(19) Deutsches Patent- und Markenamt

(10) **DE 20 2016 008 801 U1** 2019.12.12

(12) # Gebrauchsmusterschrift

(21) Aktenzeichen: **20 2016 008 801.8**
(22) Anmeldetag: **14.10.2016**
(67) aus Patentanmeldung: **EP 16 78 8876.7**
(47) Eintragungstag: **04.11.2019**
(45) Bekanntmachungstag im Patentblatt: **12.12.2019**

(51) Int Cl.: ***G06F 21/31*** (2013.01)

(30) Unionspriorität:

62/241,436	**14.10.2015**	**US**
62/264,418	**08.12.2015**	**US**
62/325,880	**21.04.2016**	**US**
62/380,467	**28.08.2016**	**US**

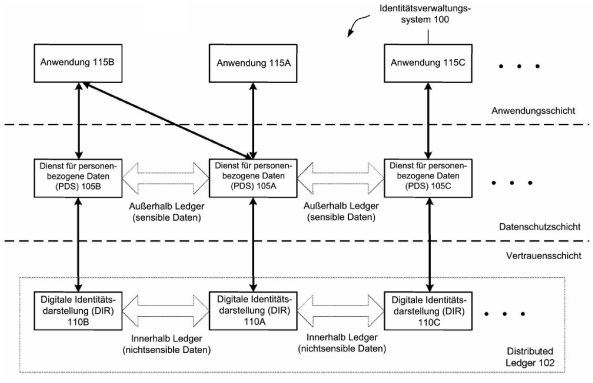
(73) Name und Wohnsitz des Inhabers:
Bhargava, Alok, Newton, MA, US; Cambridge Blockchain, LLC, Cambridge, MA, US

(74) Name und Wohnsitz des Vertreters:
Meissner Bolte Patentanwälte Rechtsanwälte Partnerschaft mbB, 80538 München, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Systeme zur Verwaltung digitaler Identitäten**

(57) Hauptanspruch: Computersystem, umfassend:
mindestens einen Prozessor; und
mindestens ein computerlesbares Medium, auf dem mehrere Anweisungen gespeichert sind, die bei Ausführung den mindestens einen Prozessor dazu veranlassen:
eine Anforderung zum Verifizieren mindestens einer Bestätigung für mindestens ein Attribut eines Identitätsinhabers zu empfangen, wobei:
die mindestens eine Bestätigung zwischen mehreren Zuständen in einem Distributed-Ledger-System beweglich ist, wobei die mehreren Zustände einen VERIFIED-Zustand beinhalten, und
die mindestens eine Bestätigung einen kryptographischen Nachweist umfasst; einen Wert, der dem mindestens einen Attribut entspricht, zu empfangen; und
zu bestimmen, ob der kryptographische Nachweis in der mindestens einen Bestätigung ein gültiger Nachweis für den empfangenen Wert ist, der dem mindestens einen Attribut entspricht;
auf Grundlage von Informationen, die auf den Identitätsinhaber bezogen sind, den empfangenen Wert, der dem mindestens einen Attribut entspricht, zu verifizieren; und
in Reaktion darauf, dass bestimmt wird, dass der kryptographische Nachweis in der mindestens einen Bestätigung ein gültiger Nachweis für den empfangenen Wert ist, der dem mindestens einen Attribut entspricht; und dass der empfange Wert, der dem mindestens einen Attribut entspricht, erfolgreich verifiziert wird:
die mindestens eine Bestätigung für das mindestens eine Attribut elektronisch zu signieren; und
über das Distributed-System zu veranlassen, ...



Beschreibung

VERWANDTE ANMELDUNGEN

[0001] Diese Anmeldung beansprucht die Priorität gemäß 35 USC § 119(e) der provisorischen US-Anmeldung mit der Seriennr. 62/380.467, eingereicht am 28. August 2016, mit der Bezeichnung „AN APPROACH FOR STRONG DIGITAL IDENTITIES“, die hier durch Bezugnahme vollumfänglich aufgenommen wird. Diese Anmeldung beansprucht die Priorität gemäß 35 USC § 119(e) der provisorischen US-Anmeldung mit der Seriennr. 62/325.880, eingereicht am 21. April 2016, mit der Bezeichnung „COUNTERPARTY CHECKS IN THE CONTEXT OF A BLOCKCHAIN ECOSYSTEM“, die hier durch Bezugnahme vollumfänglich aufgenommen wird. Diese Anmeldung beansprucht die Priorität gemäß 35 USC § 119(e) der provisorischen US-Anmeldung mit der Seriennr. 62/264.418, eingereicht am 8. Dezember 2015, mit der Bezeichnung „SELECTIVE INFORMATION SHARING PLATFORM“, die hier durch Bezugnahme vollumfänglich aufgenommen wird. Diese Anmeldung beansprucht die Priorität gemäß 35 USC § 119(e) der provisorischen US-Anmeldung mit der Seriennr. 62/241.436, eingereicht am 14. Oktober 2015, mit der Bezeichnung „IDENTITY MANAGEMENT WITH A MULTI-BLOCKCHAIN APPROACH“, die hier durch Bezugnahme vollumfänglich aufgenommen wird.

HINTERGRUND

[0002] Nahezu sämtliche Einrichtungen (z. B. Regierungsbehörden, Einrichtungen des Gesundheitswesens, Finanzinstitute, Einzelhändler, Anbieter sozialer Netzwerkdienste, Arbeitgeber usw.) erfassen und speichern personenbezogene Daten. In besonders stark regulierten Branchen, wie z. B. Banken und Versicherungen, müssen Einrichtungen strenge „Kenne deinen Kunden“-Prozesse einrichten, um Kundenidentitäten zu verifizieren. Diese Prozesse sind wichtig, um Identitätsdiebstahl, Finanzbetrug, Geldwäsche und Terrorismusfinanzierung zu verhindern.

[0003] Solche Fundgruben von personenbezogenen Daten werden häufig aus finanziellen, politischen oder anderen Gründen missbraucht. Um die Privatsphäre ihrer Bürger zu schützen, haben viele Regierungen Vorschriften verabschiedet, die einschränken, wie Einrichtungen personenbezogene Daten handhaben dürfen.

KURZDARSTELLUNG

[0004] In einigen Ausführungsformen wird ein computerimplementiertes Verfahren bereitgestellt, umfassend die Schritte: Verwenden mehrerer Messungen, die an einem Benutzer durchgeführt werden, um eine Kennung für den Benutzer zu erzeugen, wobei die Kennung einen kryptographischen Nachweis für die mehreren Messungen umfasst; Instanziieren einer digitalen Identitätsdarstellung, die der Kennung für den Benutzer zugeordnet ist, wobei die digitale Identitätsdarstellung Programmcode umfasst, der Regeln zur Bestätigung umsetzt; Erzeugen einer elektronischen Signatur über die digitale Identitätsdarstellung; und Veröffentlichen der digitalen Identitätsdarstellung und der elektronischen Signatur in einem Distributed-Ledger-System.

[0005] In einigen Ausführungsformen wird ein computerimplementiertes Verfahren bereitgestellt, umfassend die Schritte: Auswählen eines Schemas aus mehreren Schemata für Ausweise, wobei das Schema mehrere Attribute umfasst; Erzeugen, gemäß dem Schema, eines Ausweises zur Verwendung beim Bestätigen einer Identität eines Benutzers, wobei der Schritt des Erzeugens Folgendes umfasst: Identifizieren mehrerer Werte, wobei jeder Wert einem Attribut der mehreren Attribute in dem Schema entspricht; Erzeugen von mindestens einem kryptographischen Nachweis für jeden Wert der mehreren Werte; und Identifizieren einer vertrauenswürdigen Entität zum Verifizieren der mehreren Werte; und Veröffentlichen des Ausweises in einem Distributed-Ledger-System.

[0006] In einigen Ausführungsformen wird ein computerimplementiertes Verfahren bereitgestellt, umfassend: Empfangen, über ein Distributed-Ledger-System, einer Anforderung zum Verifizieren eines Ausweises, wobei der Ausweis mehrere Attributbestätigungen umfasst, die jeweils mehreren Attributen für einen Benutzer entsprechen, wobei bei jedem Attribut die entsprechende Attributbestätigung einen kryptographischen Nachweis umfasst; Empfangen, über einen Kanal außerhalb des Distributed-Ledger-Systems, mehrerer Werte, die jeweils den mehreren Attributen entsprechen; für mindestens ein Attribut der mehreren Attribute: Verifizieren, ob der Wert, der dem mindestens einen Attribut entspricht, ein korrekter Wert des mindestens einen Attributs für den Benutzer ist; und in Reaktion darauf, dass verifiziert wird, dass der Wert, der dem mindestens einen Attribut entspricht, ein korrekter Wert des mindestens einen Attributs für den Benutzer ist, Veranlassen, über das Distributed-Ledger-System, dass sich die Attributbestätigung, die dem mindestens einen Attribut entspricht, in einem VERIFIED-Zustand befindet.

[0007] In einigen Ausführungsformen wird ein computerimplementiertes Verfahren bereitgestellt, umfassend: Empfangen, über ein Distributed-Ledger-System, einer Anforderung zum Verifizieren eines ersten Ausweises, wobei der erste Ausweis mehrere Attributbestätigungen umfasst, die jeweils mehreren Attributen für einen Benutzer entsprechen, wobei bei jedem Attribut die entsprechende Attributbestätigung einen kryptographischen Nachweis umfasst; Empfangen, über einen Kanal außerhalb des Distributed-Ledger-Systems, mehrerer Werte, die jeweils den mehreren Attributen entsprechen; für mindestens ein Attribut der mehreren Attribute: Identifizieren, anhand des ersten Ausweises, einer ersten Attributbestätigung, die dem mindestens einen Attribut entspricht, wobei die erste Attributbestätigung einen ersten kryptographischen Nachweis umfasst; Identifizieren, anhand der ersten Attributbestätigung, eines Pointers zu einem zweiten Ausweis; Verwenden des Pointers, um auf den zweiten Ausweis aus dem Distributed Ledger zuzugreifen; Identifizieren, anhand des zweiten Ausweises, einer Entität, die dafür zuständig ist, den zweiten Ausweis zu verifizieren, und einer zweiten Attributbestätigung, die dem mindestens einen Attribut entspricht; Bestimmen, ob der Entität, die dafür zuständig ist, den zweiten Ausweis zu verifizieren, zu vertrauen ist; und in Reaktion darauf, dass bestimmt wird, dass der Entität, die dafür zuständig ist, den zweiten Ausweis zu verifizieren, zu vertrauen ist, Prüfen, ob: (1) sich die zweite Attributbestätigung in einem VERIFIED-Zustand befindet; (2) der zweite kryptographische Nachweis ein gültiger Nachweis für den empfangenen Wert ist, der dem mindestens einen Attribut entspricht; und (3) die zweite Attributbestätigung durch die Entität, die dafür zuständig ist, den zweiten Ausweis zu verifizieren, elektronisch signiert ist.

[0008] Gemäß einigen Ausführungsformen wird ein System bereitgestellt, umfassend mindestens einen Prozessor und mindestens ein computerlesbares Speichermedium, auf dem Anweisungen gespeichert sind, die bei Ausführung den mindestens einen Prozessor derart programmieren, dass er eines der oben genannten Verfahren durchführt.

[0009] Gemäß einigen Ausführungsformen wird mindestens ein computerlesbares Speichermedium bereitgestellt, auf dem Anweisungen gespeichert sind, die bei Ausführung mindestens einen Prozessor derart programmieren, dass er eines der oben genannten Verfahren durchführt.

Figurenliste

Fig. 1 zeigt ein veranschaulichendes Identitätsverwaltungssystem **100** gemäß einigen Ausführungsformen.

Fig. 2 zeigt einen veranschaulichenden Dienst für personenbezogene Daten (Personal Data Service - PDS) **200** gemäß einigen Ausführungsformen.

Fig. 3 zeigt eine veranschaulichende digitale Identitätsdarstellung (Digital Identity Representation - DIR) **300** gemäß einigen Ausführungsformen.

Fig. 4 zeigt eine veranschaulichende Zustandsmaschine **400**, die Übergänge zwischen verschiedenen Zuständen einer Attributbestätigung gemäß einigen Ausführungsformen steuert.

Fig. 5 zeigt einen veranschaulichenden Prozess **500** zur Bestätigung gemäß einigen Ausführungsformen.

Fig. 6 zeigt eine veranschaulichende Vertrauensstruktur **600** gemäß einigen Ausführungsformen.

Fig. 7 zeigt einen veranschaulichenden Prozess **700** für Gegenparteiüberprüfungen gemäß einigen Ausführungsformen.

Fig. 8 zeigt einen veranschaulichenden Prozess **800** für eine Datenänderung in einer Komponente der Datenschutzschicht (z. B. einem PDS) und eine resultierende Zustandsänderung in einer Vertrauensschicht (z. B. einer DIR) gemäß einigen Ausführungsformen.

Fig. 9 zeigt einen veranschaulichenden Distributed-Ledger-Ermittlungsmechanismus in einem Netzwerk **900** gemäß einigen Ausführungsformen.

Fig. 10 stellt einen veranschaulichenden Computer **10000** schematisch dar, auf dem ein beliebiger Aspekt der vorliegenden Offenbarung umgesetzt werden kann.

DETAILLIERTE BESCHREIBUNG

[0010] Aspekte der vorliegenden Offenbarung betreffen Systeme und Verfahren zum Verwalten digitaler Identitäten.

[0011] Zur Erfüllung von Datenschutzvorschriften, die den Austausch personenbezogener Daten einschränken, setzen viele Einrichtungen ihre eigenen digitalen Identitätsverwaltungssysteme um. Die Erfinder haben erkannt und verstanden, dass ein solcher Ansatz ineffizient sein kann. Beispielsweise kann es erforderlich sein, dass ein Benutzer einen gesonderten Identitätsverifizierungsprozess für jedes Konto abschließt, das der Benutzer erstellen möchte, wie z. B. ein Bankkonto, ein Maklerkonto, ein Versicherungskonto,, ein Gesundheitsdienstleisterkonto, ein Versorgungskonto usw. Ebenso kann es erforderlich sein, dass ein Benutzer einen gesonderten Identitätsverifizierungsprozess abschließt, um Zugang zu jedem eingeschränkten Bereich, wie z. B. einem Bürogebäude, einem Schulgelände, einem Freizeitbereich usw., zu erhalten. Während jedes Identitätsverifizierungsprozesses kann es erforderlich sein, dass der Benutzer die gleichen personenbezogenen Daten (z. B. Vorname, Nachname, Führerscheinnummer, Geburtsdatum, Sozialversicherungsnummer usw.) bereitstellt. In einigen Fällen kann sich durch einen aufwändigen Identitätsverifizierungsprozess eine Transaktion verzögern und/oder kann der Benutzer davon abgehalten werden, die Transaktion abzuschließen. Demnach werden in einigen Ausführungsformen Techniken zum Vereinfachen von Identitätsverifizierungsprozessen und dadurch Verbessern der Benutzererfahrung bereitgestellt.

[0012] Die Erfinder haben erkannt und verstanden, dass auch aus Sicht der Einrichtungen Ineffizienzen vorliegen können. Beispielsweise kann ein Kunde bereits über ein Konto bei Bank A in den Vereinigten Staaten verfügen und kann die Erstellung eines neuen Kontos bei derselben Bank A in Deutschland anfordern. Unter diesen Umständen kann Bank A erneut eine Identitätsverifizierung durchführen, auch wenn die Identität des Kunden bereits zum Zeitpunkt der Kontoerstellung in den Vereinigten Staaten verifiziert worden ist. Folglich können redundante Prozesse durchgeführt und doppelte Datensätze geführt werden, wodurch Zeit und Ressourcen (z. B. Prozessorzyklen, Speicher usw.) verschwendet werden können. Demnach werden in einigen Ausführungsformen Techniken zum Verringern von Redundanzen bereitgestellt, während ein geeignetes Sicherheitsniveau aufrechterhalten wird.

Dienst für personenbezogene Daten

[0013] In einigen Ausführungsformen kann ein inhaberorientierter Identitätsverwaltungsansatz bereitgestellt werden, der es einem Benutzer ermöglicht, zu steuern, wie ein oder mehrere Elemente von personenbezogenen Identifikationsinformationen (PII) und/oder anderen personenbezogenen Daten mit einer Entität (z. B. einem anderen Benutzer oder einer Einrichtung) ausgetauscht werden. Beispielsweise kann ein Dienst für personenbezogene Daten (PDS) verwendet werden, um personenbezogene Daten zu speichern, und kann eine Benutzerschnittstelle bereitgestellt werden, über die der Benutzer die personenbezogenen Daten verwalten kann (z. B. durch Hinzufügen, Löschen und/oder Modifizieren von einem oder mehreren Elementen). Zusätzlich oder alternativ dazu kann der PDS eine oder mehrere Anwendungsprogrammierschnittstellen (API) bereitstellen, die durch eine Softwareanwendung, wie z. B. eine Mobil- oder Webanwendung, aufgerufen werden können. Beispielsweise kann, wenn der Benutzer eine App herunterlädt und versucht ein Konto zu eröffnen, die App eine API des PDS aufrufen, um einen Identitätsverifizierungsprozess einzuleiten. Die App kann den PDS darüber informieren, welche Entität eine Verifizierung anfordert und/oder welche Elemente von personenbezogenen Daten zu verifizieren sind.

[0014] In einigen Ausführungsformen kann ein PDS zum Datenschutz programmiert werden, indem z. B. der Zugang zu im PDS gespeicherten personenbezogenen Daten beschränkt wird. Beispielsweise können ein oder mehrere Anmeldeinformationen erforderlich sein, um einen Benutzer zu authentifizieren, der versucht, sich bei dem PDS anzumelden, um die personenbezogenen Daten anzusehen oder zu modifizieren. Zusätzlich oder alternativ dazu kann der PDS ein oder mehrere Elemente der personenbezogenen Daten mit einer Entität nur dann austauschen, wenn dies ausdrücklich von einem authentifizierten Benutzer angewiesen wird.

[0015] In einigen Ausführungsformen kann ein PDS als ein virtueller Behälter umgesetzt sein, der nicht nur eine Benutzerschnittstelle, Anwendungsprogrammierschnittstelle, Datenverwaltung, Vertrauensverwaltung und/oder andere Funktionalitäten, sondern auch eine Laufzeitumgebung (z. B. mit Bibliotheken, Konfigurationsdateien usw.) beinhaltet. Die Erfinder haben erkannt und verstanden, dass ein Umsetzen eines PDS als ein Behälter eine Bereitstellung auf verschiedenen Rechenplattformen erleichtern kann. Es versteht sich jedoch, dass Aspekte der vorliegenden Offenbarung nicht auf das Umsetzen eines PDS als ein Behälter beschränkt sind, da andere Umsetzungen ebenfalls geeignet sein können.

Vertrauensstruktur

[0016] In einigen Ausführungsformen kann eine Vertrauensstruktur bereitgestellt werden, um Bestätigungen (z. B. Identitätsbestätigungen) zu ermöglichen, auf die über mehrere Entitäten hinweg zurückgegriffen werden

kann, wodurch Redundanzen verringert werden. Wenn ein Benutzer beispielsweise einen Identitätsverifizierungsprozess bei einer ersten Einrichtung (z. B. einer Regierungsbehörde, wie z. B. der Kraftfahrzeug-Zulassungsstelle oder KZS) abschließt und versucht, ein Konto bei einer zweiten Einrichtung (z. B. einem Versorgungsunternehmen) zu eröffnen, kann ein Identitätsverifizierungsprozess für die zweite Einrichtung stark vereinfacht werden, solange die zweite Einrichtung der ersten Einrichtung vertraut. Demnach werden in einigen Ausführungsformen Techniken zum Umsetzen einer Vertrauensstruktur bereitgestellt, die es einer Einrichtung ermöglichen, einfach zu prüfen, ob ein Element von personenbezogenen Daten von einer anderen Einrichtung verifiziert worden ist, ohne dieses Element von personenbezogenen Daten erneut verifizieren zu müssen.

[0017] In einigen Ausführungsformen kann eine Vertrauensstruktur bereitgestellt werden, die es einem Benutzer ermöglicht, genau anzugeben, welche Elemente von personenbezogenen Daten mit welcher Entität ausgetauscht und/oder gegenüber welcher Entität belegt werden sollen. Wenn beispielweise eine erste Einrichtung (z. B. die KZS) mehrere Elemente von personenbezogenen Daten (z. B. Geburtsdatum, Sozialversicherungsnummer usw.) verifiziert, kann ein gesonderter Nachweis für jedes Element bereitgestellt werden. Auf diese Weise kann der Benutzer später entscheiden, den Nachweis für ein erstes Element (z. B. über 21 Jahre alt) bei einer zweiten Einrichtung (z. B. einer Bar, die alkoholische Getränke ausschenkt) vorzulegen, ohne den Nachweis eines zweiten Elements (z. B. Sozialversicherungsnummer, Privatadresse oder sogar genaues Geburtsdatum) vorzulegen.

Distributed Ledger

[0018] Das Bitcoin-Protokoll, das 2009 eingeführt wurde, verwendet eine Blockchain, um eine digitale Währung ohne zentrale Clearingstelle bereitzustellen. Die Blockchain wird unter vielen Knoten in einem Netzwerk geteilt und wird verwendet, um Transaktionen auf kryptographisch sichere Weise aufzuzeichnen und zu prüfen. Während z. B. neue Transaktionen an die Blockchain angehängt werden können, können vergangene Transaktionen nicht verändert werden, ohne eine Kette von kryptographischen Nachweisen zu durchbrechen.

[0019] Das Bitcoin-Protokoll verwendet manipulationssichere Eigenschaften der Blockchain, um bestimmte Regeln durchzusetzen. Sobald z. B. eine erste Entität einen Bitcoin an eine zweite Entität sendet, wird ein Datensatz zu der Transaktion über das Netzwerk verbreitet und kann die Transaktion nicht umgekehrt werden, es sei denn, ein Angreifer steuert mehr als die Hälfte der Verarbeitungsleistung in dem Netzwerk. Auf diese Weise kann eine dritte Entität ohne Weiteres erkennen, dass die erste Entität den Bitcoin nicht mehr besitzt, sodass die erste Entität den Bitcoin nicht doppelt ausgeben kann.

[0020] Die Erfinder haben erkannt und verstanden, dass ein Distributed Ledger, wie z. B. eine Blockchain, bei anderen Anwendungen als digitaler Währung verwendet werden kann. Beispielsweise kann ein Distributed Ledger verwendet werden, um eine Vertrauensstruktur umzusetzen, um Bestätigungen (z. B. Identitätsbestätigungen) zu ermöglichen, auf die über mehrere Entitäten hinweg zurückgegriffen werden kann. In einigen Ausführungsformen kann ein Distributed Ledger verwendet werden, um Bestätigungen durch vertrauenswürdige Entitäten aufzuzeichnen, sodass andere Entitäten die bestätigten Tatsachen nicht unabhängig verifizieren müssen.

Identitätsverwaltungsprotokoll

[0021] Die Erfinder haben verschiedene konkurrierende Interessen in der digitalen Identitätsverwaltung erkannt und verstanden. Es kann z. B. wünschenswert sein, den Zugang zu den personenbezogenen Daten eines Benutzers zu beschränkten (z. B. durch Speichern der personenbezogenen Daten in einem virtuellen Behälter, der durch den Benutzer gesteuert wird), wodurch die Privatsphäre des Benutzers geschützt wird. Dahingegen kann es wünschenswert sein, einen transparenten Mechanismus zum Aufzeichnen von Bestätigungen zu verwenden (z. B. durch Speichern der Bestätigungen in einer öffentlich verfügbaren Datenstruktur, die auf mehreren Knoten in einem Netzwerk repliziert wird), sodass ein Angreifer nicht einfach eine Bestätigung fälschen kann. Demnach werden in einigen Ausführungsformen Techniken bereitgestellt, die es einem Benutzer ermöglichen, zu steuern, wie viele personenbezogenen Daten ausgetauscht werden, während die Transparenz von Bestätigungen gewahrt bleibt. Auf diese Weise kann eine Vertrauensstruktur umgesetzt werden, ohne übermäßig personenbezogene Daten auszutauschen.

[0022] In einigen Ausführungsformen kann ein Identitätsverwaltungsprotokoll bereitgestellt werden, um zu ermöglichen, dass Datenschutz über einen transparenten Mechanismus zum Aufzeichnen von Bestätigungen umgesetzt wird. Beispielsweise kann ein Protokollstapel bereitgestellt werden, der drei Schichten beinhaltet - eine Vertrauensschicht, eine Datenschutzschicht und eine Anwendungsschicht. Die Vertrauensschicht kann

einen Distributed Ledger zum Speichern von Bestätigungen beinhalten, die Datenschutzschicht kann virtuelle Behälter beinhalten, die durch jeweilige Benutzer gesteuert werden, und die Anwendungsschicht kann eine oder mehrere Anwendungen beinhalten, die das Identitätsverwaltungsprotokoll verwenden, um Identitäts- und/oder andere personenbezogene Daten zu verifizieren.

[0023] In einigen Ausführungsformen können verschiedene Arten von Daten auf verschiedenen Schichten eines Identitätsverwaltungsprotokolls ausgetauscht werden. Beispielsweise können sensible Daten (z. B. Elemente von PII und/oder anderen personenbezogenen Daten) auf der Datenschutzschicht ausgetauscht werden (z. B. über verschlüsselte Kommunikation), wohingegen nichtsensible Daten (z. B. kryptographische Nachweise von Elementen von PII und/oder anderen personenbezogenen Daten) auf der Vertrauensschicht ausgetauscht werden können. Auf diese Weise kann ein hohes Maß an Transparenz auf der Vertrauensschicht bereitgestellt werden, ohne den Datenschutz zu gefährden.

[0024] In einigen Ausführungsformen kann ein Identitätsverwaltungsprotokoll bereitgestellt werden, bei dem Benutzer im Gegensatz zu Einrichtungen steuern, wie Elemente von PII und/oder anderen personenbezogenen Daten mit anderen Entitäten ausgetauscht werden, während vertrauenswürdige Entitäten die Richtigkeit der Elemente von PII und/oder anderen personenbezogenen Daten bestätigen. Auf diese Weise kann ein Benutzer genau entscheiden, welches eine oder welche mehreren Elemente von personenbezogenen Daten mit einer anderen Entität (z. B. einem anderen Benutzer) ausgetauscht werden sollen, und kann die andere Entität prüfen, ob das eine oder die mehreren Elemente von personenbezogenen Daten durch eine oder mehrere vertrauenswürdige Entitäten (z. B. eine oder mehrere Regierungsbehörden und/oder einen oder mehrere Arbeitgeber) verifiziert wurden, ohne einen aufwändigen Verifizierungsprozess durchlaufen zu müssen (z. B. physisches Untersuchen von Dokumenten, wie z. B. Pässen, Sozialversicherungsausweisen, Gehaltsabrechnungen usw.).

[0025] Es versteht sich, dass die oben eingeführten und nachfolgend näher erörterten Techniken auf zahlreiche Arten umgesetzt werden können, da die Techniken nicht auf eine bestimmte Art der Umsetzung beschränkt sind. Beispiele für Einzelheiten der Umsetzung sind lediglich zur Veranschaulichung aufgeführt. Weiterhin können die hier offenbarten Techniken einzeln oder in einer beliebigen Kombination verwendet werden, da Aspekte der vorliegenden Offenbarung nicht auf die Verwendung einer bestimmten Technik oder Kombination von Techniken beschränkt sind.

Nähere Erörterungen zu veranschaulichenden Ausführungsformen

[0026] **Fig. 1** zeigt ein veranschaulichendes Identitätsverwaltungssystem **100** gemäß einigen Ausführungsformen. In diesem Beispiel beinhaltet das Identitätsverwaltungssystem **100** einen Identitätsverwaltungsprotokollstapel mit drei Schichten. Beispielsweise gibt es eine Vertrauensschicht mit einem Distributed Ledger **102** zum Speichern von Bestätigungen (z. B. Identitätsbestätigungen). Zusätzlich oder alternativ dazu kann es eine Datenschutzschicht, die mehrere Dienste für personenbezogene Daten (PDS) **105A**, **105B**, **105C**, ... umfasst, und/oder eine Anwendungsschicht, die mehrere Anwendungen **115A**, **115B**, **115C**, ... umfasst, geben. Die PDS können personenbezogene Daten jeweiliger Benutzer speichern, die Transaktionen über die Anwendungen ausüben (z. B. Eröffnen eines Kontos, Tätigen eines Kaufs usw.).

[0027] In einigen Ausführungsformen kann ein PDS ein Softwareprogramm zum Verwalten von PII und/oder anderen personenbezogenen Daten beinhalten. Beispielsweise kann ein PDS als ein virtueller Behälter umgesetzt werden, der das Softwareprogramm in einem Dateisystem umhüllt, um zu ermöglichen, dass das Softwareprogramm in einer beliebigen Umgebung konsistent ausgeführt wird. Beispielsweise kann das Dateisystem ein Laufzeitsystem, ein oder mehrere Systemwerkzeuge, eine oder mehrere Systembibliotheken usw. beinhalten. Es versteht sich jedoch, dass Aspekte der vorliegenden Offenbarung nicht darauf beschränkt sind. Alternativ oder zusätzlich dazu kann ein PDS einfach ein Softwareprogramm zum Verwalten von personenbezogenen Daten ohne ein damit einhergehendes Dateisystem beinhalten.

[0028] In einigen Ausführungsformen kann ein PDS einer digitalen Identitätsdarstellung (DIR) in dem Distributed Ledger **102** zugeordnet sein. Beispielsweise können den PDS **105A**, **105B**, **105C**, ... ein DIR **110A**, **110B** bzw. **110C** zugeordnet sein. In einigen Ausführungsformen kann jeder einzelne Benutzer einen PDS und eine entsprechende DIR steuern. Der PDS kann sensible Daten (z. B. Elemente von PII und/oder anderen personenbezogenen Daten) speichern, wohingegen die entsprechende DIR nichtsensible Daten (z. B. kryptographische Nachweise für Elemente von PII und/oder anderen personenbezogenen Daten) speichern kann. Die PDS können miteinander kommunizieren und sensible Daten auf eine sichere Weise austauschen, wohin-

gegen die DIR nichtsensible Daten (z. B. kryptographische Nachweise für Elemente von PII und/oder anderen personenbezogenen Daten) in dem Distributed Ledger **102** aufzeichnen können.

