der Blockchain liegende Dokumente sind nicht direkter Bestandteil der bisher betrachteten Merkle-Hashbäume.

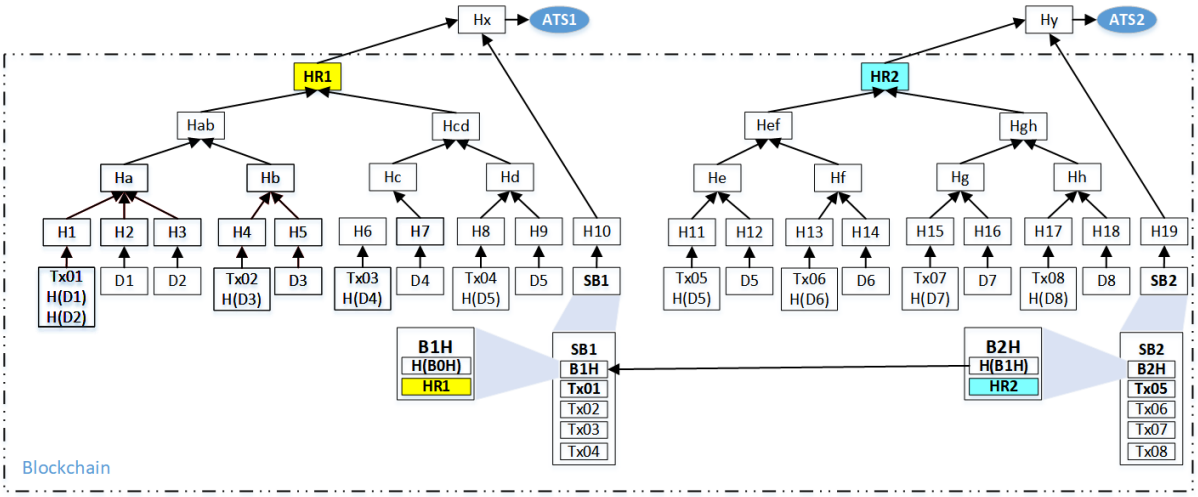

Abb. 6: Logischer Blockchain

Die Transaktionen bilden dabei zusammen mit den zugehörigen (referenzierten) Inhaltsdaten jeweils eine Datenobjektgruppe im Sinne von RFC4998 (vgl. Abschnitt 4.2 RFC4998), z.B. Tx01 mit D1 und D2 oder Tx05 mit D5. Über alle Transaktionen und die zugehörigen Inhaltsdaten wird ein Merkle-Baum gem. [RFC4998] aufgebaut, der mit dem Wurzelhashwert abgeschlossen wird (z.B. HR1). Der berechnete Wurzelhashwert wird in dem zugehörigen Blockheader (z.B. B1H) innerhalb der Blockbeschreibung[17] (z.B. SB1) abgelegt und in den gleichen Hashbaum abgesichert, womit der Hashbaum ein neues Wurzelelement bekommt (z.B. Hx), der dann entsprechend [RFC4998] mit einem qualifizierten Archivzeitstempel (z.B. ATS1) abgeschlossen wird. Analog geht man mit dem nachfolgenden Block (B2) vor. Der Blockheader von B2 (S2B) beinhaltet dabei den Hashwert berechnet über den Blockheader des Blocks B1 (B1H), womit die gewünschte Verkettung der Blöcke gewährleistet ist. Die Beweiswerterhaltung erfolgt dabei gem. [RFC4998], geschützt sind dabei sowohl alle Headers als auch die Transaktionen und die durch diese referenzierten Inhaltsdaten. Die Anforderungen aus den Abschnitten 3.1.1 und 3.1.2 sind auf diese Art und Weise inklusive des PoE erfüllbar. Hinsichtlich der Maßgaben des Datenschutzes können die Lösch-/Berichtigungs- und Datenübermittlungsvorgaben für die Inhalts- und Metadaten gelöst werden. Hierfür sind im speichernden Fremdsystem entsprechende Funktionen bereitzuhalten. Anders verhält es sich mit möglichen Identifizierungsdaten der Nutzer der privaten Blockchain sowie der Prozessdaten je Transaktion, hier sind tiefere Untersuchungen notwendig. Abschließend kann angemerkt werden, dass es deutlich wird, dass mit der steigenden Abdeckung der im Kapitel 2 gestellten Anforderungen, die vorgeschlagene Lösung stetig wachsenden Abstand vom Idealbild einer Blockchain aufweist.

