(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
02. April 2020 (02.04.2020)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2020/064055 A1

(51) Internationale Patentklassifikation:
H04L 9/32 (2006.01) *G06F 16/20* (2019.01)

(21) Internationales Aktenzeichen: PCT/DE2019/100841

(22) Internationales Anmeldedatum:
24. September 2019 (24.09.2019)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2018 123 463.5
24. September 2018 (24.09.2018) DE

(71) Anmelder: **AKARION AG** [DE/DE]; c/o ARQIS, Prinzregentenplatz 7, 81675 München (DE).

(72) Erfinder: **MASCHEK, Sascha**; Breinbauerweg 6, 4040 Linz (AT). **EMATHINGER, Paul**; Böhmerwaldstrasse 10, 4020 Linz (AT).

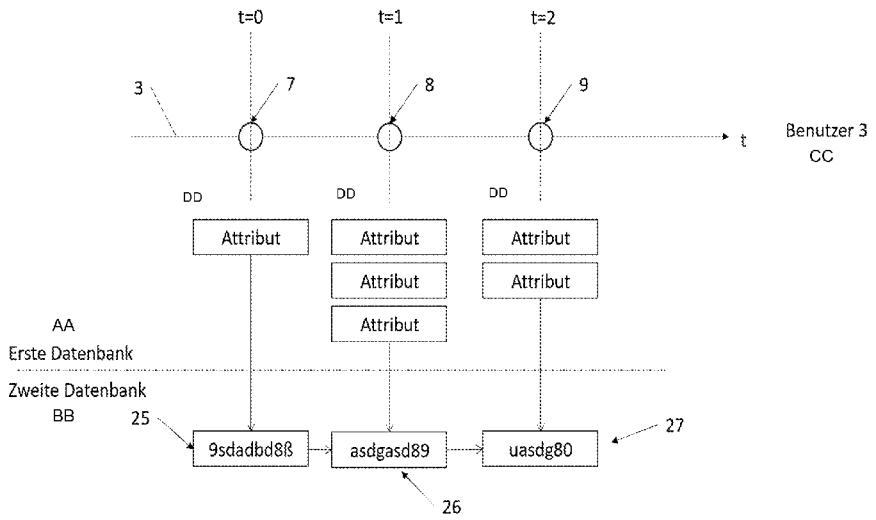
(74) Anwalt: **WHITE IP GRUNER, MERZ & STÖHR PATENTANWALT UND RECHTSANWÄLTE IN PARTNERSCHAFT MBB**; GRUNER, Leopold, George-Bähr-Straße 18, 01069 Dresden (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ,

(54) **Title:** DATABASE AND METHOD FOR DATA DELETION

(54) **Bezeichnung:** DATENBANK UND VERFAHREN ZUR DATENLÖSCHUNG



Figur 2

AA Première base de données
BB Seconde base de données
CC Utilisateur 3
DD Attribute

(57) **Abstract:** The invention relates to a method for deleting a data element from a data structure, comprising the following steps: calculating a hash value at least on the basis of the data element to be deleted within an entity, and replacing the data element in the data structure by the calculated hash value.

(57) **Zusammenfassung:** Verfahren zum Löschen eines Datenelements aus einer Datenstruktur, umfassend die folgenden Schritte: Berechnen eines Hashwertes mindestens auf Basis des zu löschenden Datenelements innerhalb einer Instanz, und Ersetzen des Datenelements in der Datenstruktur durch den berechneten Hashwert.

[Fortsetzung auf der nächsten Seite]

WO 2020/064055 A1

RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eingehen (Regel 48 Absatz 2 Buchstabe h)*

Beschreibung

Datenbank und Verfahren zur Datenlöschung

Technischer Hintergrund

Die im Folgenden diskutierte Erfindung betrifft ein computerimplementiertes Verfahren zum Verarbeiten von Datensätzen umfassend Attribute oder andere Datenelemente in einer Datenbank, wobei ein ursprünglicher Datensatz und weitere ursprüngliche Datensätze durch funktionelle und/oder logische Referenzen verbunden sind, wobei gegebenenfalls bei der Erstellung und/oder bei einer Veränderung der Datensätze mittels einer Hashfunktion ein Hashwert erstellt wird, wobei die Hashwerte die betreffenden Attribute eines Datensatzes beschreiben, wobei die Attribute zumindest ein Zeitattribut, Benutzerattribute und Referenzen zwischen den einzelnen Benutzerattributen umfassen, wobei das Zeitattribut den Zeitpunkt der Erstellung beziehungsweise der Veränderung eines Attributs oder des Datensatzes beschreibt, wobei das Benutzerattribut eine Angabe über den die Erstellung beziehungsweise die Veränderung eines Datensatzes vornehmenden Benutzer und/oder eines vom Benutzer zu bedienenden Gerätes umfasst.

Insbesondere bei der Verwaltung von personenbezogenen Daten besteht ein Interesse, sämtliche Änderungen in einer Datenbank jederzeit oder zumindest innerhalb eines definierten Zeitraumes rückverfolgen zu können.

Die vorliegende Erfindung bezieht sich auf das technische Gebiet der Datenverarbeitung. Auf diesem technischen Gebiet der Datenverarbeitung sind verschiedene Techniken aus dem Stand der Technik bekannt.

Aus dem Stand der Technik ist eine Technik bekannt, bei der aus Daten ein sogenannter Streuwert (Hash oder Hashwert) berechnet wird. Regelmäßig kommt dabei eine sogenannte Streuwertfunktion (Hashfunktion) zum Einsatz. Eine solche Hashfunktion wird im Stand der Technik beispielsweise durch den sicheren Hash-Algorithmus (SHA, secure hash algorithm) bereitgestellt. Mit einer Hashfunktion kann häufig ein in seiner Größe nicht notwendigerweise beschränkter Datenblock auf einen Datenblock fester Größe, den Hash oder Hashwert, abgebildet werden. Eine typische Länge für einen Hash ist beispielsweise 256 bit. Eine wünschenswerte Eigenschaft einer guten kryptologischen Hashfunktion ist eine näherungsweise Injektivität und eine dadurch erzielte näherungsweise Kollisionsresistenz. Die „ideale Hashfunktion" ist daher vollständig linkseindeutig und kollisionsfrei und bildet unterschiedliche Eingangsdaten immer auf unterschiedliche Hashes ab.

In einem typischen Anwendungsfall für eine Hashfunktion wird ein Hashwert für eine größere Datenmenge berechnet. Beispielsweise soll eine größere Datenmenge über ein möglicherweise nicht sicheres Übertragungsmedium, wie das Internet, übertragen werden. Zum Beispiel kann durch einen technischen Fehler ein Teil der Daten falsch übertragen werden oder ein Dritter manipuliert diese Daten.

Wenn der Sender der Daten ihren Hashwert berechnet und diesen Hashwert dem Empfänger zur Verfügung stellt, kann der Empfänger die Echtheit und Unverfälschtheit der Daten verifizieren, vorausgesetzt der Hashwert selbst ist echt und verlässlich.

Das Verfahren bringt jedoch den Nachteil mit sich, dass das Verfahren völlig außer Kraft gesetzt wird, wenn der Hashwert selbst manipuliert wird. In einem Beispiel überträgt ein Benutzer A an einen Benutzer B eine Datei und außerdem den Hashwert der Datei. Ein Angreifer C fängt diese Kommunikation ab und ersetzt die Datei durch eine gefälschte Datei. Die

gefälschte Datei enthält gefälschte Daten. Außerdem ersetzt C den Hashwert der Datei durch den Hashwert der gefälschten Datei. Wenn B nun die Daten empfängt und überprüft, indem er die Hashfunktion der Datei selbst berechnet und mit dem Hashwert vergleicht, kommt er zu dem Schluss, dass die Daten nicht manipuliert wurden. So hat C erfolgreich die Daten manipuliert, ohne dass dies von B festgestellt wurde.

