

(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. Januar 2020 (02.01.2020)



(10) Internationale Veröffentlichungsnummer
WO 2020/002341 A1

(51) Internationale Patentklassifikation:
G06F 21/64 (2013.01)

(21) Internationales Aktenzeichen: PCT/EP2019/066852

(22) Internationales Anmeldedatum:
25. Juni 2019 (25.06.2019)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2018 115 350.3
26. Juni 2018 (26.06.2018) DE

(71) Anmelder: **BUNDESDRUCKEREI GMBH** [DE/DE];
Kommandantenstraße 18, 10969 Berlin (DE).

(72) Erfinder: **RÜCKRIEMEN, Jörg**; Paul Lincke Ufer 32,
10999 Berlin (DE).

(74) Anwalt: **RICHARDT PATENTANWÄLTE PARTG
MBB**; Wilhelmstraße 7, 65185 Wiesbaden (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.

(54) Title: TAMPER-PROOF ISSUING AND STORING OF ELECTRONIC CERTIFICATES

(54) Bezeichnung: MANIPULATIONSSICHERES AUSSTELLEN UND SPEICHERN VON ELEKTRONISCHEN URKUNDEN

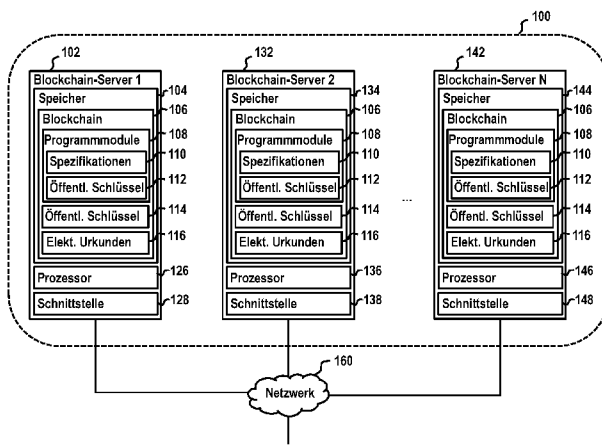


Fig. 1A

102, 132, 142 Blockchain server 1
104, 134, 144 Memory
106 Blockchain
108 Program modules
110 Specifications
112 Public key
114 Public key
116 Elec. certificates
126, 136, 146 Processor
128, 138, 148 Interface
160 Network

(57) Abstract: The invention relates to a method for tamper-proof
issuing and storing of a plurality of electronic certificates (116)
using a blockchain (106). The method comprises: receiving a
data record (210) for entry by a blockchain server (102) of a
blockchain network (100), wherein the data record (210) com-
prises data of an electronic certificate (116) to be issued accord-
ing to a specification (110) of a sovereign institution; executing pro-
gram instructions of a program module (108) of the blockchain
(106), wherein the program module (108) is configured to issue an
electronic certificate (116) according to the specification (110),
wherein the executing of the program instructions comprises an
examining of the data record (210) in respect of whether the data
record (210) fulfills the specification (110); and, if the data record
(210) fulfills the specification (110), adding the data record (210)
to an additional block of the blockchain (106).

(57) Zusammenfassung: Die Erfindung betrifft ein Verfah-
ren zum manipulationssicheren Ausstellen und Speichern einer
Mehrzahl von elektronischen Urkunden (116) unter Verwendung
einer Blockchain (106). Das Verfahren umfasst: Empfangen ei-
nes Datensatzes (210) zum Eintragen durch einen Blockchain-
Server (102) eines Blockchain-Netzwerks (100), wobei der Da-
tensatz (210) Daten einer auszustellenden elektronischen Urkun-
de (116) entsprechend ei- ner Spezifikation (110) einer hoheitli-
chen Institution umfasst, Ausführen von Programminstruktionen
eines Programmmoduls (108) der Blockchain (106), wobei das
Programmmodul (108) zum Ausstellen von elektronischen Ur-
kunde (116) entsprechend der Spezifikation (110) konfigu-
riert ist, wobei das Ausführen der



(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, 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)

Manipulationssicheres Ausstellen und Speichern von elektronischen Urkunden

B e s c h r e i b u n g

Die Erfindung betrifft ein Verfahren zum manipulationssicheren Ausstellen und Speichern einer Mehrzahl von elektronischen Urkunden unter Verwendung einer Blockchain, sowie einen Blockchain-Server und ein Blockchain-Netzwerk zum Aus-

5 führen des Verfahrens.

Urkunden dienen dazu, als schriftlich niedergelegte und häufig beglaubigte Erklärungen einen bestimmten Sachverhalt zu fixieren. Insbesondere öffentliche Urkunden werden von einer öffentlichen Behörde innerhalb der Grenzen ihrer Amtsbefug-

10 nisse oder von einer mit öffentlichem Glauben versehenen Person innerhalb eines

ihr zugewiesenen Geschäftskreises in einer vorgeschriebenen Form ausgestellt. Dabei trägt eine öffentliche Urkunde den Beweis ihrer Echtheit in sich. Mit anderen Worten beweist eine öffentliche Urkunde die Richtigkeit der Beurkundung, wobei ihre formelle Beweiskraft umfasst, dass die in Form der Urkunde manifestierte Erklärung nach Zeit, Ort und Inhalt wie beurkundet abgegeben wurde.

Einen solchen Beweis ihrer Echtheit in einer konkreten Urkunde tatsächlich zuverlässig zu implementieren, kann sich in der Praxis als schwierig erweisen. So erschöpft sich der Echtheitsbeweis bei Urkunden, wie beispielsweise Geburtsurkunden, im Allgemeinen in einem Siegel der ausstellenden Behörde, z.B. des ausstellenden Standesamtes, einer Unterschrift des beurkundenden Beamten, z.B. des beurkundenden Standesbeamten, einer Namensangabe des beurkundenden Beamten, z.B. des beurkundenden Standesbeamten, sowie Angaben zu Ort und Datum der Ausstellung. Diese Sicherheitsmerkmale lassen sich jedoch einfach nachahmen und/oder sind in der Praxis nur schwer zu überprüfen. Nichtsdestotrotz stellen Urkunden, wie beispielsweise die Geburtsurkunde, die Grundlage für die Identität einer Person dar. Mit anderen Worten werden auf dieser Grundlage weitere Ausweisdokumente ausgestellt. Ferner sind Geburtsurkunden im Zuge verschiedenen öffentlichen und privaten Bewerbungen und Anmeldungen als Identitätsnachweis vorzulegen.

Der Erfindung liegt daher die Aufgabe zugrunde, ein effizientes und sicheres Verfahren zum manipulationssicheren Ausstellen und Speichern von elektronischen Urkunden zu schaffen.

Die der Erfindung zugrunde liegende Aufgabe wird jeweils mit den Merkmalen der unabhängigen Patentansprüche gelöst. Ausführungsformen der Erfindung sind in den abhängigen Patentansprüchen angegeben.

Ausführungsformen umfassen ein computerimplementiertes Verfahren zum manipulationssicheren Ausstellen und Speichern einer Mehrzahl von elektronischen Urkunden unter Verwendung einer Blockchain.

Die elektronischen Urkunden entsprechen jeweils einer Spezifikation einer vorgegebenen Mehrzahl von Spezifikationen, wobei die Spezifikationen der Mehrzahl von Spezifikationen unterschiedlichen hoheitlichen Institutionen einer Mehrzahl von hoheitlichen Institutionen zugeordnet sind. Die Blockchain umfasst eine Mehrzahl von
5 Programmmodulen, wobei die Programmmodule jeweils einer der Spezifikationen zugeordnet sind. Die Blockchain wird von einem Blockchain-Netzwerk bereitgestellt, welches eine Mehrzahl von Blockchain-Servern umfasst. Die Blockchain-Server sind jeweils dazu konfiguriert, zusätzliche Blöcke für die Blockchain zu erstellen und in die Blockchain einzutragen, wobei die Blockchain-Server unterschiedlichen ho-
10 heitlichen Institutionen zugeordnet sind.

Das Verfahren umfasst:

- Empfangen eines ersten Datensatzes zum Eintragen in die Blockchain durch einen ersten Blockchain-Server des Blockchain-Netzwerks, wobei der erste
15 Datensatz Daten einer auszustellenden ersten elektronischen Urkunde entsprechend einer ersten Spezifikation einer ersten hoheitlichen Institution umfasst, wobei der erste Blockchain-Server der ersten hoheitlichen Institution zugeordnet ist,
- Ausführen erster Programminstruktionen eines ersten Programmmoduls der
20 Mehrzahl von Programmmodulen durch den ersten Blockchain-Server, wobei das erste Programmmodul zum Ausstellen von elektronischen Urkunde entsprechend der ersten Spezifikation konfiguriert ist, wobei das Ausführen der ersten Programminstruktionen ein Prüfen des ersten Datensatzes durch den ersten Blockchain-Server umfasst, ob der erste Datensatz die erste Spezifi-
25 kation erfüllt, falls der erste Datensatz die erste Spezifikation erfüllt, ein Hinzufügen des ersten Datensatzes zu einem ersten zusätzlichen Block der Blockchain.

Ausführungsformen können den Vorteil haben, dass elektronische Urkunden unter-
30 schiedlicher hoheitlicher Institutionen und insbesondere hoheitlicher Institutionen unterschiedlicher Staaten, welche gegebenenfalls unterschiedliche Spezifikationen aufweisen, unter Verwendung der gemeinsamen Blockchain in transparenter und

nachvollziehbarer Weise manipulationssicher gespeichert werden können. Die einzelnen elektronischen Urkunden bleiben dabei in der Verfügungsgewalt der ausstellenden hoheitlichen Institutionen, z. B. in nationaler Hoheit, und können zugleich nationale Spezifika aufweisen. Beispielsweise ist für jede dieser nationalen Spezifikationen jeweils ein eigenständiges Programmmodul vorgesehen. Mit anderen Worten wird es also jedem teilnehmenden Staat bzw. den hoheitlichen Institutionen des entsprechenden Staats ermöglicht die Verfügungsgewalt bzw. Ownership über die eigenen Datensätze bzw. Urkunden zu behalten. Ferner kann jeder Staat die eigenen hoheitlichen Institutionen, wie etwa Ämter, autorisieren auf die eigenen Datensätze bzw. Urkunden zuzugreifen und/oder diese zu verändern. Dabei sind die Autorisierungen, beispielsweise durch Eintragen bzw. Registrieren in der Blockchain, sowie die von den autorisierten Institutionen vorgenommenen Aktionen nachvollziehbar. Zudem kann jeder Staat eigene nationale nationalen Spezifikationen in eigene Programmmodule bzw. Smart Contracts einbringen. Ferner kann jeder der Staaten bzw. jede der hoheitlichen Institutionen, welche beispielsweise jeweils einen der Staaten repräsentieren, über zumindest einen der Blockchain-Server verfügen. Nach Ausführungsformen sind die Programmmodule dazu konfiguriert, nur elektronische Urkunden einzutragen, welche von der hoheitlichen Institution, welcher die von dem entsprechenden Programmmodul implementierte Spezifikation zugeordnet ist, oder von einer durch die entsprechende hoheitliche Institution autorisierten Institution stammen. Dies kann beispielsweise durch eine Signaturanforderung als Teil der Spezifikation implementiert werden. Beispielsweise müssen Datensätze, um die entsprechende Spezifikation zu erfüllen, mit einer Signatur versehen sein, deren Authentizität mit einem der entsprechenden hoheitlichen Institution zugeordneten oder einem einer durch die entsprechende hoheitliche Institution autorisierten Institution zugeordneten öffentlichen kryptografischen Schlüssel bestätigt wird. Nach Ausführungsformen haben die Blockchain-Server jeweils nur einen Schreibzugriff auf die Blockchain unter Verwendung des Programmmoduls, welches die dem entsprechenden Blockchain-Server bzw. der hoheitlichen Institution des entsprechenden Blockchain-Servers zugeordnete Spezifikation implementiert. Durch die Signaturanforderung, eigenständigen Programmmodule für nationale Spezifikationen und/oder Blockchain-Server in der Verfügung von individuellen Staaten oder hoheit-

- lichen Institutionen individueller Staaten wird es im Falle eines Verbands von Staaten, welche die Blockchain betreiben bzw. Teil des Blockchain-Netzwerks sind, den individuellen Staaten des Verbands ferner ermöglicht die eigenen Datensätze zu behalten, jederzeit aus dem Verband auszusteigen und allein weiterzumachen, d.h.
- 5 unabhängig von den anderen Staaten eigene Datensätze in die Blockchain einzutragen und zu verwalten. Nach Ausführungsformen sind die Datensätze eines Staats, welcher ausgestiegen ist, nach wie vor Teil der gemeinsamen Blockchain, aber die anderen Staaten haben beispielsweise keinen Lesezugriff mehr auf die entsprechenden Datensätze. Beispielsweise werden die Datensätze verschlüsselt.
- 10 Die zur Entschlüsselung notwendigen kryptographischen Schlüssel, z.B. symmetrische oder asymmetrische Schlüssel, insbesondere private Schlüssel, befinden sich beispielsweise in der Verfügungsgewalt der hoheitlichen Institutionen, welchen die entsprechenden Datensätze zugeordnet sind. Nach Ausführungsformen befinden sich die entsprechenden kryptographischen Schlüssel in der Verfügungsgewalt einer Mehrzahl von hoheitlichen Institutionen desselben Staats. Ein Lesezugriff durch
- 15 eine Person oder Entität, welche nicht über den zur Entschlüsselung notwendigen kryptographischen Schlüssel verfügt, bedarf daher einer Entschlüsselung durch eine hoheitliche Institution, welche über einen solchen Schlüssel verfügt. Eine Entschlüsselung erfolgt beispielsweise auf Anfrage. Beispielsweise wird eine Signatur der
- 20 Anfrage geprüft, um zu bestimmen, ob die anfragende Person oder Entität zugriffsberechtigt ist. Durch eine Verweigerung der Entschlüsselung durch die hoheitlichen Institutionen können somit Lesezugriffsrechte effektiv entzogen werden. Nach Ausführungsformen können die zur Entschlüsselung notwendigen kryptographischen Schlüssel zentral gespeichert werden und eine Entschlüsselung erfolgt auf eine erfolgreiche Prüfung der Zugriffsberechtigung einer anfragenden Person oder Entität,
- 25 etwa anhand einer Signatur der Anfrage, hin. Eine solche Prüfung kann auf Basis einer, beispielsweise von der Blockchain umfassten, Registrierung von Zugriffsrechten, welche revozierbar sind, erfolgen.
- 30 Nach Ausführungsformen umfasst der erste Datensatz einen Identifikator eines in der Blockchain eingetragenen Datensatzes, wobei der eingetragene Datensatz Daten einer ausgestellten elektronischen Urkunde entsprechend der ersten Spezifika-

tion der ersten hoheitlichen Institution oder einer weiteren Spezifikation einer weiteren hoheitlichen Institution umfasst. Ausführungsformen können den Vorteil haben, dass Links auf andere Urkunden bzw. Datensätze in Form von Identifikatoren der entsprechenden Urkunden bzw. Datensätze implementiert werden können. Beispielsweise legt die erste Spezifikation fest, welche Art von Identifikator der erste Datensatz umfassen darf, z.B. welche Spezifikationen der Datensatz erfüllen muss, auf welche der Identifikator verweist bzw. welchen der Identifikator identifiziert. Bei dem Identifikator des eingetragenen Datensatzes kann es sich um einen Identifikator des individuellen Datensatzes und/oder um einen Identifikator der ausgestellten elektronischen Urkunde handeln, auf den bzw. die mittels des Identifikators verlinkt wird.

Nach Ausführungsformen ist auf jedem der Blockchain-Server jeweils eine vollständige Kopie der Blockchain gespeichert. Mithin hat beispielsweise jeder Blockchain-Server einen Lesezugriff auf sämtliche Einträge der Blockchain. Beispielsweise sind die Datensätze verschlüsselt und für einen Lesezugriff ist eine Entschlüsselung des entsprechenden Datensatzes notwendig. In diesem Fall haben die Blockchain-Server jeweils nur einen Lesezugriff auf solche Einträge der Blockchain, für die sie auch ein Zugriffsrecht auf den zur Entschlüsselung jeweils notwendigen kryptographischen Schlüssel besitzen. Nach Ausführungsformen bildet das Blockchain-Netzwerk ein Peer-to-Peer-Netzwerk. Somit können Urkunden unterschiedlicher hoheitlicher Institutionen, insbesondere unterschiedlicher Staaten, in effizienter Weise eingesehen werden. Beispielsweise ermöglichen es Ausführungsformen, ein dezentrales multinationales, z. B. europäisches, Geburtsurkundenregister auf Basis vordefinierter Programmmodule, sog. Smart Contracts, einzurichten. Ausführungsformen können den Vorteil, dass sich auch elektronische Urkunden anderer hoheitlicher Institution der Mehrzahl von hoheitlichen Institutionen unter Verwendung der Blockchain effektiv und effizient auf ihre Gültigkeit hin prüfen lassen.

Zusätzlich können die Urkunden, z. B. Geburtsurkunden, mit identischem Inhalt und/oder auf diesen Urkunden basierende Dokumente in körperlicher Form, z. B. auf Papier oder Kunststoff, ausgestellt werden. Diese körperlichen Urkunden und

Dokumente können mit einem maschinenlesbaren Code versehen werden, z. B. einem mit optoelektronischen Erfassungsmitteln auslesbarer Code, wie etwa einem QR-Code, oder einem Code, welcher in einem Speicher, wie etwa einem elektronischen Speicher, bereitgestellt wird und unter Verwendung einer Funkverbindung auslesbar ist. Beispielsweise wird der maschinenlesbare Code unter Verwendung eines RFID-Tags bereitgestellt. Der maschinenlesbare Code kann einen Identifikator der entsprechenden manipulationssicher in der Blockchain gespeicherten Urkunde bereitstellen. Unter Verwendung des entsprechenden Identifikators können die der entsprechenden Urkunde zugeordneten Einträge in der Blockchain identifiziert und ausgelesen werden. Hierbei kann es sich beispielsweise sowohl um Einträge handeln, welche Teil der elektronischen Urkunde sind, als auch Einträge, welche auf der Urkunde basieren, etwa Verweise auf Dokumente, welche basierend auf der Urkunde ausgestellt wurden. Somit kann anhand der elektronischen Blockchain die Echtheit einer körperlichen Urkunde nachgewiesen werden, indem der Inhalt der entsprechenden körperlichen Urkunde auf Übereinstimmung mit einer in der Blockchain manipulationssicher hinterlegten elektronischen Urkunde geprüft wird. Liegt eine Übereinstimmung vor, so ist die Echtheit der vorgelegten körperlichen Urkunde nachgewiesen. Im Falle einer Prüfung eines vorgelegten Dokuments, welches auf der in der Blockchain eingetragenen Urkunde basiert, kann neben einem zumindest teilweisen inhaltlichen Abgleich zusätzlich geprüft werden, ob ein Ausstellungsmerk für das vorliegende Dokument auf Basis der elektronischen Urkunde in der Blockchain eingetragen ist. Ein entsprechender inhaltlicher Abgleich kann beispielsweise vollautomatisch durch Einscannen des auf der körperlichen Urkunde oder dem körperlichen Dokument aufgebrachten, z. B. aufgedruckten, Inhalts erfolgen. Nach Ausführungsformen kann auch ein Speichermedium der körperlichen Urkunde oder des körperlichen Dokuments mit einer Kopie des entsprechenden Inhalts in elektronischer Form mit einem Lesegerät vollautomatisch ausgelesen werden. Dies erlaubt eine effiziente und effektive Echtheitsprüfung von Urkunden und Dokumenten. Ebenso kann die Grundlage von körperlichen Dokumenten geprüft werden, welche unter Verwendung von Daten erstellt wurden, welche durch die elektronische Urkunde beurkundet werden. Beispielsweise kann ein ID-Dokument, wie etwa ein Personalausweis oder Reisepass, ein Zeugnis, wie etwa

ein Hochschulzeugnis, oder ein Zulassungsdokument, wie etwa eine Approbation, ein Meisterbrief oder ein Führerschein, Angaben zu Geburtsname, Geburtsort und/oder Geburtsdatum umfassen. Diese Angaben werden durch eine Geburtsurkunde beurkundet, welche beispielsweise als elektronischen Dokument in der

5 Blockchain manipulationssicher gespeichert sein kann. Durch einen Abgleich der entsprechenden Angaben mit den von der elektronischen Urkunde bereitgestellten Daten, kann die Korrektheit dieser grundlegenden Angaben eines entsprechenden Dokuments geprüft werden.