[17] Serialized block beinhaltet den Blockheader sowie Verweise auf alle zugehörigen Transaktionen.

3.3 Bewertung der Lösungsvorschläge

Bezüglich der Anforderungen Integritätsschutz (Integrität), Beweiswerterhaltung (Beweiswert), Verkehrsfähigkeit (Verkehrsfähig), Komplexität und Gewährleistung des Datenschutzes (Datenschutz) werden die Lösungsvorschläge mittels dedizierter Blöcke und Blockchain bzw. logischer Blockchain auf der Basis von RFC4998 gegenüber gestellt.

Vorschlag / Anforderung	Dedizierte Blöcke in Blockchain	Blockchain und RFC4998	Logische Blockchain auf Basis von RFC4998
Integrität	Ja	Ja	Ja
Beweiswert	Nein, da kein Proof of Existence und keine Neusignierung, nur Integritätsschutz	Ja Verkehrsfähigkeit des Evidence Records gegeben	Ja Verkehrsfähigkeit des Evidence Records gegeben
Verkehrsfähig	Nein	Ja	Ja
Komplexität	Höheres Datenaufkommen	Ggf. zusätzliche Komplexität durch externes System	Ggf. zusätzliche Komplexität durch externes System
Datenschutz	Nein, da keine Verkehrsfähigkeit, Übertragbarkeit mittels standardisierter Austauschformate, keine Möglichkeit zur Löschung, Berichtigung personenbezogener Daten sowie Identitätsbezogene Zugangskontrolle	Nein Keine Übertragbarkeit mittels standardisierter Austauschformate, keine Möglichkeit zur Löschung, Berichtigung personenbezogener Daten sowie Identitätsbezogene Zugangskontrolle	Grundsätzlich vorhanden Hohe Komplexität durch Teile des AIP (Content, Metadaten) in Fremdverfahren und Erhaltung des Kontexts zu Teilen (Prozessdaten, ggf. Identitätsdaten) in Blockchain; Im Fremdsystem: Übertragbarkeit, Löschung, Berichtigung standardisiert möglich; hinsichtlich der Identitäts- und Prozessdaten, die in der Blockchain verbleiben, sind weitere Untersuchungen im Kontext Datenschutz notwendig

4 Ausblick und weiterer Forschungsarbeit

Im vorstehenden Text wurde untersucht, inwieweit die Blockchain-Technologie existierende Anforderungen hinsichtlich geltender Nachweis- und Aufbewahrungspflichten, also Anforderungen an die Beweiswert- und Informationserhaltung sowie die EU-Datenschutzverordnung bereits erfüllt oder wie dies durch zusätzliche Maßnahmen erreicht werden kann. Derzeit sieht die Blockchain-Technologie keine standardisierten Prozeduren vor, um die Integrität sowie den Beweiswert der verhashten Daten über einen langen Zeitraum (z.B. bis zu 110 Jahre) zu erhalten. Ebenso liegen nur wenig standardisierte Mechanismen zur sicheren Identifikation der am

Prozess Beteiligten, zur sicheren Authentisierung und zum Beweiswerterhalt der in der Blockchain gespeicherten Daten vor.