[0029] In einigen Ausführungsformen können kryptographische Nachweise auf bekannte Weise von Elementen personenbezogener Daten abgeleitet werden und können von vertrauenswürdigen Entitäten signiert werden, welche die Richtigkeit der Elemente von personenbezogenen Daten verifizieren. Eine Entität, mit welcher ein Benutzer ein Element von personenbezogenen Daten (z. B. eine Sozialversicherungsnummer) ausgetauscht hat, kann ohne Weiteres prüfen, ob ein vorgeblicher kryptographischer Nachweis tatsächlich von dem Element personenbezogener Daten abgeleitet ist und ob der kryptographische Nachweis tatsächlich von einer vertrauenswürdigen Entität (z. B. einer Regierungsbehörde oder einem Arbeitgeber) signiert wurde. Es kann jedoch für eine andere Entität rechnerisch machbar sein, das Element von personenbezogenen Daten aus dem kryptographischen Nachweis allein zu rekonstruieren. Auf diese Weise können die konkurrierenden Ziele von Datenschutz und Transparenz gleichzeitig erreicht werden.

[0030] In einigen Ausführungsformen kann der Distributed Ledger **102** digitale Datensätze beinhalten, die unter mehreren Knoten in einem Peer-to-Peer-Netzwerk repliziert werden. Die Knoten können ein Synchronisierungsprotokoll ausführen, wodurch eine Änderung, die auf einem Knoten an einer lokalen Kopie eines digitalen Datensatzes vorgenommen wird, über das Netzwerk verbreitet werden kann und andere Knoten ihre jeweiligen Kopien des gleichen digitalen Datensatzes entsprechend aktualisieren können.

[0031] In einigen Ausführungsformen kann der Distributed Ledger unter Verwendung einer Blockchain umgesetzt werden. Die Blockchain kann mehrere Blöcke beinhalten, wobei jeder Block mehrere Transaktionen beinhalten kann. In einigen Ausführungsformen können die mehreren Transaktionen z. B. chronologisch geordnet sein. Zusätzlich oder alternativ dazu können die mehreren Blöcke derart geordnet sein, dass jeder neu hinzugefügte Block mit einem letzten vorherigen Block verknüpft ist. In einigen Ausführungsformen kann eine derartige Struktur manipulationssicher sein und kann daher verwendet werden, um zu bestätigen, ob eine jeweilige Transaktion stattgefunden hat und/oder wann die Transaktion stattgefunden hat. Beispielsweise kann ein Block der Blockchain nur dann hinzugefügt werden, wenn sich sämtliche Knoten (oder eine Untergruppe von Knoten mit ausreichender Rechenleistung) in einem Netzwerk, in dem die Blockchain umgesetzt ist, auf den Block verständigen.

[0032] In einigen Ausführungsformen kann ein Blockerzeugungsknoten (mitunter als Miner bezeichnet) Rechenleistung investieren, um einen neuen Block zu erzeugen, der mit einem letzten vorherigen Block verknüpft ist. Der schnellste Knoten, der dazu imstande ist, ein rechenintensives mathematisches Puzzle zu lösen (z. B. ein Urbild eines Hash-Werts mit einer bestimmten Anzahl von führenden Nullen zu identifizieren), wird mit einem internen digitalen Objekt (z. B. einem Bitcoin) belohnt. Je nachdem, wie viel Rechenleistung in dem Netzwerk zu einem jeweiligen Zeitpunkt verfügbar ist, kann ein mehr oder weniger komplexes mathematisches Puzzle verwendet werden. Auf diese Weise können Blöcke in einem ausgewählten Zeitfenster erzeugt werden und können Konflikte verringert werden.

[0033] Es versteht sich, dass Aspekte der vorliegenden Offenbarung nicht auf die Verwendung eines Proof-of-Work-Ansatzes wie etwa des oben beschriebenen beschränkt sind. In einigen Ausführungsformen kann ein Proof-of-Work-Ansatz verwendet werden, um einen verteilten Konsensus zu erzielen. Weiterhin versteht es sich, dass eine beliebige geeignete Blockchain-Umsetzung verwendet werden kann, um eine Vertrauensschicht bereitzustellen, einschließlich u. a. Ethereum und Hyperledger Fabric.

[0034] **Fig. 2** zeigt einen veranschaulichenden PDS **200** gemäß einigen Ausführungsformen. Beispielsweise kann es sich bei dem PDS **200** um einen der veranschaulichenden PDS **105A**-**C** in der in **Fig. 1** dargestellten veranschaulichenden Datenschutzschicht handeln. In einigen Ausführungsformen kann der PDS **200** von einem einzelnen Benutzer verwendet werden, um die digitale Identität des Benutzers zu verwalten. Als ein Beispiel kann der Benutzer ein Arbeitnehmer eines Unternehmens sein und kann den PDS **200** verwenden, um anzufordern, dass das Unternehmen einen kryptographischen Nachweis für das Jahreseinkommen des Benutzers signiert. Zusätzlich oder alternativ dazu kann das Unternehmen einen PDS ähnlich dem PDS **200** verwenden, um den kryptographischen Nachweis zu signieren und die Signatur in einem Distributed Ledger (z. B. dem in **Fig. 1** dargestellten veranschaulichenden Distributed Ledger **102**) zu veröffentlichen.

[0035] Als ein anderes Beispiel kann der Benutzer ein Kunde eines Autohändlers sein und kann den PDS **200** verwenden, um das Jahreseinkommen des Benutzers gegenüber dem Autohändler nachzuweisen. Zusätzlich oder alternativ dazu kann der Autohändler einen PDS ähnlich dem PDS **200** verwenden, um in einem Distributed Ledger (z. B. dem in **Fig. 1** dargestellten veranschaulichenden Distributed Ledger **102**) einen vorgeblichen

kryptographischen Nachweis für einen vom Benutzer bereitgestellten jährlichen Einkommensbetrag und eine vorgebliche Signatur des vorgeblichen kryptographischen Nachweises zu suchen. Der PDS des Autohändlers kann prüfen, ob der vorgebliche kryptographische Nachweis tatsächlich von dem durch den Benutzer bereitgestellten jährlichen Einkommensbetrag abgeleitet wurde und der kryptographische Nachweise tatsächlich vom Arbeitgeber des Benutzers signiert wurde.

[0036] In einigen Ausführungsformen kann der PDS **200** eine Benutzerschnittstelle **202** und eine Verwaltungskomponente **208** für personenbezogene Daten beinhalten. Die Benutzerschnittstelle **202** und die Verwaltungskomponente **208** für personenbezogene Daten kann es dem Benutzer ermöglichen, PII und/oder andere personenbezogene Daten zu speichern und die gespeicherten Daten zu verwalten (z. B. hinzuzufügen, zu löschen, zu modifizieren, zu teilen usw.). In einigen Ausführungsformen kann die Benutzerschnittstelle **202** einen Multifaktor-Authentifizierungsmechanismus verwenden, um den Zugang zu den gespeicherten Daten und verschiedenen Funktionalitäten des PDS **200** zu beschränken.

[0037] In einigen Ausführungsformen kann die Verwaltungskomponente **208** für personenbezogene Daten ein Prüfprotokoll einiger oder sämtlicher über die Benutzerschnittstelle **202** durchgeführten Aktionen führen. Dies kann es dem Benutzer ermöglichen, jegliche unautorisierten Aktionen zu identifizieren (z. B. durch einen Angreifer, der dem Benutzer gestohlene Anmeldeinformationen verwendet). Zusätzlich oder alternativ dazu kann das Prüfprotokoll von einem Ermittler verwendet werden, um zu bestimmen, ob der Benutzer an betrügerischen Handlungen beteiligt ist.

[0038] In einigen Ausführungsformen können es die Benutzerschnittstelle **202** und die Verwaltungskomponente **208** für personenbezogene Daten dem Benutzer ermöglichen, den Austausch eines oder mehrerer Elemente von personenbezogenen Daten mit einer anderen Entität festzulegen und/oder zu genehmigen. Zusätzlich oder alternativ dazu kann die Verwaltungskomponente **208** für personenbezogene Daten eine oder mehrere Regeln anwenden, um den Austausch eines oder mehrerer Elemente von personenbezogenen Daten mit einer anderen Entität zu verwalten. Beispielsweise kann eine Regel eine oder mehrere Bedingungen festlegen und kann ausgelöst werden, wenn die eine oder mehreren Bedingungen in einem vorliegenden Kontext erfüllt sind. Die Regel kann ferner ein oder mehrere Elemente von personenbezogenen Daten, die ausgetauscht werden sollen, und/oder eine oder mehrere Entitäten, mit denen ein oder mehrere Elemente von personenbezogenen Daten ausgetauscht werden sollen, festlegen. In einigen Ausführungsformen kann der Benutzer jedes Mal benachrichtigt werden, wenn eine Regel ausgelöst wird, und wird der vorgeschlagene Austausch von personenbezogenen Daten nur mit dem Einverständnis des Benutzers ausgeführt. Dies ist jedoch nicht zwingend erforderlich, da der Benutzer in einigen Ausführungsformen den Austausch personenbezogener Daten gemäß einer bestimmten Regel im Voraus genehmigen kann.

[0039] In einigen Ausführungsformen kann eine Regel von dem Benutzer festgelegt oder mit der Zeit (z. B. unter Verwendung eines oder mehrerer Algorithmen zum maschinellen Lernen) aus den Verhaltensweisen des Benutzers und/oder Kontexten, in denen die Verhaltensweisen des Benutzers beobachtet werden, erlernt werden. Zusätzlich oder alternativ dazu kann eine Regel, die sich auf ein oder mehrere Elemente von personenbezogenen Daten bezieht, von einer vertrauenswürdigen Entität abgerufen werden, die dafür zuständig ist, die Richtigkeit des einen oder der mehreren Elemente von personenbezogenen Daten nachzuweisen.

[0040] Zurück bei **Fig. 2** kann der PDS **200** in einigen Ausführungsformen eine API **206** beinhalten, über die der PDS **200** mit einer oder mehreren Anwendungen (z. B. den veranschaulichenden Anwendungen **115A**-**C** in der in **Fig. 1** dargestellten veranschaulichenden Anwendungsschicht) interagieren kann. Als ein Beispiel kann der PDS **200** mit einer Gehaltsabrechnungsanwendung eines Arbeitgebers interagieren, um eine Bestätigung für das Jahreseinkommen des Benutzers anzufordern. Als ein anderes Beispiel kann der PDS **200** mit einer Kreditbearbeitungsanwendung eines Autoverkäufers interagieren, um das Jahreseinkommen des Benutzers nachzuweisen. Zu anderen Beispielen für Anwendungen gehören u. a. Vertragsunterzeichnung, Verifizierung des Bildungsstandes, Verifizierung der Kreditwürdigkeit, digitale Zugangskontrolle, physische Zugangskontrolle usw.

[0041] In einigen Ausführungsformen kann der PDS **200** eine Kommunikationsverwaltungskomponente **210** beinhalten, über die der PDS **200** mit einem oder mehreren anderen PDS (z. B. den veranschaulichenden PDS **105A**-**C** in der in **Fig. 1** dargestellten veranschaulichenden Datenschutzschicht) kommunizieren kann. Als ein Beispiel kann der PDS **200** mit einem PDS des Arbeitgebers des Benutzers kommunizieren, um anzufordern, dass der Arbeitgeber einen kryptographischen Nachweis für das Jahreseinkommen des Benutzers signiert. Als ein anderes Beispiel kann der PDS **200** mit einem PDS eines Autohändlers kommunizieren, um das Jahreseinkommen des Benutzers nachzuweisen, so dass der Benutzer einen Fahrzeugkredit erhalten kann.

[0042] In einigen Ausführungsformen kann der PDS **200** eine Vertrauensverwaltungskomponente **212** beinhalten, über die der PDS **200** eine DIR (z. B. eine der veranschaulichenden DIR **110A**-**C** in der in **Fig. 1** dargestellten veranschaulichenden Vertrauensschicht) in einem Distributed Ledger (z. B. dem in **Fig. 1** dargestellten veranschaulichenden Distributed Ledger **102**) verwalten kann. Beispielsweise kann die Vertrauensverwaltungskomponente **212** Programmlogik beinhalten, um die DIR auf Grundlage von Kontextinformationen (z. B. welche Anwendung ruft der PDS **200** auf) zu verwalten. Die Programmlogik kann eine Zustandsänderung in der DIR z. B. auf Grundlage einer von dem Benutzer über die Benutzerschnittstelle **202** empfangenen Anweisung, einer Eingabe von einer Anwendung über die API **206**, eine von einem anderen PDS über die Kommunikationskomponente **210** empfangene nicht vom Ledger erfasste Kommunikation usw. veranlassen.

[0043] In einigen Ausführungsformen kann der PDS **200** ein direkter Teilnehmer an einem oder mehreren Distributed Ledgern (z. B. dem in **Fig. 1** dargestellten veranschaulichenden Distributed Ledger **102**) sein. Zusätzlich oder alternativ dazu kann der PDS **200** mit einer vertrauenswürdigen Entität interagieren, die einen oder mehrere Distributed Ledger im Namen des PDS **200** verwalten kann.

[0044] In einigen Ausführungsformen können ein oder mehrere Kriterien verwendet werden, um zu bestimmen, ob der PDS **200** direkt oder indirekt teilnimmt oder beides, einschließlich u. a. Überlegungen zur Systembereitstellung und/oder Anwendung.

[0045] Obwohl in **Fig. 2** Details zur Umsetzung eines PDS dargestellt und vorstehend erörtert sind, versteht es sich, dass Aspekte der vorliegenden Offenbarung nicht auf die Verwendung einer bestimmten Komponente oder Kombination von Komponenten oder eine bestimmte Anordnung von Komponenten beschränkt sind. Beispielsweise kann in einigen Ausführungsformen ein PDS bereitgestellt werden, der dynamisch erweiterbare Funktionalitäten auf Grundlage eines Kerns unterstützt, der lokal gespeicherte Daten verwaltet. Beispielsweise kann eine Modularchitektur (z. B. eine Mikrodienst-Architektur) verwendet werden, sodass ein PDS leicht angepasst werden kann, um sich ändernde Bedürfnisse (z. B. neue Anwendungsfälle und/oder Prozessabläufe) zu erfüllen.

[0046] **Fig. 3** zeigt eine veranschaulichende DIR **300** gemäß einigen Ausführungsformen. Beispielsweise kann es sich bei der DIR **300** um eine der veranschaulichende DIR **110A-C** in der in **Fig. 1** dargestellten veranschaulichenden Vertrauensschicht handeln. In einigen Ausführungsformen kann die DIR **300** durch einen PDS (z. B. den in **Fig. 2** dargestellten veranschaulichenden PDS **200**) gesteuert werden.

[0047] In einigen Ausführungsformen kann die DIR **300** in einem Distributed Ledger (z. B. dem in **Fig. 1** dargestellten veranschaulichenden Distributed Ledger **102**) umgesetzt sein und kann eine Kennung verwendet werden, um auf die DIR **300** in dem Distributed Ledger zu verweisen. In dem in **Fig. 3** dargestellten Beispiel wird auf die DIR **300** unter Verwendung einer global eindeutigen Identitätskennung (Globally Unique Identity Identifier - GUII) **302** verwiesen, sodass keine zwei DIR in dem Distributed Ledger eine gleiche Kennung teilen. In einigen Ausführungsformen kann jede DIR durch einen PDS gesteuert werden und kann die GUII für die DIR auf Grundlage einer oder mehrerer Metriken des Benutzers, die dem PDS zugeordnet sind, erzeugt werden. Eine Kombination aus Metriken kann derart ausgewählt werden, dass es bei beliebigen zwei Benutzern höchst unwahrscheinlich ist, dass die DIR für die beiden Benutzer über die gleiche GUII verfügen, was es höchst unwahrscheinlich macht, dass ein Benutzer dazu imstande ist, mehr als eine DIR zu erzeugen. Zu Beispielen für Metriken gehören u. a. Biometriken (z. B. Fingerabdruckscan, Netzhautscan, Stimmabdruck usw.), Verhaltsmetriken (z. B. Standortverlauf, Laufmuster, Schlafmuster usw.) usw.

[0048] In einigen Ausführungsformen kann eine kryptographische Einwegfunktion verwendet werden, um eine GUII aus einem oder mehreren zugrunde liegenden Metrikwerten zu erzeugen, sodass der eine oder die mehreren Werte geheim gehalten werden können, auch wenn die GUII öffentlich zugänglich gemacht wird. Zugrunde liegende Metrikwerte können sicher durch einen entsprechenden PDS zusammen mit Metadaten gespeichert werden, die einen oder mehrere Algorithmen anzeigen, die verwendet werden, um die GUII aus den zugrunde liegenden Metrikwerten zu erzeugen. Es kann den zugrunde liegenden Metrikwerten ein hohes Maß an Sicherheit auferlegt werden. Beispielsweise dürfen die zugrunde liegenden Metrikwerte nicht mit anderen Entitäten ausgetauscht werden.

[0049] In einigen Ausführungsformen kann eine DIR als ein öffentliches Datenrepository für nichtsensible Daten dienen und kann Logik beinhalten, die den Zugang zu diesen Daten steuert. Beispielsweise beinhaltet die DIR **300** in dem in **Fig. 3** dargestellten Beispiel nichtsensible Daten, die in einem oder mehreren Ausweisen **306** organisiert sind, und eine Aktions- und Ereignisspezifikation **304**, die Aktionen, die über die DIR **300** durchgeführt werden können, und/oder Ereignisse, die durch Änderungen in der DIR **300** ausgelöst werden

können, festlegt. Beispielsweise können Beteiligte, welche den Distributed Ledger führen, um Transparenz bereitzustellen, jedes Mal benachrichtigt werden, wenn eine Änderung an der DIR **300** vorgenommen wird.

[0050] In einigen Ausführungsformen kann die DIR **300** zu einem jeweiligen Zeitpunkt in einem von mehreren möglichen Zuständen vorliegen. Beispielsweise kann ein Ausweis **306** in der DIR **300** eine oder mehrere Attributbestätigungen **310** beinhalten und kann eine Attributbestätigung in einem von mehreren Zuständen (z. B. PENDING, VERIFIED, INVALID , EXPIRED usw.) vorliegen. Ein allgemeiner Zustand der DIR **300** kann von Zuständen einiger oder sämtlicher der einzelnen Attributbestätigungen der DIR **300** abhängig sein.

[0051] In einigen Ausführungsformen kann eine Veränderung der DIR **300** von einem ersten Zustand in einen zweiten Zustand über eine Transaktion in dem Distributed Ledger stattfinden. Sobald die Transaktion durch eine Mehrheit der den Distributed Ledger führenden Beteiligten bestätigt ist, kann die DIR **300** in dem zweiten Zustand bleiben, bis eine andere Transaktion bestätigt wird. In einigen Ausführungsformen können sämtliche Zustandsänderungen der DIR **300** in dem Distributed Ledger aufgezeichnet werden und können für sämtliche Beteiligten sichtbar sein, was ein transparentes Prüfprotokoll zur Folge hat.

[0052] In einigen Ausführungsformen kann die DIR **300** Regeln beinhalten, die steuern, wie Zustandsübergänge ausgelöst werden können und/oder welche Entitäten welche Übergänge auslösen können. Beispielsweise können derartige Regeln durch die Aktions- und Ereignisspezifikation **304** der DIR **300** erfasst werden. Sobald die DIR **300** eingerichtet und über den Distributed Ledger bereitgestellt wurde, kann die Programmlogik in der Aktions- und Ereignisspezifikation **304** nicht mehr geändert werden und kann der Distributed Ledger sicherstellen, dass Zustandsänderungen der DIR **300** der Aktions- und Ereignisspezifikation **304** entsprechen.

[0053] In einigen Ausführungsformen kann es für nur eine oder mehrere autorisierte Entitäten zulässig sein, Transaktionen zu erzeugen und dadurch Zustandsänderungen der DIR **300** herbeizuführen. Jede Transaktion kann durch eine Entität signiert werden, welche die Transaktion erzeugt. Auf diese Weise können Zustandsänderungen der DIR **300** prüfbar sein. In einigen Ausführungsformen können mehrere Entitäten daran beteiligt sein, eine Zustandsänderung herbeizuführen. Es kann erforderlich sein, dass sämtliche oder zumindest eine Schwellenanzahl der Entitäten innerhalb eines ausgewählten Zeitintervalls signieren, oder die Zustandsänderung kann nicht bestätigt werden.

[0054] In einigen Ausführungsformen kann ein Attribut ein Element von personenbezogenen Daten, einen Namen für das Element von personenbezogenen Daten und/oder relevante Metadaten beinhalten. Beispielsweise kann zu einem direkten Attribut ein Element von PII, wie z. B. Vorname, Nachname, Geburtsdatum, Geburtsort, Passnummer, Führerscheinnummer, Sozialversicherungsnummer, Adresse, Telefonnummer, Versicherungskennnummer, Fingerabdruckscan, Netzhautscan, Stimmabdruck usw., gehören. Zu einem indirekten Attribut können andere personenbezogene Daten gehören, wie z. B. ein Eigentum (z. B. Fahrzeug, Grundstück usw.), Status des Eigentums usw. Zusätzlich oder alternativ dazu kann ein indirektes Attribut (z. B. Alter von mindestens 21 Jahren) von einem direkten Attribut (z. B. Geburtsdatum) abgeleitet werden.

[0055] Die Erfinder haben erkannt und verstanden, dass die Richtigkeit eines Attributwerts auf eine den Datenschutz wahrende Weise nachgewiesen werden kann, ohne auf die Verwendung einer zentralen Clearingstelle zurückzugreifen. Beispielsweise kann in einigen Ausführungsformen ein Pseudonym für einen Attributwert anstelle des Attributes selbst in dem Distributed Ledger gespeichert werden. Auf diese Weise kann das Pseudonym für den Attributwert in dem Netzwerk repliziert werden, ohne den Attributwert selbst offenzulegen.

[0056] In einigen Ausführungsformen kann ein Pseudonym für einen Attributwert unter Verwendung einer kryptographischen Einwegfunktion berechnet werden. Beispielsweise können in Bezug auf das in **Fig. 3** dargestellte Beispiel ein oder mehrere Attribute in einer Datenquelle **312** gespeichert werden, die von dem PDS geführt werden kann, der die DIR **300** (z. B. durch die in **Fig. 2** dargestellte veranschaulichende Verwaltungskomponente **208** für personenbezogene Daten) steuert. In einigen Ausführungsformen kann ein Attribut aus der Datenquelle **312** abgerufen werden und kann eine kryptographische Einwegfunktion auf einen Wert des Attributs angewandt werden, um einen Nachweis für das Attribut abzuleiten. Der Nachweis und/oder die relevanten Metadaten (z. B. ein Zeitstempel, der anzeigt, wann der Nachweis erzeugt wird), nicht aber der Wert selbst, kann bzw. können in der Attributbestätigung **310** enthalten sein. Auf diese Weise kann die Attributbestätigung **310** in dem Distributed Ledger veröffentlicht werden, ohne den Wert des Attributs offenzulegen.

[0057] Die Erfinder haben erkannt und verstanden, dass es wünschenswert sein kann, einen Mechanismus zum Verwalten von Attributbestätigungen auf granulare Weise bereitzustellen. Demnach sind Attributbestäti-

gungen in einigen Ausführungsformen in einem oder mehreren Ausweisen (z. B. den in **Fig. 6** dargestellten veranschaulichenden Ausweisen **306**) angeordnet, die gesondert verwaltet werden.

[0058] In einigen Ausführungsformen kann ein Benutzer eine vertrauenswürdige Entität als für einen Ausweis zuständig angeben. Für jedes Attribut in dem Ausweis kann die vertrauenswürdige Entität die Richtigkeit eines Werts verifizieren, der von einem Benutzer für das Attribut bereitgestellt wird, prüfen, ob ein in dem Ausweis für das Attribut bereitgestellter Nachweis tatsächlich aus dem von dem Benutzer bereitgestellten Wert berechnet ist, und/oder den Nachweis signieren. Wie oben erörtert, können die Nachweise in einem Ausweis enthalten und in dem Distributed Ledger veröffentlicht sein, kann dies bei den Werten selbst jedoch nicht der Fall sein. Eine beliebige Entität kann als eine vertrauenswürdige Entität dienen, wie z. B. eine Regierungsbehörde, ein Arbeitgeber, ein Finanzinstitut, eine Bildungseinrichtung usw.

[0059] In einigen Ausführungsformen kann es sich bei einem Ausweis um eine Datenstruktur mit mehreren Feldern handeln. Ein nichteinschränkendes Beispiel für einen Ausweis ist nachfolgend aufgeführt.

```
{
        label:              "KYC by Trusted Bank"
        trustedParty: "trusted_party_identifier"
        proofAlgo:          "PBKDF2_SHA256_100000_3"
        salt:               "081627c0583380...83d51cdfdb1c8"
        schemaURI:          "http://schemas.example.org/strictKYCSchema"
        attributes:         [
                {
                        label:          "firstname"
                        proof:          "db74c940d447e877d...cbc319bcfaeab97a"
                        state:          "PENDING"
                        confirmedAt:    "1469633204"
                        references:     [
                                {
                                    badgeLabel:     "badgeX"
                                    attributeLabel: "firstname"
                                    state:          "ACTIVE"
                                }
                        ]
                }
                {
                        label:          "lastname"
                        proof:          "55b5c51f867018...187e39a768aa8231ac"
                        state:          "PENDING"
                        confirmedAt:    "1469633204"
                        references:     [
                                {
                                    badgeLabel:     "badgeX"
                                    attributeLabel: "lastname"
                                    state:          "ACTIVE"
                                }
                        ]
                }
                {
                        label:          "ssn"
                        proof:          "efa5ff7eefcfbe4...e15edbb2095934aa0e0"
                        state:          "PENDING"
                        expiryPeriod:   "1_YEAR"
                        confirmedAt:    "1469633204"
                }
                { /* more attributes */ }
        ]
}
```

[0060] In dem oben stehenden Beispiel handelt es sich bei dem Ausweis um eine Datenstruktur, die Felder wie etwa „label“, „trustedParty“, „proofAlgo“ , „salt“, „schemaURI“ und „attributes“ beinhaltet. In einigen Ausführungsformen kann das Feld „label“ den Ausweis in einer DIR eindeutig kennzeichnen. Ein derartiges Feld kann den Zugriff auf verschiedene Ausweise in einer DIR vereinfachen.

[0061] In einigen Ausführungsformen kann das Feld „trustedParty“ einen Verweis auf eine vertrauenswürdige Entität beinhalten. In einigen Ausführungsformen kann die vertrauenswürdige Entität, auf die verwiesen wird, Zugang zu dem Ausweis erhalten und kann nur die vertrauenswürdige Entität, auf die verwiesen wird, autorisiert sein, eine Zustandsänderung einer Attributbestätigung in dem Ausweis zu veranlassen.

[0062] In einigen Ausführungsformen kann das Feld „proofAlg“ einen Algorithmus angeben, der verwendet wird, um einen oder mehrere in dem Ausweis gespeicherte kryptographische Nachweise zu berechnen. Der Algorithmus kann eine kryptographische Einwegfunktion, wie z. B. eine Hash-Funktion, nutzen. Als ein Beispiel kann eine Passwort-basierte Schlüsselableitungsfunktion 2 (Password-Based Key Derivation Function 2 - PBKDF2) z. B. mit einer ausgewählten pseudozufälligen Funktion (z. B. SHA256), einer ausgewählten Anzahl von Iterationen der pseudozufälligen Funktion (z. B. 10.000) und/oder einer ausgewählten Anzahl von Ausgabebytes (z. B. 32) verwendet werden. Es versteht sich jedoch, dass Aspekte der vorliegenden Offenbarung nicht auf die Verwendung eines bestimmten Algorithmus zum Berechnen kryptographischer Nachweise beschränkt sind.

[0063] In einigen Ausführungsformen kann in dem Feld „salt“ ein Zufallswert gespeichert sein, der als Eingabe in eine kryptografische Einwegfunktion beim Berechnen eines kryptographischen Nachweises zu verwenden ist.

[0064] In einigen Ausführungsformen kann das Feld „schemaURI“ einen Verweis auf ein Schema beinhalten, das zum Erzeugen des Ausweises verwendet wird. Ein nichteinschränkendes Beispiel für ein Schema ist nachfolgend bereitgestellt.

[0065] In einigen Ausführungsformen kann das Feld „attributes“ eine oder mehrere Attributbestätigungen beinhalten, wobei jede Attributbestätigung selbst eine Datenstruktur mit einem oder mehreren Feldern sein kann. Beispielsweise kann eine Attributbestätigung Felder wie etwa „label“, „proof“, „state“, „expiryPeriod“, „confirmedAt“ und „references“ beinhalten.

[0066] In einigen Ausführungsformen kann das Feld „label“ verwendet werden, um die Attributbestätigung in dem Ausweis eindeutig zu identifizieren.

[0067] In einigen Ausführungsformen kann in dem Feld „proof“ ein kryptographischer Nachweis für einen Wert eines bestätigten Attributs gespeichert sein. Beispielsweise kann der kryptographische Nachweis unter Verwendung des im Feld „proofAlg“ angegebenen Algorithmus mit dem im Feld „salt“ gespeicherten Zufallswert als zusätzliche Eingabe berechnet werden.

[0068] In einigen Ausführungsformen kann in dem Feld „state“ ein aktueller Zustand der Attributbestätigung gespeichert sein. Beispielsweise kann es sich bei der Attributbestätigung zu einem jeweiligen Zeitpunkt um einen der folgenden Zustände handeln: PENDING, VERIFIED, INVALID oder EXPIRED. Eine veranschaulichende Zustandsmaschine, die Übergänge zwischen diesen Zuständen steuert, ist in **Fig. 4** dargestellt und nachfolgend beschrieben.

[0069] In einigen Ausführungsformen kann in dem Feld „confirmedAt“ eine Zeit angegeben sein, zu welcher der Ausweis als letztes durch den Distributed Ledger bestätigt wurde.

[0070] In einigen Ausführungsformen kann das Feld „expiryPeriod“ eine Zeitlänge angeben, für welche die Attributbestätigung in dem VERIFIED-Zustand bleiben kann. Beispielsweise kann ein Ablaufdatum wie folgt berechnet werden: expiryDate = confirmedAt + expiryPeriod. Wenn das Ablaufdatum erreicht wird, kann ein interner Übergang ausgelöst werden und kann die Attributbestätigung von dem VERIFIED-Zustand in den INVALID-Zustand übergehen.