10 Die Spezifikation, welche ein Datensatz zum Eintragen in die Blockchain erfüllen muss, kann beispielsweise neben kryptografischen Bedingungen, wie etwa eine Signatur, auch inhaltliche Bedingungen, wie ein Vorhandensein von vordefinierten Angaben umfassen.

15 Unter einer „elektronischen Urkunde“ wird hier ein Datenkonstrukt zur elektronischen Datenverarbeitung verstanden, welches Nutzdaten sowie eine Bescheinigung der Richtigkeit dieser Nutzdaten umfasst. Insbesondere kann die Gültigkeit einer elektronischen Urkunde unabhängig von einem Vorhandensein eines der Urkunde zugeordneten Urkundenkörpers sein. Mit anderen Worten kann eine elektronische
20 Urkunde aus ein oder mehreren Einträgen in ein oder mehreren Blöcken der Blockchain bestehen, unabhängig vom Speichermedium der Blockchain. Unter einer körperlichen Urkunde wird hier eine Urkunde verstanden, welche nur in Kombination mit ihrem Dokumentenkörper, beispielsweise aus Papier und/oder Kunststoff, Gültigkeit besitzt.

25

Unter einer „Blockchain“ wird hier und im Folgenden eine geordnete Datenstruktur verstanden, welche eine Mehrzahl von miteinander verketteten Datenblöcken umfasst. Insbesondere wird unter einer Blockchain eine geordnete Datenstruktur verstanden, bei welcher jeder der Blöcke (außer dem ersten Block) einen Prüfwert, beispielsweise einen Hash-Wert, seines Vorgängerblocks umfasst und somit anhand jedes Blocks die Gültigkeit aller seiner Vorgängerblocks geprüft und ggf. bestätigt werden kann. Beispiele einer Blockchain vergleiche

30

[https://en.wikipedia.org/wiki/Block_chain_\(database\)](https://en.wikipedia.org/wiki/Block_chain_(database)) und „Mastering Bitcoin“, Chapter 7, The Blockchain, Seite 161 ff. Das Konzept der Blockchain wurde beispielsweise im Jahre 2008 in einem White Paper unter dem Pseudonym Satoshi Nakamoto zu Bitcoin beschrieben („Bitcoin: Peer-to-Peer Electronic Cash System“

5 (<https://bitcoin.org/bitcoin.pdf>)). Die darin beschriebene Blockchain besteht aus einer Reihe von Datenblöcken, in denen jeweils ein oder mehrere Einträge bzw. Transaktionen zusammengefasst und mit einer Prüfsumme in Form eines Hashwerts versehen sind. Zusätzliche Blöcke der Blockchain werden beispielsweise in einem rechenintensiven Prozess erzeugt, der auch als sogenanntes Mining bezeichnet wird. Diese zusätzlich erzeugten Blöcke werden anschließend der Blockchain hinzugefügt und über ein Netzwerk an alle Teilnehmer, bzw. Knoten des Netzwerks, verbreitet.

Ausführungsformen können den Vorteil haben, dass die Blockchain durch die Speicherung kryptografischer Prüfsumme, d.h. Hashwerten, des vorangehenden Blocks im jeweils nachfolgenden Block ein hohes Maß an Sicherheit gegenüber nachträglichen Manipulationen bietet. Bei einer Blockchain werden die Einträge bzw. Transaktionen eines Blocks beispielsweise durch einen Merkle-Baum paarweise miteinander gehasht und nur der letzte auf diese Weise erhaltene Hashwert des Blocks, der sogenannte Root-Hashwert bzw. Wurzelhashwert, als Prüfsumme beispielsweise in einem Header des Blocks vermerkt. Das Verketteten der Blöcke kann dann unter Verwendung dieser Root-Hashwerte überprüft werden. Jeder Block der Blockchain enthält in seinem Header beispielsweise den Hash des gesamten vorherigen Block-headers. Somit wird die Reihenfolge der Blöcke eindeutig festgelegt und es entsteht

20 eine Kettenstruktur. Durch die so implementierte Verkettung der einzelnen Blöcke miteinander wird erreicht, dass ein nachträgliches Modifizieren vorangegangener Blöcke bzw. einzelner Transaktionen praktisch ausgeschlossen ist, da hierfür die Hashwerte aller nachfolgenden Blöcke in kurzer Zeit ebenfalls neu berechnet werden müssten.

30

Der erste Block in der Blockchain ist vorgegeben und wird Genesisblock genannt. Nach Ausführungsformen sind die öffentlichen kryptografischen Schlüssel eines

oder mehrerer Provider, welche zum Erstellen von Programmmodulen berechtigt sind, in dem Genesisblock gespeichert. Der Genesisblock ist aufgrund der zuvor beschriebenen Kettenstruktur, derjenige Block, dessen Einträge das höchste Maß an Sicherheit aufweisen, da zu seiner Änderung die gesamte Blockchain durch eine neue Blockchain ersetzt werden müsste. Mithin kann der Eintrag des öffentlichen kryptografischen Schlüssels in den Genesisblock einen Vertrauensanker mit einem ausreichenden Maß an Sicherheit darstellen, sodass beispielsweise keine zusätzliche PKI-Prüfung notwendig ist, um der Authentizität des öffentlichen kryptografischen Schlüssels zu vertrauen.

Vielmehr kann die Blockchain ausgehend von öffentlichen Schlüsseln, welche beispielsweise als Teil der Programmmodule und/oder als Teil eines Genesisblocks in die Blockchain eingetragen werden als Root-Keys oder Wurzelschlüssel für ein oder mehrere PKIs dienen, welche durch die Blockchain implementiert werden. So können beispielsweise weitere öffentliche Schlüssel in die Blockchain eingetragen werden, wenn die zugrundeliegenden Eintragungs- bzw. Registrierungsanfragen mit einer Signatur versehen sind, deren Gültigkeit sich unter Verwendung eines bereits in der Blockchain gültig eingetragenen öffentlichen Schlüssel bestätigen lässt.

Nach Ausführungsformen kann eine Blockchain durch eine Anpassung der notwendigen Rechenintensität für die Erstellung jeweils zusätzlicher Blöcke die Sicherheit der Blockchain anpassen. Die für die Erstellung zusätzlicher Blöcke notwendige Rechenintensität lässt sich beispielsweise über Anforderungen an den Hashwert des zu erstellenden zusätzlichen Blocks steuern. Der resultierende Hash-Wert ist nicht vorhersagbar, vielmehr handelt es sich um eine zufallsverteilte Zahl. Es lässt sich aber berechnen, wieviel Zeit in Abhängigkeit von der aufgewendeten Rechenleistung im statistischen Mittel zum Auffinden eines gültigen zusätzlichen Blocks notwendig ist. Der Hashwert eines Blocks lässt sich beispielsweise durch Hinzufügen und Variieren eines Nounce variieren. Aufgrund der Kettenstruktur können Daten, die einmal in einer Blockchain gespeichert sind, nicht mehr geändert oder entfernt werden, ohne große Teile der Blockchain zu ersetzen. Eine solche Ersetzung scheidet jedoch als Folge einer ausreichend rechenintensiven Generierung zusätzli-

cher Blöcke aus. Bekannte Ausführungsformen einer Blockchain, wie etwa im Fall der Kryptowährung Bitcoin, basieren auf einer Anonymität der an den Transaktionen beteiligten Partner. Demgegenüber kann durch oben beschriebene Signatur der in die Transaktionen eingetragenen Hashwerte, deren Authentizität belegt und ihr Ursprung nachgewiesen werden. Hierdurch kann die Fälschungssicherheit verbessert werden.

Eine Anforderung an einen gültigen Block kann beispielsweise darin bestehen, dass der Hashwert des Headers des Blocks kleiner gleich einem Grenzwert ist. Die

Hashwertberechnung kann beispielsweise mit dem Secure Hash Algorithm (SHA) SHA 256 erfolgen. Der resultierende Hash-Wert ist in diesem Fall eine Zufallszahl zwischen 0 und $2^{256}-1$. Die Wahrscheinlichkeit, dass beim Anwenden des Hashalgorithmus einen bestimmten Hash herauskommt, ist somit $(\text{maximaler Hash-Wert}+1)^{-1}$, im Falle des SHA 256-Algorithmus also 2^{-256} . Die Wahrscheinlichkeit, dass der re-

sultierende Hash-Wert kleiner gleich einem Grenzwert bzw. Zielwert (engl. target) ist, beträgt daher $(\text{target})/(\text{max. Hash-Wert})$. Für einen beispielhaften maximalen Grenzwert von $(2^{16}-1) \cdot 2^{208}$ beträgt die Wahrscheinlichkeit $[(2^{16}-1) \cdot 2^{208}] / 2^{256} \approx 2^{-32}$.

Die Schwierigkeit S eine Hash-Wert zu erhalten, welcher kleiner gleich einem gewählten Grenzwert bzw. target ist, kann in Abhängigkeit eines maximalen Grenzwerts bzw. max. target wie folgt angegeben werden: $S = (\text{max. target})/\text{target}$. Mithin

ist die Wahrscheinlichkeit einen Hash-Wert zu erhalten, welcher kleiner gleich dem gewählten Grenzwert ist, für das zuvor gegebene Beispiel: $2^{-32}/S$. Als Beispiel sei ein Computersystem mit einer bestimmten Hashrate betrachtet, welches im Durchschnitt alle x·Sek. einen Hash-Wert findet, welcher kleiner gleich dem gewählten

Grenzwert ist. Soll das Computersystem anstelle aller x·Sek. im Durchschnitt alle y·Sek. einen Treffer erzielen, so kann die Schwierigkeit entsprechend angepasst werden: $S_y = (x/y) \cdot S$. Entsprechende Anpassungen der Schwierigkeit können auch dazu verwendet werden die Trefferrate bei Veränderungen des Computersystems, z.B. Veränderungen der Rechenleistung durch Erhöhen oder Verringern der Anzahl an Blockchain-Servern, konstant zu halten. Wird die Schwierigkeit so angepasst,

dass alle y·Sek. ein Treffer erzielt wird, kann die Hashrate R des Computersystems wie folgt parametrisiert werden: $R = (2^{32} \cdot S)/(y \cdot \text{Sek.})$.

- Eine Blockchain kann beispielsweise auch in Form einer privaten, d.h. zugangsbeschränkten, Blockchain implementiert werden, wobei nur eine ausgewählte Gruppe von Teilnehmern eine Berechtigung zum Hinzufügen gültiger Blöcke und/oder zum
- 5 Lesen von Blöcken besitzt. Eine entsprechende Berechtigung kann beispielsweise mittels einer Signatur unter Verwendung eines privaten kryptografischen Schlüssels nachgewiesen werden. Der private kryptografische Schlüssel kann zu einem asymmetrischen Schlüsselpaar gehören, zu welchem auch ein öffentlicher kryptografischer Schlüssel gehört, mit dem die Signatur geprüft werden kann. Dem asymmetri-
- 10 schen Schlüsselpaar kann zudem beispielsweise ein Zertifikat zugeordnet sein, welches die Berechtigung zum Erzeugen eines gültigen Blocks der Blockchain belegt. Dieses Zertifikat kann ferner einer PKI zugeordnet sein, welche die Authentizität des Zertifikats belegt. Nach einer weiteren Ausführungsform kann beispielsweise für jeden Teilnehmer aus der ausgewählten Gruppe ein öffentlicher Schlüssel in der
- 15 Blockchain hinterlegt sein. Anhand dieser öffentlichen Schlüssel kann geprüft werden, ob Signaturen von Blöcken und damit die entsprechenden Blöcke selbst gültig sind. Mit anderen Worten kann die Blockchain in diesem Fall selbst eine eigenständige PKI bereitstellen.
- 20 Ein Konsens über eine Gültigkeit eines zusätzlichen Blocks für die Blockchain bzw. über ein Hinzufügen eines zusätzlichen Blocks zu der Blockchain kann auch auf andere Weise in einer Blockchain implementiert werden. So kann etwa ein Konsens erreicht werden, indem über eine Aufnahme vorgeschlagener Einträge in die Blockchain abgestimmt wird. Beispielsweise führt jeder Teilnehmer eine eindeutige Liste
- 25 anderer Teilnehmer, welchen er als Gruppe vertraut. Bei diesen Teilnehmern kann es sich beispielsweise um Blockchain-Server handeln. Jeder Teilnehmer kann zusätzliche Einträge vorschlagen, die in einen zusätzlichen Block der Blockchain aufgenommen werden sollen. Über die Aufnahme und damit die Anerkennung der Gültigkeit der vorgeschlagenen Einträge wird abgestimmt. So stimmt beispielsweise
- 30 jeder Teilnehmer nur über diejenigen Vorschläge ab, welche von Teilnehmer seiner Liste stammen. Mit anderen Worten werden für die Entscheidung, ob ein Vorschlag für einen zusätzlichen Eintrag als gültig anerkannt wird, d.h. ob bezüglich der Gül-

tigkeit dieses Eintrages ein Konsens zwischen den Teilnehmern besteht, nur die Stimmen derjenigen Teilnehmer berücksichtig, die von der Liste desjenigen Teilnehmers umfasst sind, der den entsprechenden Vorschlag macht. Damit ein Vorschlag für einen Eintrag als gültig angenommen wird, muss ein bestimmter Minimumanteil an stimmberechtigten Teilnehmern mit Ja stimmen, beispielsweise 80%. Alle vorgeschlagenen Einträge, die dieses Kriterium erfüllen werden in die Blockchain aufgenommen. Eine solche Abstimmung kann mehrere Runden umfassen. Alle anderen Vorschläge, die das zuvor genannte Kriterium nicht erfüllen, werden verworfen oder bei der Abstimmung über den nächsten Block der Blockchain erneut zur Abstimmung gestellt. Die zuvor genannten Listen stellen Untergruppen des Blockchain-Netzwerks dar, denen der Teilnehmer, welcher die jeweilige Liste führt, als Gruppe insgesamt traut, ohne dass dies erfordert, dass er jedem einzelnen Teilnehmer der Liste traut. Ein Beispiel für ein solches Konsensverfahren bietet der Ripple Protokoll Konsens Algorithmus (David Schwartz et al.: „The Ripple Protocol Consensus Algorithm“, Ripple Labs Inc., 2014, https://ripple.com/files/ripple_consensus_whitepaper.pdf).

Beispielsweise kann es sich bei der Blockchain um eine private oder öffentliche Blockchain handeln. Beispielsweise handelt es sich um eine Bitcoin-, Litecoin- oder Ethereum-Blockchain.

Ein „Programmmodul“ bezeichnet hier ein eigenständiges Programm, welches in einer Blockchain gespeichert ist. Das Programmmodul kann dazu konfiguriert sein das Erstellen von dem Programmmodul zugeordneten Einträgen in der Blockchain zu steuern. Das Programmmodul kann in einem Block der Blockchain oder über mehrere Blöcke der Blockchain verteilt gespeichert sein. Jeder Urkundenspezifikation ist beispielsweise ein individuelles Programmmodul zugeordnet. Bei einem Programmmodul kann es sich beispielsweise um einen „smart contract“ handeln, wie er beispielsweise in der Open Source Ethereum Blockchain implementierbar ist.

Unter einem „Programm“ bzw. „Programminstruktionen“ wird hier ohne Einschränkung jede Art von Computerprogramm verstanden, welches maschinenlesbare Instruktionen zur Steuerung einer Funktionalität des Computers umfasst.

- 5 Unter einem „Zertifikat“ wird hier ein digitales Zertifikat verstanden, welches auch als Public-Key-Zertifikat bezeichnet wird. Durch solche Zertifikate basierend auf asymmetrischen Schlüsselpaaren wird eine so genannte Public Key Infrastructure (PKI) realisiert. Bei einem solchen Zertifikat handelt es sich um strukturierte Daten, die dazu dienen, einen öffentlichen Schlüssel eines asymmetrischen Kryptosystems
- 10 einer Identität, wie zum Beispiel einer Person oder einer Vorrichtung, zuzuordnen. Ein Zertifikat kann beispielsweise einen öffentlichen Schlüssel beinhalten und signiert sein. Alternativ sind auch Zertifikate basierend auf zero-knowledge Kryptosystemen möglich. Beispielsweise kann das Zertifikat dem Standard X.509 oder einem anderen Standard entsprechen. Beispielsweise handelt es sich bei dem Zertifikat
- 15 um ein CV-Zertifikat oder auch Card Verifiable Certificate (CVC). Eine Implementierung von solchen CVCs ist beispielsweise in der ISO/IEC 7816-8 spezifiziert.