Mechanismen zur Übertragbarkeit, Berichtigung oder Löschung personenbezogener Daten sind ebenso wenig vorhanden, wie für die langfristige Verfügbarkeit, also Interpretierbarkeit der in Blockchain gespeicherten Unterlagen. In Kapitel 3 wurde mit der logischen Blockchain im Verbund mit [RFC4998] ein Lösungsweg zur Verknüpfung von Blockchain mit etablierten wie standardisierten Verfahren vorgestellt, um trotz vorgenannter Defizite mögliche Lösungswege für die Beweiswerterhaltung sowie den Datenschutz für Inhalts- und Metadaten der AIP aufzuzeigen. Dies wird allerdings mit einer erhöhten Komplexität durch den parallelen Betrieb von Blockchain und Fremdsystemen sowie Performancenachteile erkauft, so dass Aufwand und Nutzen einer Verwendung von Blockchain kritisch zu betrachten sind. Im Fall der Lösungsoptionen nach Abschnitt 3.2.1 und 3.2.2 sind die Aufwände für einen performanten Betrieb noch deutlich höher einzuschätzen, da sich das komplette AIP in der Blockchain befindet. Insofern erscheint eine kritische Prüfung der Sinnhaftigkeit einer Umsetzung der vorgeschlagenen Lösungen in Anwendungsfällen, bei denen umfangreiche Dokumentations- und Aufbewahrungserfordernisse sowie Datenschutzvorgaben vorliegen, empfehlenswert. Aus Praxissicht bedeutet, dies, dass von einer Speicherung personenbezogener Daten in Blockchain derzeit eher abzuraten ist, die Ablage aufbewahrungspflichtiger Daten ist im Einzelfall zu bewerten. Je länger die Aufbewahrungsfrist sowie je höher die Nachweispflichten, desto eher erscheint die Ablage in Blockchain derzeit kritisch. Bei Speicherung personenbezogener sowie aufbewahrungspflichtiger Daten außerhalb der Blockchain sind Aufwand und Nutzen der sich ergebenden technischen wie organisatorischen Komplexität im Einzelfall kritisch zu prüfen. Alternativ käme die Nutzung von Smart Contracts auf Basis Blockchain als reiner Infrastrukturservice zur Gewährung verfahrensübergreifender Zugriffe bspw. im Rahmen der Registerautomatisierung in Frage, wobei die Daten nicht in Blockchain abgelegt, sondern nur mittels blockchainbasierter Technologien zugreifbar gestaltet werden. Das Ausloten der möglichen Anwendungsfälle sowie die Schaffung der notwendigen Lösungswege für die Nutzung von Blockchain für personenbezogene (Content, Metadaten, Identitätsdaten) wie aufbewahrungspflichtige Daten sind zwei Schwerpunkte weiterer Forschungsarbeiten, wie dies z.B. im Rahmen des Programms Horizon 2020 der EU bereits geplant ist[18].

Zusammenfassend lässt sich feststellen, dass insbesondere der beschriebene Vorschlag einer logischen Blockchain im Verbund mit [RFC4998] als Basis für weitere Forschungs- und vor allem Standardisierungsarbeiten dienen kann. Deren Ziel wäre es, die Verfahren zur Beweiswerterhaltung auf Basis der Blockchain im Rahmen der geltenden rechtlichen Vorgaben [eIDAS], [VDG], [EUDSGVO] sowie des Stands der Technik [RFC4998], [SR019510], [TR03125] zu standardisieren, um zum einen hohe Aufwände für Individualentwicklungen zu vermeiden, zum anderen komplexitätsreduzierte wie performantere Lösungen zu entwickeln. Für den Fall, dass komplette oder Teile von AIP, so z.B. Identitäts- und Prozessdaten (vgl. Abschnitt 3.2.3), in der Blockchain verbleiben, sind darüber hinaus weitere, umfangreiche Forschungs- und Normungsarbeiten insbesondere hinsichtlich einer standardisierten Berichtigung und Löschung sowie Übertragbarkeit in maschinenlesbare Standardformate gem. [EUDSGVO] sowie zur Informationserhaltung [ISO14721] notwendig. Gleiches gilt für die sichere Identifikation und Authentisierung.

[18] Vgl. z.B. Programm Horizon 2020 „Transformative impact of disruptive technologies in public services“

Literatur

[BSIGS] IT-Grundschutz-Kompendium. Bundesamt für Sicherheit in der Informationstechnik, Köln 2018.

[BuBa15] N. Buchmann und H. Baier: Elektronische Identifizierung und vertrauenswürdige Dienste, DACH-Security 2015. S. 49-50. Frechen 2015.

[CGR11] C. Cachin, R. Guerraoui, L. Rodrigues, Reliable and Secure Distributed Programming, Berlin, Heidelberg, 2011.

[Di18] Digiconomist, Bitcoin Energy Consumption Index, https://digiconomist.net/bitcoin-energy-consumption, 2018.

[DIN31647] DIN 31647:2015 Beweiswerterhalt kryptografisch signierter Dokumente, 2015.

[EIDAS] VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG“ vom 23.07.2014.

[EUDSGVO] VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschtz-Grundverordnung).

[Fi06] S. Fischer-Dieskau: Das elektronisch signierte Dokument als Mittel zur Beweissicherung, Baden-Baden, 2006.

