(19) Deutsches Patent- und Markenamt

(10) **DE 10 2017 000 167 A1** 2018.07.12

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2017 000 167.7**
(22) Anmeldetag: **11.01.2017**
(43) Offenlegungstag: **12.07.2018**

(51) Int Cl.: ***G06F 21/60*** (2013.01)
G06Q 10/00 (2012.01)

(71) Anmelder:
Giesecke+Devrient Mobile Security GmbH, 81677 München, DE

(72) Erfinder:
Gawlas, Florian, Dr., 80805 München, DE; Spitz, Stephan, Dr., 85757 Karlsfeld, DE

(56) Ermittelter Stand der Technik:

US	**2014 / 0 365 781**	**A1**
US	**2015 / 0 127 940**	**A1**
EP	**0 908 810**	**B1**

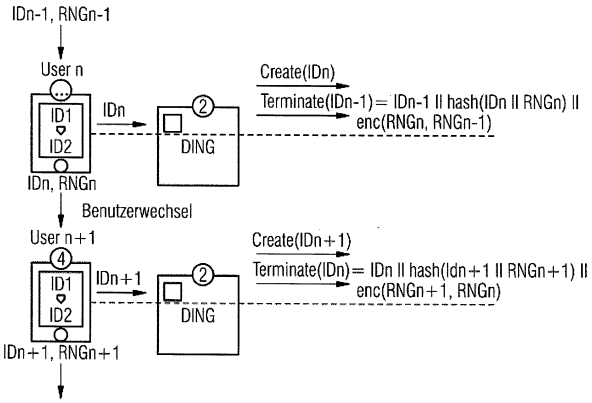
K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in IEEE Access, vol. 4, no. , pp. 2292-2303, 2016.

Rechercheantrag gemäß § 43 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Anonymisierung einer Blockkette**

(57) Zusammenfassung: Die vorliegende Erfindung ist gerichtet auf ein Verfahren zur Anonymisierung von Transaktionen einer Blockkette, welches es ermöglicht, dass beispielsweise ein Besitzer eines Gegenstands in einer Datenhistorie bzw. einer sogenannten Blockkette Information bezüglich vergangener Transaktionen bzw. Datenbeständen erhält, nicht jedoch zukünftige Besitzer. So kann beispielsweise eine Information bezüglich einer Fahrzeugwartung stets dem aktuellen Besitzer zugänglich gemacht werden, ohne dass dieser aktuelle Besitzer Information bezüglich zukünftiger Besitzer abrufen kann. Die Erfindung ist ferner gerichtet auf ein entsprechend eingerichtetes Kommunikationsprotokoll sowie auf ein Kommunikationssystem zur Anonymisierung von Transaktionen einer Blockkette. Ferner wird ein Computerprogrammprodukt vorgeschlagen, mit Steuerbefehlen, welche das vorgeschlagene Verfahren ausführen bzw. das vorgeschlagene Kommunikationssystem betreiben.



Beschreibung

[0001] Die vorliegende Erfindung ist gerichtet auf ein Verfahren zur Anonymisierung von Transaktionen einer Blockkette, welches es ermöglicht, dass ein Besitzer eines Gegenstands in einer Datenhistorie bzw. einer sogenannten Blockkette Information bezüglich vergangener Transaktionen bzw. Datenbeständen erhält, nicht jedoch zukünftige Besitzer. So kann beispielsweise eine Information bezüglich einer Fahrzeugwartung stets dem aktuellen Besitzer zugänglich gemacht werden, ohne dass dieser aktuelle Besitzer Information bezüglich zukünftiger Besitzer abrufen kann. Die Erfindung ist ferner gerichtet auf ein entsprechend eingerichtetes Kommunikationsprotokoll sowie auf ein Kommunikationssystem zur Anonymisierung von Transaktionen einer Blockkette. Ferner wird ein Computerprogrammprodukt vorgeschlagen, mit Steuerbefehlen, welche das vorgeschlagene Verfahren ausführen bzw. das vorgeschlagene Kommunikationssystem betreiben.

[0002] DE 10 2011122 767 A1 zeigt ein Verfahren zur Bezahlung mit mindestens einem elektronischen Zahlungsmittelschlüssel, wobei auf einem Serversystem mindestens ein Zahlungsmittelverifizierungsdatensatz mit einem Zahlungswert und mit einem Verifizierungsschlüssel gespeichert ist.

[0003] DE 10 2016104 478 A1 zeigt ein Verfahren zum Sichern von Datenoperationen in einem computergestützten System, das untereinander verbundene Knoten aufweist, die so konfiguriert sind, dass sie Daten senden, empfangen und speichern.

[0004] EP 0 908 810 B1 zeigt eine Vorrichtung zur Verarbeitung von Programminformationen unter Verwendung einer Blockkette.

[0005] Gemäß herkömmlicher Verfahren sind sogenannte Blockketten bekannt, welche auch als Block-Chains bezeichnet werden. Hierbei handelt es sich um verteilte Datensätze, welche Transaktionen abspeichern und diese derart redundant bereitstellen, dass Fehler stets erkannt werden können. So werden diese Daten auf unterschiedliche Netzwerkknoten derart verteilt, dass sie von mehreren Teilnehmern einsehbar sind und hierdurch Fehler dadurch erkannt werden können, dass stets ein Vergleichen eines aktuellen Datensatzes mit einer Mehrzahl von weiteren Datensätzen erfolgt und hierbei die Mehrzahl typischerweise die richtige Information widerspiegelt. Liegen also mehrere Datensätze redundant vor und ein Datensatz weicht bezüglich seiner Werte von anderen Datensätze ab, so kann festgestellt werden, dass dieser eine Datensatz falsch ist. Hierzu wird eine hohe Rechenleistung gefordert, da stets diverse Datensätze evaluiert werden müssen und zudem die entsprechenden Transaktionen abgespeichert werden müssen. Daher werden solche Verfahren typischerweise verteilt implementiert, so dass diverse Netzwerkknoten auch die Rechenleistung bereitstellen. Somit erfolgt also nicht nur die Datenhaltung verteilt, sondern vielmehr wird die Infrastruktur, welche das beschriebene Verfahren betreibt, auch über ein verteiltes Netzwerk angeboten.

[0006] Viele Anwendungsbeispiele im Zusammenhang mit Blockkettentechnologien handeln von der Eigentumsverwaltung von Gütern. Beispielsweise werden hier genannt: Autos, Gebrauchsgegenstände, Häuser, Grundstücke, Diamanten, Gemälde. Die Blockkette hat zunächst volle Transparenz und kann im Fall der öffentlichen Blockkette von jedem gelesen werden. Die eindeutige Zuordnung der Güter in der Blockkette und die Eigenschaft der Blockkette verhindert eine nachträgliche Manipulation der Daten in der Blockkette. Andererseits führt die Transparenz der Blockkette auch zu einem Mangel an Datenschutz. Ein Beispiel: Ein Auto sendet in regelmäßigen Abständen Verbrauchsdaten und Fahrleistung an die Blockkette. Diese Daten werden dort unter einer ID des Autos gespeichert und sind für Dienste oder einen potentiellen neuen Kunden auffindbar soweit er die entsprechende ID hat. Wird das Auto verkauft, will man aber nicht, dass der Vorbesitzer die ID weiter kennt und auch in der Zukunft Verbrauchsdaten des neuen Besitzers zuordnen kann. Das Auto braucht eine neue ID. Das Problem ist aber, dass der neue Besitzer sehr wohl die ganze Vergangenheit sehen soll, während der alte Besitzer nicht in der Lage sein soll, die Werte in der Zukunft zuzuordnen.

