(19) Deutsches Patent- und Markenamt

(10) **DE 20 2018 002 074 U1** 2018.07.19

(12) # Gebrauchsmusterschrift

(21) Aktenzeichen: **20 2018 002 074.5**
(22) Anmeldetag: **24.04.2018**
(47) Eintragungstag: **08.06.2018**
(45) Bekanntmachungstag im Patentblatt: **19.07.2018**

(51) Int Cl.: ***G06F 21/00*** (2013.01)
G06F 21/60 (2013.01)
G06F 21/32 (2013.01)

(30) Unionspriorität:
PCT/US2018/26956 10.04.2018 US

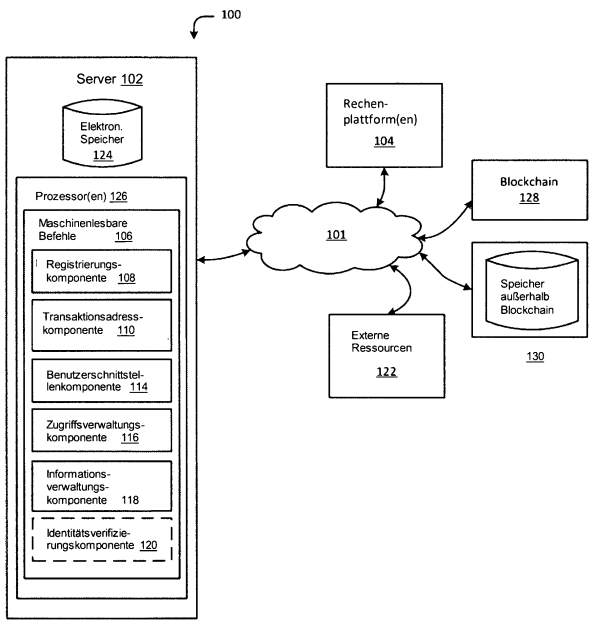
(73) Name und Wohnsitz des Inhabers:
Black Gold Coin, Inc., Las Vegas, Nev., US

(74) Name und Wohnsitz des Vertreters:
Bosch Jehle Patentanwaltsgesellschaft mbH, 80639 München, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **System zur sicheren Speicherung von elektronischem Material**

(57) Hauptanspruch: System zum Bereitstellen einer sicheren Speicherung von elektronischem Material, das aufweist:
einen Hardware-Prozessor (126), der dazu konfiguriert ist, eine Datei mit verständlichen elektronischen Informationen, die zu dem Benutzer gehören, zu empfangen und sicher zu speichern und nach Empfang der Datei mit elektronischen Informationen Fragmente (232, 314, 442) der Datei mit elektronischen Informationen zu bilden, die wenigstens ein erstes Fragment (#1) und ein zweites Fragment (#2) davon aufweisen;
ein verteiltes Datenspeichersystem (234A, 316A, 444A), das mehrere Knoten zum Speichern von Informationsblöcken in einer ersten nicht flüchtigen Speichervorrichtung hat;
eine zweite nicht flüchtige Speichervorrichtung (234B, 316B, 444B), die sich außerhalb des verteilten Datenspeichersystems befindet; und
wobei der Prozessor des Weiteren dazu konfiguriert ist, wenigstens das erste Fragment (#1) der Datei in dem verteilten Datenspeichersystem (234A, 316A, 444A) zu speichern und wenigstens das zweite Fragment (#2) der Datei außerhalb des verteilten Datenspeichersystems (234B, 316B, 444B) zu speichern.



Beschreibung

HINTERGRUND DER ERFINDUNG

Gebiet der Erfindung

[0001] Die vorliegende Offenbarung bezieht sich auf Systeme zur sicheren Speicherung von elektronischem Material.

Beschreibung der verwandten Technik

[0002] Die sichere Speicherung von elektronischem Material in beliebiger Form, beispielsweise Datendateien, Graphikdateien, Bilddateien, Videodateien, biometrischen Dateien, biometrischen Daten und/oder die Speicherung derartiger Informationen in Dateiform oder nicht, ist schon immer ein Thema gewesen. Seit der Einführung des Internets kann potenziell jedermann weltweit unberechtigten Zugriff auf Computersysteme einer Person oder einer Entität erlangen, egal wie sicher sie sind. Zum Beispiel können Benutzernamen und Passwörter gestohlen werden, z.B. durch clevere Phishingmaschen, Onlineviren, Trojaner, Würmer und mehr. Elektronischer Identitätsdiebstahl und andere Cyberkriminalität greifen um sich. Niemand ist immun.

[0003] Es gibt viele herkömmliche Verfahren zur Bekämpfung unberechtigten Zugriffs. Ein Verfahren ist zum Beispiel, Personal auszubilden, so dass es die Maschen erkennt, aber Menschen sind nicht unfehlbar. Der Einsatz von Sicherheitssoftware, wie zum Beispiel Firewalls, Antiviren-Anwendungen, und viele andere Varianten, kann gewissen Schutz liefern. Je mehr Sicherheit besteht, desto mehr kann jedoch die Computerleistung verlangsamt werden, und/oder desto schwieriger wird es, auf das eigene elektronische Material Zugriff zu erhalten.

[0004] Eine andere Sicherheitsebene ist als Zweifaktor- oder Mehrfaktor-Verifizierung bekannt. Mehrfaktor-Verifizierung kombiniert zwei (bei Zweifaktor) oder mehr unabhängige (Benutzer-) Berechtigungsnachweise. Beispielsweise kann es erforderlich sein, dass ein Benutzer ein Passwort eingibt und ein Sicherheits-Token oder Authentifizierungs-Token (eine kleine Hardwarevorrichtung, die der Benutzer mit sich trägt) bereitstellt, um den Zugriff zu autorisieren. Häufig ist ein solches Authentisierungs-Token ein Schlüsselanhänger oder eine Chipkarte. Der Benutzer hat oft eine PIN (persönliche Identifizierungsnummer), die benötigt wird, damit das Authentifizierungs-Token funktioniert, um die Möglichkeit einer Sicherheitsverletzung durch Verlust oder Diebstahl des Authentisierungs-Tokens zu minimieren.

[0005] Weitere Mechanismen für Mehrfaktor-Verifizierung beinhalten das Einloggen in eine Website und das Erhalten eines einmaligen Passworts auf dem Telefon des Benutzers oder an der Emailadresse des Benutzers, das Beantworten einer Sicherheitsfrage, das Herunterladen eines VPN-Clients mit einem gültigen digitalen Zertifikat und das Einloggen in das VPN vor der Zugriffsbewilligung, und biometrisches Scannen, z.B. Fingerabdrücke, Retinascans, Gesichtserkennung, Spracherkennung, und andere biometrische Informationen. Siehe z.B. das US-Patent Nr. 9,838,388 und die veröffentlichte US-Patentanmeldung Nr. 2016/0373440, die beide von Mather sind und sich beide auf biometrische Protokollstandards zur Authentifizierung und sicheren Kommunikation beziehen.

[0006] Bedauerlicherweise kann beim Speichern biometrischer Information die biometrische Information selbst gestohlen werden. Ein Diebstahl biometrischer Information könnte für eine Person ebenso verheerend sein wie, wenn nicht noch verheerender als, der Diebstahl der Sozialversicherungsnummer der Person.

[0007] Traditionelle Sicherheitsverfahren wurden und werden angewendet, um elektronisches Material auf einem sicheren Server zu speichern. Jedoch können auch diese gut geschützten Server Opfer von Cyberangriffen werden.

[0008] Aktuell fehlen Systeme und Verfahren zum Sichern von Informationen, die sich auf eine Person beziehen, auf verschiedene Art. Es besteht ein Bedarf an verbesserten Verfahren zum Sichern von Informationen, die sich auf Dokumente und dergleichen beziehen. Es gibt zum Beispiel einen Bedarf an verbesserten Verfahren, die sich auf biometrische Sicherheit beziehen.

[0009] In den vergangenen Jahren wurde eine Technologie entwickelt, die als „Blockchain“ bzw. „Blockkette“ bekannt ist, um eine Sicherheitsmaßnahme, anfangs für Kryptowährung, bereitzustellen. Blockchain-Speicherung ist eine Art Distributed Ledger bzw. verteiltes Kontobuch und bezieht sich auf eine verteilte Datenspeicherung, bei der Benutzer Informationen auf einer Anzahl von Knoten speichern, oder ein Computernetzwerk, in dem Benutzer Informationen auf einer Anzahl von Peer-Netzwerkknoten speichern. Peer-Netzwerk bedeutet, dass jeder Benutzer oder jedes Mitglied des Datenspeichernetzwerks mit dem verteilten Datenspeicher durch seinen Computer verbunden ist. Jeder Benutzer und sein Computer wird als „Knoten“ bezeichnet. Jeder Knoten speichert dieselben Informationen und trägt zur Validierung und/oder zum Abgleich des verteilten Datenspeichers bei. Die Informationen können nicht verfälscht werden, weil die Theorie von Blockchain/Distributed Ledger ist, dass es so viele Benutzer gibt, dass ein Cyber-Angreifer Daten ändern müsste, die auf einer Mehrzahl der oder allen Knoten gespeichert sind, und dies in kurzer Zeit tun müsste, um das Sys-

tem zu korrumpieren. Der Grund, warum eine Mehrzahl der Knoten geändert werden muss, ist, dass bei der Kryptowährung jeder Knoten dieselben Daten hat, und dass Daten gespeichert werden, wenn unter den Knoten Übereinstimmung herrscht, dass die Daten korrekt sind. Im Fall von Kryptowährung stellen die Blockchain-Daten ein Kontobuch aller digitalen Transaktionen der bestimmten Kryptowährung bereit.

[0010] Wegen der verteilten Beschaffenheit (alle Knoten speichern dieselben Daten) der Blockchain/des Distributed Ledger liefert eine Blockchain/ein Distributed Ledger Sicherheit vor Veränderungen und/oder Korruption solcher Daten. Weil jedoch eine Blockchain/ein Distributed Ledger alle Transaktionen speichert und diese Transaktionen an jeden Knoten (ein Kontobuch) kopiert, ist es für den effizienten Betrieb der Blockchain/des Distributed Ledger sehr wichtig, dass die auf der Blockchain gespeicherte Datenmenge begrenzt ist. Begrenzungen der Blockchain/des Distributed Ledger unterscheiden sich stark von Begrenzungen der sicheren Serverspeicherung.

[0011] Dies bedeutet zum Beispiel, dass jeder Knoten eines bestimmten Typs von Kryptowährung jede Transaktion speichert, die jemals für diesen Typ von Kryptowährung erfolgt ist.

[0012] Blockchain/Distributed Ledger schützt auch die Dateien, sowohl auf den Knoten als auch bei der Übertragung, durch Verwendung von Blockchain-/Distributed Ledger-Technologie und Kryptographie zum Verschlüsseln von Dateien. Die gespeicherten Daten werden typischerweise auch nur gelesen.

[0013] Insbesondere sind alle Benutzer von Blockchain/Distributed Ledger über das Peer-zu-Peer-Netzwerk verbunden. Dieses Netzwerk ist sicherer, bis zu zehn Mal schneller, und fünfzig Prozent kostengünstiger als die traditionellen rechenzentrumbasierten Cloudspeicher-Lösungen. Somit ermöglicht Blockchain/Distributed Ledger, dass die Benutzer Daten sicher und dezentral speichern. Dies erfolgt durch Verwenden von Blockchain-/Distributed Ledger-Merkmalen, wie zum Beispiel Transaktionsbücher, kryptographische Hash-Funktionen und Verschlüsselung mit öffentlichen/privaten Schlüsseln.

[0014] Der dezentrale Aspekt von Blockchain/Distributed Ledger bedeutet, dass es keinen zentralen Server gibt, der gefährdet werden kann, und wegen der Verwendung von Verschlüsselung auf der Client-Seite haben nur die Endbenutzer kompletten Zugriff auf ihre unverschlüsselten Dateien und Verschlüsselungsschlüssel.

[0015] Bei einigen Ausführungsformen speichert die auf Blockchain-Technologie basierende Datenspeicherung nur Hashes ihrer Datenblöcke. Und die verschlüsselten und verteilten Hashes genügen, um die Legitimität oder Authentizität der Datenblöcke zu verifizieren. Blockchain speichert nicht nur Daten in verteilter und verschlüsselter Form, sondern sieht auch eine sequenzielle Kette vor, in der jeder Block einen kryptografischen Hash des Blocks enthält. Dies verbindet die Blöcke und erzeugt dadurch ein dezentrales Transaktionsbuch.

[0016] Für viele Datenexperten ist die größte Chance, die Blockchains/Distributed Ledgers wahrscheinlich mit sich bringen, Disintermediation. Denn eine gut gestaltete und öffentlich/privat zugängliche Blockchain/Distributed Ledger kann viele Funktionen ersetzen, auf die wir aktuell als Intermediäre setzen zum Bereitstellen einer vertrauenswürdigen Handelsumgebung, zum Abschirmen gegen Betrug und Falschbehandlung, zum Garantieren von Vertragseinhaltung, und für Finanztransaktionen.

[0017] Die Kraft von Blockchain/Distributed Ledger liegt nicht nur in der starken Verschlüsselung; die Verteilung über eine Kette von Computern macht es auch schwieriger, Blockchain/Distributed Ledger anzugreifen. Blockchain/Distributed Ledger ist ein selbstverifizierendes Speicherschema, das verwendet werden kann, um Transaktionen, Eigentum oder Identität unveränderlich aufzuzeichnen, Verträge zu verhandeln und durchzusetzen, und vieles mehr.

[0018] Das Problem bei der Verwendung von Blockchain/Distributed Ledger bei der Speicherung ist jedoch, dass, weil Blockchain/Distributed Ledger eine Kopie des Kontobuchs oder der Transaktionen auf allen Knoten speichert, und weil keine früheren Transaktionen gelöscht werden können, der Speicherbedarf schnell unhandlich werden kann. Außerdem wird, um verschiedene Zugriffskontrollen zu schaffen, beispielsweise eine rollenbasierte Zugriffskontrolle bzw. Role-Based Access Control (RBAC), bevorzugt ein zentrales System verwendet. Wenn man jedoch das zentrale System hackt, kann man unberechtigten Zugriff auf die Blockchain erlangen. Wenn auf der Blockchain/dem Distributed Ledger sensible Informationen gespeichert werden, dann muss man bessere Sicherheit vorsehen, weil die Blockchain/der Distributed Ledger nicht ohne weiteres gelöscht werden kann.

[0019] Außer den oben genannten Sicherheitsverfahren gibt es einige Systeme sicherer Speicherung, die Dateien zerlegen und speichern, damit sie bei Bedarf wieder zusammengesetzt werden können, wie zum Beispiel die veröffentlichte US-Patentanmeldung Nr. 2016/0196218 von Kumar, die veröffentlichte US-Patentanmeldung Nr. 2017/0272100 von Yanovsky und das US-Patent Nr. 8,694,467 von Sun.

[0020] Einige haben vorgeschlagen, Blockchain zu verwenden, aber diese Verwendung ist begrenzt

und nicht für Dateispeicherung vorgesehen, wie zum Beispiel Zyskind in „Decentralizing Privacy: Using Blockchain to Protect Personal Data“ [Dezentralisieren des Datenschutzes: Die Verwendung von Blockchain zum Schutz persönlicher Daten] und die WO 2017/145010 von Wright.

[0021] Wegen der oben genannten Begrenzungen für Blockchain/Distributed Ledger und für zentrale Serverspeicherung ist kein System so sicher und funktionell, wie es gewünscht wäre.

[0022] Es gibt Bedarf an einer verbesserten Art und Weise zum sicheren Speichern von elektronischem Material.

ÜBERBLICK

[0023] Einige Implementierungen gemäß der vorliegenden Technologie sind darauf gerichtet, Software zu verwenden, um die Rechnerfunktionalität durch Ansprechen des Sicherheitsthemas zu verbessern. Im Hinblick auf die Sicherheit ist es erwünscht, Informationen sicher speichern zu können, die zu einer Person (einem Benutzer) gehören, und/oder Informationen, die zu einer Entität gehören. Der Benutzer kann im Namen einer Entität handeln, zum Beispiel einem privaten Unternehmen, einer Regierungsbehörde, oder einer anderen Entität.

[0024] Bei einer oder mehreren Ausführungsformen gibt es ein sicheres Speichersystem zum Speichern von elektronischem Material, z.B. digitalen Dateien. In dem System wird eine digitale Datei in Dateifragmente zerlegt, und ein oder mehrere Fragmente werden auf einer Blockchain/einem Distributed Ledger oder auf Blockchains/Distributed Ledgers gespeichert, und die restlichen (ein oder mehr) Fragmente werden außerhalb der Blockchain/des Distributed Ledger gespeichert, z.B. auf einem sicheren Server oder auf sicheren Servern und/oder auf einem Benutzergerät oder Benutzergeräten. Die Dateien, die gespeichert werden, können biometrische oder teilbiometrische Dateien und/oder beliebige Datendateien sein. Die Dateien können verschlüsselt oder gehasht sein. Die Dateifragmente sind bevorzugt unverständlich, außer wenn sie entschlüsselt und vollständig zusammengesetzt sind. Bei einigen oder allen Ausführungsformen kann ein Fragment oder können Fragmente der Datei offline gespeichert werden, z.B. in einem USB-Stick oder Flash-Laufwerk, oder einem anderen digitalen Speichergerät, das normalerweise keinen eigenen Hauptprozessor hat. Bei diesen und/oder allen anderen Ausführungsformen kann ein Dateifragment oder Dateifragmente den gesamten oder nur Abschnitte eines Dateiheaders aufweisen.

[0025] Zum Beispiel wird der Diebstahl oder das Kopieren oder Hacken eines Dateifragments nicht wirksam sein, um verständliche, nützliche Informationen zu stehlen oder zu kopieren.

[0026] Bei einigen Ausführungsformen sind die Vorteile des Speicherns auf Blockchain(s)/Distributed Ledger(s) mit den Vorteilen des Speicherns auf einem sicheren Server oder sicheren Servern (und/oder auf einem Benutzergerät oder Benutzergeräten) oder beides kombiniert.

[0027] Bei einer oder mehreren Ausführungsformen kann eine unverständliche teilbiometrische Datei unabhängig von ihrem Speicherort ausreichende Informationen für Nachweisbarkeit bereitstellen.

[0028] Bei jeder Ausführungsform kann es einen verteilten Datenspeicher geben, der einige oder alle Eigenschaften von Blockchain(s)/Distributed Ledger(s) hat, zum Beispiel einen oder mehrere von unveränderlichem Speicher, Verschlüsselung, Peer-zu-Peer, Dezentralisierung und/oder Übereinstimmung bzw. Konsens. Bei jeder Ausführungsform kann es Varianten des Typs der Blockchain oder des Distributed Ledger geben, wie zum Beispiel ein teilweise dezentrales Kontobuch (z.B. eine Konsortiums-Blockchain).

[0029] Diese und weitere Merkmale und Eigenschaften der vorliegenden Technologie sowie die Betriebsverfahren und die Funktion der verwandten Strukturelemente und die Kombination von Teilen und die Herstellungswirtschaftlichkeit werden bei Betrachtung der folgenden Beschreibung und der beigefügten Ansprüche unter Bezug auf die beigefügten Zeichnungen offensichtlicher. Sie alle bilden einen Teil der vorliegenden Anmeldung, wobei gleiche Bezugszeichen korrespondierende Teile in den verschiedenen Figuren bezeichnen. Es wird jedoch ausdrücklich angemerkt, dass die Zeichnungen nur dem Zweck der Erläuterung und Beschreibung dienen und nicht als Definition der Grenzen der Erfindung beabsichtigt sind. In der Verwendung in der Beschreibung und in den Ansprüchen umfasst die Singularform von „ein“, „eine“ und „der, die das“ auch den Plural, außer der Zusammenhang gibt anderes vor.

Figurenliste

Fig. 1 zeigt ein System zum Bereitstellen eines universellen dezentralen Speichers, der mit einem sicheren Serverspeicher eines elektronischen Materials eines Benutzers verbunden ist, gemäß einer oder mehreren Implementierungen;

Fig. 2 zeigt einen beispielhaften Vorgang zum sicheren Speichern von elektronischem Material;

Fig. 2A zeigt einen beispielhaften Vorgang in einem schematischen Flussdiagramm zum Spei-

chern eines biometrischen Bilds oder einer beliebigen Bilddatei;

Fig. 3 zeigt einen beispielhaften Vorgang zum Aufteilen und Speichern von elektronischem Material, zum Beispiel einer biometrischen Datei und/oder eines beliebigen anderen Dateityps;

Fig. 3A zeigt einen beispielhaften Vorgang in einem schematischen Flussdiagramm zum Speichern eines beliebigen Dateityps, der als Teil der Vorgänge von **Fig. 2A** und **Fig. 4A** verwendet werden kann;

Fig. 4 zeigt einen beispielhaften Vorgang zum Aufteilen und Speichern von elektronischem Material, zum Beispiel einer biometrischen Datei;

Fig. 4A zeigt einen anderen beispielhaften Vorgang in einem schematischen Flussdiagramm zum Speichern eines biometrischen Bilds oder einer beliebigen Bilddatei;

Fig. 5 zeigt ein Verfahren zum Abrufen und Wiederzusammensetzen einer sicher gespeicherten Datei, zum Beispiel einer biometrischen Datei;

Fig. 6 zeigt ein Verfahren zum Abrufen und Wiederzusammensetzten einer sicher gespeicherten Datei, zum Beispiel einer aufgeteilten biometrischen Datei bzw. Split Biometric File (SPBF);

Fig. 7 zeigt einen beispielhaften allgemeinen Wiederzusammensetzungs-Vorgang für eine beliebige Datei;

Fig. 8 zeigt einen beispielhaften Dateilöschvorgang;

Fig. 9 zeigt einen beispielhaften Vorgang für biometrische Authentifizierung unter Verwendung von verschlüsselten SPBF-Dateien;

Fig. 10 zeigt einen beispielhaften Vorgang für biometrische Authentifizierung unter Verwendung gehashter SPBF-Dateien;

Fig. 11 zeigt einen beispielhaften Vorgang für biometrische Authentifizierung unter Verwendung einer SPBF-Datei und eines biometrischen Vektors;

Fig. 12 zeigt einen beispielhaften Vorgang für biometrische Authentifizierung unter Verwendung einer gehashten biometrischen Vektordatei;

Fig. 13 zeigt einen beispielhaften Vorgang zur Registrierung eines Benutzers;

Fig. 14 zeigt einen beispielhaften Vorgang des Anfragens nach Speicherung durch einen Benutzer und des sicheren Speicherns von elektronischem Material;

Fig. 15 zeigt einen beispielhaften Vorgang des Anfragens nach Abrufen eines sicher gespeicherten elektronischen Materials durch einen Benutzer; und

Fig. 16 zeigt einen Überblick über eine beispielhaft angewandte Blockchain oder ein Distributed Ledger.