[Gia11] D. Giaretta: Advance Digital Preservation. Berlin, Heidelberg 2011

[GOS16] Distributed Ledger Technology:beyond block chain, a report by the UK Government Chief Scientific Adviser.

[ISO13527] ISO 13527:2010, Space data and information transfer systems - XML formatted data unit (XFDU) structure and construction rules, 2010.

[ISO14721] ISO 14721:2012, Space data aninformation transfer systems - Open archival information system - Reference model, 2nd Edition, 2012.

[ISO15489] ISO 15489-1:2016: Information and documentation - Records management - Part 1: Concepts and principles. 2016.

[ISO27001] ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements. 2013

[Ko13] U. Korte, S. Schwalm, D. Hühnlein: Vertrauenswürdige und beweiswerterhaltende Langzeitspeicherung auf Basis von DIN 31647 und BSI TR-03125, Informatik 2013, GI-LNI, P220, ISBN 978-3-88579-614-5, S. 550-566, 2013.

[Ko14] U. Korte, S. Schwalm, D. Hühnlein: Standards und Lösungen zur langfristigen Beweiswerterhaltung. DACH-Security 2014, S. 46-58. Frechen 2014.

[KSDV15] T. Kusber, S. Schwalm, A. Dörner, T. Vogt, Die Bedeutung der eIDAS-Verordnung für Unternehmen und Behörden. Neue Chancen und Herausforderungen für vertrauenswürdige elektronische Geschäftsprozesse in Europa, Berlin, 2015.

[KuSc16] T. Kusber, S. Schwalm: Elektronische Langzeitspeicherung als SOA-Dienst – Kernelement eines vertrauenswürdigen Informationsmanagements. INFORMATIK 2016 S. 869-882.

[Lem16] V. L. Lemieux: "Trusting Records: Is Blockchain Technology the Answer?", Records Management Journal 26.2.2016.

[Merk] R. Merkle: Protocols for Public Key Cryptosystems, Proceedings of the 1980 IEEE Symposium on Security and Privacy (1980) 122-134.

[Na08] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

[DEO17] OECD Digital Economy Outlook 2017, OECD Publishing, Paris. Chapter 7, Technology Outlook (page 293).

[RFC4998] T. Gondrom, R. Brandner, U. Pordesch: Evidence Record Syntax (ERS), IETF RFC 4998, http://www.ietf.org/rfc/rfc4998.txt, August 2007.

[RFC6283] A. J. Blazic, S. Saljic, T. Gondrom: Extensible Markup Language Evidence Record Syntax, IETF RFC 6283, http://www.ietf.org/rfc/rfc6283.txt, Juli 2011.

[Ro07] A. Rossnagel: Langfristige Aufbewahrung elektronischer Dokumente, Anforderungen und Trends, Baden-Baden, 2007.

[Sc17] S. Schwalm: A service for the preservation of evidence and data – a key for a trustworthy & sustainable electronic business. Open Identity Summit 2017. Lecture Notes in Informatics (LNI). Proceedings. Bonn 2017 S. 131-144.

[SR019510] ETSI SR 019 510, Electronic Signatures and Infrastructures (ESI); Scoping Study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures, ETSI V1.1.1 (2017-05).

[To07] P. M. Toebak: Records Management. Ein Handbuch. Baden 2007.

[TR03125] BSI: Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR), TR 03125, V1.2.1, 2018.

[TR03125-F] BSI Technische Richtlinie 03125. Beweiswerterhaltung kryptographisch signierter Dokumente. Anlage TR-ESOR-F: Formate. Version 1.2,1 Stand: 15.03.2018.

[VDG] Vertrauensdienstegesetz vom 18. Juli 2017 (BGBl. I S. 2745), das durch Artikel 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist

[WEKJ17] C. Welzel, K. Eckert, F. Kirstein, V. Jacumeit: Mythos Blockchain - Herausforderung für den öffentlichen Sektor, Berlin, 2017.

[We18] M. Weber, T Vogt, W. Krogel, S. Schwalm: Records Management nach ISO 15489. Einführung und Anleitung. Berlin 2018.

[Wi15] B. Wildhaber et.al.: Leitfaden Information Governance. Zürich 2015.

[Zi17] S. Zimprich: Blockchain der Hype und das Recht. Berlin 2017.