[0007] Bezüglich der Verwaltung von Transaktionen, also dem Ausführen und Übersenden von Steuerbefehlen, gibt es in technischer Hinsicht Probleme, da die zugrundeliegenden Datensätze besonders umfangreich sind. Dies ist insbesondere deshalb der Fall, da Datensätze oftmals redundant abgespeichert werden müssen und somit ein Vielfaches des eigentlichen Speicherbedarfs einnehmen können. Ferner besteht die technische Überlegung, dass Sicherheitsmechanismen, die auf einer solchen Blockkette basieren, besonders hohe Rechenleistung erfordern, welche eben auch die verteilten Speicher analysieren muss. Ausgehend von bekannten Verfahren ist es somit notwendig, eine besonders effiziente Datenverwaltung vorzusehen.

[0008] Ferner ist es gegenüber dem Stand der Technik nachteilig, dass gemäß der bekannten Blockkettentechnologie eine Vielzahl von Nutzern Daten einsehen muss. Hierbei wird nicht gewährleistet, dass auch Datensätze mindestens teilweise einer Vertraulichkeit unterliegen und dass bestimmte Benutzer ein berechtigtes Interesse daran haben, dass nicht alle weiteren Benutzer deren Daten einsehen können. Wird beispielsweise ein Fahrzeug veräußert und die Wartungshistorie mittels der Blockkettentechnologie abgespeichert, so hat ein Folgebesitzer ein berech-

tigtes Interesse daran, dass er zwar Daten der Vorgänger bzw. der Vorbesitzer einsehen kann, diese seine Daten aber nicht einsehen können, da das Eigentum an der Sache bereits übergegangen ist.

[0009] Es ist somit eine Aufgabe der vorliegenden Erfindung, ein Verfahren bereitzustellen, welches effizient und dezentral in sicherer Weise betrieben werden kann und hierbei dennoch eine hohe Vertraulichkeit der Daten gewährleistet. Es ist ferner eine Aufgabe der vorliegenden Erfindung, ein entsprechendes Kommunikationsprotokoll sowie ein entsprechend eingerichtetes Kommunikationssystem vorzuschlagen. Ferner ist es eine Aufgabe der vorliegenden Erfindung, ein Computerprogrammprodukt bereitzustellen, welches Steuerbefehle aufweist, welche das vorgeschlagene Verfahren ausführen bzw. die vorgeschlagene Kommunikationsanordnung und das Kommunikationssystem betreiben.

[0010] Die Aufgabe wird gelöst durch ein Verfahren zur Anonymisierung von Daten in einer Blockkette gemäß Patentanspruch 1. Weitere vorteilhafte Ausgestaltungen sind in den Unteransprüchen angegeben.

[0011] Dementsprechend wird ein Verfahren zur Anonymisierung von Transaktionen in einer Blockkette in einem verteilten Rechensystem vorgeschlagen. Hierbei erfolgt ein Erstellen einer ersten Identitätsinformation in einer ersten Recheneinheit und Zuweisen dieser ersten Identitätsinformation an ein Endgerät. Ferner erfolgt ein Erstellen einer zweiten Identitätsinformation in einer zweiten Recheneinheit und Zuweisen dieser zweiten Identitätsinformation an das Endgerät, wobei insbesondere der folgende Verfahrensschritt vorgesehen ist. Dieser Verfahrensschritt sieht ein Übersenden der ersten Identitätsinformation von der ersten Recheneinheit an die zweite Recheneinheit vor, sowie ein Terminieren der ersten Identitätsinformation unter Verwendung einer Hash-Funktion über die zweite Identitätsinformation und einer erzeugten Zufallszahl.

[0012] Das vorgeschlagene Verfahren erlaubt eine Identifizierung von Gütern in einer Blockkette mit der folgenden Eigenschaft: Bei einem Wechsel der ID-Nummer muss es möglich sein, das Gut in der Vergangenheit zuzuordnen, aber es dem Besitzer der vorhergehenden ID-Nummer nicht zu ermöglichen, das Gut in der Zukunft zu identifizieren. Die vorgeschlagene Lösung ist besonders robust gegen unberechtigte Korrelationsversuche von ID-Nummern.

[0013] Aus bekannten Verfahren kennt der Fachmann die sogenannte Block-Chain-Technologie, auch als Blockkettentechnologie bezeichnet. Ein Block enthält typischerweise eine Historie, beispielsweise eine Transaktionshistorie. Jeder neue Block ist verbunden mit dem vorhergehenden Block und erhält die Historie in Form einer Prüfsumme des vorhergehenden Blocks. Zusätzlich zur Prüfsumme des vorhergehenden Blocks kann ein Block auch immer die Prüfsumme der gesamten Kette enthalten. Auf diese Art und Weise sind einzelne Datensätze, also Transaktionen, untereinander verbunden. Somit wird unter einer Blockkette eine erweiterbare Liste von Datensätzen verstanden, deren Integrität, also die Sicherung gegen nachträgliche Manipulation, durch Speichern der Prüfsumme, also eines Hash-Werts, des vorangegangenen Datensatzes im jeweils nachfolgenden gesichert ist. Auf diese Art und Weise wird also zugesichert, dass ein einzelner Datensatz innerhalb dieser verketteten Liste nicht manipuliert werden kann. Dies wird durch die entsprechenden Prüfsummen bzw. Hash-Werte sichergestellt. Somit ist die verkettete Liste, also die Blockkette, derart ausgestaltet, dass von einem Datensatz Rückschlüsse auf einen vorhergehenden Datensatz gezogen werden können.

[0014] Hierbei ist es besonders vorteilhaft, dass erfindungsgemäß ein Benutzer, also jegliche Person, welche an dem erfindungsgemäßen Verfahren teilnimmt, nicht zukünftige Datensätze auslesen kann. So wird es erfindungsgemäß vermieden, dass ein Benutzer entlang der verketteten Liste in beide Richtungen navigiert. Dies bedeutet also, dass er nur Transaktionen, also Listeneinträge, einsehen kann, die ab einem gewissen Zeitpunkt nur einen älteren Zeitstempel aufweisen. Datensätze mit einem Zeitstempel oberhalb eines vorgegebenen Zeitstempels können nicht ausgelesen werden.

[0015] Dieses technische Verfahren soll im Folgenden anhand eines kurzen Beispiels verdeutlicht werden. Beispielsweise wird ein Fahrzeug erworben, dessen Wartungshistorie anhand einer Blockkette verwaltet wird. Dies ist insbesondere deshalb vorteilhaft, da die Blockkette mittels eines Netzwerks verifiziert werden kann, da diese typischerweise redundant abgespeichert wird und somit auch von mehreren Benutzern verifiziert werden kann. Mehrere Benutzer erhalten somit Zugriff auf die Daten, und gemäß einer vorbestimmten Metrik wird entschieden, welche Daten nunmehr richtig sind. Beispielsweise wird ein Datensatz fünffach abgespeichert, wobei vier Datensätze einen ersten Wert aufweisen und ein Datensatz einen zweiten Wert. Hierdurch kann also festgestellt werden, dass der zweite Wert falsch ist, da redundante Daten stets gleich abgespeichert werden, vier Teilnehmer jedoch einen anderen Wert, nämlich den ersten Wert, vorschlagen. Somit können also Manipulationen bezüglich von Wartungsintervallen oder Tachoständen vermieden werden.

[0016] Nunmehr wird von dem erworbenen Fahrzeug die Blockkette ausgelesen, die mehrere Wartungstermine widerspiegelt. Insgesamt wurden beispielsweise drei Wartungstermine wahrgenommen, was in der Blockkette als drei aneinandergereihte

Datensätze ersichtlich ist. Wird nunmehr das Fahrzeug weiterveräußert, so kann der neue Benutzer zwei weitere Wartungstermine wahrnehmen, welche jeweils als Datensätze an die Blockkette angefügt werden. Hierbei hat der zweite Fahrzeugbesitzer ein berechtigtes Interesse daran, die gesamte Blockkette, also alle Wartungstermine, einzusehen. Der erste Fahrzeugbesitzer soll jedoch nicht Einblick in den zweiten Teil der Blockkette erhalten, welche die Wartungstermine des zweiten Benutzers bzw. Eigentümers widerspiegelt. Somit wird also erfindungsgemäß sichergestellt, dass jeder der Fahrzeuginhaber stets nur alle vergangenen Wartungsintervalle einsehen kann.