BESCHREIBUNG DER BEVORZUGTEN AUSFÜHRUNGSFORM(EN)

[0030] **Fig. 1** zeigt ein System **100** zum Bereitstellen einer universellen dezentralen Lösung zur sicheren Speicherung des elektronischen Materials eines Benutzers gemäß einer oder mehrerer Implementierungen. Bei einigen Implementierungen kann das System **100** einen oder mehrere Server **102** aufweisen. Der/die Server **102** kann/können dazu konfiguriert sein, mit einer oder mehreren Rechenplattformen **104** gemäß einer Client-/Server-Architektur, einer Peer-zu-Peer-Architektur und/oder anderen Architekturen, z.B. über die Cloud **101** (z.B. das Internet) zu kommunizieren. Die Benutzer können auf das System **100** über die Rechenplattform(en) **104** zugreifen, die für einen solchen Zugriff eine Anwendungsprogrammierschnittstelle bzw. Application Programming Interface, API, aufweisen können. Der/die Server **102** kann/können dazu konfiguriert sein, maschinenlesbare Befehle **106** auszuführen. Die maschinenlesbaren Befehle **106** können eines oder mehrere der folgenden aufweisen: eine Registrierungskomponente **108**, eine Transaktionsadresskomponente **110**, eine Benutzerschnittstellenkomponente **114**, eine Zugriffsverwaltungskomponente **116** und eine Informationsverwaltungskomponente **118**. Bei einer oder mehreren optionalen Ausführungsformen kann es eine Identitätsverifizierungskomponente **120** geben. Wie für den Durchschnittsfachmann offensichtlich ist, kann es andere maschinenlesbare Befehlskomponenten geben. Die Komponenten können aufgeteilt und/oder kombiniert werden. Die maschinenlesbaren Befehle 106 können ausführbar sein, um Transaktionsadressen für ein Blockchain- oder Distributed Ledger-Netzwerk zu erstellen. Allgemein ausgedrückt ist eine Blockchain oder ein Distributed Ledger eine Transaktionsdatenbank, die sich einige oder alle Knoten, die an dem System **100** beteiligt sind, teilen. Es kann zum Beispiel wenigstens einhundert, eintausend, zehntausend, einhunderttausend oder eine Million Knoten oder mehr geben. Eine solche Beteiligung kann auf dem Bitcoin Protokoll, dem Ethereum Protokoll, dem Ripple Consensus Network (Ripple Transaction Protocol oder RTXP), Hyperledger von Linux, R3's Corda, Symbiont Distributed Ledger (Assembly) und/oder anderen Protokollen basieren, die sich auf digitale Währungen, Distributed Ledgers und/oder Blockchains beziehen. Eine vollständige Kopie der Blockchain oder des Distributed Ledger enthält jede Transaktion, die jemals in einer zugehörigen digitalen Währung oder einer anderen Transaktionsart, zum Beispiel Smart Contract, durchgeführt worden ist. Zusätzlich zu den Transaktionen können andere Infor-

mationen in der Blockchain enthalten sein, wie zum Beispiel vorliegend weiter beschrieben ist.

[0031] Wo der Begriff „Blockchain“ vorliegend verwendet wird, würde eine alternative Ausführungsform oder alternative Ausführungsformen „Distributed Ledger“ verwenden. Transaktionen können unabhängig vom Typ in einem verteilten Netzwerk oder einem Netzwerkdatenspeicher gespeichert werden, einschließlich eines verteilten Speichers, eines Distributed Ledger, einer Blockchain oder eines anderen geeigneten verteilten oder netzwerkbasierten Transaktionsmechanismus. Ein verteilter Speicher (oder „verteilter Datenspeicher“) kann Dateien oder Dateisegmente enthalten, die auf einem oder mehreren Netzwerkknoten gespeichert sind oder als Datenstrom in einem Netzwerkdatenspeicher gespeichert sind. Der verteilte Speicher ist nicht auf ein spezifisches Format oder Protokoll beschränkt, sondern kann Dateien jedes Typs enthalten, die auf einem beliebigen zugreifbaren Netzwerkknoten gespeichert sind, zum Beispiel Servern, Desktops, mobilen Geräten, Wechselspeichern oder anderen geeigneten Vorrichtungen. Bei einer Ausführungsform kann eine Datei vollständig auf einem einzigen Knoten gespeichert werden und eine andere Datei in einem anderen Netzwerkknoten gespeichert werden. Alternativ kann eine einzelne Datei in eine Vielzahl von Segmenten aufgeteilt und auf einem oder mehreren Netzwerkknoten gespeichert werden. Bei einer Ausführungsform kann eine Datei vollständig in einem einzigen Netzwerkdatenspeicher gespeichert werden und eine andere Datei kann in einem anderen Netzwerkdatenspeicher gespeichert werden. Alternativ kann eine einzelne Datei in eine Vielzahl von Segmenten aufgeteilt und auf einem oder mehreren Netzwerkdatenspeichern gespeichert werden. Einige Transaktionsnetzwerke sind dazu ausgelegt, ein dezentrales Zahlungssystem, ein teildezentrales Zahlungssystem oder ein zentrales Zahlungssystem zu sein.

[0032] Bei einer Ausführungsform kann ein Distributed Ledger eine Datenbank oder Repliken einer Datenbank sein, die gemeinsam verwendet werden und über ein verteiltes Netzwerk oder verteilte Netzwerke synchronisiert werden. Alternativ kann ein Distributed Ledger ein Datenstrom sein, der in einem Netzwerkdatenspeicher fließt. Der Distributed Ledger ermöglicht, dass Transaktionen öffentlich oder privat sichtbar sind und repliziert werden, wodurch ein Cyberangriff erschwert wird. Der Distributed Ledger kann auch eine Übereinkunft bzw. einen Konsens über die Existenz und den Status gemeinsamer Sachverhalte in nicht vertrauenswürdigen Umgebungen speichern (d.h., wenn die Teilnehmer, die die gemeinsame Datenbank betreiben, unabhängige Akteure sind, die einander nicht trauen). Konsens kann ein Erfordernis für das Speichern der Daten sein. Konsens ist kein einzigartiges Merkmal des Distributed Ledger per se: andere verteilte Datenbanken verwenden ebenfalls Konsensalgorithmen, wie zum Beispiel Paxos oder Raft. Dasselbe gilt für Unveränderlichkeit: unveränderliche Datenbanken existieren außerhalb von DL (Google HDFS, Zebra, CouchDB, Datomic, etc.).

[0033] Der Distributed Ledger kann sich von einer allgemeinen verteilten Datenbank wie folgt unterscheiden: (a) die Steuerung des Lese-/Schreib-Zugriffs ist echt dezentral oder teildezentral und nicht logisch zentral wie für andere verteilte Datenbanken, und als Folge; und (b) es gibt die Möglichkeit für sichere Transaktionen in Wettbewerbsumgebungen ohne vertrauenswürdige Dritte. Distributed Ledger-Strukturen können linear sein, wie zum Beispiel Blockchain, oder gerichtete azyklische Graphe bzw. Directed Acyclic Graphs (DAG) aufweisen, wie zum Beispiel Iota Tangle. Blockchain Iota Tangle und Hedera Hashgraph sind spezifische Fälle eines Distributed Ledger, die vorgegebene Formate und Zugriffsprotokolle haben.

[0034] Blockchain ist ein Distributed Ledger, der Transaktionen chronologisch speichert. Bei einem Blockchain Ledger werden alle Transaktionen periodisch verifiziert und in einem „Block“ gespeichert, der über einen kryptographischen Hash mit dem vorhergehenden Block verbunden ist. Der Blockchain Ledger ist öffentlich sichtbar und ermöglicht es der allgemeinen Öffentlichkeit, die Transaktionen zu sehen und zu verfolgen. Jeder Netzwerkknoten kann eine Kopie der Blockchain empfangen und speichern.

[0035] Zusätzlich zu dem oben Erwähnten kann der vorliegende Speicher ein Netzwerkdatenspeicher sein, der sich auf Daten bezieht, die in einem Netzwerk gespeichert werden, wobei solche Daten in dem Netzwerk gespeichert werden, jedoch nicht in den Knoten eines Netzwerks.

[0036] Bei einigen Ausführungsformen kann der Speicher ein typischer digitaler Speicher sein, oder er kann in einem Quantendatenspeicher oder einem Quantenspeichernetzwerk (z.B. cloudbasiert) vorliegen. Beim Quantenspeicher werden die Informationen als Energie in einem Partikel oder in Partikeln gespeichert und zum Beispiel durch Kollisionen von Partikeln, wie zum Beispiel Photonen, übertragen. Da diese Partikel ihre Energie übertragen, während die Informationen übertragen werden, werden die Informationen aus den Trägerpartikeln bei jeder Kollision mit einem neuen Partikel gelöscht.

[0037] Die Registrierungskomponente **108** kann dazu konfiguriert sein, einen individuellen Benutzer (eine Person oder eine Entität) zu registrieren (und zu ihrer Identifizierung beizutragen).

[0038] Das System kann von einer Entität, an einer vertrauenswürdigen Blockchain Utility bzw. Blockchain-Dienstprogramm, Informationen empfangen,

die sich auf ein oder mehrere verifizierte Dokumente beziehen. Das eine oder die mehreren verifizierten Dokumente können mit einem solchen Benutzer (z.B. einer Person) assoziiert werden und können Identifizierungsdokumente sein, d.h. Dokumente, die die Identität des Benutzers bestätigen. Die Entität kann eines oder mehrere einer Institution, eines Geschäfts, einer Firma, einer Regierungsbehörde und/oder andere Entitäten aufweisen.

[0039] Die Blockchain kann auf mehreren Blöcken basieren. Ein Block kann einen Eintrag aufweisen, der eine oder mehrere wartende Transaktionen enthält und bestätigt. Periodisch (je nach Art von Transaktion und Menge von Benutzern in der Kette) kann ein neuer Block, der Transaktionen und/oder andere Informationen aufweist, an die Blockchain angehängt werden. Bei einigen Implementierungen enthält ein gegebener Block in der Blockchain einen Hash des vorhergehenden Blocks. Dies kann bewirken, dass eine Kette von Blöcken von einem Ursprungsblock (d.h. dem ersten Block in der Blockchain) bis zu einem aktuellen Block erzeugt wird. Es kann garantiert werden, dass der gegebene Block chronologisch auf einen vorhergehenden Block folgt, weil der gegebene Block den Hash des vorhergehenden Blocks enthält. Der gegebene Block kann wegen der Eigenschaften der Hash-Funktionen rechnerisch unpraktisch zu modifizieren sein, sobald er in der Blockchain enthalten ist. Außerdem wird in der Blockchain eine Kopie jeder Transaktion auf allen oder zumindest mehreren Knoten (z.B. allen Computern, die zu der bestimmten Blockchain-Gesamtheit gehören) gespeichert. Daher müsste jeder entsprechende Block auf allen Knoten in dem Blockchain-Netzwerk (oder zumindest eine Mehrheit) ebenso geändert werden, sonst könnte jeder, der das Netzwerk überwacht, die Unstimmigkeit entdecken. Andere Mitglieder des Netzwerks von Knoten, die die Blockchain unterstützen, können die Inhalte der Blöcke sehen.

[0040] Die Transaktionsadresskomponente **110** kann einem individuellen Benutzer oder Benutzern des Systems eine Transaktionsadresse oder -adressen zuteilen, wie nachstehend im Einzelnen erläutert werden wird. Eine solche Transaktionsadresse kann in der Blockchain ein notwendiges Erfordernis sein, um auf die Informationen in einem bestimmten Block zuzugreifen, der zu der Transaktionsadresse gehört, zusätzlich zu einem zugehörigen öffentlichen und privaten Schlüssel oder einer anderen Authentifizierungs- und Zugriffskontrolle.

[0041] Die Benutzerschnittstellenkomponente **114** kann eine Benutzerschnittstelle bereitstellen.

[0042] Das System **100** kann zum Beispiel über die Registrierungskomponente **108** dazu konfiguriert sein, einen Benutzer zu registrieren. Der Registrierungsvorgang kann ein typischer Registrierungsvorgang sein, wie er in **Fig. 13** gezeigt ist. Beispielsweise kann bei Schritt **1302** das System über die System-API in der Benutzerschnittstellenkomponente **114** eine Benutzeranfrage zum Registrieren empfangen. Bei Schritt **1304** kann das System die Identitätsdaten des Benutzers empfangen, z.B. Name, Adresse und Emailadresse. Bei einer bevorzugten Ausführungsform, die hier an anderer Stelle erläutert wird, können die Identitätsdaten auch urkundliche Belege aufweisen, die zum Verifizieren der Identität des Benutzers ausreichend sind. Bei Schritt **1306** kann das System dem Benutzer einzigartige Kennung(en) zuteilen, zum Beispiel einen einzigartigen Berechtigungsnachweis oder -nachweise, die eines oder mehr sein können von beispielsweise einem Benutzernamen, einem Passwort oder einem Benutzernamen und einem Passwort gekoppelt, einer Nummer, eines alphanumerischen Codes und/oder anderer Berechtigungsnachweis(e) und/oder andere Informationen, die mit einer Person verbunden werden können. Bei Schritt **1308** kann das System optional biometrische Informationen von dem Benutzer erhalten, um ein relativ hohes Sicherheitsniveau zur Benutzerauthentifizierung bereitzustellen.

[0043] Gemäß einigen Implementierungen kann eine Person, die eine früher verifizierte persönliche Identität hat, die früher verifizierte persönliche Identität durch eine Vielzahl von Herangehensweisen erhalten haben. Bei einigen Implementierungen kann es zum Beispiel nötig sein, dass die Person einen Nachweis über die Identität der Person liefert. Ein solcher Nachweis (die oben genannten Informationen) kann eines oder mehrere beinhalten von Bereitstellen einer amtlich ausgestellten Identifikation (z.B. Pass und/oder Führerschein), Bereitstellen einer Kopie eines Poststücks, das von der Person empfangen wurde (z.B. eine Rechnung eines Versorgungsunternehmens), Nachweis, der durch einen Dritten bereitgestellt wird, und/oder anderer Nachweis der Identität einer Person. Der Nachweis kann an eine Entität erbracht werden, die zu dem/den Server(n) 102 gehört.

[0044] Bei einigen Implementierungen können die Informationen, die sich auf das eine oder die mehreren verifizierten Dokumente beziehen, die zu dem Benutzer gehören, mit einem ersten Schlüssel und einem zweiten Schlüssel verschlüsselt werden. Der erste Schlüssel kann ein Server-Schlüssel (z.B. ein privater Schlüssel) sein, der auf einem Backend-Server gespeichert ist. Der zweite Schlüssel kann ein Client-Schlüssel sein, der ein Hash biometrischer Daten ist, die zu dem ersten Benutzer gehören. Bei einigen Implementierungen können die ersten und zweiten Schlüssel zur Über-Verschlüsselung sensitiver Datenformate und/oder zugehöriger Dokumentation für die unveränderliche Blockchain-ID angewendet werden. Die Identitätsverifizierung ist optional und kann als Teil des Registrierungsvorgangs stattfinden.

[0045] Das System **100** kann dazu konfiguriert sein, unter Verwendung der Transaktionsadresskomponente **110** den registrierten Personen Transaktionsadressen auf einer Blockchain zuzuteilen. Eine gegebene Transaktionsadresse kann mit einem öffentlichen Schlüssel und einem privaten Schlüssel assoziiert sein (wie es zum Beispiel bei auf Blockchain basierender Kryptowährung typisch ist). Beispielsweise kann eine erste Transaktionsadresse der Person zugeteilt werden. Die erste Transaktionsadresse kann einen ersten öffentlichen Schlüssel und einen ersten privaten Schlüssel aufweisen.

[0046] Allgemein ausgedrückt kann ein öffentliches und privates Schlüsselpaar für die Verschlüsselung und Entschlüsselung gemäß einem oder mehreren öffentlichen Schlüsselalgorithmen verwendet werden. Beispielsweise, jedoch nicht einschränkend, kann ein Schlüsselpaar für digitale Signaturen verwendet werden. Ein solches Schlüsselpaar kann einen privaten Schlüssel zum Signieren und einen öffentlichen Schlüssel zum Verifizieren einer digitalen Signatur aufweisen. Der öffentliche Schlüssel kann weit verbreitet sein, während der private Schlüssel geheim gehalten wird (z.B. nur dem Eigentümer bekannt ist). Die Schlüssel können mathematisch in Beziehung stehen, jedoch ist das Berechnen des privaten Schlüssels aus dem öffentlichen Schlüssel nicht möglich.

[0047] Bei einigen Implementierungen kann das System **100** so konfiguriert sein, dass private Schlüssel in Rechenplattform(en) **104** gespeichert werden können. Beispielsweise kann der erste private Schlüssel in einer Rechenplattform **104** und/oder an anderen Orten, die zu der Person gehören, gespeichert werden. Gemäß einigen Implementierungen kann ein privater Schlüssel in einer oder mehreren einer „verify.dat“ bzw. „verifiziere.Daten“ -Datei, einer SIM-Karte und/oder an anderen Orten gespeichert werden.

[0048] Bei einigen Implementierungen kann das System **100** so konfiguriert sein, dass einzelnen Personen mehrere Transaktionsadressen zugeteilt werden können. Beispielsweise kann zusätzlich zu der ersten Transaktionsadresse einer ersten Person eine zweite Transaktionsadresse zugeteilt werden. Gemäß einer oder mehreren Implementierungen kann der ersten Person eine oder mehrere zusätzliche Transaktionsadressen zugeteilt werden. Eine zweite Person, die sich bei dem System registriert, kann eine dritte Transaktionsadresse erhalten, etc.

[0049] Das System **100** kann dazu konfiguriert sein, Kennungen und biometrische Daten, die zu den Personen gehören, an korrespondierenden Transaktionsadressen einzutragen. Beispielsweise können die erste Kennung und die ersten biometrischen Daten, die zu der ersten Person gehören, an der ersten Transaktionsadresse eingetragen werden. Das Eintragen von Informationen an einer gegebenen Transaktionsadresse kann das Eintragen eines Hashs oder einer anderen verschlüsselten Darstellung der Informationen umfassen. Bei einigen Implementierungen können verschiedene biometrische Daten an mehreren Transaktionsadressen eingetragen werden, die einer einzigen gegebenen Person zugeteilt sind. Beispielsweise können zusätzlich zu der ersten Kennung und den ersten biometrischen Daten, die der ersten Person (dem ersten Benutzer) gehören, und die an der ersten Transaktionsadresse eingetragen werden, die erste Kennung und zweite biometrische Daten, die zu der ersten Person gehören, an einer zweiten Transaktionsadresse eingetragen werden.

[0050] Allgemein ausgedrückt können biometrische Daten Metrik enthalten, die sich auf menschliche Eigenschaften beziehen. Biometrische Kennungen sind unterscheidende, messbare Eigenschaften, die verwendet werden können, um Personen zu kennzeichnen und zu beschreiben. Biometrische Kennungen weisen typischerweise physiologische Eigenschaften auf, können jedoch auch Verhaltenseigenschaften und/oder andere Eigenschaften aufweisen. Physiologische Eigenschaften können sich auf die Körperform einer Person beziehen. Beispiele für physiologische Eigenschaften, die als biometrische Daten verwendet werden, können eines oder mehrere aufweisen von Fingerabdruck, Handvenen, Gesichtserkennung, Genominformationen, DNA-Sequenz(en) und DNA-Modifizierung(en), proteomischen Informationen und Proteinsequenz(en) und Proteinmodifizierung(en), Handflächendruck, Handgeometrie, Iriserkennung, Retina, Geruch oder Duft und/oder andere physiologische Eigenschaften. Verhaltenseigenschaften können sich auf ein Verhaltensmuster einer Person beziehen. Beispiele für Verhaltenseigenschaften, die als biometrische Daten verwendet werden, können eines oder mehrere aufweisen von Schreibrhythmus, Gangart, Stimme, Herzfrequenz und/oder andere Verhaltenseigenschaften.

[0051] Die biometrischen Daten können eines oder mehrere aufweisen von einem Bild oder einer anderen visuellen Darstellung einer physiologischen Eigenschaft, einer Aufzeichnung einer Verhaltenseigenschaft, eines Musters einer physiologischen Eigenschaft und/oder Verhaltenseigenschaft und/oder andere biometrische Daten. Ein Muster kann eine Synthese relevanter Merkmale aufweisen, die aus der Quelle extrahiert wurden. Ein Muster kann eines oder mehrere aufweisen von einem Vektor, der Merkmale einer physiologischen Eigenschaft und/oder Verhaltenseigenschaft beschreibt, einer numerischen Darstellung einer physiologischen Eigenschaft und/oder Verhaltenseigenschaft, eines Bilds mit bestimmten Eigenschaften und/oder andere Informationen.

[0052] Biometrische Daten können über Rechenplattformen **104** empfangen werden, die zu den Personen gehören. Zum Beispiel können biometrische Daten, die zu einer ersten Person gehören, über eine erste Rechenplattform **104** empfangen werden, die zu der ersten Person gehört. Die erste Rechenplattform **104** kann eine (nicht gezeigte) Eingangsvorrichtung aufweisen, die dazu konfiguriert ist, eine physiologische Eigenschaft und/oder Verhaltenseigenschaft der ersten Person zu erfassen und/oder aufzuzeichnen. Beispiele für eine solche Eingangsvorrichtung können eines oder mehrere aufweisen von einer Kamera und/oder einer anderen Abbildungsvorrichtung, einem Fingerabdruck-Scanner, einem Mikrofon, einem Beschleunigungsmesser und/oder anderen Eingangsvorrichtungen.

[0053] Das System **100** kann dazu konfiguriert sein, eine Schnittstelle zur Darstellung an Personen über zugehörige Rechenplattformen bereitzustellen. Die Schnittstelle kann eine grafische Benutzerschnittstelle über die Benutzerschnittstellenkomponente **114** aufweisen, die über individuelle Rechenplattformen **104** präsentiert wird. Gemäß einigen Implementierungen kann die Schnittstelle dazu konfiguriert sein, es einer gegebenen Person zu ermöglichen, Speicheradressen, die der gegebenen Person zugeteilt sind, hinzuzufügen oder zu löschen, solange wenigstens eine Speicheradresse der gegebenen Person zugeteilt ist.

[0054] Bei einigen Implementierungen kann das System **100** dazu konfiguriert sein, auf ein oder mehrere Benutzerprofile und/oder Benutzerinformationen, die zu Benutzern des Systems **100** gehören, zuzugreifen und/oder diese zu verwalten. Das eine oder die mehreren Benutzerprofile und/oder Benutzerinformationen können Informationen aufweisen, die von Server(n) 102, einer oder mehreren der Rechenplattform(en) **104** und/oder anderen Speicherorten gespeichert werden. Die Benutzerprofile können zum Beispiel Informationen aufweisen, die Benutzer identifizieren (z.B. einen Benutzernamen oder -decknamen, eine Nummer, eine Kennung und/oder andere Identifizierungsinformationen), Sicherheitslogininformationen (z.B. einen Logincode oder ein Passwort), Systemkonteninformationen, Teilnehmerinformationen, Kontoinformationen über digitale Währung (die sich zum Beispiel auf Währung beziehen, für die ein Benutzer im Plus ist), Beziehungsinformationen (z.B. Informationen, die sich auf Beziehungen zwischen Benutzern in dem System **100**) beziehen, Systemverwendungsinformationen, demografische Informationen, die zu Benutzern gehören, Wechselwirkungshistorie zwischen Benutzern in dem System **100**, Informationen, die von Benutzern angegeben werden, Kaufinformationen von Benutzern, Browsing-Historie von Benutzern, eine Rechenplattformkennung, die zu einem Benutzer gehört, eine Telefonnummer, die zu einem Benutzer gehört, und/oder andere Informationen, die sich auf Benutzer beziehen.

[0055] Die maschinenlesbaren Befehle **106** können ausführbar sein, um auf Blockchain und sicherem Server oder sicheren Servern basiertes Speichern von elektronischem Material in Zusammenhang mit einer oder mehreren individuellen Kennungen und Transaktionsadresse(n) durchzuführen.

[0056] In **Fig. 14** ist ein Vorgang gezeigt, bei dem ein Benutzer das sichere Speichern von elektronischem Material anfordert. Dieses elektronische Material liegt im Allgemeinen im Dateiformat oder in einem diskreten Format vor. Bei Schritt **1402** kann das System die Anmeldeanfrage des Benutzers über die API empfangen. Bei Schritt **1404** kann das System den Benutzer authentifizieren, z.B. unter Verwendung der gespeicherten biometrischen Informationen des Benutzers und anderer Kennung(en), die während des Registrierungsvorgangs eingetragen wurden. Bei Schritt **1406** kann das System die Speicheranfrage des Benutzers empfangen. Bei Schritt **1408** kann das System das elektronische Material des Benutzers zum Speichern empfangen. Bei Schritt **1410** kann das System das elektronische Material in Dateifragmente zerlegen, wobei jedes Fragment vorzugsweise ein Teil der Datei ist, der jedoch allein und insgesamt unverständlich ist, außer wenn alle Fragmente der Datei vollständig zu der (durch eine Maschine oder einen Menschen) verständlichen Datei zusammengesetzt sind. Bei einer oder mehreren Ausführungsformen kann zum Beispiel ein Fragment ein Datei-Header sein, und ein anderes Fragment oder andere Fragmente können Daten oder Bilddaten aus der Datei sein. Der Datei-Header selbst kann in mehr als ein Fragment aufgeteilt sein. Bei Schritt **1412** kann das System ein oder mehrere Dateifragmente auf einer Blockchain oder auf Blockchains in einem oder mehreren Blöcken (z.B. bevorzugt als Transaktionen), auf einem Distributed Ledger oder auf Distributed Ledgers an einer oder mehreren Stellen (z.B. bevorzugt als Transaktionen) oder in einer verteilten Datenbank an einer oder mehreren Stellen speichern und das verbleibende Dateifragment oder die verbleibenden Dateifragmente außerhalb der Blockchain, außerhalb des Distributed Ledger oder außerhalb einer verteilten Datenbank speichern, z.B. in einem sicheren Server oder sicheren Servern und/oder auf einem Benutzergerät oder Benutzergeräten. Ein Fragment oder Fragmente kann/können online oder offline gespeichert werden, zum Beispiel in einer anderen digitalen Speichervorrichtung oder -vorrichtungen, die von online entfernt werden kann/können und normalerweise keinen eigenen Hauptprozessor hat/haben, zum Beispiel USB, SIM-Karte, Flash-Laufwerk oder eine andere geeignete Vorrichtung.