[0071] In einigen Ausführungsformen kann das Feld „references“ einen Verweis auf eine entsprechende Attributbestätigung in einem anderen Ausweis beinhalten. Beispielsweise kann das Feld „references“ ein Feld „badgeLabel“ [Ausweisbezeichnung], in dem eine Bezeichnung für den anderen Ausweis gespeichert ist, ein Feld „attributeLabel“, in dem eine Bezeichnung für die Attributbestätigung in dem anderen Ausweis, auf den verwiesen wird, gespeichert ist, und ein Feld „state“, das einen Zustand der Attributbestätigung, auf die verwiesen wird, angibt (z. B. ACTIVE, INVALIDATED, EXPIRED usw.), auf beinhalten.

[0072] Die Erfinder haben erkannt und verstanden, dass ein Verweis von einer Attributbestätigung in einem ersten Ausweis auf eine entsprechende Attributbestätigung in einem zweiten Ausweis in der gleichen DIR es der vertrauenswürdigen Entität, die für den ersten Ausweis zuständig ist, ermöglichen kann, sich auf die entsprechende Attributbestätigung in dem zweiten Ausweis zu stützen. Beispielsweise kann in dem oben stehenden Beispiel, wenn der Benutzer die in dem Feld „trustedParty“ angegebene vertrauenswürdige Entität dazu auffordert, einen Wert (z. B. John) der mit „firstname“ bezeichneten Attributbestätigung zu verifizieren, die vertrauenswürdige Entität eine entsprechende Attributbestätigung in einem anderen Ausweis (z. B. ein At-

tribut, das in einem mit „badgeX“bezeichneten Ausweis mit „firstname“ bezeichnet ist) prüfen. Wenn die Prüfung erfolgreich ist, kann die vertrauenswürdige Entität den im Feld „proof“ der mit „firstname“ bezeichneten Attributbestätigung gespeicherten Nachweis signieren, ohne einen aufwändigen Verifizierungsprozess (z. B. physisches Untersuchen des Passes des Benutzers, um zu bestätigen, dass der Vornahme des Benutzers tatsächlich John lautet) durchführen zu müssen.

[0073] In einigen Ausführungsformen kann, um die entsprechende Attributbestätigung in dem anderen Ausweis zu prüfen, die vertrauenswürdige Entität die im Feld „badgeLabel“ gespeicherte Bezeichnung (z. B. „badgeX“) verwenden, um den anderen Ausweis zu suchen, und kann die im Feld „attributeLabel“ gespeicherte Bezeichnung (z. B. „firstname“) verwenden, um die entsprechende Attributbestätigung in dem anderen Ausweis zu suchen. Die vertrauenswürdige Entität kann prüfen, ob sich das entsprechende Attribut in einem „VALID“-Zustand befindet, und kann einen in einem Feld „proofAlgo“ des anderen Ausweises angegebenen Algorithmus auf den vom Benutzer bereitgestellten Attributwert (z. B. John) und ein in einem Feld „salt“ des anderen Ausweises gespeichertes Salt verwenden, um zu prüfen, ob ein im Feld „proof“ gespeicherter Nachweis der entsprechenden Attributbestätigung tatsächlich durch Anwenden dieses Algorithmus auf den Attributwert und dieses Salt erzeugt wurde.

[0074] In einigen Ausführungsformen kann sich die vertrauenswürdige Entität nur dann auf die entsprechende Attributbestätigung in dem anderen Ausweis stützen, wenn die vertrauenswürdige Entität einer Entität vertraut, die in dem Feld „trustedParty“ des anderen Ausweises angegeben ist. Beispielsweise kann sich die vertrauenswürdige Entität dazu entscheiden, sich auf die Bestätigung zu stützen, wenn die im Feld „trustedParty“ des anderen Ausweises angegebene Entität eine Regierungsbehörde ist, kann sich jedoch entscheiden, sich nicht auf die Bestätigung zu stützen, wenn die im Feld „trustedParty“ des anderen Ausweises angegebene Entität eine Person oder Einrichtung ist, die der vertrauenswürdigen Entität nicht bekannt ist.

[0075] Während die Erfinder verschiedene Vorteile des Organisierens von Attributbestätigungen in Ausweisen erkannt und verstanden haben, versteht es sich, dass Aspekte der vorliegenden Offenbarung nicht auf die hier bereitgestellten konkreten Beispiele oder die Verwendung von Ausweisen allgemein beschränkt sind. In einigen Ausführungsformen können Attributbestätigungen auf eine andere Weise organisiert sein oder können einzeln verwaltet werden.

[0076] In einigen Ausführungsformen kann eine kryptographische Einwegfunktion in Kombination mit einem öffentlichen Salt und/oder einem oder mehreren privaten Salts verwendet werden. Beispielsweise kann ein öffentliches Salt ein Zufallswert sein, der von allen Attributbestätigungen in dem Ausweis geteilt, bei der Ausweiserzeugung berechnet und in dem Distributed Ledger veröffentlicht wird. Ein derartiges öffentliches Salt< kann als ein bindender Wert für den Ausweis verwendet werden.

[0077] Dahingegen kann in einigen Ausführungsformen ein privates Salt ein Zufallswert sein, der unabhängig für jedes Attribut jedes Mal berechnet wird, wenn ein Wert des Attributs verifiziert wird, und nicht in dem Distributed Ledger veröffentlicht wird. Um es einer vertrauenswürdigen Entität zu ermöglichen, einen Wert des Attributs zu verifizieren, können das für dieses Attribut berechnete private Salt und diese bestimmte Verifizierung mit der vertrauenswürdigen Entität über einen sicheren nicht im Ledger erfassten Kanal zusammen mit dem Wert des Attributs ausgetauscht werden.

[0078] In einigen Ausführungsformen kann ein kryptographischer Nachweis für einen Attributwert wie folgt berechnet werden:

(1) public_salt = random(X), wobei die Funktion random() an Eingabe X eine zufällige Bytefolge der Länge X ausgibt.

(2) private_salt = random(Y), wobei die Funktion random() an Eingabe Y eine zufällige Bytefolge der Länge Y ausgibt.

(3) proof = HASH(public_salt || private_salt || attribute_value),
wobei || eine Verkettungsfunktion für Bytefolgen ist.

[0079] In einigen Ausführungsformen kann die Funktion HASH() eine Einwegfunktion sein, die komplexer als ein einfacher kryptographischer Hash ist. Beispielsweise kann ein PBKDF2-Algorithmus in Verbindung mit einer starken Hash-Funktion (z. B. SHA256), einer ausreichend großen Anzahl von Iterationen (z. B. 10.000) und/oder einer ausreichend großen Anzahl von ausgegebenen Bytes (z. B. 32) verwendet werden, um mögliche Angreifer zu verlangsamen, wodurch die Widerstandsfähigkeit gegen gezielte Brute-Force-Angriffe verbessert wird. Es versteht sich jedoch, dass Aspekte der vorliegenden Offenbarung nicht auf die Verwendung

eines bestimmten Nachweisalgorithmus beschränkt sind. In einigen Ausführungsformen können verschiedene Nachweisalgorithmen für verschiedene Ausweise, selbst jene in derselben DIR, verwendet werden.

[0080] In einigen Ausführungsformen können, um die Sicherheit zu verbessern, Salt-Werte derart ausgewählt werden, dass sie mindestens so viele Bits wie eine Ausgabe der Funktion HASH() aufweisen. Derartige Salts können unabhängig in einem PDS berechnet werden. Beispielsweise können öffentliche Salts nicht zwischen Ausweisen wiederverwendet werden und können private Salts nicht zwischen Attributbestätigungen wiederverwendet werden.

[0081] Die Erfinder haben erkannt und verstanden, dass die Verwendung eines privaten Salts das Ungültigmachen einer bestehenden Bestätigung ermöglichen kann, auch wenn sich der Attributwert nicht verändert. Beispielsweise kann eine bestätigende Entität (z. B. eine Wirtschaftsauskunftei) eine vorherige Bestätigung durch eine neue Bestätigung unter Verwendung eines neuen privaten Salts ersetzen, um einen neuen Nachweis für denselben Attributwert zu erzeugen. Aspekte der vorliegenden Offenbarung sind jedoch nicht auf die Verwendung eines privaten Salts beschränkt, da in einigen Ausführungsformen kein privates Salt verwendet werden kann und damit sämtliche vorhergehenden Bestätigungen gültig bleiben können. Zudem sind Aspekte der vorliegenden Offenbarung nicht auf die Verwendung eines öffentlichen Salts beschränkt. Beispielsweise können in einigen Ausführungsformen private Salts anstelle eines öffentlichen Salts verwendet werden.

[0082] In einigen Ausführungsformen kann ein Ausweis auf Grundlage eines Ausweisschemas erzeugt werden (auf das in einem Feld „schema“ des Ausweises verwiesen werden kann). Ein Ausweisschema kann beschreiben, welche Daten in einem Ausweis gespeichert werden können, wie die Daten organisiert sein können, schematische Beziehungen zwischen den Daten und/oder Regeln, die steuern, wie die Daten verwaltet werden können. In einigen Ausführungsformen kann ein Ausweisschema unter Verwendung einer semantischen Sprache, wie z. B. W3C Web Ontology Language (OWL) oder Resource Description Framework Schema (RDFS), geschrieben sein. Dies ist jedoch nicht zwingend erforderlich, da in einigen Ausführungsformen zudem eine Auszeichnungssprache wie etwa XML verwendet werden kann. Ein nichteinschränkendes Beispiel für ein Ausweisschema ist nachfolgend bereitgestellt.

```
{
        id: "http://schemas.example.org/strictKYCSchema"
        schemaType: "001 - KYC for Individuals"
        riskProfile: "Low"
        description: "The following schema defines attributes needed for a Know Your
        Customer (KYC) check of a low risk individual."
        attributes: [
                {
                        label: "firstname"
                        description: "The first name of the person as specified."
                        required: true
                        validationCriteria: "Must match the first name on a government issued
                        photo ID.  Checked in person or via high quality scan of the photo ID,
                        transmitted via secure digital channel."
                        enhancedPrivacy: "The label can be protected by substituting the label
                        'firstname' with a related one-way salted hash."
                        storageLocation: "PDS"
                        dataType: "String"
                        format: "Plaintext or Hashed"
                }
                {
                        label: "lastname"
                        required: true
                        validationCriteria: "Must match the last name on the government
                        issued photo ID used to check the first name.  Checked in person or via
                        high quality scan of the photo ID, transmitted via secure digital
                        channel."
                        enhancedPrivacy: "The label can be protected by substituting the label
                        'lastname' with a related one-way salted hash."
                        storageLocation: "PDS"
                        dataType: "String"
                        format: "Plaintext or Hashed"
                }
                {
                        label: "ssn"
                        required: true
                        validationCriteria: "Social Security Number must be related to the
                        same person shown on the government issued photo ID used to check
                        the first name and the last name "
                        enhancedPrivacy: "The label can be protected by substituting the label
                        'ssn' with a related one-way salted hash."
                        dataType: "String"
                        storageLocation: "PDS"
                        format: "Plaintext or Hashed"
                }
                { /* more attribute specifications */ }
        ]
}
```

In dem oben stehenden Beispiel definiert das Ausweisschema einen Satz von Attributen, für die Bestätigungen in einem Ausweis enthalten sein können. Jede Attributbestätigung kann ausgefüllt werden, wenn der Ausweis erzeugt wird, oder kann dem Ausweis zu einem späteren Zeitpunkt hinzugefügt werden. In einigen Ausführungsformen kann ein Ausweisschema eine oder mehrere Regeln definieren, die steuern, wie eine Attributbestätigung zu verwalten ist. Beispielsweise kann eine Regel festlegen, dass ein Ablaufzeitraum für eine Attributbestätigung zwischen 5 Jahren und 10 Jahren liegen muss.

[0083] Die Erfinder haben erkannt und verstanden, dass Ausweisschemata es ermöglichen können, dass Ausweise auf standardisierte Weise erzeugt werden. Dies kann eine Zuordnung zwischen zu verschiedenen Zwecken erzeugten Ausweisen vereinfachen, wodurch sich wiederum die Interoperabilität verschiedener Systeme innerhalb derselben Vertikalen (z. B. verschiedene Finanzinstitute) oder über verschiedene Vertikalen (z. B. eine Regierungsbehörde wie etwa die Transportsicherheitsbehörde oder TSA unter Verwendung eines „Kenne deinen Kunden"- oder KYC-Bankenschemas zum Verifizieren von Fahrgastidentitäten) verbessern kann. Es versteht sich jedoch, dass Aspekte der vorliegenden Offenbarung nicht auf die Verwendung von Ausweisschemata zum Erzeugen von Ausweisen beschränkt sind.

[0084] **Fig. 4** zeigt eine veranschaulichende Zustandsmaschine **400**, die Übergänge zwischen verschiedenen Zuständen einer Attributbestätigung gemäß einigen Ausführungsformen steuert. Beispielsweise kann die Zustandsmaschine **400** Zustandsübergänge von Attributbestätigungen in einem oder mehreren der in **Fig. 3** dargestellten veranschaulichenden Ausweise **306** steuern.

[0085] In einigen Ausführungsformen kann, wenn ein Ausweis mit einer Attributbestätigung erzeugt wird (oder wenn eine Attributbestätigung einem bestehenden Ausweis hinzugefügt wird), die Attributbestätigung auf einen PENDING-Zustand initialisiert werden. In diesem Zustand kann die Attributbestätigung weder gültig noch ungültig sein.

[0086] In einigen Ausführungsformen kann ein Benutzer, für den der Ausweis erzeugt wird, anfordern, dass eine dem Ausweis zugeordnete vertrauenswürdige Entität einen Wert des Attributs verifiziert. Falls die vertrauenswürdige Entität den Wert des Attributs verifiziert, kann die vertrauenswürdige Entität veranlassen, dass sich die Attributbestätigung in einem VERIFIED-Zustand befindet. Falls die vertrauenswürdige Entität den Wert des Attributs ablehnt, kann die vertrauenswürdige Entität veranlassen, dass sich die Attributbestätigung in einem INVALID-Zustand befindet.

[0087] In einigen Ausführungsformen kann, falls sich die Attributbestätigung in dem VERIFIED-Zustand, dem EXPIRED-Zustand oder dem INVALID-Zustand befindet und der Benutzer veranlasst, dass das Attribut einen anderen Wert aufweist, die Attributbestätigung in den PENDING-Zustand zurückkehren.

[0088] In einigen Ausführungsformen kann, falls sich die Attributbestätigung in dem VERIFIED-Zustand befindet und die vertrauenswürdige Entität die vorherige Verifizierung widerruft, die vertrauenswürdige Entität veranlassen, dass sich die Attributbestätigung im INVALID-Zustand befindet.

[0089] In einigen Ausführungsformen kann, falls sich die Attributbestätigung in dem VERIFIED-Zustand befindet und ein Ablaufzeitraum verstreicht, die Attributbestätigung in einen EXPIRED-Zustand übergehen, in dem die Attributbestätigung bleiben kann, bis die vertrauenswürdige Entität den Wert des Attributs erneut verifiziert.

[0090] Es versteht sich, dass die Zustandsmaschine **400** lediglich zur Veranschaulichung in **Fig. 4** dargestellt und vorstehend beschrieben ist, da Aspekte der vorliegenden Offenbarung nicht auf eine bestimmte Kombination aus Zuständen und/oder Zustandsübergängen beschränkt sind.

[0091] In einigen Ausführungsformen kann ein Zustand einer verweisenden Attributbestätigung mit dem einer Attributbestätigung, auf die verwiesen wird, synchronisiert werden. Dies ist jedoch nicht zwingend erforderlich, da in einigen Ausführungsformen Zustandsänderungen einer verweisenden Attributbestätigung unabhängig von Zustandsänderungen einer Attributbestätigung sein können, auf die verwiesen wird.

[0092] Wie oben erörtert, kann eine DIR Regeln beinhalten, die steuern, wie Zustandsübergänge ausgelöst werden können und/oder welche Entitäten welche Übergänge auslösen können. Beispielsweise können derartige Regeln durch eine Aktions- und Ereignisspezifikation (z. B. die in **Fig. 3** dargestellte veranschaulichende Aktions- und Ereignisspezifikation **304**) erfasst werden. Nichteinschränkende Beispiele für Aktionen (z. B. Zustandsänderungen und/oder Nachweisaktualisierungen), die über eine DIR durchgeführt werden können, sind in der nachfolgenden Tabelle aufgeführt.

Aktion	Eingabe/Ausgabe	Attributzustand/-zustände	Nebenwirkung
createBadge	Eingabe (1) Ausweisbezeichnung (2) Vertrauenswürdige Entität Ausgabe: Keine	Keine	„Ausweis-erzeugt-Ereignis“ ausgelöst
setAttribute	(1) Ausweisbezeichnung (2) Attributbezeichnung (3) Attributnachweis	PENDING	„Attribut-festgelegt-Ereignis“ ausgelöst
submitVerification-Request	Eingabe (1) Ausweisbezeichnung Ausgabe: Keine	Keine	„Verifizierungsanforderungsereignis“ ausgelöst
changeAttribute-State	Eingabe (1) Ausweisbezeichnung (2) Attributbezeichnung (3) Attributzustand Ausgabe: Keine	PENDING zu VERIFIED oder INVALID	„Attributzustandsänderungsereignis“ ausgelöst

[0093] In einigen Ausführungsformen kann eine „createBadge“-Aktion als Eingabe eine Ausweisbezeichnung und eine Kennung für eine vertrauenswürdige Entität verwenden. Infolge einer DIR eines Benutzers, der die „createBadge“-Aktion ausführt, kann ein Ausweis mit der Eingabe Ausweisbezeichnung in einem Feld „label“ und der eingegebenen Kennung für die vertrauenswürdige Entität in einem Feld „trustedParty“ erzeugt werden. Zusätzlich oder alternativ dazu kann ein „Ausweis erzeugt“-Ereignis ausgelöst werden, das den neu erzeugten Ausweis in dem Distributed Ledger veröffentlichen kann.

[0094] In einigen Ausführungsformen kann eine „setAttribute“-Aktion als Eingabe eine Ausweisbezeichnung, eine Attributbezeichnung und einen Attributnachweis verwenden. Infolge einer DIR eines Benutzers, der die „setAttribute“-Aktion ausführt, kann ein Feld „attributes“ eines Ausweises, der durch die eingegebene Ausweisbezeichnung angegeben wird, aktualisiert werden. Beispielsweise kann eine durch die eingegebene Attributbezeichnung angegebene Attributbestätigung hinzugefügt und/oder mit dem eingegebenen Attributnachweis in einem Feld „proof“ modifiziert werden. Zusätzlich oder alternativ dazu kann ein Zustand der Attributbestätigung auf PENDING festgelegt werden und/oder kann ein „Attribut festgelegt“-Ereignis ausgelöst werden, das diese Veränderungen der Attributbestätigung in dem Distributed Ledger veröffentlichen kann.

[0095] In einigen Ausführungsformen kann eine „submitVerificationRequest“-Aktion als Eingabe eine Ausweisbezeichnung verwenden. Infolge einer DIR eines Benutzers, der die „setAttribute“-Aktion ausführt, kann ein „Verifizierungsanforderung“-Ereignis ausgelöst werden, das veranlassen kann, dass eine Verifizierungsanforderung an eine DIR einer vertrauenswürdigen Entität gesendet wird, die für den durch die eingegebene Ausweisbezeichnung angegebenen Ausweis zuständig ist.

[0096] In einigen Ausführungsformen kann eine „changeAttributeState“-Aktion als Eingabe eine Ausweisbezeichnung, eine Attributbezeichnung und einen Attributzustand (z. B. VERIFIED oder INVALID) verwenden. Infolge einer DIR einer vertrauenswürdigen Entität, welche die „changeAttributeState“-Aktion ausführt, kann ein Feld „attributes“ eines durch die eingegebene Ausweisbezeichnung angegebenen Ausweises aktualisiert werden. Beispielsweise kann eine durch die eingegebene Attributbezeichnung angegebene Attributbestätigung mit dem eingegebenen Attributzustand (z. B. VERIFIED oder INVALID) in einem Feld „state“ modifiziert werden. Zusätzlich oder alternativ dazu kann ein „Attributzustandsänderung“-Ereignis ausgelöst werden, das diese Änderung der Attributbestätigung in dem Distributed Ledger veröffentlichen kann.

[0097] Nichteinschränkende Beispiele für „Ausweis erzeugt“-, „Attribut festgelegt“-, „Verifizierungsanforderung“- und „Attributzustandsänderung“-Ereignisse sind in der nachfolgenden Tabelle aufgeführt.

Ausweis-erzeugt -Ereignis		
Felder	Anrufer	GUII der Entität, die dieses Ereignis ausgelöst hat
	Ausweis	Bezeichnung des erzeugten Ausweises
	Vertrauenswürdige Partei	GUII der vertrauenswürdigen Entität, die dafür zuständig ist, Attributwerte zu verifizieren und die Richtigkeit derselben nachzuweisen
Verifizierungsanforderungsereignis Beispiel		
Felder	Anrufer	GUII der Entität, die dieses Ereignis erzeugt hat
	Ausweis	Bezeichnung des zu verifizierenden Ausweises
Attribut-festgelegt-Ereignis Beispiel		
Felder	Anrufer	GUII der Entität, die dieses Ereignis erzeugt hat
	Ausweis	Bezeichnung des Ausweises, in dem der Attributwert festgelegt wird
	Attributschlüssel	Bezeichnung des Attributs, für das ein Wert festgelegt wird
	Attributwert	Ein oder mehrere kryptographische Nachweise für den Attributwert
Attributzustand-ändern-Ereignis Beispiel		
Felder	Anrufer	GUII der Entität, die dieses Ereignis erzeugt hat
	Ausweis	Bezeichnung des Ausweises, in dem die Attributbestätigung ihren Zustand ändert
	Attributschlüssel	Bezeichnung der Attributbestätigung, die ihren Zustand ändert
	Alter Zustand	Zustand der Attributbestätigung vor dem Zustandsübergang
	Neuer Zustand	Zustand der Attributbestätigung nach dem Zustandsübergang

[0098] In einigen Ausführungsformen können Attributwerte durch vertrauenswürdige Entitäten, wie z. B. Regierungsbehörden (z. B. Passbehörden), Arbeitgeber, Finanzinstitute usw., verifiziert werden. Eine vertrauenswürdige Entität kann einen Wert eines Attributs verifizieren, indem sie z. B. physische Dokumente (z. B. Geburtsurkunden, Führerscheine, Sozialversicherungsausweise, Gehaltsabrechnungen usw.) prüft und/oder einen Benutzer persönlich befragt. Nach erfolgreicher Verifizierung kann die vertrauenswürdige Entität veranlassen, dass eine entsprechende Attributbestätigung in einem VERIFIED-Zustand vorliegt. Wenn es ein Problem gibt, kann die vertrauenswürdige Entität veranlassen, dass die entsprechende Attributbestätigung in einem INVALID-Zustand vorliegt.

[0099] **Fig. 5** zeigt einen veranschaulichenden Prozess **500** zur Bestätigung durch eine vertrauenswürdige Entität gemäß einigen Ausführungsformen. Beispielsweise kann der Prozess **500** zwischen einem Benutzer und einem Finanzinstitut während einer „Kenne deinen Kunden“(KYC)-Prüfung durchgeführt werden.

[0100] In einigen Ausführungsformen kann der Benutzer vor Einleiten des Prozesses **500** mit der vertrauenswürdigen Entität über eine oder mehrere nicht im Ledger erfasste Schnittstellen in einer Anwendungsschicht (z. B. der in **Fig. 1** dargestellten veranschaulichenden Anwendungsschicht) kommunizieren. Beispielsweise kann der Benutzer die Website der vertrauenswürdigen Entität besuchen und/oder eine App der vertrauenswürdigen Entität herunterladen und starten. Eine derartige Kommunikation in der Anwendungsschicht kann einen PDS des Benutzers oder einen PDS der vertrauenswürdigen Entität dazu veranlassen, bei Schritt **505** einen Handshake in einer Datenschutzschicht (z. B. der in **Fig. 2** dargestellten veranschaulichenden Datenschutzschicht) einzuleiten. Über diesen Handshake kann der PDS der vertrauenswürdigen Entität bestätigen, dass die vertrauenswürdige Entität dafür zuständig sein wird, einen oder mehrere Attributwerte zu verifizieren. Zusätzlich oder alternativ dazu kann der PDS der vertrauenswürdigen Entität an den PDS des Benutzers eine GUII der vertrauenswürdigen Entität und/oder ein Schema zum Erzeugen eines Ausweises mit einer oder mehreren Attributbestätigungen (z. B. jene, die für den KYC-Prozess relevant sind) senden.

[0101] Bei Schritt **510** kann der PDS des Benutzers einen Ausweis (z. B. unter Verwendung einer GUII der vertrauenswürdigen Entität und/oder gemäß einem Schema, das von dem PDS der vertrauenswürdigen Entität bereitgestellt wird) erzeugen und kann den Ausweis in einem Distributed Ledger in einer Vertrauensschicht (z. B. der in **Fig. 1** dargestellten veranschaulichenden Vertrauensschicht) veröffentlichen. Der PDS des Benutzers kann dann bei Schritt **515** an den PDS der vertrauenswürdigen Entität über nicht im Ledger erfasste Kommu-

nikation einen Verweis auf die DIR des Benutzers zusammen mit einem oder mehreren zu verifizierenden Attributwerten senden. In einigen Ausführungsformen kann die DIR des Benutzers ein im Ledger erfasstes Ereignis (z. B. ein „Verifizierungsanforderung“-Ereignis) auslösen, um die DIR der vertrauenswürdigen Entität zu benachrichtigen.

[0102] Bei Schritt **520** kann die DIR der vertrauenswürdigen Entität den bei Schritt **515** empfangenen Verweis verwenden, um den Ausweis in dem Distributed Ledger zu suchen. Für jede Attributbestätigung in dem Ausweis kann die DIR der vertrauenswürdigen Entität prüfen, ob kryptographische Nachweise in dem Ausweis aus den empfangenen Attributwerten unter Verwendung eines in dem Ausweis angegebenen Algorithmus erzeugt werden. Dann kann die DIR der vertrauenswürdigen Entität dazu übergehen, die empfangenen Attributwerte zu verifizieren (z. B. entweder indirekt über einen Ausweis, auf den verwiesen wird, oder direkt durch die vertrauenswürdige Entität selbst).

[0103] Beispielsweise kann die DIR der vertrauenswürdigen Entität für eine jeweilige Attributbestätigung prüfen, ob es einen Verweis auf einen anderen Ausweis gibt. Wenn dies der Fall ist, kann die DIR der vertrauenswürdigen Entität nach dem anderen Ausweis in dem Distributed Ledger suchen und kann eine oder mehrere Prüfungen durchführen. Beispielsweise kann die vertrauenswürdige Entität prüfen, ob eine Entität, die den anderen Ausweis verifiziert hat, vertrauenswürdig ist, wird ein kryptographischer Nachweis in dem anderen Ausweis aus dem empfangenen Attributwert unter Verwendung eines in dem anderen Ausweis angegebenen Algorithmus erzeugt und/oder wird der andere Ausweise durch die verifizierende Entität signiert. Es kann ein beliebiges geeignetes elektronisches Signaturschema verwendet werden, da Aspekte der vorliegenden Offenbarung nicht darauf beschränkt sind.

[0104] Zusätzlich oder alternativ dazu kann die vertrauenswürdige Entität den empfangenen Attributwert direkt verifizieren, indem sie z. B. physische Dokumente prüft und/oder den Benutzer persönlich befragt.

[0105] Wenn es kein Problem gibt, kann die DIR der vertrauenswürdigen Entität den Ausweis signieren und veranlassen, dass sich jede Attributbestätigung in dem Ausweis in einem VERIFIED-Zustand befindet. Wenn eine oder mehrere problematische Attributbestätigungen vorliegen, kann die DIR der vertrauenswürdigen Entität veranlassen, dass sich eine solche Attributbestätigung in einem INVALID-Zustand befindet.

[0106] In einigen Ausführungsformen können Entitäten eine Vertrauensstruktur bilden, in der eine Entität einer oder mehreren anderen Entitäten vertrauen kann und sich auf Attributbestätigungen stützen kann, die von einer beliebigen der einen oder mehreren vertrauenswürdigen Entitäten signiert wurden (z. B. wie oben in Verbindung mit **Fig. 5** erörtert). Auf diese Weise kann eine Entität dazu imstande sein, eine Attributbestätigung zu verifizieren, ohne eine physische Verifizierung durchführen zu müssen.

[0107] Eine Vertrauensstruktur kann eine beliebige geeignete Anzahl von Entitäten mit einer beliebigen geeigneten Vertrauensbeziehung zwischen den Entitäten beinhalten. Überdies kann sich die Mitgliedschaft in einer Vertrauensstruktur mit der Zeit weiterentwickeln, während bestehende Mitglieder austreten, neue Mitglieder eintreten und/oder sich Vertrauensverhältnisse ändern.

[0108] **Fig. 6** zeigt eine veranschaulichende Vertrauensstruktur **600** gemäß einigen Ausführungsformen. In diesem Beispiel gibt es vier Ausweise **605A**-**D** in einer DIR. Die Ausweise **605A**-**D** können vertrauenswürdigen Entitäten A, B, C bzw. D entsprechen. Der Ausweis **605A** kann die folgenden Attributbestätigungen beinhalten: „Vorname“, „Nachname“, „Sozialversicherungsnummer“ und „Privatadresse“, die allesamt direkt durch die Entität A (z. B. eine Bank) verifiziert wurden.

[0109] In einigen Ausführungsformen kann der Ausweis **605C** die folgenden Attributbestätigungen beinhalten: „Privatadresse“, „Vorname“, „Nachname“ und „E-Mail-Adresse“. Jede dieser Attributbestätigungen kann direkt durch die Entität C (z. B. einen Onlinehändler) verifiziert worden sein, mit der Ausnahme, dass die Attributbestätigung „Privatadresse“ einen Verweis auf den Ausweis **605A** enthält, was anzeigt, dass die Entität C der Entität A in Bezug auf die Attributbestätigung „Privatadresse“ vertraut. Dies kann es der Entität C ermöglichen, einen Zustand der Attributbestätigung „Privatadresse“ in dem Ausweis **605A** zu sehen.

[0110] In einigen Ausführungsformen kann der Ausweis **605D** die folgenden Attributbestätigungen beinhalten: „Postadresse“, „vollständiger Name“, „Sozialversicherungsnummer“ und „Beziehungsstatus“. Jede dieser Attributbestätigungen kann direkt durch die Entität D (z. B. einen Anbieter sozialer Netzwerkdienste) verifiziert worden sein, mit der Ausnahme, dass die Attributbestätigung „Privatadresse“ einen Verweis auf den Ausweis **605A** enthält, was anzeigt, dass die Entität D der Entität A in Bezug auf die Attributbestätigung „Privatadresse“

vertraut. Dies kann es der Entität **D** ermöglichen, einen Zustand der Attributbestätigung „Privatadresse“ in dem Ausweis **605A** zu sehen.