[0017] Erfindungsgemäß erfolgt dies dadurch, dass einem Gegenstand, vorzugsweise einem Endgerät, eine neue Identitätsinformation zugewiesen wird, welche also einen Benutzerwechsel bzw. einen Eigentümerwechsel darstellt. Hierauf folgt ein sogenanntes Terminieren der vorhergehenden Identitätsinformation derart, dass der Benutzer, welchem die vorherige Identitätsinformation zugeordnet ist, keinerlei weiteren Zugriff auf die Blockkette erhält. Beispielsweise kann ein Terminieren ein Aussperren bzw. ein Verweigern von Zugriffsrechten eines Benutzers umfassen. So ist es generell möglich, auf alle Informationen des Endgeräts Zugriffsrechte zu vergeben, welche an eine Identität gekoppelt sind. Hierbei kennt der Fachmann weitere Techniken, wie er solche Zugriffsrechte implementieren kann. Dies kann beispielsweise mittels einer asymmetrischen Verschlüsselung erfolgen, derart, dass ein Benutzer einen öffentlichen und einen geheimen Schlüssel bereitstellen muss. Bei diesem öffentlichen Schlüssel kann es sich beispielsweise um eine Identitätsinformation handeln. Als geheimer Schlüssel kann ein Passwort wie beispielsweise eine erzeugte Zufallszahl Verwendung finden. Somit wird also Zugriff auf die Blockkette nur einem Benutzer mit einer bestimmten Identitätsinformation gewährt, der ggf. auch ein Passwort bereitstellen muss.

[0018] Als ein Terminieren wird somit ein Verwehren von Zugriffsrechten unter Verwendung der Identitätsinformation bezeichnet. Somit umfasst das Terminieren beispielsweise ein Verwehren von Zugriffsberechtigung und/oder Schreibberechtigung auf die Datensätze der Blockkette. Ferner wird erfindungsgemäß ein Übergang von einer ersten Identitätsinformation zu einer zweiten Identitätsinformation derart bewerkstelligt, dass einem unberechtigten Dritten keine Information vorliegt, wer nun tatsächlich die jeweils zweite Identitätsinformation benutzt. Somit können generell Benutzer Zugriff auf entsprechende Transaktionen bzw. Datensätze der Blockketten erhalten, diese weist dann jedoch die zweite Identitätsinformation auf, die keinem speziellen Benutzer zuzuordnen ist. Auf diese Art und Weise werden aus Sicht eines Benutzers mit der ersten Identitätsinformation, also der ersten Identität, Datensätze verwehrt, die durch die zweite Identität, aufweisend die zweite Identitätsinformation, erstellt wurden. Zwar kann es generell möglich sein, dass der erste Benutzer die Datensätze des zweiten Benutzers einsehen kann, er stellt hierbei jedoch nicht fest, dass es sich um die Datensätze des Endgeräts handelt, bezüglich dem die Identitätsinformationen erstellt wurden.

[0019] In dem oben beschriebenen Beispiel ist es also so, dass ein erster Fahrzeugeigentümer eine erste Identität mit einer ersten Identitätsinformation aufweist. Wird nunmehr das Fahrzeug veräußert, so tritt ein weiterer, neuer Fahrzeugeigentümer auf, der eine zweite Identität, also eine zweite Identitätsinformation, aufweist. Hierbei können generell die entsprechenden Informationen in einem Netzwerk in Form einer Blockkette verteilt werden. Hierbei weiß der erste Eigentümer jedoch nicht, welche Identitätsinformation der zweite Eigentümer hat. Somit wird also sichergestellt, dass der erste Besitzer nicht gezielt nach Wartungsintervallen suchen kann, die durch den zweiten Fahrzeugbesitzer in die Blockkette eingetragen wurden.

[0020] Somit wird also ein Verfahren zur Anonymisierung von Transaktionen einer Blockkette vorgeschlagen. Das Anonymisieren erfolgt also derart, dass auch, falls Datensätze der Blockkette verfügbar sind, nicht mehr eindeutig klar ist, welchem Benutzer diese Datensätze zuzuordnen sind. Dies ist insbesondere deshalb vorteilhaft, da bestehende Verfahren weiter verwendet werden können, und kein großer technischer Aufwand zur Anonymisierung der Daten geleistet werden muss.

[0021] Das Erstellen der ersten Identitätsinformation erfolgt bevorzugt in der ersten Recheneinheit, beispielsweise einem Smartphone. Diese Recheneinheit weist die erste Identitätsinformation einem Endgerät zu, beispielsweise ein Fahrzeug oder ein Internet-of-Things-Device. Somit kann also ein erster Benutzer aufweisend die erste Identitätsinformation Einträge in die Blockkette schreiben. Das entsprechende Endgerät ist somit mit der Identität dieses ersten Benutzers verknüpft.

[0022] In analoger Weise erfolgt ein Erstellen einer zweiten Identitätsinformation in einer zweiten Recheneinheit und ein Zuweisen dieser zweiten Identitätsinformation an das Endgerät. In dem geschilderten Beispiel tritt also nunmehr ein neuer Fahrzeugeigentümer auf, der seine neue Identitätsinformation dem Endgerät, bzw. im vorliegenden Beispiel dem Fahrzeug, zuweist. Somit soll also sichergestellt werden, dass die erste Identitätsinformation bezüglich dem Endgerät bzw. dem Fahrzeug nicht weiter verwendet wird und dass vielmehr nunmehr der zweite Benutzer mit der zweiten Identitätsinformation al-

le Leseoperationen und Schreiboperationen auf die Blockkette durchführen kann.

[0023] Hierbei wurde erfindungsgemäß besonders überraschend festgestellt, dass sich die Verkettung der einzelnen Datensätze insbesondere deshalb zur Anonymisierung von einzelnen Datensätzen eignet, da diese Verkettung mittels eines Hash-Werts durchgeführt werden kann, mittels dem es möglich ist, innerhalb der Blockkette zu navigieren. Anhand der entsprechenden Hash-Funktion ist es einem Benutzer also in der bekannten Datenstruktur möglich, die Datensätze, beispielsweise in Form von Knoten, abzuwandern. Dies heißt also, dass unter Bereitstellung eines öffentlichen und ggf. geheimen Schlüssels von einem ersten Datensatz Rückschlüsse auf einen zweiten Datensatz gewonnen werden können. Hierzu wird eine Hash-Funktion verwendet, wie sie der Fachmann bereits als eine Streuwertfunktion kennt. Dies entspricht der Verkettung einer herkömmlichen Blockkette unter Verwendung eines öffentlichen Schlüssels und eines geheimen Schlüssels. Im vorliegenden Beispiel ist der öffentliche Schlüssel die zweite Identitätsinformation, und die erzeugte Zufallszahl der geheime Schlüssel.

[0024] Mittels des Terminierens, also des Ausschließens der ersten Identitätsinformation von Leseoperationen und/oder Schreiboperationen, wird nunmehr sichergestellt, dass innerhalb der Blockkette lediglich die zweite Identitätsinformation Zugriffsrechte erhält. Bildlich gesprochen wird also der erste Benutzer abgeschaltet und der zweite Benutzer erhält vollen Zugriff auf die Datensätze der Blockkette. Die Hash-Funktion über die zweite Identitätsinformation und einer erzeugten Zufallszahl wird derart ausgeführt, dass beispielsweise eine bekannte Hash-Funktion wiederverwendet wird, die als Eingabeparameter die zweite Identitätsinformation und die erzeugte Zufallszahl verarbeitet.