- Die PKI stellt ein System zum Ausstellen, Verteilen und Prüfen digitaler Zertifikate. Ein digitales Zertifikat dient in einem asymmetrischen Kryptosystem dazu die Au-
- 20 thentizität eines öffentlichen Schlüssels und seinen zulässigen Anwendungs- und Geltungsbereich zu bestätigen. Eine solche Bestätigung kann auch über einen Eintrag in der Blockchain erfolgen, in welchem Fall diese Einträge als Zertifikate zu verstehen sind. Das digitale Zertifikat ist selbst durch eine digitale Signatur geschützt, deren Echtheit mit dem öffentlichen Schlüssel des Ausstellers des Zertifikats
- 25 geprüft werden kann. Um die Authentizität des Ausstellerschlüssels zu prüfen, wird wiederum ein digitales Zertifikat verwendet. Auf diese Weise lässt sich eine Kette von digitalen Zertifikaten aufbauen, die jeweils die Authentizität des öffentlichen Schlüssels bestätigen, mit dem das vorhergehende Zertifikat geprüft werden kann. Eine solche Kette von Zertifikaten bildet einen sogenannten Validierungspfad
- 30 oder Zertifizierungspfad. Auf die Echtheit des letzten Zertifikats, des sogenannten Wurzelzertifikats, und des durch dieses Zertifikat zertifizierten Schlüssels, müssen sich die Teilnehmer der PKI ohne ein weiteres Zertifikat verlassen können. Das

Wurzelzertifikat wird von einer sogenannten Wurzelzertifizierungsinstanz verwaltet, auf deren als gesichert vorausgesetzten Authentizität die Authentizität aller Zertifikate der PKI zurückgeht.

- 5 Ein Zertifikat kann einer elektronischen Signatur zugeordnet sein, wenn der zu dem öffentlichen Schlüssel gehörende private Schlüssel zur Generierung der zu prüfenden elektronischen Signatur verwendet wurde. Dadurch, dass ein Zertifikat in Assoziation mit einem öffentlichen Schlüssel der Allgemeinheit zur Verfügung gestellt wird, wird es Nutzern asymmetrischer Kryptosysteme ermöglicht den öffentlichen
- 10 Schlüssel einer Identität, beispielsweise einer Person, einer Organisation, oder einem Computersystem, zuzuordnen.

- Asymmetrische Schlüsselpaare werden für eine Vielzahl von Kryptosystemen eingesetzt und spielen auch bei der Signatur elektronischer Dokumente eine wichtige
- 15 Rolle. Ein asymmetrisches Schlüsselpaar besteht aus einem öffentlichen Schlüssel, welcher zur Ver- und/oder Entschlüsselung von Daten verwendet wird und an Dritte, beispielsweise an einen Dienstanbieter, weitergegeben werden darf sowie einem privaten Schlüssel, welcher zur Ver- und/oder Entschlüsselung von Daten verwendet wird und im Regelfall geheim gehalten werden muss. Der öffentliche Schlüssel
- 20 ermöglicht es jedermann, Daten für den Inhaber des privaten Schlüssels zu verschlüsseln, digitale Signaturen von dessen Dokumenten zu prüfen oder ihn zu authentifizieren. Ein privater Schlüssel ermöglicht es seinem Inhaber, mit dem öffentlichen Schlüssel verschlüsselte Daten zu entschlüsseln oder digitale Signaturen für elektronische Dokumente zu erstellen. Eine mit einem privaten Schlüssel erstellte
- 25 Signatur kann mit dem zugehörigen öffentlichen Schlüssel verifiziert werden.

- Digitale Signaturen werden zum sicheren elektronischen Datenaustausch, beispielsweise im Internet, eingesetzt und ermöglichen die Prüfung von Identitäten und/oder Berechtigungen und der Unverfälschtheit der ausgetauschten Daten. Um
- 30 dies zu gewährleisten, ist in der Regel eine Public-Key-Infrastruktur notwendig, die die Gültigkeit der verwendeten Schlüssel durch Zertifikate bestätigt.

Die Erstellung einer digitalen Signatur, im Folgenden auch lediglich als „Signatur“ bezeichnet, ist ein kryptografisches Verfahren, bei dem zu beliebigen Daten, zum Beispiel einem elektronischen Dokument, ein weiterer Datenwert, welcher als „Signatur“ bezeichnet wird, berechnet wird. Die Signatur kann zum Beispiel ein verschlüsselter Hashwert des elektronischen Dokumentes sein, insbesondere ein mit einem privaten Schlüssel eines einem Zertifikat zugeordneten kryptografischen Schlüsselpaars verschlüsselter Hashwert. Ein entsprechendes Verschlüsseln eines Hashwerts wird mithin als Signieren des Hashwerts bezeichnet. Die Besonderheit einer solchen Signatur besteht darin, dass deren Urheberschaft und Zugehörigkeit zu einer bestimmten Person oder Instanz durch jeden Dritten geprüft werden kann.

Unter einer digitalen Signatur wird hier auch ein digitales Siegel verstanden, welches nicht einer natürlichen Person, sondern einer juristischen Person zugeordnet ist. Ein digitales Siegel dient somit nicht der Abgabe einer Willenserklärung einer einzelnen Person, sondern einer Institution als Herkunftsnachweis. Es kann somit den Ursprung und die Unversehrtheit digitaler Dokumente sicherstellen und nachweisen, dass diese von einer bestimmten juristischen Person stammen.

Unter einem „Speicher“ werden hier sowohl flüchtige als auch nicht flüchtige Speicher, insbesondere elektronische Speicher bzw. digitale Speichermedien verstanden.

Unter einem „nichtflüchtigen Speicher“ wird hier ein elektronischer Speicher zur dauerhaften Speicherung von Daten verstanden. Ein nichtflüchtiger Speicher kann als nichtänderbarere Speicher konfiguriert sein, der auch als Read-Only Memory (ROM) bezeichnet wird, oder als änderbarer Speicher, der auch als Non-Volatile Memory (NVM) bezeichnet wird. Insbesondere kann es sich hierbei um ein EEPROM, beispielsweise ein Flash-EEPROM, kurz als Flash bezeichnet, handeln. Ein nichtflüchtiger Speicher zeichnet sich dadurch aus, dass die darauf gespeicherten Daten auch nach Abschalten der Energieversorgung erhalten bleiben.

Unter einem „flüchtigen elektronischen Speicher“ wird hier ein Speicher zur vorübergehenden Speicherung von Daten, welcher dadurch gekennzeichnet ist, dass alle Daten nach dem Abschalten der Energieversorgung verloren gehen. Insbesondere kann es sich hierbei um einen flüchtigen Direktzugriffsspeicher, der auch als

5 Random-Access Memory (RAM) bezeichnet wird, oder einen flüchtigen Arbeitsspeicher des Prozessors handeln.

Unter einem „geschützten Speicherbereich“ wird hier ein Bereich eines elektronischen Speichers verstanden, auf den ein Zugriff, das heißt ein Lesezugriff oder ein

10 Schreibzugriff, nur über einen Prozessor des entsprechenden elektronischen Geräts möglich ist. Nach Ausführungsformen ist der Zugriff von dem mit dem Speicher gekoppelten Prozessor nur dann möglich, wenn eine hierzu erforderliche Bedingung erfüllt ist. Hierbei kann es sich zum Beispiel um eine kryptografische Bedingung, insbesondere eine erfolgreiche Authentisierung und/oder eine erfolgreiche Berechtigungsprüfung, handeln.

15

Unter einem „Prozessor“ wird hier und im Folgenden eine Logikschaltung verstanden, die zur Ausführung von Programminstruktionen dient. Die Logikschaltung kann auf einem oder mehreren diskreten Bauelementen implementiert sein, insbesondere

20 auf einem Chip. Insbesondere wird unter einem „Prozessor“ ein Mikroprozessor oder ein Mikroprozessorsystem aus mehreren Prozessorkernen und/oder mehreren Mikroprozessoren verstanden.

Unter einer „Kommunikationsschnittstelle“ wird hier eine Schnittstelle verstanden, über die Daten empfangen und gesendet werden können, wobei die Kommunikationsschnittstelle kontaktbehaftet oder kontaktlos konfiguriert sein kann. Bei der

25 Kommunikationsschnittstelle kann es sich um eine interne Schnittstelle oder um eine externe Schnittstelle handeln, welche beispielsweise mittels eines Kabels oder kabellos mit einem zugeordneten Gerät verbunden ist.

30

Eine Kommunikation kann beispielsweise über ein Netzwerk erfolgen. Unter einem „Netzwerk“ wird hier jedes Übertragungsmedium mit einer Anbindung zur Kommuni-

kation verstanden, insbesondere eine lokale Verbindung oder ein lokales Netzwerk, insbesondere ein Local Area Network (LAN), ein privates Netzwerk, insbesondere ein Intranet, und ein virtuelles privates Netzwerk (Virtual Private Network – VPN). Beispielsweise kann ein Computersystem eine Standardfunkschnittstelle zur Anbin-

5 dung an ein WLAN aufweisen. Ferner kann es sich um ein öffentliches Netzwerk, wie beispielsweise das Internet handeln. Je nach Ausführungsform kann diese Verbindung auch über ein Mobilfunknetz hergestellt werden.

Unter einem „Mobilfunknetzwerk“ wird hier und im Folgenden ein digitales zellulARES

10 Mobilfunknetzwerk verstanden, welches nach einem Mobilfunkstandard wie zum Beispiel GSM, UMTS, LTE, CDMA oder einem anderen Standard aufgebaut sein kann.

Nach Ausführungsformen ist der erste Datensatz signiert. Die Signatur des ersten

15 Datensatzes dient als ein Nachweis einer Berechtigung zum Ausstellen einer elektronischen Urkunde entsprechend der ersten Spezifikation der ersten hoheitlichen Institution und der erste Blockchain-Server prüft als eine Voraussetzung für die Eintragung des ersten Datensatzes in die Blockchain unter Verwendung eines ersten öffentlichen kryptografischen Schlüssels, ob die Signatur des ersten Datensatzes

20 gültig ist.

Ausführungsformen können den Vorteil haben, dass durch eine Überprüfung der Signatur sichergestellt werden kann, dass ein in die Blockchain einzutragender Datensatz von einem dazu berechtigten Ersteller vorgelegt wird und dass der Inhalt

25 des vorgelegten Datensatzes mit dem Inhalt zum Zeitpunkt der Signatur übereinstimmt, d.h. dass der Inhalt des Datensatzes von dem eintragungsberechtigten Ersteller bestätigt wird.

Nach Ausführungsformen umfasst die erste Spezifikation eine gültige Signatur des

30 ersten Datensatzes und das Ausführen der ersten Programminstruktionen umfasst das Prüfen der Signatur des ersten Datensatzes unter Verwendung des ersten öffentlichen kryptografischen Schlüssels.

Ausführungsformen können den Vorteil haben, dass eine Signaturprüfung als Teil der zu erfüllenden Spezifikation durch das Programmmodul, genauer gesagt durch die von dem Programmmodul bereitgestellten Programminstruktionen, vorgegeben und somit im Zuge der Eintragung automatisch implementiert wird.

Nach Ausführungsformen wird der erste öffentliche kryptografische Schlüssel zur Prüfung der Signatur des ersten Datensatzes von der Blockchain zur Verfügung gestellt. Ausführungsformen können den Vorteil haben, dass neben der Blockchain keine weitere umfangreiche PKI notwendig ist, sondern dass die Blockchain vielmehr eine eigene PKI umfasst.

Nach Ausführungsformen wird der erste Datensatz über eine Ende-zu-Ende-verschlüsselte Kommunikationsverbindung empfangen. Ausführungsformen können den Vorteil haben, dass eine sichere Übertragung des Datensatzes von einem als Sender fungierenden Computersystem über ein Netzwerk, ein privates oder öffentliches Netzwerk, an den Blockchain-Server in sicherer Weise erfolgen kann. Bei alternativen Ausführungsformen handelt es sich bei dem Datensatz um einen von dem Blockchain-Server selbst ausgestellten Datensatz.

Eine Urkunde umfasst beispielsweise ein oder mehrere der folgenden Angabe: Einen Namen einer die Urkunde ausstellenden juristischen Person, einen Namen einer beurkundenden natürlichen Person, einen Ort der Ausstellung, ein Datum der Ausstellung, ein Siegel der ausstellenden juristischen Person, z.B. ein elektronisches Siegel, eine Signatur der beurkundenden natürlichen Person, z.B. eine elektronische Signatur, sowie zu beurkundende Angaben, d.h. Daten.

Nach Ausführungsformen handelt es sich bei den elektronischen Urkunden um Geburtsurkunden.

Eine Geburtsurkunde eines Kindes umfasst beispielsweise ein oder mehrere der folgenden Angabe: Einen Namen des ausstellenden Standesamts, eine laufende

Nummer des Geburtseintrags, z.B. zusammen mit dem Jahr der Geburt, alle Vornamen des Kindes, einen Geburtsname des Kindes, ein Geschlecht des Kindes, ein Geburtsdatum des Kindes, einen Geburtsort des Kindes, Angaben zu rechtlichen Eltern, z.B. Vornamen und Familiennamen sowie Angaben zu Religion des Kindes und Elternteils, einen Ort des ausstellenden Standesamts, ein Datum der Ausstellung der Geburtsurkunde, ein Siegel des Standesamtes, z.B. ein elektronisches Siegel, d.h. eine elektronische Signatur, deren zugrundeliegendes asymmetrische Schlüsselpaar keiner natürlichen Person sondern einer juristischen Person zugeordnet ist, eine Signatur des beurkundenden Standesbeamten, z.B. eine elektronische Signatur des beurkundenden Standesbeamten, einen Namen des beurkundenden Standesbeamten.

Nach Ausführungsformen umfasst das Verfahren ferner:

- Empfangen eines zweiten Datensatzes zum Eintragen in die Blockchain durch einen zweiten Blockchain-Server des Blockchain-Netzwerks, wobei der zweite Datensatz Daten einer auszustellenden zweiten elektronischen Urkunde entsprechend einer zweiten Spezifikation einer zweiten hoheitlichen Institution umfasst, wobei der zweite Blockchain-Server der zweiten hoheitlichen Institution zugeordnet ist,
- Ausführen zweiter Programminstruktionen eines zweiten Programmmoduls der Mehrzahl von Programmmodulen durch den zweiten Blockchain-Server, wobei das zweite Programmmodul zum Ausstellen von elektronischen Urkunden entsprechend der zweiten Spezifikation konfiguriert ist, wobei das Ausführen der zweiten Programminstruktionen ein Prüfen des zweiten Datensatzes durch den zweiten Blockchain-Server umfasst, ob der zweite Datensatz die zweite Spezifikation erfüllt, falls der zweite Datensatz die zweite Spezifikation erfüllt, ein Hinzufügen des zweiten Datensatzes zu einem zweiten zusätzlichen Block der Blockchain.

Ausführungsformen können den Vorteil haben, dass die einzelnen hoheitlichen Institutionen unabhängig voneinander elektronische Urkunden mit unterschiedlichen Spezifikationen ausstellen und manipulationssicher in der Blockchain speichern

können.

Nach Ausführungsformen umfasst das Verfahren ferner:

- 5 • Empfangen eines dritten Datensatzes zum Eintragen in die Blockchain durch den ersten Blockchain-Server des Blockchain-Netzwerks, wobei der dritte Datensatz Daten zur Ergänzung des ersten Datensatzes der ausgestellten ersten elektronischen Urkunde und einen Identifikator des ersten Datensatzes umfasst,
- 10 • Ausführen der ersten Programminstruktionen durch den ersten Blockchain-Server, wobei das Ausführen der ersten Programminstruktionen ein Prüfen des dritten Datensatzes durch den ersten Blockchain-Server umfasst, ob der dritte Datensatz ein oder mehrere von dem ersten Programmmodul festgelegte erste Voraussetzungen erfüllt, falls der dritte Datensatz die ersten Voraussetzungen erfüllt, ein Hinzufügen des dritten Datensatzes zu einem dritten zusätzlichen Block der Blockchain.
- 15

Ausführungsformen können den Vorteil haben, dass sie Ergänzungen der elektronischen Urkunden ermöglichen. Bei entsprechenden Ergänzungen kann es sich entweder um Korrekturen handeln, d.h. Angaben der ursprünglichen elektronischen

20 Urkunde werden durch Angaben ersetzt, welche der Datensatz, d.h. Ergänzungsdatsatz, bereitgestellt, oder um Zusätze, d.h. es werden zusätzliche Angaben ergänzt, welche die ursprüngliche elektronische Urkunde noch nicht umfasst hat. So wird beispielsweise nach deutschem Recht im Fall einer Geburtsurkunde bei einem Kind, welches während einer bestehenden Ehe geboren wird, der Vater, der zum

25 Zeitpunkt der Geburt mit der Mutter des Kindes verheiratet ist, als Vater des Kindes in die Geburtsurkunde eingetragen. Handelt es sich bei dem mit der Mutter verheirateten Mann nicht um den leiblichen Vater, so kann die Angabe zum Vater des Kindes später korrigiert werden, wobei der leibliche Vater als Vater des Kindes eingetragen wird.

30

Nach Ausführungsformen umfasst der erste Datensatz einen öffentlichen kryptografischen Schlüssel eines asymmetrischen Schlüsselpaars der ersten elektronischen

Urkunde. Der dritte Datensatz ist mit einem privaten kryptografischen Schlüssel des asymmetrischen Schlüsselpaars der ersten elektronischen Urkunde signiert. Eine der ersten Voraussetzungen ist eine gültige Signatur des dritten Datensatzes mit dem privaten kryptografischen Schlüssel des asymmetrischen Schlüsselpaars der ersten elektronischen Urkunde und das Ausführen der dritten Programminstruktionen umfasst das Prüfen der Signatur des dritten Datensatzes unter Verwendung des von dem ersten Datensatz bereitgestellten öffentlichen kryptografischen Schlüssel.

- 5
- 10 Ausführungsformen können den Vorteil haben, dass der elektronischen Urkunde ein asymmetrisches Schlüsselpaar zugeordnet werden kann, welches es dem Besitzer des privaten kryptografischen Schlüssels des entsprechenden asymmetrischen Schlüsselpaars ermöglicht, weitere Daten in die Blockchain einzutragen und somit an die elektronische Urkunde anzuhängen. Beispielsweise kann ein privater Schlüssel des entsprechenden kryptografischen Schlüsselpaars von einer körperlichen
- 15 Version der elektronischen Urkunde umfasst sein. So kann etwa bei jeder Verwendung der entsprechenden körperlichen Urkunde ein Hinzufügen eines entsprechenden Vermerks in die Blockchain als zusätzlicher Eintrag ermöglicht werden. Durch die Signatur mit dem privaten Schlüssel kann dabei nachgewiesen werden kann,
- 20 dass die körperliche Version der elektronischen Urkunde tatsächlich vorgelegen hat.

