Konsistentes Löschen in der Block Chain

Dr. Ulrich Kampffmeyer

PROJECT CONSULT
Unternehmensberatung
Dr. Ulrich Kampffmeyer GmbH

Hamburg, 2019

Konsistentes Löschen in der Block Chain

Dr. Ulrich Kampffmeyer, PROJECT CONSULT Unternehmensberatung GmbH, Hamburg
Artikel aus dem PROJECT-CONSULT-Newsletter 01-2019 vom 27.02.2019

Es gibt nicht die EINE Art der Blockchain sondern verschiedene.

Blockchain verhindert das Löschen. So die gängige Meinung. Wird etwas in der Blockchain verändert, führt dies sofort zur Inkonsistenz. Die meisten Menschen gehen immer von der öffentlichen Distributed Ledger Blockchain mit verteiltem Proof-of-Work aus, wie z.B. virtuellen "Währungen" (BITCOIN und Co.) zu Grunde liegt. Hier wird durch die Verteilung und das Verfahren der Bestätigung der Transaktionen durch alle Beteiligten die Veränderung ausgeschlossen.

Es geht aber auch anders. Blockchain ist in erster Linie eine besondere Art der Verkettung. Wikipedia sagt zu Blockchain:

"*Eine Blockchain (auch Block Chain, englisch für Blockkette) ist eine kontinuierlich erweiterbare Liste von Datensätzen, genannt „Blöcke“, welche mittels kryptografischer Verfahren miteinander verkettet sind. Jeder Block enthält dabei typischerweise einen kryptografisch sicheren Hash (Streuwert) des vorhergehenden Blocks, einen Zeitstempel und Transaktionsdaten*".

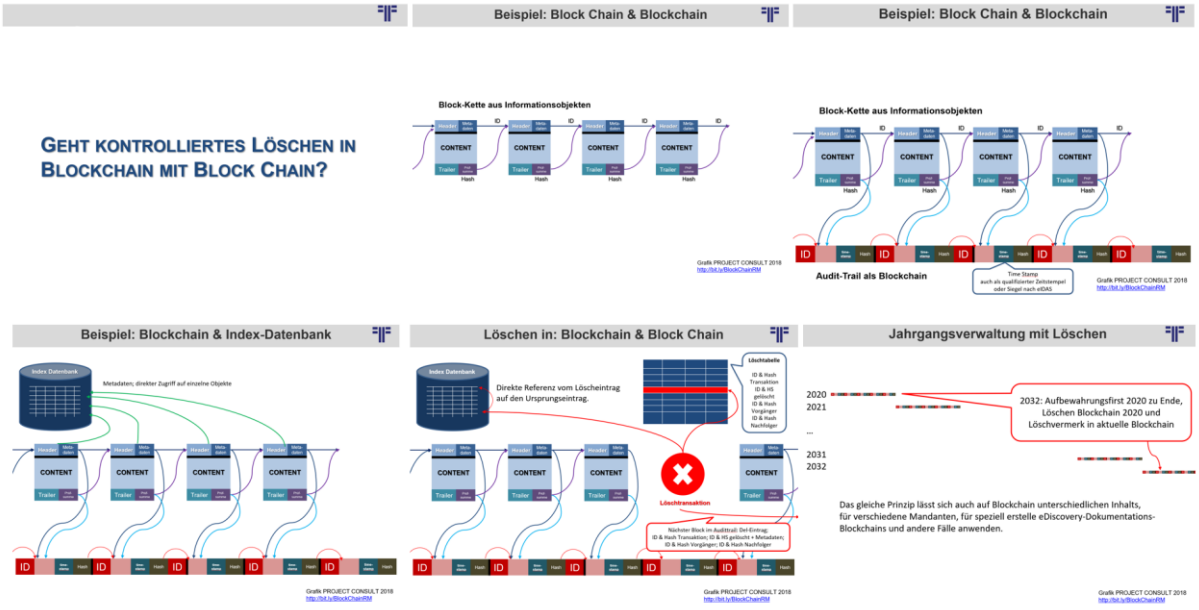
Beim Einsatz im Records Management und der revisionssicheren Archivierung geht es eher um das Modell "Auditing-Blockchain", Wikipedia schreibt hierzu (:

"*Beim Auditing in der Informationstechnik geht es darum, sicherheitskritische Operationen von Softwareprozessen aufzuzeichnen. Dies betrifft insbesondere den Zugriff auf und die Veränderung von vertraulichen oder kritischen Informationen. Das Auditing eignet sich hierbei deshalb für eine Blockchain, weil es relativ geringe Datenmengen produziert und gleichzeitig hohe Sicherheitsanforderungen aufweist. Eine Blockchain kann hierbei das Audit-Log (auch als Audit-Trail bezeichnet) vor Veränderung schützen. Zudem sollten die einzelnen Einträge mit einer digitalen Signatur versehen werden, um die Echtheit zu gewährleisten. Ein dezentraler Konsensmechanismus, wie bei Bitcoin, wird nicht zwingend benötigt.*"

Kombination von Block Chain mit Audit-Blockchain

Gehen wir einen Schritt weiter: Verkettung plus Audit-Trail zur zusätzlichen Absicherung. Für Records-Management- und Archivsysteme, die Inhouse oder in einer eigenen privaten Cloud laufen, lassen sich so andere Blockchain-Architekturen aufbauen, die nicht wie die Internet-Währungen funktionieren. Sie sichern sich durch die Verkettung sowie zusätzlich durch einen Audit-Trail, der ebenfalls als Blockchain aufgebaut ist. So etwas kann man dann als "Block Chain mit Blockchain" nennen. Zur einfacheren Unterscheidung benutzen wir für die nur verketteten Blöcke den Begriff Block Chain in zwei Worten.

Die Bildung von Prüfsummen mit Hash und deren Anhängen an Informationsobjekte gibt es schon sehr lange in der elektronischen Archivierung. Hieraus lässt sich einfach der nächste Schritt der Verkettung generieren. Dies alles wird in einem Audit-Trail protokolliert, in dem die Operationen mit den Transaktionsdaten, dem Zeitstempel und anderen Attributen kontinuierlich aufgezeichnet werden. Die Informationsobjekte (oder Dokumente) liegen vereinzelt vor und sind nicht Bestandteil des Audit-Trails selbst. Wie das Eintragen eines neuen Blocks kann nun auch das Austragen eines Blockes geschehen. Hierfür müssen aber zusätzlich noch ID, Hashwert und Transaktionsdaten des dem zu löschenden Block vorausgehenden und folgenden eingetragen werden. Erfolgt das Lesen der Retrieval-Information vom Jüngsten zum Ältesten wird zunächst die "Block-Löschungs-Information" gefunden. Die Audit-Trail-Daten inkl. den dort mitgespeicherten Metadaten stehen aber weiterhin zur Verfügung und sorgen für Nachvollziehbarkeit. Das Thema der Absicherung über Zeitstempel lässt sich entsprechend eIDAS auch mit zertifizierten Zeitstempeln als Fernsignaturen erreichen, die als qualifizierte Signaturen einen noch höheren Nachweiswert haben. Alternativ kann auch in verteilten Organisationen oder Verbünden über Master-Nodes nachgedacht werden.



Konsistentes Löschen in einer Block Chain

Eines der Argumente gegen die Blockchain ist die DSGVO, die das bedarfsweise Löschen von Informationen vorschreibt. Blockchain-Lösungen à la Bitcoin sind so für Archivierung und Records Management nicht geeignet.

In unserem Ansatz der Kombination von Block Chain - verketteten Informationsobjekten - mit der Blockchain - als zusätzlich kontinuierlich durch Hashwert-Bildung abgesichertem Protokoll (Audittrail) - wird es möglich, Informationsobjekte konsistent sowohl logisch als auch physisch aus der Block Chain zu entfernen. Das Entfernen entspricht dem Ersetzen oder Ändern