[0057] **Fig. 2** zeigt beispielsweise ein beispielhaftes System **100**, das die folgenden Schritte durchführen

kann, um elektronisches Material, wie zum Beispiel biometrische und/oder andere höchst persönliche und/oder vertrauliche Informationen, sicher zu speichern. Das System kann in diese sichere Speicherkomponente während der Benutzerregistrierung in das sichere Speichersystem eintreten, zum Beispiel, um das biometrische elektronische Material eines Benutzers zu speichern, das als Teil eines Authentifizierungserfordernisses zu verwenden ist, und/oder diese Speicherung kann stattfinden, wenn der Benutzer das System verwenden möchte, um elektronisches Material, wie zum Beispiel das biometrische elektronische Material des Benutzers, im Ansprechen auf eine Nachregisterierungsanfrage zum sicheren Speichern elektronischer Informationen durch einen Benutzer sicher zu speichern.

[0058] In Schritt **202** kann das System während der Registrierung oder nach dem Registrieren eines Benutzers und dem Zuteilen einer Benutzeridentifikation und -authentifizierung (vorzugsweise doppelte Authentifizierung oder mehr) die biometrischen elektronischen Informationen in mehrere Merkmalsblöcke zerlegen und jeden Merkmalsblock mit einer Indexnummer kennzeichnen. Die Indexnummer kann als optionaler Aspekt des Indiziervorgangs randomisiert werden, zum Beispiel mit einem Pseudozufallszahl-Generator oder einer anderen geeigneten Randomisiervorrichtung.

[0059] Bei Schritt **204**, welcher optional ist, kann das System optional einen oder mehrere der Merkmalsblöcke transformieren durch Rotieren, Umdrehen, Maskieren und/oder ein anderes Verfahren, bevorzugt zufällig, aber es könnte auch pseudozufällig oder auf vorgegebene Art und Weise erfolgen. Wenn die biometrische Information Sprache ist und die Merkmalsblöcke Sprachblöcke sind, kann jeder Block optional umgekehrt, maskiert, tonhöhenumtransformiert werden und/oder einem anderen Manipulierverfahren unterzogen werden. Das System zeichnet die Transformationsdaten (z.B. die Umdreh-/Rotationsinformationen) auf. Es wird angemerkt, dass bei jeder vorliegenden Ausführungsform Transformationen nicht zwingend stattfinden müssen, und nicht zwingend in diesem Stadium, und früher oder später während des Verfahrens erfolgen könnten.

[0060] Bei Schritt **206** kann das System die Indexnummer, Transformationsdaten und geometrische Speicherstellen jedes Datenblocks abbilden.

[0061] Bei Schritt **208** erzeugt das System eine Abbildungsdatei mit der Indexnummer, den Transformationsdaten und den geometrischen Speicherstellen, die in dem vorherigen Schritt erhalten wurden.

[0062] Bei Schritt **210**, der optional ist, verschlüsselt das System die Abbildungsdatei.

[0063] Bei Schritt **211** teilt das System (optional) die Abbildungsdatei auf und speichert sie auch. Einzelheiten, die eine Ausführungsform beschreiben, wie das System die Abbildungsdatei aufteilen und speichern kann, sind im Vorgang **300** in **Fig. 3** gezeigt.

[0064] Bei Schritt **212** kann das System einen Teil der Merkmalsblöcke auswählen und sie zusammen gruppieren (z.B. einen Prozentsatz von beispielsweise 30% der Merkmalsblöcke), bevorzugt zufällig, aber es könnte auch pseudozufällig oder auf vorgegebene Art und Weise erfolgen. Dieser Schritt kann mehrmals zusammen mit den Schritten **214**, **216** und **300** durchgeführt werden, um mehrere aufgeteilte biometrische Dateien zu erzeugen. Beim Vorgang des Auswählens eines Teils der Merkmalsblöcke zum Gruppieren kann ein gegebener Merkmalsblock öfter als einmal ausgewählt werden.

[0065] Bei Schritt **214** kann das System eine Gruppierung der Merkmalsblöcke nehmen und die Merkmalsblöcke zusammensetzen, um ein verwürfeltes teilbiometrisches Merkmal bzw. Scrambled Partial Biometric Feature (SPBF) durch Erzeugen einer neuen Datei zu bilden. Dieser Schritt kann mehrmals durchgeführt werden, um mehrere SPBFs zu erzeugen, gemäß einer oder mehreren unten erläuterten Herangehensweisen.

[0066] Bei Schritt **216**, welcher optional ist, kann das System die SPBF-Datei verschlüsseln. Die Verschlüsselung der SPBF-Datei kann über einen AES-Algorithmus, einen PGP-Algorithmus, einen Blowfish bzw. Kugelfisch-Algorithmus oder einen anderen geeigneten Verschlüsselungsalgorithmus erreicht werden.

[0067] Bei Schritt **218** kann das System wieder zu Vorgang **300** weitergehen, um die SPBF-Datei aufzuteilen und zu speichern.

[0068] Bezüglich des Speicherns von biometrischen Dateien sollte beachtet werden, dass mehrere Herangehensweisen zum Aufteilen und Speichern der Datei verwendet werden können. Eine Herangehensweise kann zum Beispiel sein, eine ursprüngliche biometrische Merkmalsdatei oder eine SPBF-Datei (entweder verschlüsselt oder nicht) in mehr als ein Fragment aufzuteilen und für jedes Fragment Dateien zum Speichern in einer oder mehreren Speichervorrichtungen zu erzeugen. Diese Herangehensweise kann auch für das Speichern einer Indexdatei, einer Abbildungsdatei, einer geometrischen Speicherstellendatei und/oder anderer Dateien verwendet werden, die nötig sind, um das ursprüngliche elektronische Material zu rekonstruieren.

[0069] Alles einer aufgeteilten Datei (d.h. alle „Fragment“-Dateien, die durch Aufteilen oder Zerlegen einer Datei gebildet werden) sollte gespeichert wer-

den, um die ursprüngliche Datei zu rekonstruieren. Es sollte eine zusätzliche Datei oder Dateien zum Speichern der Informationen darüber geben, wie die Datei aufgeteilt worden ist, d.h. eine Indexdatei, die die Reihenfolge (Indexreihenfolge) der Dateifragmente zum Zusammensetzen enthält. Die Indexdatei wird zum späteren Rekonstruieren der ursprünglichen Datei benötigt. Diese Herangehensweise kann auch auf eine gehashte Datei einer ursprünglichen biometrischen Merkmalsdatei angewendet werden. In einem solchen Fall müssen keine SPBF-Dateien erzeugt werden und werden bevorzugt auch nicht erzeugt. Bei einer Ausführungsform wird die Indexdatei selbst optional aufgeteilt, genauso wie die ursprüngliche Datei, und bevorzugt teilweise auf der Blockchain, auf dem Distributed Ledger oder in der verteilten Datenbank gespeichert, und teilweise außerhalb der Blockchain, außerhalb des Distributed Ledger oder außerhalb der verteilten Datenbank. Es gibt dann eine Indexdatei für die (primäre) Indexdatei. Diese „sekundäre“ Indexdatei sollte auf die sicherste Art und Weise gespeichert werden, ggf. offline, und verschlüsselt werden, vorzugsweise mit einem anderen Verschlüsselungsverfahren als die primäre Indexdatei.

[0070] Eine andere Herangehensweise zum Handhaben des Zerlegens und Speicherns von biometrischen Dateien ist das Auswählen verschiedener Merkmalsblöcke, um verschiedene SPBF-Dateien (entweder verschlüsselt oder nicht) zu bilden, und das Speichern dieser verschiedenen SPBF-Dateien in einer oder mehreren Speichervorrichtungen. Die Merkmalsblöcke der SPBF-Dateien können die Gesamtheit oder einen Teil (z.B. im Fall der Verwendung zur Authentifizierung) der ursprünglichen biometrischen Merkmalsdatendatei abdecken. Bei dieser Herangehensweise können für ein einziges biometrisches Merkmal eine oder mehrere SPBF-Dateien in beliebiger Kombination für eine oder mehrere biometrische Authentifizierungen verwendet werden.

[0071] Für ein einziges biometrisches Merkmal können SPBF-Dateien (falls mehr als eine erzeugt werden) und die korrespondierenden Fragmentdateien separat an verschiedenen Stellen auf einer Blockchain unter einer oder mehreren Transaktionsadressen und/oder unter einer oder mehreren Smart Contract-Adressen und/oder unter einer oder mehreren Blockchain-Utility bzw. Dienstprogramm-Adressen gespeichert werden. Für ein einziges biometrisches Merkmal können SPBF-Dateien (falls mehr als eine erzeugt werden) und Fragmentdateien separat auf einer oder mehreren unabhängigen Blockchains und/oder in einer oder mehreren Transaktionsaufzeichnungen auf einer oder jeder Blockchain, auf einem oder mehreren unabhängigen Distributed Ledgers und/oder in einer oder mehreren Transaktionsaufzeichnungen auf einem oder jedem Distributed Ledger oder in einer oder mehreren unabhängigen verteilten Datenbanken und/oder in einer oder mehreren Aufzeichnungen in einer jeder verteilten Datenbank gespeichert werden. Für ein einziges biometrisches Merkmal können eine oder mehrere SPBF-Dateien oder Fragmentdateien vor dem Speichern verschlüsselt werden. Für eine oder mehrere verschlüsselte SPBF-Dateien und/oder Fragmentdateien, die sich aus einem einzigen biometrischen Merkmal ergeben, hat nur der Besitzer des biometrischen Merkmals die Passphrase/den Schlüssel zum Entschlüsseln dieser Dateien, insbesondere, wenn diese Dateien in einer Blockchain, einem Distributed Ledger oder einer verteilten Datenbank (entweder öffentlich oder privat) gespeichert sind. Dies trägt dazu bei sicherzustellen, dass niemand anderes als der Besitzer des biometrischen Merkmals diese verschlüsselten Dateien zur biometrischen Authentifizierung verwenden kann. Die SPBF-Dateien können vor dem Speichern gehasht werden.

[0072] Jede der oben genannten Herangehensweisen zum Zerlegen und Speichern biometrischer Dateien kann allein oder in Kombination verwendet werden.

[0073] **Fig. 2A** zeigt einen beispielhaften Vorgang in einem schematischen Flussdiagramm zur Speicherung eines biometrischen Bildes. Bei Schritt **220** kann das System ein Bild eines biometrischen Merkmals empfangen (beispielsweise um in **Fig. 2** zu starten). Bei Schritt **222** (wie bei Schritt **202**) kann das System das Bild in Blöcke (Merkmalsblöcke) zerlegen. Bei Schritt **224** (wie bei den Schritten **204**, **208**, **212** und **214**) kann das System einige Merkmalsblöcke auswählen (z.B. zufällig für mehr Sicherheit, eine solche Auswahl könnte jedoch auch pseudozufällig oder gemäß einem nicht zufälligen Auswahlverfahren stattfinden), um sie zu verbinden oder zusammen zu gruppieren. Bei diesem Vorgang kann das System die Merkmalsblöcke transformieren, z.B. durch Rotation, zum Beispiel durch Rotieren um einen vorgegebenen Betrag von beispielsweise neunzig Grad oder einen zufälligen Betrag. Bei Schritt **230** erzeugt das System die Abbildungsdatei (wie bei den Schritten **206**, **208**, **210**). Die Abbildungsdatei oder die Abbildungsdateien kann/können dann bei den Schritten **232** und **234** (optional) aufgeteilt werden, und die Dateifragmente können teilweise auf der Blockchain, auf dem Distributed Ledger oder in der verteilten Datenbank gespeichert werden (in 234A als Speicheroptionen bezeichnet) und teilweise auf einem Speicher außerhalb der Blockchain, einem Speicher außerhalb des Distributed Ledger oder einem Speicher außerhalb der verteilten Datenbank, wie zum Beispiel in dem Cloud-Server oder den Cloud-Servern, einem sicheren Server oder Servern (die z.B. einer Entität oder einer Person gehören) und/oder auf einem Clientgerät oder Clientgeräten, z.B. dem Mobiltelefon eines Benutzers, einem Tablet, Laptop und/oder Desktop-Computer oder einem anderen Benutzergerät (wie in den Schritten **211** und **218** von **Fig. 2** und

dem Vorgang **300** von **Fig. 3**, und wie in 234B als Speicheroptionen bezeichnet). Die Speicheroptionen **234B** können Netzwerkdatenspeicherung umfassen.

[0074] Ein Fragment oder Fragmente kann/können in einer anderen digitalen Speichervorrichtung oder -vorrichtungen gespeichert werden, die normalerweise keinen eigenen Hauptprozessor haben, zum Beispiel SIM-Karte, Flash-Laufwerk oder andere geeignete Vorrichtung. Bei Schritt **226** (wie bei Schritt **216**) oder Schritt **228** (im Vorgang **200** nicht gezeigt, könnte jedoch optional hier anstelle von Schritt **216** verwendet werden) kann das System selektiv und optional Verschlüsselung bzw. Hashing für die teilbiometrische Datei, die SPBF-Datei oder -Dateien, die bei Schritt **224** gebildet werden, anwenden. Bei einer Ausführungsform kann das Hashing der teilbiometrischen/SPBF-Datei durch Anwenden eines MD5 Algorithmus, eines SHA Algorithmus (z.B. SHA-**0**), eines SHA-**2** Algorithmus (z.B. SHA-**256**) oder eines anderen geeigneten MD5 Algorithmus erzielt werden. Bei einer anderen Ausführungsform kann die Verschlüsselung der teilbiometrischen/SPBF-Datei durch Anwenden eines AES Algorithmus, eines PGP Algorithmus, eines Kugelfisch-Algorithmus oder eines anderen geeigneten Verschlüsselungsalgorithmus erzielt werden. Es wird angemerkt, dass, wie im Fall der Indexdatei, die Abbildungsdatei selbst optional aufgeteilt wird, ebenso wie die ursprüngliche Datei, und vorzugsweise teilweise (oder vollständig) auf der Blockchain und teilweise außerhalb der Blockchain, teilweise (oder vollständig) auf dem Distributed Ledger und teilweise außerhalb des Distributed Ledger, oder teilweise (oder vollständig) in der verteilten Datenbank und teilweise außerhalb der verteilten Datenbank gespeichert wird. Es gibt dann eine Abbildungs- oder Index-Datei für die (primäre) Abbildungsdatei. Diese „sekundäre“ Abbildungs- oder Index-Datei sollte auf die sicherste Art und Weise gespeichert werden, möglichst offline, und verschlüsselt werden, vorzugsweise mit einem anderen Verschlüsselungsverfahren als die primäre Abbildungsdatei. Bevorzugt findet bei jeder vorliegenden Ausführungsform das Speichern der Abbildungsdatei oder wenigstens eines Teils der Abbildungsdatei in der Blockchain oder dem Distributed Ledger statt.

[0075] Fig. 3 zeigt eine beispielhafte Version der Routine **300**, z.B. wie in anderen Figuren verwendet, die die folgenden Schritte durchführen kann, um elektronisches Material wie zum Beispiel eine biometrische Datei und/oder einen beliebigen anderen Dateityp aufzuteilen und zu speichern.

[0076] Bei Schritt **302** kann das System das elektronische Material in Fragmente (zwei oder mehr) aufteilen, wobei jedes Fragment eine Datei (eine „Fragmentdatei“) ist und eine solche Fragmentdatei einen Block oder Blöcke, oder eine Scheibe oder Scheiben, oder ein anderes Stück oder andere Stücke des zu speichernden elektronischen Materials repräsentiert. Das System kann auch die Reihenfolge der Fragmentdateien indizieren („Indexordnung“). Für eine biometrische Datei kann das System die Datei in Fragmente, wie zum Beispiel Merkmalsblöcke, mit Indexordnung aufteilen. Eine aus dem elektronischen Material gebildete Fragmentdatei kann einen Teil der Daten und/oder Bild und/oder Ton und/oder Video einer elektronischen Datei oder anderes elektronisches Material aufweisen. Bei einigen Ausführungsformen kann die Fragmentdatei ein Datei-Header oder ein Abschnitt eines Datei-Headers sein oder diese aufweisen. Als Teil dieses Schritts kann das System auch die Dateifragmente speichern, wie oben erwähnt, eines oder mehrere auf der Blockchain und eines oder mehrere außerhalb der Blockchain, eines oder mehrere auf dem Distributed Ledger und eines oder mehrere außerhalb des Distributed Ledger, oder eines oder mehrere in der verteilten Datenbank und eines oder mehrere außerhalb der verteilten Datenbank (siehe Schritt **310** unten).

[0077] Bei Schritt **304** kann das System eine Indexdatei zum Wiederzusammensetzen der ursprünglichen Datei erzeugen.

[0078] Bei Schritt **306** kann das System die Indexdatei optional verschlüsseln.

[0079] Bei Schritt **308** kann das System die Indexdatei (zur späteren Dateizusammensetzung) speichern. Das System kann die Indexdatei auf dem Blockchain-Speicher oder außerhalb des Blockchain-Speichers speichern und eine Hash-Tabelle für Speicherstellendaten verwenden, bevorzugt auf alle Knoten auf der Blockchain verteilt, z.B. während des Speicherns der Indexdatei außerhalb der Blockchain. Die Indexdatei selbst kann, wie bei anderen vorliegend erläuterten Ausführungsformen, aufgeteilt und gespeichert werden, bevorzugt ein Teil auf der Blockchain und ein Teil außerhalb der Blockchain, ein Teil auf dem Distributed Ledger und ein Teil außerhalb des Distributed Ledger, oder ein Teil in der verteilten Datenbank und ein Teil außerhalb der verteilten Datenbank.

[0080] Bei Schritt **310** kann das System eine beliebige Auswahl speichern, am bevorzugtesten eine zufällige Auswahl (oder sie könnte pseudozufällig sein oder mit einem vorgegebenen Verfahren erfolgen) eines Fragments oder einer Gruppe der Fragmente des elektronischen Materials, das sicher auf einem Speicher außerhalb der Blockchain, einem Speicher außerhalb des Distributed Ledger oder außerhalb des verteilten Datenspeichers gespeichert ist, der ein sicherer Server oder sichere Server sein kann, z.B. einer Entität oder einer Person gehört, und/oder ein Clientgerät, z.B. Mobiltelefon eines Benutzers, Tablet, Laptop und/oder Desktop-Computer oder eine andere Benutzervorrichtung. Ein Fragment oder Fragmente kann/können in einer anderen digitalen Spei-

chervorrichtung oder -vorrichtungen gespeichert werden, welches/welche normalerweise keinen eigenen Hauptprozessor hat/haben, beispielsweise SIM-Karte, Flash-Laufwerk oder eine andere geeignete Vorrichtung. Wie bei allen vorliegenden Ausführungsformen kann die zeitliche Planung, wann ein Schritt im Verhältnis zu anderen Schritten stattfindet, wo möglich variiert werden.

[0081] Das System kann wenigstens ein Fragment des elektronischen Materials auf der Blockchain, auf dem Distributed Ledger oder in der verteilten Datenbank speichern. Dieses Fragment oder diese Fragmente sollte/sollten erforderlich sein, um die Datei (elektronisches Material) zu einer verständlichen Datei (d.h. die wenigstens einiges verständliche Material hat) zu rekonstruieren, verständlich für eine Maschine und/oder einen Menschen. Beispielsweise kann, wie bei jeder vorliegenden Ausführungsform, dieses wenigstens eine Fragment der Headerabschnitt einer Datei sein, die sicher gespeichert ist, oder ein Abschnitt des Headers, und es kann einen Teil des Rests der Datei enthalten oder nicht. Dieses wenigstens eine Fragment ist vorzugsweise auch die kleinste Größe aus einer Datenspeicherperspektive (kleinste Bitgröße), die sinnvoll möglich ist, um das Ziel zu erreichen, dass das elektronische Material ohne dieses Fragment bedeutungslos wird, um die Speicher- und Abruflast auf dem Blockchain-System zu minimieren. Das System kann optional mehrere Fragmente in separaten Speichern auf der Blockchain, auf dem Distributed Ledger oder in der verteilten Datenbasis speichern. Dieser Speicherschritt ist in **Fig. 3A** schematisch gezeigt und wird unten erläutert.

[0082] Bei allen vorliegend offenbarten Ausführungsformen kann das System beim Speichern eines Fragments oder von Fragmenten auf der Blockchain solche Fragmente in mehreren Blöcken (z.B. als Transaktionen) auf der Blockchain speichern. Beim Speichern eines Fragments oder von Fragmenten auf dem Distributed Ledger kann das System solche Fragmente an mehreren Stellen (z.B. als Transaktionen) auf dem Distributed Ledger speichern. Oder das System kann beim Speichern eines Fragments oder von Fragmenten in der verteilten Datenbank solche Fragmente an mehreren Stellen in der verteilten Datenbank speichern. Das System, die Blockchain, der Distributed Ledger und/oder die verteilte Datenbank können auch dazu ausgelegt sein, das Fragment oder die Fragmente, das/die gespeichert wird/werden, weiter zu zerlegen und solche Fragmente über die Blockchain-Knoten, die Distributed Ledger-Knoten, die verteilten Datenspeicher-Knoten als Datenstrom in einem Netzwerkdatenspeicher zu verteilen. Vorzugsweise erfordert der Zugriff auf einen Blockchain-Knoten, einen Distributed Ledger-Knoten, einen verteilten Datenspeicher-Knoten oder einen Netzwerkdatenspeicher, um ein Dateifragment zum Wiederzusammensetzen zu verwenden, Authentifizierung und die Verwendung eines privaten Schlüssels sowie die Transaktionsadresse oder die Smart Contract Adresse. Für verbesserte Sicherheit können die Transaktionsadressen oder die Smart Contract Adressen zeitbasiert periodisch und/oder nach jedem Gebrauch aktualisiert werden.

[0083] **Fig. 3A** zeigt einen beispielhaften Vorgang in einem schematischen Flussdiagramm zum Speichern eines beliebigen Dateityps, der als Teil der Vorgänge von **Fig. 2A** und **Fig. 4A** verwendet werden kann. Er kann als Erweiterung von Schritt **310** in **Fig. 3** betrachtet werden.

[0084] Bei Schritt **312** kann das System eine Datei zum Aufteilen und Speichern empfangen. Bei Schritt **314** kann das System die Datei in Fragmente aufteilen. Bei Schritt **316** kann das System wenigstens ein Fragment oder Fragmente auf der Blockchain, dem Distributed Ledger oder der verteilten Datenbank speichern und das restliche Fragment oder Fragmente außerhalb des Blockchain-Speichers, außerhalb des Distributed Ledger-Speichers oder außerhalb des verteilten Datenspeichers (in Kästchen **316A** zusammen gruppiert), zum Beispiel einem Cloud-Server oder - Servern, einem sicheren Server oder Servern, z.B. einer Entität oder Person gehörend, und/oder einem Clientgerät oder-geräten, z.B. dem Mobiltelefon eines Benutzers, einem Tablet, Laptop und/oder einem Desktop-Computer oder einer anderen Benutzervorrichtung (in Kästchen **316B** zusammen gruppiert). Ein Fragment oder Fragmente kann/können in einer anderen digitalen Speichervorrichtung oder -vorrichtungen gespeichert werden, die normalerweise keinen eigenen Hauptprozessor haben, zum Beispiel SIM Karte, Flash-Laufwerk oder eine andere geeignete Vorrichtung.