- Nach Ausführungsformen umfasst das Verfahren ferner ein Ausstellen einer ersten körperlichen Urkunde, welche inhaltlich mit der ersten elektronischen Urkunde übereinstimmt, unter Verwendung des ersten Datensatz. Die erste körperliche Urkunde umfasst einen maschinenlesbaren Code, wobei der maschinenlesbare Code einen Identifikator des ersten Datensatzes und/oder einen Identifikator des dritten Datensatzes umfasst.
- 25

- Ausführungsformen können den Vorteil haben, dass die Echtheit einer körperlichen Urkunde durch die Blockchain in effektiver und effizienter Weise mittels eines Abgleichs der von der körperlichen Urkunde bereitgestellten Daten mit den in der Blockchain gespeicherten Daten implementiert werden kann.
- 30

Bei dem maschinenlesbaren Code kann es sich beispielsweise um einen ein- oder zweidimensionalen graphischen Code handeln, welcher mittels eines optoelektronischen Lesegeräts lesbar ist. Der Code kann gängige Schrift-, Zahl- und/oder Sonderzeichen umfassen. ferner kann der Code geometrische Formen, wie etwa Striche und Punkte unterschiedlicher Dimensionierung umfassen. Bei dem Code handelt es sich beispielsweise um einen eindimensionalen Strichcode, einen gestapelten eindimensionalen Strichcode, einen Array-Code, wie etwa einen Matrix-Code, z.B. einen QR-Code, oder einen Punktcode. Ferner kann es sich um einen zusammengesetzten Code (Composite-Codes) wie etwa einen Doppelcode handeln. Ein Doppelcode setzt sich beispielsweise zusammen aus einem linearen Barcode und einem zusätzlichen zweidimensionalen Code. Ferner kann es sich um einen eindimensionalen Barcode, welcher zusätzlich die zweite Dimension in Form von unterschiedlich langen Strichen zur Codierung nutzt. Auch höherdimensionale Codes mit drei oder mehr Dimensionen können implementiert werden, etwa über eine Verwendung von unterschiedlichen Farben.

Bei dem maschinenlesbaren Code kann es sich ferner um in einem Speicher, etwa eines Chips oder eines RFID-Tags, gespeicherte Daten handeln, welche mit einem Lesegerät ausgelesen werden können.

Nach Ausführungsformen umfasst der maschinenlesbare Code eine Signatur der Daten der Urkunde mit einem privaten kryptografischen Schlüssel.

Nach Ausführungsformen umfasst das Verfahren ferner:

- Empfangen eines vierten Datensatzes zum Eintragen in die Blockchain durch den ersten Blockchain-Server des Blockchain-Netzwerks, wobei der vierte Datensatz Daten einer ausgestellten dritten elektronischen Urkunde entsprechend der ersten Spezifikation der ersten hoheitlichen Institution oder entsprechend einer vierten Spezifikation einer vierten von der Mehrzahl von hoheitlichen Institutionen nicht umfassten hoheitlichen Institution umfasst,

- Ausführen vierter Programminstruktionen des ersten Programmmoduls durch den ersten Blockchain-Server, wobei das Ausführen der vierten Programminstruktionen ein Prüfen des vierten Datensatzes durch den ersten Blockchain-Server umfasst, ob der vierte Datensatz ein oder mehrere von dem ersten Programmmodul festgelegte zweite Voraussetzungen erfüllt, falls der vierte Datensatz die zweiten Voraussetzungen erfüllt, ein Hinzufügen des vierten Datensatzes zu einem vierten zusätzlichen Block der Blockchain.

Ausführungsformen können den Vorteil haben, dass bereits ausgestellte Urkunden, wie etwa Geburtsurkunden, nachträglich in der Blockchain ergänzt werden können. Insbesondere können beispielsweise Geburtsurkunden anderer hoheitlicher Institutionen, welche nicht zu den das Blockchain-Netzwerk betreibenden hoheitlichen Institutionen gehören, in der Blockchain nachgetragen werden. Dies kann beispielsweise im Zuge von Visum-, Asyl- und/oder Einbürgerungsverfahren von Vorteil sein.

Nach Ausführungsformen sind die vierten Programminstruktionen und zweiten Voraussetzungen identisch zu den ersten Programminstruktionen und ersten Spezifikation. Ausführungsformen können den Vorteil haben, dass sie ein effektives und effizientes Verfahren zur Digitalisierung, d.h. elektronischen Erfassung, von bestehenden Dokumenten bereitstellen.

Nach Ausführungsformen umfasst das Verfahren ferner:

- Empfangen eines fünften Datensatzes zum Eintragen in die Blockchain durch den ersten Blockchain-Server des Blockchain-Netzwerks, wobei der fünfte Datensatz einen Identifikator eines unter Verwendung des ersten Datensatzes ausgestellten körperlichen ID-Dokuments und den Identifikator des ersten Datensatzes umfasst,
- Ausführen fünfter Programminstruktionen des ersten Programmmoduls durch den ersten Blockchain-Server, wobei das Ausführen der fünften Programminstruktionen ein Prüfen des fünften Datensatzes durch den ersten Blockchain-Server umfasst, ob der fünfte Datensatz ein oder mehrere von dem ersten

Programmmodul festgelegte dritte Voraussetzungen erfüllt, falls der fünfte Datensatz die dritten Voraussetzungen erfüllt, ein Hinzufügen des fünften Datensatzes zu einem fünften zusätzlichen Block der Blockchain.

- 5 Ausführungsformen können den Vorteil haben, dass die Blockchain Informationen bereitstellen kann, welche körperliche ID-Dokumente auf Basis der elektronischen Urkunde, die in der Blockchain manipulationssicher gespeichert ist, ausgestellt werden. Beispielsweise kann auf Basis einer in der Blockchain gespeicherten Geburtsurkunde ein Ausweis, wie etwa ein Kinderpass, ein Personalausweis und/oder ein
- 10 Reisepass, oder ein Führerschein ausgestellt werden.

- Nach Ausführungsformen werden auf analoge Weise Ausstellungen von körperlichen Versionen der in der Blockchain gespeicherten elektronischen Urkunde vermerkt. Somit kann anhand der Blockchain stets nachvollzogen, wie viele körperlichen Versionen einer elektronischen Urkunde ausgegeben wurden. Als Identifikatoren der körperlichen Versionen einer elektronischen Urkunde kann beispielsweise
- 15 jeweils eine fortlaufende Nummer oder eine Zufallszahl dienen. Nach Ausführungsformen wird auf analoge Weise ein Verlust einer der ausgestellten und in der Blockchain registrierten körperlichen Version der elektronischen Urkunde vermerkt. Durch
- 20 einen solchen Vermerk wird die entsprechende körperliche Version der elektronischen Urkunde ungültig.

- Nach Ausführungsformen umfasst das Verfahren ferner ein Ausstellen des körperlichen ID-Dokuments unter Verwendung des ersten Datensatzes, wobei das ID-
- 25 Dokument einen maschinenlesbaren Code umfasst. Der maschinenlesbare Code umfasst zumindest einen der folgenden Identifikatoren: den Identifikator des ersten Datensatzes, den Identifikator des ersten Datensatzes oder einen Identifikator des fünften Datensatzes.

- 30 Ausführungsformen können den Vorteil haben, dass anhand eines vorgelegten körperlichen Dokuments effektiv und effizient überprüft werden kann, auf Basis welcher Urkunde, z. B. Geburtsurkunde, das entsprechende ID-Dokument ausgestellt wurde

und/oder ob die von dem entsprechenden körperlichen ID-Dokument umfassten Angaben mit den von der elektronischen Urkunde beurkundeten Angaben übereinstimmen. Eine Überprüfung kann beispielsweise durch einen automatischen Abgleich der Inhalte des körperlichen ID-Dokuments der durch das entsprechende ID-Dokument identifizierten von der Blockchain bereitgestellten elektronischen Urkunde erfolgen. Hierzu wird beispielsweise der von dem körperlichen ID-Dokument bereitgestellte Inhalt, etwa durch Einscannen oder Auslesen aus einem auslesbaren elektronischen Speichermedium, erfasst und mit den in der Blockchain abgespeicherten Angaben des elektronischen Dokuments verglichen. Bei einer Übereinstimmung stellt die in der Blockchain elektronische Urkunde eine manipulationssichere Bestätigung der Angaben des vorgelegten ID-Dokuments dar.

Bei dem maschinenlesbaren Code kann es sich beispielsweise um einen ein- oder zweidimensionalen graphischen Code handeln, welcher mittels eines optoelektronischen Lesegeräts lesbar ist. Der Code kann gängige Schrift-, Zahl- und/oder Sonderzeichen umfassen. ferner kann der Code geometrische Formen, wie etwa Striche und Punkte unterschiedlicher Dimensionierung umfassen. Bei dem Code handelt es sich beispielsweise um einen eindimensionalen Strichcode, einen gestapelten eindimensionalen Strichcode, einen Array-Code, wie etwa einen Matrix-Code, z.B. einen QR-Code, oder einen Punktcode. Ferner kann es sich um einen zusammengesetzten Code (Composite-Codes) wie etwa einen Doppelcode handeln. Ein Doppelcode setzt sich beispielsweise zusammen aus einem linearen Barcode und einem zusätzlichen zweidimensionalen Code. Ferner kann es sich um einen eindimensionalen Barcode, welcher zusätzlich die zweite Dimension in Form von unterschiedlich langen Strichen zur Codierung nutzt. Auch höherdimensionale Codes mit drei oder mehr Dimensionen können implementiert werden, etwa über eine Verwendung von unterschiedlichen Farben.

Bei dem maschinenlesbaren Code kann es sich ferner um in einem Speicher, etwa eines Chips oder eines RFID-Tags, gespeicherte Daten handeln, welche mit einem Lesegerät ausgelesen werden können.

Unter einem „ID-Dokument“ wird insbesondere ein Ausweis- oder Sicherheitsdokument, insbesondere ein hoheitliches Dokument, insbesondere ein papierbasiertes und/oder kunststoffbasiertes Dokument, wie zum Beispiel ein elektronisches Ausweisdokument, insbesondere Reisepass, Personalausweis, Visum, Führerschein, Gesundheitskarte, oder einen Firmenausweis, eine Chipkarte, Bankkarte oder Kreditkarte. Insbesondere kann es sich bei dem ID-Dokument um ein Machine-Readable Travel Document, wie beispielsweise von der Internationalen Luftfahrtbehörde (ICAO) und/oder dem BSI standardisiert, handeln.

- 10 Nach Ausführungsformen umfasst das Verfahren ferner ein Ausstellen des körperlichen Dokuments unter Verwendung des ersten Datensatzes, wobei das Dokument einen maschinenlesbaren Code umfasst. Der maschinenlesbare Code umfasst zumindest einen der folgenden Identifikatoren: den Identifikator des ersten Datensatzes, den Identifikator des ersten Datensatzes oder einen Identifikator des fünften
- 15 Datensatzes.

- Unter einem „Dokument“ wird insbesondere ein Ausweis-, Wert- oder Sicherheitsdokument, insbesondere ein hoheitliches Dokument, insbesondere ein papierbasiertes und/oder kunststoffbasiertes Dokument, wie zum Beispiel ein elektronisches
- 20 Ausweisdokument, insbesondere Reisepass, Personalausweis, Visum, Führerschein, Fahrzeugschein, Fahrzeugbrief, Gesundheitskarte, oder einen Firmenausweis, oder eine anderes ID-Dokument, eine Chipkarte, Zahlungsmittel, insbesondere Banknote, Bankkarte oder Kreditkarte, Frachtbrief oder ein sonstiger Berechtigungsnachweis verstanden. Insbesondere kann es sich bei dem Dokument um ein
- 25 Machine-Readable Travel Document, wie beispielsweise von der Internationalen Luftfahrtbehörde (ICAO) und/oder dem BSI standardisiert, handeln.

Nach Ausführungsformen umfasst das Verfahren ferner:

- Empfangen einer Leseanfrage zum Lesen eines der Datensätze der Blockchain durch den ersten Blockchain-Server, wobei die Leseanfrage signiert ist,
- 30

- Prüfen durch den ersten Blockchain-Server unter Verwendung eines zweiten öffentlichen kryptografischen Schlüssels, ob die Signatur der Leseanfrage gültig ist,
 - falls die Signatur der Leseanfrage gültig ist, Senden einer Kopie des ange-
- 5 fragten Datensatzes an einen Absender der Leseanfrage.

Ausführungsformen können den Vorteil haben, dass sie ein effizientes und effektives Verfahren zum Auslesen von Datensätzen aus der Blockchain bereitstellen. Insbesondere kann so ein Verfahren zur Zugriffskontrolle und -beschränkung auf die

10 in der Blockchain manipulationssicher gespeicherten Daten implementiert werden. Beispielsweise umfassen alle Blockchain-Server des Blockchain-Netzwerks eine vollständige Kopie der Blockchain. Um die elektronische Urkunde vorzulegen, die Gültigkeit der Angaben einer körperlichen Version der elektronischen Urkunde nachzuweisen oder die Gültigkeit von Angaben nachzuweisen, welche die elektroni-

15 sche Urkunde beurkundet und auf welchen ein weiteres Dokument beruht, genügt mithin eine Identifikation der entsprechenden elektronischen Urkunde, welche manipulationssicher in der Blockchain gespeichert ist.

Beispielsweise sind alle einer elektronischen Urkunde zugeordneten Einträge in der

20 Blockchain mit einem Identifikator der elektronischen Urkunde versehen. Auf Basis des entsprechenden Identifikators kann über eine Leseanfrage ein Datensatz mit den Daten der in der Blockchain gespeicherten elektronischen Urkunde abgerufen werden. Der entsprechende Identifikator kann beispielsweise in Form eines maschinenlesbaren Codes von der entsprechenden körperlichen Version der elektroni-

25 schen Urkunde oder einem entsprechenden körperlichen Dokument, welches auf der Urkunde beruht, bereitgestellt werden. Alternativerweise kann der entsprechende Identifikator aber auch in anderer Form bereitgestellt werden. So kann er etwa als maschinenlesbarer Code in Unterlagen, wie etwa Bewerbungsunterlagen, angegeben werden oder in einem Speicher eines mobilen tragbaren Kommunikationsge-

30 räts mitgeführt werden. Wird die elektronische Urkunde benötigt, so kann der Identifikator von dem mobilen tragbaren Kommunikationsgerät gesendet, aus dem Speicher des mobilen tragbaren Kommunikationsgeräts ausgelesen oder auf einem Dis-

play des mobilen tragbaren Kommunikationsgeräts angezeigt werden.

Nach Ausführungsformen wird der zweite öffentliche kryptografische Schlüssel zur Prüfung der Signatur der Leseanfrage von der Blockchain zur Verfügung gestellt.

- 5 Ausführungsformen können den Vorteil haben, dass die Blockchain eine eigenständige PKI zum Überprüfen von Leseberechtigungen zum Lesen von Daten aus der Blockchain bereitstellt.

Nach Ausführungsformen umfasst das Verfahren ferner:

- 10
- Empfangen einer Anfrage nach einer Kopie der Blockchain durch den ersten Blockchain-Server, wobei die Anfrage signiert ist,
 - Prüfen durch den ersten Blockchain-Server unter Verwendung eines dritten öffentlichen kryptografischen Schlüssels, ob die Signatur der Anfrage gültig ist,
- 15
- falls die Signatur der Anfrage gültig ist, Senden der Kopie der Blockchain an einen Absender der Anfrage.

Ausführungsformen können den Vorteil haben, dass neben dem Blockchain-Server, welche eine Berechtigung zum Eintragen zusätzlicher Blöcke in die Blockchain be-
20 sitzt, weitere Computersysteme eine vollständige Kopie der Blockchain zu Lesezwecken umfassen können. Nach Ausführungsformen wird der dritte öffentliche kryptografische Schlüssel zur Prüfung der Signatur der Anfrage nach einer Kopie der Blockchain von der Blockchain zur Verfügung gestellt.

- 25 Nach Ausführungsformen umfasst das Verfahren auf eine Änderung der Blockchain hin, ferner ein Senden einer Kopie der geänderten Blockchain an einen registrierten Empfänger durch den ersten Blockchain-Server. Ausführungsformen können den Vorteil haben, dass weitere Computersysteme, bei welchen es sich um keine Blockchain-Server handelt, stets über eine aktuelle Version der Blockchain zu Lesezwe-
30 cken verfügen.

Nach Ausführungsformen ist der registrierten Empfänger in der Blockchain eingetragen. Ausführungsformen können den Vorteil haben, dass beispielsweise von den Blockchain-Servern anhand der Blockchain in effektiver und effizienter Weise festgestellt werden kann, welche zusätzliche Computersysteme mit einer entsprechenden Kopie einer aktualisierten Version der Blockchain zu versehen sind.

Nach Ausführungsformen umfasst das Verfahren ferner:

- Empfangen einer ersten Registrierungsanforderung zum Registrieren eines Empfängers von Kopie der Blockchain im Fall einer Änderung der Blockchain durch den ersten Blockchain-Server, wobei die erste Registrierungsanforderung signiert ist,
- Prüfen durch den ersten Blockchain-Server unter Verwendung eines vierten öffentlichen kryptografischen Schlüssels, ob die Signatur der ersten Registrierungsanforderung gültig ist,
- falls die Signatur der ersten Registrierungsanforderung gültig ist, Registrieren des Empfängers in der Blockchain, wobei das Registrieren ein Hinzufügen der Adresse des zu registrierenden Empfängers zu einem sechsten zusätzlichen Block der Blockchain umfasst.

Ausführungsformen können den Vorteil haben, dass ein effektives und effizientes Verfahren zum Registrieren von Empfängern von Kopie der Blockchain bereitgestellt wird. Nach Ausführungsformen wird der vierte öffentliche kryptografische Schlüssel zur Prüfung der Signatur der ersten Registrierungsanforderung von der Blockchain zur Verfügung gestellt.

Nach Ausführungsformen umfasst das Verfahren ferner:

- Empfangen einer zweiten Registrierungsanforderung zum Eintragen eines von der Blockchain bereitzustellenden öffentlichen kryptografischen Schlüssels durch den ersten Blockchain-Server, wobei die zweite Registrierungsanforderung signiert ist,

- Prüfen durch den ersten Blockchain-Server unter Verwendung eines fünften öffentlichen kryptografischen Schlüssels, ob die Signatur der zweiten Registrierungsanforderung gültig ist,
- falls die Signatur der zweiten Registrierungsanforderung gültig ist, Eintragen
5 des bereitzustellenden öffentlichen kryptografischen Schlüssels in die Blockchain, wobei des bereitzustellenden öffentlichen kryptografischen Schlüssels zu einem siebten zusätzlichen Block der Blockchain umfasst.

Ausführungsformen können den Vorteil haben, dass ein effektives und effizientes
10 Verfahren zum Bereitstellen von öffentlichen Schlüsseln in der Blockchain implementiert wird. Das entsprechende Verfahren kann beispielsweise auf einer hierarchischen Autorisierung beruhen. So können beispielsweise im Zuge des Einbringens der Programmmodule in die Blockchain von den die Programmmodule einbringenden Institutionen ein oder mehrere Root-Instanzen in Form von öffentlichen
15 kryptografischen Schlüsseln in der Blockchain implementiert werden. Registrierungsanforderungen zum Eintragen von weiteren öffentlichen Schlüsseln in die Blockchain können mit einer Signatur, welche unter Verwendung eines privaten Schlüssels eines kryptografischen Schlüsselpaars, von welchem der öffentliche Schlüssel bereits in der Blockchain eingetragen wurde, autorisiert werden. Somit
20 kann die Blockchain eine eigenständige PKI implementieren. Nach Ausführungsformen wird der fünfte öffentliche kryptografische Schlüssel zur Prüfung der Signatur der zweiten Registrierungsanforderung von der Blockchain zur Verfügung gestellt.