[0111] In einigen Ausführungsformen kann der Ausweis **605B** die folgenden Attributbestätigungen beinhalten: „Nachname“, „Vorname“, „Passnummer“ und „Telefonnummer“. Jede dieser Attributbestätigungen kann direkt durch die Entität B (z. B. ein Reisebüro) verifiziert worden sein, mit der Ausnahme, dass die Attributbestätigung „Nachname“ einen Verweis auf den Ausweis **605A** und einen Verweis auf den Ausweis **605C** enthält, was anzeigt, dass die Entität B die Attributbestätigung „Nachname“ nur dann signieren kann, wenn sowohl die Entität A als auch die Entität C direkt und unabhängig den Attributwert für „Nachname“ verifiziert haben. Dies kann es der Entität B ermöglichen, einen Zustand der Attributbestätigung „Nachname“ in dem Ausweis **605A** und einen Zustand der Attributbestätigung „Nachname“ in dem Ausweis **605C** zu sehen.

[0112] Somit kann in dem in **Fig. 6** dargestellten Beispiel die Attributbestätigung „Privatadresse“ einen Vertrauenskreis aufweisen, der drei Entitäten, A, C und D, beinhaltet, wobei die Entität A den Attributwert für „Nachname“ direkt sorgfältig verifiziert hat und sich die Entitäten C und D auf die Bestätigung von A in Bezug auf die „Privatadresse“ stützen. Dahingegen kann die Attributbestätigung „Nachname“ einen Vertrauenskreis aufweisen, der drei Entitäten, A, B und C, beinhaltet, wobei die Entitäten A und C unabhängig den Attributwert für „Nachname“ direkt sorgfältig verifiziert haben und sich die Entität C auf die Bestätigung von A in Bezug auf die „Privatadresse“ stützt.

[0113] **Fig. 7** zeigt einen veranschaulichenden Prozess **700** für Gegenparteiüberprüfungen gemäß einigen Ausführungsformen. In diesem Beispiel kann ein Benutzer A mit einem Benutzer B interagieren. Beispielsweise kann der Benutzer A ein Käufer bei einer Immobilientransaktion sein und kann der Benutzer B der Verkäufer sein. Der Prozess **700** kann entweder durch den Benutzer A oder den Benutzer B eingeleitet werden.

[0114] In einigen Ausführungsformen können die Benutzer A und B vor dem Prozess **700** über einen oder mehrere nicht im Ledger erfasste Kanälen kommunizieren. Beispielsweise können die Benutzer A und B indirekt (z. B. über einen oder mehrere Vermittler) oder direkt (z. B. per E-Mail) kommunizieren. Infolge einer solchen Kommunikation kann der Benutzer A einen PDS des Benutzers A dazu anweisen, bei Schritt **705** einen Handshake in einer Datenschutzschicht (z. B. der in **Fig. 1** dargestellten veranschaulichenden Datenschutzschicht) mit einem PDS des Benutzers B oder umgekehrt einzuleiten.

[0115] Zusätzlich oder alternativ dazu können die Benutzer A und B über eine oder mehrere nicht im Ledger erfasste Schnittstellen in einer Anwendungsschicht (z. B. der in **Fig. 1** dargestellten veranschaulichenden Anwendungsschicht) kommunizieren. Eine derartige Kommunikation in der Anwendungsschicht kann einen PDS des Benutzers A oder einen PDS des Benutzers B dazu veranlassen, bei Schritt **705** einen Handshake in einer Datenschutzschicht (z. B. der in **Fig. 1** dargestellten veranschaulichenden Datenschutzschicht) einzuleiten.

[0116] Bei Schritt **710** können der PDS des Benutzers A und der PDS des Benutzers B personenbezogene Daten (z. B. vollständige Namen, Privatadressen, E-Mail-Adressen, Telefonnummer usw.) und/oder Verweise auf jeweilige DIR austauschen. Falls Ausweise verwendet werden, um Attributbestätigungen zu organisieren, können Bezeichnungen jeweiliger Ausweise ebenfalls ausgetauscht werden. In einigen Ausführungsformen kann derselbe Satz von personenbezogenen Daten von jeder Seite bereitgestellt werden. Dies ist jedoch nicht zwingend erforderlich, da der Benutzer A Informationen von dem Benutzer B anfordern kann, die nicht durch den Benutzer B von dem Benutzer A angefordert werden, und umgekehrt.

[0117] In einigen Ausführungsformen kann die DIR des Benutzers A die von dem Benutzer B empfangenen Informationen verwenden, um eine Attributbestätigung in dem Distributed Ledger zu suchen und eine oder mehrere Prüfungen durchzuführen. Beispielsweise kann die DIR des Benutzers A prüfen, ob eine Entität, welche die Attributbestätigung verifiziert hat, vertrauenswürdig ist, sich die Attributbestätigung in einem VERIFIED-Zustand befindet, ein kryptographischer Nachweis in der Attributbestätigung unter Verwendung eines Algorithmus, der in einem Ausweis angegeben ist, der die Attributbestätigung enthält, aus einem entsprechenden von dem Benutzer B empfangenen Attributwert erzeugt wird und/oder die Attributbestätigung von der verifizierenden Entität signiert wird. Die DIR des Benutzers B kann ähnliche Prüfungen durchführen.

[0118] Die Erfinder haben erkannt und verstanden, dass es wünschenswert sein kann, die Sicherheit einer Umgebung, die eine Komponente einer Datenschutzschicht (z. B. einen PDS) hostet, zu erhöhen. Zusätzlich oder alternativ dazu kann es wünschenswert sein, die Zugangskontrolle zu einer Datenschutzschicht und/oder einer Vertrauensschicht zu verbessern.

[0119] In einigen Ausführungsformen kann die Sicherheit in einer Host-Umgebung verbessert werden, indem Daten verschlüsselt werden, die von einer Komponente einer Datenschutzschicht (z. B. einem PDS) gehandhabt werden, sodass eine Host-Entität (z. B. ein Anbieter einer öffentlichen Cloud) möglicherweise nicht dazu imstande ist, auf die Daten zuzugreifen, da sie auf einen physischen oder virtuellen Datenträger geschrieben sind. Eine derartige Verschlüsselung kann zusätzlich zum Umsetzen der Komponente der Datenschutzschicht in einer virtualisierten Umgebung (z. B. ein PDS je virtuelle Maschine, aber mehrere PDS je physische Maschine) oder einer dedizierten Umgebung (z. B. ein PDS je physische Maschine) erfolgen. Es versteht sich jedoch, dass Aspekte der vorliegenden Offenbarung nicht auf eine solche Datenverschlüsselung beschränkt sind.

[0120] In einigen Ausführungsformen können ein oder mehrere Verschlüsselungsschlüssel außerhalb einer Komponente einer Datenschutzschicht (z. B. eines PDS) gespeichert werden, sodass eine Host-Entität möglicherweise keinen Zugang zu dem einen oder den mehreren Verschlüsselungsschlüsseln hat. Es kann ein beliebiges geeignetes Schlüsselverwaltungsschema verwendet werden. Beispielsweise kann ein Schlüssel von einem Benutzer der Komponente der Datenschutzschicht geführt werden.

[0121] In einigen Ausführungsformen kann Datenänderungen in einer Datenschutzschicht und/oder Zustandsänderungen in einer Vertrauensschicht eine Zugangssteuerung auferlegt werden. **Fig. 8** zeigt einen veranschaulichenden Prozess **800** für einen Datenaustausch in einer Komponente einer Datenschutzschicht (z. B. einem PDS) und eine resultierende Zustandsänderung in einer Komponente einer Vertrauensschicht (z. B. einer DIR) gemäß einigen Ausführungsformen.

[0122] In dem in **Fig. 8** dargestellten Beispiel wird der Prozess **800** durch einen Benutzer eingeleitet, der versucht, ein Element von personenbezogenen Daten, das in der Komponente der Datenschutzschicht gespeichert ist, zu ändern, wodurch eine Zugangskontrollprüfung auf der Datenschutzschicht ausgelöst werden kann. In einigen Ausführungsformen kann ein Zugangskontrollmechanismus der Datenschutzschicht einen Authentifizierungs- und/oder Autorisierungsprozess beinhalten, der je nach Art der vom Benutzer angeforderten Aktion mehr oder weniger streng sein kann. Beispielsweise kann ein Versuch, kritische Daten (z. B. Passnummer) zu ändern, einen strengeren Authentifizierungsprozess (z. B. eine Multifaktor-Authentifizierung) auslösen als ein Versuch, nichtkritische Daten (z. B. E-Mail-Adresse) zu ändern. Somit kann eine stärkere Sicherheit auf eine granuläre Weise je nach der Sensibilität einer angeforderten Datenänderung bereitgestellt werden.

[0123] In einigen Ausführungsformen kann eine erfolgreiche Authentifizierung und/oder Autorisierung auf der Datenschutzschicht es dem Benutzer ermöglichen, den versuchten Datenaustausch auf der Komponente der Datenschutzschicht abzuschließen. Zusätzlich oder alternativ dazu kann die Komponente der Datenschutzschicht in Reaktion auf eine erfolgreiche Authentifizierung und/oder Autorisierung einen oder mehrere Schlüssel der Vertrauensschicht zur Verwendung beim Zugreifen auf die Vertrauensschicht abrufen. Beispielsweise kann ein Schlüssel der Vertrauensschicht ein kryptographischer Schlüssel sein, der anzugeben ist, um eine Berechtigung dafür nachzuweisen, eine Komponente der Vertrauensschicht dazu zu veranlassen, eine oder mehrere Aktionen durchzuführen.

[0124] In einigen Ausführungsformen können verschiedene Schlüssel der Vertrauensschicht angegeben werden, um eine Berechtigung dafür nachzuweisen, verschiedene Arten von Aktionen durchzuführen. Beispielsweise kann ein Schlüssel, der einer höheren Berechtigungsebene zugeordnet ist, angegeben werden, um eine Berechtigung dafür nachzuweisen, kritische Daten (z. B. Passnummer) zu ändern, im Vergleich zu einem Versuch, nichtkritische Daten (z. B. E-Mail-Adresse) zu ändern. In einigen Ausführungsformen kann die Komponente der Datenschutzschicht dazu angewiesen werden, eine oder mehrere Aktionen (z. B. eine Zustandsänderung) nur dann durchzuführen, wenn die erforderliche Autorisierung erhalten wurde (z. B. durch Angeben eines oder mehrerer geeigneter Schlüssel).

[0125] Zusätzlich oder alternativ dazu können ein oder mehrere Zugangsregeln bereitgestellt werden, die eine dynamische Zugangskontrolle auf Grundlage eines Kontextes ermöglichen. Auf diese Weise kann ein Zugang nicht nur von einer Art einer angeforderten Aktion abhängig sein, sondern auch von einer oder mehreren externen Bedingungen, wodurch sich die Sicherheit verbessert. Beispielsweise können strengere Zugangsregeln durchgesetzt werden, wenn ein laufender Angriff vorliegt.

[0126] In einigen Ausführungsformen kann eine Entität (z. B. ein Benutzer oder eine Einrichtung) mehreren kryptographischen Schlüsseln zugeordnet sein. Die Erfinder haben erkannt und verstanden, dass es einen Kompromiss zwischen Sicherheit und Nutzbarkeit geben kann. Demnach kann in einigen Ausführungsformen ein System bereitgestellt werden, das es einer Entität ermöglicht, eine geeignete Anzahl von Schlüsseln auszuwählen, um ein gewünschtes Gleichgewicht zwischen Sicherheit und Nutzbarkeit zu erzielen. In Bezug auf

das in **Fig. 3** dargestellte Beispiel kann eine Schlüsselverwaltungskomponente **308** in einigen Ausführungsformen bereitgestellt werden, um mehrere kryptographische öffentliche Schlüssel nachzuverfolgen, die mit einer Entität zusammenhängen, die eine DIR steuert. Eine derartige Komponente kann eine Abstraktion gegenüber einer zugrunde liegenden Infrastruktur für öffentliche Schlüssel (Public Key Infrastructure - PKI) bereitstellen. Auf diese Weise können Benutzer und/oder Anwendungen in einer Anwendungsschicht nur mit DIR über jeweilige PDS interagieren, ohne direkt mit zugrunde liegenden kryptographischen Schlüsseln zu interagieren.

[0127] In einigen Ausführungsformen kann die Schlüsselverwaltungskomponente **308** eine rollenbasierte Zugangskontrolle durchführen. Beispielsweise kann es mindestens zwei Rollen, Bestätigender und Identitätsinhaber, geben. Die Schlüsselverwaltungskomponente **308** kann es nur einer vertrauenswürdigen Entität, die einem jeweiligen Ausweis zugewiesen ist, ermöglichen, einen Zustand einer Attributbestätigung in diesem Ausweis zu modifizieren.

[0128] Wie oben erörtert, haben die Erfinder erkannt und verstanden, dass es wünschenswert sein kann, bestimmten Attributen, wie z. B. Passinformationen, einen höheren Grad an Sicherheit aufzuerlegen. In einigen Ausführungsformen kann dies über eine oder mehrere Maßnahmen zur Authentifizierung und/oder Autorisierung erfolgen. Beispielsweise können ein oder mehrere biometrische Marker verwendet werden, um einen Zuverlässigkeitsgrad in einem Authentifizierungsprozess zu erhöhen. Zusätzlich oder alternativ dazu können ein oder mehrere biometrische Marker verwendet werden, um eine GUII zu erzeugen, was einen Benutzer daran hindern kann, mehrere DIR zu erzeugen. In einigen Ausführungsformen können derartige biometrische Marker als hochsensible Informationen behandelt werden und dürfen nicht mit einer anderen Entität ausgetauscht werden.

[0129] Zusätzlich oder alternativ dazu können eine oder mehrere Verhaltensmetriken (z. B. Standortverlauf, Laufmuster, Schlafmuster, Fahrtmuster usw.) verwendet werden, um einen Zuverlässigkeitsgrad in einem Authentifizierungsprozess zu erhöhen.

[0130] In einigen Ausführungsformen können sensible Attributwerte (z. B. Passnummer) unter Verwendung einer Autorisierung mit mehreren Schlüsseln geschützt werden. Beispielsweise kann ein Benutzer eine Autorisierung dafür verlangen, einen solchen Attributwert zu ändern, indem er bei der Authentifizierung mehrere Schlüssel angibt. In einigen Ausführungsformen kann jeder Schlüssel einer anderen Vorrichtung zugeordnet sein. Beispielsweise kann ein Benutzer einen ersten Schlüssel für einen Laptop, einen zweiten Schlüssel für ein Smartphone, einen dritten Schlüssel für eine Smartwatch usw. aufweisen. Ein veranschaulichender Prozess zum Ändern eines Attributwerts kann die folgenden Schritte umfassen:

1) Der Benutzer kann auf eine Schnittstelle eines PDS (z. B. eine Webschnittstelle) zugreifen und eine Änderungsaktion auslösen.

2) Die Änderungsaktion kann als eine ausstehende Aktion mit einer Angabe, dass eine weitere Bestätigung von dem Benutzer erforderlich sein kann, aufgezeichnet werden.

3) Der Benutzer kann die Änderungsaktion über mindestens eine zusätzliche persönliche Vorrichtung bestätigen. Beispielsweise kann die Änderungsaktion über eine Fingerabdruck-Authentifizierung mit einem registrierten Smartphone und einer registrierten biometrischen Signatur bestätigt werden.

[0131] In einigen Ausführungsformen kann ein Benutzer M Schlüssel aufweisen und können mindestens N Schlüssel (wobei N<=M) verwendet werden, um eine bestimmte Aktion (z. B. Modifizieren eines Attributwerts) durchzuführen. Auf diese Weise kann ein Sicherheitsgrad erhöht werden, sodass es schwieriger sein kann, sich für den Benutzer auszugeben. In einigen Ausführungsformen kann M gleich einer Gesamtzahl von für den Benutzer registrierten Vorrichtungen sein.

[0132] Zusätzlich oder alternativ dazu kann eine Autorisierung nur dann gewährt werden, wenn sich zwei oder mehr persönliche Vorrichtungen, wie z. B. eine Smartwatch, ein Smartphone, ein Laptop usw., innerhalb eines festgelegten Abstands (z. B. 10 Meter) voneinander befinden. Zusätzlich oder alternativ dazu kann eine Autorisierung nur dann gewährt werden, wenn sich eine persönliche Vorrichtung an einem festgelegten Standort befindet (z. B. wie auf Grundlage von GPS-Daten bestimmt). In einigen Ausführungsformen kann, wenn ein Schlüssel kompromittiert wird (z. B. wenn eine Vorrichtung gestohlen wird), der kompromittierte Schlüssel widerrufen werden und kann durch einen neuen Schlüssel ersetzt werden. Dadurch kann sich die Sicherheit verbessern, indem z. B. eine Wahrscheinlichkeit erhöht wird, dass es sich bei einer Entität, die eine Aktion anfordert, tatsächlich um den Benutzer handelt, welcher dem PDS und der DIR entspricht.

[0133] Die Erfinder haben erkannt und verstanden, dass, wenn mehrere Schlüssel verwendet werden, ein kompromittierter Authentifizierungsschlüssel widerrufen und ersetzt werden kann, während die Fähigkeit des Benutzers gewahrt wird, zwischenzeitlich auf den PDS und die DIR zuzugreifen. In einigen Ausführungsformen können ein oder mehrere Schlüssel zusammen mit einem oder mehreren Zugangsrechten über den Distributed Ledger verteilt werden, sodass der eine oder die mehreren Schlüssel und das eine oder die mehreren Zugangsrechte manipulationssicher und durch eine beliebige Entität verifizierbar werden. Wie oben erörtert, kann Datenschutz in einigen Ausführungsformen erreicht werden, indem kryptographische Einwegfunktionen verwendet werden, um Nachweise für sensible Daten abzuleiten. Es kann rechnerisch schwierig sein, die ursprünglichen sensiblen Daten aus den Nachweisen abzuleiten. Indem nur nichtsensible Nachweise in den geteilten Distributed Ledger eingeschlossen werden, kann ein hohes Niveau an Datenschutz erreicht werden. Sichere nicht vom Ledger erfasste Kommunikationskanäle zwischen Entitäten können verwendet werden, um die ursprünglichen sensiblen Informationen auszutauschen. Zusätzlich oder alternativ dazu kann ein Schema verwendet werden, um eine granulare Struktur von Attributen bereitzustellen, wodurch der Datenschutz weiter verbessert werden kann. Beispielsweise können, anstatt unnötige Informationen (z. B. Privatadresse oder tatsächliches Geburtsdatum) auszutauschen, nur Informationen, die für einen bestimmten Kontext relevant sind (z. B. Alter von über 21 Jahren zum Kauf eines alkoholischen Getränks), mit einer anderen Entität ausgetauscht werden. Um den Datenschutz weiter zu verbessern, kann eine Entität in einigen Ausführungsformen unter Verwendung verschiedener Kennungen in den verschiedenen Ausweisen identifiziert werden. Auf diese Weise kann es für einen Angreifer schwieriger sein, die Interaktionen zur Entität zurückzuverfolgen.

[0134] Die Erfinder haben erkannt und verstanden, dass es wünschenswert sein kann, einen Mechanismus bereitzustellen, um es einem Benutzer zu ermöglichen, Knoten zu finden, die einen bestimmten Distributed Ledger verwalten. Unter einigen Umständen lassen sich Knoten, die einen Distributed Ledger verwalten, über einen individuellen Ermittlungsmechanismus, eine oder mehrere HTTP-Anforderungen und/oder einen DNS-Auflösungsprozess finden. In einigen Ausführungsformen kann ein URI-Schema bereitgestellt werden, das einen Satz von Eigenschaften umfasst, die erfüllt sein müssen, damit eine Auffindbarkeit von Distributed Ledgern in einem Netz im Internetmaßstab gegeben ist. Unter einigen Umständen können Knoten einem Distributed Ledger beitreten und/oder diesen verlassen. Aus diesem Grund kann es wünschenswert sein, dass eine Liste von Knoten, die an eine anfordernde Entität zurückgegeben wird, aktuell ist.

[0135] In einigen Ausführungsformen kann mehr als ein Distributed Ledger (z. B. mehr als eine Blockchain) verwendet werden. Bei einer derartigen Architektur kann ein Ermittlungsmechanismus bereitgestellt werden, um Knoten unter den mehreren Distributed Ledgern zu finden. Im Vergleich zu einer Architektur mit einem einzigen Distributed Ledger kann der Kommunikationsaufwand bei einer Architektur mit mehreren Distributed Ledgern gering sein und kann nur eine Anforderung umfassen, die eine Distributed-Ledger-Kennung angibt. Eine Antwort kann eine Liste von Knoten umfassen, die derzeit den angeforderten Distributed Ledger verwalten. In einigen Ausführungsformen kann eine zugrunde liegende Datenstruktur eine verteilte Hashtabelle (Distributed Hash Table - DHT) sein. Jedes Mal, wenn ein Knoten beginnt, einen Distributed Ledger zu verwalten, kann er seine Aktion an das Netzwerk melden. Knoten können es zudem melden, wenn sie aufhören, einen Distributed Ledger zu verwalten.

[0136] **Fig. 9** veranschaulicht ein Beispiel für einen Distributed-Ledger-Ermittlungsmechanismus in einem Netzwerk **900** gemäß einigen Ausführungsformen. Bei Schritt **1** kann ein Knoten **2** Zugang zu einer Blockchain **X** von einem Knoten **1** anfordern. In Reaktion darauf kann der Knoten **1** in Schritt **2** einem Knoten **2** eine Genehmigung gewähren. In Schritt **3** kann der Knoten **2** der Blockchain **X** melden, dass er nun die Blockchain **X** verwaltet. In Schritt **3** kann zudem ein Knoten **3** Zugang zu der Blockchain **X** gegenüber dem Knoten **1** anfordern. In Reaktion darauf kann der Knoten **1** bei Schritt **4** dem Knoten **3** eine Genehmigung erteilen. In Schritt **5** kann der Knoten **3** der Blockchain **X** melden, dass er nun die Blockchain **X** verwaltet. In Schritt **6** kann der Knoten **2** entscheiden, die Blockchain **X** zu verlassen, und kann seinen Austritt an die Blockchain **X** melden. In Schritt **7** kann ein Knoten **4** danach suchen, welche Knoten die Blockchain **X** verwalten. Die Blockchain kann eine aktualisierte Liste von verwaltenden Knoten in Schritt **8** zurückgeben.

[0137] Eine oder mehrere beliebige der hier beschriebenen Techniken können in verschiedenen Situationen verwendet werden, um die Verifizierung von personenbezogenen Daten zu vereinfachen. Beispielsweise kann in einigen Ausführungsformen ein individuelles Ausweisschema für jeden Anwendungsfall bereitgestellt werden, das sämtliche Attribute beinhaltet, die für diesen Anwendungsfall relevant sind. Auf diese Weise kann ein auf Grundlage des Schemas erzeugter Ausweis sämtliche relevanten Daten beinhalten und kann ein PDS, der den Ausweis verwaltet, die Daten aktuell halten.

[0138] Nichteinschränkende Beispiele für Anwendungsfälle sind nachfolgend beschrieben.

Kenne deinen Kunden (KYC)

[0139] Eine dieser Anwendungen sind Kenne-deinen-Kunden(KYC)-Prüfungen, die von Finanzinstituten, wie z. B. Banken, durchgeführt werden können. Die Identität eines Benutzers (z. B. eines Kunden einer Bank) kann durch einen Prozess validiert werden, bei dem eine vertrauenswürdige Entität (z. B. die Bank) einen oder mehrere von dem Benutzer übermittelte Attributwerte verifiziert. Dieser Prozess kann unter Verwendung einer oder mehrerer der hier beschriebenen Techniken durchgeführt werden. Sobald der eine oder die mehreren Attributwerte verifiziert wurden, kann die vertrauenswürdige Entität eine oder mehrere entsprechende Attributbestätigungen signieren und kann sich anschließend eine andere vertrauenswürdige Entität auf eine derartige Bestätigung stützen, solange die erstgenannte vertrauenswürdige Entität und die letztgenannte vertrauenswürdige Entität Teil einer Vertrauensstruktur sind.

[0140] Es kann sein, dass Finanzinstitute strenge Regeln und Vorschriften befolgen müssen, um zu verifizieren, wer ihre Kunden sind. Einerseits kann es sein, dass Finanzinstitute Aufzeichnungen zu ihren Kunden führen. Andererseits kann es sein, dass Finanzinstitute solche Daten geheim und sicher aufbewahren müssen. Indem es Benutzern (z. B. Bankkunden) ermöglicht wird, ihre eigenen Daten zu steuern, und indem den Benutzern eine Plattform bereitgestellt wird, um ihre Daten zu verwalten und auszutauschen, können die resultierenden KYC-Prüfungen wesentlich effizienter sein und Datendopplungen begrenzt werden. Aus Sicht eines Benutzers können Daten zu dem Zeitpunkt eingegeben werden, zu dem ein PDS erzeugt wird, und anschließend nur dann, wenn ein Attribut geändert wird. Auf diese Weise kann die Belastung entfallen, die gleichen Informationen mehrmals eingeben zu müssen. Aus Sicht eines Finanzinstituts kann die Richtigkeit von Daten wesentlich erhöht werden, da z. B. Aktualisierungen automatisch auf alle relevanten vertrauenswürdigen Entitäten verteilt werden.

Arbeitnehmerbestätigung

[0141] Im Vergleich zu KYC-Prüfungen ist eine Bestätigung von Arbeitnehmern weniger reguliert. Nichtsdestotrotz können Arbeitnehmer eine oder mehrere beliebige der hier beschriebenen Techniken verwenden, um die Identität und/oder andere Informationen ihrer Arbeitnehmer zu bestätigen. Derartige Bestätigungen können intern zu Authentifizierungs- und/oder Autorisierungszwecken und/oder extern zum sicheren Austausch von Informationen mit Partnern und/oder anderen Beteiligten verwendet werden. Auf diese Weise kann Gewissheit in Bezug auf eine vorgebliche Identität garantiert werden. In einigen Ausführungsformen kann ein Prozess zum Gewähren einer Autorisierung an Arbeitnehmer, um bestimmte Aufgaben für den Arbeitgeber durchzuführen, signifikant vereinfacht werden. Da Attribute auf alle vertrauenswürdigen Beteiligten verteilt werden können, ist ein gewünschter Autorisierungsgrad stets aktuell.

Sicherheitskontrollen

[0142] Eine oder mehrere beliebige der hier beschriebenen Techniken können verwendet werden, um eine Beschleunigung von Sicherheitskontrollen (z. B. Sicherheitskontrollen, die an Flughäfen durchgeführt werden, Sicherheitskontrollen zum Gewähren von Zugang zu eingeschränkten Bereichen oder Gebäuden usw.) zu ermöglichen. Beispielsweise kann, anstatt Identitätsunterlagen (Ausweise) oder andere identifizierende Informationen manuell zu prüfen, eine Sicherheitskontrolle automatisiert werden.

[0143] In einigen Ausführungsformen kann eine automatisierte Sicherheitskontrolle einen Abruf eines aktuellen Führungszeugnisses (z. B. innerhalb der letzten sechs Monate aktualisiert) in Echtzeit beinhalten, das durch eine entsprechende vertrauenswürdige Entität bestätigt wurde.

Transportsicherheitsbehörde (TSA)

[0144] In einem Beispiel kann ein Reisender einen PDS und eine zugehörige DIR, die einen Satz von Attributbestätigungen beinhaltet, aufweisen. Die DIR kann ein Schema beinhalten, das für TSA-Prüfungen geeignet ist. Auf diese Weise können Sicherheitskontrollen an Flughäfen von einem TSA-Beamten durchgeführt werden, indem er eine Gegenparteiüberprüfung durchführt. Ein Beispiel für eine solche Gegenparteiüberprüfung kann die folgenden Schritte umfassen:

1) ein Reisender kann sich einem TSA-Sicherheitskontrollbereich auf dem Flughafen nähern;

2) die Mobilvorrichtung des Reisenden kann Attributwerte mit einem TSA-System austauschen;

3) das TSA-System kann den Empfang der ausgetauschten Attributwerte bestätigen;

4) ein TSA-Beamter öffnet die ausgetauschten Attributwerte und vergleicht die Werte visuell mit dem Reisenden. Zusätzlich oder alternativ dazu kann der Reisende einen Fingerabdruck und/oder andere biometrische Merkmale scannen. Derartige Merkmale können mit entsprechenden Merkmalen verglichen werden, die in den ausgetauschten Attributwerten enthalten sind.

5) das TSA-System kann: prüfen, ob die empfangenen Attributwerte legitim sind, indem die Werte gegen den Distributed Ledger geprüft werden, während sichergestellt wird, dass der signierenden vertrauenswürdigen Entität von der TSA vertraut wird; einen oder mehrere Attributwert mit externen Listen (z. B. No-Fly- oder Terrorlisten) gegenprüfen; und/oder eine Gesichtserkennung durchführen oder einen empfangenen Lichtbildausweis gegen einen Videostream in Echtzeit gegenprüfen.

[0145] Wenn er sämtliche der oben genannten Prüfungen bestanden hat, kann der Reisende als vertrauenswürdig markiert werden. Demnach muss die TSA keine großen Datenbanken mehr führen. Darüber hinaus kann dieser Ansatz die physische Passkontrolle und sämtliche Hintergrundprüfungen in einem einzigen Schritt kombinieren. Auf diese Weise können Hintergrundprüfungen leicht bei jeder Begegnung durchgeführt werden.

Check-ins

[0146] Check-ins erfordern häufig, dass ein Kunde in einer Schlange wartet. Dieses Warten lässt sich unter Verwendung einer oder mehrerer beliebiger der hier beschriebenen Techniken signifikant verkürzen. Beispielsweise kann ein Kunde einen PDS und eine zugehörige DIR aufweisen und können seine Identität und/oder andere relevante Daten durch eine bestätigende Einrichtung (z. B. Hotel, Autovermietung usw.) durch Prüfen von Attributverweisen bestätigt werden. Während einer Buchungsphase kann ein Kunde einen PDS verwenden, um relevante Informationen mit der Einrichtung auszutauschen. Anstatt personenbezogene Informationen manuell einzutragen, kann das System der Einrichtung den Kunden darüber benachrichtigen, welche Attributwerte erforderlich sind. Während einer Check-in-Phase kann der Kunde direkt die Kontrolle über ein Hotelzimmer, ein Fahrzeug usw. übernehmen, ohne sich an einen Bearbeiter wenden zu müssen oder personenbezogene Informationen bereitstellen zu müssen. In einigen Ausführungsformen kann der Kunde das Hotelzimmer oder Fahrzeug aufschließen, indem er nachweist, dass er Zugang zu der digitalen Identitätsdarstellung hat, die während der Buchungsphase verwendet wurde. Beispielsweise kann der Kunde eine Mobilvorrichtung verwenden, die dazu imstande ist, den PDS zu steuern.