[0025] Erfindungsgemäß ist es besonders vorteilhaft, dass das vorgeschlagene Verfahren derart iterativ durchlaufen werden kann, dass wechselweise eine erste Identitätsinformation und eine zweite Identitätsinformation bzw. eine erste Recheneinheit und eine zweite Recheneinheit berücksichtigt werden können. So ist die Begrifflichkeit der ersten Identitätsinformation und der zweiten Identitätsinformation bzw. der ersten Recheneinheit und der zweiten Recheneinheit keinesfalls einschränkend zu verstehen.

[0026] Sind beispielsweise an dem vorgeschlagenen Verfahren drei Benutzer mit drei Recheneinheiten beteiligt, so kann es sich in einer ersten Iteration um den ersten und den zweiten Benutzer handeln. In einer zweiten Iteration kann der vormals zweite Benutzer zu dem ersten Benutzer werden, und der dritte Benutzer kann zu dem zweiten Benutzer werden. Somit wird also die Rolle des ersten und des zweiten Benutzers in jeder Iteration neu vergeben. Somit kann man die erste Identitätsinformation und die erste Recheneinheit als generell eine Identitätsinformation und eine erste Recheneinheit bezeichnen, wobei die zweite Identitätsinformation und die zweite Recheneinheit jeweils eine weitere Identitätsinformation und eine weitere Recheneinheit darstellen. Auf diese Art und Weise kann sukzessive eine Vielzahl von Benutzern mit unterschiedlichen Recheneinheiten erfindungsgemäß berücksichtigt werden. Bei dem ersten und dem zweiten Benutzer handelt es sich somit lediglich um eine Rolle.

[0027] Gibt es beispielsweise bei einer Veräußerung eines Fahrzeugs drei Käufer A, B, C, so kann beispielsweise der zweite Verkäufer B zum ersten Benutzer werden, und der dritte Verkäufer C kann zum zweiten Benutzer werden. In folgenden Iterationen kann der zweite Verkäufer C zum ersten Verkäufer werden, und ein weiterer Verkäufer D kann zum zweiten Verkäufer werden. Somit werden also in jeder Iteration des vorliegenden Verfahrens erste Identitätsinformation und erste Recheneinheit sowie zweite Identitätsinformation und zweite Recheneinheit neu vergeben.

[0028] Gemäß einem weiteren Aspekt der vorliegenden Erfindung erfolgt eine Datenspeicherung mindestens teilweise dezentral. Dies hat den Vorteil, dass auf das Verfahren der Blockkette zurückgegriffen werden kann, derart, dass die Speicherung der einzelnen Datensätze bzw. Transaktionen über ein Netzwerk verteilt werden kann. Die Datenspeicherung bezieht sich hierbei auf anfallende Datenmengen, beispielsweise die Identitätsinformationen mitsamt entsprechender Zuweisungen. Auch können die einzelnen Verfahrensschritte mitprotokolliert und somit abgespeichert werden. Auch kann die entsprechende Hash-Funktion mitsamt erzeugter Zufallszahl dezentral abgespeichert werden.

[0029] Gemäß einem weiteren Aspekt der vorliegenden Erfindung erfolgt die Datenspeicherung mindestens teilweise redundant. Dies hat den Vorteil, dass die Datensätze, wie sie bereits beschrieben wurden, mehrfach vorliegen und somit diverse Teilnehmer an dem Verfahren teilnehmen bzw. eine zugrundeliegende Infrastruktur evaluieren können bzw. verifizieren können, ob die entsprechenden Datensätze korrekt sind. So kann gemäß der Blockkettentechnologie festgestellt werden, ob die Datenintegrität gewährleistet ist. Insbesondere ist es vorteilhaft, die Datenspeicherung mindestens teilweise dezentral und mindestens teilweise redundant durchzuführen. Somit wird in besonders überraschender Weise der Vorteil der Blockkettentechnologie auf die Anonymisierung von entsprechenden Datensätzen angewendet. Erfindungsgemäß ist es also möglich, Datensätze sowohl zu anonymisieren als auch zu verifizieren. Dies stellt einen erheblichen Vorteil gegenüber bekannter

Verfahren dar, die sich darauf verlassen, dass eine zentrale Instanz, beispielsweise ein Server, die Überwachung der Datensätze übernimmt.

[0030] Gemäß einem weiteren Aspekt der vorliegenden Erfindung stellt die Hash-Funktion einen Rückschluss auf die erste Identitätsinformation bereit. Dies hat den Vorteil, dass anhand der Hash-Funktion innerhalb der Blockkette derart zurücknavigiert werden kann, dass einem zweiten Benutzer aufweisend eine zweite Identitätsinformation stets Zugang zu Daten, welche von einem ersten Benutzer abgespeichert wurden, gewährt wird. Da die erste Identitätsinformation von der ersten Recheneinheit an die zweite Recheneinheit übersendet wird, liegt also der zweiten Recheneinheit stets die Identitätsinformation der ersten Recheneinheit vor. Anhand dieser Information ist es der zweiten Recheneinheit nunmehr möglich, stets auf Datensätze der ersten Recheneinheit zuzugreifen. Dies erfolgt iterativ sukzessive derart, bis das Ende bzw. der Anfang der Blockkette erreicht ist. Somit kann stets der zweite Benutzer mittels der Information bezüglich des ersten Benutzers innerhalb der Blockkette alle zurückliegenden Datensätze der Blockkette iterativ aufschlüsseln. In anderer Richtung ist dies jedoch nicht möglich, da dem ersten Benutzer aufweisend die erste Identitätsinformation nicht die Identitätsinformation des zweiten Benutzers vorliegt. Dies kann beispielsweise deshalb der Fall sein, da der erste Benutzer aufweisend die erste Identitätsinformation terminiert bzw. abgeschaltet wird.

[0031] Gemäß einem weiteren Aspekt der vorliegenden Erfindung wird die erzeugte Zufallszahl stets verschlüsselt abgespeichert. Dies bietet den Vorteil, dass die Hash-Funktion stets jeweils nur von der Recheneinheit ausgeführt werden kann, die nicht nur die entsprechende Identitätsinformation aufweist, sondern vielmehr auch der die erzeugte Zufallszahl bekannt ist. Somit kann also auch eine asymmetrische Verschlüsselung durchgeführt werden.

[0032] Gemäß einem weiteren Aspekt der vorliegenden Erfindung werden zwischen dem Herstellen der zweiten Identitätsinformation und dem Terminieren der ersten Identitätsinformation weitere Steuerbefehle ausgeführt und/oder über ein Netzwerk übertragen. Dies hat den Vorteil, dass die beiden Verfahrensschritte nicht korreliert werden, sondern dass vielmehr eine zeitliche Dekorrelierung stattfindet. So ist es erfindungsgemäß besonders vorteilhaft, dass die zweite Identitätsinformation nicht bekannt sein muss, was wiederum zur Anonymisierung beiträgt. Da stets nach einem Erstellen einer Identitätsinformation ein Terminieren der vorangegangenen Identitätsinformation erfolgt, könnten hierbei jedoch Rückschlüsse darauf gezogen werden, mit welcher zweiten Identitätsinformation die erste Identitätsinformation ausgetauscht wird. Somit müsste ein Angreifer lediglich auf das Erstellen der zweiten Identitätsinformation warten und ferner auslesen, welche erste Identitätsinformation terminiert wird. Somit würde eine Verknüpfung zwischen der ersten und der zweiten Identitätsinformation bestehen. Dies soll erfindungsgemäß gerade vermieden werden, da ein erster Benutzer keinerlei Hinweise auf den zweiten Benutzer erhalten soll. Somit können zwischen den beiden Verfahrensschritten des Erstellens und des Terminierens irgendwelche weiteren Verfahrensschritte eingestreut werden, welche verbergen, welche Identitätsinformation mit welcher weiteren Identitätsinformation ausgetauscht wurde. Somit erfolgt ein zeitliches und/oder logisches Dekorrelieren. Dies stellt ein weiteres Sicherheitsmerkmal des vorgeschlagenen Verfahrens dar.