[0085] **Fig. 4** ist eine beispielhafte Version der Routine **400**, die z.B. in anderen Figuren anstelle der Routine **300** verwendet werden kann, um elektronisches Material, beispielsweise eine biometrische Datei, aufzuteilen und zu speichern.

[0086] Bei Schritt **402** kann das System eine Biometrie in Merkmalsblöcke zerlegen und jeden Merkmalsblock einer biometrischen Datei mit einer Indexnummer kennzeichnen, gleich oder ähnlich wie bei Schritt **202** oben. Diese Indexnummer kann als optionaler Teil des Indiziervorgangs randomisiert werden, kann jedoch wie bei jeder vorliegenden Ausführungsform pseudozufällig ausgewählt oder mit einem vorgegebenen Verfahren ausgewählt werden.

[0087] Bei Schritt **404**, der optional ist, kann das System einen Merkmalsblock gleich oder ähnlich wie bei Schritt **204** oben transformieren. Das System zeichnet die Transformationsdaten (z.B. die Umdreh-/Rotationsinformationen) auf.

[0088] Bei Schritt **406** bildet das System die Indexnummer, die Transformationsdaten und geometrische Speicherstellen jedes Merkmalsblocks gleich oder ähnlich wie bei Schritt **206** oben ab.

[0089] Bei Schritt **408** erzeugt das System eine Abbildungsdatei (oder Abbildungsdatendatei) mit der Indexnummer, den Transformationsdaten und den geometrischen Speicherstellen, die im vorhergehenden Schritt **406** erhalten wurden.

[0090] Bei Schritt **410**, der optional ist, verschlüsselt das System die Abbildungsdatendatei. Die Verschlüsselung der Abbildungsdatei kann über einen AES Algorithmus, einen PGP Algorithmus, einen Kugelfisch-Algorithmus oder einen anderen geeigneten Verschlüsselungsalgorithmus erzielt werden.

[0091] Bei Schritt **411** teilt (optional) und speichert das System die Abbildungsdatei wie oben erläutert mittels des im Einzelnen in **Fig. 3** gezeigten Vorgangs **300**. Wie bei den anderen vorliegenden Ausführungsformen kann die primäre Abbildungs- und/oder Indexdatei selbst mittels desselben Vorgangs wie beim Aufteilen und Speichern der ursprünglichen Datei aufgeteilt werden, und zur verbesserten Sicherheit teilweise online (wie zum Beispiel auf der Blockchain und außerhalb der Blockchain) und/oder teilweise offline gespeichert werden.

[0092] Bei Schritt **412** wählt das System zufällig einen Abschnitt der Merkmalsblöcke (z.B. dreißig Prozent der Merkmalsblöcke) aus und setzt sie in zufälliger Reihenfolge (oder in pseudozufälliger oder vorgegebener Reihenfolge) auf zweidimensionale oder mehrdimensionale Art und Weise zusammen.

[0093] Dieser Schritt kann zusammen mit den Schritten **414**, **416**, **418**, **300**, **420**, **422**, **424**, 300 mehrmals erfolgen, um mehrere SPBF-, Blockauswahl- und geometrische Daten-Dateien zu erzeugen.

[0094] Insbesondere kann bei Schritt **414** das System die ZusammensetzungsreihenfolgeDaten für die Merkmalsblöcke in einer Zusammensetzungsreihenfolge-Datendatei aufzeichnen.

[0095] Bei Schritt **416** kann das System die Zusammensetzungsreihenfolge-Datendatei verschlüsseln. Die Verschlüsselung der Zusammensetzungsreihenfolge-Datendatei kann über einen AES Algorithmus, einen PGP Algorithmus, einen Kugelfisch-Algorithmus oder einen anderen geeigneten Verschlüsselungsalgorithmus erzielt werden.

[0096] Bei Schritt **418** kann das System Blockauswahldaten- und geometrische Datendateien, zum Beispiel unter Verwendung des Vorgangs **300**, aufteilen und speichern.

[0097] Bei Schritt **420** kann das System die Merkmalsblöcke zusammensetzen, um das verwürfelte teilbiometrische Merkmal (SPBF) durch Erzeugen einer neuen Datei zu bilden.

[0098] Bei Schritt **422**, der optional ist, kann das System einen biometrischen SPBF-Vektor extrahieren.

[0099] Bei Schritt **424**, der optional ist, kann das System die SPBF-Datei oder die biometrische SPBF-Vektordatei verschlüsseln/hashen.

[0100] Bei Schritt **426** kann, wie im Vorgang **300** oben gezeigt ist, das System die SPBF (SPBF-Vektor-) Datei unter Verwendung der in Vorgang **300** dargelegten Vorgangsschritte aufteilen und speichern.

[0101] **Fig. 4A** zeigt einen anderen beispielhaften Vorgang in einem schematischen Flussdiagramm zum Speichern eines biometrischen Bildes. Bei Schritt **428** kann das System ein Bild eines biometrischen Merkmals (beispielsweise um in **Fig. 4** zu starten) empfangen. Bei Schritt 430 (wie bei Schritt **402** von **Fig. 4**) kann das System das Bild in Blöcke (Merkmalsblöcke) zerlegen. Bei Schritt **432** (wie bei Schritt **404** und den Schritten **406**, **412**, **420** und **422**) kann das System einige Merkmalsblöcke zum Zusammensetzen auswählen (z.B. zufällig für mehr Sicherheit, aber eine solche Auswahl könnte auch pseudozufällig oder gemäß einem nicht zufälligen Auswahlverfahren stattfinden). Bei diesem Vorgang kann das System die Merkmalsblöcke transformieren (z.B. durch Rotation, beispielsweise durch Rotieren um einen vorgegebenen Betrag von z.B. neunzig Grad oder einen zufälligen Betrag). Bei Schritt **438** erzeugt das System die biometrische Blockauswahl- und Zusammensetzungsreihenfolge-Datendatei (wie bei den Schritten **414** und **416** in **Fig. 4**). Die biometrische Blockauswahl- und Zusammensetzungsreihenfolge-Datendatei oder -dateien kann/können dann bei den Schritten **442** und **444** aufgeteilt werden und die Dateifragmente können teilweise auf der Blockchain, auf dem Distributed Ledger oder in der verteilten Datenbank und teilweise außerhalb des Blockchain-Speichers, außerhalb des Distributed Ledger-Speichers oder außerhalb des verteilten Datenspeichers gespeichert werden, zum Beispiel in dem Cloud-Server oder den Cloud-Servern, einem sicheren Server oder Servern, und/oder auf einem Clientgerät oder Clientgeräten, dem Mobiltelefon eines Benutzers, einem Tablet, Laptop und/oder Desktop-Computer oder einer anderen Benutzervorrichtung. Das Kästchen **444A** zeigt Speicheroptionen auf der Blockchain, dem Distributed Ledger oder in der verteilten Datenbank, und das Kästchen **444B** zeigt Speicheroptionen außerhalb der Blockchain, außerhalb des Distributed Ledger und/oder außerhalb der verteilten Datenbank. Ein Fragment oder Fragmente kann/können in einer anderen digitalen Speichervorrichtung oder -vorrichtungen gespeichert werden, die

normalerweise keinen eigenen Hauptprozessor haben, beispielsweise einer SIM Karte, einem Flash-Laufwerk oder einer anderen geeigneten Vorrichtung. Bei Schritt **433** (optional) kann das System einen biometrischen Vektor aus der teilbiometrischen Datei extrahieren. Dann kann bei Schritt **434** (wie bei Schritt **424** in **Fig. 4**) oder Schritt **436** (wie bei Schritt **424** in **Fig. 4**) das System selektiv und optional Verschlüsselung bzw. Hashing für die SPBF-Datei, die biometrische SPBF-Vektordatei oder -dateien, die bei Schritt **432** gebildet wurden anwenden. Bei Schritt **440** kann das System eine biometrische Abbildungsdatei erzeugen (und optional verschlüsseln) (wie bei den Schritten **408** und **410** in **Fig. 4**). Bei Schritt **442** kann das System die Abbildungsdatei oder -dateien in Fragmente teilen (wie bei den Schritten **411**, **418**, **426** von **Fig. 4** und dem Vorgang **300** von **Fig. 3**). Bei Schritt **444** kann das System die Dateifragmente teilweise auf der Blockchain, auf dem Distributed Ledger oder in der verteilten Datenbank und teilweise auf einem Speicher außerhalb der Blockchain, einem Speicher außerhalb des Distributed Ledger oder einem Speicher außerhalb der verteilten Datenbank speichern, wie zum Beispiel dem Cloud-Server oder den Cloud-Servern, einem sicheren Server oder Servern und/oder auf einem Clientgerät oder -geräten (wie in den Schritten **411**, **418**, **426** in **Fig. 4** und dem Vorgang **300** von **Fig. 3**). Ein Fragment oder Fragmente kann/können in einer anderen digitalen Speichervorrichtung oder -vorrichtungen gespeichert werden, die normalerweise keinen eigenen Hauptprozessor hat/haben, zum Beispiel einer SIM Karte, einem Flash-Laufwerk oder einer anderen geeigneten Vorrichtung.

[0102] Nachdem das sichere Speichern einer biometrischen Datei stattgefunden hat, kann ein Benutzer auf die biometrische Datei zugreifen wollen, oder das System kann Zugriff auf die biometrische oder SPBF-Datei benötigen, um sie mit Biometrik oder SPBF eines Benutzers zu vergleichen, um den Benutzer zu authentifizieren.

[0103] In **Fig. 15** ist ein Vorgang gezeigt, bei dem ein Benutzer das Abrufen sicher gespeicherten elektronischen Materials anfordert. Bei Schritt **1502** kann das System die Anmeldungsanfrage des Benutzers über die API empfangen. Bei Schritt **1504** kann das System den Benutzer authentifizieren, z.B. unter Verwendung der gespeicherten biometrischen Informationen des Benutzers und anderer Kennung(en), die während des Registrierungsvorgangs aufgezeichnet wurden. Bei Schritt **1506** kann das System die Abrufanfrage des Benutzers empfangen. Bei Schritt 1508 kann das System die Fragmente elektronischen Materials des Benutzers aus dem Speicher abrufen. Bei Schritt **1510** kann das System die Dateifragmente zu einer oder mehreren Dateien zusammensetzen. Bei Schritt **1512** kann das System die Datei(en) an den Benutzer ausgeben, z.B. durch Anzeige oder Nurlesen, durch Herunterladen und/oder durch andere Mittel.

[0104] **Fig. 5** zeigt ein Verfahren zum Abrufen und Wiederzusammensetzen einer sicher gespeicherten Datei, wie zum Beispiel einer biometrischen Datei. Bei Schritt **502** kann das System die Abbildungsdatei und die Speicherstellenindexdatei abrufen.

[0105] Bei Schritt **504** kann das System die Abbildungsdatei-Speicherstellenindexdatei entschlüsseln.

[0106] Bei Schritt **506** kann das System aufgeteilte Abbildungsdateien und die Abbildungsindexdatei unter Verwendung der Abbildungsdatei-Speicherstellenindexdatei abrufen.

[0107] Bei Schritt **508**, der optional ist, kann das System die Abbildungsindexdatei entschlüsseln.

[0108] Bei Schritt **510** kann das System die Abbildungsdatei unter Verwendung der Abbildungsindexdatei und der aufgeteilten Abbildungsdateien zusammensetzen.

[0109] Bei Schritt **512**, der optional ist, kann das System die Abbildungsdatei entschlüsseln.

[0110] Bei Schritt **514** kann das System die SPBF-Indexdatei und die aufgeteilten SPBF-Dateien abrufen.

[0111] Bei Schritt **516**, der optional ist, kann das System die SPBF-Indexdatei entschlüsseln.

[0112] Bei Schritt **518** kann das System die SPBF-Datei unter Verwendung der SPBF-Indexdatei und der aufgeteilten SPBF-Dateien zusammensetzen.

[0113] Bei Schritt **520**, der optional ist, kann das System die SPBF-Datei entschlüsseln.

[0114] Bei Schritt **522** kann das System eine Teilbiometrik unter Verwendung der Abbildungsdatei und der SPBF-Datei zusammensetzen.

[0115] Bei Schritt **524** kann das System eine vollständige Biometrik unter Verwendung von zwei oder mehr Teilbiometriken zusammensetzen.

[0116] Alternativ kann das Wiederzusammensetzen des SPBF den Vorgang von **Fig. 6** verwenden.

[0117] Bei Schritt **602** kann das System die Abbildungsdatei-Speicherstellenindexdatei abrufen.

[0118] Bei Schritt **604**, der optional ist, kann das System die Abbildungsdatei-Speicherstellenindexdatei entschlüsseln.

[0119] Bei Schritt **606** kann das System die aufgeteilten Abbildungsdateien und die Abbildungsindexdatei unter Verwendung der Abbildungsdatei-Speicherstellenindexdatei abrufen.

[0120] Bei Schritt **608**, der optional ist, kann das System die Abbildungsindexdatei entschlüsseln.

[0121] Bei Schritt **610** kann das System die Abbildungsdatei unter Verwendung der Abbildungsindexdatei und der aufgeteilten Abbildungsdateien zusammensetzen.

[0122] Bei Schritt **612**, der optional ist, kann das System die Abbildungsdatei entschlüsseln.

[0123] Bei Schritt **614** kann das System die aufgeteilten SPBF-Dateien-Speicherstellenindexdatei abrufen.

[0124] Bei Schritt **616**, der optional ist, kann das System die aufgeteilten SPBF-Dateien-Speicherstellenindexdatei entschlüsseln.

[0125] Bei Schritt **618** kann das System die SPBF-Indexdatei und die aufgeteilten SPBF-Dateien unter Verwendung der aufgeteilten SPBF-Dateien-Speicherstellenindexdatei abrufen.

[0126] Bei Schritt **620**, der optional ist, kann das System die SPBF-Indexdatei entschlüsseln.

[0127] Bei Schritt **622** kann das System die SPBF-Datei unter Verwendung der SPBF-Indexdatei und der aufgeteilten SPBF-Dateien zusammensetzen.

[0128] Bei Schritt **624**, der optional ist, kann das System die SPBF-Datei entschlüsseln.

[0129] Bei Schritt **626** kann das System die Teilbiometrik unter Verwendung der Abbildungsdatei und der SPBF-Datei zusammensetzen. Die biometrische Abbildungsdatei sollte genügend Informationen zur biometrischen Wiederzusammensetzung enthalten.

[0130] Bei Schritt **628** kann das System eine vollständige Biometrik unter Verwendung von zwei oder mehr Teilbiometriken zusammensetzen.

[0131] **Fig. 7** zeigt einen beispielhaften allgemeinen Wiederzusammensetzungsvorgang für eine beliebige Datei.

[0132] Bei Schritt **702** kann das System die Dateispeicherstellen-Indexdatei abrufen. Bei Schritt **704**, der optional ist, kann das System die Dateispeicherstellen-Indexdatei entschlüsseln. Bei Schritt **706** kann das System die Dateiindexdatei abrufen. Bei Schritt **708**, der optional ist, kann das System die Dateiindexdatei entschlüsseln. Bei Schritt **710** kann das System die aufgeteilten Datei-Dateien abrufen. Bei Schritt **712** kann das System die Datei unter Verwendung der aufgeteilten Datei-Dateien und der Indexdatei zusammensetzen. Bei Schritt **714**, der optional ist, kann das System die Datei entschlüsseln.

[0133] **Fig. 8** zeigt einen beispielhaften Dateilöschvorgang. Bei Schritt **802** kann das System die Dateiindexdatei abrufen. Bei Schritt **804**, der optional ist, kann das System die Dateiindexdatei entschlüsseln. Bei Schritt **806** kann das System eine Fragmentdatei oder -dateien unter Verwendung der Dateiindexdatei-Speicherstellen wo zutreffend löschen (z.B. von außerhalb der Blockchain, dem Cloud-Speicher, dem Firmenserver oder dem Clientgerät).

[0134] **Fig. 9** zeigt einen beispielhaften Vorgang zur biometrischen Authentifizierung unter Verwendung verschlüsselter SPBF-Dateien. Diese biometrische Authentifizierung kann verwendet werden, um den Benutzer zu identifizieren, so dass der Benutzer auf die sicher gespeicherte(n) Datei(en) zugreifen oder den Zugriff darauf bewilligen kann. Es wird angemerkt, dass, wenn eine SPBF-Datei nachfolgend verwendet wird, um einen vollständigen Abschnitt oder einen Teilabschnitt einer ursprünglichen biometrischen Datei zu rekonstruieren, eine solche SPBF-Datei bevorzugt vor dem Speichern nicht gehasht werden sollte, weil Hashing irreversibel ist und somit eine Rekonstruierung unwahrscheinlich ist. Das Extrahieren eines biometrischen Vektors aus einem SPBF (das nicht verschlüsselt und nicht gehasht ist) ist optional. Wenn ein biometrischer Vektor verwendet wird, sollte Hashing (optional) bevorzugt nur für eine nicht verschlüsselte und nicht gehashte biometrische Vektordatei, aber nicht für eine SPBF-Datei erfolgen. Denn im Allgemeinen kann ein nützlicher biometrischer Vektor nur aus einer nicht verschlüsselten und nicht gehashten SPBF-Datei oder SPBF-Dateien oder aus der nicht verschlüsselten und nicht gehashten ursprünglichen biometrischen Datei oder biometrischen Dateien extrahiert werden.

[0135] Unter Bezug auf **Fig. 9** kann bei Schritt **902** das System eine biometrische Aufnahme der Person (des Benutzers) empfangen, der unter Verwendung der biometrischen Vorrichtung zu verifizieren ist. Bei Schritt **904** kann das System ein SPBF unter Verwendung eines der identifizierten Vorgänge **500** von **Fig. 5** oder **Fig. 600** von **Fig. 6** abrufen. Bei Schritt **906** kann das System einen Vergleich von Bildern oder Mustern anwenden, die aus dem gespeicherten SPBF und Eingangsbiometrik wiederhergestellt wurden. Bei Schritt **908** kann das System positive oder negative Ergebnisse basierend auf den Vergleichsergebnissen ausgeben.

[0136] **Fig. 10** zeigt einen beispielhaften Vorgang für biometrische Authentifizierung unter Verwendung gehashter SPBF-Dateien (z.B. im Ansprechen auf ei-

ne Benutzeranfrage nach Authentifizierung und/oder Zugriff). Bei Schritt **1002** kann das System eine Eingangsbiometrik empfangen, z.B. von dem Benutzer, der ein biometrisches Aufnahmegerät verwendet und die aufgenommenen biometrischen Informationen an das System überträgt.

[0137] Bei Schritt **1004** kann das System die eingegebene Biometrik in eine SPBF-Datei umwandeln unter Verwendung des Umwandlungsverfahrens wie beim Speichern der SPBF-Datei des Benutzers (z.B. wie in **Fig. 2**, **Fig. 4** oder **Fig. 4A**). Das heißt, das System kann Abbildungsdaten, Transformationsdaten, Zusammensetzungsreihenfolge und Indexdateien, die während der Erzeugung der ursprünglichen SPBF-Datei verwendet wurden, abrufen und dieselben Merkmalsblöcke auswählen und alle Transformationen und Zusammensetzungen durchführen, die während der ursprünglichen Speicherung durchgeführt wurden.

[0138] Bei Schritt **1006** kann das System die SPBF-Datei unter Verwendung derselben Hashing-Routine hashen wie beim Hashing der SPBF-Datei des Benutzers während des Speichern (z.B. wie in **Fig. 2**, **Fig. 4** oder **Fig. 4A**).

[0139] Bei Schritt **1008** kann das System die SPBF-Hashdatei mit der gespeicherten SPBF-Hashdatei vergleichen.

[0140] Bei Schritt **1010** kann das System die Ergebnisse des Vergleichs, d.h. eine Übereinstimmung oder Nichtübereinstimmung, ausgeben und dieses Ergebnis für den biometrischen Teil einer Authentifizierungsroutine verwenden.

[0141] **Fig. 11** zeigt einen beispielhaften Vorgang für biometrische Authentifizierung unter Verwendung eines biometrischen SPBF-Vektors. Bei Schritt **1102** kann das System eine Eingangsbiometrik empfangen, z.B. von dem Benutzer, der eine biometrische Aufnahmevorrichtung verwendet und die aufgenommenen biometrischen Informationen an das System überträgt.

[0142] Bei Schritt **1104** kann das System die eingegebene Biometrik in eine SPBF-Datei umwandeln unter Verwendung des Umwandlungsverfahrens wie beim Speichern der SPBF-Datei des Benutzers (z.B. wie in **Fig. 4** oder **Fig. 4A**). Das heißt, das System kann Abbildungsdaten, Transformationsdaten, Zusammensetzungsreihenfolgedaten und Indexdateien, die während der Erzeugung der ursprünglichen SPBF-Datei verwendet wurden, abrufen und dieselben Merkmalsblöcke auswählen und alle Transformationen und Zusammensetzungen durchführen, die während der ursprünglichen Speicherung durchgeführt wurden.

[0143] Bei Schritt **1106** kann das System den biometrischen SPBF-Vektor unter Verwendung derselben Extrahierungsroutine für einen biometrischen Vektor wie beim Extrahieren des biometrischen Vektors während des Speicherns extrahieren.

[0144] Bei Schritt **1108** kann das System die biometrische SPBF-Vektordatei mit der gespeicherten biometrischen SPBF-Vektordatei vergleichen.

[0145] Bei Schritt **1110** kann das System die Ergebnisse des Vergleichs, d.h. eine Übereinstimmung oder Nichtübereinstimmung, ausgeben und dieses Ergebnis für den biometrischen Teil einer Authentifizierungsroutine verwenden.

[0146] **Fig. 12** zeigt einen beispielhaften Vorgang zur biometrischen Authentifizierung unter Verwendung einer gehashten biometrischen Vektordatei. Bei diesem Vorgang sind die Schritte **1202**, **1204** und **1206** dieselben wie die Schritte **1102**, **1104** und **1106** von **Fig. 11**.

[0147] Dann kann bei Schritt **1208** das System die aus dem neu gebildeten SPBF erhaltene (z.B. neu vom Benutzer erhaltene) biometrische Vektordatei unter Verwendung derselben Hashfunktion, wie sie beim Speichern des ursprünglich erhaltenen biometrischen SPBF-Vektors verwendet wurde, hashen.

[0148] Bei Schritt **1210** kann das System die biometrische SPBF-Hashdatei mit der gespeicherten biometrischen SPBF-Hashdatei vergleichen.

[0149] Bei Schritt **1212** kann das System die Ergebnisse des Vergleichs, d.h. eine Übereinstimmung oder Nichtübereinstimmung, ausgeben und dieses Ergebnis für den biometrischen Teil einer Authentifizierungsroutine verwenden.

[0150] Es gibt unzählige Anwendungen eines sicheren Speichersystems, wie es vorliegend offenbart ist. Bei einer derartigen Anwendung kann das System **100** dazu konfiguriert sein, eine oder mehrere Kennungen in Verbindung mit einer oder mehreren Anfragen zu empfangen, um die Identität einer oder mehrerer Personen zu verifizieren. Das System kann auf eine solche Anfrage durch die Verwendung einer Identitätsverifizierungskomponente **120** antworten, die in **Fig. 1** gezeigt ist. Beispielsweise kann die oben erörterte erste Kennung in Verbindung mit einer Anfrage empfangen werden, die Identität der ersten Person zu verifizieren. Anfragen nach Identitätsverifizierung können in Verbindung mit und/oder in Bezug zu Finanztransaktionen, Informationsaustausch und/oder anderen Interaktionen bereitgestellt werden. Anfragen können von anderen Personen und/oder Dritten empfangen werden.