Einrichtungen mit Altersbeschränkung

[0147] Bestimmte Einrichtungen, wie z. B. Bars, können es erfordern, dass ihre Kunden Nachweise dafür liefern, dass sie älter als ein bestimmtes Alter sind. Um einen Altersnachweis bereitzustellen, kann ein Kunde einen Ausweis erzeugen, um relevante Informationen mit einer Einrichtung auszutauschen. Der Ausweis kann unter Verwendung eines bestimmten Schemas gebildet werden, das nur das Alter des Kunden oder das Alter und den Namen des Kunden umfassen kann. Das Austauschen von Informationen kann unter Verwendung einer Mobilvorrichtung durchgeführt werden. Wenn das Alter von einer anderen vertrauenswürdigen Partei bestätigt wurde, kann die Einrichtung daraus schließen, dass die vom Kunden bereitgestellten Altersinformationen tatsächlich wahr sind.

[0148] In einigen Ausführungsformen werden vorteilhafte technische Wirkungen über dezentralisierte und schützende Speicherorte bereitgestellt, wodurch sensible und (höchst) anfällige Benutzerinformationen auf geschützte Weise durch Anwenden einer kryptographischen Einwegfunktion gespeichert werden können. Weiterhin lässt sich eine Redundanz von Verifizierungsverfahren zum Bestimmen der Richtigkeit von (Benutzer-) Informationen leicht durch Austauschen von Zustandsinformationen (z. B. ob ein Attributwert verifiziert ist) zu einer jeweiligen Anforderung zwischen unabhängigen Entitäten, die einander vertrauen, verringern. Es können nicht nur Zeit, sondern auch andere Ressourcen dadurch eingespart werden, z. B. durch Vermeiden von unnötigen Arbeitsabläufen (womit sich der Netzwerkverkehr verringert), Dopplungen von personenbezogenen Datensätzen (und damit Computerspeicher) und äußerst teuren Infrastrukturen zum Bereitstellen zentralisierter Speicher- und Verwaltungssysteme, wie z. B. einer zentralen Clearingstelle, um vergleichbare Datenbanken stets unter allen erdenklichen Umständen verfügbar zu halten. Somit kann eine erhöhte Effizienz der Datenverwaltung zudem z. B. eine Verringerung der Infrastruktur und nötigen Rechenleistung und/oder eine Verringerung der Reaktionszweit zur Folge haben.

[0149] In einigen Ausführungsformen können durch Austauchen von (Benutzer-) Informationen auf geschützte Weise, z. B. unter Verwendung vorteilhafter Hash-Algorithmen, sogar sensible (Benutzer-) Informationen an einer zugänglichen Stelle ohne gefährdenden Diebstahl, unzulässige oder betrügerische Manipulation und

dergleichen durch fremde, nicht vertrauenswürdige Entitäten innerhalb einer Netzwerkumgebung aus mehreren verschiedenen Entitäten, die einander vertrauen können, gehalten werden.

[0150] Einige veranschaulichende Aspekte der vorliegenden Offenbarung sind nachfolgend beschrieben. Dabei kann eine personenbezogene Identitätsdarstellung von mindestens einer der mehreren Entitäten als die digitale Identitätsdarstellung (DIR) betrachtet werden und kann eine Benutzerdatenstruktur von mindestens einer der mehreren Entitäten als der Dienst für personenbezogene Daten (PDS) betrachtet werden.

1. Computerimplementiertes Verfahren, umfassend die Schritte:

Verwenden mehrerer Messungen, die an einem Benutzer durchgeführt werden, um eine Kennung für den Benutzer zu erzeugen, wobei die Kennung einen kryptographischen Nachweis für die mehreren Messungen umfasst;

Instanziieren einer digitalen Identitätsdarstellung, die der Kennung für den Benutzer zugeordnet ist, wobei die digitale Identitätsdarstellung Programmcode umfasst, der Regeln zur Bestätigung umsetzt;

Erzeugen einer elektronischen Signatur über die digitale Identitätsdarstellung; und

Veröffentlichen der digitalen Identitätsdarstellung und der elektronischen Signatur in einem Distributed-Ledger-System.

2. Computerimplementiertes Verfahren nach Aspekt 1, wobei die mehreren Messungen mindestens eine biometrische Messung und mindestens eine Verhaltensmessung umfassen.

3. Computerimplementiertes Verfahren nach Anspruch 1, ferner umfassend einen Schritt zum:

Empfangen einer Bestätigung von dem Distributed-Ledger-System, dass ein Datensatz der digitalen Identitätsdarstellung erzeugt wurde.

4. Computerimplementiertes Verfahren nach Aspekt 3, wobei das Distributed-Ledger-System unter Verwendung von mindestens einer Blockchain umgesetzt wird.

5. Computerimplementiertes Verfahren nach Aspekt 1, ferner umfassend Schritte zum:

Senden, über das Distributed-Ledger-System, einer Anforderung an eine vertrauenswürdige Entität, einen Ausweis zu verifizieren, wobei der Ausweis mehrere kryptographische Nachweise umfasst, die jeweils mehreren Attributen entsprechen, wobei jeder kryptographische Nachweis auf Grundlage eines Werts des Attributs, das dem kryptographischen Nachweis entspricht, erzeugt wird; und

Senden, über einen Kanal außerhalb des Distributed-Ledger-Systems, an die vertrauenswürdige Entität, der mehreren Werte der mehreren Attribute.

6. Computerimplementiertes Verfahren nach Aspekt 1, ferner umfassend Schritte zum:

Empfangen eines Pointers zu einem Ausweis;

Verwenden des Pointers, um auf den Ausweis aus dem Distributed-Ledger-System zuzugreifen, wobei der Ausweis mehrere Attributbestätigungen umfasst, die jeweils den mehreren Attributen entsprechen, wobei bei jedem Attribut die entsprechende Attributbestätigung einen kryptographischen Nachweis umfasst;

Empfangen, über einen Kanal außerhalb des Distributed-Ledger-Systems, mehrerer Werte, die jeweils den mehreren Attributen entsprechen;

Identifizieren, anhand des Ausweises, einer Entität, die dafür zuständig ist, den Ausweis zu verifizieren;

Bestimmen, ob der Entität, die dafür zuständig ist, den Ausweis zu verifizieren, zu vertrauen ist; und

in Reaktion darauf, dass bestimmt wird, dass die Entität, die dafür zuständig ist, den Ausweis zu verifizieren, zu vertrauen ist, Prüfen für jede Attributbestätigung der mehreren Attributbestätigungen, ob:

sich die Attributbestätigung in einem VERIFIED-Zustand befindet;

der kryptographische Nachweis in der Attributbestätigung ein gültiger Nachweis für den empfangenen Wert ist, der dem Attribut entspricht; und

die Attributbestätigung durch die Entität, die dafür zuständig ist, den Ausweis zu verifizieren, elektronisch signiert ist.

7. Computerimplementiertes Verfahren, umfassend Schritte zum:

Auswählen eines Schemas aus mehreren Schemata für Ausweise, wobei das Schema mehrere Attribute umfasst;

Erzeugen, gemäß dem Schema, eines Ausweises zur Verwendung beim Bestätigen einer Identität eines Benutzers, wobei der Schritt des Erzeugens Folgendes umfasst:

Identifizieren mehrerer Werte, wobei jeder Wert einem Attribut der mehreren Attribute in dem Schema entspricht;

Erzeugen von mindestens einem kryptographischen Nachweis für jeden Wert der mehreren Werte; und

Identifizieren einer vertrauenswürdigen Entität zum Verifizieren der mehreren Werte; und Veröffentlichen des Ausweises in einem Distributed-Ledger-System.

8. Computerimplementiertes Verfahren nach Aspekt 7, wobei das Distributed-Ledger-System eine digitale Identitätsdarstellung umfasst, der eine Kennung für den Benutzer zugeordnet ist, wobei die digitale Identitätsdarstellung Programmcode umfasst, der Regeln zur Bestätigung umsetzt.

9. Computerimplementiertes Verfahren nach Aspekt 8, wobei:

für jedes Attribut der mehreren Attribute der Ausweis eine Attributbestätigung für dieses Attribut umfasst, wobei die Attributbestätigung mindestens einen kryptographischen Nachweis für einen entsprechenden Attributwert umfasst; und

der Programmcode bei Ausführung durch mindestens einen Prozessor Zustandsinformationen für die Attributbestätigung jedes Attributs der mehreren Attribute verwaltet.

10. Computerimplementiertes Verfahren nach Aspekt 9, wobei sich mindestens eine Attributbestätigung in einem Zustand befindet, der ausgewählt ist aus einer Gruppe, bestehend aus: PENDING, VERIFIED, EXPIRED und INVALID.

11. Computerimplementiertes Verfahren nach Aspekt 10, wobei der Programmcode bei Ausführung durch den mindestens einen Prozessor veranlasst, dass die mindestens eine Attributbestätigung von einem PENDING-Zustand in einen VERIFIED-Zustand nur in Reaktion auf eine Benachrichtigung von der vertrauenswürdigen Entität, dass ein entsprechender Attributwert durch die vertrauenswürdige Entität verifiziert wurde, übergeht.

12. Computerimplementiertes Verfahren nach Aspekt 10, wobei der Programmcode bei Ausführung durch den mindestens einen Prozessor veranlasst, dass die mindestens eine Attributbestätigung von einem VERIFIED-Zustand in einen EXPIRED-Zustand nach Ablauf eines Zeitgebers, der gestellt wurde, als ein entsprechender Attributwert zuletzt verifiziert wurde, übergeht.

13. Computerimplementiertes Verfahren nach Aspekt 10, wobei der Programmcode bei Ausführung durch den mindestens einen Prozessor einen Zugang zu einem kryptographischen Nachweis für einen entsprechenden Attributwert nur dann ermöglicht, wenn sich die mindestens eine Attributbestätigung in einem VERIFIED-Zustand befindet.

14. Computerimplementiertes Verfahren, umfassend:

Empfangen, über ein Distributed-Ledger-System, einer Anforderung zum Verifizieren eines Ausweises, wobei der Ausweis mehrere Attributbestätigungen umfasst, die jeweils mehreren Attributen für einen Benutzer entsprechen, wobei für jedes Attribut die entsprechende Attributbestätigung einen kryptographischen Nachweis umfasst;

Empfangen, über einen Kanal außerhalb des Distributed-Ledger-Systems, mehrerer Werte, die jeweils den mehreren Attributen entsprechen;

für mindestens ein Attribut der mehreren Attribute:

Verifizieren, ob der Wert, der dem mindestens einen Attribut entspricht, ein korrekter Wert des mindestens einen Attributs für den Benutzer ist;

in Reaktion darauf, dass verifiziert wird, dass der Wert, der dem mindestens einen Attribut entspricht, ein korrekter Wert des mindestens einen Attributs für den Benutzer ist, Veranlassen, über das Distributed-Ledger-System, dass sich die Attributbestätigung, die dem mindestens einen Attribut entspricht, in einem VERIFIED-Zustand befindet.

15. Computerimplementiertes Verfahren, umfassend:

Empfangen, über ein Distributed-Ledger-System, einer Anforderung zum Verifizieren eines ersten Ausweises, wobei der erste Ausweis mehrere Attributbestätigungen umfasst, die jeweils mehreren Attributen für einen Benutzer entsprechen, wobei bei jedem Attribut die entsprechende Attributbestätigung einen kryptographischen Nachweis umfasst;

Empfangen, über einen Kanal außerhalb des Distributed-Ledger-Systems, mehrerer Werte, die jeweils den mehreren Attributen entsprechen;

für mindestens ein Attribut der mehreren Attribute:

Identifizieren, anhand des ersten Ausweises, einer ersten Attributbestätigung, die dem mindestens einen Attribut entspricht, wobei die erste Attributbestätigung einen ersten kryptographischen Nachweis umfasst;

Identifizieren, anhand der ersten Attributbestätigung, eines Pointers zu einem zweiten Ausweis;

Verwenden des Pointers, um auf den zweiten Ausweis aus dem Distributed Ledger zuzugreifen;

Identifizieren, anhand des zweiten Ausweises, einer Entität, die dafür zuständig ist, den zweiten Ausweis zu verifizieren, und einer zweiten Attributbestätigung, die dem mindestens einen Attribut entspricht;

Bestimmen, ob der Entität, die dafür zuständig ist, den zweiten Ausweis zu verifizieren, zu vertrauen ist; und

in Reaktion darauf, dass bestimmt wird, dass der Entität, die dafür zuständig ist, den zweiten Ausweis zu verifizieren, zu vertrauen ist, Prüfen, ob:

(1) sich die zweite Attributbestätigung in einem VERIFIED-Zustand befindet;

(2) der zweite kryptographische Nachweis ein gültiger Nachweis für den empfangenen Wert ist, der dem mindestens einen Attribut entspricht; und

(3) die zweite Attributbestätigung durch die Entität, die dafür zuständig ist, den zweiten Ausweis zu verifizieren, elektronisch signiert ist.

16. Verfahren nach Aspekt 15, ferner umfassend einen Schritt zum Prüfen, ob:

(4) der erste kryptographische Nachweis ein gültiger Nachweis für den empfangenen Wert ist, der dem mindestens einen Attribut entspricht.

17. Verfahren nach Aspekt 16, ferner umfassend Schritte zum, in Reaktion darauf, dass geprüft wird, ob (1)-(4) erfüllt sind:

elektronischen Signieren der ersten Attributbestätigung; und

Veranlassen, dass die erste Attributbestätigung in einen VERIFIED-Zustand übergeht.

18. System, umfassend:

mehrere Entitäten, die ein Netzwerk bilden, wobei mindestens eine erste Entität der mehreren Entitäten Folgendes umfasst:

○ mindestens ein Speichermedium, auf dem Folgendes gespeichert ist:

■ eine lokale Kopie einer verteilten Datenstruktur, die unter den mehreren Entitäten repliziert ist;

■ mindestens eine Benutzerdatenstruktur, die Benutzerdaten speichert, wobei die Benutzerdatenstruktur mindestens Folgendes umfasst:

• einen Datenwert; und

• eine Kennung, die der den Datenwert schreibenden Entität entspricht;

○ mindestens zwei Kommunikationsschnittstellen zum Kommunizieren mit mindestens einer zweiten Entität, umfassend eine erste Kommunikationsschnittstelle, um innerhalb einer Datenschutzschicht zu kommunizieren, und eine zweite Kommunikationsschnittstelle, um innerhalb einer Vertrauensschicht zu kommunizieren;

○ mindestens einen Prozessor, der ausgelegt ist zum:

■ Senden und/oder Empfangen mindestens eines Teils der verteilten Datenstruktur von/an die mindestens eine zweite Entität;

■ Verifizieren von mindestens dem Datenwert der ersten Entität und;

■ auf Grundlage des Ergebnisses der Verifizierung Ändern eines Status, der dem Datenwert in der verteilten Datenstruktur entspricht.

19. System nach Aspekt 18, wobei die verteilte Datenstruktur, insbesondere ein Distributed Ledger, eine Blockchain ist.

20. System nach Aspekt 18 oder 19, wobei die verteilte Datenstruktur einen Nachweiswert umfasst, der dem Datenwert entspricht, wobei der Nachweiswert durch eine kryptographische Einwegfunktion, insbesondere eine Hash-Funktion, erzeugt wird, die auf mindestens den Datenwert angewandt wird.

21. System nach einem der Aspekte 18 bis 20, wobei die lokale Kopie der verteilten Datenstruktur der mindestens ersten Entität eine personenbezogene Identitätsdarstellung, in der Daten gespeichert sind, die durch eine kryptographische Einwegfunktion, insbesondere eine Hash-Funktion, erzeugt werden, die auf mindestens einen Teil der Benutzerdaten der mindestens ersten der mehreren Entitäten angewandt wird, und/oder eine Kennung, die der mindestens ersten der mehreren Entitäten zugeordnet ist, umfasst.

22. System nach einem der Aspekte 18 bis 21, wobei das System ferner mindestens eine dritte Entität in dem Netzwerk umfasst, wobei die dritte Entität Folgendes umfasst:

o mindestens ein Speichermedium, auf dem eine lokale Kopie der verteilten Datenstruktur gespeichert ist;

o mindestens eine Kommunikationsschnittstelle zum Kommunizieren mit den mehreren Entitäten in dem Netzwerk;

o einen Prozessor, der ausgelegt ist zum:

■ Empfangen von Daten von der zweiten Entität, wobei die Daten mindestens eine Kennung, die der zweiten Entität zugeordnet ist, und einen empfangenen Datenwert umfassen;

■ Erzeugen eines Validierungswerts des empfangenen Datenwerts durch Anwenden einer kryptographischen Einwegfunktion auf den empfangenen Datenwert;

■ Identifizieren von (den) Nachweisdaten, die in der lokalen Kopie der verteilten Datenstruktur gespeichert sind, unter Verwendung der Kennung der zweiten Entität;

■ Bestimmen, ob sich die identifizierten Nachweisdaten in einem verifizierten Zustand befinden;

■ Vergleichen des Validierungswerts mit den identifizierten Nachweisdaten, um zu bestimmen, ob die empfangenen Daten von der zweiten Entität verifiziert wurden.

23. Verfahren, das insbesondere durch ein System nach einem der Aspekte 18 bis 22 ausführbar ist, umfassend die folgenden Schritte:

○ Instanziieren von mindestens einer Benutzerdatenstruktur für mindestens eine/die zweite Entität einer/der mehreren Entitäten, die ein/das Netzwerk bildet;

○ Modifizieren einer bestehenden und/oder Erzeugen einer personenbezogenen Identitätsdarstellung in einer/der verteilten Datenstruktur, insbesondere unter Verwendung einer kryptographischen Einwegfunktion, durch die zweite Entität;

○ Verteilen der personenbezogenen Identitätsdarstellung auf mindestens eine Untergruppe der mehreren Entitäten;

○ Signieren der mindestens einen verteilten personenbezogenen Identitätsdarstellung durch eine/die mindestens erste Entität, wobei eine Kennung, die der ersten Entität zugeordnet ist, der zweiten Entität als vertrauenswürdig bekannt ist.

24. Verfahren nach Aspekt 23, wobei eine Vertrauenswürdigkeit der ersten Entität für die zweite Entität durch Kommunikation zwischen der ersten Entität und der zweiten Entität über eine der mindestens zwei Kommunikationsschnittstellen festgelegt und/oder freigegeben ist, sodass der zweiten Entität die erste Entität als vertrauenswürdig bekannt ist und/oder die zweite Entität die erste Entität als vertrauenswürdig annimmt.

25. Verfahren nach Aspekt 23 oder 24, wobei mindestens eine personenbezogene Identitätsdarstellung durch Anwenden einer kryptographischen Einwegfunktion auf mindestens einen Teil der Benutzerdatenstruktur von mindestens einer der mehreren Entitäten bereitgestellt wird.

26. Verfahren nach einem der Aspekte 23 bis 25, wobei die bestehende personenbezogene Identitätsdarstellung erneut auf die mehreren Entitäten verteilt wird, wenn eine Veränderung ihres Datenwerts oder eines Zustands der personenbezogenen Identitätsdarstellung eintritt.

27. Verfahren nach einem der Aspekte 23 bis 26, wobei der Zustand der mindestens einen personenbezogenen Identitätsdarstellung einer der folgenden ist: „PENDING“, „VERIFIED“, „EXPIRED“, „INVALID“.

28. Verfahren nach einem der Aspekte 23 bis 27, wobei der Zustand der modifizierten oder erzeugten personenbezogenen Identitätsdarstellung vor der Verifizierung „PENDING“ ist und der Zustand auf „VERIFIED“ nach einer erfolgreichen Verifizierung durch die vertrauenswürdige erste Entität geändert wird.

29. Verfahren nach einem der Aspekte 23 bis 28, wobei die verteilte Datenstruktur, insbesondere ein Distributed Ledger, als eine Blockchain konfiguriert ist.

30. Verfahren, das insbesondere durch ein System nach einem der Aspekte 18 bis 22 ausführbar ist, umfassend die folgenden Schritte:

o Empfangen, durch eine erste Entität, mindestens einer Kopie einer verteilten Datenstruktur, die mindestens eine personenbezogene Identitätsdarstellung umfasst, in der Daten gespeichert sind, die durch eine kryptographische Einwegfunktion erzeugt werden, und der eine Kennung einer zweiten Entität zugeordnet ist und ein Zustand zugeordnet ist;

o Bestimmen, durch die zweite Entität, ob eine Kennung der ersten Entität in einer Liste von vertrauenswürdigen Entitäten gespeichert ist;

o Senden einer Anforderung, durch die zweite Entität, an die erste Entität zum Verifizieren von Daten, insbesondere eines Nachweiswerts, die in der verteilten Datenstruktur gespeichert sind;

o Verifizieren, durch die erste Entität, eines Datenwerts, der von der zweiten Entität über einen anderen Kanal als die verteilte Datenstruktur empfangen wird;

o Bestimmen, durch die erste Entität, ob der Nachweiswert aus dem Datenwert unter Verwendung der kryptographischen Einwegfunktion erzeugt wird; und

o wenn der Datenwert verifiziert wird und bestimmt wird, dass der Nachweiswert aus dem Datenwert unter Verwendung der kryptographischen Einwegfunktion erzeugt wird, Signieren des Nachweiswerts durch die erste Entität.

31. Verfahren nach Aspekt 30, wobei der Zustand, der den Daten zugeordnet ist, die der zweiten Entität zugeordnet sind, von „EXPIRED“ zu „VERIFIED“ durch die erste Einheit geändert wird, wenn der Datenwert verifiziert wird und bestimmt wird, dass der Nachweiswert aus dem Datenwert unter Verwendung der kryptographischen Einwegfunktion erzeugt wird.

32. Computerlesbares Medium, auf dem Anweisungen gespeichert sind, wobei die Anweisungen eine oder mehrere Anweisungen umfassen, die bei Ausführung durch einen oder mehrere Prozessoren den einen oder die mehreren Prozessoren dazu veranlassen, das Verfahren nach einem der Aspekte 23 bis 31 umzusetzen.

[0151] Fig. 10 stellt einen veranschaulichenden Computer **10000** schematisch dar, auf dem ein beliebiger Aspekt der vorliegenden Offenbarung umgesetzt werden kann. In der in **Fig. 10** dargestellten Ausführungsform beinhaltet der Computer **10000** eine Verarbeitungseinheit **10001** mit einem oder mehreren Prozessoren und einem dauerhaften computerlesbaren Speichermedium **10002**, das z. B. flüchtigen und/oder nichtflüchtigen Speicher beinhalten kann. Der Speicher **10002** kann eine oder mehrere Anweisungen speichern, um die Verarbeitungseinheit **10001** so zu programmieren, dass sie eine beliebige der hier beschriebenen Funktionen durchführt. Der Computer **10000** kann zudem andere Arten eines dauerhaften computerlesbaren Mediums beinhalten, wie z. B. einen Speicher **10005** (z. B. ein oder mehrere Plattenlaufwerke) neben dem Systemspeicher **10002**. Der Speicher **10005** kann zudem ein oder mehrere Anwendungsprogramme und/oder externe Komponenten, die von Anwendungsprogrammen (z. B. Softwarebibliotheken) verwendet werden, speichern, die in den Speicher **10002** geladen werden können.

[0152] Der Computer **10000** kann eine oder mehrere Eingabevorrichtungen und/oder Ausgabevorrichtungen, wie z. B. die in **Fig. 10** veranschaulichten Vorrichtungen **10006** und **10007**, aufweisen. Diese Vorrichtungen können u. a. verwendet werden, um eine Benutzerschnittstelle darzustellen. Zu Beispielen für Ausgabevorrich-

tungen, die verwendet werden können, um eine Benutzerschnittstelle bereitzustellen, gehören Drucker oder Anzeigebildschirme zur visuellen Darstellung von Ausgaben und Lautsprecher oder andere klangerzeugende Vorrichtungen zur hörbaren Darstellung von Ausgaben. Zu Beispielen für Eingabevorrichtungen, die für eine Benutzerschnittstelle verwendet werden können, gehören Tastaturen und Zeigevorrichtungen, wie z. B. Mäuse, Berührungsfelder und Grafiktabletts. Als ein anderes Beispiel können die Eingabevorrichtungen **10007** ein Mikrophon zum Aufnehmen von Audiosignalen beinhalten und können die Ausgabevorrichtungen **10006** einen Anzeigebildschirm zum visuellen Wiedergeben und/oder Lautsprecher zum hörbaren Wiedergeben von erkanntem Text beinhalten.

[0153] Wie in **Fig. 10** dargestellt, kann der Computer **10000** zudem eine oder mehrere Netzwerkschnittstellen (z. B die Netzwerkschnittstelle **10010**) umfassen, um Kommunikation über verschiedene Netzwerke (z. B. das Netzwerk **10020**) zu ermöglichen. Zu Beispielen für Netzwerke gehören ein lokales Netzwerk oder ein Weitverkehrsnetz, wie z. B. ein Unternehmensnetzwerk oder das Internet. Derartige Netzwerke können auf einer beliebigen geeigneten Technik beruhen und können gemäß einem beliebigen geeigneten Protokoll betrieben werden und können drahtlose Netzwerke, drahtgebundene Netzwerke oder Glasfasernetze einschließen.

[0154] Nachdem somit mehrere Aspekte von mindestens einer Ausführungsform beschrieben wurden, versteht es sich, dass verschiedene Änderungen, Modifikationen und Verbesserungen für den Fachmann ohne Weiteres auf der Hand liegen. Diese Änderungen, Modifikationen und Verbesserungen sollen im Wesen und Umfang der vorliegenden Offenbarung liegen. Demnach sind die vorstehende Beschreibung und die Zeichnungen lediglich beispielhaft.

[0155] Die oben beschriebenen Ausführungsformen der vorliegenden Offenbarung können auf einen beliebigen von zahlreichen Wegen umgesetzt werden. Beispielsweise können die Ausführungsformen unter Verwendung von Hardware, Software oder einer Kombination davon umgesetzt werden. Bei einer Umsetzung als Software kann der Softwarecode auf einem beliebigen geeigneten Prozessor oder einer Sammlung von Prozessoren unabhängig davon ausgeführt werden, ob sie auf einem einzigen Computer bereitgestellt oder unter vielen Computern verteilt ist.

[0156] Zudem können die verschiedenen hier umrissenen Verfahren oder Prozesse als Software codiert werden, die auf einem oder mehreren Prozessoren ausführbar ist, die ein beliebiges aus einer Vielfalt an Betriebssystemen oder Plattformen einsetzen. Überdies kann solche Software unter Verwendung eines beliebigen aus einer Reihe geeigneter Programmiersprachen und/oder Programmier- oder Skriptwerkzeuge geschrieben sein und kann auch als ausführbarer Code in Maschinensprache oder Zwischencode kompiliert werden, der auf einem Framework oder einer virtuellen Maschine ausgeführt wird.

[0157] In dieser Hinsicht können die hier offenbarten Konzepte als ein dauerhaftes computerlesbares Medium (oder mehrere computerlesbare Medien) (z. B. ein Computerspeicher, eine oder mehrere Disketten, Compact Disks, optische Platten, Magnetbänder, Flash-Speicher, Schaltungskonfigurationen in feldprogrammierbaren Gate-Arrays oder andere Halbleitervorrichtungen oder ein anderes dauerhaftes, greifbares Computerspeichermedium) umgesetzt sein, auf dem ein oder mehrere Programme codiert sind, die bei Ausführung auf einem oder mehreren Computern oder anderen Prozessoren Verfahren durchführen, welche die verschiedenen oben erörterten Ausführungsformen der vorliegenden Offenbarung umsetzen. Das computerlesbare Medium oder die computerlesbaren Medien können transportierbar sein, sodass das Programm oder die Programme, die darauf gespeichert sind, auf einen oder mehrere verschiedene Computer oder andere Prozessoren geladen werden können, um verschiedene Aspekte der vorliegenden Offenbarung, wie oben erörtert, umzusetzen.

[0158] Die Ausdrücke „Programm“ oder „Software“ beziehen sich im vorliegenden Zusammenhang auf eine beliebige Art von Computercode oder Satz aus computerausführbaren Anweisungen, der eingesetzt werden kann, um einen Computer oder anderen Prozessor so zu programmieren, dass er verschiedene Aspekte der vorliegenden Offenbarung, wie oben offenbart, umsetzt. Überdies versteht es sich, dass gemäß einem Aspekt dieser Ausführungsform ein oder mehrere Computerprogramme, die bei Ausführung Verfahren der vorliegenden Offenbarung durchführen, sich nicht auf einem einzelnen Computer oder Prozessor befinden müssen, sondern auf modulare Weise auf eine Reihe von verschiedenen Computern oder Prozessoren verteilt sein können, um verschiedene Aspekte der vorliegenden Offenbarung umzusetzen.

[0159] Computerausführbare Anweisungen können in vielen Formen, wie z. B. Programmmodulen, vorliegen, die von einem oder mehreren Computern oder anderen Vorrichtungen ausgeführt werden. Im Allgemeinen schließen Programmmodule Routinen, Programme, Objekte, Komponenten, Datenstrukturen usw. ein, die bestimmte Aufgaben durchführen oder bestimmte abstrakte Datentypen umsetzen. Typischerweise kann

die Funktionalität der Programmmodule nach Wunsch in verschiedenen Ausführungsformen kombiniert oder verteilt sein.

[0160] Zudem können Datenstrukturen in computerlesbaren Medien auf eine beliebige geeignete Form gespeichert sein. Zur einfacheren Veranschaulichung können Datenstrukturen so dargestellt werden, dass sie Felder aufweisen, die gemäß ihrer Position in der Datenstruktur in Beziehung stehen. Derartige Beziehungen können ebenso durch Zuweisen von Speicher für die Felder mit Positionen in einem computerlesbaren Medium erreicht werden, das eine Beziehung zwischen den Feldern vermittelt. Es kann jedoch ein beliebiger geeigneter Mechanismus verwendet werden, um eine Beziehung zwischen Informationen in Feldern einer Datenstruktur herzustellen, einschließlich durch die Verwendung von Pointern, Tags oder anderen Mechanismen, die eine Beziehung zwischen Datenelementen herstellen.