[0033] Gemäß einem weiteren Aspekt der vorliegenden Erfindung wird die erste Identitätsinformation gelöscht. Dies hat den Vorteil, dass beispielsweise im Rahmen des Terminierens verborgen wird, welche erste Identitätsinformation vorlag. Somit wird also wiederum vermieden, dass die zweite Identitätsinformation mitsamt der ersten Identitätsinformation abgespeichert wird. Dies könnte wiederum ein Angriffspotenzial bieten, welches erfindungsgemäß vermieden wird.

[0034] Gemäß einem weiteren Aspekt der vorliegenden Erfindung wird das Verfahren unter Verwendung eines dezentralen Netzwerks ausgeführt. Dies hat den Vorteil, dass zur Abgrenzung gegenüber dem Stand der Technik auf die Blockkettentechnologie zurückgegriffen werden kann und insbesondere, dass keine zentrale Instanz, wie beispielsweise ein Server, vorgesehen ist. So können zwar generell Server am vorgeschlagenen Verfahren beteiligt werden, diese übernehmen jedoch keine gesonderte Rolle, sondern die Datenverwaltung wird dezentral auf mindestens mehreren Servern durchgeführt. So gibt es auch keine zentrale Instanz, welche die Richtigkeit der vorliegenden Daten, also die Datenintegrität, verifiziert, sondern vielmehr finden hierzu Rechenkomponenten der Blockkettentechnologie Einsatz. Somit handelt es sich um ein besonders fehlerrobustes und ausfallrobustes Verfahren.

[0035] Gemäß einem weiteren Aspekt der vorliegenden Erfindung wird die Ausführung der Verfahrensschritte in einer Historie abgespeichert. Dies hat den Vorteil, dass die Historie der Verfahrensschritte redundant und dezentral abgespeichert werden kann und somit eine Datenmanipulation vermieden wird. So kann die Historie ganz oder teilweise auf unterschiedlichen Rechnerknoten abgelegt werden. So können willkürlich einzelne Fragmente beliebiger Größe der Historie gebildet werden und diese redundant und verteilt abgespeichert werden. Aufgrund der zu erwartenden Überlappungen der Teilfragmente können die Daten dann auf ihre Integrität überprüft werden. Somit kann auch festgestellt werden, welche

Teile der Historie korrekt sind und welche manipuliert werden. Beispielsweise können diejenigen Datensätze als korrekt angesehen werden, welche den Datensätzen entsprechen, die mindestens die Hälfte der relevanten Rechenknoten vorhalten. Wird beispielsweise ein Datensatz zehnmal abgespeichert, wobei er siebenmal einen ersten Wert aufweist und dreimal einen zweiten Wert, so kann einfach verifiziert werden, dass das siebenmalige Abspeichern überlegen ist bezüglich dem dreimaligen Abspeichern. Somit ist es wahrscheinlicher, dass sich die drei Datensätze auf manipulierten Rechnerknoten befinden. Somit können die drei Datensätze ignoriert werden, und es wird verifiziert, dass die sieben Datensätze richtig sind.

[0036] Gemäß einem weiteren Aspekt der vorliegenden Erfindung wird die Ausführung der Verfahrensschritte in einer Historie derart abgespeichert, dass mehrere Verfahrensschritte zu Einheiten zusammengefasst werden. Dies hat den Vorteil, dass die einzelnen Datensätze strukturiert abgelegt werden. Beispielsweise können Transaktionen einzelner Benutzer, d. h. einzelner Identitätsinformationen, gruppiert abgespeichert werden. Hierzu sind dem Fachmann weitere Metriken bekannt, die beispielsweise ein Clustering beinhalten. Auch können die einzelnen Datensätze anhand ihres Zeitstempels oder ihrer Kommunikationspartner gruppiert werden. Somit lassen sich also einzelne Transaktionen zusammenfassen und als eine Einheit abspeichern. Dies kann auch als ein Klassifizieren der Transaktionen bezeichnet werden.

[0037] Gemäß einem weiteren Aspekt der vorliegenden Erfindung werden die Einheiten gemäß einer bereitgestellten Logik hierarchisch in Verbindung gesetzt. Dies hat den Vorteil, dass beispielsweise eine übergeordnete Transaktion in weitere einzelne Transaktionen aufgeschlüsselt werden kann. Beispielsweise kann als eine übergeordnete Dateneinheit eine Kommunikationsverbindung zwischen einem ersten Benutzer und einem zweiten Benutzer bzw. deren Endgeräte bereitgestellt werden. Hierdurch lässt sich eine Hierarchie erzeugen, da die Datenverbindung wiederum weitere Teilverbindungen aufweist. Somit können also größere Transaktionen feingranular aufgelöst werden.

[0038] Gemäß einem weiteren Aspekt der vorliegenden Erfindung werden den Einheiten unterschiedliche Zugriffsberechtigungen zugewiesen. Dies hat den Vorteil, dass auch je nach Detaillierungsgrad unterschiedliche Zugriffsrechte möglich sind. So ist es z. B. möglich, einem Benutzer Zugriff derart zu gewähren, dass festgestellt werden kann, dass ein erster Benutzer mit einem zweiten Benutzer kommuniziert hat. Hierbei kann jedoch ausgeblendet werden, um welche Transaktionen es sich im Einzelnen handelt. Dies führt wiederum zu einer Anonymisierung der zugrundeliegenden Datensätze und einem feingranularen Rechtemanagement.

[0039] Die Aufgabe wird auch gelöst durch ein Kommunikationsprotokoll zur Anonymisierung von Transaktionen einer Blockkette in einem verteilten Rechensystem, welches Steuerbefehle umfasst, die das vorgeschlagene Verfahren implementieren.

[0040] Die Aufgabe wird auch gelöst durch ein Kommunikationssystem zur Anonymisierung von Transaktionen einer Blockkette in einem verteilten Rechensystem, aufweisend eine erste Recheneinheit, eingerichtet zum Erstellen einer ersten Identitätsinformation und Zuweisen dieser ersten Identitätsinformation an ein Endgerät sowie eine zweite Recheneinheit, eingerichtet zum Erstellen einer zweiten Identitätsinformation und Zuweisen dieser zweiten Identitätsinformation an das Endgerät, wobei das Kommunikationssystem eingerichtet ist zum Übersenden der ersten Identitätsinformation von der ersten Recheneinheit an die zweite Recheneinheit und Terminieren der ersten Identitätsinformation unter Verwendung einer Hash-Funktion über die zweite Identitätsinformation und einer erzeugten Zufallszahl.

[0041] Ein verteiltes Rechensystem ist hierbei ein Rechnerverbund bzw. einzelne Rechenknoten, welche netzwerktechnisch verbunden sind.

[0042] Erfindungsgemäß ist es besonders vorteilhaft, dass das Verfahren geeignet ist, das Kommunikationsprotokoll zu beschreiben, und dass das Kommunikationsprotokoll einzelne Rechenkomponenten veranlasst, das Verfahren durchzuführen. Ferner ist das Verfahren geeignet, das Kommunikationssystem zu betreiben, und das Kommunikationssystem ist wiederum eingerichtet, das vorgeschlagene Verfahren auszuführen. Hierbei erkennt der Fachmann, dass die Verfahrensschritte als strukturelle Merkmale des Kommunikationssystems umgesetzt werden, und dass gleichfalls die strukturellen Merkmale des Kommunikationssystems auch als Verfahrensschritte implementiert werden können.