25 Nach Ausführungsformen ist jedes der Programmmodule einer Spezifikation zugeordnet, welche genau einer der unterschiedlichen hoheitlichen Institutionen zugeordnet ist. Ausführungsformen können den Vorteil haben, dass für jede hoheitliche Institution ein individuelles Programmmodul von der Blockchain bereitgestellt wird. Handelt es sich bei den hoheitlichen Institutionen beispielsweise um hoheitliche In-
30 stitutionen unterschiedlicher Staaten, so behält jeder Staat die volle Verfügungsgewalt über elektronische Urkunden, welche eine ihm zugeordnete hoheitliche Institution ausstellt. Dies hoheitliche Institution kann beispielsweise weitere öffentliche Be-

hörden, wie etwa Standesämter, dazu autorisieren innerhalb der Grenzen ihrer Amtsbefugnisse entsprechende elektronische Urkunden, etwa Geburtsurkunden, in der vorgeschriebenen Form auszustellen bzw. in die Blockchain einzutragen. Ebenso kann die hoheitliche Institution ein oder mehreren mit öffentlichem Glauben versehenen Person, wie etwa Notaren, Konsuln, Gerichtsvollziehern, etc., dazu autorisieren innerhalb des ihnen zugewiesenen Geschäftskreises entsprechende elektronische Urkunden in der vorgeschriebenen Form ausgestellt auszustellen bzw. in die Blockchain einzutragen.

- 10 Nach Ausführungsformen ist jeder der Blockchain-Server genau einer der unterschiedlichen hoheitlichen Institutionen zugeordnet. Ausführungsformen können den Vorteil haben, dass jeder hoheitlichen Institution ein Blockchain-Server zugeordnet ist. Mit anderen Worten verfügt jede hoheitliche Institution über einen eigenen Blockchain-Server als Teil des Blockchain-Netzwerks zum Eintragen von elektronischen Urkunden. Somit behält beispielsweise im Fall von hoheitlichen Institutionen unterschiedlicher Staaten jeder dieser Staaten die volle Verfügungsgewalt über das Eintragungsverfahren von elektronischen Urkunden seiner hoheitlichen Institution, wobei sich diese physikalische Verfügungsgewalt auch auf die elektronische Implementierung des zugrunde liegenden Hardwaresystems, d.h. das Blockchain-
- 15
- 20 netzwerk.

- Nach Ausführungsformen ist zumindest eines der Programmmodule einer Spezifikation zugeordnet, welche mehr als einer der unterschiedlichen hoheitlichen Institutionen zugeordnet ist. Ausführungsformen können den Vorteil haben, dass mehrere unterschiedliche hoheitliche Institutionen beispielsweise dasselbe Programmmodul nutzen können, um elektronische Urkunden mit derselben Spezifikation manipulations-
- 25
- onssicher auszustellen und in der Blockchain zu speichern.

- Nach Ausführungsformen ist jeder der Blockchain-Server mehr als einer der unterschiedlichen hoheitlichen Institutionen zugeordnet. Ausführungsformen können den Vorteil haben, dass mehrere unterschiedliche hoheitliche Institutionen denselben
- 30

Blockchain-Server zum Eintragen elektronischer Urkunden in die Blockchain nutzen können.

Ausführungsformen umfassen ein Blockchain-Server eines Blockchain-Netzwerks
5 zum manipulationssicheren Ausstellen und Speichern von elektronischen Urkunden
entsprechend einer Spezifikation einer hoheitlichen Institution einer Mehrzahl von
hoheitlichen Institutionen unter Verwendung einer von dem Blockchain-Netzwerk
bereitgestellten Blockchain. Der Blockchain-Server ist der hoheitlichen Institution
zugeordnet. Das Blockchain-Netzwerk umfasst eine Mehrzahl von Blockchain-
10 Servern, welche jeweils einer der hoheitlichen Institutionen zugeordnet sind. Die
Blockchain umfasst eine Mehrzahl von Programmmodulen, wobei die Programm-
module jeweils einer der Spezifikationen zugeordnet sind.

Der Blockchain-Server ist konfiguriert zum:

- 15 • Empfangen eines Datensatzes zum Eintragen in die Blockchain, wobei der
Datensatz Daten einer auszustellenden elektronischen Urkunde entspre-
chend der Spezifikation der hoheitlichen Institution umfasst,
- Ausführen von Programminstruktionen eines Programmmoduls der Mehrzahl
von Programmmodulen, wobei das entsprechende Programmmodul zum
20 Ausstellen von elektronischen Urkunden entsprechend der Spezifikation kon-
figuriert ist, wobei das Ausführen der Programminstruktionen ein Prüfen des
Datensatzes durch den Blockchain-Server umfasst, ob der Datensatz die
Spezifikation erfüllt, falls der Datensatz die Spezifikation erfüllt, ein Hinzufü-
gen des Datensatzes zu einem zusätzlichen Block der Blockchain.

25 Nach Ausführungsformen ist der Blockchain-Server dazu konfiguriert ein oder meh-
rere der zuvor genannten Ausführungsformen des Verfahrens zum manipulationssi-
cheren Ausstellen und Speichern einer Mehrzahl von elektronischen Urkunden un-
ter Verwendung der Blockchain auszuführen.

30 Ausführungsformen umfassen ein Blockchain-Netzwerk zum manipulationssicheren
Ausstellen und Speichern von elektronischen Urkunden unter Verwendung einer

von dem Blockchain-Netzwerk bereitgestellten Blockchain. Die elektronischen Urkunden entsprechen jeweils einer Spezifikation einer vorgegebenen Menge von Spezifikationen, wobei die Spezifikationen der Menge von Spezifikationen unterschiedlichen hoheitlichen Institutionen zugeordnet sind. Das Blockchain-Netzwerk umfasst eine Mehrzahl von Blockchain-Servern, wobei die Blockchain-Server dazu konfiguriert sind, zusätzliche Blöcke für die Blockchain zu erstellen und in die Blockchain einzutragen. Die Blockchain-Server sind unterschiedlichen hoheitlichen Institutionen zugeordnet, wobei die Blockchain eine Mehrzahl von Programmmodulen umfasst. Die Programmmodule sind jeweils einer der Spezifikationen zugeordnet sind zugeordnet.

Das Blockchain-Netzwerk ist konfiguriert zum:

- Empfangen eines Datensatzes zum Eintragen in die Blockchain durch einen Blockchain-Server des Blockchain-Netzwerks, wobei der Datensatz Daten einer auszustellenden elektronischen Urkunde entsprechend einer Spezifikation einer hoheitlichen Institution umfasst, wobei der Blockchain-Server der hoheitlichen Institution zugeordnet ist,
- Ausführen Programminstruktionen eines Programmmoduls der Mehrzahl von Programmmodulen durch den Blockchain-Server, wobei das Programmmodul zum Ausstellen von elektronischen Urkunden entsprechend der Spezifikation konfiguriert ist, wobei das Ausführen der Programminstruktionen ein Prüfen des Datensatzes durch den Blockchain-Server umfasst, ob der Datensatz die Spezifikation erfüllt, falls der Datensatz die Spezifikation erfüllt, ein Hinzufügen des Datensatzes zu einem zusätzlichen Block der Blockchain.

Nach Ausführungsformen ist das Blockchain-Netzwerk dazu konfiguriert ein oder mehrere der zuvor genannten Ausführungsformen des Verfahrens zum manipulationssicheren Ausstellen und Speichern einer Mehrzahl von elektronischen Urkunden unter Verwendung der Blockchain auszuführen.

Die Verwendung von Ordinalzahlen wie erstes, zweites, drittes etc. dient hier, soweit sich aus dem konkreten Zusammenhang nicht eindeutig etwas anderes ergibt, allein der Unterscheidung voneinander verschiedener Elemente und soll keine bestimmte Reihenfolge implizieren.

5

Im Weiteren werden Ausführungsformen der Erfindung mit Bezugnahme auf die Zeichnungen näher erläutert. Es zeigen

- 10 Figuren 1 schematische Blockdiagramme einer ersten Ausführungsform eines exemplarischen Systems zum manipulationssicheren Ausstellen und Speichern von elektronischen Urkunden unter Verwendung einer Blockchain,
- 15 Figur 2 ein schematisches Blockdiagramm einer Ausführungsform einer exemplarischen körperlichen Urkunde,
- 20 Figur 3 ein schematisches Blockdiagramm einer Ausführungsform eines exemplarischen körperlichen ID-Dokuments,
- 25 Figur 4 ein Flussdiagramm einer Ausführungsform eines exemplarischen Verfahrens zum Ausstellen einer elektronischen Urkunde unter Verwendung der Blockchain,
- 30 Figur 5 ein Flussdiagramm einer Ausführungsform eines exemplarischen Verfahrens zum Ergänzen eines elektronischen Dokuments in der Blockchain,
- 30 Figur 6 ein Flussdiagramm einer Ausführungsform eines exemplarischen Verfahrens zum Registrieren eines ID-Dokuments, welches unter Verwendung eines von der Blockchain bereitgestellten elektronischen Urkunde ausgestellt wurde,

Figur 7 ein Flussdiagramm einer Ausführungsform eines exemplarischen Verfahrens zum Auslesen von Datensätzen aus der Blockchain,

Figur 8 ein Flussdiagramm einer Ausführungsform eines exemplarischen Verfahrens zum Registrieren von öffentlichen kryptografischen Schlüsseln in der Blockchain, und

Figur 9 ein Flussdiagramm einer Ausführungsform eines exemplarischen Verfahrens zum Registrieren von Empfängern von Updates der Blockchain.

Elemente der nachfolgenden Ausführungsformen, die einander entsprechen, werden mit denselben Bezugszeichen gekennzeichnet.

Figuren 1A und 1B zeigen eine Ausführungsform eines exemplarischen Systems zum manipulationssicheren Ausstellen und Speichern von elektronischen Urkunden 116 unter Verwendung einer Blockchain 106. Die Blockchain 106 wird von einem Blockchain-Netzwerk 100 bereitgestellt, welches eine Mehrzahl von N Blockchain-Servern 102, 132, 142 umfasst. Die einzelnen Blockchain-Servern 102, 132, 142 des Blockchain-Netzwerks 100 umfassen jeweils einen Speicher 104, 134, 144, in welchem jeweils eine Kopie der Blockchain 106 gespeichert ist. Ferner umfasst die Blockchain 106 eine Mehrzahl von Programmmodulen 108, welche jeweils eine Spezifikation 110 für in der Blockchain 106 zu speichernde elektronische Urkunden 116 bereitstellt. Ferner können die Programmmodule 108 jeweils einen oder mehrere öffentliche kryptografische Schlüssel 112 bereitstellen, anhand derer Registrierungsanfragen zum Registrieren weiterer öffentlicher kryptografischer Schlüssel 114 in der Blockchain 106 auf ihre Berechtigung geprüft werden können. So kann die Blockchain 106 beispielsweise eine eigenständige PKI zum hierarchischen Autorisieren von Ausstellern von elektronischen Urkunden 116 implementieren.

Die Server 102, 132, 142 umfassen ferner jeweils einen Prozessor 126, 136, 146 zum Ausführen von Programminstruktionen, welche von den Programmmodulen 108 der Blockchain 106 bereitgestellt werden. Zudem umfassen die Blockchain-

Server 102, 132, 142 jeweils eine Kommunikationsschnittstelle 128, 138, 148 zum Empfangen von Datensätzen zur Eintragung in der Blockchain 106 über das Netzwerk 160. Nach Ausführungsformen werden Datensätze zum Ausstellen von elektronischen Urkunden 116, welche in die Blockchain 106 eingetragen werden, von
5 den Blockchain-Servern 102, 132, 142 über das Netzwerk 160 von Computersystemen 200, 220, 240 empfangen. Nach alternativen Ausführungsformen werden die entsprechenden Datensätze zum Ausstellen elektronischer Urkunden 116 von den Blockchain-Servern 102, 132, 142 selbst erstellt.

10 Die Blockchain-Server 102, 132, 142 dienen somit sowohl zum Speichern der Blockchain 106 als auch zum Eintragen von elektronischen Urkunden 116 in die Blockchain 106. Ihre jeweilige Berechtigung zum Eintragen eines Blocks in die Blockchain 106 können die Blockchain-Server 102, 132, 142 beispielsweise jeweils durch eine Signatur des von ihnen erstellten zusätzlichen Blocks für die Blockchain
15 106 nachweisen. Hierzu verfügen die einzelnen Blockchain-Server 102, 132, 142 beispielsweise über einen privaten kryptografischen Signaturschlüssel. Die entsprechenden privaten kryptografischen Schlüssel sind beispielsweise jeweils in einem geschützten Speicherbereich der elektronischen Speicher 104, 134, 144 gespeichert. Nach alternativen Ausführungsformen sind die von den Blockchain-Servern
20 102, 132, 142 erzeugten zusätzlichen Blöcke für die Blockchain nicht durch die Blockchain-Server 102, 132, 142 signiert, sondern weisen ihre Korrektheit ausschließlich durch ihre Konformität mit den von den Programmmodulen 108 definierten Spezifikationen 110 nach. Die entsprechenden Spezifikationen 110 umfassen beispielsweise eine Signatur der einzelnen von den Blöcken umfassten Datensätze
25 mit privaten kryptografischen Schlüsseln, welche zu kryptografischen Schlüsselpaaren gehören, deren öffentliche kryptografische Schlüssel 114 in der Blockchain 108 gespeichert sind.

Datensätze 210, 230, 250 zum Eintragen in der Blockchain 106 werden beispielsweise von einem oder mehreren Computersystemen 200, 220, 240 erstellt und über
30 das Netzwerk 160 an das Blockchain-Netzwerk 100 zur Eintragung in der Blockchain 106 gesendet. Nach Ausführungsformen erfolgt das Senden der Datensätze

ze 210, 230, 250 beispielsweise über Kommunikationsverbindungen, welche Ende-zu-Ende verschlüsselt sind. Die Computersysteme 200, 220, 240 umfassen beispielsweise jeweils einen elektronischen Speicher 202, 222, 242, in welchem die einzutragenden Datensätze 210, 230, 250 gespeichert sind. Ferner umfassen die
5 Computersysteme 200, 220, 240 jeweils einen Prozessor 212, 232, 252 zum Ausführen von Programminstruktionen. Ein Ausführen der entsprechenden Programminstruktionen führt beispielsweise zur Erstellung der Datensätze 210, 230, 250. Die entsprechenden Datensätze 210, 230, 250 werden über Kommunikationsschnittstellen 214, 234, 254 der Computersysteme 200, 220, 240 und das Netzwerk
10 160 an das Blockchain-Netzwerk 100 gesendet.

Nach Ausführungsformen umfassen die elektronischen Speicher 202, 222, 242 jeweils geschützte Speicherbereiche 204, 224, 244 mit einem privaten Schlüssel 206, 226, 246. Die privaten kryptografischen Schlüssel 206, 226, 246 sind jeweils dem
15 entsprechenden Computersystem 200, 220, 240 und/oder deren Nutzer zugeordnet, wobei es sich bei dem Nutzer sowohl um eine natürliche Person als auch um eine juristische Person handeln kann. Mit den privaten Schlüsseln 206, 226, 246 können die Datensätze 210, 230, 250 signiert werden. Handelt es sich bei den privaten kryptografischen Schlüsseln 206, 226, 246 um private kryptografische Schlüssel
20 eines asymmetrischen Schlüsselpaars, dessen öffentlicher kryptografischer Schlüssel 114 in der Blockchain 106 registriert ist, so dient die Signatur mit dem entsprechenden privaten Schlüssel 206, 226, 246 als Nachweis einer Autorisierung zum Eintragen des entsprechenden Datensatzes 210, 230, 250 in die Blockchain 106.

25 Ferner können die Computersysteme 200, 220, 240 dazu konfiguriert sein, durch Ausführen von Programminstruktionen unter Verwendung der Prozessoren 212, 222, 252 Leseanfragen 208, 228, 248 zum Auslesen elektronischer Urkunden aus der Blockchain 106 bzw. den elektronischen Urkunden zugeordneter Einträge an das Blockchain-Netzwerk zu senden. Beispielsweise sind die Leseanfragen 208,
30 228, 248 mit den privaten Schlüsseln 206, 226, 246 signiert, um die Leseberechtigung der Computersysteme 200, 220, 240 nachzuweisen. Werden die entsprechenden Leseanfragen 208, 228, 248 von einem Blockchain-Server 102, 132, 142

des Blockchain-Netzwerks 100 über das Netzwerk 160 empfangen, so prüft der entsprechende Blockchain-Server 102, 122, 142 durch Ausführen eines der Programmmodule 108 die Autorisierung der Signatur der entsprechenden Leseanfrage. Ist das anfragende Computersystem 200, 220, 240 zum Lesen der angefragten Datensätze berechtigt, so werden diese von dem entsprechenden Blockchain-Server 102, 132, 142 über das Netzwerk 160 an das anfragende Computersysteme 200, 220, 240 in Antwort auf die Leseanfragen 208, 228, 248 gesendet. Nach Ausführungsformen sind die Programmmodule 108 jeweils selektiv bestimmten Blockchain-Servern 102, 132, 142 zugeordnet, sodass nur ein einem bestimmten Programmmodul 108 zugeordneter Blockchain-Server 102, 132, 142 dieses erfolgreich zum Eintragen von elektronischen Urkunden 116 nutzen kann. Nach Ausführungsformen können elektronische Urkunden 116 mit einer bestimmten Spezifikation 110 nur unter Verwendung des dieser Spezifikation 110 zugeordneten Programmmoduls 108 in die Blockchain 106 eingetragen werden. Nach Ausführungsformen können alle Blockchain-Server 102, 132, 142 und/oder alle dazu berechtigten Computersysteme 200, 220, 240 alle Einträge der Blockchain 106 lesen.

Nach Ausführungsformen werden die auszulesenden Datensätze durch einen Identifikator der auszulesenden elektronischen Urkunde 116 bestimmt. Anhand des entsprechenden Identifikators können all diejenigen Blöcke bzw. Einträge in der Blockchain 106 identifiziert werden, welche der auszulesenden elektronischen Urkunde 116 zugeordnet sind. Beispielsweise bilden diese Einträge zusammen die entsprechende elektronische Urkunde 116.

Bei den Leseanfragen 208, 228, 248 kann es sich beispielsweise auch um Leseanfragen zum Auslesen der vollständigen Blockchain 106 handeln. Nach Ausführungsformen kann es sich bei dem Netzwerk 160 um ein öffentliches Netzwerk oder ein privates, d.h. zugriffsbeschränktes, Netzwerk handeln. Beispielsweise kann es sich bei dem Netzwerk 160 um ein Mobilfunknetzwerk handeln, über welches mit einem mobilen Kommunikationsgerät auf die Blockchain zugegriffen werden kann.