Um dies zu vermeiden, ist ein anderes Verfahren als sogenannte Blockverkettung (block chain) bekannt. Eine Blockverkettung besteht aus Daten, welche in Form von aneinandergereihten Datenblöcken organisiert sind. Einer Blockverkettung kann so bei Bedarf ein weiterer Datenblock am Ende der Blockverkettung angefügt werden. Dabei wird ein Hashwert des vorhergehenden Blocks, zusätzlich zu eventuellen Nutzerdaten, in jedem neuen Block gespeichert.

Wird ein Block innerhalb der Blockverkettung durch einen Angreifer manipuliert, wird die Verkettung inkonsistent. Für eine erfolgreiche Manipulation muss durch den Angreifer daher ein gewisser Teil der Kette neu berechnet werden. Die Blockverkettung stellt so eine hohe Datenintegrität der auf ihr gespeicherten Daten zur Verfügung.

Blockverkettungen haben verschiedene Anwendungsbereiche. Im Bereich der virtuellen Währungen können Blockverkettungen eingesetzt werden, beispielsweise bei der Währung Bitcoin. Bei Bitcoin besteht eine Blockverkettung aus einer Reihe von Datenblöcken, in denen jeweils eine oder mehrere Transaktionen zusammengefasst und mit einer Prüfsumme versehen sind, d. h., sie werden jeweils paarweise zu einem Hash-Baum zusammengefasst.

Der Stand der Technik für Blockverkettung hat jedoch den Nachteil, dass er schlecht skalierbar ist. Da Blockverkettungen kommunikations- und rechenintensiv sind, weil alle „Knoten", die an der Blockverkettung beteiligt sind, untereinander abgeglichen

werden müssen, können nach derzeitigem Stand nur sehr wenige Transaktionen (d.h. Einträge in eine Blockverkettung) pro Sekunde weltweit durchgeführt werden. Allerdings besteht ein wachsender Bedarf an Speicherplatz und anderen Ressourcen wie Bandbreite.

Zu Zwecken der Transparenz, sind Blockverkettungen häufig öffentlich zugänglich, wodurch sie überprüfbar werden, aber auch für andere einsehbar sind. Das hat den Nachteil, dass vertrauliche Daten nicht in die Kette eingebracht werden können, oder die Kenntnisnahme der Daten durch Dritte in Kauf genommen werden muss.

Ein weiterer Nachteil besteht in der geringen Flexibilität der Verkettung. Häufig werden Daten nur für einen gewissen Zeitraum benötigt, und sind danach überflüssig, sollen anonymisiert oder pseudonymisiert werden (oder sollen sogar ganz gelöscht werden, z.B. um gesetzliche Vorgaben z. B. im Datenschutz zu erfüllen). Sind diese Daten aber nun in die Blockverkettung eingebracht, sind sie fester Teil der Kette, belegen Ressourcen, und können nicht problemlos entfernt oder geändert werden, ohne die Verkettung dabei zu zerstören.

Zudem ist die redundante Speicherung von Daten, die aufgrund der Geheimhaltung und dem damit verbundenen Erfordernis der Unveränderbarkeit von Daten erforderlich ist, sehr kostenintensiv, wobei schon für die Speicherung von geringen Datenmengen enorme Kosten entstehen können.

Der vorliegenden Erfindung liegt daher die technische Aufgabe zugrunde, Verfahren bereitzustellen, die die Nachteile des Standes der Technik überwinden und neue Lösungen ermöglichen. Insbesondere werden flexiblere, skalierbare, sicherere, datenschutzkonformere, verlässlichere Lösungen benötigt. Auch der Faktor der Kostenminimierung spielt eine wesentliche Rolle.

Die Nachteile des Standes der Technik werden überwunden durch das Verfahren zum sicheren Löschen von Daten einer Datenstruktur nach Anspruch 1.

Beschreibung der Erfindung

Die vorliegende Erfindung schafft ein Verfahren zum Löschen eines Datenelements mit den Merkmalen des Anspruchs 1.

Weitere vorteilhafte Ausgestaltungen sind in den Unteransprüchen angegeben.

Demgemäß ist ein Verfahren zum Löschen eines Datenelements aus einer Datenstruktur vorgesehen, umfassend die folgenden Schritte: Berechnen eines Hashwertes mindestens auf Basis des zu löschenden Datenelements innerhalb einer Instanz und Ersetzen des Datenelements in der Datenstruktur durch den berechneten Hashwert.

Durch das Ersetzen wird das Datenelement selbst datenschutzkonform gelöscht. Ein Datenelement kann durch die Berechnung seines Hashwertes und dem Vergleichen dieses Hashwertes mit einem Referenzwert verifiziert werden. Wenn ein Datenelement bereits aus der Datenstruktur mit einem Verfahren nach Anspruch 1 gelöscht wurde, so kann die Datenintegrität nach wie vor verifiziert werden, indem der Hash ausgelesen wird. Dies ist möglich, da der Hash noch vorhanden ist und ausgelesen werden kann, wenn das Datenelement mit dem Verfahren nach Anspruch 1 gelöscht wurde. So wird sichergestellt, dass eine Instanz auch dann verifiziert werden kann, wenn ein oder mehrere Datenelemente bereits gelöscht wurden. Dadurch wird zudem sichergestellt, dass die Verifikation von übrigen Daten auch nicht durch das gelöschte Element beeinträchtigt wird.

Es kann insbesondere der Hashwert, oder ein anderer Fingerabdruck, der auf diesem Hashwert beruht, in einem

öffentlichen Medium und/oder einem nur schwer veränderlichen Medium gespeichert werden, wie beispielsweise einer Blockverkettung. Die Datenintegrität kann dann mit diesem sehr sicheren Hashwert überprüft werden. Gleichzeitig ist die Vertraulichkeit gewahrt, und das Verfahren nach Anspruch 1 kann das Datenelement datenschutzkonform löschen. In dem schwer veränderlichen und/oder öffentlichen Medium, bleibt nur der Hashwert zurück. Der Angreifer kann dort die Quelldaten, die das gelöschte Datenelement konstituieren, nicht finden. Der Angreifer kann gelöschte Datenelemente nicht rekonstruieren, da der Hash auf dem öffentlichen Medium aus vielen Einzelhashes aggregiert wurde.

Gemäß einer Weiterbildung erfolgt die Berechnung von Hashwerten für Datenelemente auf Basis einer Struktur, welche das Datenelement und ein weiteres Datenelement, insbesondere einen Seed/Salt, umfasst.

Eine gute Hashfunktion sollte nicht oder nur unter schwierigen Umständen umkehrbar sein. Sogenannte Brute-Force-Angriffe sind jedoch möglich. In einer Variante wird von einem Angreifer eine sogenannte Wörterbuchattacke eingesetzt.

In einem einfachen Beispiel mit nur einem Datenelement ist das Datenelement durch „John" gegeben. Der zugehörige SHA256-Hashwert ist durch a8cfcd74832004951b4408cdb0a5dbcd8c7e52d43f7fe244bf720582e05241da gegeben. Ein Angreifer entscheidet sich für einen Wörterbuchangriff und prüft bekannte Vornamen. Durch seine Beschränkung auf Vornamen ist sein Angriff sehr effizient. Nach kurzer Zeit stellt er durch Ausprobieren auf Grundlage des Wörterbuchs fest, dass der oben zitierte Hash dem Datenelement „John" entspricht. So hat der Angreifer auf Basis eines

Hashwertes die ursprünglichen Daten erlangt. Ein solcher Angriff ist auch für Instanzen mit mehreren Datenelementen denkbar.

Durch den Einbezug eines weiteren Datenelements werden Wörterbuchattacken stark erschwert, insbesondere wenn es keinen systematisch-inhaltlichen Bezug zu den Datenelementen aufweist.