[0151] Das System **100** kann dazu konfiguriert sein, die biometrischen Daten, die zu der einen oder mehreren Personen gehören, aus den korrespondierenden Speicheradressen zu extrahieren. Beispielsweise können die ersten biometrischen Daten, die zu der ersten Person gehören, aus der ersten Speicheradresse extrahiert werden. Das Extrahieren von Informationen (z.B. biometrischen Daten) aus einer Speicheradresse kann das Entschlüsseln von Informationen beinhalten.

[0152] Gemäß einigen Implementierungen kann das System **100** so konfiguriert sein, dass im Ansprechen auf das Empfangen einer Anfrage, die Identität der ersten Person zu verifizieren, eine Aufforderung an die erste Person erfolgen kann hinsichtlich biometrischer Daten, die mit den ersten biometrischen Daten übereinstimmen, und hinsichtlich eines privaten Schlüssels, der mit dem ersten privaten Schlüssel übereinstimmt. Die Aufforderung kann über eine Rechenplattform 104 erfolgen, die zu der ersten Person gehört. Die Aufforderung kann über eine grafische Benutzerschnittstelle und/oder eine andere Benutzerschnittstelle erfolgen, die von der Rechenplattform **104** bereitgestellt wird, die zu der ersten Person gehört. Die Aufforderung kann eine Angabe aufweisen, die eines oder mehrere ist von visuellen, hörbaren, haptischen und/oder anderen Angaben.

[0153] Bei einigen Implementierungen kann das System so konfiguriert sein, dass im Ansprechen auf das Empfangen einer Anfrage, die Identität der ersten Person zu verifizieren, eine Aufforderung an eine Rechenplattform **104** erfolgen kann, die zu der ersten Person gehört. Die Aufforderung kann veranlassen, dass die Rechenplattform **104** automatisch an den/die Server **102** biometrische Daten liefert, die mit den ersten biometrischen Daten übereinstimmen und/oder einen privaten Schlüssel, der mit dem ersten privaten Schlüssel übereinstimmt.

[0154] Das System **100** kann dazu konfiguriert sein, die Identität der einen oder der mehreren Personen nach dem oder im Ansprechen auf das Empfangen übereinstimmender biometrischer Daten und privater Schlüssel zu verifizieren. Beispielsweise kann die persönliche Identität der ersten Person verifiziert werden nach Empfang von (i) biometrischen Daten, die mit den ersten biometrischen Daten übereinstimmen und (ii) einem privaten Schlüssel, der mit dem ersten privaten Schlüssel übereinstimmt. Das Verifizieren der persönlichen Identität der ersten Person kann das Vergleichen der gespeicherten Informationen mit neu empfangenen Informationen umfassen. Gemäß einigen Implementierungen kann das Identitätssystem **100** so konfiguriert sein, dass die persönliche Identität der ersten Person verifiziert werden kann nach Erhalt von (i) biometrischen Daten, die mit den ersten biometrischen Daten oder den zweiten biometrischen Daten übereinstimmen und (ii) einem privaten Schlüssel, der mit dem ersten privaten Schlüssel übereinstimmt. Solche Implementierungen können sogenannte „M-von-N"-Signaturen zur Identitätsverifizierung bereitstellen, bei denen eine Teilmenge einer größeren Menge von Identifizierungsinformationen benötigt wird.

[0155] Bei einigen Implementierungen kann das System **100** so konfiguriert sein, dass die biometrischen Daten, die mit den ersten biometrischen Daten übereinstimmen, und der private Schlüssel, der mit dem ersten privaten Schlüssel übereinstimmt, verwendet werden können, um den Smart Contract zur Verifizierung der persönlichen Identität der ersten Person zu signieren.

[0156] Bei einigen Implementierungen führt wenigstens ein dedizierter Knoten das Signieren des Smart Contract zum Verifizieren der persönlichen Identität der ersten Person oder des Benutzers durch. Ein gegebener dedizierter Knoten kann einen oder mehrere des/der Server **102** aufweisen. Der gegebene dedizierte Knoten kann ein öffentlicher Knoten oder ein privater Knoten sein, der dazu konfiguriert ist, neue Transaktionen zu erzeugen und/oder die Smart Contracts zur Verifizierung zu signieren.

[0157] **Fig. 16** zeigt einen Überblick **1600** über eine beispielhafte angewandte Blockchain gemäß einer oder mehreren Implementierungen. Wie gezeigt ist, kann eine Datenschutzebene **1602**, die als Erlaubnisverwaltungsebene für Blockchain-Zugriff, Distributed Ledger-Zugriff oder verteilten Datenbankzugriff fungieren kann, verwendet werden. Sie kann zum Beispiel auf einer Ethereum Blockchain, z.B. Blockchain oder einem Hyperledger Distributed Ledger, z.B. Distributed Ledger **1606** zur Führung und Überwachung eingebaut sein. Wie gezeigt ist, kann es einen Mechanismus zum Speichern von Dateien (z.B. biometrische Daten und andere Dateien) geben. Diese Einzelheiten können mit einer Anwendungsprogrammierschnittstelle bzw. Application Programming Interface (API) **1604**, zum Beispiel einer RESTful API, und z.B. einer Blockchain-Datenbank **1608** verbunden sein, um Speicherung, z.B. BigChainDB, bereitzustellen und/oder zu verbessern. Dies kann zum Beispiel unter anderem mit einer biometrischen App und einer Webseite gekoppelt werden. Andere Konfigurationen können verwendet werden.

[0158] Beispielhafte Implementierungen können den Zugriff auf persönliche Daten erleichtern. Es kann mehrere Zugriffsebenen für die persönlichen Daten in der Blockchain geben. Zugriffskontrollen können auf öffentlichen/privaten Schlüsselpaarebenen erteilt werden. Beispiele von Zugriffsebenen können eines oder mehrere aufweisen von Super Admin (voller Zugriff auf Blockchain), Behörden-Landebene (voller Nurlese-Zugriff), Behörden-Staats-/Ortsebene (eingeschränkter Nurlese-Zugriff), Polizei und ande-

re Dienste einschließlich Notdienste (Zugriff auf bestimmte persönliche Daten durch Fingerabdruck/Augenretina ausschließlich von dieser Person), teilnehmende Händler (eingeschränkter Zugriff) und/oder andere Zugriffsebenen.

[0159] Diese Aspekte können sich auf die mobilen Daten beziehen, die verarbeitet, sortiert und/oder in der Blockchain gespeichert werden können (hinsichtlich der biometrischen Identität einer Person und/oder eines Client).

[0160] Obwohl die vorliegende Technologie im Einzelnen zum Zweck der Erläuterung basierend auf dem beschrieben worden ist, was aktuell als die praktischsten und bevorzugtesten Implementierungen angesehen wird, ist es selbstverständlich, dass solche Einzelheiten nur für diesen Zweck bestimmt sind, und dass die Technologie nicht auf die offenbarten Implementierungen beschränkt ist, sondern im Gegenteil beabsichtigt ist, dass sie Modifizierungen und äquivalente Anordnungen umfasst, die im Geist und Umfang der beigefügten Ansprüche liegen. Es ist zum Beispiel selbstverständlich, dass die vorliegende Technologie vorsieht, dass soweit möglich ein oder mehrere Merkmale jeder Implementierung mit einem oder mehreren Merkmalen jeder anderen Implementierung kombiniert werden kann/können.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

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

Zitierte Patentliteratur

- US 9838388 [0005]
- US 2016/0373440 [0005]
- US 2016/0196218 [0019]
- US 2017/0272100 [0019]
- US 8694467 [0019]
- WO 2017/145010 [0020]

Schutzansprüche

1. System zum Bereitstellen einer sicheren Speicherung von elektronischem Material, das aufweist:
einen Hardware-Prozessor (126), der dazu konfiguriert ist, eine Datei mit verständlichen elektronischen Informationen, die zu dem Benutzer gehören, zu empfangen und sicher zu speichern und nach Empfang der Datei mit elektronischen Informationen Fragmente (232, 314, 442) der Datei mit elektronischen Informationen zu bilden, die wenigstens ein erstes Fragment (#1) und ein zweites Fragment (#2) davon aufweisen;
ein verteiltes Datenspeichersystem (234A, 316A, 444A), das mehrere Knoten zum Speichern von Informationsblöcken in einer ersten nicht flüchtigen Speichervorrichtung hat;
eine zweite nicht flüchtige Speichervorrichtung (234B, 316B, 444B), die sich außerhalb des verteilten Datenspeichersystems befindet; und
wobei der Prozessor des Weiteren dazu konfiguriert ist, wenigstens das erste Fragment (#1) der Datei in dem verteilten Datenspeichersystem (234A, 316A, 444A) zu speichern und wenigstens das zweite Fragment (#2) der Datei außerhalb des verteilten Datenspeichersystems (234B, 316B, 444B) zu speichern.

2. System nach Anspruch 1, wobei der Prozessor dazu konfiguriert ist, eine Abbildungsdatei zu erzeugen, um Speicherstellendaten für das wenigstens eine erste Fragment und das wenigstens eine zweite Fragment der Datei zu speichern, einschließlich Zusammensetzungsdaten für das wenigstens eine erste Fragment und das wenigstens eine zweite Fragment der Datei, und die Abbildungsdatei oder wenigstens einen Teil der Abbildungsdatei in einem Distributed Ledger-Speicher zu speichern.

3. System nach Anspruch 1, wobei jedes der Fragmente der Datei unverständlich ist, wenn es nicht teilweise oder vollständig wieder zu der Datei zusammengesetzt ist.

4. System nach Anspruch 1, wobei der Prozessor dazu konfiguriert ist, als elektronische Information eine digitale biometrische Datei zu empfangen, die wenigstens einige biometrische Informationen enthält, die zu dem Benutzer gehören.

5. System nach Anspruch 1, wobei der Prozessor dazu konfiguriert ist, als Datei eine digitale Datei zu empfangen, die zu dem Benutzer gehört.

6. System nach Anspruch 1, wobei das verteilte Datenspeichersystem ein vertrauenswürdiges Dienstprogramm bzw. eine Trust Utility zum Speichern unveränderlicher Daten ist.

7. System nach Anspruch 1, wobei der Prozessor dazu konfiguriert ist, als elektronische Information eine Grafik- oder Bilddatei zu empfangen, die zu dem Benutzer gehört, und die Grafik oder das Bild in einen Satz von Merkmalsblöcken aufzuteilen, eine Abbildungsdatei zu erzeugen, um die Speicherstelle der Merkmalsblöcke, die die Grafik oder das Bild ergeben, abzubilden, wenigstens einen ersten der Merkmalsblöcke in dem verteilten Datenspeichersystem zu speichern, und wenigstens einen zweiten der Merkmalsblöcke außerhalb des verteilten Datenspeichersystems zu speichern.

8. System nach Anspruch 7, wobei der Prozessor dazu konfiguriert ist, wenigstens den ersten und den zweiten der Merkmalsblöcke vor dem Speichern des ersten und des zweiten der Merkmalsblöcke zu transformieren und die Transformationen in der Abbildungsdatei zu speichern.

9. System nach Anspruch 8, wobei der Prozessor dazu konfiguriert ist, die Abbildungsdatei in wenigstens ein erstes Abbildungsdatei-Fragment und ein zweites Abbildungsdatei-Fragment aufzuteilen, wenigstens das erste Abbildungsdatei-Fragment in dem verteilten Datenspeichersystem zu speichern und wenigstens das zweite Abbildungsdatei-Fragment außerhalb des verteilten Datenspeichersystems zu speichern.

10. System nach Anspruch 8, wobei der Prozessor dazu konfiguriert ist, wenigstens den ersten der Merkmalsblöcke und wenigstens den zweiten der Merkmalsblöcke zu verschlüsseln.

11. System nach Anspruch 9, wobei der Prozessor dazu konfiguriert ist, wenigstens den ersten der Merkmalsblöcke und wenigstens den zweiten der Merkmalsblöcke zu verschlüsseln.

12. System nach Anspruch 8, wobei der Prozessor dazu konfiguriert ist, wenigstens die Abbildungsdatei zu verschlüsseln.

13. System nach Anspruch 8, wobei der Satz von Merkmalsblöcken eine Teilmenge der Merkmalsblöcke ist, die die Grafik oder das Bild bilden.

14. System nach Anspruch 8, wobei die Grafik- oder Bilddatei eine Datei ist, die wenigstens einige biometrische Informationen enthält, die zu dem Benutzer gehören.

15. System nach Anspruch 13, wobei der Prozessor dazu konfiguriert ist, die Teilmenge der Merkmalsblöcke zu verschlüsseln, die verschlüsselte Teilmenge von Merkmalsblöcken in wenigstens ein erstes Fragment und ein zweites Fragment zu zerlegen und wenigstens das erste Fragment in dem verteilten Datenspeichersystem zu speichern und wenigstens das zweite Fragment außerhalb des verteilten Datenspeichersystems zu speichern.

16. System nach Anspruch 13, wobei der Prozessor dazu konfiguriert ist, einen Hash der Teilmenge der biometrischen Grafik zu erzeugen und wenigstens einen Teil des Hashes in dem verteilten Datenspeichersystem zu speichern und wenigstens einen anderen Teil des Hashes außerhalb des verteilten Datenspeichersystems zu speichern.

17. System nach Anspruch 15, wobei der Prozessor dazu konfiguriert ist, im Ansprechen auf eine Benutzeranfrage zum Zugriff auf gespeicherte Informationen in dem System, das zu dem Benutzer gehört, den Benutzer vor dem Bewilligen des Zugriffs zu authentifizieren, was das Vergleichen wenigstens eines Teils eines Hashes einer biometrischen Grafikdatei, die durch das System von dem Benutzer neu empfangen worden ist, mit einem Hash beinhaltet, der von dem wenigstens ersten Fragment von dem verteilten Datenspeichersystem erhalten worden ist und dem wenigstens zweiten Fragment von außerhalb des verteilten Datenspeichersystems, wobei eine positive Übereinstimmung als wenigstens ein Teil des Authentifizierens des Benutzers erforderlich ist, und wobei der Prozessor dazu konfiguriert ist, im Ansprechen auf eine Benutzeranfrage zum Zugriff auf gespeicherte Informationen in dem System, das zu dem Benutzer gehört, den Benutzer vor dem Bewilligen des Zugriffs zu authentifizieren, was das Vergleichen der Teilmenge der Merkmalsblöcke der biometrischen Grafik mit einer Datei entsprechend einer Teilmenge von Merkmalsblöcken einer neu empfangenen biometrischen Datei durch das System von dem Benutzer beinhaltet, wobei eine positive Übereinstimmung als wenigstens ein Teil des Authentifizierens des Benutzers erforderlich ist.

18. System nach Anspruch 13, wobei die Teilmenge der Merkmalsblöcke entweder fortlaufende Blöcke aus der biometrischen Grafik oder nicht fortlaufende Blöcke sind, die zusammen gruppiert sind.

19. System nach Anspruch 13, wobei Merkmalsblöcke in der Teilmenge der Merkmalsblöcke vor dem Speichern transformiert werden.

20. System nach Anspruch 7, wobei der Prozessor dazu konfiguriert ist, eine zweite Grafik- oder Bilddatei, die zu dem Benutzer gehört, zu speichern und die Grafik oder das Bild in der zweiten Grafik- oder Bilddatei in einen Satz von Merkmalsblöcken aufzuteilen, eine Abbildungsdatei zu erzeugen, um die Speicherstelle der Merkmalsblöcke, die die Grafik oder das Bild ergeben, abzubilden, wenigstens einen ersten der Merkmalsblöcke in dem verteilten Datenspeichersystem zu speichern und wenigstens einen zweiten der Merkmalsblöcke außerhalb des verteilten Datenspeichersystems zu speichern.

21. System nach Anspruch 17, wobei der Prozessor dazu konfiguriert ist, eine zweite Grafik- oder Bilddatei, die zu dem Benutzer gehört, zu speichern und die Grafik oder das Bild in der zweiten Grafik- oder Bilddatei in einen Satz von Merkmalsblöcken aufzuteilen, eine Abbildungsdatei zu erzeugen, um die Speicherstelle der Merkmalsblöcke, die die Grafik oder das Bild ergeben, abzubilden, wenigstens einen ersten der Merkmalsblöcke in dem verteilten Datenspeichersystem zu speichern und wenigstens einen zweiten der Merkmalsblöcke außerhalb des verteilten Datenspeichersystems zu speichern.

22. System nach Anspruch 1, wobei der Prozessor des Weiteren durch die maschinenlesbaren Befehle dazu konfiguriert ist, eine Indexdatei darüber zu erzeugen, wie die Fragmente wieder zusammenpassen, um die Datei wieder zusammenzusetzen.

23. System nach Anspruch 22, wobei der Prozessor des Weiteren dazu konfiguriert ist, Fragmente der Indexdatei zu bilden, die wenigstens ein erstes Fragment und ein zweites Fragment davon aufweisen;
wenigstens das erste Fragment der Indexdatei in einem verteilten Datenspeichersystem zu speichern; und
wenigstens das zweite Fragment der Indexdatei außerhalb des verteilten Datenspeichersystems zu speichern.

24. System nach Anspruch 1, wobei die Prozessoren des Weiteren dazu konfiguriert sind, wenigstens ein drittes Fragment der Datei zu bilden und das dritte Fragment in dem verteilten Datenspeichersystem getrennt von dem in dem verteilten Datenspeichersystem gespeicherten ersten Fragment zu speichern.

25. System nach Anspruch 1, wobei die Prozessoren des Weiteren dazu konfiguriert sind, wenigstens das erste Fragment als Transaktion in dem verteilten Datenspeichersystem zu speichern.

26. System nach Anspruch 24, wobei der Prozessor des Weiteren dazu konfiguriert ist, wenigstens das erste Fragment und das dritte Fragment als separate Transaktionen in dem verteilten Datenspeichersystem zu speichern.

27. System nach Anspruch 1, wobei der Prozessor des Weiteren durch die maschinenlesbaren Befehle dazu konfiguriert ist, die Datei aus den Dateifragmenten im Ansprechen auf eine Anfrage von dem Benutzer wieder zusammenzusetzen.

28. System nach Anspruch 1, wobei der Prozessor des Weiteren durch die maschinenlesbaren Befehle dazu konfiguriert ist, das erste Dateifragment mit wenigstens einem Abschnitt des Datei-Headers zu bilden.

29. System nach Anspruch 1, wobei der äußere verteilte Datenspeicher eine digitale Speichervorrichtung ohne eigenen Hauptprozessor ist.

30. System nach Anspruch 1, wobei der verteilte Datenspeicher ein dezentraler Kontobuchspeicher bzw. Ledger-Speicher ist.

Es folgen 19 Seiten Zeichnungen

Anhängende Zeichnungen

FIG. 1

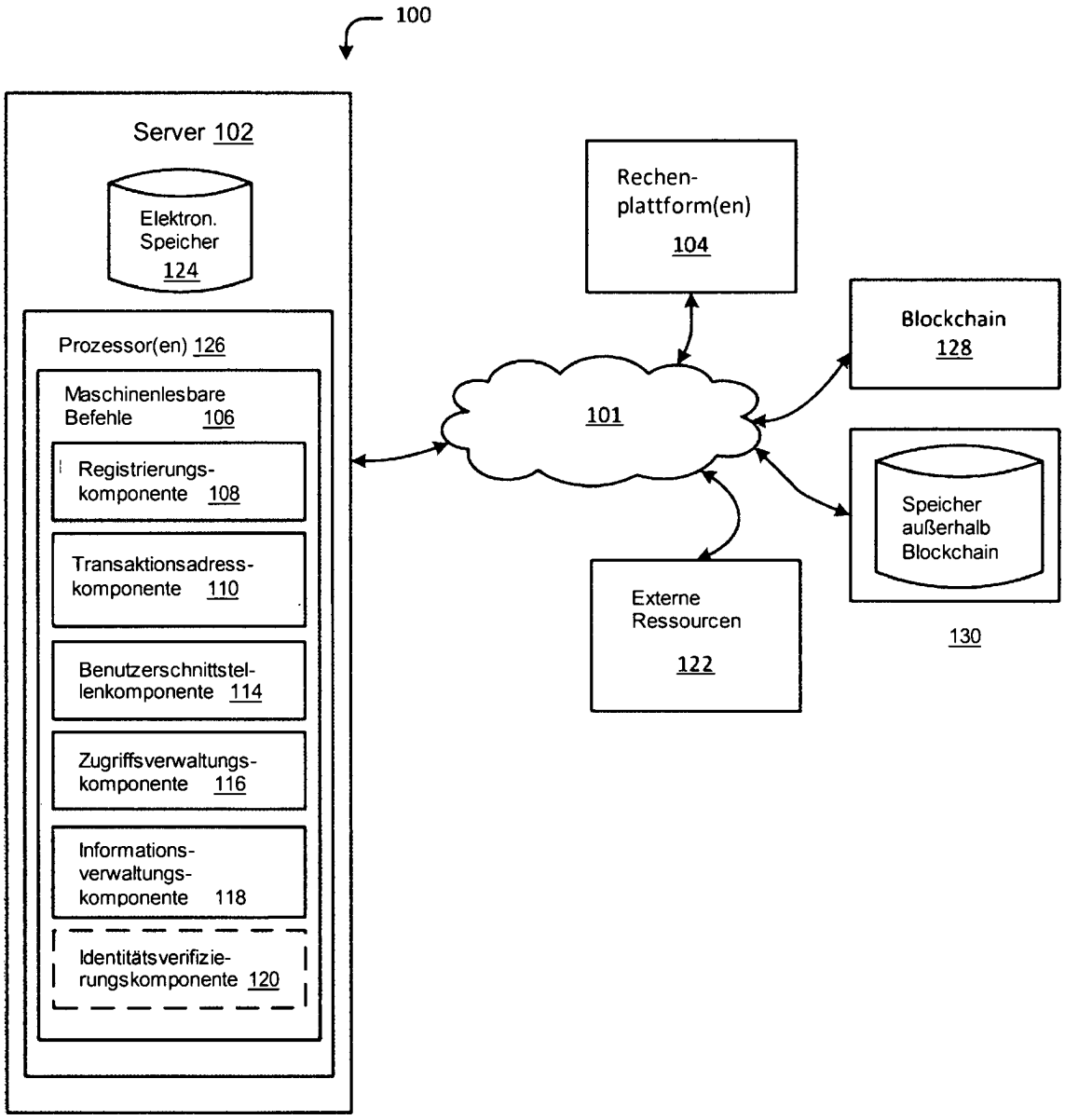
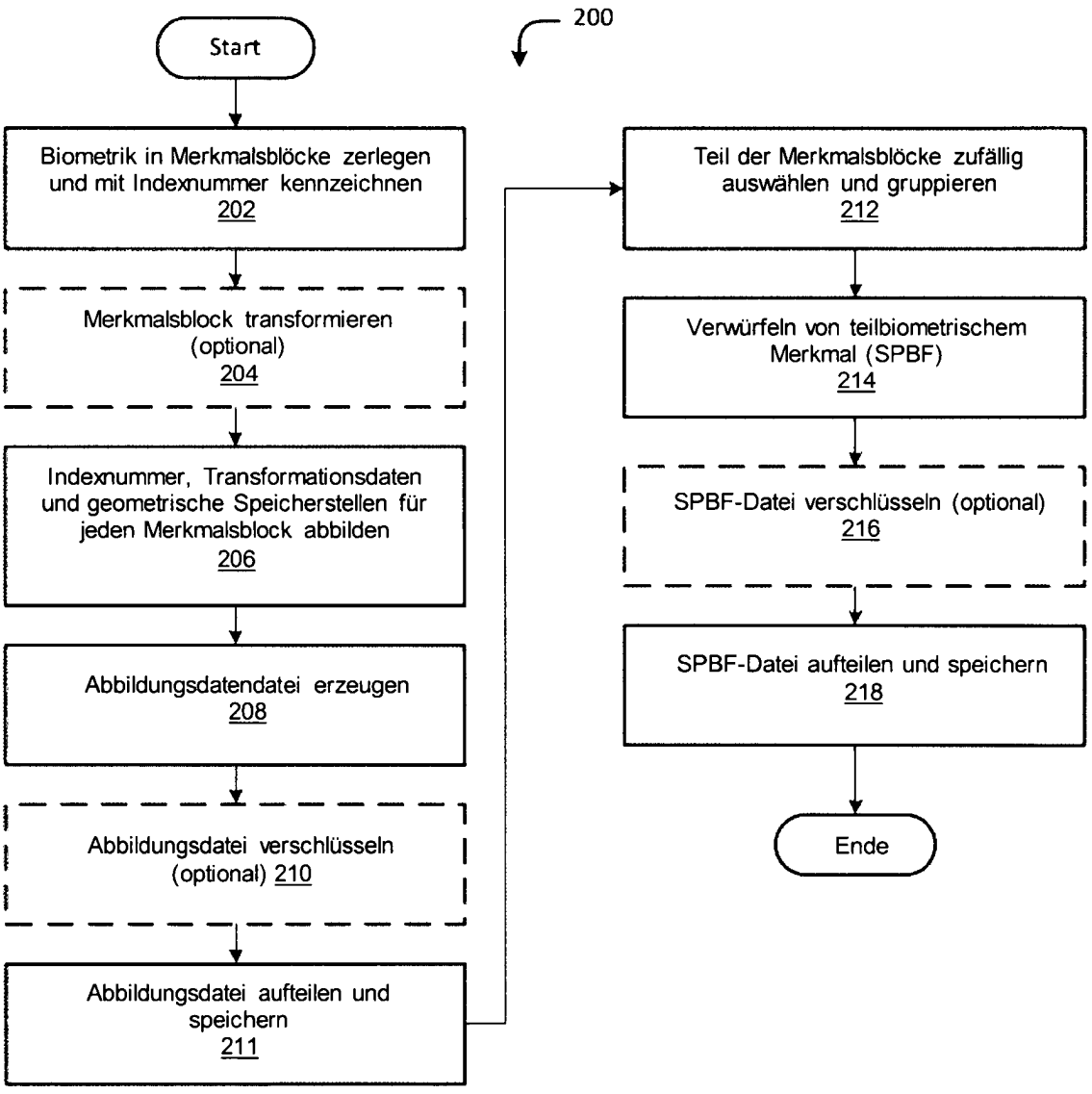