[0043] Weitere vorteilhafte Ausgestaltungen werden anhand der beigefügten Figuren näher erläutert. Es zeigen:

Fig. 1: ein Kommunikationssystem zur Anonymisierung von Transaktionen einer Blockkette gemäß einem Aspekt der vorliegenden Erfindung;

Fig. 2: ein weiteres Kommunikationssystem zur Anonymisierung gemäß einem weiteren Aspekt der vorliegenden Erfindung; und

Fig. 3: ein Ablaufdiagramm eines Verfahrens zum Anonymisieren von Transaktionen einer Blockkette gemäß einem Aspekt der vorliegenden Erfindung.

[0044] In der vorliegenden **Fig. 1** sind eine erste Recheneinheit **1** und eine zweite Recheneinheit **3** vorgesehen. Bei dem Endgerät **2** handelt es sich beispielsweise um ein Endgerät als ein sogenanntes Internet-of-Things-Device. Hierbei kann es sich jedoch um jegliches Gut handeln, beispielsweise ein Fahrzeug. Bei einem Internet-of-Things-Device handelt es sich typischerweise um ein Hardware-Endgerät, welches nur geringe Rechenkapazität aufweist. Ferner ist ein solches Endgerät passiv mit Strom versorgt, d. h. dass beispielsweise eine Elektrizität zur Versorgung verbauter Komponenten mittels einer Induktionsspule erzeugt wird.

[0045] Im Folgenden wird näher beschrieben, wie ein Benutzerwechsel, also ein Wechsel der Identitätsinformation, durchgeführt wird. Hierbei ist ersichtlich, dass ein Benutzer stets einer Recheneinheit entspricht. So hat beispielsweise der Benutzer **1** ein Smartphone bzw. eine Recheneinheit **1**. Der zweite Benutzer hat eine weitere Recheneinheit **3**. Somit erkennt der Fachmann, dass eine Identitätsinformation sowohl der Recheneinheit als auch dem Benutzer zuzuordnen ist. Somit können also die Begriffe „Benutzer“, „Recheneinheit“ und „Identitätsinformation“ austauschbar verwendet werden. Dies ist insbesondere deshalb der Fall, da der Benutzer stets mit seiner eigenen Recheneinheit, beispielsweise einem Smartphone, unter seiner eigenen Identitätsinformation kommuniziert. Die Abstraktion anhand der Identitätsinformation dient hierbei der konkreten technischen Beschreibung, wobei unter der jeweiligen Identitätsinformation ein bevorzugt menschlicher Benutzer identifizierbar ist.

[0046] Im Vorliegenden wird eine Identitätsinformation als „ID“ bezeichnet und eine erzeugte Zufallszahl als eine „RNG“. Das Erstellen wird in der vorliegenden Anwendungsdomäne als ein „Create“ bezeichnet, und ein Terminieren wird als „Terminate“ bezeichnet. Das Anwenden einer Hash-Funktion wird als „Hash“ bezeichnet.

[0047] Die erste Blockkettengeräte-ID (ID1) wird auf dem mobilen Endgerät (Smartphone) (**1**) des Nutzers generiert (bzw. in der zugehörigen App) und an das IoT-Gerät (**2**) übertragen. Bei der Kommunikation von (**2**) mit der Blockkette wird ID1 verwendet. Alternativ kann auch (**2**) die ID1 generieren und an (**1**) übertragen.

[0048] Wechselt (**2**) den Besitzer muss auch die ID gewechselt werden. Der ID-Wechsel wird von dem neuen Besitzer (User **2**) angestoßen, der im Besitz des Smartphone (**3**) mit der entsprechenden App ist.

[0049] Zunächst wird eine neue ID (ID2) auf (**3**) generiert und auf (**2**) übertragen. (**3**) erhält von (**1**) ID1. (**3**) terminiert auch ID1 durch ein entsprechendes Kommando. Die Hash-Funktion erlaubt für alle späteren Besitzer den Wechsel der IDs zu verifizieren. Anschließend kennt (**3**) ID1. Er kann jederzeit durch die Bildung eines Hashes über ID2 und RNG2 das entsprechende Terminate-Kommando von ID1 wiederfinden und damit auch ID1 im Klartext rekonstruieren. Die Zufallszahl RNG2 wird im Klartext in der Blockkette nicht verwendet. Die Zufallszahl stellt sicher, dass man nicht durch Ausprobieren aller bestehenden IDs eine Zuordnung der IDs herausbekommen kann.

[0050] Das neue Create-Kommando darf nicht durch zeitliche Korrelation dem Terminate zuzuordnen sein, damit keine Zuordnung von ID1 und ID2 möglich ist. Es sollte beispielsweise nicht direkt hintereinander gesendet werden.

[0051] Bei erneutem Besitzerwechsel wird immer nur die aktuelle (geheime) Zufallszahl RNG und die aktuelle ID weitergegeben (hier ID2, RNG2). Mit diesen Werten kann das Terminate-Kommando für ID2 gesendet werden und anschließend wird ID2 und RNG2 wieder gelöscht. Nur ID3 und RNG3 müssen gespeichert bleiben.

[0052] Benötigt der User **3** auch die vorherigen IDs (ID2, ID1), kann er diese wie folgt ermitteln: Er berechnet hash(ID3 II RNG3) und findet damit in der Blockkette das Terminate-Kommando für ID2. Mit RNG3 berechnet er RNG2 durch Entschlüsselung, da enc(RNG3, RNG2) Teil desselben Terminate-Kommandos ist und generiert anschließend hash(ID2 II RNG2), womit er das Terminate-Kommando von ID1 in der Blockkette findet. Er kennt damit ID3, ID2 und ID1.

[0053] **Fig. 2** zeigt in einer analogen Form einen Benutzerwechsel, der abstrakt für eine natürliche Zahl an Benutzern n demonstriert wird. Hierbei wird deutlich, dass es sich beispielsweise bei der zweiten Identitätsinformation um eine weitere Identitätsinformation handelt, und bei der zweiten Recheneinheit um eine weitere Recheneinheit handelt. Recheneinheiten können beispielsweise in Form eines mobilen Endgeräts, beispielsweise eines Smartphones, vorliegen.

[0054] **Fig. 3** zeigt ein Ablaufdiagramm eines Verfahrens zur Anonymisierung von Transaktionen einer Blockkette in einem verteilten Rechensystem, aufweisend ein Erstellen **100** einer ersten Identitätsinformation in einer ersten Recheneinheit und Zuweisen **101** dieser ersten Identitätsinformation an ein Endgerät sowie ein Erstellen **102** einer zweiten Identitätsinformation in einer zweiten Recheneinheit und Zuweisen **103** der zweiten Identitätsinformation an das Endgerät, wobei folgender Verfahrensschritt ausgeführt wird, nämlich des Übersendens **104** der ersten Identitätsinformation von der ersten Recheneinheit an die zweite Recheneinheit und des Terminierens **105** der ersten Identitätsinformation unter Ver-

wendung einer Hash-Funktion über die zweite Identitätsinformation und einer erzeugten Zufallszahl.

[0055] Im Folgenden werden weitere Sicherheitsmechanismen beschrieben, welche sich auf das Erzeugen einer Hierarchie von Transaktionseinheiten beziehen. Diese lassen sich mit dem vorgeschlagenen Verfahren kombinieren und sorgen dafür, dass eine feingranulare Rechteverwaltung implementiert werden kann.