Durch den Einbezug eines weiteren Datenelements, insbesondere eines Seeds/Salts, beim Verfahren zum Sichern wird sichergestellt, dass es für einen Angreifer äußerst schwierig oder praktisch unmöglich ist, die Daten aus dem Master-Hashwert, der auf dem Medium oder System, welches die Integrität der auf ihm gespeicherten Daten algorithmisch und/oder mathematisch absichert, gesichert wird, zu rekonstruieren.

Durch den Einbezug eines weiteren Datenelements, insbesondere eines Seeds/Salts, beim Verfahren zum Löschen eines Datenelements wird zudem sichergestellt, dass es für einen Angreifer äußerst schwierig oder praktisch unmöglich ist, das gelöschte Datenelement aus dem Hashwert, durch den das Datenelement beim Löschen ersetzt wurde, zu rekonstruieren.

Dadurch ist es möglich, die Vertraulichkeit der Daten besser abzusichern und datenschutzkonform zu arbeiten.

Gemäß einer Weiterbildung wird zumindest teilweise das ursprüngliche Datenelement in der Datenstruktur durch den berechneten Hashwert überschrieben und/oder es werden Bereiche des ursprünglichen Datenelements, die nicht durch den berechneten Hashwert überschrieben wurden mit anderen Daten, insbesondere randomisierten Daten, insbesondere mehrfach, überschrieben.

So wird das zu löschende Datenelement besonders sicher und datenschutzkonform gelöscht, und kann von einem Angreifer nicht aus dem überschriebenen Speicherbereich rekonstruiert werden.

Bevorzugt wird die gesamte ursprüngliche Struktur, welche das Datenelement und ein weiteres Datenelement, vorzugsweise einen Seed/Salt, umfasst, in der Datenstruktur durch den ursprünglich berechneten (Einzel-)Hashwert überschrieben.

Alternativ kann vorgesehen sein, dass zumindest das Datenelement der usprünglichen Struktur, welche das Datenelement und ein weiteres Datenelement, vorzugsweise einen Seed/Salt, umfasst, innerhalb der Datenstruktur mit anderen Daten, insbesondere randomisierten Daten, insbesondere mehrfach, überschrieben wird. Wichtig ist hierbei, dass die Daten, die zum Überschreiben des Datenelements verwendet werden, zusammen mit dem verbleibenden weiteren Datenelement, vorzugsweise dem Seed/Salt, dem Hashwert abbilden, der ursprünglich auf Basis der Struktur, welche das zu überschreibende Datenelement und das weitere Datenelement, insbesondere den Seed/Salt, umfasst, berechnet wurde.

Die vorliegende Erfindung umfasst auch einen Computer, ein Computernetzwerk oder ein Computersystem, insbesondere ein verteiltes Computersystem, welches eingerichtet ist, um ein hierin offenbartes Verfahren zum Löschen eines Datenelements auszuführen.

Ergänzend zu dem vorgenannten Computer, Computernetzwerk bzw. Computersystem, umfasst die vorliegende Erfindung ferner auch ein Computerprogramm, das Befehle umfasst, die bewirken, dass der Computer, das Computernetzwerk oder das Computersystem die Verfahrensschritte des hierin offenbarten Verfahrens ausführt.

Abschließend ist von der vorliegenden Erfindung auch ein computerlesbares Medium eingeschlossen, auf dem das vorgenannte Computerprogramm gespeichert ist.

Weitere technische Vorteile ergeben sich dem Fachmann aus den folgenden Ausführungen zur Erfindung:

Unter dem Begriff Datensatz versteht der Fachmann eine Gruppe von inhaltlich zusammenhängenden Attributen, d.h. Datenelementen, die zu einem bestimmten Objekt gehören und die innerhalb eines Datenbestands identische Strukturen aufweisen. Datensätze entsprechen dabei einer logischen Struktur, die bei der Erstellung eines Dokuments (z.B. im konzeptionellen Schema der Datenmodellierung) festgelegt wurde.

Wie hierin deutlich ist, ist ein Attribut demnach ein Datenelement innerhalb eines Datensatzes. Als Daten, die in ein solches Datenelement eingebracht sind, kommen beispielsweise Textdaten, d.h. Zeichenketten, zum Einsatz, wenngleich die Erfindung nicht auf Textdaten als Datentyp beschränkt ist, sondern auch andere Datentypen wie beispielsweise Bilddaten, Audiodaten, Videodaten, Binärdaten etc. enthalten kann. Es können auch Dateien oder Teile von Dateien als Daten zum Einsatz kommen. Beispielsweise können die Daten so auch in einem Dateiformat vorliegen oder einem Format oder in einer Form, welche einem Dateiformat ähnelt. In einem weiteren Beispiel kommen Daten im Format JavaScript Object Notation (JSON-Format) zum Einsatz.

Die Daten können beispielsweise so ausgestaltet sein, dass sie Datenelemente enthalten, die in einem Dateiformat vorliegen. Zum Beispiel kann ein Bild ein Datenelement sein und im JPEG-Format vorliegen. Datenelemente können aber auch kleinere Einheiten sein. Insbesondere kann dabei ein Dateiformat beispielsweise die den Datenelementen übergeordnete Struktur festlegen. Beispielsweise kann eine Datei im JSON-Format vorliegen und

viele Datenelemente enthalten, wobei die Datenelemente selbst beispielsweise Textdaten enthalten.

Das erfindungsgemäße Verfahren widmet sich dem Problem der Rückverfolgbarkeit von Änderungen von Datensätzen einer Datenbank. Die im Folgenden skizzierte technische Lösung sieht vor, dass eine generische Datenbank geschaffen wird, wobei die Datenbank insbesondere für die Verwaltung von Personendaten, aber auch zur Verwaltung von beliebig gestalteten Objektdaten geeignet ist. Ein Datensatz kann ein beliebig gestalteter Satz von Daten sein. Verschiedene Datensätze können identisch, verschieden oder überlappend sein, und werden daher auch als Dateninstanzen oder Instanzen bezeichnet.

Erfindungsgemäß wird dies dadurch erreicht, dass bei einer vom Benutzer angeordneten Veränderung eines Eintrages des Datensatzes durch einen Benutzer ein ursprünglicher Datensatz unverändert aufrechterhalten wird und ein neuer Datensatz umfassend den geänderten Eintrag erstellt wird, wobei neue Referenzen von dem neuen Datensatz zu den weiteren ursprünglichen Datensätzen und eine Modifikationsreferenz von dem neuen Datensatz zu dem ursprünglichen Datensatz erstellt wird, wobei die Modifikationsreferenz eine zeitliche Entwicklung dokumentiert und gegebenenfalls eine funktionelle Referenz und gegebenenfalls eine logische Referenz und gegebenenfalls eine instanzielle Referenz zwischen dem ursprünglichen Datensatz und dem zeitlich nachfolgenden Datensatz ausgewiesen wird.

Das erfindungsgemäße Verfahren löst die eingangs angeführte technische Aufgabe der Rückverfolgung von Änderungen, indem der ursprüngliche Datensatz nicht verändert und ein neuer Datensatz umfassend ein neues oder ein geändertes Attribut erstellt wird. Sämtliche Änderungen sind anhand des ursprünglichen Datensatzes und des neuen Datensatzes nachvollziehbar.

Eine logische Referenz liegt dann vor, wenn ein Datensatz A1 auf einer ersten Zeitlinie mittels logischer Referenz auf eine

zweite Zeitlinie B verweist, wobei hierdurch stets die neueste Version des Datensatzes auf der Zeitlinie B ausgewiesen wird.

Die Wirkung einer logischen Referenz kann durch das folgende Beispiel verdeutlicht werden. A1 ist ein Personendatensatz, wobei der Personendatensatz der mittels einer logischen Referenz "Lebenslauf" auf einen Datensatz B1 verweist, wobei der Datensatz B1 unter anderem das Feld "Arbeitgeber" enthält. Bei einem Arbeitgeberwechsel entsteht ein neuer Datensatz B2, wobei bei dem Datensatz B2 das Feld "Arbeitgeber" mit dem aktuellen Wert belegt ist. A1 kann dabei völlig unverändert bleiben, da die logische Referenz "Lebenslauf" immer implizit auf die neueste Version des Lebenslaufs referenziert, was in diesem Fall der Datensatz B2 ist.