[0161] Verschiedene Merkmale und Aspekte der vorliegenden Offenbarung können allein, in einer beliebigen Kombination aus zwei oder mehr oder in einer Vielfalt von Anordnungen verwendet werden, die in den vorstehend beschriebenen Ausführungsformen nicht konkret erörtert sind, und daher ist sie in ihrer Anwendung nicht auf die Details und Anordnung von Komponenten beschränkt, die in der vorstehenden Beschreibung dargelegt oder in den Zeichnungen veranschaulicht sind. Beispielsweise können in einer Ausführungsform beschriebene Aspekte auf eine beliebige Art und Weise mit in einer anderen Ausführungsform beschriebenen Aspekten kombiniert werden.

[0162] Zudem können die hier offenbarten Konzepte als ein Verfahren umgesetzt sein, von dem hier ein Beispiel bereitgestellt wurde. Die als Teil des Verfahrens durchgeführten Schritte können auf eine beliebige geeignete Weise geordnet sein. Demnach können Ausführungsformen konstruiert werden, bei denen Schritte in einer anderen als der veranschaulichten Reihenfolge durchgeführt werden, was beinhalten kann, dass einige Schritte gleichzeitig durchgeführt werden, obwohl sie in veranschaulichenden Ausführungsformen als aufeinanderfolgende Schritte dargestellt sind.

[0163] Die Verwendung von Ordnungszahlwörtern, wie z. B. „erstes“, „zweites“, „drittes“ usw., in den Ansprüchen, um ein Anspruchselement zu modifizieren, bedeutet an sich keine Priorität, keinen Vorrang oder keine Reihenfolge eines Anspruchselements gegenüber einem anderen oder keine zeitliche Abfolge, in der Schritte eines Verfahrens durchgeführt werden, vielmehr werden sie lediglich als Bezeichnungen verwendet, um ein Anspruchselement mit einem bestimmten Namen von einem anderen Element mit einem gleichen Namen (mit Ausnehme des Ordnungszahlworts) zu unterscheiden, um die Anspruchselemente zu unterscheiden.

[0164] Zudem dienen die hier verwendete Phraseologie und Terminologie zur Beschreibung und sind nicht als einschränkend anzusehen. Die Verwendung von „einschließlich“, „umfassend“, „aufweisend“, „enthaltend“, „beinhaltend“ und Variationen davon in dieser Schrift soll die danach aufgeführten Elemente und Äquivalente davon sowie weitere Elemente einschließen.

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 62/325880 [0001]
- US 62/264418 [0001]
- US 62/241436 [0001]

Schutzansprüche

1. Computersystem, umfassend:
mindestens einen Prozessor; und
mindestens ein computerlesbares Medium, auf dem mehrere Anweisungen gespeichert sind, die bei Ausführung den mindestens einen Prozessor dazu veranlassen:
eine Anforderung zum Verifizieren mindestens einer Bestätigung für mindestens ein Attribut eines Identitätsinhabers zu empfangen, wobei:
die mindestens eine Bestätigung zwischen mehreren Zuständen in einem Distributed-Ledger-System beweglich ist, wobei die mehreren Zustände einen VERIFIED-Zustand beinhalten, und
die mindestens eine Bestätigung einen kryptographischen Nachweist umfasst; einen Wert, der dem mindestens einen Attribut entspricht, zu empfangen; und
zu bestimmen, ob der kryptographische Nachweis in der mindestens einen Bestätigung ein gültiger Nachweis für den empfangenen Wert ist, der dem mindestens einen Attribut entspricht;
auf Grundlage von Informationen, die auf den Identitätsinhaber bezogen sind, den empfangenen Wert, der dem mindestens einen Attribut entspricht, zu verifizieren; und
in Reaktion darauf, dass bestimmt wird, dass der kryptographische Nachweis in der mindestens einen Bestätigung ein gültiger Nachweis für den empfangenen Wert ist, der dem mindestens einen Attribut entspricht; und dass der empfange Wert, der dem mindestens einen Attribut entspricht, erfolgreich verifiziert wird:
die mindestens eine Bestätigung für das mindestens eine Attribut elektronisch zu signieren; und
über das Distributed-System zu veranlassen, dass sich die mindestens eine Bestätigung für das mindestens eine Attribut im VERIFIED-Zustand befindet.

2. Computersystem nach Anspruch 1, wobei:
das Distributed-Ledger-System unter Verwendung von mindestens einer Blockchain umgesetzt wird.

3. Computersystem nach einem der Ansprüche 1 oder 2, wobei:
die Anforderung einen Pointer zu der mindestens einen Bestätigung umfasst; und
die mehreren Anweisungen bei Ausführung den mindestens einen Prozessor ferner veranlassen, den Pointer zu verwenden, um auf die mindestens eine Bestätigung aus dem Distributed-Ledger-System zuzugreifen.

4. Computersystem nach Anspruch 3, wobei:
der Pointer auf einen Ausweis verweist, der in dem Distributed-Ledger-System gespeichert ist; und
der Ausweis mehrere Bestätigungen umfasst, die jeweils mehreren Attributen des Identitätsinhabers entsprechen, wobei die mehreren Bestätigungen die mindestens eine Bestätigung umfassen.

5. Computersystem nach einem der Ansprüche 1 bis 4, wobei:
das Distributed-Ledger-System eine digitale Identitätsdarstellung umfasst, die dem Identitätsinhaber zugeordnet ist, wobei die digitale Identitätsdarstellung Programmcode umfasst, der Regeln zur Bestätigung umsetzt.

6. Computersystem nach Anspruch 5, wobei:
der Programmcode bei Ausführung Zustandsinformationen für die mindestens eine Bestätigung verwaltet.

7. Computersystem nach Anspruch 6, wobei:
die mehreren Zustände der mindestens einen Bestätigung ferner Folgendes umfassen: PENDING, EXPIRED und INVALID; und
der Programmcode bei Ausführung die mindestens eine Bestätigung in einem der mehreren Zustände hält.

8. Computersystem nach einem der Ansprüche 6 bis 7, wobei:
der Programmcode bei Ausführung veranlasst, dass die mindestens eine Bestätigung von einem PENDING-Zustand in den VERIFIED-Zustand nur in Reaktion auf eine Anweisung einer Entität, die dafür zuständig ist, das mindestens eine Attribut zu verifizieren, übergeht.

9. Computersystem nach einem der Ansprüche 6 bis 8, wobei:
der Programmcode bei Ausführung veranlasst, dass die mindestens eine Bestätigung von dem VERIFIED-Zustand in einen EXPIRED-Zustand nach Ablauf eines Zeitgebers, der gestellt wurde, als die mindestens eine Bestätigung zuletzt in den VERIFIED-Zustand übergegangen ist, übergeht.

10. Computersystem nach einem der Ansprüche 5 bis 9, wobei:

der Programmcode bei Ausführung einen Zugang zu dem kryptographischen Nachweis in der mindestens einen Bestätigung nur dann ermöglicht, wenn sich die mindestens eine Bestätigung in dem VERIFIED-Zustand befindet.

11. Computersystem nach einem der Ansprüche 1 bis 10, wobei der Identitätsinhaber ein Benutzer ist.

12. Computersystem nach einem der Ansprüche 1 bis 11, wobei:
der Wert, der dem mindestens einen Attribut entspricht, über einen Kanal außerhalb des Distributed Ledger empfangen wird.

13. Computersystem, umfassend:
mindestens einen Prozessor; und
mindestens ein computerlesbares Medium, auf dem mehrere Anweisungen gespeichert sind, die bei Ausführung den mindestens einen Prozessor dazu programmieren:
mindestens eine Bestätigung zur Verwendung beim Bestätigen eines Attributs eines Identitätsinhaber zu erzeugen, wobei die mindestens eine Bestätigung einen kryptographischen Nachweis für einen Wert, der dem Attribut des Identitätsinhabers entspricht, umfasst;
eine Entität als dafür zuständig, die mindestens eine Bestätigung zu verifizieren, identifizieren;
die mindestens eine Bestätigung in einem Distributed-Ledger-System zu veröffentlichen, wobei die mindestens eine Bestätigung zwischen mehreren Zuständen in dem Distributed-Ledger-System beweglich ist, wobei die mehreren Zustände einen VERIFIED-Zustand beinhalten, und
eine Anforderung an die verantwortliche Entität zu senden, die mindestens eine Bestätigung zu verifizieren.

14. Computersystem nach Anspruch 13, wobei:
das Distributed-Ledger-System unter Verwendung von mindestens einer Blockchain umgesetzt wird.

15. Computersystem nach einem der Ansprüche 13 oder 14, wobei:
die Anforderung einen Pointer zu der mindestens einen Bestätigung zur Verwendung durch die zuständige Partei, um auf die mindestens eine Bestätigung aus dem Distributed-Ledger-System zuzugreifen, umfasst.

16. Computersystem nach Anspruch 15, wobei:
der Pointer auf einen Ausweis verweist, der in dem Distributed-Ledger-System gespeichert ist; und
der Ausweis mehrere Bestätigungen umfasst, die jeweils mehreren Attributen des Identitätsinhabers entsprechen, wobei die mehreren Bestätigungen die mindestens eine Bestätigung umfassen.

17. Computersystem nach Anspruch 16, wobei die mehreren Anweisungen bei Ausführung den mindestens einen Prozessor ferner dazu programmieren:
ein Schema aus mehreren Schemata für Ausweise auszuwählen, wobei das Schema die mehreren Attribute umfasst, und
gemäß dem Schema den Ausweis zu erzeugen.

18. Computersystem nach einem der Ansprüche 13 bis 17, wobei:
das Distributed-Ledger-System eine digitale Identitätsdarstellung umfasst, die dem Identitätsinhaber zugeordnet ist, wobei die digitale Identitätsdarstellung Programmcode umfasst, der Regeln zur Bestätigung umsetzt.

19. Computersystem nach Anspruch 18, wobei:
der Programmcode bei Ausführung Zustandsinformationen für die mindestens eine Bestätigung verwaltet.

20. Computersystem nach Anspruch 19, wobei:
die mehreren Zustände der mindestens einen Bestätigung ferner Folgendes umfassen: PENDING, EXPIRED und INVALID; und
der Programmcode bei Ausführung die mindestens eine Bestätigung in einem der mehreren Zustände hält.

21. Computersystem nach einem der Ansprüche 19 oder 20, wobei:
der Programmcode bei Ausführung veranlasst, dass die mindestens eine Bestätigung von einem PENDING-Zustand in den VERIFIED-Zustand nur in Reaktion auf eine Anweisung der Entität, die dafür zuständig ist, das mindestens eine Attribut zu verifizieren, übergeht.

22. Computersystem nach einem der Ansprüche 19 bis 21, wobei:

der Programmcode bei Ausführung veranlasst, dass die mindestens eine Bestätigung von dem VERIFIED-Zustand in einen EXPIRED-Zustand nach Ablauf eines Zeitgebers, der gestellt wurde, als die mindestens eine Bestätigung zuletzt in den VERIFIED-Zustand übergegangen ist, übergeht.

23. Computersystem nach einem der Ansprüche 13 bis 22, wobei:
der Programmcode bei Ausführung einen Zugang zu dem kryptographischen Nachweis in der mindestens einen Bestätigung nur dann ermöglicht, wenn sich die mindestens eine Bestätigung in dem VERIFIED-Zustand befindet.

24. Computersystem nach einem der Ansprüche 13 bis 23, wobei die mehreren Anweisungen bei Ausführung den mindestens einen Prozessor ferner dazu veranlassen:
über einen Kanal außerhalb des Distributed Ledger den Wert, der dem Attribut des Identitätsinhabers entspricht, an die zuständige Entität zu senden.

25. Computersystem nach einem der Ansprüche 13 bis 24, wobei das Erzeugen von mindestens einer Bestätigung Schritte umfasst zum:
Verwenden mehrerer Messungen, die an dem Identitätsinhaber durchgeführt werden, um eine Kennung für den Identitätsinhaber zu erzeugen, wobei die Kennung einen kryptographischen Nachweis für die mehreren Messungen umfasst;
Instanziieren der digitalen Identitätsdarstellung, wobei die digitale Identitätsdarstellung der Kennung für den Identitätsinhaber zugeordnet ist; und
Erzeugen einer elektronischen Signatur über die digitale Identitätsdarstellung, wobei das Veröffentlichen der mindestens einen Bestätigung das Veröffentlichen der digitalen Identitätsdarstellung und der elektronischen Signatur in dem Distributed-Ledger-System umfasst.

26. Computersystem nach Anspruch 25, wobei:
der Identitätsinhaber eine natürliche Person ist; und
die mehreren Messungen mindestens eine biometrische Messung und mindestens eine Verhaltensmessung umfassen.

27. Computerlesbares Medium, auf dem mehrere Anweisungen gespeichert sind, die bei Ausführung den mindestens einen Prozessor dazu programmieren:
eine Anforderung zum Verifizieren mindestens einer Bestätigung für mindestens ein Attribut eines Identitätsinhabers zu empfangen, wobei:
die mindestens eine Bestätigung zwischen mehreren Zuständen in einem Distributed-Ledger-System beweglich ist, wobei die mehreren Zustände einen VERIFIED-Zustand beinhalten, und
die mindestens eine Bestätigung einen kryptographischen Nachweist umfasst; einen Wert, der dem mindestens einen Attribut entspricht, zu empfangen; und
zu bestimmen, ob der kryptographische Nachweis in der mindestens einen Bestätigung ein gültiger Nachweis für den empfangenen Wert ist, der dem mindestens einen Attribut entspricht;
auf Grundlage von Informationen, die auf den Identitätsinhaber bezogen sind, den empfangenen Wert, der dem mindestens einen Attribut entspricht, zu verifizieren; und
in Reaktion darauf, dass bestimmt wird, dass der kryptographische Nachweis in der mindestens einen Bestätigung ein gültiger Nachweis für den empfangenen Wert ist, der dem mindestens einen Attribut entspricht; und dass der empfange Wert, der dem mindestens einen Attribut entspricht, erfolgreich verifiziert wird:
die mindestens eine Bestätigung für das mindestens eine Attribut elektronisch zu signieren; und
über das Distributed-System zu veranlassen, dass sich die mindestens eine Bestätigung für das mindestens eine Attribut im VERIFIED-Zustand befindet.

28. Computerlesbares Medium nach Anspruch 27, wobei:
das Distributed-Ledger-System unter Verwendung von mindestens einer Blockchain umgesetzt wird.

29. Computerlesbares Medium nach einem der Ansprüche 27 bis 28, wobei:
die Anforderung einen Pointer zu der mindestens einen Bestätigung umfasst; und
die mehreren Anweisungen bei Ausführung den mindestens einen Prozessor ferner programmieren, den Pointer zu verwenden, um auf die mindestens eine Bestätigung aus dem Distributed-Ledger-System zuzugreifen.

30. Computerlesbares Medium nach Anspruch 29, wobei:
der Pointer auf einen Ausweis verweist, der in dem Distributed-Ledger-System gespeichert ist; und

der Ausweis mehrere Bestätigungen umfasst, die jeweils mehreren Attributen des Identitätsinhabers entsprechen, wobei die mehreren Bestätigungen die mindestens eine Bestätigung umfassen.

31. Computerlesbares Medium nach einem der Ansprüche 27 bis 30, wobei:
das Distributed-Ledger-System eine digitale Identitätsdarstellung umfasst, die dem Identitätsinhaber zugeordnet ist, wobei die digitale Identitätsdarstellung Programmcode umfasst, der Regeln zur Bestätigung umsetzt.

32. Computerlesbares Medium nach Anspruch 31, wobei:
der Programmcode bei Ausführung Zustandsinformationen für die mindestens eine Bestätigung verwaltet.

33. Computerlesbares Medium nach Anspruch 31 oder 32, wobei:
die mehreren Zustände der mindestens einen Bestätigung ferner Folgendes umfassen: PENDING, EXPIRED und INVALID; und
der Programmcode bei Ausführung die mindestens eine Bestätigung in einem der mehreren Zustände hält.

34. Computerlesbares Medium nach Anspruch 31 bis 33, wobei:
der Programmcode bei Ausführung veranlasst, dass die mindestens eine Bestätigung von einem PENDING-Zustand in den VERIFIED-Zustand nur in Reaktion auf eine Anweisung einer Entität, die dafür zuständig ist, das mindestens eine Attribut zu verifizieren, übergeht.

35. Computerlesbares Medium nach Anspruch 31 bis 34, wobei:
der Programmcode bei Ausführung veranlasst, dass die mindestens eine Bestätigung von dem VERIFIED-Zustand in einen EXPIRED-Zustand nach Ablauf eines Zeitgebers, der gestellt wurde, als die mindestens eine Bestätigung zuletzt in den VERIFIED-Zustand übergegangen ist, übergeht.

36. Computerlesbares Medium nach Anspruch 31 bis 35, wobei:
der Programmcode bei Ausführung einen Zugang zu dem kryptographischen Nachweis in der mindestens einen Bestätigung nur dann ermöglicht, wenn sich die mindestens eine Bestätigung in dem VERIFIED-Zustand befindet.

37. Computerlesbares Medium nach einem der Ansprüche 27 bis 36, wobei der Identitätsinhaber ein Benutzer ist.

38. Computerlesbares Medium nach einem der Ansprüche 27 bis 37, wobei:
der Wert, der dem mindestens einen Attribut entspricht, über einen Kanal außerhalb des Distributed Ledgers empfangen wird.

39. Computerlesbares Medium, auf dem mehrere Anweisungen gespeichert sind, die bei Ausführung den mindestens einen Prozessor dazu programmieren:
mindestens eine Bestätigung zur Verwendung beim Bestätigen eines Attributs eines Identitätsinhabers zu erzeugen, wobei die mindestens eine Bestätigung einen kryptographischen Nachweis für einen Wert, der dem Attribut des Identitätsinhabers entspricht, umfasst;
eine Entität als dafür zuständig, die mindestens eine Bestätigung zu verifizieren, identifizieren;
die mindestens eine Bestätigung in einem Distributed-Ledger-System zu veröffentlichen, wobei die mindestens eine Bestätigung zwischen mehreren Zuständen in dem Distributed-Ledger-System beweglich ist, wobei die mehreren Zustände einen VERIFIED-Zustand beinhalten, und
eine Anforderung an die verantwortliche Entität zu senden, die mindestens eine Bestätigung zu verifizieren.

40. Computerlesbares Medium nach Anspruch 39, wobei:
das Distributed-Ledger-System unter Verwendung von mindestens einer Blockchain umgesetzt wird.

41. Computerlesbares Medium nach einem der Ansprüche 39 oder 40, wobei:
die Anforderung einen Pointer zu der mindestens einen Bestätigung zur Verwendung durch die zuständige Partei, um auf die mindestens eine Bestätigung aus dem Distributed-Ledger-System zuzugreifen, umfasst;

42. Computerlesbares Medium nach Anspruch 41, wobei:
der Pointer auf einen Ausweis verweist, der in dem Distributed-Ledger-System gespeichert ist; und
der Ausweis mehrere Bestätigungen umfasst, die jeweils mehreren Attributen des Identitätsinhabers entsprechen, wobei die mehreren Bestätigungen die mindestens eine Bestätigung umfassen.

43. Computerlesbares Medium nach Anspruch 42, wobei die mehreren Anweisungen bei Ausführung den mindestens einen Prozessor ferner dazu veranlassen:
ein Schema aus mehreren Schemata für Ausweise auszuwählen, wobei das Schema die mehreren Attribute umfasst, und gemäß dem Schema den Ausweis zu erzeugen.

44. Computerlesbares Medium nach einem der Ansprüche 39 bis 43, wobei:
das Distributed-Ledger-System eine digitale Identitätsdarstellung umfasst, die dem Identitätsinhaber zugeordnet ist, wobei die digitale Identitätsdarstellung Programmcode umfasst, der Regeln zur Bestätigung umsetzt.

45. Computerlesbares Medium nach Anspruch 44, wobei:
der Programmcode bei Ausführung Zustandsinformationen für die mindestens eine Bestätigung verwaltet.

46. Computerlesbares Medium nach einem der Ansprüche 44 oder 45, wobei:
die mehreren Zustände der mindestens einen Bestätigung ferner Folgendes umfassen: PENDING, EXPIRED und INVALID; und
der Programmcode bei Ausführung die mindestens eine Bestätigung in einem der mehreren Zustände hält.

47. Computerlesbares Medium nach einem der Ansprüche 45 oder 46, wobei:
der Programmcode bei Ausführung veranlasst, dass die mindestens eine Bestätigung von einem PENDING-Zustand in den VERIFIED-Zustand nur in Reaktion auf eine Anweisung der Entität, die dafür zuständig ist, das mindestens eine Attribut zu verifizieren, übergeht.

48. Computerlesbares Medium nach einem der Ansprüche 45 bis 47, wobei:
der Programmcode bei Ausführung veranlasst, dass die mindestens eine Bestätigung von dem VERIFIED-Zustand in einen EXPIRED-Zustand nach Ablauf eines Zeitgebers, der gestellt wurde, als die mindestens eine Bestätigung zuletzt in den VERIFIED-Zustand übergegangen ist, übergeht.

49. Computerlesbares Medium nach einem der Ansprüche 39 bis 48, wobei:
der Programmcode bei Ausführung einen Zugang zu dem kryptographischen Nachweis in der mindestens einen Bestätigung nur dann ermöglicht, wenn sich die mindestens eine Bestätigung in dem VERIFIED-Zustand befindet.

50. Computerlesbares Medium nach einem der Ansprüche 39 bis 49, wobei die mehreren Anweisungen bei Ausführung den mindestens einen Prozessor ferner dazu veranlassen:
über einen Kanal außerhalb des Distributed Ledger den Wert, der dem Attribut des Identitätsinhabers entspricht, an die zuständige Entität zu senden.

51. Computerlesbares Medium nach einem der Ansprüche 39 bis 50, wobei das Erzeugen von mindestens einer Bestätigung Schritte umfasst zum:
Verwenden mehrerer Messungen, die an dem Identitätsinhaber durchgeführt werden, um eine Kennung für den Identitätsinhaber zu erzeugen, wobei die Kennung einen kryptographischen Nachweis für die mehreren Messungen umfasst;
Instanziieren der digitalen Identitätsdarstellung, wobei die digitale Identitätsdarstellung der Kennung für den Identitätsinhaber zugeordnet ist; und
Erzeugen einer elektronischen Signatur über die digitale Identitätsdarstellung; wobei das Veröffentlichen der mindestens einen Bestätigung das Veröffentlichen der digitalen Identitätsdarstellung und der elektronischen Signatur in dem Distributed-Ledger-System umfasst.

52. Computerlesbares Medium nach Anspruch 51, wobei:
der Identitätsinhaber eine natürliche Person ist; und
die mehreren Messungen mindestens eine biometrische Messung und mindestens eine Verhaltensmessung umfassen.

53. Mindestens ein computerlesbares Medium, auf dem Anweisungen gespeichert sind, die bei Ausführung mindestens einen Prozessor dazu programmieren, ein Verfahren auszuführen, umfassend Schritte zum:
Empfangen eines Pointers zu einem Ausweis zur Verwendung beim Bestätigen einer Identität eines Benutzers;
Verwenden des Pointers, um auf den Ausweis aus einer digitalen Identitätsdarstellung in einem Distributed-Ledger-System zuzugreifen, wobei:
die digitale Identitätsdarstellung einer Kennung für den Benutzer zugeordnet ist, wobei die digitale Identitätsdarstellung Programmcode umfasst, der Regeln zur Bestätigung umsetzt;

der Ausweis mehrere Attributbestätigungen umfasst, die jeweils mehreren Attributen entsprechen; und
für jedes Attribut der mehreren Attribute die entsprechende Attributbestätigung einen kryptographischen Nachweis umfasst;
Empfangen, über einen Kanal außerhalb des Distributed-Ledger-Systems, mehrerer Werte, die für jedes Attribut der mehreren Attribute, einen Wert umfassen, der diesem Attribut entspricht;
Identifizieren, anhand des Ausweises, einer Entität, die dafür zuständig ist, den Ausweis zu verifizieren;
Bestimmen, ob der Entität, die dafür zuständig ist, den Ausweis zu verifizieren, zu vertrauen ist; und
in Reaktion darauf, dass bestimmt wird, dass der Entität, die dafür zuständig ist, den Ausweis zu verifizieren, zu vertrauen ist, Prüfen, für jede Attributbestätigung der mehreren Attributbestätigungen, ob:
sich die Attributbestätigung in einem VERIFIED-Zustand befindet;
der kryptographische Nachweis in der Attributbestätigung ein gültiger Nachweis für den empfangenen Wert ist, der dem Attribut entspricht, das der Attributbestätigung entspricht; und
die Attributbestätigung durch die Entität, die dafür zuständig ist, den Ausweis zu verifizieren, elektronisch signiert ist.

54. Mindestens ein computerlesbares Medium nach Anspruch 53, auf dem weitere Anweisungen gespeichert sind, wobei der mindestens eine Prozessor ferner derart programmiert ist, dass, wenn die Anweisungen ausgeführt werden:
auf die digitale Identitätsdarstellung aus dem Distributed-Ledger-System zugegriffen wird, zusammen mit einer elektronischen Signatur, die über die digitale Identitätsdarstellung erzeugt wird.

55. Mindestens ein computerlesbares Medium nach einem der Ansprüche 53 oder 54, wobei:
das Distributed-Ledger-System unter Verwendung von mindestens einer Blockchain umgesetzt wird.

56. Mindestens ein computerlesbares Medium nach einem der Ansprüche 53 bis 55, wobei
der Ausweis gemäß einem Schema erzeugt wird, das aus mehreren Schemata für Ausweise ausgewählt ist, wobei das Schema die mehreren Attribute umfasst.

57. Mindestens ein computerlesbares Medium nach einem der Ansprüche 53 bis 56, wobei:
der Programmcode bei Ausführung durch mindestens einen Prozessor Zustandsinformationen für die Attributbestätigung jedes Attributs der mehreren Attribute verwaltet.

58. Mindestens ein computerlesbares Medium nach Anspruch 57, wobei der Programmcode bei Ausführung durch den mindestens einen Prozessor eine Attributbestätigung der mehreren Attributbestätigungen in einem Zustand hält, der ausgewählt ist aus einer Gruppe, bestehend aus: PENDING, VERIFIED, EXPIRED und INVALID.

59. Mindestens ein computerlesbares Medium nach Anspruch 58, wobei der Programmcode bei Ausführung durch den mindestens einen Prozessor veranlasst, dass die Attributbestätigung der mehreren Attributbestätigungen von einem PENDING-Zustand in den VERIFIED-Zustand nur in Reaktion auf eine Benachrichtigung von der Entität, die dafür zuständig ist, den Ausweis zu verifizieren, dass ein entsprechender Attributwert durch die vertrauenswürdige Entität, die dafür zuständig ist, den Ausweis zu verifizieren, verifiziert wurde, übergeht.

60. Mindestens ein computerlesbares Medium nach einem der Ansprüche 58 bis 59, wobei der Programmcode bei Ausführung durch den mindestens einen Prozessor veranlasst, dass die Attributbestätigung der mehreren Attributbestätigungen von dem VERIFIED-Zustand in einen EXPIRED-Zustand nach Ablauf eines Zeitgebers, der gestellt wurde, als ein entsprechender Attributwert zuletzt verifiziert wurde, übergeht.

61. Mindestens ein computerlesbare Mediums nach einem der Ansprüche 58 bis 60, wobei der Programmcode bei Ausführung durch den mindestens einen Prozessor einen Zugang zu einem kryptographischen Nachweis in der Attributbestätigung nur dann ermöglicht, wenn sich die Attributbestätigung in dem VERIFIED-Zustand befindet.

62. Mindestens ein computerlesbares Medium, auf dem Anweisungen gespeichert sind, die bei Ausführung mindestens einen Prozessor dazu programmieren, ein Verfahren auszuführen, umfassend Schritte zum:
Empfangen, über ein Distributed-Ledger-System, einer Anforderung zum Verifizieren eines ersten Ausweises, wobei der erste Ausweis mehrere Attributbestätigungen umfasst, die jeweils mehreren Attributen für einen Benutzer entsprechen, wobei für jedes Attribut der mehreren Attribute die entsprechende Attributbestätigung einen kryptographischen Nachweis umfasst;

Empfangen, über einen Kanal außerhalb des Distributed-Ledger-Systems, mehrerer Werte, die für jedes Attribut der mehreren Attribute, einen Wert umfassen, der diesem Attribut entspricht; und
für mindestens ein Attribut der mehreren Attribute:
Identifizieren, anhand des ersten Ausweises, einer ersten Attributbestätigung, die dem mindestens einen Attribut entspricht, wobei die erste Attributbestätigung einen ersten kryptographischen Nachweis umfasst;
Identifizieren, anhand der ersten Attributbestätigung, eines Pointers zu einem zweiten Ausweis;
Verwenden des Pointers, um auf den zweiten Ausweis aus dem Distributed Ledger zuzugreifen;
Identifizieren, anhand des zweiten Ausweises, einer Entität, die dafür zuständig ist, den zweiten Ausweis zu verifizieren, und einer zweiten Attributbestätigung, die dem mindestens einen Attribut entspricht;
Bestimmen, ob der Entität, die dafür zuständig ist, den zweiten Ausweis zu verifizieren, zu vertrauen ist; und
in Reaktion darauf, dass bestimmt wird, dass der Entität, die dafür zuständig ist, den zweiten Ausweis zu verifizieren, zu vertrauen ist, Prüfen, ob:
(1) sich die zweite Attributbestätigung in einem VERIFIED-Zustand befindet;
(2) der zweite kryptographische Nachweis ein gültiger Nachweis für den empfangenen Wert ist, der dem mindestens einen Attribut entspricht; und
(3) die zweite Attributbestätigung durch die Entität, die dafür zuständig ist, den zweiten Ausweis zu verifizieren, elektronisch signiert ist.

63. Mindestens ein computerlesbares Medium nach Anspruch 62, auf dem weitere Anweisungen gespeichert sind, wobei der mindestens eine Prozessor ferner dazu programmiert ist, wenn die Anweisungen ausgeführt werden, einen Schritt zum Prüfen auszuführen, ob:
(4) der erste kryptographische Nachweis ein gültiger Nachweis für den empfangenen Wert ist, der dem mindestens einen Attribut entspricht.

64. Mindestens ein computerlesbares Medium nach Anspruch 63, auf dem weitere Anweisungen gespeichert sind, wobei der mindestens eine Prozessor ferner dazu programmiert ist, wenn die Anweisungen ausgeführt werden, in Reaktion darauf, dass bestimmt wird, dass (1)-(4) erfüllt sind, Schritte auszuführen zum:
elektronischen Signieren der ersten Attributbestätigung; und
Veranlassen, dass die erste Attributbestätigung in einen VERIFIED-Zustand übergeht.