unrichtiger Information ebenso wie dem Löschen nicht mehr benötigter oder unzulässiger Information. Im unveränderbaren, kontinuierlich weiter geschriebenen Audittrail werden zusätzlich zur eigentlichen Transaktion der Typ der Transaktion, die notwendigen Daten des Vorgängers in der Kette und des Nachfolgers in der Kette mit gespeichert, so dass die Lücke über das Protokoll nachvollziehbar geschlossen wird. Das Protokoll gibt außerdem den Nachweis, welches Objekt mit welchem Inhalt entfernt wurde. Dies entspricht auch den Prinzipien des Records Management, dass nicht geändert oder gelöscht wird ohne einen Nachweis. Um Fehler und Inkonsistenzen bereits programmtechnisch schneller als das Durchsuchen der Audittrail-Blockchain zu ermöglichen, empfiehlt sich ein gesichertes Extra-Protokoll oder eine Tabelle mit den Änderungen und Löschungen zu führen. Ein solches Änderungs- und Löschprotokoll gehörte bereits zu den Prinzipien der revisionssicheren Archivierung Mitte der 90er Jahre. Stößt man beim Arbeiten mit Dokumenten (Informationsobjekten) auf ein entferntes Objekt, so wird dieser Fehler zunächst performant gegen das Löschprotokoll/Löschtabelle (und andere Fehler-Tabellen) geprüft und eine entsprechende Information ausgegeben. Ob Informationsobjekte nun logisch oder physisch gelöscht werden (müssen) obliegt dem Inhalt und dem Anwendungsfall. Ältere Archivsysteme haben nur Dokumente direkt gespeichert und sind daher - leider - nicht in der Lage den Informationsobjekt-basierten Ansatz der Kombination von Blockchain mit Block Chain umzusetzen.

Die Zukunft

Blockchain als Audittrail-Blockchain wird vielfältige Anwendungen im Records Management und bei der elektronischen Archivierung finden. Der Verknüpfungsansatz von Block Chain mit Audittrail-Blockchain steht noch am Anfang. Generell ist aber bei der elektronischen Archivierung von Massendaten, die nicht mehr mit bisherigen Referenz-Datenbank-Architekturen von Archivsystemen erfasst werden können, der Einsatz von Standard-Blockchain-Technologien unterschiedlicher Ausprägung (fast alle ohne Löschmöglichkeit) auf dem Vormarsch. 2019 wird dies sicherlich noch ein Hype-Thema bleiben. Die Zukunft der Blockchain im Records Management und der Archivierung wird erst später beginnen.

Impressum

Quelle: PROJECT-CONSULT-Newsletter 01-2019 vom 27.02.2019, der ISSN 1349-0809, Creative Commons CC by-nc-nd 4.0 Open Access.

Geschäftsleitung und V. i. S. d. P.: Dr. Ulrich Kampffmeyer
Anschrift der Redaktion:
PROJECT CONSULT Unternehmensberatung
Dr. Ulrich Kampffmeyer GmbH
Isestraße 63, 20149 Hamburg
Telefon: +49 40 412856 53
E-Mail: presse@project-consult.com
http://www.project-consult.de

Über den Autor

Dr. Ulrich Kampffmeyer ist seit über 35 Jahren im Thema Informationsmanagement zu Hause. Als Geschäftsführer und Unternehmensberater seines Beratungsunternehmens PROJECT CONSULT (http://PROJECT-CONSULT.de) berät er Unternehmen bei der Strategie, Konzeption, Einführung, Ausbau und Migration von Information Management-Lösungen.

Er gründete und leitete Fachverbände, arbeitete bei internationalen Standardisierungen mit und gilt als Mentor der Information-Management-Branche in Europa.

Dr. Kampffmeyer ist international anerkannter Autor, Kongressleiter, Referent und Moderator zu Themen wie Information Management, Information Governance, elektronische Archivierung, Records Management, ECM Enterprise Content Management, Dokumentenmanagement, Workflow, Rechtsfragen, Wissensmanagement, Digitalisierung und Collaboration. Auf zahlreichen nationalen und internationalen Kongressen und Konferenzen wirkte er als Keynote-Sprecher mit. Er engagiert sich besonders für die Rolle und Ausbildung des Information Professional der Zukunft.

Von Fachzeitschriften wurde zweimal unter die 100 wichtigsten IT Macher Deutschlands gewählt. Sein Curriculum Vitae findet sich auf Wikipedia http://bit.ly/WP_DrUKff

PROJECT CONSULT

Die PROJECT CONSULT GmbH ist ein hersteller- und produktunabhängiges Beratungsunternehmen für Information Management und Information Governance.

Zum Beratungsportfolio gehören IT-Strategie, Fachberatung, Planung und Organisation zu Einführung, Migration und Abnahme von Informationssystemen; Projektmanagement, Change Management und Coaching für Projekte des Informationsmanagement wie elektronische Archivierung, Knowledge-, Dokumenten-, E-Mail-, Enterprise-Content-Management und Compliance.