Eine instanzielle Referenz liegt dann vor, wenn ein Datensatz A1 auf Zeitlinie A mittels logischer Referenz auf eine ganz bestimmte Version B(n) eines anderen Datensatzes auf Zeitlinie B zeigt. Auch wenn neuere Versionen B(n+1) des Datensatzes auf der Zeitlinie B entstehen, zeigt diese Referenz immer fortwährend auf ein und dieselbe Datensatz-Instanz B(n).

Eine Instanzenreferenz kann anhand des folgenden Beispiels erläutert werden. A1 enthält einen Personendatensatz bestehend aus Nachname und Geburtsjahr wie beispielsweise die Werte "Mustermann" beziehungsweise "1980". Zusätzlich enthält A1 eine Instanzreferenz auf B1. B1 enthält das Datenschema der zugehörigen Datensätze, in diesem Beispiel die Werte

"Nachname":"Zeichenkette" und "Geburtsjahr":"Zahl". Später wird das Datenschema verändert, wodurch B2 entsteht und beispielsweise die Werte "SV-Nummer":"Zahl" und "Geburtsdatum":"Zeichenkette" enthält. Neu entstehende Datensätze A(1+n) sollen nun auf B2 referenzieren, wobei der existierende Datensatz A1 jedoch soll nach wie vor auf B1 referenzieren soll, da sein Inhalt im Kontext von B2 gar keinen Sinn ergeben würde.

Eine funktionelle Referenz weist einen funktionellen

Zusammenhang zwischen einem ersten Datensatz und einem zweiten Datensatz aus. Beispielsweise kann ein erster Datensatz oder ein durch den ersten Datensatz wiedergegebenes Objekt wie ein Auto den zweiten Datensatz oder ein durch den zweiten Datensatz wiedergegebenes Objekt wie einen Autoschlüssel bedingen, sodass der erste Datensatz und der zweite Datensatz oder die durch die Datensätze wiedergegebenen Objekte gemeinsam eine Funktion ausführen.

Gleichzeitig wird durch das Erstellen einer Modifikationsreferenz der ursprüngliche Datensatz von dem neuen Datensatz referenziert, was wiederum den Effekt hat, dass die aufgrund des geänderten Eintrages abzuspeichernde Datenmenge auf den neuen Datensatz umfassend den geänderten Eintrag reduziert werden kann. Es muss sohin nicht die gesamte Menge an Daten neu abgespeichert werden.

Die Modifikationsreferenz weist stets die zeitliche Entwicklung vom geänderten Datensatz zum ursprünglichen Datensatz aus, wodurch die Historie der Änderungen beschreibbar ist.

Die Modifikationsreferenz kann in Ergänzung zu der Dokumentation der Historie auch eine funktionelle Referenz und/oder eine logische Referenz und/oder eine instanzielle Referenz vom geänderten Datensatz zu dem ursprünglichen Datensatz umfassen.

Der Begriff des geänderten Eintrages ist im Rahmen der Offenbarung des erfindungsgemäßen Verfahrens einem neuen Eintrag, welcher die Erstellung eines neuen Attributes bedingt, gleichzusetzen, zumal ein neuer Eintrag im Vergleich zu dem ursprünglich nicht vorhandenen Eintrag eine Änderung darstellt.

Die einzelnen ursprünglichen Datensätze weisen Referenzen auf. Ein neu abgespeicherter Datensatz umfassend den neuen Eintrag weist auch eben diese Referenzen auf. Nachdem durch die Referenzen zwischen den Attributen ein funktioneller und/oder logischer Zusammenhang dokumentiert ist, kann die Erstellung des neuen Datensatzes in Hinblick auf diesen funktionellen und/oder

logischen Zusammenhang im Rahmen der Durchführung des erfindungsgemäßen Verfahrens überprüft werden. Die Erstellung des neuen Attributs als ein Teil des erfindungsgemäßen Verfahrens ist sohin integer gegen eine Manipulation von außen.

Das erfindungsgemäße Verfahren kann auch einen Verfahrensschritt umfassen, dass die ursprünglichen Datensätze, welche älter als eine definierte Zeitspanne sind, gelöscht und/oder überschrieben und/oder in eine weitere Datenbank ausgelagert werden.

Das erfindungsgemäße Verfahren widmet sich auch dem Problem des Löschens von Datensätzen oder von Attributen der Daten in Blockchain Datenbanken. Nach dem Stand der Technik ist es nicht möglich, Datensätze oder Attribute in der Form zu löschen, dass die in Form dieser Daten oder Attributen abgespeicherten

Informationen nicht mehr einsehbar sind.

Das erfindungsgemäße Verfahren löst das oben stehende Problem in der Weise, dass die Datenwerte der vom Benutzer zu löschen georderten Datensätze und/oder die Attributwerte der Attribute durch deren gegebenenfalls unter Verwendung eines applikationsspezifischen Geheimschlüssels erstellten Hashwert ersetzt werden, sodass die lesbare Information nicht mehr rekonstruiert werden kann. Ein solcher applikationsspezifischer Geheimschlüssel ist auch unter den Begriffen Seed oder Salt bekannt. Das im Folgenden beschriebene Verfahren kann auch als ein von dem oben beschriebenen Verfahren unabhängiges Verfahren durchgeführt werden.

Die Art der Erstellung des Hashwertes, insbesondere des Geheimschlüssels ist für Dritte nicht ersichtlich.

Erfindungsgemäß wird dies dadurch erreicht, dass bei einer von einem Benutzer angeordneten Löschfunktion eines Attributwertes der betreffende Attributwert durch den Hashwert des zu löschenden Attributes überschrieben wird.

Das erfindungsgemäße Verfahren löst das Problem des Löschens durch Überschreiben oder – bildlich ausgedrückt – durch

„Schwärzen". Die im Folgenden beschriebene Erfindung basiert darauf, dass die durch Überschreiben zu löschenden Attribute in einer Datenbank auffindbar sind und dass sämtliche Attribute überschrieben werden können.

Durch das Überschreiben des zu löschenden Eintrages mit dem betreffenden Hashwert wird der zu löschende Eintrag unlesbar gemacht. Nachdem das tatsächliche Ausführen eines Löschbefehls nicht umsetzbar ist, zielt die hier aufgezeigte Lösung darauf ab, den Eintrag durch Überschreiben mittels einer nicht reversiblen Repräsentation der ursprünglichen Daten (Hashwert) zu überschreiben. Die hier aufgezeigte Lösung sieht insbesondere vor, dass der zu löschende Eintrag mit jenem Hashwert, welcher ursprünglich aus dem zu löschenden Eintrag generiert wurde, überschrieben wird. Es ist der zu löschende Eintrag aus dem Hashwert nicht mehr erstellbar.

Das erfindungsgemäße Verfahren kann sich dadurch auszeichnen, dass

der Attributwert durch den Hashwert umfassend einen Wert zur Kennzeichnung der Überschreibung überschrieben wird. So eine Kennzeichnung wird gemeinhin als Flag bezeichnet.

Die einfache Überschreibung eines Attributwertes eines Datensatzes mit ausschließlich einem Hashwert führt dazu, dass bei Erstellung eines den Datensatz beschreibenden Hashwertes aus dem Attributwert überschreibenden Hashwert wiederum ein Hashwert erstellt wird. Dieser Vorgang ist zu einer – im Sinne der oben angeführten Aufgabenstellung – hinreichenden Schwärzung oder zur Lösung des Löschproblems nicht erforderlich.

Aus diesem Grund kann der den Attributwert überschreibende Hashwert eine Kennzeichnung umfassen.

Das Verfahren des Überschreibens eines Attributwertes kann auch unabhängig von dem oben beschriebenen Verfahren des Erstellens von neuen Datensätzen und der Referenzen sowie Modifikationsreferenzen durchgeführt werden.