[0056] Mehrere Blockketten werden miteinander verbunden. Dabei werden in der übergeordneten Blockkette die Ergebnisse mehrerer Transaktionen der untergeordneten Blockkette in einer neuen Transaktion zusammengefasst. Die Blockkette mit dem höchsten Detaillierungsgrad an Transaktionen benötigt für einen Zugriff die höchste Berechtigung. Die Blockkette, in der „nur“ die Ergebnisse aus mehreren Einzeltransaktionen zusammengefasst sind, hat ein geringeres Sicherheitsniveau und erfordert eine geringere Berechtigung. Diese Abstufung kann über beliebige Sicherheitsniveaus und Blockketten erfolgen.

[0057] Ergänzend können Lese- und Schreibberechtigungen nach einem BellLa-Padula-Sicherheitsmodell erfolgen, d.h. auch niedrigere Sicherheitsstufen können Transaktionen in die Blockkette schreiben, aber nicht lesen (no-readup). Umgekehrt können Transaktionen, die in der hohen Sicherheitsstufe durchgeführt werden, nicht 1:1 in die Blockkette der niedrigeren Sicherheitsstufe geschrieben werden (no-write-down). Einzig die Aggregation von Transaktionen der höheren Stufen in eine neue Transaktion ist erlaubt.

[0058] Informationen in einer Blockkette können abhängig von einer Berechtigung zur Verfügung gestellt werden. Die Entität mit der höchsten Berechtigung hat Zugriff auf den höchsten Detaillierungsgrad an Transaktionen. Ein Beispiel können Finanztransaktionen sein, d.h. mit einer mittleren Berechtigung kann eine monatliche Bilanz eingesehen werden, aber um einzelnen Finanztransaktionen zu sichten, wird eine höherer Berechtigungsgrad benötigt.

[0059] Somit wurde ein fehlerrobustes Verfahren bzw. ein Kommunikationssystem vorgeschlagen, welches es erlaubt, die Datenintegrität sicherzustellen und dennoch ohne technischen Aufwand bestehende Infrastrukturen zu erweitern.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- DE 102011122767 A1 [0002]
- DE 102016104478 A1 [0003]
- EP 0908810 B1 [0004]

Patentansprüche

1. Verfahren zur Anonymisierung von Transaktionen einer Blockkette in einem verteilten Rechensystem, aufweisend:
- Erstellen (100) einer ersten Identitätsinformation in einer ersten Recheneinheit (1) und Zuweisen (101) dieser ersten Identitätsinformation an ein Endgerät (2);
- Erstellen (102) einer zweiten Identitätsinformation in einer zweiten Recheneinheit (3) und Zuweisen (103) dieser zweiten Identitätsinformation an das Endgerät (2), **dadurch gekennzeichnet**, dass folgender Verfahrensschritt vorgesehen ist:
- Übersenden (104) der ersten Identitätsinformation von der ersten Recheneinheit (1) an die zweite Recheneinheit (3) und Terminieren (105) der ersten Identitätsinformation unter Verwendung einer Hash-Funktion über die zweite Identitätsinformation und einer erzeugten Zufallszahl.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, dass eine Datenspeicherung mindestens teilweise dezentral erfolgt.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, dass die Datenspeicherung mindestens teilweise redundant erfolgt.

4. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass die Hash-Funktion einen Rückschluss auf die erste Identitätsinformation bereitstellt.

5. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass die erzeugte Zufallszahl stets verschlüsselt abgespeichert wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass zwischen dem Erstellen (102) der zweiten Identitätsinformation und dem Terminieren (105) der ersten Identitätsinformation weitere Steuerbefehle ausgeführt und/ oder über ein Netzwerk übertragen werden.

7. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass die erste Identitätsinformation gelöscht wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass das Verfahren unter Verwendung eines dezentralen Netzwerks ausgeführt wird.

9. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass die Ausführung der Verfahrensschritte in einer Historie abgespeichert wird.

10. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass die Ausführung der Verfahrensschritte in einer Historie derart abgespeichert wird, dass mehrere Verfahrensschritte zu Einheiten zusammengefasst werden.

11. Verfahren nach Anspruch 10, **dadurch gekennzeichnet**, dass die Einheiten gemäß einer bereitgestellten Logik hierarchisch in Verbindung gesetzt werden.

12. Verfahren nach einem der Ansprüche 10 oder 11, **dadurch gekennzeichnet**, dass den Einheiten unterschiedliche Zugriffsberechtigungen zugewiesen werden.

13. Kommunikationsprotokoll zur Anonymisierung von Transaktionen einer Blockkette in einem verteilten Rechensystem, welches folgende Steuerbefehle veranlasst:
- Erstellen (100) einer ersten Identitätsinformation in einer ersten Recheneinheit und Zuweisen (101) dieser ersten Identitätsinformation an ein Endgerät;
- Erstellen (102) einer zweiten Identitätsinformation in einer zweiten Recheneinheit und Zuweisen (103) dieser zweiten Identitätsinformation an das Endgerät, **dadurch gekennzeichnet**, dass folgender Verfahrensschritt vorgesehen ist:
- Übersenden (104) der ersten Identitätsinformation von der ersten Recheneinheit an die zweite Recheneinheit und Terminieren (105) der ersten Identitätsinformation unter Verwendung einer Hash-Funktion über die zweite Identitätsinformation und einer erzeugten Zufallszahl.

14. Kommunikationssystem zur Anonymisierung von Transaktionen einer Blockkette in einem verteilten Rechensystem, aufweisend:
- eine erste Recheneinheit (1) eingerichtet zum Erstellen (100) einer ersten Identitätsinformation und Zuweisen (101) dieser ersten Identitätsinformation an ein Endgerät (2);
- eine zweite Recheneinheit (3) eingerichtet zum Erstellen (102) einer zweiten Identitätsinformation und Zuweisen (103) dieser zweiten Identitätsinformation an das Endgerät (2), **dadurch gekennzeichnet**, dass das Kommunikationssystem eingerichtet ist, zum:
- Übersenden (104) der ersten Identitätsinformation von der ersten Recheneinheit (1) an die zweite Recheneinheit (3) und Terminieren (105) der ersten Identitätsinformation unter Verwendung einer Hash-Funktion über die zweite Identitätsinformation und einer erzeugten Zufallszahl.