Ferner können über das Netzwerk 160 eine oder mehrere Registrierungscomputer-

systeme 300, 320, 340 mit dem Blockchain-Netzwerk 100 in Kommunikation stehen. Die Registrierungscomputersysteme 300, 320, 340 können beispielsweise jeweils dazu konfiguriert sein, durch Ausführen von Programminstruktionen unter Verwendung der Prozessoren 312, 332, 342 eine Registrierungsanfrage 308, 328, 348 zu erstellen zum Registrieren öffentlicher Schlüssel 114 in der Blockchain 106. Die öffentlichen kryptografischen Schlüssel gehören beispielsweise jeweils mit den privaten kryptografischen Schlüsseln 206, 226, 246 zu gemeinsamen asymmetrischen Schlüsselpaaren. Beispielsweise empfangen die Registrierungscomputersysteme 300, 320, 340 die zu registrierenden öffentlichen Schlüssel 114 von den Computersystemen 200, 220, 240 über das Netzwerk 160. Hierzu werden die entsprechenden Registrierungsanfragen 308, 328, 348 beispielsweise mit privaten kryptografischen Schlüsseln 306, 326, 346, welche in geschützten Speicherbereichen 304, 324, 344 der elektronischen Speicher 302, 322, 342 gespeichert sind, signiert. Handelt es sich bei den entsprechenden privaten kryptografischen Schlüsseln 306, 326, 346 um private kryptografische Schlüssel, die zu kryptografischen Schlüsselpaaren gehören, deren öffentliche kryptografische Schlüssel 112 in der Blockchain 106, insbesondere in den Programmmodulen 108 gespeichert ist, so gilt die signierte Registrierungsanfrage 308, 328, 348 als autorisiert. Auch in dieser Weise kann beispielsweise ein hierarchisches Autorisierungsverfahren unter Verwendung der Blockchain 106 implementiert werden. Nach alternativen Ausführungsformen werden die Funktionen der Registrierungscomputersysteme 300, 320, 340 von den Blockchain-Servern ausgeführt.

Figur 2 zeigt ein schematisches Blockdiagramm einer Ausführungsform einer körperlichen Version 400 einer in der Blockchain manipulationssicher gespeicherten Urkunde, beispielsweise einer Geburtsurkunde. Die entsprechende Urkunde 400 umfasst Daten 404 sowie einen maschinenlesbaren Code 410 mit einem Identifikator der elektronischen Urkunde, welcher dem körperlichen Dokument 400 entspricht. Der maschinenlesbare Code 410 kann mit einer dafür vorgesehenen Erfassungsvorrichtung, z. B. einem Scanner, einer Kamera oder einem Empfänger ausgelesen werden, gelesen werden. Die Daten 404 der Urkunde 400 können mit den in der Blockchain gespeicherten Daten der elektronischen Urkunde verglichen werden,

welche der maschinenlesbare Code 410 identifiziert. Stimmen die Daten 404 der körperlichen Urkunde 400 mit den in der Blockchain manipulationssicher gespeicherten Daten der elektronischen Urkunde überein, ist die körperliche Urkunde 400 gültig.

5

Figur 3 zeigt ein schematisches Blockdiagramm einer Ausführungsform eines exemplarischen ID-Dokuments, welches unter Verwendung von Daten ausgestellt wurde, welche von der in der Blockchain gespeicherten elektronischen Urkunde be-
urkundet werden. Bei dem entsprechend ID-Dokument 404 handelt es sich bei-
spielsweise um einen Ausweis, Reisepass, Kinderpass oder Führerschein. Das ent-
sprechende ID-Dokument 420 umfasst beispielsweise ein Lichtbild 424 des Inha-
bers des ID-Dokuments 420 sowie Daten 422, welche beispielsweise maschinen-
lesbare Form bereitgestellt werden. Ferner umfasst das ID-Dokument 420 bei-
spielsweise einen maschinenlesbaren Code 430, welcher die elektronische Urkunde
in der Blockchain identifiziert unter deren Verwendung das ID-Dokument 420 aus-
gestellt wurde. So kann überprüft werden, ob die Daten 422 mit den von der zu-
grunde liegenden Urkunde, z. B. Geburtsurkunde, zumindest teilweise übereinstim-
men, z. B. Geburtsort, Geburtsdatum, etc.

10

15

20

25

30

Figur 4 zeigt ein Flussdiagramm einer Ausführungsform eines Verfahrens zum Ein-
tragen von Datensätzen in eine Blockchain. Bei den entsprechenden Datensätzen
handelt es sich um Datensätze einer elektronischen Urkunde, welche unter Ver-
wendung der Blockchain manipulationssicher ausgestellt und gespeichert werden
soll. In Block 500 empfängt ein Blockchain-Server des Blockchain-Netzwerks einen
Datensatz zum Eintragen in die Blockchain. Der Datensatz umfasst Daten einer
auszustellenden elektronischen Urkunde entsprechend einer Spezifikation einer
hoheitlichen Institution, welcher der empfangende Blockchain-Server zugeordnet ist.
In der Blockchain 502 prüft der Blockchain-Server, ob der Datensatz der entspre-
chenden Spezifikation entspricht. Hierzu führt der Blockchain-Server Programmin-
struktionen eines Programmmoduls der Blockchain aus, welches zum Ausstellen
von elektronischen Urkunden entsprechend dieser Spezifikation konfiguriert ist. Die
Spezifikation umfasst beispielsweise eine Bedingung, dass der entsprechende Da-

tensatz eine bestimmte kryptografische Sicherung, beispielsweise eine gültige Signatur aufweist, und/oder einen bestimmten Satz an Daten mit festgelegtem Inhalt umfasst. Falls der empfangene Datensatz die Spezifikation erfüllt, erfolgt in Block 504 die Eintragung des Datensatzes in die Blockchain. Mit Eintragung des Datensatzes in die Blockchain gilt die entsprechende elektronische Urkunde als ausgestellt und kann anhand des Eintrags in der Blockchain auf ihre Echtheit geprüft werden.

Figur 5 zeigt ein Flussdiagramm einer Ausführungsform eines exemplarischen Verfahrens zum Ergänzen von elektronischen Urkunden, welche durch die Blockchain bereitgestellt werden. In Block 510 wird ein Ergänzungsdatensatz mit Daten zur Ergänzung elektronischen Urkunde empfangen. Der entsprechende Ergänzungsdatensatz umfasst beispielsweise einen Identifikator eines Datensatzes der ausgestellten elektronischen Urkunde und/oder der elektronischen Urkunde selbst. In Block 512 wird geprüft, ob der empfangene Ergänzungsdatensatz eine von einem Programmmodul der Blockchain festgelegte Spezifikation zur Ergänzung der ausgestellten elektronischen Urkunde erfüllt. Die entsprechende Spezifikation legt beispielsweise eine bestimmte Signatur des Ergänzungsdatensatzes, z. B. mit einem der elektronischen Urkunde zugeordneten privaten kryptografischen Schlüssel oder mit einem privaten kryptografischen Schlüssel eines in der Blockchain registrierten asymmetrischen Schlüsselpaars, und/oder Ergänzungsdaten fest, welche einen festgelegten Inhalt aufweisen. Die entsprechenden Ergänzungsdaten können beispielsweise zusätzliche Daten umfassen, welche der bereits bestehenden elektronischen Urkunde zusätzlich hinzuzufügen sind und/oder Daten, welche bestehende Daten der Urkunde updaten, d.h. ersetzen, sollen. Erfüllt der Ergänzungsdatensatz die entsprechende Spezifikation, so erfolgt in Block 514 eine Eintragung des Ergänzungsdatensatzes in die Blockchain, womit die bestehende elektronische Urkunde um den Ergänzungsdatensatz ergänzt wird.

Figur 6 zeigt ein Flussdiagramm einer Ausführungsform eines exemplarischen Verfahrens zum Registrieren von ID-Dokumenten, welche unter Verwendung von elektronischen Urkunden ausgestellt werden, die in der Blockchain manipulationssicher

gespeichert sind. In Block 520 wird eine ID-Dokumentenregistrierung empfangen. Eine entsprechende Registrierung für ein ID-Dokument wird beispielsweise erstellt, wenn das entsprechende ID-Dokument unter Verwendung einer in der Blockchain gespeicherten Urkunde, z. B. Geburtsurkunde, ausgestellt wird. In Block 522 wird

5 die ID-Dokumentenregistrierung auf ihre Gültigkeit geprüft. Hierzu wird geprüft, ob ein empfangener Datensatz, mit dessen Aufnahme in die Blockchain das entsprechende Dokument registriert wird, die von einem Programmmodul der Blockchain für eine ID-Dokumentenregistrierung festgelegte Voraussetzung erfüllt. Erfüllt der entsprechende Datensatz die festgelegte Voraussetzung, so erfolgt in Block 524 die

10 Eintragung der entsprechenden Registrierung in die Blockchain. Hierbei umfasst der entsprechende Datensatz beispielsweise einen Identifikator des ausgestellten ID-Dokuments sowie einen Identifikator der von der Blockchain bereitgestellten Urkunde, basierend auf der das ID-Dokument ausgestellt wurde. Die entsprechenden Voraussetzungen umfassen beispielsweise eine gültige Signatur, einen Identifikator

15 des ausgestellten ID-Dokuments und/oder einen gültigen Identifikator einer in der Blockchain eingetragenen gültigen Urkunde.

Figur 7 zeigt ein Flussdiagramm einer Ausführungsform eines beispielhaften exemplarischen Verfahrens zum Auslesen von Datensätze, d.h. Dokumenten aus

20 der Blockchain, d.h. von dem entsprechenden Dokument zugeordneten Einträgen in der Blockchain. In Block 530 wird eine entsprechende Leseanfrage empfangen. Die entsprechende Leseanfrage umfasst beispielsweise einen Identifikator des auszulesenden Dokuments. In Block 532 wird geprüft, ob die Leseanfrage Voraussetzungen erfüllt, welche von einem Programmmodul festgelegt werden, welches ein die

25 Leseanfrage empfangender Blockchain-Server ausführt. Die entsprechenden Voraussetzungen umfassen beispielsweise eine gültige Signatur der Leseanfrage sowie einen von der Leseanfrage bereitgestellten gültigen Identifikator einer gültigen von der Blockchain bereitgestellten Urkunde. Ist das Prüfungsergebnis positiv, so wird in Block 534 der angefragte Datensatz in Antwort auf die Leseanfrage an den

30 Sender der Leseanfrage gesendet.

Figur 8 zeigt ein Flussdiagramm einer Ausführungsform eines exemplarischen Ver-

fahrens zum Registrieren von öffentlichen Schlüsseln in der Blockchain. Hierdurch kann eine eigene PKI in der Blockchain hinterlegt werden, d.h. eine hierarchische Autorisierung von Erstellern von Datensätzen zum Eintragen in die Blockchain kann implementiert werden. In Schritt 540 empfängt ein Blockchain-Server des Blockchain-Netzwerks eine Registrierungsanfrage für einen öffentlichen Schlüssel, wobei die Registrierungsanfrage beispielsweise den entsprechenden öffentlichen Schlüssel umfasst. In Block 542 wird die Registrierungsanfrage auf ihre Gültigkeit geprüft. Hierbei führt der empfangene Blockchain-Server beispielsweise ein Programmmodul aus, welches die Blockchain bereitstellt. Eine Gültigkeit der Registrierungsanfrage setzt beispielsweise voraus, dass die Registrierungsanfrage selbst eine gültige Signatur umfasst. Die Gültigkeit der Signatur der Registrierungsanfrage kann beispielsweise mit einem von dem Programmmodul umfassten öffentlichen kryptografischen Schlüssel überprüft werden. Bei dem entsprechenden öffentlichen kryptografischen Schlüssel handelt es sich beispielsweise um den öffentlichen kryptografischen Schlüssel eines asymmetrischen Schlüsselpaars, welches einem Aussteller des Programmmoduls zugeordnet ist und als Root-Instanz dient. Erweist sich die Registrierungsanfrage als gültig, so wird der öffentliche kryptografische Schlüssel in Block 544 in der Blockchain registriert, d.h. in der Blockchain gespeichert. Nach Ausführungsformen wird der öffentliche kryptografische Schlüssel nur als Berechtigungsnachweis für Eintragungen unter Verwendung dieses einen Programmmoduls in der Blockchain gespeichert. In diesem Fall stellt der öffentliche kryptografische Schlüssel keinen gültigen Berechtigungsnachweis für Eintragungen unter Verwendung von anderen Programmmodulen der Blockchain dar.

Figur 9 zeigt ein Flussdiagramm einer Ausführungsform eines exemplarischen Verfahrens zum Registrieren von Empfängern von Updates der Blockchain. Beispielsweise ist die Blockchain nicht nur in den Blockchain-Servern gespeichert, sondern in weiteren Computersystemen, welche durch Updates stets auf dem aktuellen Stand gehalten werden. Mit anderen Worten erfolgt, sobald ein zusätzlicher Block zu der Blockchain hinzugefügt wird, eine Aktualisierung der Blockchain-Kopien, welche in den entsprechenden zusätzlichen Computersystemen gespeichert sind. Hierzu werden nun die zusätzlichen Computersysteme in der Blockchain registriert. In Block

550 empfängt ein Blockchain-Server des Blockchain-Netzwerks eine Registrierungsanfrage zur Registrierung eines Empfängers für Updates. In Block 552 wird die Registrierungsanfrage auf ihre Gültigkeit geprüft. Gültigkeitsvoraussetzung, wie sie von einem von dem Blockchain-Server auf den Empfang der Registrierungsanfrage hin ausgeführten Programmmodul festgelegt werden, ist beispielsweise eine gültige Signatur der Registrierungsanfrage. Die Gültigkeit der Signatur der Registrierungsanfrage kann beispielsweise mit einem öffentlichen kryptografischen Schlüssel, welcher von der Blockchain bereitgestellt wird, geprüft werden. Handelt es sich bei der Signatur um eine gültige Signatur, so erfolgt in Block 554 eine Registrierung des Empfängers für Updates in der Blockchain. Hierzu wird beispielsweise eine Adresse des Empfängers in die Blockchain eingetragen. Im Fall einer Aktualisierung der Blockchain, d.h. eines Hinzufügens eines zusätzlichen Blocks zu der Blockchain im Zuge eines Ausführens eines der Programmmodule, wird automatisch eine Kopie der Blockchain oder des zusätzlichen Blocks an die in der Blockchain eingetragenen Empfänger für solche Aktualisierungen gesendet. Hierzu werden die in der Blockchain registrierten Adressen verwendet.

B e z u g s z e i c h e n l i s t e

5	100	Blockchain-Netzwerk
	102	Blockchain-Server
	104	Speicher
	106	Blockchain
	108	Programmmodul
10	110	Spezifikation
	112	öffentlicher Schlüssel
	114	öffentlicher Schlüssel
	116	elektronische Urkunde
	126	Prozessor
15	128	Kommunikationsschnittstelle
	132	Blockchain-Server
	134	Speicher
	136	Prozessor
	138	Kommunikationsschnittstelle
20	142	Blockchain-Server
	144	Speicher
	146	Prozessor
	148	Kommunikationsschnittstelle
	160	Netzwerk
25	200	Computersystem
	202	Speicher
	204	geschützter Speicherbereich
	206	privater Schlüssel
	208	Leseanfrage
30	210	Datensatz
	212	Prozessor
	214	Kommunikationsschnittstelle
	220	Computersystem

	222	Speicher
	224	geschützter Speicherbereich
	226	privater Schlüssel
	228	Leseanfrage
5	230	Datensatz
	232	Prozessor
	234	Kommunikationsschnittstelle
	240	Computersystem
	242	Speicher
10	244	geschützter Speicherbereich
	246	privater Schlüssel
	248	Leseanfrage
	250	Datensatz
	252	Prozessor
15	254	Kommunikationsschnittstelle
	300	Registrierungscomputersystem
	302	Speicher
	304	geschützter Speicherbereich
	306	privater Schlüssel
20	308	Registrierungsanforderung
	310	öffentlicher Schlüssel
	312	Prozessor
	314	Kommunikationsschnittstelle
	320	Registrierungscomputersystem
25	322	Speicher
	324	geschützter Speicherbereich
	326	privater Schlüssel
	328	Registrierungsanforderung
	330	öffentlicher Schlüssel
30	332	Prozessor
	334	Kommunikationsschnittstelle
	340	Registrierungscomputersystem

	342	Speicher
	344	geschützter Speicherbereich
	346	privater Schlüssel
	348	Registrierungsanforderung
5	350	öffentlicher Schlüssel
	352	Prozessor
	354	Kommunikationsschnittstelle
	400	Geburtsurkunde
	404	Datensatz
10	410	maschinenlesbarer Code
	420	ID-Dokument
	422	Datensatz
	424	Lichtbild
	430	maschinenlesbarer Code
15		

Patentansprüche

1. Computerimplementiertes Verfahren zum manipulationssicheren Ausstellen
5 und Speichern einer Mehrzahl von elektronischen Urkunden (116) unter Verwen-
dung einer Blockchain (106), wobei die elektronischen Urkunden (116) jeweils einer
Spezifikation (110) einer vorgegebenen Mehrzahl von Spezifikationen (110) ent-
sprechen, wobei die Spezifikationen (110) der Mehrzahl von Spezifikationen (110)
10 unterschiedlichen hoheitlichen Institutionen einer Mehrzahl von hoheitlichen Institu-
tionen zugeordnet sind, wobei die Blockchain(106) eine Mehrzahl von Programm-
modulen (108) umfasst, wobei die Programmmodule (108) jeweils einer der Spezifi-
kationen (110) zugeordnet sind, wobei die Blockchain (106) von einem Blockchain-
Netzwerk (100) bereitgestellt wird, welches eine Mehrzahl von Blockchain-Servern
15 (102, 132, 142) umfasst, wobei die Blockchain-Server (102, 132, 142) jeweils dazu
konfiguriert sind, zusätzliche Blöcke für die Blockchain (106) zu erstellen und in die
Blockchain (106) einzutragen, wobei die Blockchain-Server (102, 132, 142) unter-
schiedlichen hoheitlichen Institutionen zugeordnet sind,
wobei das Verfahren umfasst:
- Empfangen eines ersten Datensatzes (210) zum Eintragen in die Blockchain
20 (106) durch einen ersten Blockchain-Server (102) des Blockchain-Netzwerks
(100), wobei der erste Datensatz (210) Daten einer auszustellenden ersten
elektronischen Urkunde (116) entsprechend einer ersten Spezifikation (110)
einer ersten hoheitlichen Institution umfasst, wobei der erste Blockchain-
Server (102) der ersten hoheitlichen Institution zugeordnet ist,
 - Ausführen erster Programminstruktionen eines ersten Programmmoduls
25 (108) der Mehrzahl von Programmmodulen (108) durch den ersten Block-
chain-Server (102), wobei das erste Programmmodul (108) zum Ausstellen
von elektronischen Urkunde (116) entsprechend der ersten Spezifikation
(110) konfiguriert ist, wobei das Ausführen der ersten Programminstruktionen
30 ein Prüfen des ersten Datensatzes (210) durch den ersten Blockchain-Server
(102) umfasst, ob der erste Datensatz (210) die erste Spezifikation (110) er-
füllt, falls der erste Datensatz (210) die erste Spezifikation (110) erfüllt, ein

Hinzufügen des ersten Datensatzes (210) zu einem ersten zusätzlichen Block der Blockchain (106).