Nach dem Stand der Technik kann die Existenz von Datensätzen über die Erstellung von Hashwerten bewiesen werden, ohne den Inhalt der Datensätze vorab preisgeben zu müssen. Der im Rahmen des erfindungsgemäßen Verfahrens aufgezeigte Lösungsansatz sieht vor, dass eben diese Erstellung der Hashwerte basierend auf den in Datensätzen oder Attributen abgespeicherten Informationen verwendet wird, um die in den Datensätzen oder Attributen abgespeicherten Informationen als nicht mehr lesbare Daten oder Attribute für den späteren Beweis der Manipulationsfreiheit in Evidenz zu halten.

Das erfindungsgemäße Verfahren kann auch dadurch ergänzt werden, dass gegebenenfalls ein erster Hashwert beschreibend den Datensatz zu einem Zeitpunkt t1 und ein zweiter Hashwert beschreibend den Datensatz zu einem Zeitpunkt t2 erstellt werden, wobei der erste Hashwert und wobei der zweite Hashwert in einer weiteren Datenbank abgespeichert werden, und zu einem Zeitpunkt t1‘ gegebenenfalls ein den zum Zeitpunkt t1 abgespeicherten Datensatz beschreibender weiterer erster Hashwert und zu einem Zeitpunkt t2‘ ein den zum Zeitpunkt t2 abgespeicherten Datensatz beschreibender weiterer zweiter Hashwert erstellt werden, wobei der Zeitpunkt t1‘ nach dem Zeitpunkt t1 und der Zeitpunkt t2’nach dem Zeitpunkt t2 liegt.

Dieser Verfahrensschritt eignet sich insbesondere zur Feststellung, ob die in einer ersten Datenbank abgespeicherten Datensätze nach der Erstellung des jeweiligen Hashwertes korrumpiert worden sind. Es wird hierzu ein in Form eines ersten Hashwertes dargestellter „Fingerabdruck“ des Datensatzes in der ersten Datenbank und/oder in einer zweiten Datenbank erstellt. Die zweite Datenbank kann auch eine öffentliche Datenbank sein, z. B. eine öffentliche Blockverkettung, zumal der Datensatz lediglich durch den Hashwert repräsentiert und somit nicht mehr auf die lesbare Form rückführbar ist.

Dieser erste Hashwert wird mit einem später erstellten weiteren ersten Hashwert verglichen, wobei der weitere Hashwert nach

denselben Kriterien wie der erste Hashwert erstellt wird. Durch diesen Vergleich kann festgestellt werden, ob der Datensatz zwischen der Erstellung des ersten Hashwertes und der Erstellung des weiteren Hashwertes verändert wurde.

Das Verfahren kann umfassen, dass der zweite Hashwert und der weitere zweite Hashwert verglichen werden. Das Verfahren kann ferner umfassen, dass der erste Hashwert und der weitere erste Hashwert verglichen werden.

Der Verfahrensschritt des Vergleiches der Hashwerte und der weiteren Hashwerte kann auch als ein eigenständiges Verfahren durchgeführt werden.

Es wird festgestellt, dass der hier und im Folgenden beschriebene Verfahrensschritt des Löschens eines Attributes von Daten auch unabhängig von den oben und nachstehend angeführten Verfahrensschritten durchführbar ist.

Zudem erkennt der Fachmann, dass dieses Prinzip des Überschreibens eines Eintrages eines Attributes auch für mehrere Einträge von Attributen anwendbar ist, um so Daten zu löschen.

Die erfindungsgemäßen Teilverfahren sind in den Figuren 1 bis 2 dargestellt sowie in der nachstehenden Figurenbeschreibung erläutert. Der Fachmann ist in der Lage die in den Figuren dargestellten Verfahren gemäß der untenstehenden Beschreibung als voneinander getrennte Verfahren oder als ein Verfahren unter Kombination der einzeln beschriebenen Verfahren durchzuführen. Der Fachmann ist auch in der Lage die in anhand der Figuren beschriebenen Verfahren mit den Merkmalen des allgemeinen Beschreibungsteils zu kombinieren.

Figur 1 veranschaulicht die Systematik der Erstellung der Referenzen und Modifikationsreferenzen des erfindungsgemäßen Verfahrens zur Verarbeitung von personenbezogenen Daten sowie die Vorteile dieser.

Figur 2 zeigt die Möglichkeiten des Vergleiches der Hashwerte und der weiteren Hashwerte auf.

Es sind in den Figuren die nachstehenden Elemente durch die vorangestellten Bezugszeichen gekennzeichnet.

1 bis 4 Linien
5 bis 12 Datensätze
13 bis 15, 16, 17, 19, 20 Referenzen
19, 21 Modifikationsreferenzen
22, 23, 24 zusammenfassende Datensätze
25 erster Hashwert
26 zweiter Hashwert
27 dritter Hashwert

Figur 1 veranschaulicht die dem erfindungsgemäßen Verfahren zu Grunde liegende Systematik zur Verarbeitung von personenbezogenen Daten umfassend Attribute in einem

Computerimplementierten Verfahren.
Die diesem Anwendungsbeispiel zu Grunde liegenden Datensätze umfassen Benutzerattribute, Zeitattribute als Attribute und gegebenenfalls Wertangaben.

Die Benutzerattribute werden durch eine Eingabe über ein von einer Person bedientes Eingabegerät oder Lesegerät geschaffen.

Das Benutzerattribut umfasst Angaben über eine Person.
Das Zeitattribut beschreibt den Zeitpunkt der Erstellung beziehungsweise der Veränderung der Daten beziehungsweise des jeweiligen Attributs.

Die Figur 1 umfasst mehrere durch waagerechte strichlierte Linien 1 bis 4 dargestellte Zeilen, wobei eine Linie 1 bis 4 für ein Benutzerattribut steht. Ferner wird durch die Linien 1 bis 4 das Zeitattribut in Form einer Zeitachse beginnend mit einem Zeitpunkt t0 symbolisiert. Die Linien 1 bis 4 veranschaulichen das zeitliche Eingabeverhalten der Benutzer 1 bis 4.

Die personenbezogenen Daten, welche – wie oben dargestellt – mehrere Attribute umfassen, sind in Figur 1 durch die einzelnen Datensätze dargestellt. Die einzelnen Datensätze sind in Figur 1

durch die Punkte 5 bis 12 dargestellt, wobei die personenbezogenen Daten die einzelnen, durch die Punkt 5 bis 12 dargestellten Datensätze umfassen.

Zum Zeitpunkt t0 umfassen die personenbezogenen Daten die durch die Punkte 5 bis 6 dargestellten Datensätze. Die Datensätze 5 und 6 stehen wie durch die Referenzen 13 bis 15 angedeutet in einem funktionellen und/oder logischen Zusammenhang, wobei der Zusammenhang nicht Thema der Offenbarung des erfindungsgemäßen Verfahrens ist. Derartige Referenzen sind nach dem Stand der Technik bekannt.

Wenn zu einem Zeitpunkt t1 eine Eingabe durch den Benutzer 3 vorgenommen wird, so wird ein neuer Datensatz 8 unter Aufrechterhaltung des dazugehörenden ursprünglichen Datensatzes 7 generiert.

Die nach dem Stand der Technik bekannten Referenzen zwischen dem Datensatz 7 und dem Datensatz 5 beziehungsweise dem Datensatz 6 werden in einer analogen Weise auch für den Datensatz 8 erstellt. Das erfindungsgemäße Verfahren zeichnet sich sohin dadurch aus, dass die Referenzen 16, 17 geschaffen werden, wobei die Referenzen 16, 17 einen funktionellen und/oder logischen und/oder instanziellen Zusammenhang zwischen dem Datensatz 8 und dem Datensatz 5 beziehungsweise dem Datensatz 6 angeben.