15. Computerprogrammprodukt mit Steuerbefehlen, welche das Verfahren gemäß einem der Ansprüche 1 bis 12 implementieren.

Es folgen 3 Seiten Zeichnungen

Anhängende Zeichnungen

FIG 1

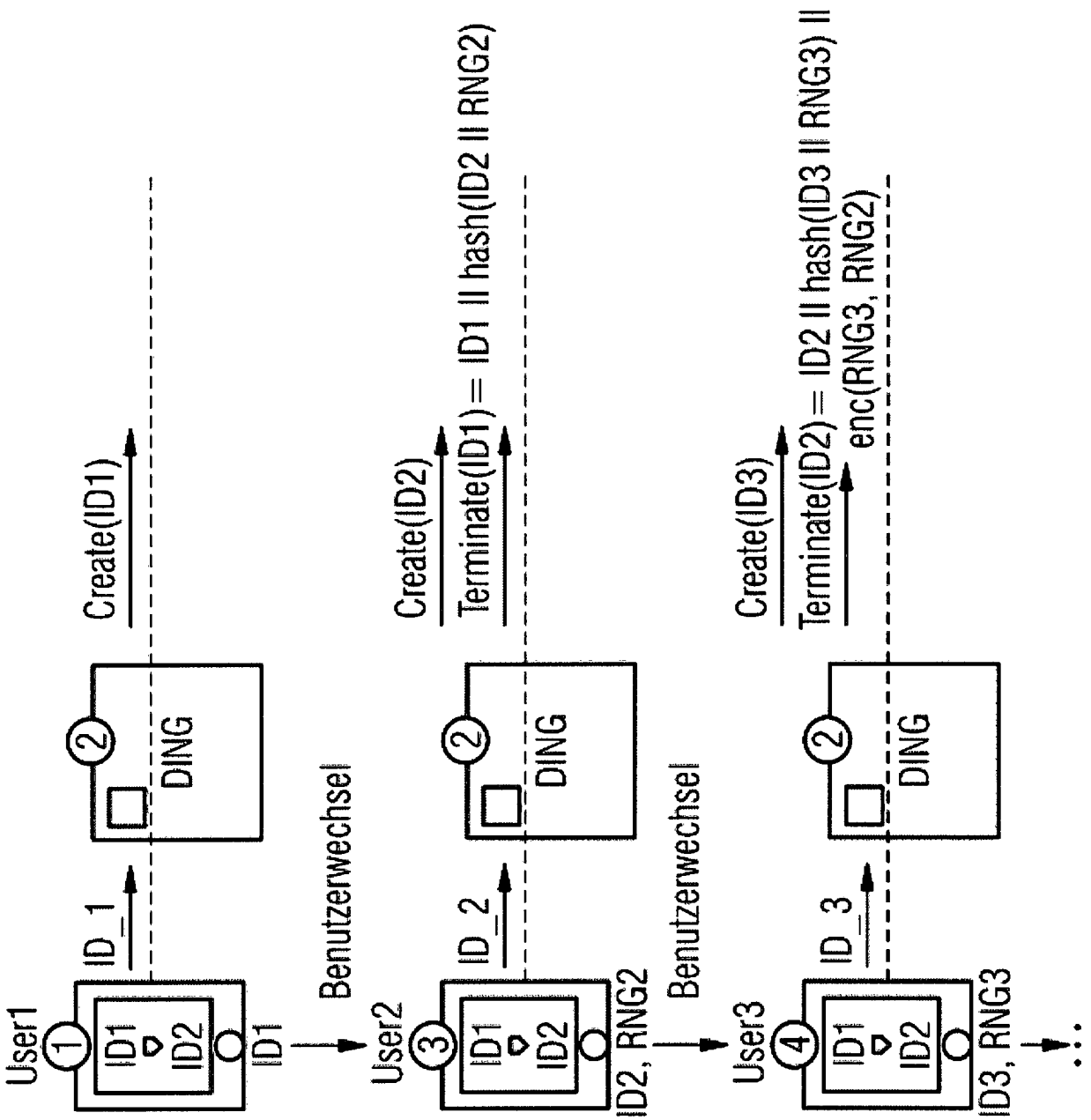
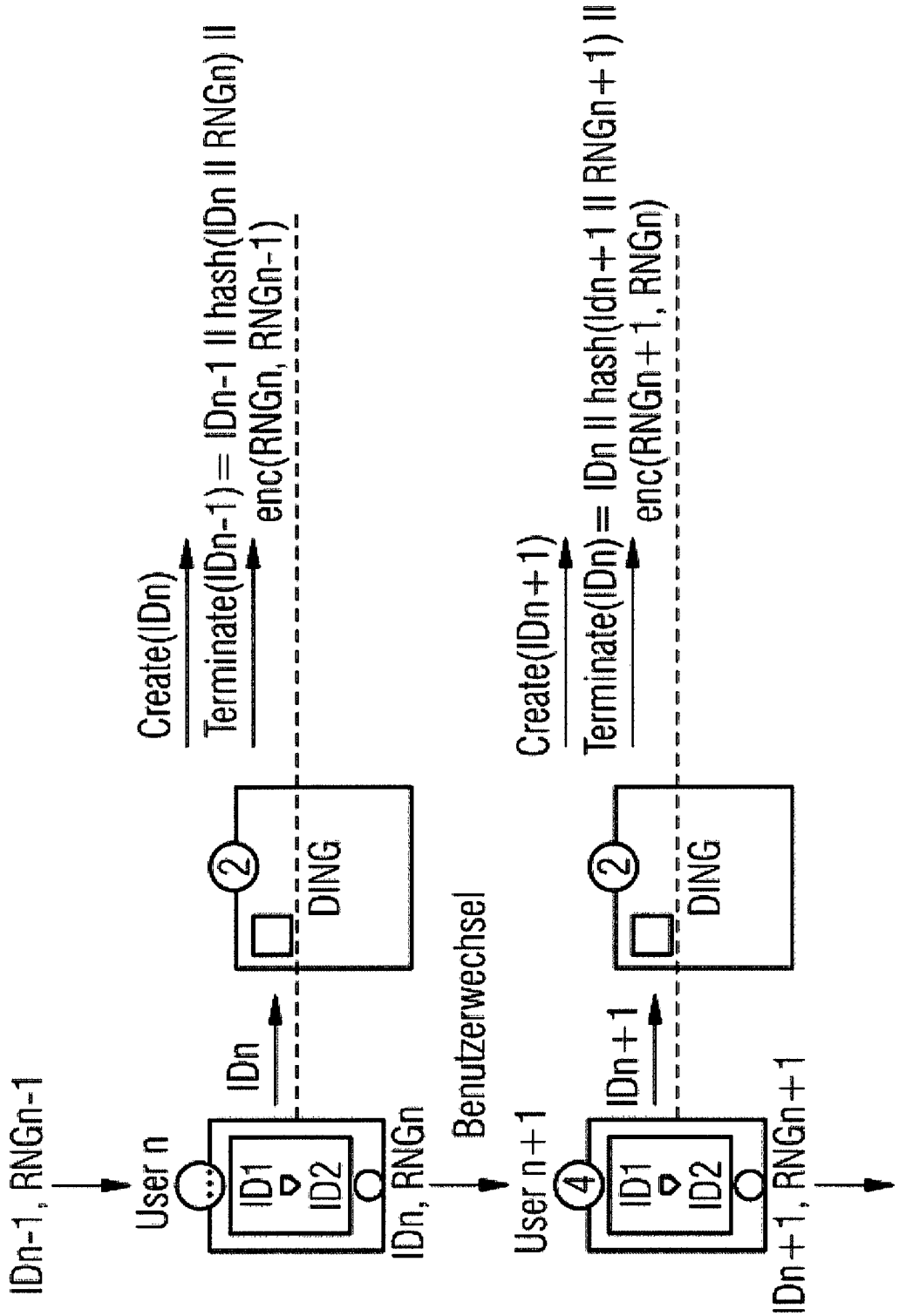


FIG 2


IDn-1, RNGn-1
User n
ID1
ID2
IDn
IDn, RNGn
2
DING
Create(IDn)
Terminate(IDn-1) = IDn-1 II hash(IDn II RNGn) II enc(RNGn, RNGn-1)
Benutzerwechsel
User n+1
4
ID1
ID2
IDn+1
IDn+1, RNGn+1
2
DING
Create(IDn+1)
Terminate(IDn)= IDn II hash(Idn+1 II RNGn+1) II enc(RNGn+1, RNGn)

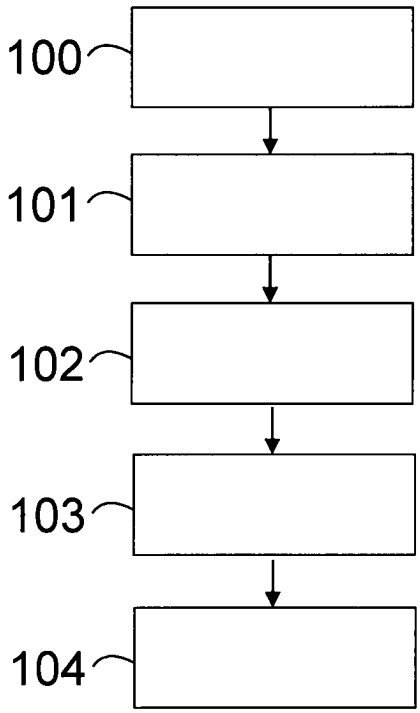


FIG 3