65. System umfassend:
mindestens einen Prozessor;
mindestens ein computerlesbares Medium, auf dem Anweisungen gespeichert sind, die bei Ausführung den mindestens einen Prozessor dazu programmieren:
einen Pointer zu einem Ausweis zur Verwendung beim Bestätigen einer Identität eines Benutzers zu empfangen;
den Pointer zu verwenden, um auf den Ausweis aus einer digitalen Identitätsdarstellung in einem Distributed-Ledger-System zuzugreifen, wobei:
die digitale Identitätsdarstellung einer Kennung für den Benutzer zugeordnet ist, wobei die digitale Identitätsdarstellung Programmcode umfasst, der Regeln zur Bestätigung umsetzt;
anhand des Ausweises mehrere Attributbestätigungen zu identifizieren, die jeweils mehreren Attributen entsprechen;
für jedes Attribut der mehreren Attribute anhand der entsprechenden Attributbestätigung einen kryptographischen Nachweis zu identifizieren;
über einen Kanal außerhalb des Distributed-Ledger-Systems, mehrere Werte zu empfangen, die für jedes Attribut der mehreren Attribute, einen Wert umfassen, der diesem Attribut entspricht;
anhand des Ausweises, eine Entität zu identifizieren, die dafür zuständig ist, den Ausweis zu verifizieren;
zu bestimmen, ob der Entität, die dafür zuständig ist, den Ausweis zu verifizieren, zu vertrauen ist; und
in Reaktion darauf, dass bestimmt wird, dass der Entität, die dafür zuständig ist, den Ausweis zu verifizieren, zu vertrauen ist, für jede Attributbestätigung der mehreren Attributbestätigungen zu prüfen, ob:
sich die Attributbestätigung in einem VERIFIED-Zustand befindet;
der kryptographische Nachweis in der Attributbestätigung ein gültiger Nachweis für den empfangenen Wert ist, der dem Attribut entspricht, das der Attributbestätigung entspricht; und
die Attributbestätigung durch die Entität, die dafür zuständig ist, den Ausweis zu verifizieren, elektronisch signiert ist.

66. System nach Anspruch 65, wobei auf dem computerlesbaren Medium weitere Anweisungen gespeichert sind, die bei Ausführung den mindestens einen Prozessor, wenn die Anweisungen ausgeführt werden, dazu veranlassen, dass:

auf die digitale Identitätsdarstellung aus dem Distributed-Ledger-System zugegriffen wird, zusammen mit einer elektronischen Signatur, die über die digitale Identitätsdarstellung erzeugt wird.

67. System nach einem der Ansprüche 65 oder 66, wobei:
das Distributed-Ledger-System unter Verwendung von mindestens einer Blockchain umgesetzt wird.

68. System nach einem der Ansprüche 65 bis 67, wobei:
der Ausweis gemäß einem Schema erzeugt wird, das aus mehreren Schemata für Ausweise ausgewählt ist, wobei das Schema die mehreren Attribute umfasst.

69. System nach einem der Ansprüche 65 bis 68, wobei:
der Programmcode bei Ausführung Zustandsinformationen für die Attributbestätigung jedes Attributs der mehreren Attribute verwaltet.

70. System nach Anspruch 69, wobei der Programmcode bei Ausführung eine Attributbestätigung der mehreren Attributbestätigungen in einem Zustand hält, der ausgewählt ist aus einer Gruppe, bestehend aus: PENDING, VERIFIED, EXPIRED und INVALID.

71. System nach einem der Ansprüche 69 bis 70, wobei:
der Programmcode bei Ausführung veranlasst, dass die Attributbestätigung der mehreren Attributbestätigungen von einem PENDING-Zustand in den VERIFIED-Zustand nur in Reaktion auf eine Benachrichtigung von der Entität, die dafür zuständig ist, den Ausweis zu verifizieren, dass ein entsprechender Attributwert durch die vertrauenswürdige Entität, die dafür zuständig ist, den Ausweis zu verifizieren, verifiziert wurde, übergeht.

72. System nach einem der Ansprüche 70 bis 71, wobei:
der Programmcode bei Ausführung veranlasst, dass die Attributbestätigung der mehreren Attributbestätigungen von dem VERIFIED-Zustand in einen EXPIRED-Zustand nach Ablauf eines Zeitgebers, der gestellt wurde, als ein entsprechender Attributwert zuletzt verifiziert wurde, übergeht.

73. System nach einem der Ansprüche 70 bis 72, wobei:
der Programmcode bei Ausführung einen Zugang zu einem kryptographischen Nachweis in der Attributbestätigung nur dann ermöglicht, wenn sich die Attributbestätigung in dem VERIFIED-Zustand befindet.

74. System, umfassend:
mindestens einen Prozessor;
mindestens ein computerlesbares Medium, auf dem Anweisungen gespeichert sind, die bei Ausführung den mindestens einen Prozessor dazu programmieren:
über ein Distributed-Ledger-System eine Anforderung zum Verifizieren eines ersten Ausweises zu empfangen, wobei der erste Ausweis mehrere Attributbestätigungen umfasst, die jeweils mehreren Attributen für einen Benutzer entsprechen, wobei für jedes Attribut der mehreren Attribute die entsprechende Attributbestätigung einen kryptographischen Nachweis umfasst;
über einen Kanal außerhalb des Distributed-Ledger-Systems mehrere Werte zu empfangen, die für jedes Attribut der mehreren Attribute, einen Wert umfassen, der diesem Attribut entspricht; und
für mindestens ein Attribut der mehreren Attribute:
anhand des ersten Ausweises eine erste Attributbestätigung zu identifizieren, die dem mindestens einen Attribut entspricht, wobei die erste Attributbestätigung einen ersten kryptographischen Nachweis umfasst;
anhand der ersten Attributbestätigung einen Pointer zu einem zweiten Ausweis zu identifizieren;
den Pointer zu verwenden, um auf den zweiten Ausweis aus dem Distributed Ledger zuzugreifen;
anhand des zweiten Ausweises eine Entität, die dafür zuständig ist, den zweiten Ausweis zu verifizieren, und eine zweite Attributbestätigung, die dem mindestens einen Attribut entspricht, zu identifizieren;
zu bestimmen, ob der Entität, die dafür zuständig ist, den zweiten Ausweis zu verifizieren, zu vertrauen ist; und
in Reaktion darauf, dass bestimmt wird, dass der Entität, die dafür zuständig ist, den zweiten Ausweis zu verifizieren, zu vertrauen ist, zu prüfen, ob:
(1) sich die zweite Attributbestätigung in einem VERIFIED-Zustand befindet;
(2) der zweite kryptographische Nachweis ein gültiger Nachweis für den empfangenen Wert ist, der dem mindestens einen Attribut entspricht; und
(3) die zweite Attributbestätigung durch die Entität, die dafür zuständig ist, den zweiten Ausweis zu verifizieren, elektronisch signiert ist.

75. System nach Anspruch 74, wobei auf dem computerlesbaren Medium weitere Anweisungen gespeichert sind, die bei Ausführung den mindestens einen Prozessor dazu programmieren, zu prüfen ob:
(4) der erste kryptographische Nachweis ein gültiger Nachweis für den empfangenen Wert ist, der dem mindestens einen Attribut entspricht.

76. System nach Anspruch 75, wobei auf dem computerlesbaren Medium weitere Anweisungen gespeichert sind, die bei Ausführung den mindestens einen Prozessor dazu programmieren, in Reaktion darauf, dass bestimmt wird, dass (1)-(4) erfüllt sind:
die erste Attributbestätigung elektronisch zu signieren; und
zu veranlassen, dass die erste Attributbestätigung in einen VERIFIED-Zustand übergeht.

77. Mindestens ein computerlesbares Medium, auf dem Anweisungen gespeichert sind, die bei Ausführung mindestens einen Prozessor dazu programmieren, ein Verfahren auszuführen, umfassend Schritte zum:
Erzeugen eines Ausweises zur Verwendung beim Bestätigen einer Identität eines Identitätsinhabers, wobei der Schritt zum Erzeugen Folgendes umfasst:
Identifizieren mehrerer Werte, wobei jeder Wert einem Attribut von mehreren Attributen entspricht,
Erzeugen einer Attributbestätigung für jedes Attribut der mehreren Attribute, wobei die Attributbestätigung mindestens einen kryptographischen Nachweis des Wertes umfasst, der dem Attribut der mehreren Attribute entspricht; und
Identifizieren einer Entität als dafür zuständig, den Ausweis zu verifizieren;
Veröffentlichen des Ausweises in einem Distributed-Ledger-System, wobei:
der Ausweis die Attributbestätigung für jedes Attribut der mehreren Attribute beinhaltet;
das Distributed-Ledger-System eine digitale Identitätsdarstellung umfasst, die dem Identitätsinhaber zugeordnet ist;
die digitale Identitätsdarstellung Programmcode umfasst, der Regeln zur Bestätigung umsetzt; und
für mindestens ein Attribut der mehreren Attribute der Programmcode bei Ausführung einen Zugang zu einem kryptographischen Nachweis in der Attributbestätigung für das mindestens eine Attribut nur dann ermöglicht, wenn sich die Attributbestätigung in einem VERIFIED-Zustand befindet; und
Senden, über das Distributed-Ledger-System, einer Anforderung an eine Entität, die dafür zuständig ist, den Ausweis zu verifizieren; und
Senden, über einen Kanal außerhalb des Distributed-Ledger-Systems, der mehreren Werte, die jeweils den mehreren Attributen entsprechen, an die zuständige Entität.

78. Mindestens ein computerlesbares Medium nach Anspruch 77, auf dem weitere Anweisungen gespeichert sind, die bei Ausführung den mindestens einen Prozessor dazu programmieren, Schritte auszuführen zum:
Verwenden mehrerer Messungen, die an dem Identitätsinhaber durchgeführt werden, um eine Kennung für den Identitätsinhaber zu erzeugen, wobei die Kennung einen kryptographischen Nachweis für die mehreren Messungen umfasst;
Instanziieren der digitalen Identitätsdarstellung, wobei die digitale Identitätsdarstellung der Kennung für den Identitätsinhaber zugeordnet ist;
Erzeugen einer elektronischen Signatur über die digitale Identitätsdarstellung; und
Veröffentlichen der digitalen Identitätsdarstellung und der elektronischen Signatur in dem Distributed-Ledger-System.

79. Mindestens ein computerlesbares Medium nach Anspruch 78, wobei:
der Identitätsinhaber eine natürliche Person ist, und
die mehreren Messungen mindestens eine biometrische Messung und mindestens eine Verhaltensmessung umfassen.

80. Mindestens ein computerlesbares Medium nach einem der Ansprüche 77 oder 78, auf dem weitere Anweisungen gespeichert sind, die bei Ausführung den mindestens einen Prozessor dazu programmieren, einen Schritt auszuführen zum:
Empfangen einer Bestätigung von dem Distributed-Ledger-System, dass ein Datensatz der digitalen Identitätsdarstellung erzeugt wurde.

81. Mindestens ein computerlesbares Medium nach einem der Ansprüche 77 bis 80, wobei:
das Distributed-Ledger-System unter Verwendung von mindestens einer Blockchain umgesetzt wird.

82. Mindestens ein computerlesbares Medium nach einem der Ansprüche 77 bis 81, auf dem weitere Anweisungen gespeichert sind, die bei Ausführung den mindestens einen Prozessor dazu programmieren, einen Schritt auszuführen zum:
Auswählen eines Schemas aus mehreren Schemata für Ausweise, wobei das Schema die mehreren Attribute umfasst, wobei der Ausweis gemäß dem Schema erzeugt wird.

83. Mindestens ein computerlesbares Medium, auf dem Anweisungen gespeichert sind, die bei Ausführung mindestens einen Prozessor dazu programmieren, ein Verfahren für eine Entität auszuführen, wobei das Verfahren Schritte umfasst zum:
Empfangen, über ein Distributed-Ledger-System, einer Anforderung zum Verifizieren eines Ausweises, wobei der Ausweis mehrere Attributbestätigungen umfasst, die jeweils mehreren Attributen für einen Identitätsinhaber entsprechen, wobei für jedes Attribut der mehreren Attribute die entsprechende Attributbestätigung einen kryptographischen Nachweis umfasst, und wobei der Ausweis die Entität als dafür zuständig, den Ausweis zu verifizieren, identifiziert;
Empfangen, über einen Kanal außerhalb des Distributed-Ledger-Systems, mehrerer Werte, die für jedes Attribut der mehreren Attribute, einen Wert umfassen, der diesem Attribut entspricht; und
für mindestens ein Attribut der mehreren Attribute:
Prüfen, ob der kryptographische Nachweis in der Attributbestätigung, der dem mindestens einen Attribut entspricht, ein gültiger Nachweis für den empfangenen Wert ist, der dem mindestens einen Attribut entspricht;
Verifizieren auf Grundlage von Informationen, die auf den Identitätsinhaber bezogen sind, des empfangenen Werts, der dem mindestens einen Attribut entspricht; und
in Reaktion darauf, dass bestimmt wird, dass der kryptographische Nachweis ein gültiger Nachweis für den empfangenen Wert ist, der dem mindestens einen Attribut entspricht; und dass der empfange Wert, der dem mindestens einen Attribut entspricht, erfolgreich verifiziert wird:
elektronisches Signieren der Attributbestätigung, die dem mindestens einen Attribut entspricht; und
Veranlassen, über das Distributed-Ledger-System, dass sich die Attributbestätigung, die dem mindestens einen Attribut entspricht, im VERIFIED-Zustand befindet.

84. Mindestens ein computerlesbares Medium nach Anspruch 83, wobei:
das Distributed-Ledger-System eine digitale Identitätsdarstellung umfasst, die dem Identitätsinhaber zugeordnet ist, wobei die digitale Identitätsdarstellung Programmcode umfasst, der Regeln zur Bestätigung umsetzt.

85. Mindestens ein computerlesbares Medium nach Anspruch 84, wobei:
der Programmcode bei Ausführung durch mindestens einen Prozessor Zustandsinformationen für die Attributbestätigung jedes Attributs der mehreren Attribute verwaltet.

86. Mindestens ein computerlesbares Medium nach einem der Ansprüche 84 oder 85, wobei:
der Programmcode bei Ausführung durch den mindestens einen Prozessor die Attributbestätigung, die dem mindestens einen Attribut entspricht, in einem Zustand hält, der ausgewählt ist aus einer Gruppe, bestehend aus: PENDING, VERIFIED, EXPIRED und INVALID.

87. Mindestens ein computerlesbares Medium nach Anspruch 86, wobei:
der Programmcode bei Ausführung durch den mindestens einen Prozessor veranlasst, dass die Attributbestätigung, die dem mindestens einen Attribut entspricht, von einem PENDING-Zustand in den VERIFIED-Zustand nur in Reaktion auf eine Anweisung der Entität, die dafür zuständig ist, den Ausweis zu verifizieren, übergeht.

88. Mindestens ein computerlesbares Medium nach einem der Ansprüche 86 bis 87, wobei:
der Programmcode bei Ausführung durch den mindestens einen Prozessor veranlasst, dass die Attributbestätigung, die dem mindestens einen Attribut entspricht, von dem VERIFIED-Zustand in einen EXPIRED-Zustand nach Ablauf eines Zeitgebers, der gestellt wurde, als die Attributbestätigung zuletzt in den VERIFIED-Zustand übergegangen ist, übergeht.

89. Mindestens ein computerlesbares Medium nach einem der Ansprüche 86 bis 88, wobei:
der Programmcode bei Ausführung durch den mindestens einen Prozessor einen Zugang zu dem kryptographischen Nachweis in der Attributbestätigung, die dem mindestens einen Attribut entspricht, nur dann ermöglicht, wenn sich die Attributbestätigung in dem VERIFIED-Zustand befindet.

90. System umfassend:
mindestens einen Prozessor;

mindestens ein computerlesbares Medium, auf dem Anweisungen gespeichert sind, die bei Ausführung den mindestens einen Prozessor dazu programmieren:
einen Ausweis zur Verwendung beim Bestätigen einer Identität eines Identitätsinhabers zu erzeugen, wobei der mindestens eine Prozessor dazu programmiert ist, den Ausweis zumindest teilweise durch Folgendes zu erzeugen:
Identifizieren mehrerer Werte, wobei jeder Wert einem Attribut von mehreren Attributen entspricht,
Erzeugen einer Attributbestätigung für jedes Attribut der mehreren Attribute, wobei die Attributbestätigung mindestens einen kryptographischen Nachweis des Wertes umfasst, der dem Attribut der mehreren Attribute entspricht; und
Identifizieren einer Entität als dafür zuständig, den Ausweis zu verifizieren;
den Ausweis in einem Distributed-Ledger-System zu veröffentlichen, wobei:
der Ausweis die Attributbestätigung für jedes Attribut der mehreren Attribute beinhaltet;
das Distributed-Ledger-System eine digitale Identitätsdarstellung umfasst, die dem Identitätsinhaber zugeordnet ist;
die digitale Identitätsdarstellung Programmcode umfasst, der Regeln zur Bestätigung umsetzt; und
für mindestens ein Attribut der mehreren Attribute der Programmcode bei Ausführung einen Zugang zu einem kryptographischen Nachweis in der Attributbestätigung für das mindestens eine Attribut nur dann ermöglicht, wenn sich die Attributbestätigung in einem VERIFIED-Zustand befindet; und
über das Distributed-Ledger-System eine Anforderung an die Entität zu senden, die dafür zuständig ist, den Ausweis zu verifizieren; und
über einen Kanal außerhalb des Distributed-Ledger-Systems die mehreren Werte, die jeweils den mehreren Attributen entsprechen, an die zuständige Entität zu senden.

91. System nach Anspruch 90, wobei auf dem mindestens einen computerlesbaren Medium weitere Anweisungen gespeichert sind, die bei Ausführung den mindestens einen Prozessor dazu programmieren:
mehrere Messungen zu verwenden, die an dem Identitätsinhaber durchgeführt werden, um eine Kennung für den Identitätsinhaber zu erzeugen, wobei die Kennung einen kryptographischen Nachweis für die mehreren Messungen umfasst;
die digitale Identitätsdarstellung zu instanziieren, wobei die digitale Identitätsdarstellung der Kennung für den Identitätsinhaber zugeordnet ist;
eine elektronische Signatur über die digitale Identitätsdarstellung zu erzeugen; und
die digitale Identitätsdarstellung und die elektronische Signatur in dem Distributed-Ledger-System zu veröffentlichen.

92. System nach Anspruch 91, wobei
der Identitätsinhaber eine natürliche Person ist; und
die mehreren Messungen mindestens eine biometrische Messung und mindestens eine Verhaltensmessung umfassen.

93. System nach einem der Ansprüche 91 oder 92, wobei auf dem mindestens einen computerlesbaren Medium weitere Anweisungen gespeichert sind, die bei Ausführung den mindestens einen Prozessor dazu programmieren:
eine Bestätigung von dem Distributed-Ledger-System zu empfangen, dass ein Datensatz der digitalen Identitätsdarstellung erzeugt wurde.

94. System nach einem der Ansprüche 90 bis 93, wobei das Distributed-Ledger-System unter Verwendung von mindestens einer Blockchain umgesetzt wird.

95. System nach einem der Ansprüche 90 bis 94, wobei auf dem mindestens einen computerlesbaren Medium weitere Anweisungen gespeichert sind, die bei Ausführung den mindestens einen Prozessor dazu programmieren:
ein Schema aus mehreren Schemata für Ausweise auszuwählen, wobei das Schema die mehreren Attribute umfasst, wobei der Ausweis gemäß dem Schema erzeugt wird.

96. System umfassend:
mindestens einen Prozessor;
mindestens ein computerlesbares Medium, auf dem Anweisungen gespeichert sind, die bei Ausführung den mindestens einen Prozessor dazu programmieren:
über ein Distributed-Ledger-System eine Anforderung zum Verifizieren eines Ausweises zu empfangen, wobei der Ausweis mehrere Attributbestätigungen umfasst, die jeweils mehreren Attributen für einen Identitätsinha-

ber entsprechen, wobei für jedes Attribut der mehreren Attribute die entsprechende Attributbestätigung einen kryptographischen Nachweis umfasst, und wobei der Ausweis die Entität als dafür zuständig, den Ausweis zu verifizieren, identifiziert;
über einen Kanal außerhalb des Distributed-Ledger-Systems mehrere Werte zu empfangen, die für jedes Attribut der mehreren Attribute, einen Wert umfassen, der diesem Attribut entspricht; und
für mindestens ein Attribut der mehreren Attribute:
zu prüfen, ob der kryptographische Nachweis in der Attributbestätigung, der dem mindestens einen Attribut entspricht, ein gültiger Nachweis für den empfangenen Wert ist, der dem mindestens einen Attribut entspricht;
auf Grundlage von Informationen, die auf den Identitätsinhaber bezogen sind, den empfangenen Wert, der dem mindestens einen Attribut entspricht, zu verifizieren; und
in Reaktion darauf, dass bestimmt wird, dass der kryptographische Nachweis ein gültiger Nachweis für den empfangenen Wert ist, der dem mindestens einen Attribut entspricht; und dass der empfange Wert, der dem mindestens einen Attribut entspricht, erfolgreich verifiziert wird:
elektronisches Signieren der Attributbestätigung, die dem mindestens einen Attribut entspricht; und
Veranlassen, über das Distributed-Ledger-System, dass sich die Attributbestätigung, die dem mindestens einen Attribut entspricht, im VERIFIED-Zustand befindet.

97. System nach Anspruch 96, wobei das Distributed-Ledger-System eine digitale Identitätsdarstellung umfasst, die dem Identitätsinhaber zugeordnet ist, wobei die digitale Identitätsdarstellung Programmcode umfasst, der Regeln zur Bestätigung umsetzt.

98. System nach Anspruch 97, wobei der Programmcode bei Ausführung Zustandsinformationen für die Attributbestätigung jedes Attributs der mehreren Attribute verwaltet.

99. System nach einem der Ansprüche 97 oder 98, wobei:
der Programmcode bei Ausführung die Attributbestätigung, die dem mindestens einen Attribut entspricht, in einem Zustand hält, der ausgewählt ist aus einer Gruppe, bestehend aus: PENDING, VERIFIED, EXPIRED und INVALID.

100. System nach Anspruch 99, wobei der Programmcode bei Ausführung veranlasst, dass die Attributbestätigung, die dem mindestens einen Attribut entspricht, von einem PENDING-Zustand in den VERIFIED-Zustand nur in Reaktion auf eine Anweisung der Entität, die dafür zuständig ist, den Ausweis zu verifizieren, übergeht.

101. System nach einem der Ansprüche 99 bis 100, wobei:
der Programmcode bei Ausführung veranlasst, dass die Attributbestätigung, die dem mindestens einen Attribut entspricht, von dem VERIFIED-Zustand in einen EXPIRED-Zustand nach Ablauf eines Zeitgebers, der gestellt wurde, als die Attributbestätigung zuletzt in den VERIFIED-Zustand übergegangen ist, übergeht.

102. System nach einem der Ansprüche 99 bis 101, wobei:
der Programmcode bei Ausführung einen Zugang zu dem kryptographischen Nachweis in der Attributbestätigung, die dem mindestens einen Attribut entspricht, nur dann ermöglicht, wenn sich die Attributbestätigung in dem VERIFIED-Zustand befindet.

103. Computersystem, umfassend:
mindestens einen Prozessor; und
mindestens ein computerlesbares Medium, auf dem mehrere Anweisungen gespeichert sind, die bei Ausführung den mindestens einen Prozessor dazu programmieren:
einen Pointer zu verwenden, um in einem Distributed-Ledger-System auf mindestens eine Bestätigung für mindestens ein Attribut eines Identitätsinhabers zuzugreifen, wobei:
die mindestens eine Bestätigung zwischen mehreren Zuständen in dem Distributed-Ledger-System beweglich ist, wobei die mehreren Zustände einen VERIFIED-Zustand beinhalten, und
die mindestens eine Bestätigung einen kryptographischen Nachweist umfasst;
einen Wert, der dem mindestens einen Attribut entspricht, zu empfangen; und
zu bestimmen, ob sich die mindestens eine Bestätigung für das mindestens eine Attribut im VERIFIED-Zustand befindet;
zu bestimmen, ob einer Entität, die als dafür zuständig angegeben ist, die mindestens eine Bestätigung zu verifizieren, zu vertrauen ist;
zu bestimmen, ob der kryptographische Nachweis in der mindestens einen Bestätigung ein gültiger Nachweis für den empfangenen Wert ist, der dem mindestens einen Attribut entspricht;

zu bestimmen, ob die mindestens eine Bestätigung elektronisch von der Entität signiert wurde, die als dafür zuständig angegeben ist, die mindestens eine Bestätigung zu verifizieren; und
in Reaktion darauf, dass bestimmt wird, dass sich die mindestens eine Bestätigung im VERIFIED-Zustand befindet, dass der Entität, die als dafür zuständig angegeben ist, die mindestens eine Bestätigung zu verifizieren, zu vertrauen ist, dass der kryptographische Nachweis ein gültiger Nachweis für den empfangenen Wert ist, und dass die mindestens eine Bestätigung elektronisch von der Entität signiert wurde, die dafür zuständig ist, die mindestens eine Bestätigung zu verifizieren:
zu einer Transaktion mit dem Identitätsinhaber übergehen.

104. Computersystem nach Anspruch 103, wobei:
das Distributed-Ledger-System unter Verwendung von mindestens einer Blockchain umgesetzt wird.

105. Computersystem nach einem der Ansprüche 103 oder 104, wobei:
die mindestens eine Bestätigung in einem Ausweis gespeichert ist, die dem Identitätsinhaber zugeordnet ist, und wobei der Pointer einen Verweis auf den Ausweis beinhaltet.

106. Computersystem nach Anspruch 105, wobei:
der Ausweis gemäß einem Schema erzeugt wird, das aus mehreren Schemata für Ausweise ausgewählt ist, wobei das Schema mehrere Attribute umfasst, wobei die mehreren Attribute das mindestens eine Attribut umfassen.

107. Computersystem nach einem der Ansprüche 103 bis 106, wobei:
die mehreren Zustände der mindestens einen Bestätigung einen PENDING-Zustand beinhalten; und
die mehreren Anweisungen bei Ausführung den mindestens einen Prozessor ferner veranlassen, zu veranlassen, dass die mindestens eine Bestätigung von dem PENDING-Zustand in den VERIFIED-Zustand übergeht, wenn der Wert, der dem mindestens einen Attribut entspricht, von der Entität verifiziert wurde, die als dafür zuständig angegeben ist, die mindestens eine Bestätigung zu verifizieren.

108. Computersystem nach einem der Ansprüche 103 bis 107, wobei:
die mehreren Zustände der mindestens einen Bestätigung einen EXPIRED-Zustand beinhalten; und
die mehreren Anweisungen bei Ausführung den mindestens einen Prozessor ferner veranlassen, zu veranlassen, dass die mindestens eine Bestätigung von dem VERIFIED-Zustand in den EXPIRED-Zustand nach Ablauf eines Zeitgebers, der gestellt wurde, als der Wert, der dem mindestens einen Attribut entspricht, zuletzt verifiziert wurde, übergeht.

109. Computersystem nach einem der Ansprüche 103 bis 108, wobei:
ein Zugang zu dem kryptographischen Nachweis in der mindestens einen Bestätigung nur dann ermöglicht wird, wenn sich die mindestens eine Bestätigung in dem VERIFIED-Zustand befindet.

110. Computersystem nach einem der Ansprüche 103 bis 109, wobei der Identitätsinhaber ein Benutzer ist.

111. Computersystem nach einem der Ansprüche 103 bis 110, wobei:
auf die mindestens eine Bestätigung aus einer digitalen Identitätsdarstellung zugegriffen wird, die in dem Distributed Ledger gespeichert ist; und
die digitale Identitätsdarstellung dem Identitätsinhaber zugeordnet ist und Programmcode beinhaltet, der Regeln zur Bestätigung umsetzt.

112. Computersystem nach einem der Ansprüche 103 bis 111, wobei:
der Wert, der dem mindestens einen Attribut entspricht, über einen Kanal außerhalb des Distributed Ledger empfangen wird.

113. Computerlesbares Medium, auf dem weitere Anweisungen gespeichert sind, die bei Ausführung durch mindestens einen Prozessor den mindestens einen Prozessor dazu programmieren, folgende Schritte auszuführen:
Verwenden eines Pointers, um in einem Distributed-Ledger-System auf mindestens eine Bestätigung für mindestens ein Attribut eines Identitätsinhabers zuzugreifen, wobei:
die mindestens eine Bestätigung zwischen mehreren Zuständen in dem Distributed-Ledger-System beweglich ist, wobei die mehreren Zustände einen VERIFIED-Zustand beinhalten, und
die mindestens eine Bestätigung einen kryptographischen Nachweist umfasst;
Empfangen eines Wertes, der dem mindestens einen Attribut entspricht; und

Bestimmen, ob sich die mindestens eine Bestätigung für das mindestens eine Attribut im VERIFIED-Zustand befindet;
Bestimmen, ob einer Entität, die als dafür zuständig angegeben ist, die mindestens eine Bestätigung zu verifizieren, zu vertrauen ist;
Bestimmen, ob der kryptographische Nachweis in der mindestens einen Bestätigung ein gültiger Nachweis für den empfangenen Wert ist, der dem mindestens einen Attribut entspricht;
Bestimmen, ob die mindestens eine Bestätigung elektronisch von der Entität signiert wurde, die als dafür zuständig angegeben ist, die mindestens eine Bestätigung zu verifizieren; und
in Reaktion darauf, dass bestimmt wird, dass sich die mindestens eine Bestätigung im VERIFIED-Zustand befindet, dass der Entität, die als dafür zuständig angegeben ist, die mindestens eine Bestätigung zu verifizieren, zu vertrauen ist, dass der kryptographische Nachweis ein gültiger Nachweis für den empfangenen Wert ist, und dass die mindestens eine Bestätigung elektronisch von der Entität signiert wurde, die dafür zuständig ist, die mindestens eine Bestätigung zu verifizieren:
Übergehen zu einer Transaktion mit dem Identitätsinhaber.

114. Computerlesbares Medium nach Anspruch 113, wobei:
das Distributed-Ledger-System unter Verwendung von mindestens einer Blockchain umgesetzt wird.

115. Computerlesbares Medium nach einem der Ansprüche 113 oder 114, wobei:
die mindestens eine Bestätigung in einem Ausweis gespeichert ist, der dem Identitätsinhaber zugeordnet ist; und
der Pointer einen Verweis auf den Ausweis beinhaltet.