Das erfindungsgemäße Verfahren zeichnet sich ferner dadurch aus, dass zwischen dem zum Zeitpunkt t=1 durch den Benutzer 3 erstellten Datensatz 8 und dem zum Zeitpunkt t=0 ursprünglichen Datensatz 7 eine sogenannte Modifikationsreferenz 18 erstellt wird. Durch die Modifikationsreferenz 18 wird die historische Entwicklung zwischen dem ursprünglichen Datensatz 7 und dem neuen Datensatz 8 abgebildet. Es ist somit die Veränderung des neuen Datensatzes 8 im Vergleich zu dem ursprünglichen Datensatz 7 dokumentierbar.

Das erfindungsgemäße Verfahren kann vorsehen, dass nur die veränderten Attribute im neuen Datensatz 8 abgespeichert werden,

während die unveränderten Attribute im ursprünglichen Datensatz 7 abgespeichert sind. Die Generierung der Modifikationsreferenz 18, wobei die Modifikationsreferenz einen historischen Zusammenhang zwischen den Attributen des ursprünglichen Datensatzes 7 und dem neuen Datensatz 8 ausweist, ermöglicht eine effiziente Gestaltung der Datenbank.

Durch die Modifikationsreferenz 18 wird in einer für den kontrollierenden Benutzer übersichtlichen Weise die Veränderung des ursprünglichen Datensatzes 7 oder des vom ursprünglichen Datensatz 7 umfassten Attributs zu dem neuen Datensatz 8 beziehungsweise des vom neuen Datensatz 8 umfassten Attributs dargestellt.

Figur 1 zeigt die Erstellung eines weiteren neuen Datensatzes 9

zu einem Zeitpunkt t=2 durch den Benutzer 3. Es werden wiederum die funktionellen und/oder logischen Referenzen 19, 20 zwischen dem weiteren neuen Datensatz 9 und dem Datensatz 6 beziehungsweise dem Datensatz 7 geschaffen. Die Schaffung der Referenzen 19, 20 erfolgt in Analogie zu den Referenzen 13, 14

und/oder zu den Referenzen 16, 17.

Es wird eine weitere Modifikationsreferenz 21 geschaffen, wobei die weitere Modifikationsreferenz 21 ähnlich zu der Modifikationsreferenz 18 einen historischen Zusammenhang zwischen dem neuen Datensatz 9 und dem ursprünglichen Datensatz 8 ausweist.

Das erfindungsgemäße Verfahren kann vorsehen, dass Datensätze, welche Datensätze älter als der Zeitpunkt t=2 sind oder in den Zeitraum beginnend mit t=0 bis t=2 fallen, gelöscht und/oder in eine weitere Datenbank ausgelagert werden. Im Rahmen der Offenbarung des erfindungsgemäßen Verfahrens werden das Löschen eines Attributs in der Datenbank und das Auslagern, d.h. Kopieren des Attributs in eine weitere Datenbank und das Löschen des Attributs in der Datenbank, als in Bezug auf die Datenbank

äquivalente Verfahrensschritte angesehen, da in beiden Fällen das Attribut in der Datenbank gelöscht wird.

Die oben beschriebene Generierung der Referenzen zwischen den neuen Datensätzen 8, 9 und den ursprünglichen Datensätzen 5, 6, 7 erlaubt das einfache und rasche Erstellen von sogenannten zusammenfassenden Datensätzen 22, 23, 24 zu einem Zeitpunkt t=3, da insbesondere durch die Modifikationsreferenzen 28, 21 die zeitlich letzten Änderungen ausgewiesen werden. Es sind in Figur 1 die zusammenfassenden Datensätze 22, 23, 24 auf den Linien 1 bis 3 dargestellt, da diese das Ergebnis der Eingaben oder Veränderungen des jeweiligen Benutzers zusammenfassend darstellen.

Figur 1 zeigt eine weitere vorteilhafte Wirkung des erfindungsgemäßen Verfahrens.

Unabhängig, jedoch auch in Ergänzung zu der oben beschriebenen Systematik der Erstellung der Referenzen 13 - 15, 16, 17, 19, 20 und der Modifikationsreferenzen 18, 21 kann zu dem Zeitpunkt t=0 und vor einer etwaigen Änderung des Datensatzes 8 zu dem Zeitpunkt t=1 ein erster Hashwert 25 beschreibend die Datensätze 5, 6, 7 erstellt werden. Der erste Hashwert 25 kann in einer von der ersten Datenbank, wobei in der ersten Datenbank die Datensätze 5 bis 9 abgespeichert sind, physisch unabhängigen in einer zweiten Datenbank abgespeichert werden. Ferner kann zu dem Zeitpunkt t=3 ein zweiter Hashwert 26 beschreibend die Datensätze 22, 23, 24 zu dem Zeitpunkt t=3 und sohin nach der Modifikation des ursprünglichen Datensatzes 7 zu dem neuen Datensatz 8 und dem weiteren neuen Datensatz 9 erstellt werden. Der die Zugrunde liegenden Daten des zweiten Hashwertes 26 unterscheidet sich sohin um das Maß der vorgenommenen Modifikationen des ursprünglichen Datensatzes 7 vom ersten Hashwert 25.

Es kann zu einem späteren Zeitpunkt t=3 ein weiterer erster Hashwert beschreibend die Datensätze zu dem Zeitpunkt t=0 (in Figur 1 nicht dargestellt) und ein weiterer zweiter Hashwert

beschreibend die Datensätze zu dem Zeitpunkt t=3 (in Figur 1 nicht dargestellt) erstellt werden. Ein Vergleich der Hashwerte und eine Abweichung des zweiten Hashwertes 26 vom weiteren zweiten Hashwert wird als ein eindeutiger Hinweis auf eine unberechtigte Manipulation der ersten Datenbank angesehen.

Die Erstellung der Referenzen 13 – 15, 16, 17, 19, 20 und die Modifikationsreferenzen 18, 21 erlauben es, eine etwaige durch den Vergleich der Hashwerte festgestellte Manipulation nachzuverfolgen.

Figur 2 veranschaulicht nochmals in einem im Vergleich zu Figur 1 vereinfachten Diagramm das erfindungsgemäße Teilverfahren des Erkennens einer Manipulation in der ersten Datenbank.

Die Figur 2 umfasst eine Zeitachse 3, wobei auf der Zeitachse 3 die zu dem Zeitpunkt vorhandenen beziehungsweise veränderten Datensätze 7, 8, 9 aufgetragen sind. Die Datensätze 7, 8, 9 umfassen eine unterschiedliche Anzahl von Attributen.

Es wird zu dem Zeitpunkt t=0 ein erster Hashwert 25 beschreibend den Datensatz 7 zum Zeitpunkt t=0 und sohin vor einer Veränderung des Datensatzes erstellt. Der Datensatz 7 umfasst ein Attribut. Der Datensatz 7 ist in einer ersten Datenbank abgespeichert. Der erste Hashwert 25 wird vorzugsweise in einer von der ersten Datenbank physisch getrennten zweiten Datenbank zum Zeitpunkt t=0 abgespeichert.

Es wird zu dem Zeitpunkt t=1 ein Datensatz 8 erstellt. Die Erstellung des Datensatzes 8 erfolgt, nachdem durch den Benutzer 3 zu dem Attribut des Datensatzes 7 zwei weitere Attribute hinzugefügt werden. Wie oben beschrieben wird der neue Datensatz 8 erstellt, um den ursprünglichen Datensatz 7 unverändert aufrecht erhalten zu können. Es wird zum Zeitpunkt t=1 ein zweiter Hashwert 26 beschreibend den neuen Datensatz 8 zum Zeitpunkt t=1 erstellt. Es ist der neue Datensatz 8 in der ersten Datenbank abgespeichert, während der zweite Hashwert 26 in einer zweiten Datenbank abgespeichert ist.