FIG. 2


200
Start
Biometrik in Merkmalsblöcke zerlegen und mit Indexnummer kennzeichnen 202
Merkmalsblock transformieren (optional) 204
Indexnummer, Transformationsdaten und geometrische Speicherstellen für jeden Merkmalsblock abbilden 206
Abbildungsdatendatei erzeugen 208
Abbildungsdatei verschlüsseln (optional) 210
Abbildungsdatei aufteilen und speichern 211
Teil der Merkmalsblöcke zufällig auswählen und gruppieren 212
Verwürfeln von teilbiometrischem Merkmal (SPBF) 214
SPBF-Datei verschlüsseln (optional) 216
SPBF-Datei aufteilen und speichern 218
Ende

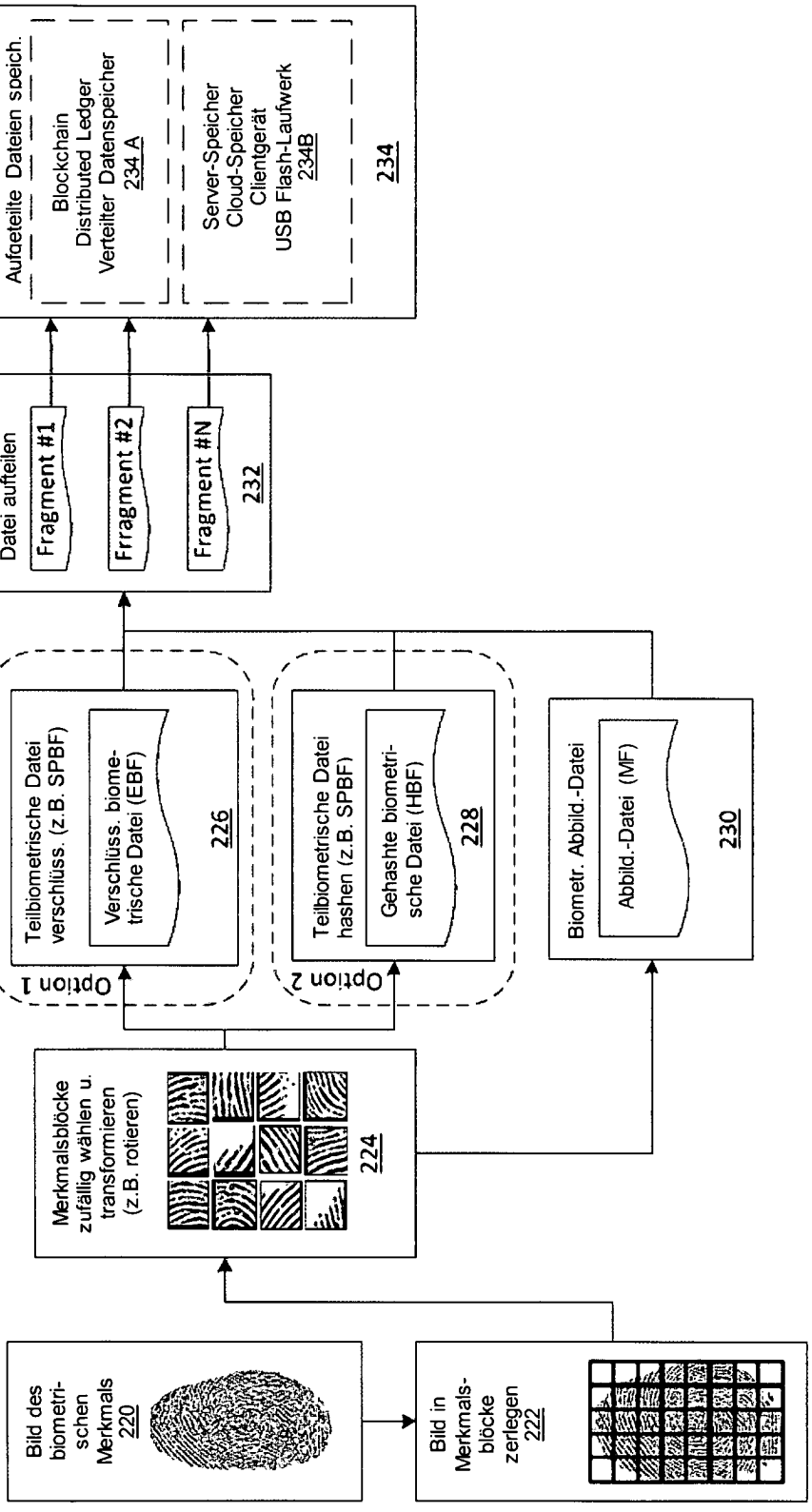


Bild des biometrischen Merkmals 220
Bild in Merkmalsblöcke zerlegen 222
Merkmalsblöcke zufällig wählen u. transformieren (z.B. rotieren)
224
Option 1
Teilbiometrische Datei verschlüss. (z.B. SPBF)
Verschlüss. biometrische Datei (EBF)
226
Option 2
Teilbiometrische Datei hashen (z.B. SPBF)
Gehashte biometrische Datei (HBF)
228
Biometr. Abbild.-Datei
Abbild.-Datei (MF)
230
Datei aufteilen
Fragment #1
Fragment #2
Fragment #N
232
Aufgeteilte Dateien speich.
Blockchain
Distributed Ledger
Verteilter Datenspeicher
234 A
Server-Speicher
Cloud-Speicher
Clientgerät
USB Flash-Laufwerk
234B
234

FIG. 2A

FIG. 3

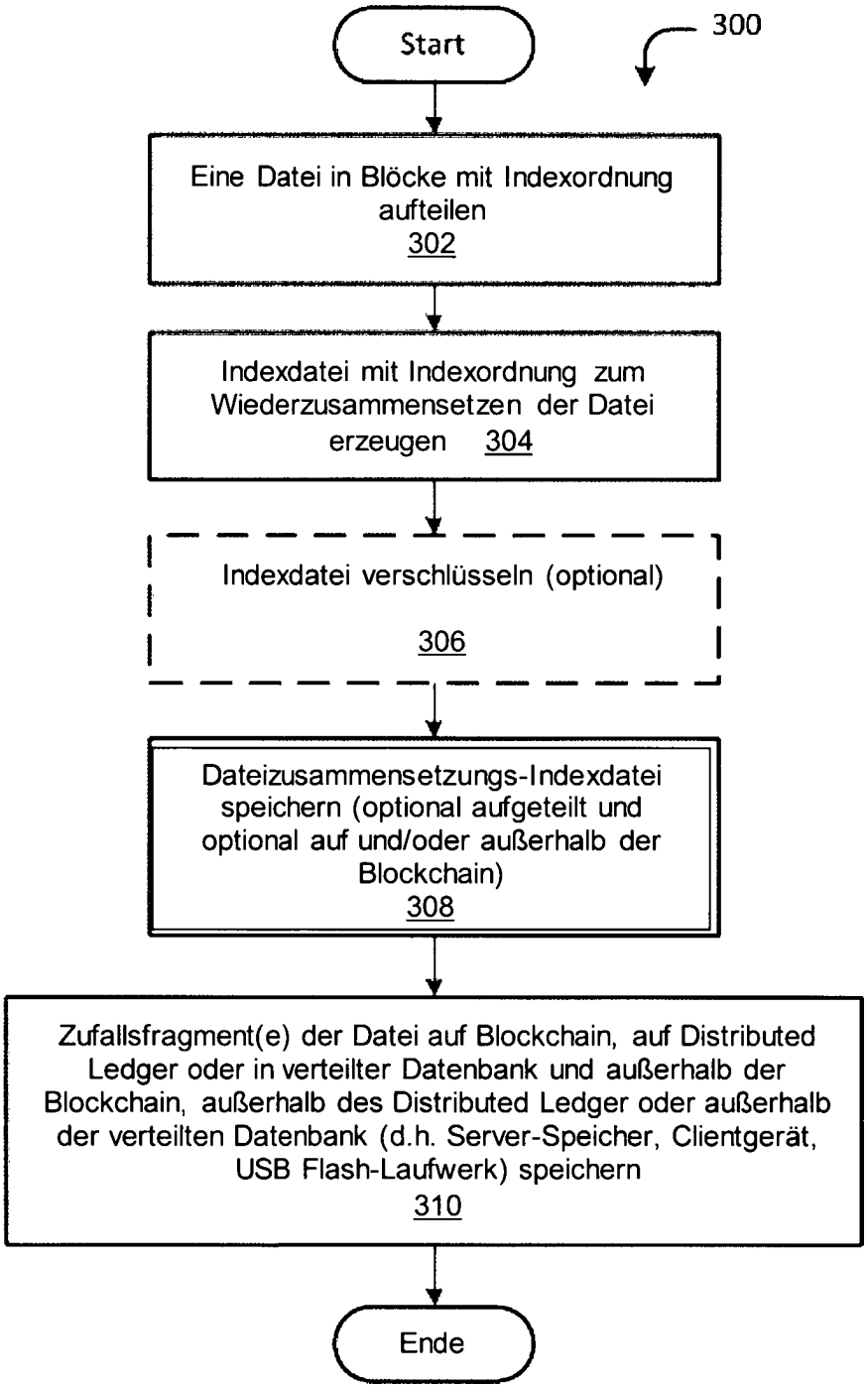

Start
300
Eine Datei in Blöcke mit Indexordnung aufteilen
302
Indexdatei mit Indexordnung zum Wiederzusammensetzen der Datei erzeugen 304
Indexdatei verschlüsseln (optional)
306
Dateizusammensetzungs-Indexdatei speichern (optional aufgeteilt und optional auf und/oder außerhalb der Blockchain)
308
Zufallsfragment(e) der Datei auf Blockchain, auf Distributed Ledger oder in verteilter Datenbank und außerhalb der Blockchain, außerhalb des Distributed Ledger oder außerhalb der verteilten Datenbank (d.h. Server-Speicher, Clientgerät, USB Flash-Laufwerk) speichern
310
Ende

FIG. 3A

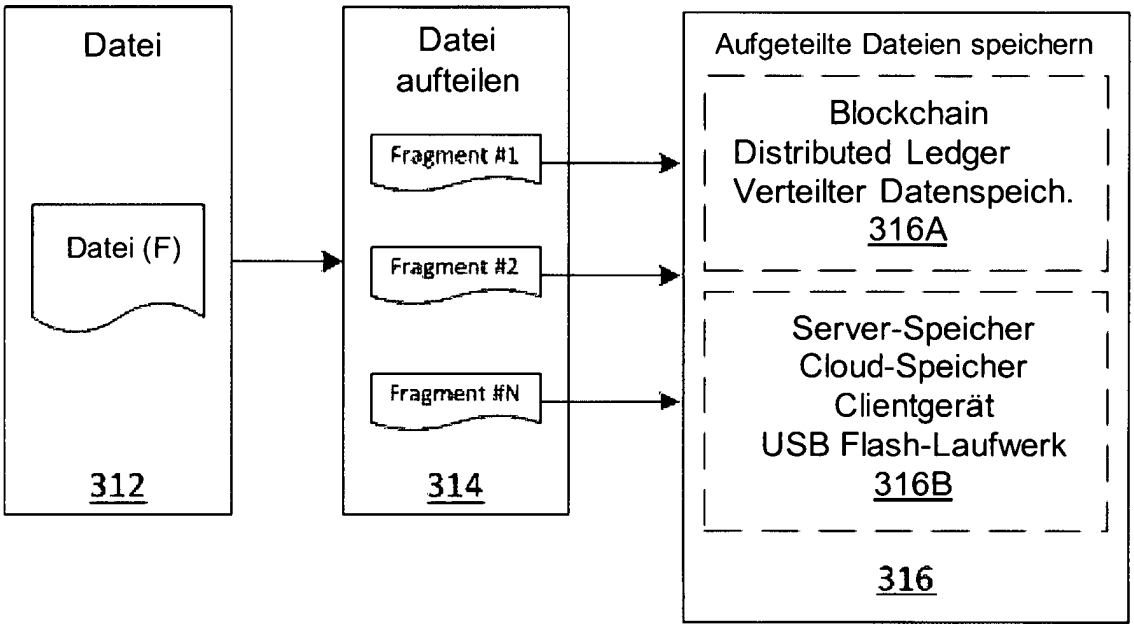
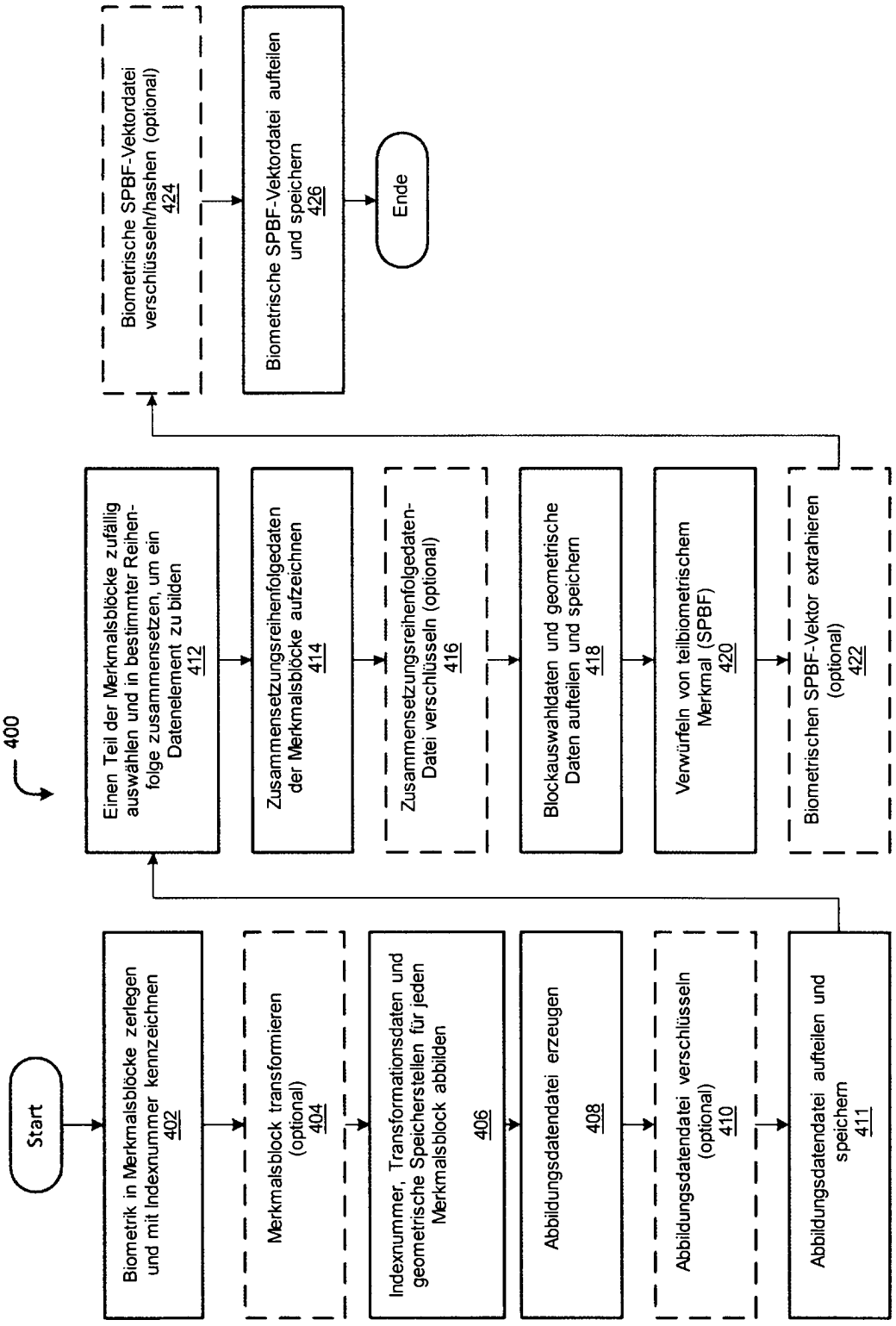

Datei
Datei (F)
312
Datei aufteilen
Fragment #1
Fragment #2
Fragment #N
314
Aufgeteilte Dateien speichern
Blockchain
Distributed Ledger
Verteilter Datenspeich.
316A
Server-Speicher
Cloud-Speicher
Clientgerät
USB Flash-Laufwerk
316B
316

FIG. 4


400
Start
Biometrik in Merkmalsblöcke zerlegen und mit Indexnummer kennzeichnen 402
Merkmalsblock transformieren (optional) 404
Indexnummer, Transformationsdaten und geometrische Speicherstellen für jeden Merkmalsblock abbilden 406
Abbildungsdatendatei erzeugen 408
Abbildungsdatendatei verschlüsseln (optional) 410
Abbildungsdatendatei aufteilen und speichern 411
Einen Teil der Merkmalsblöcke zufällig auswählen und in bestimmter Reihenfolge zusammensetzen, um ein Datenelement zu bilden 412
Zusammensetzungsreihenfolgedaten der Merkmalsblöcke aufzeichnen 414
Zusammensetzungsreihenfolgedaten-Datei verschlüsseln (optional) 416
Blockauswahldaten und geometrische Daten aufteilen und speichern 418
Verwürfeln von teilbiometrischem Merkmal (SPBF) 420
Biometrischen SPBF-Vektor extrahieren (optional) 422
Biometrische SPBF-Vektordatei verschlüsseln/hashen (optional) 424
Biometrische SPBF-Vektordatei aufteilen und speichern 426
Ende

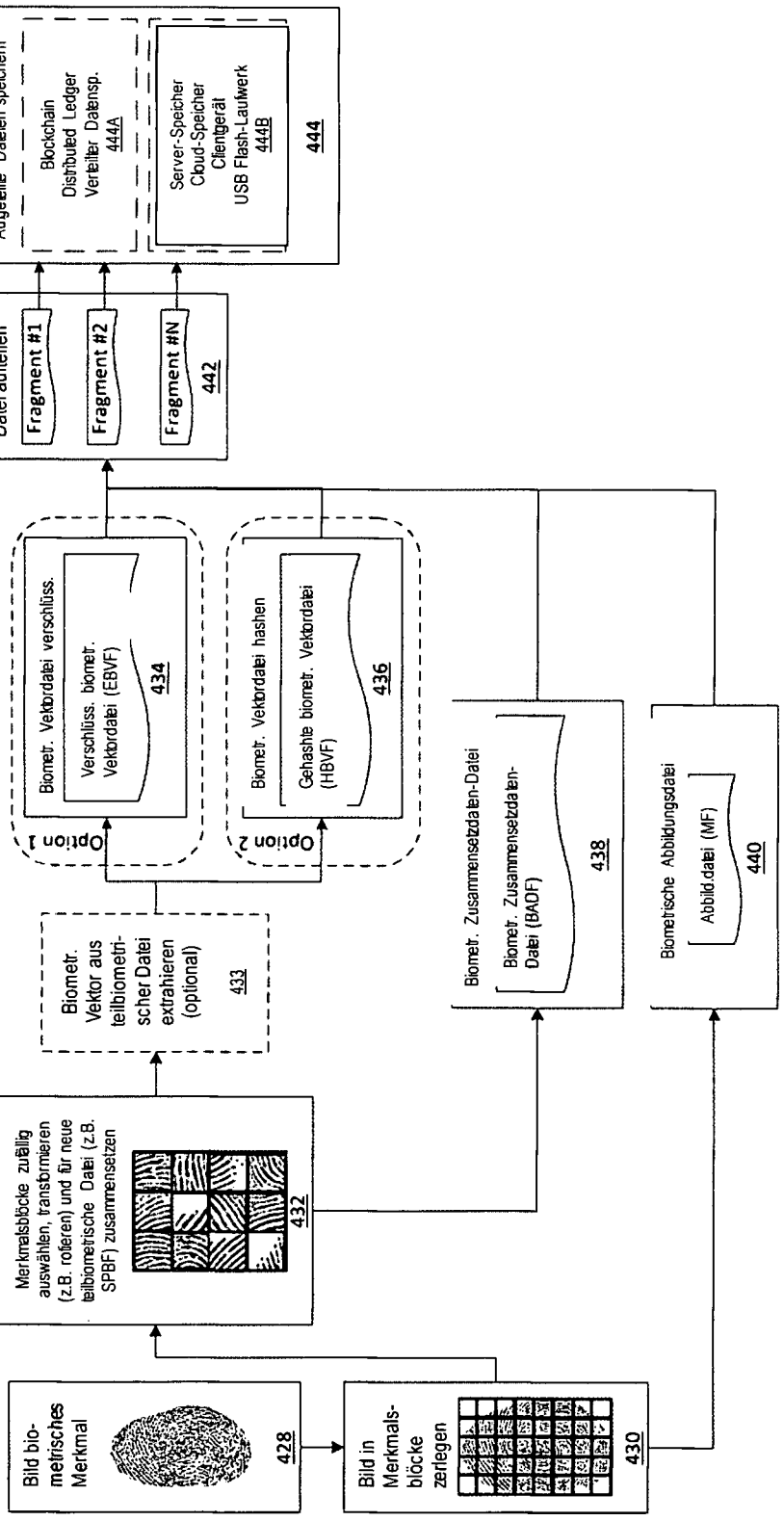


Bild biometrisches Merkmal
428
Bild in Merkmalsblöcke zerlegen
430
Merkmalsblöcke zufällig auswählen, transformieren (z.B. roferen) und für neue teilbiometrische Datei (z.B. SPBF) zusammensetzen
432
Biometr. Vektor aus teilbiometrischer Datei extrahieren (optional)
433
Option 1
Biometr. Vektordatei verschlüss.
Verschlüss. biometr. Vektordatei (EBVF)
434
Option 2
Biometr. Vektordatei hashen
Gehashte biometr. Vektordatei (HBVF)
436
Biometr. Zusammensetzdaten-Datei
Biometr. Zusammensetzdaten-Datei (BADF)
438
Biometrische Abbildungsdatei
Abbild.datei (MF)
440
Datei aufteilen
Fragment #1
Fragment #2
Fragment #N
442
Aufgeteilte Dateien speichern
Blockchain
Distributed Ledger
Verteilter Datensp.
444A
Server-Speicher
Cloud-Speicher
Clientgerät
USB Flash-Laufwerk
444B
444