2. Computerimplementiertes Verfahren nach Anspruch 1, wobei der erste Datensatz (210) signiert ist, wobei die Signatur des ersten Datensatzes (210) als ein Nachweis einer Berechtigung zum Ausstellen einer elektronischen Urkunde (116) entsprechend der ersten Spezifikation (110) der ersten hoheitlichen Institution dient und der erste Blockchain-Server (102) als eine Voraussetzung für die Eintragung des ersten Datensatzes (210) in die Blockchain (106) unter Verwendung eines ersten öffentlichen kryptografischen Schlüssels (114) prüft, ob die Signatur des ersten Datensatzes (210) gültig ist.
3. Computerimplementiertes Verfahren nach Anspruch 2, wobei die ersten Spezifikation (110) eine gültige Signatur des ersten Datensatzes (210) umfasst und wobei das Ausführen der ersten Programminstruktionen das Prüfen der Signatur des ersten Datensatzes (210) unter Verwendung des ersten öffentlichen kryptografischen Schlüssels (114) umfasst.
4. Computerimplementiertes Verfahren nach einem der Ansprüche 2 bis 3, wobei der erste öffentliche kryptografische Schlüssel (114) zur Prüfung der Signatur des ersten Datensatzes (210) von der Blockchain (106) zur Verfügung gestellt wird.
5. Computerimplementiertes Verfahren nach einem der vorangehenden Ansprüche, wobei der erste Datensatz (210) über eine Ende-zu-Ende-verschlüsselte Kommunikationsverbindung empfangen wird.
6. Computerimplementiertes Verfahren nach einem der vorangehenden Ansprüche, wobei es sich bei den elektronischen Urkunden (116) um Geburtsurkunden handelt.
7. Computerimplementiertes Verfahren nach einem der vorangehenden Ansprüche, wobei das Verfahren ferner umfasst:

- Empfangen eines zweiten Datensatzes (230) zum Eintragen in die Blockchain (106) durch einen zweiten Blockchain-Server (104) des Blockchain-Netzwerks (100), wobei der zweite Datensatz (230) Daten einer auszustellenden zweiten elektronischen Urkunde (116) entsprechend einer zweiten Spezifikation (110) einer zweiten hoheitlichen Institution umfasst, wobei der zweite Blockchain-Server (104) der zweiten hoheitlichen Institution zugeordnet ist,
 - Ausführen zweiter Programminstruktionen eines zweiten Programmmoduls (108) der Mehrzahl von Programmmodulen (108) durch den zweiten Blockchain-Server (104), wobei das zweite Programmmodul (108) zum Ausstellen von elektronischen Urkunden (116) entsprechend der zweiten Spezifikation (110) konfiguriert ist, wobei das Ausführen der zweiten Programminstruktionen ein Prüfen des zweiten Datensatzes (230) durch den zweiten Blockchain-Server (104) umfasst, ob der zweite Datensatz (230) die zweite Spezifikation (110) erfüllt, falls der zweite Datensatz (230) die zweite Spezifikation (110) erfüllt, ein Hinzufügen des zweiten Datensatzes (230) zu einem zweiten zusätzlichen Block der Blockchain (106).
8. Computerimplementiertes Verfahren nach einem der vorangehenden Ansprüche, wobei das Verfahren ferner umfasst:
- Empfangen eines dritten Datensatzes zum Eintragen in die Blockchain (106) durch den ersten Blockchain-Server (102) des Blockchain-Netzwerks (100), wobei der dritte Datensatz Daten zur Ergänzung des ersten Datensatzes (210) der ausgestellten ersten elektronischen Urkunde (116) und einen Identifikator des ersten Datensatzes (210) umfasst,
 - Ausführen der ersten Programminstruktionen durch den ersten Blockchain-Server (102), wobei das Ausführen der ersten Programminstruktionen ein Prüfen des dritten Datensatzes durch den ersten Blockchain-Server (102) umfasst, ob der dritte Datensatz ein oder mehrere von dem ersten Programmmodul (108) festgelegte erste Voraussetzungen erfüllt, falls der dritte Datensatz die ersten Voraussetzungen erfüllt, ein Hinzufügen des dritten Datensatzes zu einem dritten zusätzlichen Block der Blockchain (106).

9. Computerimplementiertes Verfahren nach Anspruch 8, wobei der erste Datensatz (210) einen öffentlichen kryptografischen Schlüssel eines asymmetrischen Schlüsselpaars der ersten elektronischen Urkunde (116) umfasst, wobei der dritte
5 Datensatz mit einem privaten kryptografischen Schlüssel des asymmetrischen Schlüsselpaars der ersten elektronischen Urkunde (116) signiert ist,

wobei eine der ersten Voraussetzungen eine gültige Signatur des dritten Datensatzes mit dem privaten kryptografischen Schlüssel des asymmetrischen Schlüsselpaars der ersten elektronischen Urkunde (116) ist und wobei das Ausfüh-
10 ren der dritten Programminstruktionen das Prüfen der Signatur des dritten Datensatzes unter Verwendung des von dem ersten Datensatz (210) bereitgestellten öffentlichen kryptografischen Schlüssel umfasst.

10. Computerimplementiertes Verfahren nach Anspruch, wobei das Verfahren
15 ferner umfasst:

Ausstellen einer ersten körperlichen Urkunde (400), welche inhaltlich mit der ersten elektronischen Urkunde (116) übereinstimmt, unter Verwendung des ersten Datensatz (210), wobei die erste körperliche Urkunde (400) einen maschinenlesbaren Code (410) umfasst, wobei der maschinenlesbare Code (410) einen Identifikator
20 des ersten Datensatzes (210) und/oder einen Identifikator des dritten Datensatzes umfasst.

11. Computerimplementiertes Verfahren nach einem der vorangehenden Ansprüche wobei das Verfahren ferner umfasst:

- 25 • Empfangen eines vierten Datensatzes zum Eintragen in die Blockchain (106) durch den ersten Blockchain-Server (102) des Blockchain-Netzwerks (100), wobei der vierte Datensatz Daten einer ausgestellten dritten elektronischen Urkunde (116) entsprechend der ersten Spezifikation (110) der ersten hoheitlichen Institution oder entsprechend einer vierten Spezifikation (110) einer
30 vierten von der Mehrzahl von hoheitlichen Institutionen nicht umfassten hoheitlichen Institution umfasst,

- Ausführen vierter Programminstruktionen des ersten Programmmoduls (108) durch den ersten Blockchain-Server (102), wobei das Ausführen der vierten Programminstruktionen ein Prüfen des vierten Datensatzes durch den ersten Blockchain-Server (102) umfasst, ob der vierte Datensatz ein oder mehrere von dem ersten Programmmodul (108) festgelegte zweite Voraussetzungen erfüllt, falls der vierte Datensatz die zweiten Voraussetzungen erfüllt, ein Hinzufügen des vierten Datensatzes zu einem vierten zusätzlichen Block der Blockchain (106).

5
- 10 12. Computerimplementiertes Verfahren nach Anspruch 11, wobei die vierten Programminstruktionen und zweiten Voraussetzungen identisch zu den ersten Programminstruktionen und ersten Spezifikation (110) sind.
- 15 13. Computerimplementiertes Verfahren nach einem der vorangehenden Ansprüche, wobei das Verfahren ferner umfasst:
 - Empfangen eines fünften Datensatzes zum Eintragen in die Blockchain (106) durch den ersten Blockchain-Server (102) des Blockchain-Netzwerks (100), wobei der fünfte Datensatz einen Identifikator eines unter Verwendung des ersten Datensatzes (210) ausgestellten körperlichen ID-Dokuments (420) und den Identifikator des ersten Datensatzes (210) umfasst,

20
 - Ausführen fünfter Programminstruktionen des ersten Programmmoduls (108) durch den ersten Blockchain-Server (102), wobei das Ausführen der fünften Programminstruktionen ein Prüfen des fünften Datensatzes durch den ersten Blockchain-Server (102) umfasst, ob der fünfte Datensatz ein oder mehrere von dem ersten Programmmodul (108) festgelegte dritte Voraussetzungen erfüllt, falls der fünfte Datensatz die dritten Voraussetzungen erfüllt, ein Hinzufügen des fünften Datensatzes zu einem fünften zusätzlichen Block der Blockchain (106).

25
- 30 14. Computerimplementiertes Verfahren nach Anspruch 13, wobei das Verfahren ferner umfasst:

Ausstellen des körperlichen ID-Dokuments (420) unter Verwendung des ersten Datensatzes (210), wobei das ID-Dokument (420) einen maschinenlesbaren Code (430) umfasst, wobei der maschinenlesbare Code (430) zumindest einen der folgenden Identifikatoren umfasst: den Identifikator des ersten Datensatzes (210),
5 den Identifikator des ersten Datensatzes (210) oder einen Identifikator des fünften Datensatzes.

15. Computerimplementiertes Verfahren nach einem der vorangehenden Ansprüche, wobei das Verfahren ferner umfasst:

- 10 • Empfangen einer Leseanfrage (208) zum Lesen eines der Datensätze (210, 230, 250) der Blockchain durch den ersten Blockchain-Server (102), wobei die Leseanfrage (208) signiert ist,
- Prüfen durch den ersten Blockchain-Server (102) unter Verwendung eines zweiten öffentlichen kryptografischen Schlüssels (114), ob die Signatur der
15 Leseanfrage (208) gültig ist,
- falls die Signatur der Leseanfrage (208) gültig ist, Senden einer Kopie des angefragten Datensatzes (210, 230, 250) an einen Absender (200, 220, 240) der Leseanfrage (208).

- 20 16. Computerimplementiertes Verfahren nach Anspruch 15, wobei der zweite öffentliche kryptografische Schlüssel (114) zur Prüfung der Signatur der Leseanfrage (208) von der Blockchain (106) zur Verfügung gestellt wird.

25 17. Computerimplementiertes Verfahren nach einem der vorangehenden Ansprüche, wobei das Verfahren ferner umfasst:

- Empfangen einer Anfrage nach einer Kopie der Blockchain (106) durch den ersten Blockchain-Server (102), wobei die Anfrage signiert ist,
- Prüfen durch den ersten Blockchain-Server (102) unter Verwendung eines dritten öffentlichen kryptografischen Schlüssels (114), ob die Signatur der An-
30 frage gültig ist,
- falls die Signatur der Anfrage gültig ist, Senden der Kopie der Blockchain (106) an einen Absender der Anfrage.

18. Computerimplementiertes Verfahren nach Anspruch 17, wobei der dritte öffentliche kryptografische Schlüssel (114) zur Prüfung der Signatur der Anfrage nach einer Kopie der Blockchain (106) von der Blockchain (106) zur Verfügung gestellt wird.

19. Computerimplementiertes Verfahren nach einem der vorangehenden Ansprüche, wobei das Verfahren auf eine Änderung der Blockchain (106) hin, ferner ein Senden einer Kopie der geänderten Blockchain (106) an einen registrierten Empfänger durch den ersten Blockchain-Server (102) umfasst.

20. Computerimplementiertes Verfahren nach Anspruch 19, wobei der registrierten Empfänger in der Blockchain (106) eingetragen ist.

21. Computerimplementiertes Verfahren nach Anspruch 20, wobei das Verfahren ferner umfasst:

- Empfangen einer ersten Registrierungsanforderung (308, 328, 348) zum Registrieren eines Empfängers von Kopie der Blockchain (106) im Fall einer Änderung der Blockchain (106) durch den ersten Blockchain-Server (102), wobei die erste Registrierungsanforderung (308, 328, 348) signiert ist,
- Prüfen durch den ersten Blockchain-Server (102) unter Verwendung eines vierten öffentlichen kryptografischen Schlüssels (114), ob die Signatur der ersten Registrierungsanforderung (308, 328, 348) gültig ist,
- falls die Signatur der ersten Registrierungsanforderung (308, 328, 348) gültig ist, Registrieren des Empfängers in der Blockchain (106), wobei das Registrieren ein Hinzufügen der Adresse des zu registrierenden Empfängers zu einem sechsten zusätzlichen Block der Blockchain (106) umfasst.

22. Computerimplementiertes Verfahren nach Anspruch 21, wobei der vierte öffentliche kryptografische Schlüssel (114) zur Prüfung der Signatur der ersten Registrierungsanforderung (308, 328, 348) von der Blockchain (106) zur Verfügung gestellt wird.

23. Computerimplementiertes Verfahren nach Anspruch, wobei das Verfahren ferner umfasst:

- Empfangen einer zweiten Registrierungsanforderung (308, 328, 348) zum Eintragen eines von der Blockchain (106) bereitzustellenden öffentlichen kryptografischen Schlüssels (114) durch den ersten Blockchain-Server (102), wobei die zweite Registrierungsanforderung (308, 328, 348) signiert ist,
- Prüfen durch den ersten Blockchain-Server (102) unter Verwendung eines fünften öffentlichen kryptografischen Schlüssels (112), ob die Signatur der zweiten Registrierungsanforderung (308, 328, 348) gültig ist,
- falls die Signatur der zweiten Registrierungsanforderung (308, 328, 348) gültig ist, Eintragen des bereitzustellenden öffentlichen kryptografischen Schlüssels in die Blockchain (106), wobei des bereitzustellenden öffentlichen kryptografischen Schlüssels (114) zu einem siebten zusätzlichen Block der Blockchain (106) umfasst.

24. Computerimplementiertes Verfahren nach Anspruch 23, wobei der fünfte öffentliche kryptografische Schlüssel (112) zur Prüfung der Signatur der zweiten Registrierungsanforderung (308, 328, 348) von der Blockchain (106) zur Verfügung gestellt wird.

25. Computerimplementiertes Verfahren nach einem der vorangehenden Ansprüche, wobei jedes der Programmmodule (108) einer Spezifikation (110) zugeordnet ist, welche genau einer der unterschiedlichen hoheitlichen Institutionen zugeordnet ist.

26. Computerimplementiertes Verfahren nach einem der Ansprüche 1 bis 24, wobei jeder der Blockchain-Server (102, 132, 142) genau einer der unterschiedlichen hoheitlichen Institutionen zugeordnet ist.

27. Computerimplementiertes Verfahren nach einem der vorangehenden Ansprüche, wobei zumindest eines der Programmmodule (108) einer Spezifikation

(110) zugeordnet ist, welche mehr als einer der unterschiedlichen hoheitlichen Institutionen zugeordnet ist.

28. Computerimplementiertes Verfahren nach einem der Ansprüche 1 bis 26, wobei jeder der Blockchain-Server (102, 132, 142) mehr als einer der unterschiedlichen hoheitlichen Institutionen zugeordnet ist.

29. Blockchain-Server (102, 132, 142) eines Blockchain-Netzwerks (100) zum manipulationssicheren Ausstellen und Speichern von elektronischen Urkunden (116) entsprechend einer Spezifikation (110) einer hoheitlichen Institution einer Mehrzahl von hoheitlichen Institutionen unter Verwendung einer von dem Blockchain-Netzwerk (100) bereitgestellten Blockchain (106), wobei der Blockchain-Server (102, 132, 142) der hoheitlichen Institution zugeordnet ist und das Blockchain-Netzwerk (100) eine Mehrzahl von Blockchain-Servern (102, 132, 142) umfasst, welche jeweils einer der hoheitlichen Institutionen zugeordnet sind, wobei die Blockchain (106) eine Mehrzahl von Programmmodulen (108) umfasst, wobei die Programmmodule (108) jeweils einer der Spezifikationen (110) zugeordnet sind, wobei der Blockchain-Server (102, 132, 142) konfiguriert ist zum:

- Empfangen eines Datensatzes (210) zum Eintragen in die Blockchain (106), wobei der Datensatz (210) Daten einer auszustellenden elektronischen Urkunde (116) entsprechend der Spezifikation (110) der hoheitlichen Institution umfasst,
- Ausführen Programminstruktionen eines Programmmoduls (108) der Mehrzahl von Programmmodulen (108), wobei das entsprechende Programmmodul (108) zum Ausstellen von elektronischen Urkunden (116) entsprechend der Spezifikation (110) konfiguriert ist, wobei das Ausführen der Programminstruktionen ein Prüfen des Datensatzes (210) durch den Blockchain-Server (102, 132, 142) umfasst, ob der Datensatz (210) die Spezifikation (110) erfüllt, falls der Datensatz (210) die Spezifikation (110) erfüllt, ein Hinzufügen des Datensatzes (210) zu einem zusätzlichen Block der Blockchain (106).

30. Blockchain-Netzwerk (100) zum manipulationssicheren Ausstellen und Speichern von elektronischen Urkunden (116) unter Verwendung einer von dem Blockchain-Netzwerk (100) bereitgestellten Blockchain (106), wobei die elektronischen Urkunden (116) jeweils einer Spezifikation (110) einer vorgegebenen Menge von Spezifikationen (110) entsprechen, wobei die Spezifikationen (110) der Menge von Spezifikationen (110) unterschiedlichen hoheitlichen Institutionen zugeordnet sind, wobei das Blockchain-Netzwerk (100) eine Mehrzahl von Blockchain-Servern (102, 132, 142) umfasst, wobei die Blockchain-Server (102, 132, 142) dazu konfiguriert sind, zusätzliche Blöcke für die Blockchain (106) zu erstellen und in die Blockchain (106) einzutragen, wobei die Blockchain-Server (102, 132, 142) unterschiedlichen hoheitlichen Institutionen zugeordnet sind, wobei die Blockchain (106) eine Mehrzahl von Programmmodulen (108) umfasst, wobei die Programmmodule (108) jeweils einer der Spezifikationen (110) zugeordnet sind zugeordnet sind, wobei das Blockchain-Netzwerk (100) konfiguriert ist zum:

- Empfangen eines Datensatzes (210) zum Eintragen in die Blockchain (106) durch einen Blockchain-Server (102) des Blockchain-Netzwerks (100), wobei der Datensatz (210) Daten einer auszustellenden elektronischen Urkunde (116) entsprechend einer Spezifikation (110) einer hoheitlichen Institution umfasst, wobei der Blockchain-Server (102) der hoheitlichen Institution zugeordnet ist,
- Ausführen von Programminstruktionen eines Programmmoduls (108) der Mehrzahl von Programmmodulen (108) durch den Blockchain-Server (102), wobei das entsprechende Programmmodul (108) zum Ausstellen von elektronischen Urkunden (116) entsprechend der Spezifikation (110) konfiguriert ist, wobei das Ausführen der Programminstruktionen ein Prüfen des Datensatzes (210) durch den Blockchain-Server (102) umfasst, ob der Datensatz die Spezifikation (110) erfüllt, falls der Datensatz (210) die Spezifikation (110) erfüllt, ein Hinzufügen des Datensatzes (210) zu einem zusätzlichen Block der Blockchain (106).