In Analogie zu obigen wird unter der Entfernung eines Attributs ein weiterer neuer Datensatz 9 zum Zeitpunkt t=2 und sohin nach dem Entfernen eines Attributs erstellt. Es wird ein dritter Hashwert 27 beschreibend den weiteren neuen Datensatz 9 zum Zeitpunkt t=2 erstellt, wobei der dritte Hashwert 27 wiederum in der zweiten Datenbank abgespeichert wird.

Es kann zu einem beliebigen Zeitpunkt nach dem Zeitpunkt t=0 wiederum ein weiterer erster Hashwert 25 erstellt werden, wobei der weitere erste Hashwert 25 den Datensatz 7 beschreibt. Ebenso kann zu einem Zeitpunkt nach t=1 und zu einem Zeitpunkt nach t=2 ein weiterer zweiter Hashwert beziehungsweise ein weiterer dritter Hashwert erstellt werden, wobei der weitere Hashwerte die Datensätze 7, 8 zum Zeitpunkt der Erstellung der weiteren Hashwerte beschreiben.

Durch einen Vergleich der weiteren Hashwerte mit den Hashwerten 7, 8, 9 kann eine Manipulation der Datensätze nach dem Zeitpunkt des Erstellens dieser festgestellt werden.

Weitere Aspekte und Weiterbildungen

1. Computerimplementiertes Verfahren zum Verarbeiten von personenbezogenen Datensätzen umfassend Attribute in einer Datenbank,
   wobei ein ursprünglicher Datensatz und weitere ursprüngliche Datensätze durch funktionelle und/oder logische Referenzen verbunden sind,
   wobei gegebenenfalls bei der Erstellung und/oder bei einer Veränderung der Datensätze mittels einer Hashfunktion ein Hashwert erstellt wird, wobei der Hashwerte die betreffenden Attribute eines Datensatzes beschreiben,

   wobei die Attribute zumindest ein Zeitattribut, Benutzerattribute und Referenzen zwischen den einzelnen Benutzerattributen umfassen, wobei das Zeitattribut den Zeitpunkt der Erstellung beziehungsweise der Veränderung

eines Attributs oder des Datensatzes beschreibt, wobei das Benutzerattribut eine Angabe über den die Erstellung beziehungsweise die Veränderung eines Datensatzes vornehmenden Benutzer und/oder eines vom Benutzer zu bedienenden Gerätes umfasst, dadurch gekennzeichnet, dass bei einer vom Benutzer angeordneten Veränderung eines Eintrages des Datensatzes durch einen Benutzer ein ursprünglicher Datensatz unverändert aufrechterhalten wird und ein neuer Datensatz umfassend den geänderten Eintrag erstellt wird, wobei neue Referenzen von dem neuen Datensatz zu den weiteren ursprünglichen Datensätzen und eine Modifikationsreferenz von dem neuen Datensatz zu dem ursprünglichen Datensatz erstellt werden, wobei die Modifikationsreferenz zumindest eine zeitliche Entwicklung dokumentiert und gegebenenfalls eine funktionelle Referenz und gegebenenfalls eine logische Referenz und gegebenenfalls eine instanzielle Referenz zwischen dem ursprünglichen Datensatz und dem zeitlich nachfolgenden Datensatz ausgewiesen wird.

2. Verfahren nach Aspekt 1, dadurch gekennzeichnet, dass die ursprünglichen Datensätze, welche älter als eine definierte Zeitspanne sind, gelöscht und/oder überschrieben und/oder in eine weitere Datenbank ausgelagert werden.

3. Verfahren nach einem der Aspekte 1 bis 2, dadurch gekennzeichnet, dass
bei einer von einem Benutzer angeordneten Löschfunktion eines Attributwertes der betreffende Attributwert durch dessen unter Verwendung gegebenenfalls eines applikationsspezifischen Geheimschlüssels erstellten Hashwertes des zu löschenden Attributes überschrieben wird.

4. Verfahren nach Aspekt 3, dadurch gekennzeichnet, dass der Attributwert durch den Hashwert umfassend einen Wert zur Kennzeichnung der Überschreibung überschrieben wird.

5. Verfahren nach einem der Aspekte 1 bis 4, dadurch gekennzeichnet, dass gegebenenfalls ein erster Hashwert beschreibend den Datensatz zu einem Zeitpunkt t1 und ein zweiter Hashwert beschreibend den Datensatz zu einem Zeitpunkt t2 erstellt werden, wobei der erste Hashwert und wobei der zweite Hashwert in einer weiteren Datenbank abgespeichert werden, und zu einem Zeitpunkt t1‘ gegebenenfalls ein den zum Zeitpunkt t1 abgespeicherten Datensatz beschreibender weiterer erster Hashwert und zu einem Zeitpunkt t2‘ ein den zum Zeitpunkt t2 abgespeicherten Datensatz beschreibender weiterer zweiter Hashwert erstellt werden, wobei der Zeitpunkt t1‘ nach dem Zeitpunkt t1 und der Zeitpunkt t2’nach dem Zeitpunkt t2 liegt.

6. Verfahren nach Aspekt 5, dadurch gekennzeichnet, dass der zweite Hashwert und der weitere zweite Hashwert verglichen werden.

7. Verfahren nach einem der Aspekte 5 bis 6, dadurch gekennzeichnet, dass der erste Hashwert und der weitere erste Hashwert verglichen werden.

Die obigen Ausgestaltungen und Weiterbildungen lassen sich, sofern sinnvoll, beliebig miteinander kombinieren. Weitere mögliche Ausgestaltungen, Weiterbildungen und Implementierungen der Erfindung umfassen auch nicht explizit genannte Kombinationen von zuvor oder im Folgenden bezüglich der Ausführungsbeispiele beschriebenen Merkmalen der Erfindung. Insbesondere wird dabei der Fachmann auch Einzelaspekte als Verbesserungen oder Ergänzungen zu der jeweiligen Grundform der vorliegenden Erfindung hinzufügen.

Patentansprüche

1. Verfahren zum Löschen eines Datenelements aus einer Datenstruktur, umfassend die folgenden Schritte:

   a) Berechnen (L01) eines Hashwertes mindestens auf Basis des zu löschenden Datenelements innerhalb einer Instanz, und

   b) Ersetzen (L02) des Datenelements in der Datenstruktur durch den berechneten Hashwert.

2. Verfahren nach Anspruch 1, wobei das Berechnen (L01) des Hashwertes auf Basis einer Datenstruktur, welche das Datenelement und ein weiteres Element, insbesondere einen Seed/Salt, umfasst, geschieht.