FIG. 4A

FIG. 5

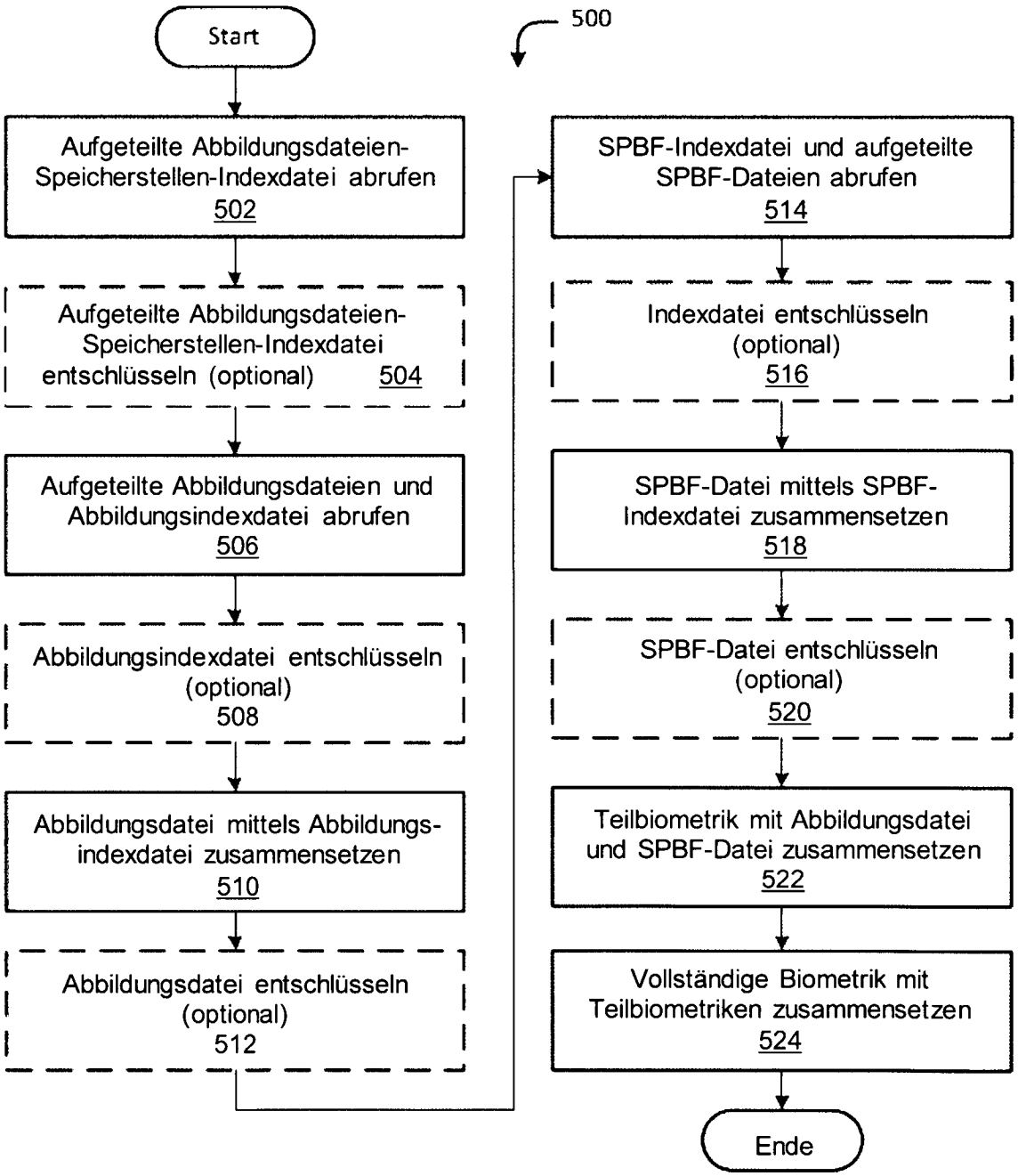

Start
500
Aufgeteilte Abbildungsdateien-Speicherstellen-Indexdatei abrufen 502
Aufgeteilte Abbildungsdateien-Speicherstellen-Indexdatei entschlüsseln (optional) 504
Aufgeteilte Abbildungsdateien und Abbildungsindexdatei abrufen 506
Abbildungsindexdatei entschlüsseln (optional) 508
Abbildungsdatei mittels Abbildungs-indexdatei zusammensetzen 510
Abbildungsdatei entschlüsseln (optional) 512
SPBF-Indexdatei und aufgeteilte SPBF-Dateien abrufen 514
Indexdatei entschlüsseln (optional) 516
SPBF-Datei mittels SPBF-Indexdatei zusammensetzen 518
SPBF-Datei entschlüsseln (optional) 520
Teilbiometrik mit Abbildungsdatei und SPBF-Datei zusammensetzen 522
Vollständige Biometrik mit Teilbiometriken zusammensetzen 524
Ende

FIG. 6

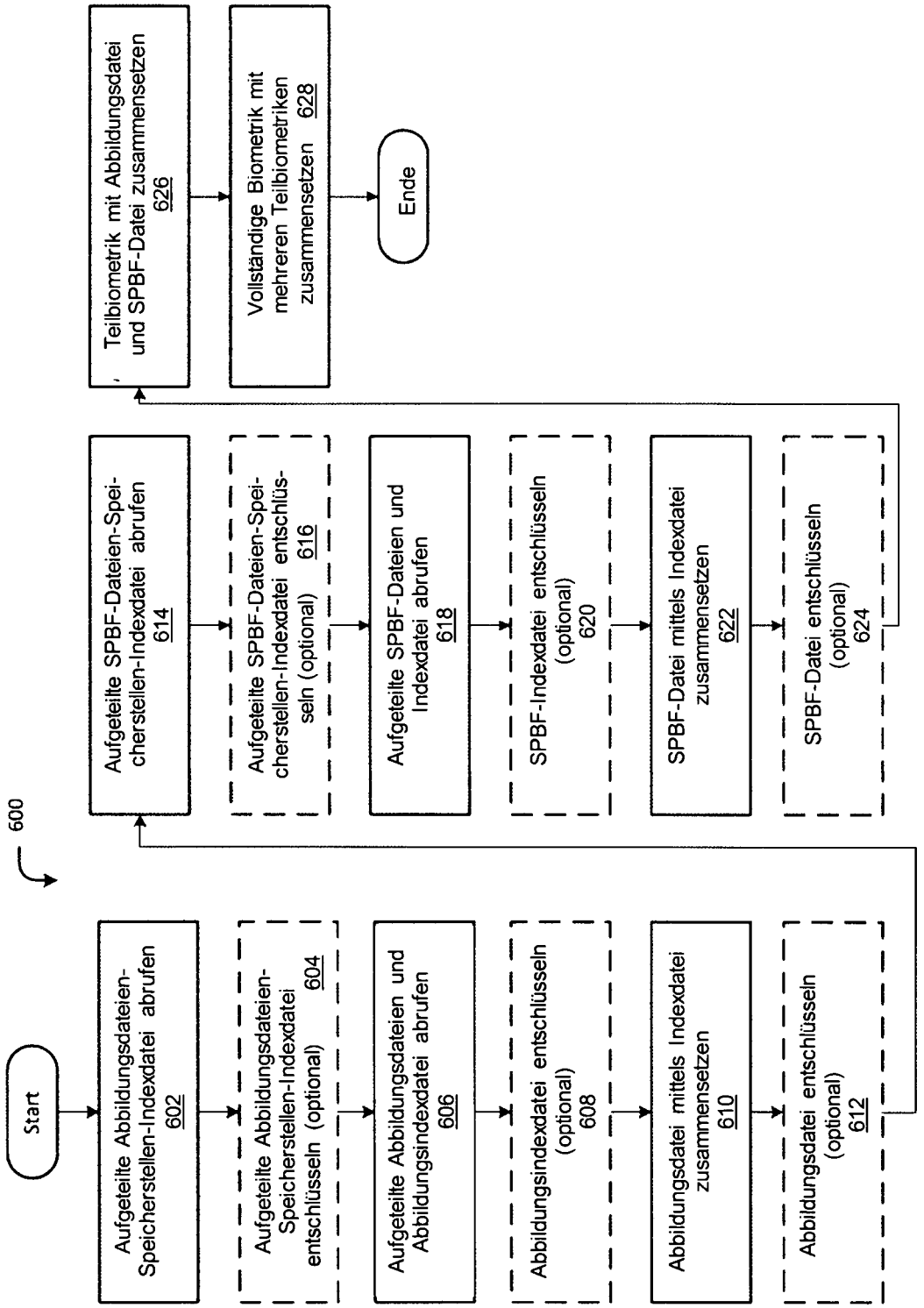

600
Start
Aufgeteilte Abbildungsdateien-Speicherstellen-Indexdatei abrufen 602
Aufgeteilte Abbildungsdateien-Speicherstellen-Indexdatei entschlüsseln (optional) 604
Aufgeteilte Abbildungsdateien und Abbildungsindexdatei abrufen 606
Abbildungsindexdatei entschlüsseln (optional) 608
Abbildungsdatei mittels Indexdatei zusammensetzen 610
Abbildungsdatei entschlüsseln (optional) 612
Aufgeteilte SPBF-Dateien-Speicherstellen-Indexdatei abrufen 614
Aufgeteilte SPBF-Dateien-Speicherstellen-Indexdatei entschlüsseln (optional) 616
Aufgeteilte SPBF-Dateien und Indexdatei abrufen 618
SPBF-Indexdatei entschlüsseln (optional) 620
SPBF-Datei mittels Indexdatei zusammensetzen 622
SPBF-Datei entschlüsseln (optional) 624
Teilbiometrik mit Abbildungsdatei und SPBF-Datei zusammensetzen 626
Vollständige Biometrik mit mehreren Teilbiometriken zusammensetzen 628
Ende

FIG. 7

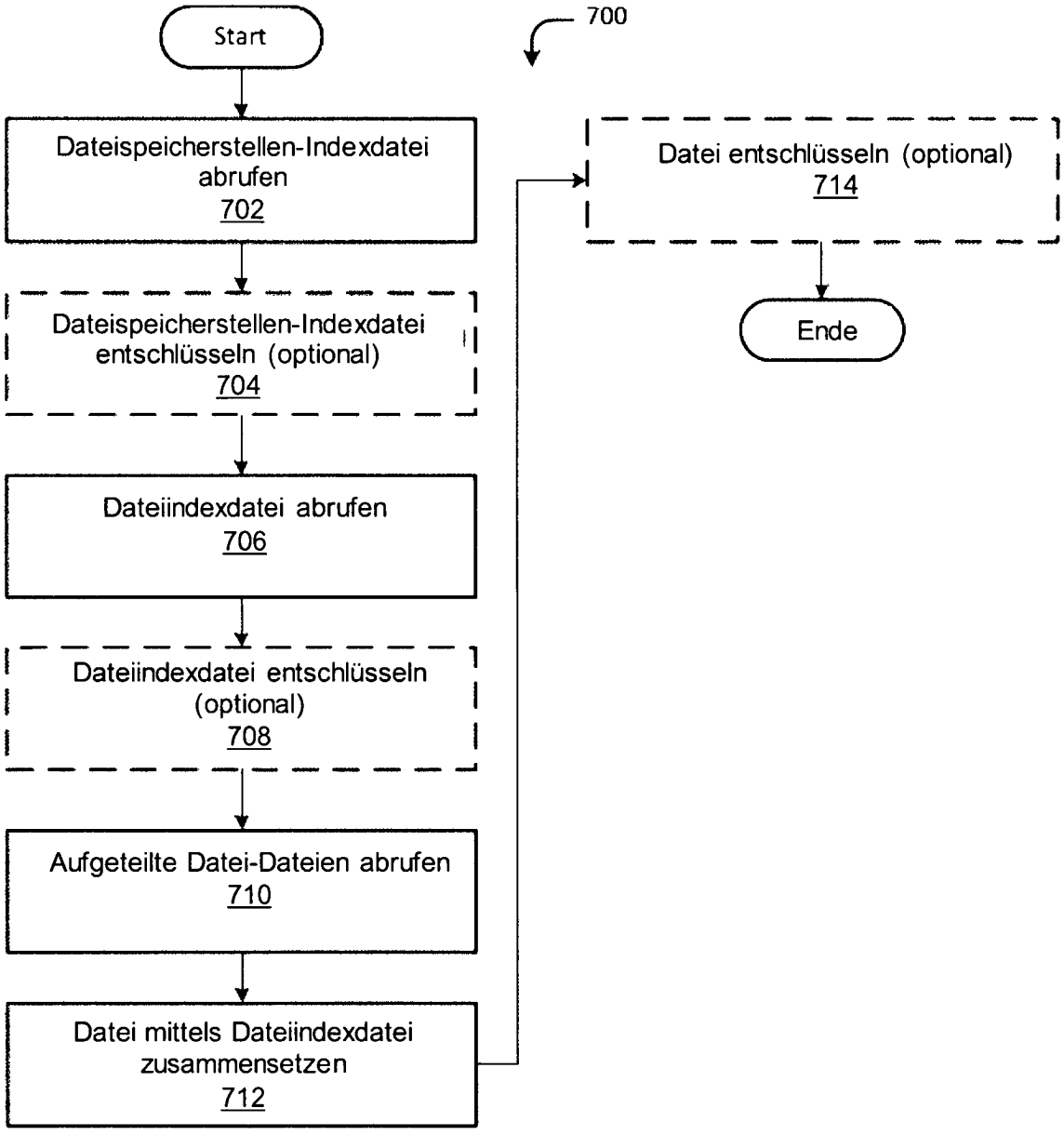

Start
700
Dateispeicherstellen-Indexdatei abrufen
702
Dateispeicherstellen-Indexdatei entschlüsseln (optional)
704
Dateiindexdatei abrufen
706
Dateiindexdatei entschlüsseln (optional)
708
Aufgeteilte Datei-Dateien abrufen
710
Datei mittels Dateiindexdatei zusammensetzen
712
Datei entschlüsseln (optional)
714
Ende

FIG. 8

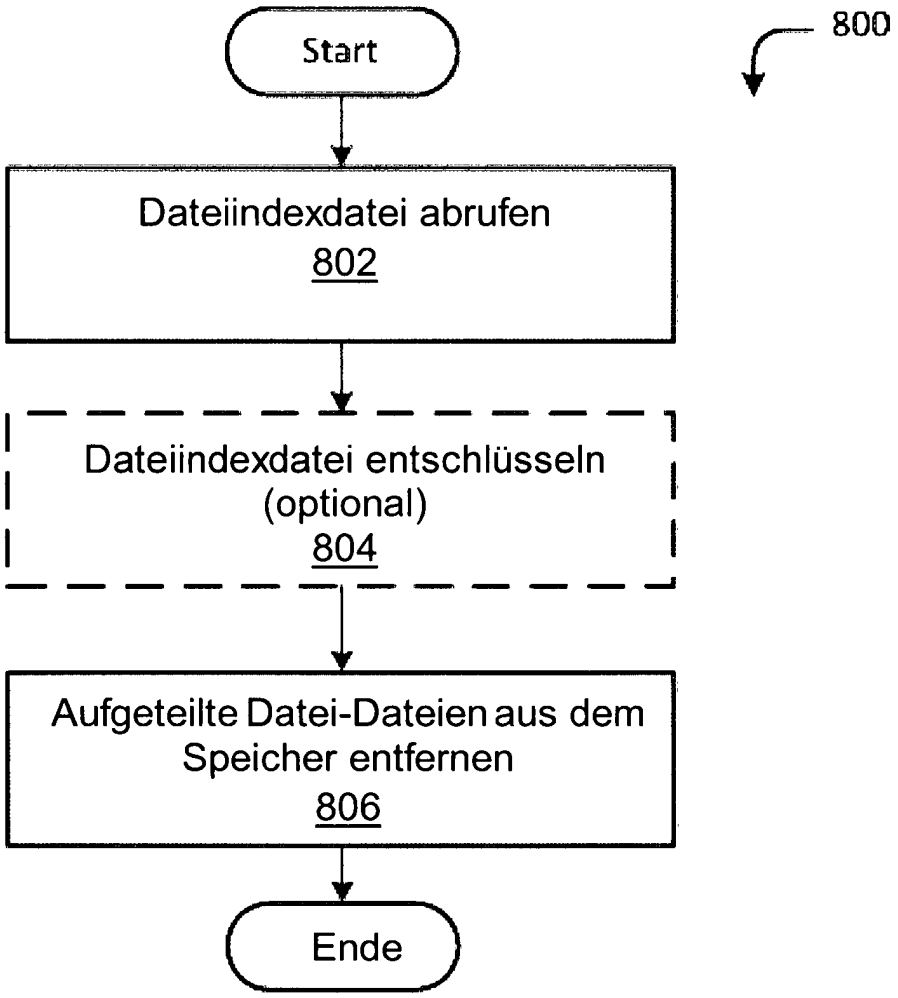

800
Start
Dateiindexdatei abrufen
802
Dateiindexdatei entschlüsseln
(optional)
804
Aufgeteilte Datei-Dateien aus dem
Speicher entfernen
806
Ende

FIG. 9

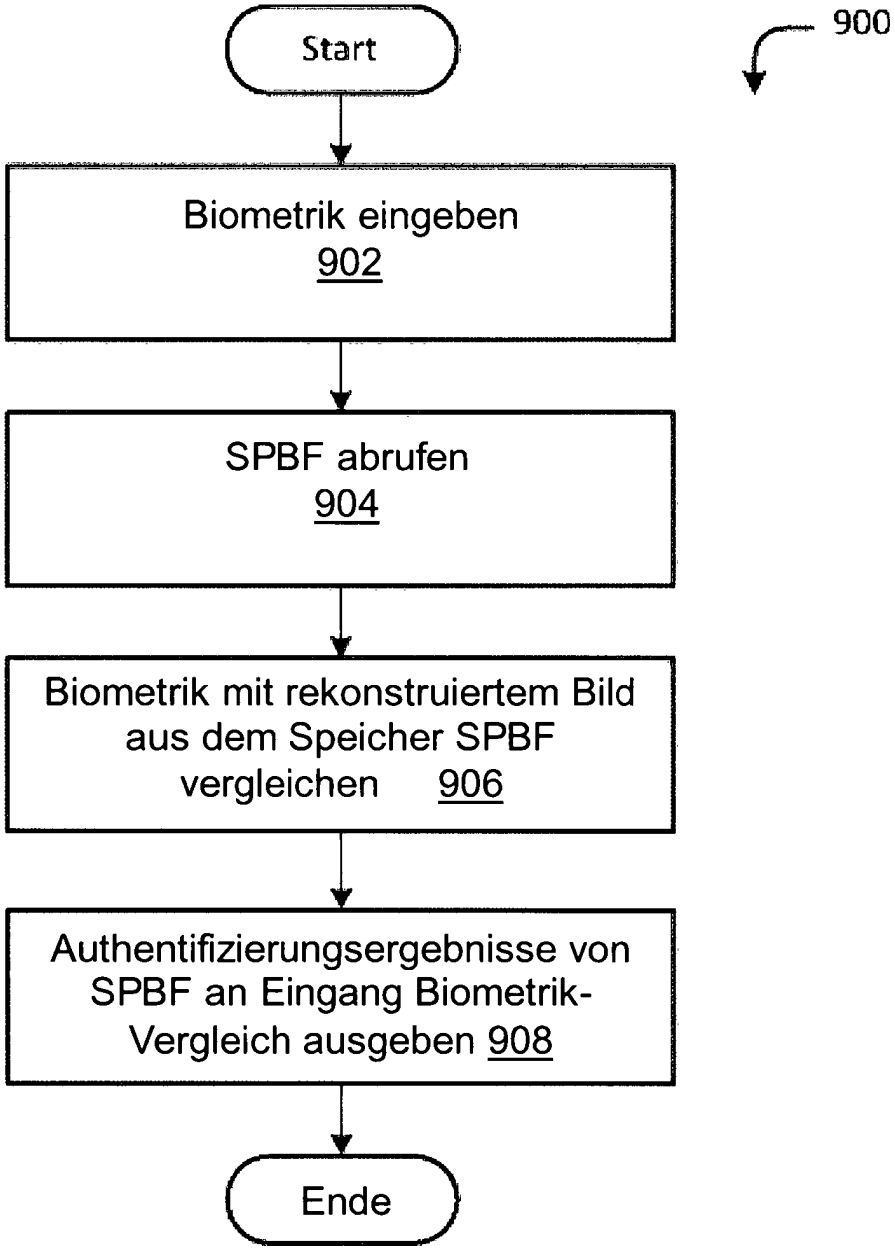

900
Start
Biometrik eingeben
902
SPBF abrufen
904
Biometrik mit rekonstruiertem Bild aus dem Speicher SPBF vergleichen 906
Authentifizierungsergebnisse von SPBF an Eingang Biometrik-Vergleich ausgeben 908
Ende

FIG. 10

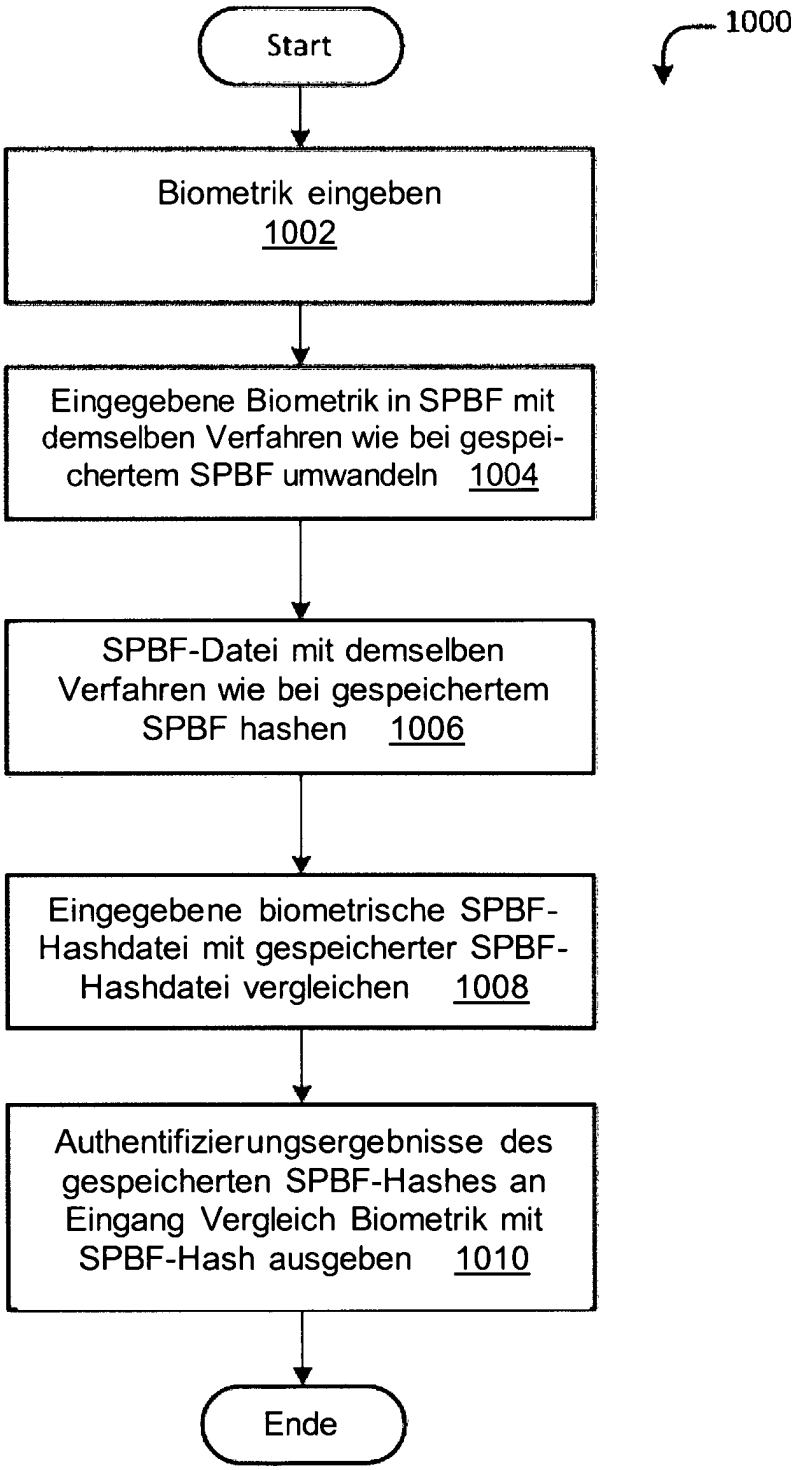

Start
1000
Biometrik eingeben
1002
Eingegebene Biometrik in SPBF mit demselben Verfahren wie bei gespeichertem SPBF umwandeln 1004
SPBF-Datei mit demselben Verfahren wie bei gespeichertem SPBF hashen 1006
Eingegebene biometrische SPBF-Hashdatei mit gespeicherter SPBF-Hashdatei vergleichen 1008
Authentifizierungsergebnisse des gespeicherten SPBF-Hashes an Eingang Vergleich Biometrik mit SPBF-Hash ausgeben 1010
Ende