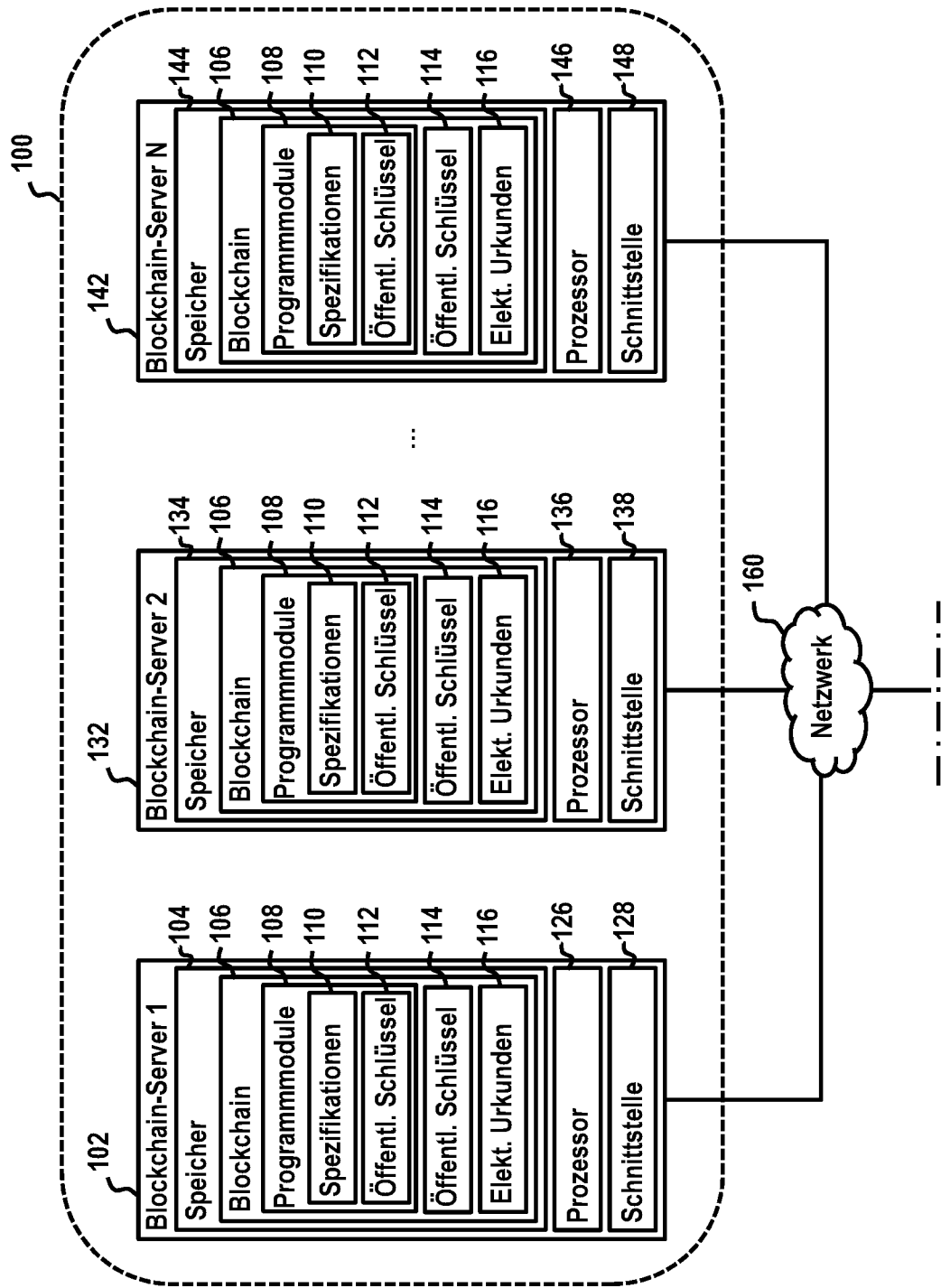


Fig. 1A

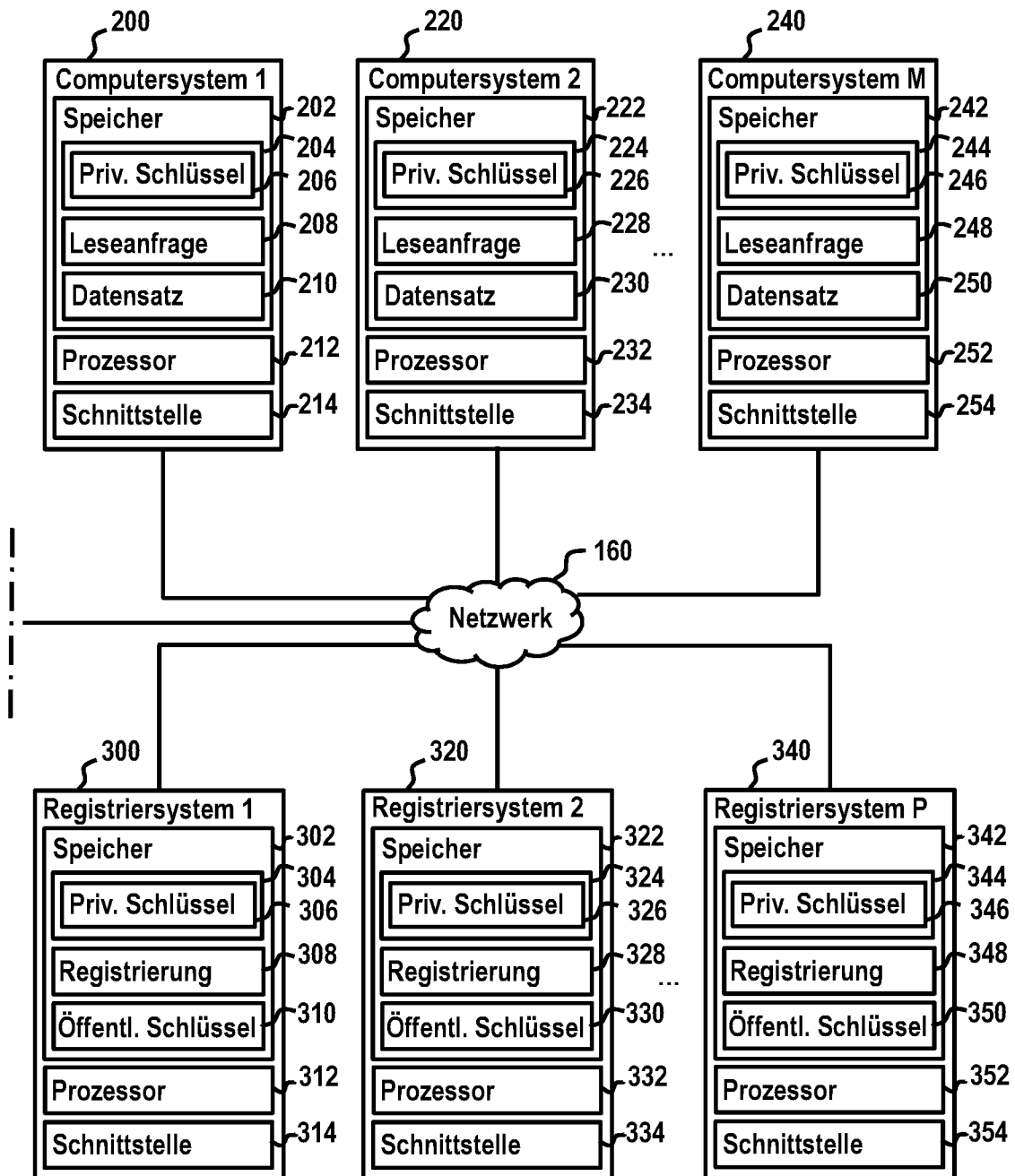


Fig. 1B

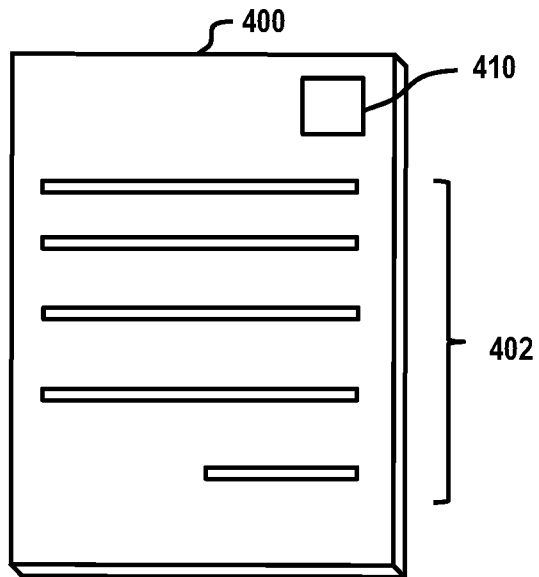


Fig. 2

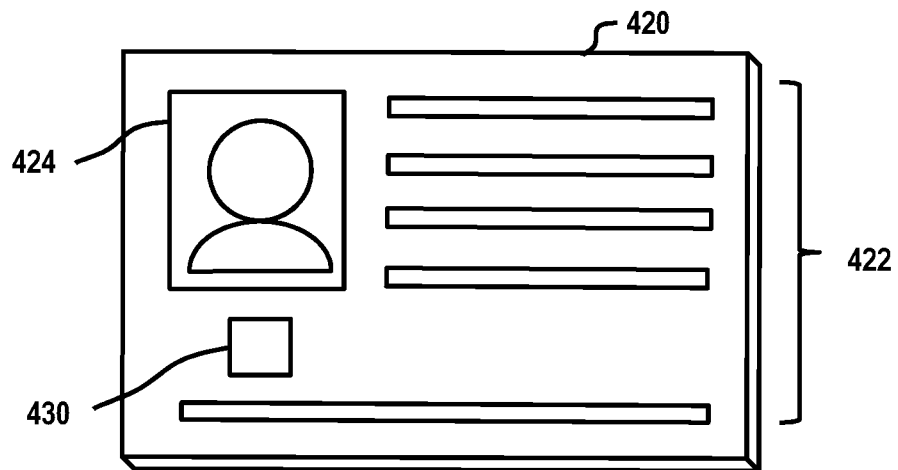


Fig. 3

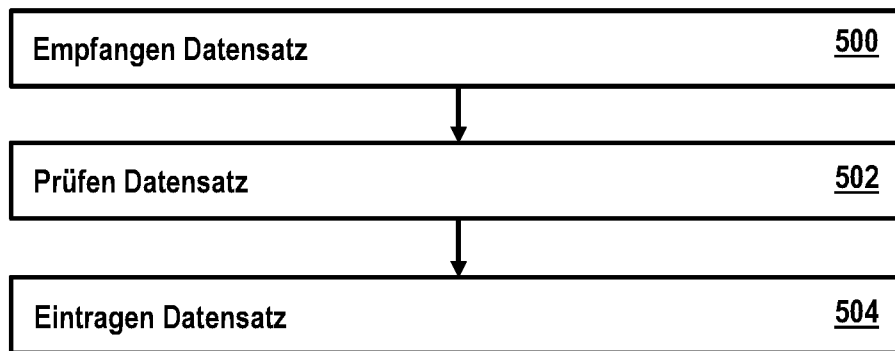


Fig. 4

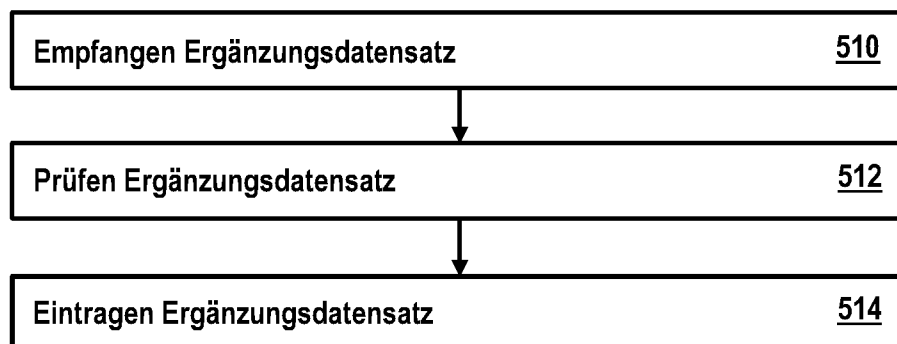


Fig. 5

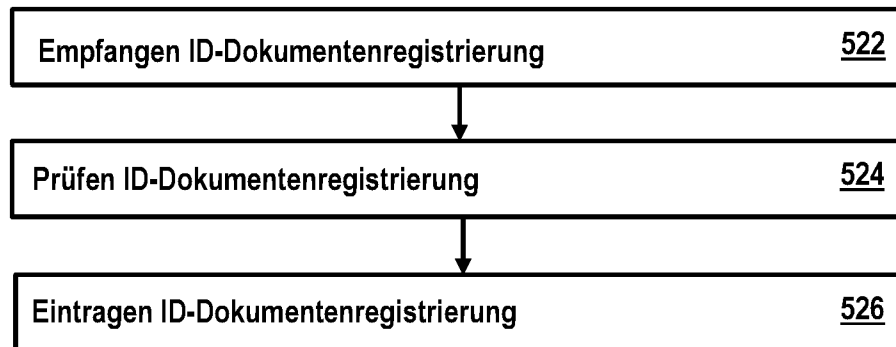


Fig. 6

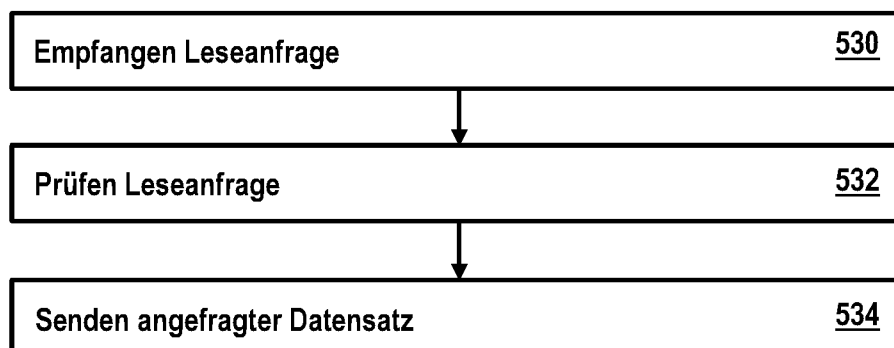


Fig. 7

6/6

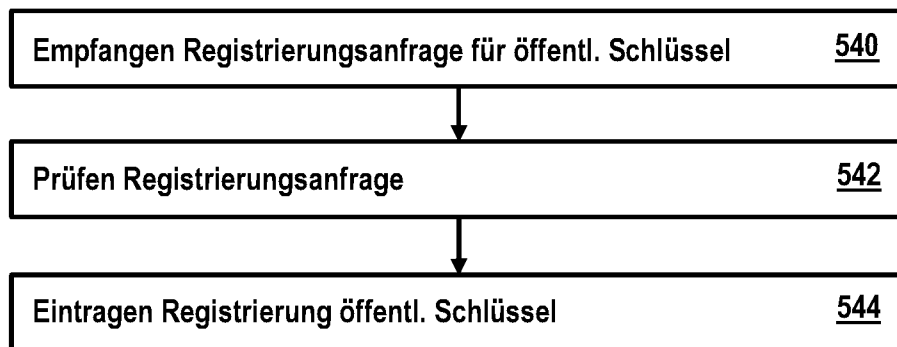


Fig. 8

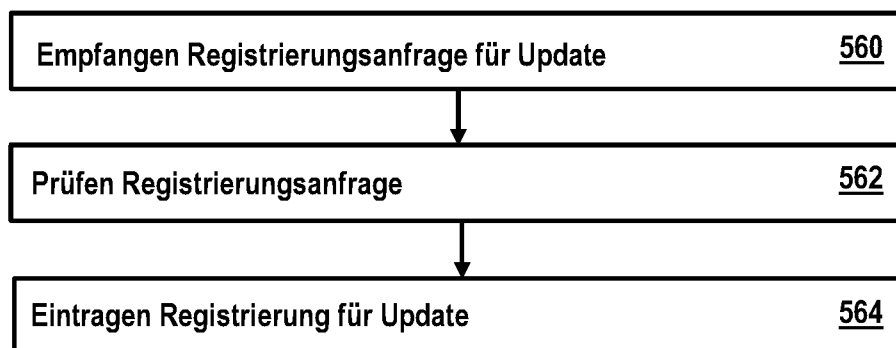


Fig. 9

INTERNATIONAL SEARCH REPORT

International application No.

PCT/EP2019/066852**A. CLASSIFICATION OF SUBJECT MATTER****G06F 21/64**(2013.01)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)

G06F; H04L

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 102017204536 B3 (BUNDESDRUCKEREI GMBH [DE]) 08 March 2018 (2018-03-08) paragraph [0021] - paragraph [0126]; figures 1A-8	1-30
A	EP 3318999 A1 (BUNDESDRUCKEREI GMBH [DE]) 09 May 2018 (2018-05-09) the whole document	1-30

☐ 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

23 September 2019

Date of mailing of the international search report

01 October 2019

Name and mailing address of the ISA/EP

European Patent Office
p.b. 5818, Patentlaan 2, 2280 HV Rijswijk
Netherlands

Telephone No. (+31-70)340-2040

Facsimile No. (+31-70)340-3016

Authorized officer

Savvides, George

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/EP2019/066852

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
DE	102017204536	B3	08 March 2018	DE	102017204536	B3	08 March 2018
				WO	2018167252	A1	20 September 2018
EP	3318999	A1	09 May 2018	DE	102016221699	A1	09 May 2018
				EP	3318999	A1	09 May 2018

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06F21/64
ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G06F H04L

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 204536 B3 (BUNDESDRUCKEREI GMBH [DE]) 8. März 2018 (2018-03-08) Absatz [0021] - Absatz [0126]; Abbildungen 1A-8	1-30
A	----- EP 3 318 999 A1 (BUNDESDRUCKEREI GMBH [DE]) 9. Mai 2018 (2018-05-09) das ganze Dokument -----	1-30



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

23. September 2019

Absendedatum des internationalen Recherchenberichts

01/10/2019

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Savvides, George

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2019/066852

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 102017204536 B3	08-03-2018	DE 102017204536 B3	08-03-2018
		WO 2018167252 A1	20-09-2018

EP 3318999 A1	09-05-2018	DE 102016221699 A1	09-05-2018
		EP 3318999 A1	09-05-2018