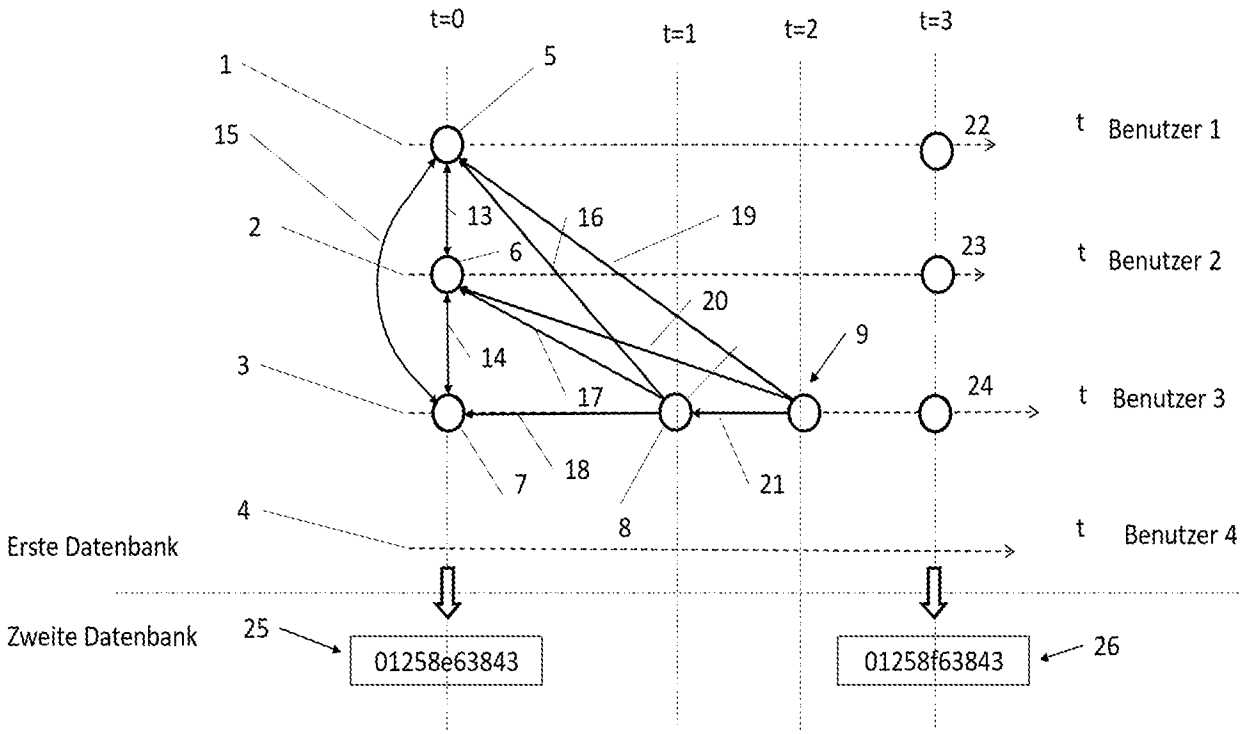
3. Verfahren nach Anspruch 1 oder 2, wobei zumindest teilweise das ursprüngliche Datenelement in der Datenstruktur durch den berechneten Hashwert überschrieben wird und/oder Bereiche des ursprünglichen Datenelements, die nicht durch den berechneten Hashwert überschrieben wurden mit anderen Daten, insbesondere randomisierten Daten, insbesondere mehrfach, überschrieben werden.

4. Computer, Computernetzwerk oder Computersystem, insbesondere verteiltes Computersystem, welches eingerichtet ist, um das Verfahren zum Löschen eines Datenelements nach einem der Ansprüche 1 – 3 auszuführen.

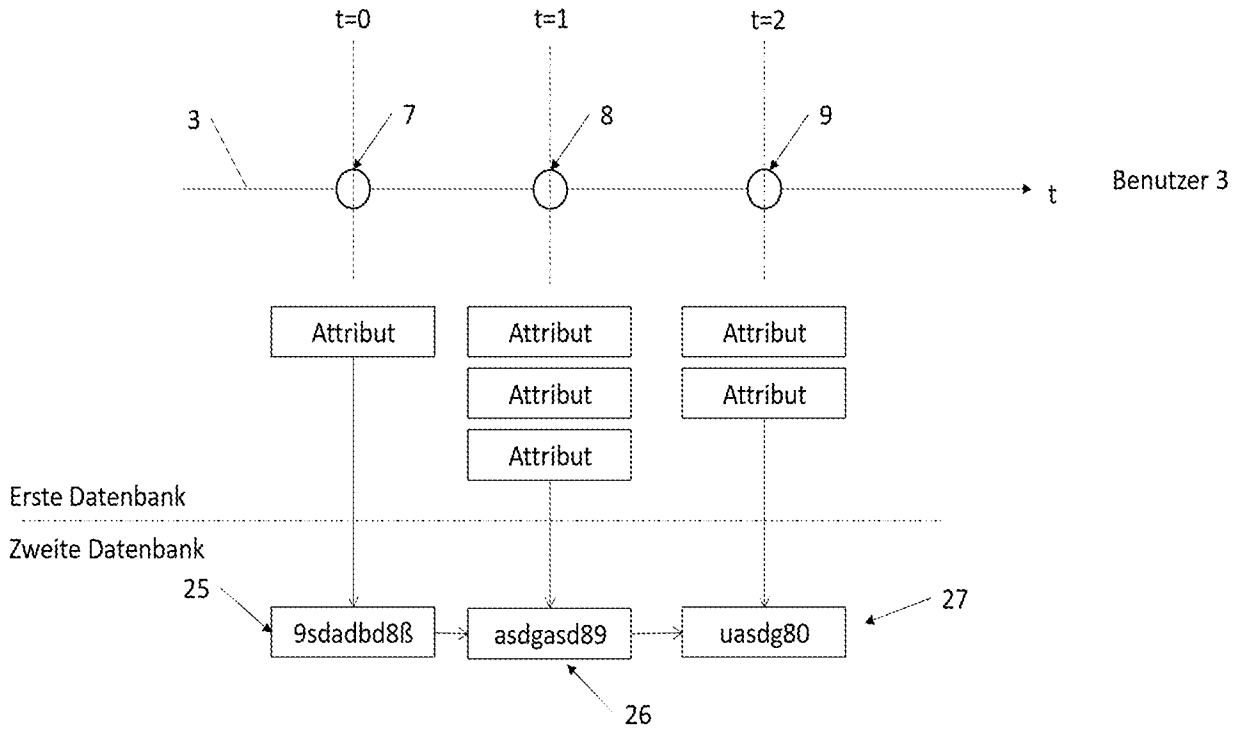
5. Computerprogramm, umfassend Befehle, die bewirken, dass der Computer, das Computernetzwerk oder das Computersystem gemäß Anspruch 4 die Verfahrensschritte nach einem der Ansprüche 1 – 3 ausführt.

6. Computerlesbares Medium, auf dem das Computerprogramm nach Anspruch 5 gespeichert ist.

Zeichnungen



Figur 1



Figur 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/DE2019/100841

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i; ***G06F 16/20***(2019.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 102017204250 A1 (BOSCH GMBH ROBERT [DE]) 20 September 2018 (2018-09-20) paragraph [0003] - paragraph [0004] paragraph [0007] - paragraph [0015]	1-6
X	DE 102010064399 A1 (SIEMENS AG [DE]) 05 July 2012 (2012-07-05) paragraph [0010] - paragraph [0012] paragraph [0015]	1-6
X	EP 3318999 A1 (BUNDESDRUCKEREI GMBH [DE]) 09 May 2018 (2018-05-09) paragraphs [0009] - [0011], [0014] paragraphs [0039], [0044], [0045], [0092], [0093], [0095]	1-6

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 January 2020	**22 January 2020**

Name and mailing address of the ISA/EP	Authorized officer
European Patent Office **p.b. 5818, Patentlaan 2, 2280 HV Rijswijk** **Netherlands** Telephone No. **(+31-70)340-2040** Facsimile No. **(+31-70)340-3016**	**Wolters, Robert** Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/DE2019/100841

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
DE 102017204250 A1	20 September 2018	NONE	
DE 102010064399 A1	05 July 2012	NONE	
EP 3318999 A1	09 May 2018	DE 102016221699 A1	09 May 2018
		EP 3318999 A1	09 May 2018

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE2019/100841

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L9/32 G06F16/20
ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L G06F

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 10 2017 204250 A1 (BOSCH GMBH ROBERT [DE]) 20. September 2018 (2018-09-20) Absatz [0003] - Absatz [0004] Absatz [0007] - Absatz [0015] -----	1-6
X	DE 10 2010 064399 A1 (SIEMENS AG [DE]) 5. Juli 2012 (2012-07-05) Absatz [0010] - Absatz [0012] Absatz [0015] -----	1-6
X	EP 3 318 999 A1 (BUNDESDRUCKEREI GMBH [DE]) 9. Mai 2018 (2018-05-09) Absätze [0009] - [0011], [0014] Absätze [0039], [0044], [0045], [0092], [0093], [0095] -----	1-6

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
9. Januar 2020	22/01/2020

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Wolters, Robert

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/DE2019/100841

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 102017204250 A1	20-09-2018	KEINE	
DE 102010064399 A1	05-07-2012	KEINE	
EP 3318999 A1	09-05-2018	DE 102016221699 A1	09-05-2018
		EP 3318999 A1	09-05-2018