FIG. 11

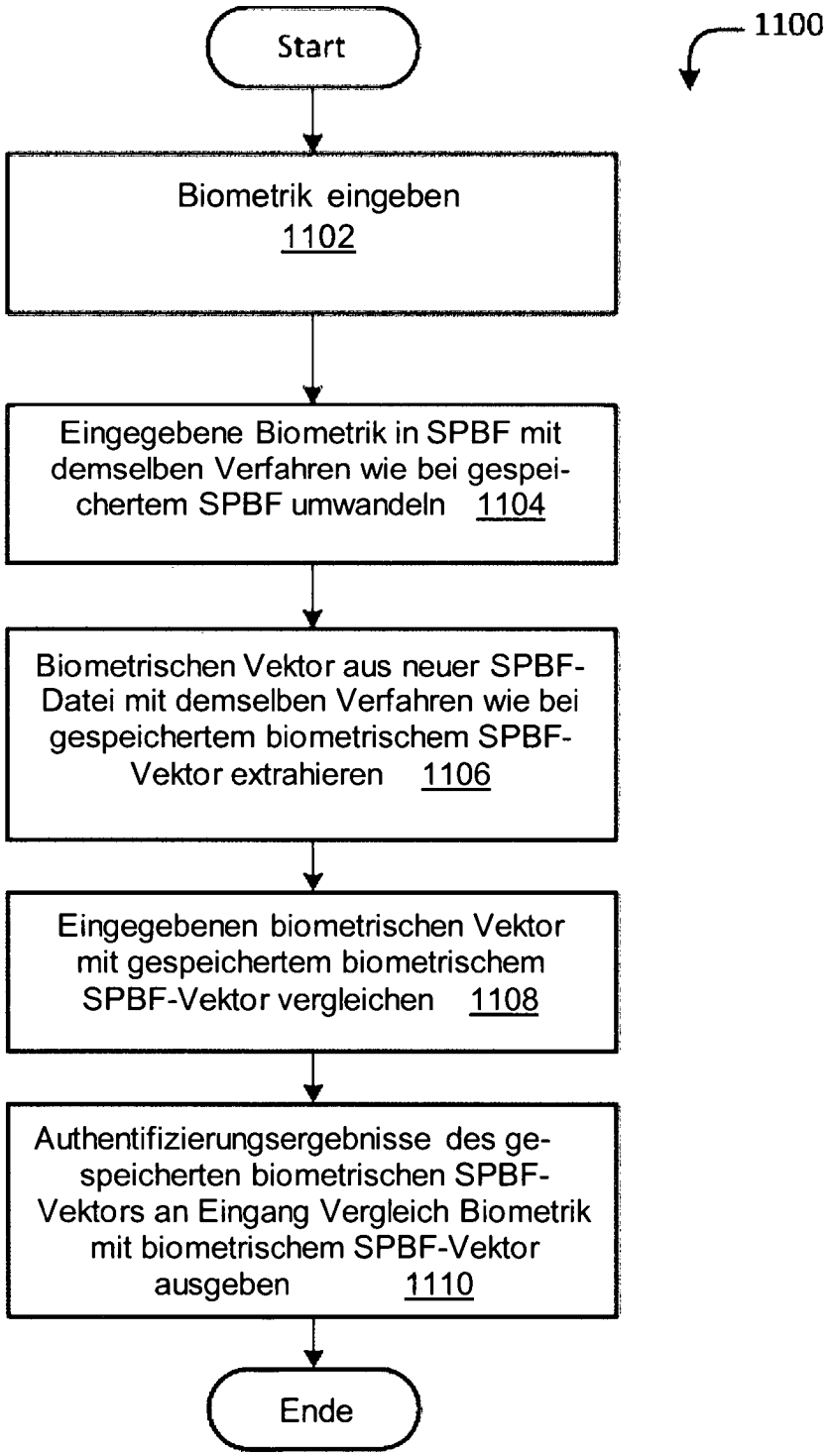

1100
Start
Biometrik eingeben
1102
Eingegebene Biometrik in SPBF mit demselben Verfahren wie bei gespeichertem SPBF umwandeln 1104
Biometrischen Vektor aus neuer SPBF-Datei mit demselben Verfahren wie bei gespeichertem biometrischem SPBF-Vektor extrahieren 1106
Eingegebenen biometrischen Vektor mit gespeichertem biometrischem SPBF-Vektor vergleichen 1108
Authentifizierungsergebnisse des gespeicherten biometrischen SPBF-Vektors an Eingang Vergleich Biometrik mit biometrischem SPBF-Vektor ausgeben 1110
Ende

FIG. 12

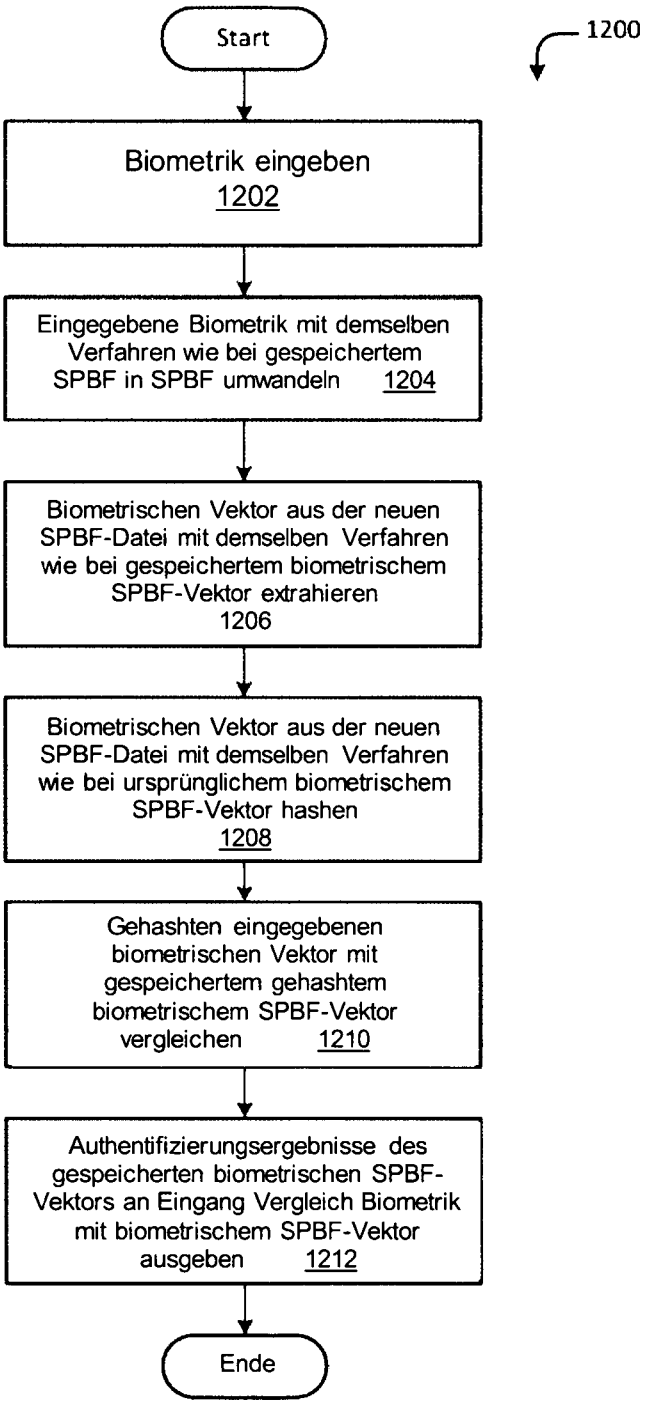

Start
1200
Biometrik eingeben
1202
Eingegebene Biometrik mit demselben Verfahren wie bei gespeichertem SPBF in SPBF umwandeln 1204
Biometrischen Vektor aus der neuen SPBF-Datei mit demselben Verfahren wie bei gespeichertem biometrischem SPBF-Vektor extrahieren
1206
Biometrischen Vektor aus der neuen SPBF-Datei mit demselben Verfahren wie bei ursprünglichem biometrischem SPBF-Vektor hashen
1208
Gehashten eingegebenen biometrischen Vektor mit gespeichertem gehashtem biometrischem SPBF-Vektor vergleichen 1210
Authentifizierungsergebnisse des gespeicherten biometrischen SPBF-Vektors an Eingang Vergleich Biometrik mit biometrischem SPBF-Vektor ausgeben 1212
Ende

FIG. 13

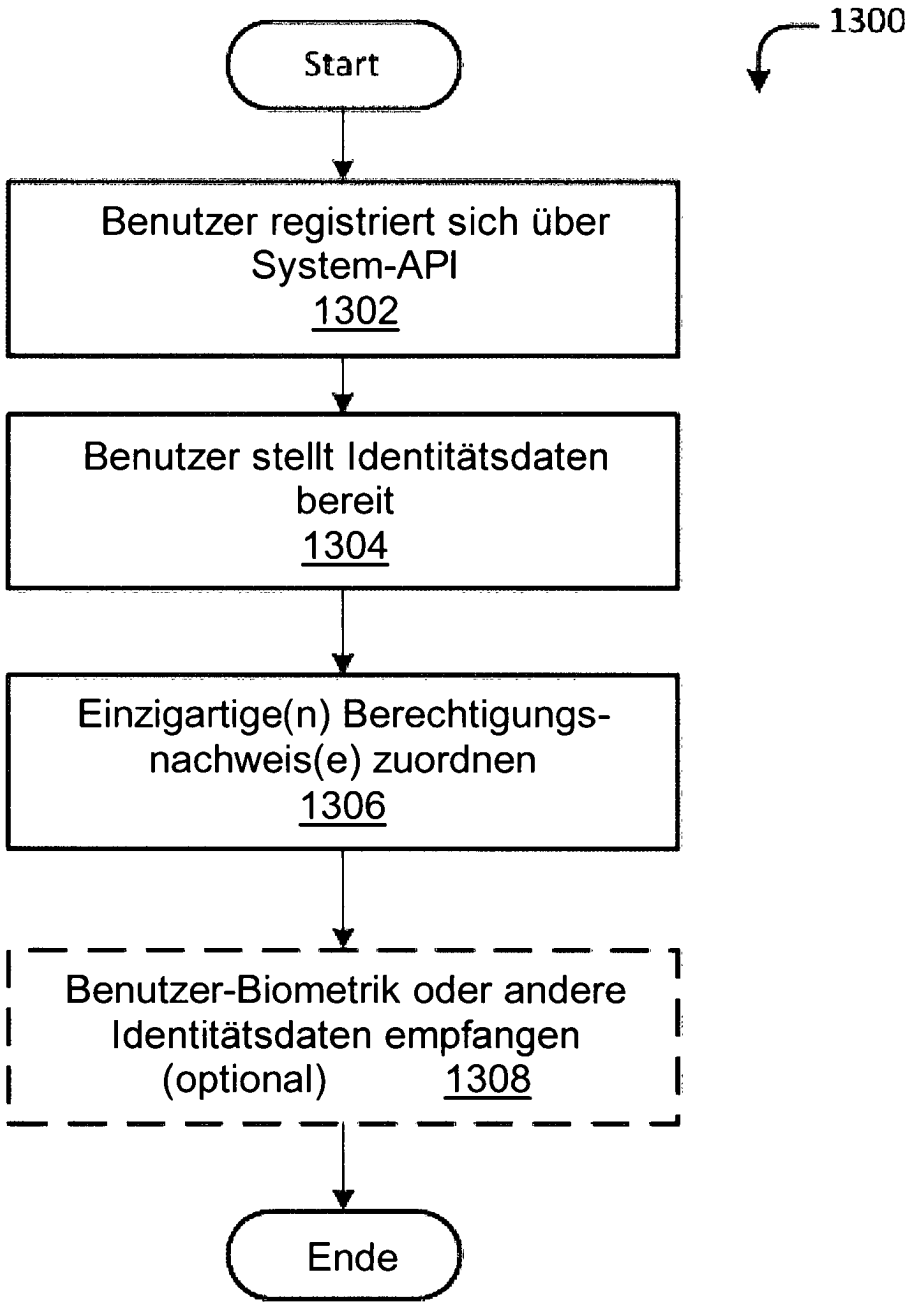

1300
Start
Benutzer registriert sich über System-API
1302
Benutzer stellt Identitätsdaten bereit
1304
Einzigartige(n) Berechtigungs-nachweis(e) zuordnen
1306
Benutzer-Biometrik oder andere Identitätsdaten empfangen (optional) 1308
Ende

FIG. 14

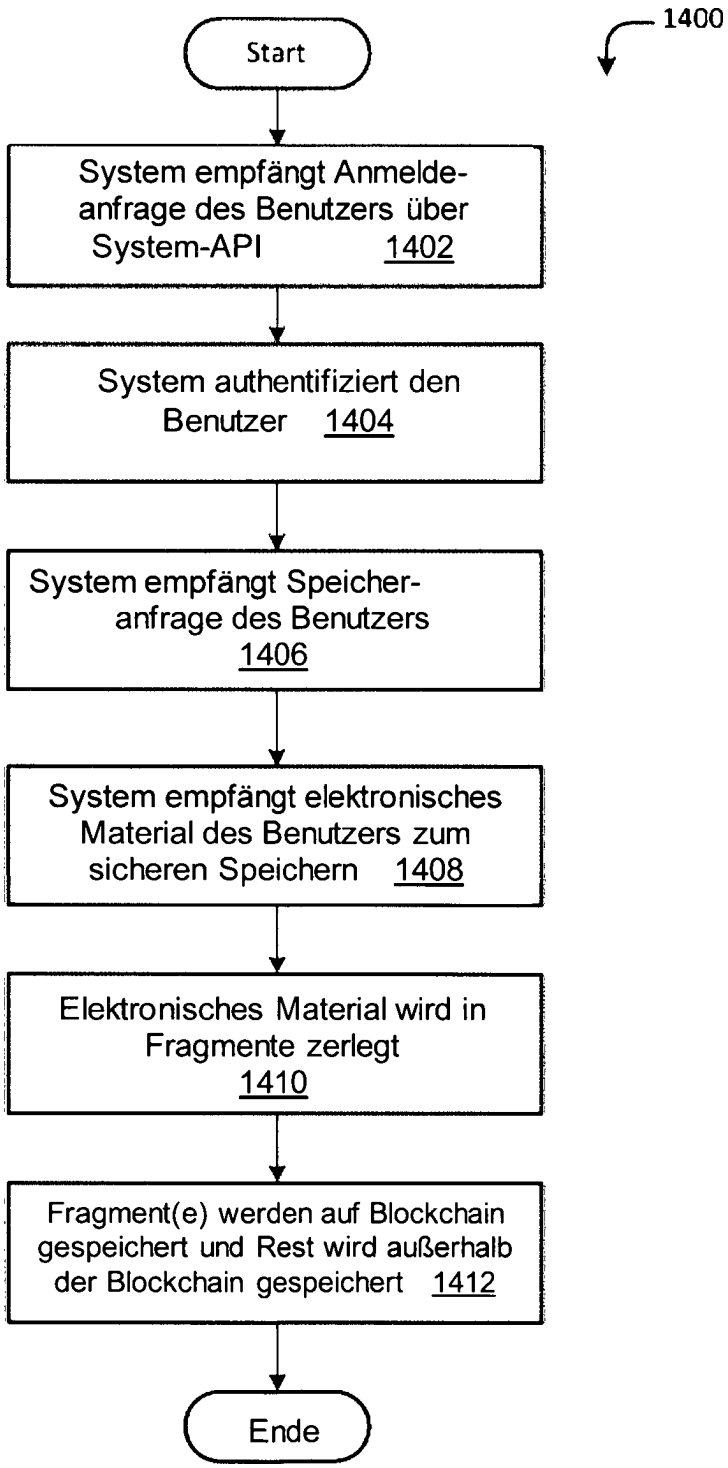

1400
Start
System empfängt Anmelde-anfrage des Benutzers über System-API 1402
System authentifiziert den Benutzer 1404
System empfängt Speicher-anfrage des Benutzers 1406
System empfängt elektronisches Material des Benutzers zum sicheren Speichern 1408
Elektronisches Material wird in Fragmente zerlegt 1410
Fragment(e) werden auf Blockchain gespeichert und Rest wird außerhalb der Blockchain gespeichert 1412
Ende

FIG. 15

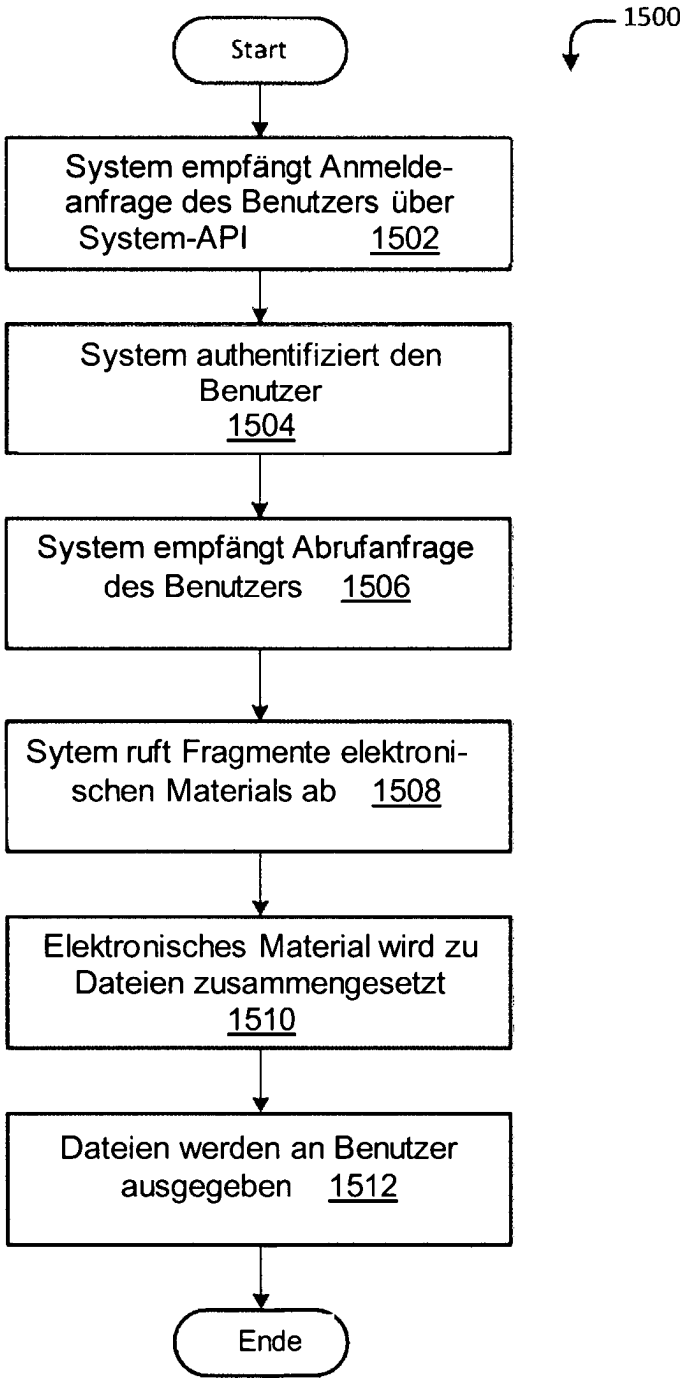
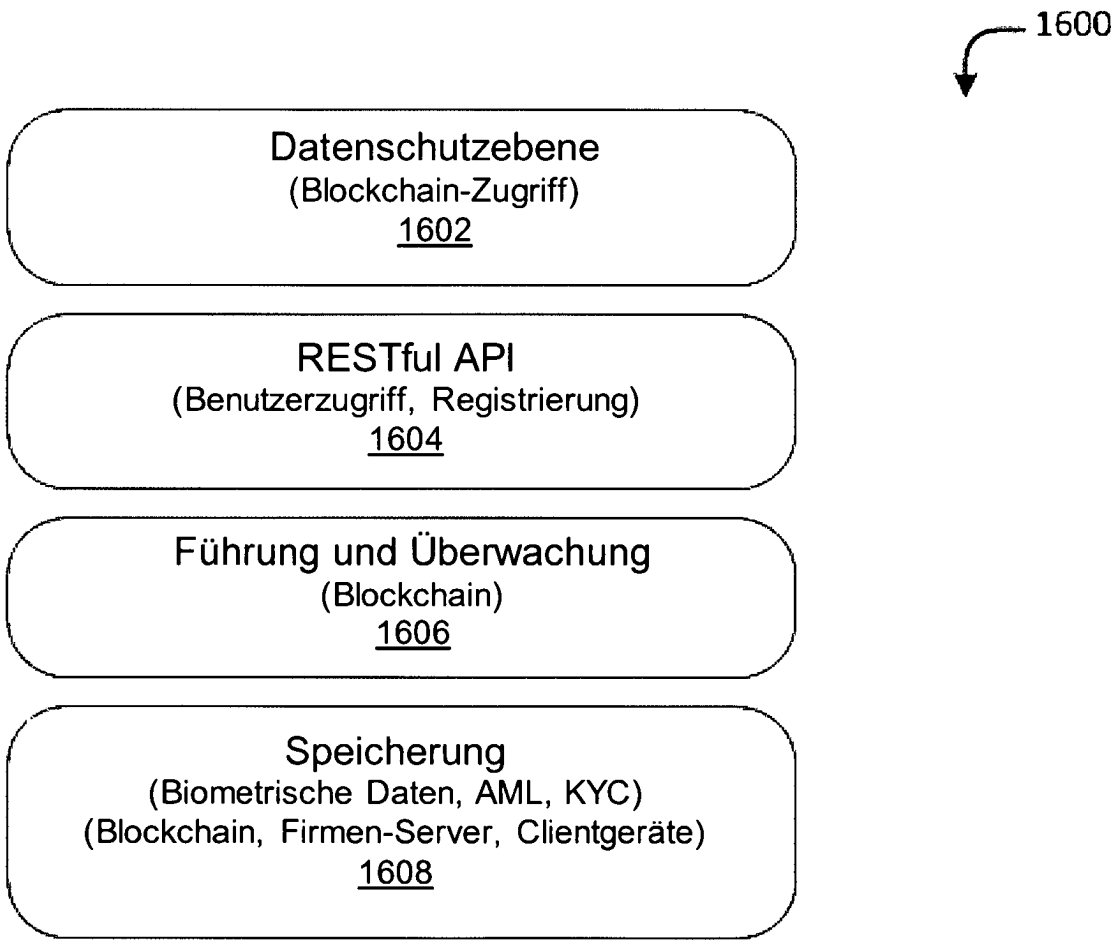

1500
Start
System empfängt Anmelde-anfrage des Benutzers über System-API 1502
System authentifiziert den Benutzer 1504
System empfängt Abrufanfrage des Benutzers 1506
Sytem ruft Fragmente elektroni-schen Materials ab 1508
Elektronisches Material wird zu Dateien zusammengesetzt 1510
Dateien werden an Benutzer ausgegeben 1512
Ende

FIG. 16


1600
Datenschutzebene
(Blockchain-Zugriff)
1602
RESTful API
(Benutzerzugriff, Registrierung)
1604
Führung und Überwachung
(Blockchain)
1606
Speicherung
(Biometrische Daten, AML, KYC)
(Blockchain, Firmen-Server, Clientgeräte)
1608