116. Computerlesbares Medium nach Anspruch 115, wobei:
der Ausweis gemäß einem Schema erzeugt wird, das aus mehreren Schemata für Ausweise ausgewählt ist, wobei das Schema mehrere Attribute umfasst, wobei die mehreren Attribute das mindestens eine Attribut umfassen.

117. Computerlesbares Medium nach einem der Ansprüche 113 bis 116, wobei:
die mehreren Zustände der mindestens einen Bestätigung einen PENDING-Zustand beinhalten; und
auf dem computerlesbaren Medium weitere Anweisungen gespeichert sind, die bei Ausführung den mindestens einen Prozessor dazu programmieren, einen Schritt auszuführen zum Veranlassen, dass die mindestens eine Bestätigung von dem PENDING-Zustand in den VERIFIED-Zustand übergeht, wenn der Wert, der dem mindestens einen Attribut entspricht, von der Entität verifiziert wurde, die als dafür zuständig angegeben ist, die mindestens eine Bestätigung zu verifizieren.

118. Computerlesbares Medium nach einem der Ansprüche 113 bis 117, wobei:
die mehreren Zustände der mindestens einen Bestätigung einen EXPIRED-Zustand beinhalten; und
auf dem computerlesbaren Medium weitere Anweisungen gespeichert sind, die bei Ausführung den mindestens einen Prozessor dazu programmieren, einen Schritt auszuführen zum Veranlassen, dass die mindestens eine Bestätigung von dem VERIFIED-Zustand in den EXPIRED-Zustand nach Ablauf eines Zeitgebers, der gestellt wurde, als der Wert, der dem mindestens einen Attribut entspricht, zuletzt verifiziert wurde, übergeht.

119. Computerlesbares Medium nach einem der Ansprüche 113 bis 118, wobei:
ein Zugang zu dem kryptographischen Nachweis in der mindestens einen Bestätigung nur dann ermöglicht wird, wenn sich die mindestens eine Bestätigung in dem VERIFIED-Zustand befindet.

120. Computerlesbares Medium nach einem der Ansprüche 113 bis 119, wobei der Identitätsinhaber ein Benutzer ist.

121. Computerlesbares Medium nach einem der Ansprüche 113 bis 120, wobei:
auf die mindestens eine Bestätigung aus einer digitalen Identitätsdarstellung zugegriffen wird;, die in dem Distributed Ledger gespeichert ist; und
die digitale Identitätsdarstellung dem Identitätsinhaber zugeordnet ist und Programmcode beinhaltet, der Regeln zur Bestätigung umsetzt.

122. Computerlesbares Medium nach einem der Ansprüche 113 bis 121, wobei:
der Wert, der dem mindestens einen Attribut entspricht, über einen Kanal außerhalb des Distributed Ledgers empfangen wird.

123. System, umfassend:
mehrere Entitäten, die ein Netzwerk bilden, wobei mindestens eine erste Entität der mehreren Entitäten Folgendes umfasst:
○ mindestens ein Speichermedium, auf dem Folgendes gespeichert ist;
• eine lokale Kopie einer verteilten Datenstruktur, die unter den mehreren Entitäten repliziert ist, wobei die lokale Kopie der verteilten Datenstruktur eine personenbezogene Identitätsdarstellung umfasst, auf der Folgendes gespeichert ist:
• Daten, die durch eine kryptographische Einwegfunktion erzeugt werden, die auf mindestens einen Teil von Benutzerdaten von mindestens einer zweiten Entität der mehreren Entitäten angewandt wird und
• eine Kennung, die der mindestens einen zweiten Entität der mehreren Entitäten zugeordnet ist;
• mindestens eine Benutzerdatenstruktur, die Benutzerdaten speichert, wobei die Benutzerdatenstruktur mindestens Folgendes umfasst:
• einen oder mehrere Attributwerte; und
• die Kennung, die der mindestens einen zweiten Entität zugeordnet ist;
wobei die Daten, die in der personenbezogenen Identitätsdarstellung in der verteilten Datenstruktur gespeichert sind, einen Nachweiswert umfassen, der dem einen oder den mehreren Attributwerten entspricht, wobei der Nachweiswert durch die kryptographische Einwegfunktion erzeugt wird, die auf mindestens den einen oder die mehreren Attributwerte angewandt wird
○ mindestens zwei Kommunikationsschnittstellen zum Kommunizieren mit der mindestens einen zweiten Entität, umfassend eine erste Kommunikationsschnittstelle, um innerhalb einer Datenschutzschicht zu kommunizieren, um das eine oder die mehreren Attribute über verschlüsselte Kommunikation auszutauschen, und eine zweite Kommunikationsschnittstelle, um innerhalb einer Vertrauensschicht zu kommunizieren, um den Nachweiswert auszutauschen;
○ mindestens einen Prozessor, der ausgelegt ist zum:
• Empfangen eines Verweises auf die personenbezogene Identitätsdarstellung in der verteilten Datenstruktur zusammen mit dem einen oder den mehreren Attributwerten von der mindestens einen zweiten Entität über die erste Kommunikationsschnittstelle zum Kommunizieren innerhalb der Datenschutzschicht;
• Verifizieren von mindestens dem einen oder den mehreren Attributwerten der zweiten Entität;
• auf Grundlage des Ergebnisses der Verifizierung Ändern eines Status des Nachweiswertes in der verteilten Datenstruktur;
• Verteilen der personenbezogenen Identitätsdarstellung auf die mehreren Entitäten.

124. System nach Anspruch 123, wobei die verteilte Datenstruktur, insbesondere ein Distributed Ledger, eine Blockchain ist.

125. System nach Anspruch 123 oder 124, wobei der Status ausgewählt wird aus der Gruppe VALID, PENDING, EXPIRED und VERIFIED.

126. System nach einem der Ansprüche 123 bis 125, wobei die kryptographische Einwegfunktion eine Hash-Funktion ist.

127. System nach einem der Ansprüche 123 bis 126, wobei das System ferner mindestens eine dritte Entität in dem Netzwerk umfasst, wobei die dritte Entität Folgendes umfasst:
○ mindestens ein Speichermedium, auf dem eine lokale Kopie der verteilten Datenstruktur gespeichert ist;
○ mindestens eine Kommunikationsschnittstelle zum Kommunizieren mit den mehreren Entitäten in dem Netzwerk;
○ einen Prozessor, der ausgelegt ist zum:
• Empfangen von Daten von der zweiten Entität, wobei die Daten die Kennung, die der mindestens einen zweiten Entität zugeordnet ist, und einen oder mehrere Attributwerte umfassen;
• Erzeugen eines Validierungswerts des empfangenen einen oder der mehreren Attributwerte durch Anwenden einer kryptographischen Einwegfunktion auf den empfangenen einen oder die mehreren Attributwerte;
• Identifizieren von Nachweisdaten, die in der lokalen Kopie der verteilten Datenstruktur gespeichert sind, unter Verwendung der Kennung, die der mindestens einen zweiten Entität zugeordnet ist;
• Bestimmen, ob sich die identifizierten Nachweisdaten in einem verifizierten Zustand befinden;
• Vergleichen des Validierungswerts mit den identifizierten Nachweisdaten, um zu bestimmen, ob die empfangenen Daten von der zweiten Entität verifiziert wurden.

128. Computerlesbares Medium, auf dem Anweisungen gespeichert sind, die bei Ausführung durch mindestens einen Prozessor den mindestens einen Prozessor veranlassen, folgende Schritte auszuführen:

○ Instanziieren durch mindestens eine zweite Entität von mindestens einer Benutzerdatenstruktur mehrerer Entitäten, die ein Netzwerk bilden;
○ durch die mindestens eine zweite Entität Erzeugen einer personenbezogenen Darstellung in einer verteilten Datenstruktur, wobei:
• die personenbezogene Identitätsdarstellung kryptografische Nachweise personenbezogener Daten in einem oder mehreren Ausweisen beinhaltet, die eine oder mehrere Attributbestätigungen umfassen,
• sich eine Attributbestätigung in einem von mehreren Zuständen befinden kann,
• die personenbezogene Identitätsdarstellung eine Aktions- und Ereignisspezifikation umfasst, die Aktionen spezifiziert, die über die personenbezogene Identitätsdarstellung ausgeführt werden können und/oder Ereignisse, die durch Veränderungen der personenbezogenen Identitätsdarstellung ausgelöst werden können, und
• die personenbezogene Identitätsdarstellung durch Anwenden einer kryptographischen Einwegfunktion auf mindestens einen Teil der Benutzerdatenstruktur von mindestens einer der mehreren Entitäten bereitgestellt wird;
○ Verteilen der personenbezogenen Identitätsdarstellung auf mindestens eine Untergruppe der mehreren Entitäten;
○ Signieren der mindestens einen verteilten personenbezogenen Identitätsdarstellung durch eine mindestens erste Entität, die die Richtigkeit der personenbezogenen Daten verifiziert und Veranlassen, dass sich die Attributbestätigung in einem VERIFIED-Zustand befindet, wobei die erste Entität einer dritten Entität als vertrauenswürdig bekannt ist und wobei ein Ausweis der Benutzerdatenstruktur einen Verweis auf die erste Entität umfasst und nur die erste Entität eine Zustandsänderung einer Attributbestätigung im Ausweis veranlassen darf,
○ Erneutes Verteilen der personenbezogenen Identitätsdarstellung auf die mehreren Entitäten, wenn eine Veränderung ihres Zustands der personenbezogenen Identitätsdarstellung eintritt.

129. Computerlesbares Medium nach Anspruch 128, wobei der Zustand der mindestens einen personenbezogenen Identitätsdarstellung einer der Folgenden ist: „PENDING“, „VERIFIED“, „EXPIRED“, „INVALID“.

130. Computerlesbares Medium nach einem der Ansprüche 128 bis 129, wobei der Zustand der modifizierten oder erzeugten personenbezogenen Identitätsdarstellung vor der Verifizierung „PENDING“ ist und der Zustand auf „VERIFIED“ nach einer erfolgreichen Verifizierung durch die vertrauenswürdige erste Entität geändert wird.

131. Computerlesbares Medium nach einem der Ansprüche 128 bis 130, wobei die verteilte Datenstruktur, insbesondere ein Distributed Ledger, als eine Blockchain konfiguriert ist.

Es folgen 10 Seiten Zeichnungen

Anhängende Zeichnungen

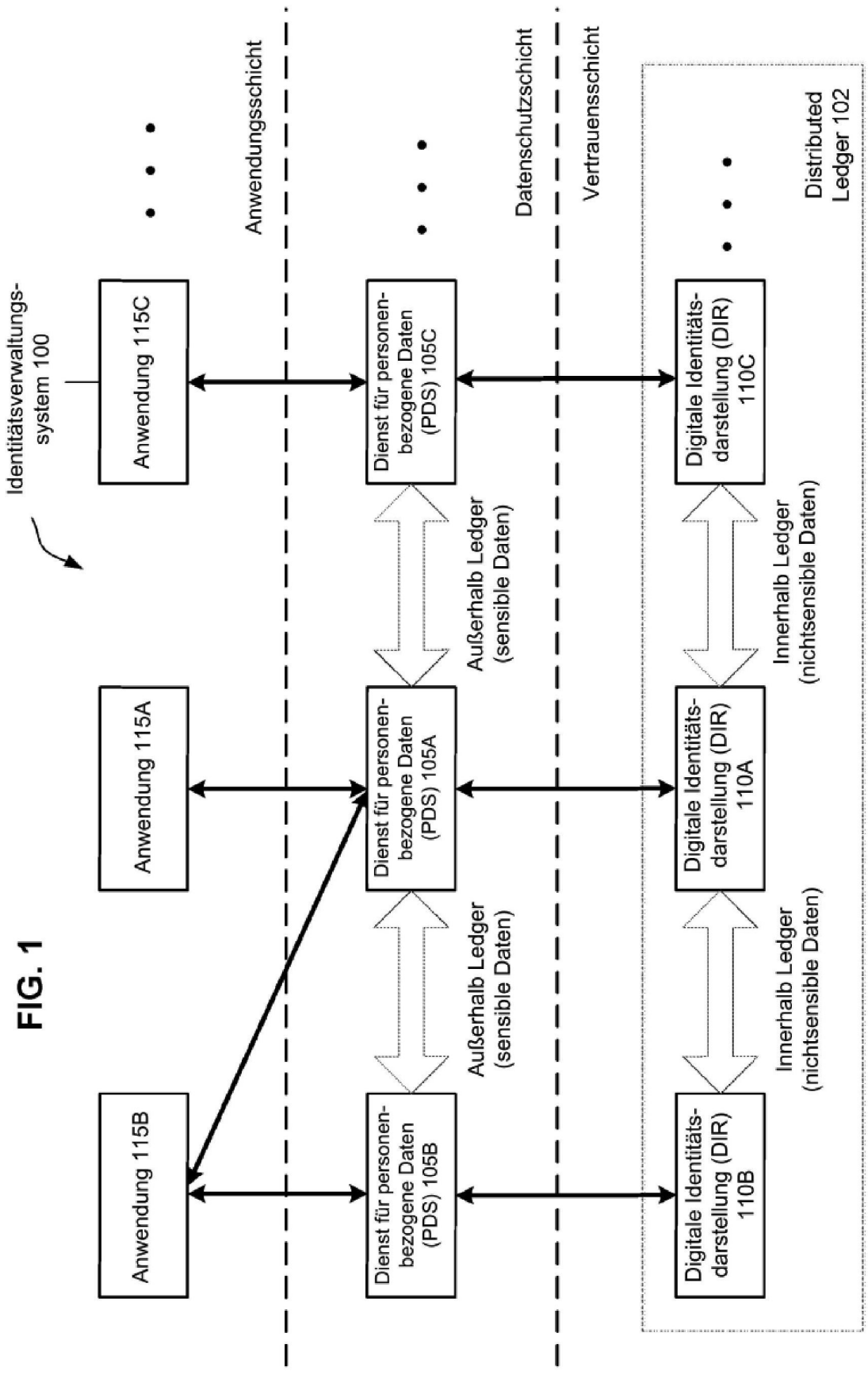


FIG. 1

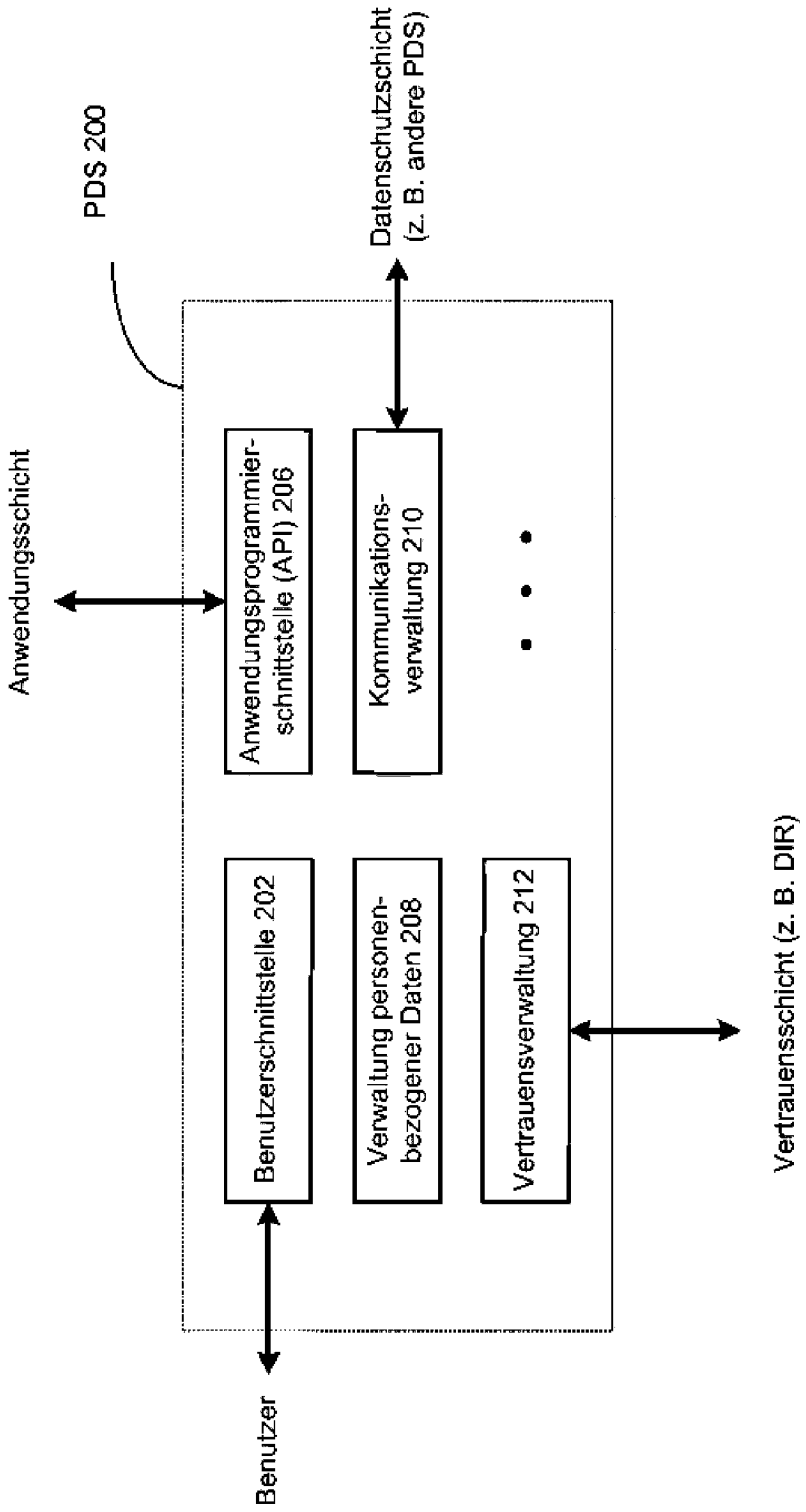

PDS 200
Datenschutzschicht (z. B. andere PDS)
Anwendungsschicht
Anwendungsprogrammier-schnittstelle (API) 206
Kommunikations-verwaltung 210
Benutzerschnittstelle 202
Verwaltung personen-bezogener Daten 208
Vertrauensverwaltung 212
Vertrauensschicht (z. B. DIR)
Benutzer

FIG. 2

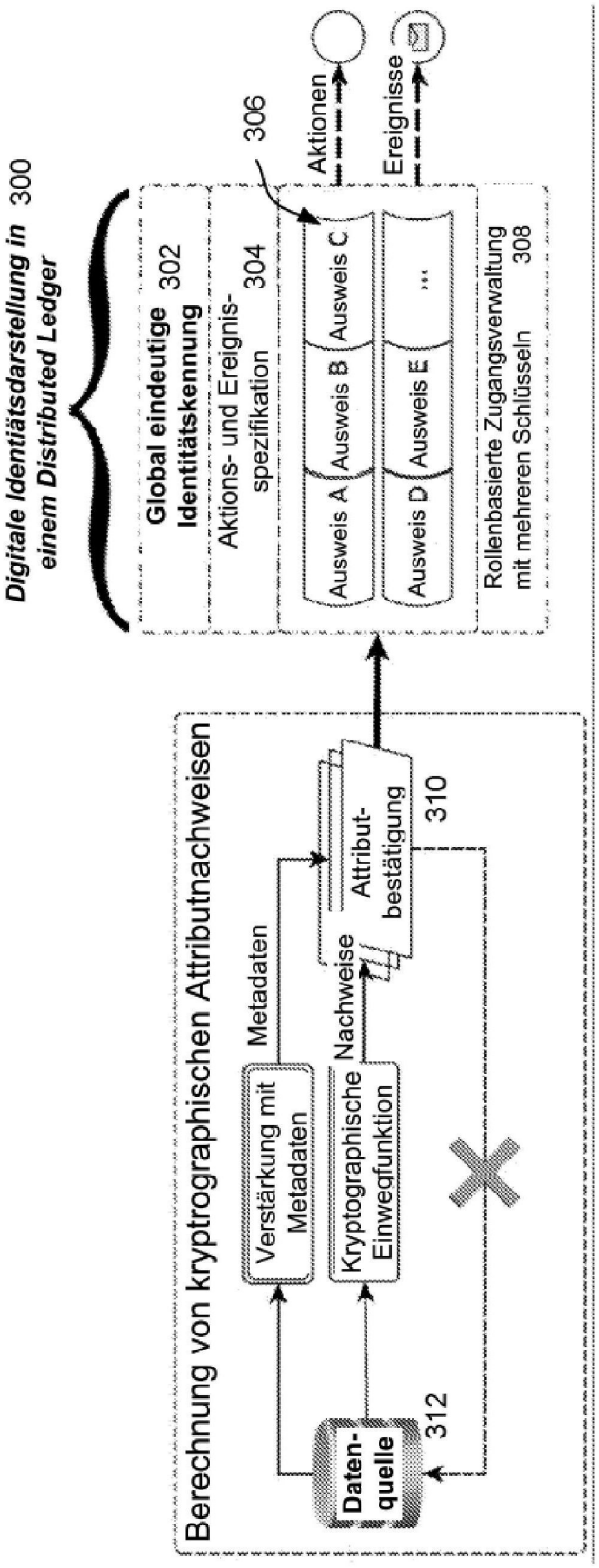

Digitale Identitätsdarstellung in einem Distributed Ledger
300
Global eindeutige Identitätskennung
302
Aktions- und Ereignis-spezifikation
304
306
Aktionen
Ereignisse
Ausweis A
Ausweis B
Ausweis C
Ausweis D
Ausweis E
...
Rollenbasierte Zugangsverwaltung mit mehreren Schlüsseln
308
Berechnung von kryptrographischen Attributnachweisen
Verstärkung mit Metadaten
Metadaten
Kryptographische Einwegfunktion
Nachweise
Attribut-bestätigung
310
Daten-quelle
312

FIG. 3

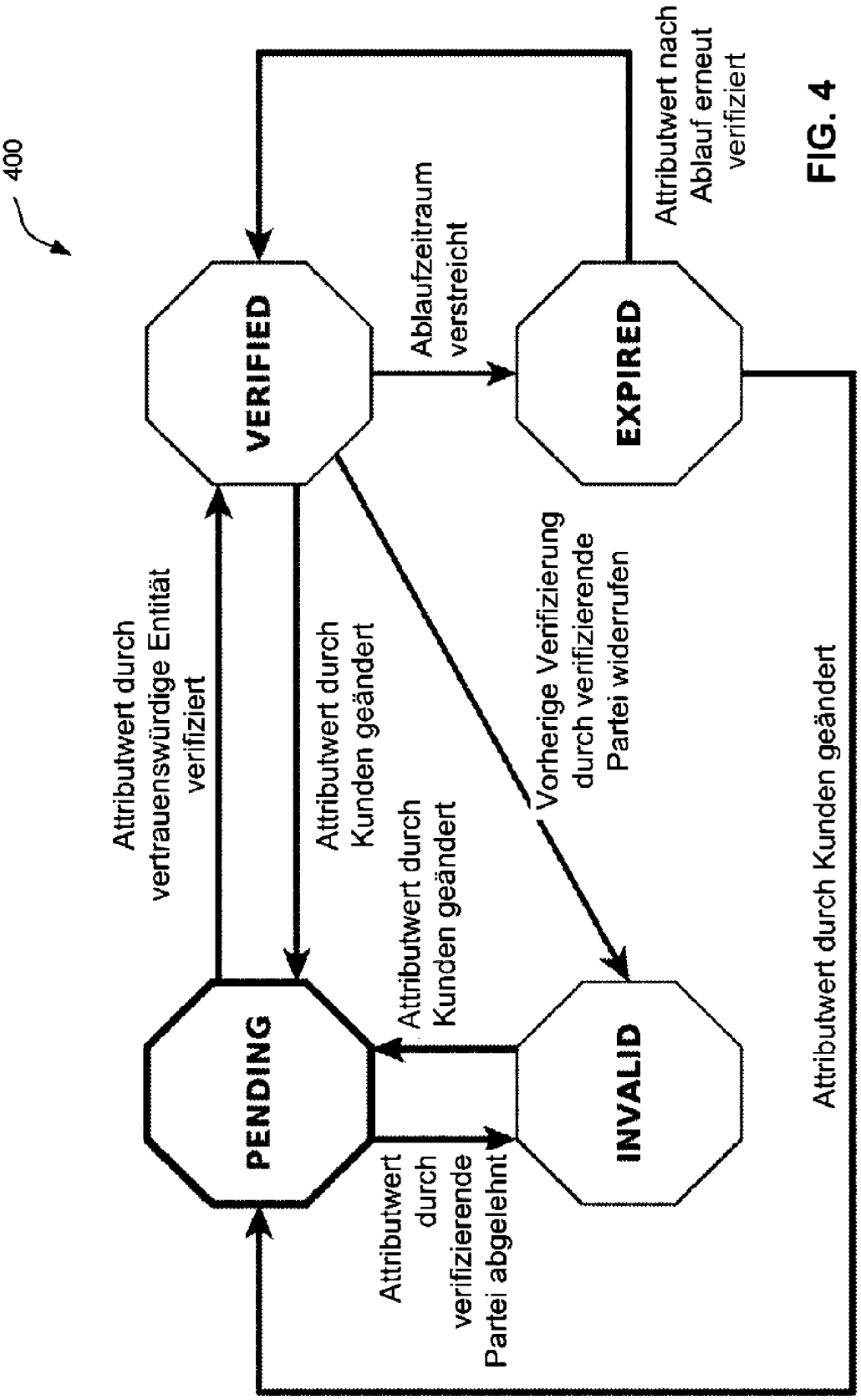

400
VERIFIED
EXPIRED
PENDING
INVALID
Ablaufzeitraum verstreicht
Attributwert nach Ablauf erneut verifiziert
Attributwert durch vertrauenswürdige Entität verifiziert
Attributwert durch Kunden geändert
Attributwert durch Kunden geändert
Vorherige Verifizierung durch verifizierende Partei widerrufen
Attributwert durch verifizierende Partei abgelehnt
Attributwert durch Kunden geändert

FIG. 4

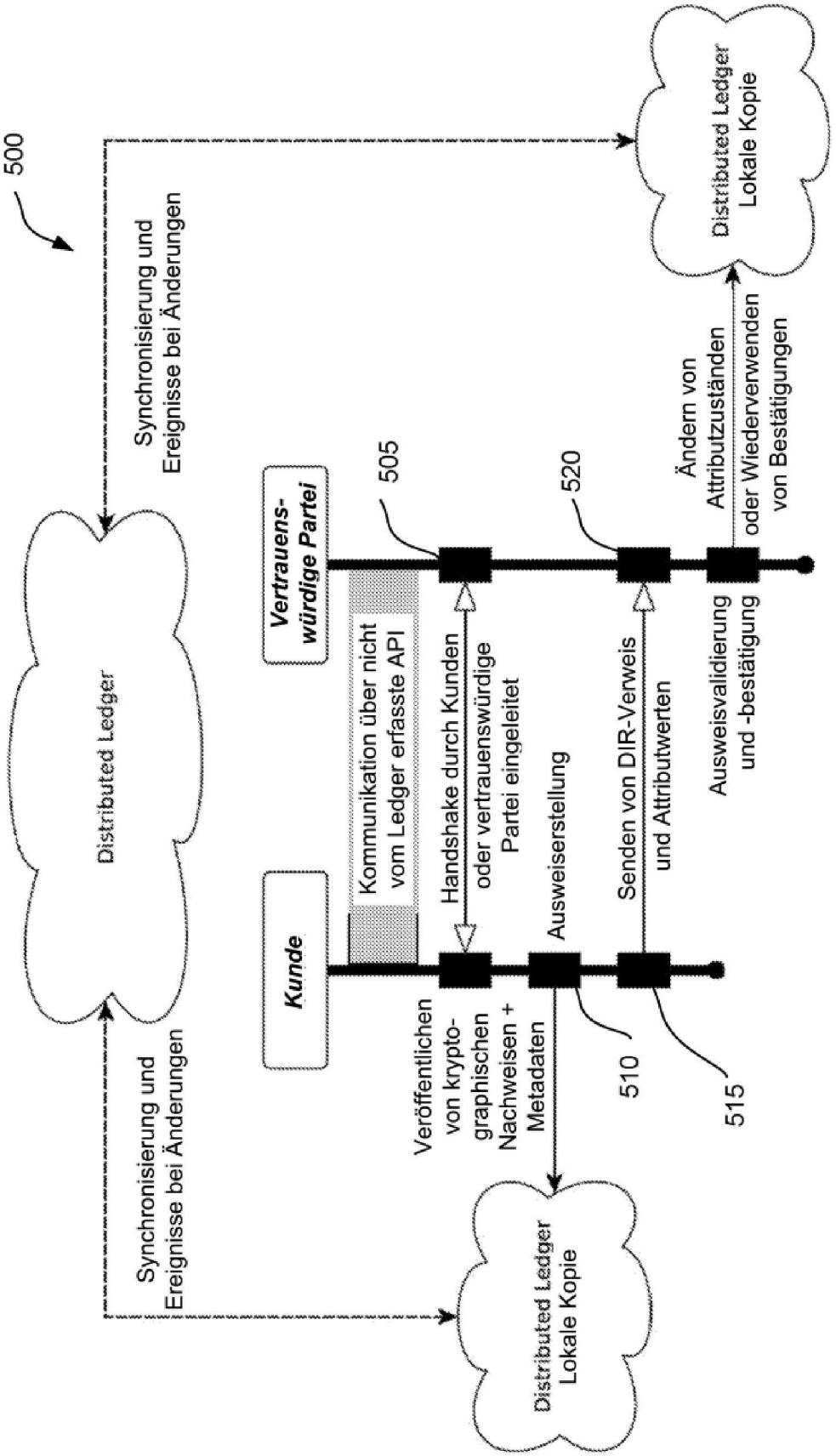

500
Distributed Ledger
Lokale Kopie
Synchronisierung und
Ereignisse bei Änderungen
Distributed Ledger
Synchronisierung und
Ereignisse bei Änderungen
Vertrauens-
würdige Partei
505
520
Ändern von
Attributzuständen
oder Wiederverwenden
von Bestätigungen
Kommunikation über nicht
vom Ledger erfasste API
Handshake durch Kunden
oder vertrauenswürdige
Partei eingeleitet
Ausweisvalidierung
und -bestätigung
Kunde
Ausweiserstellung
Senden von DIR-Verweis
und Attributwerten
Veröffentlichen
von krypto-
graphischen
Nachweisen +
Metadaten
510
515
Distributed Ledger
Lokale Kopie

FIG. 5

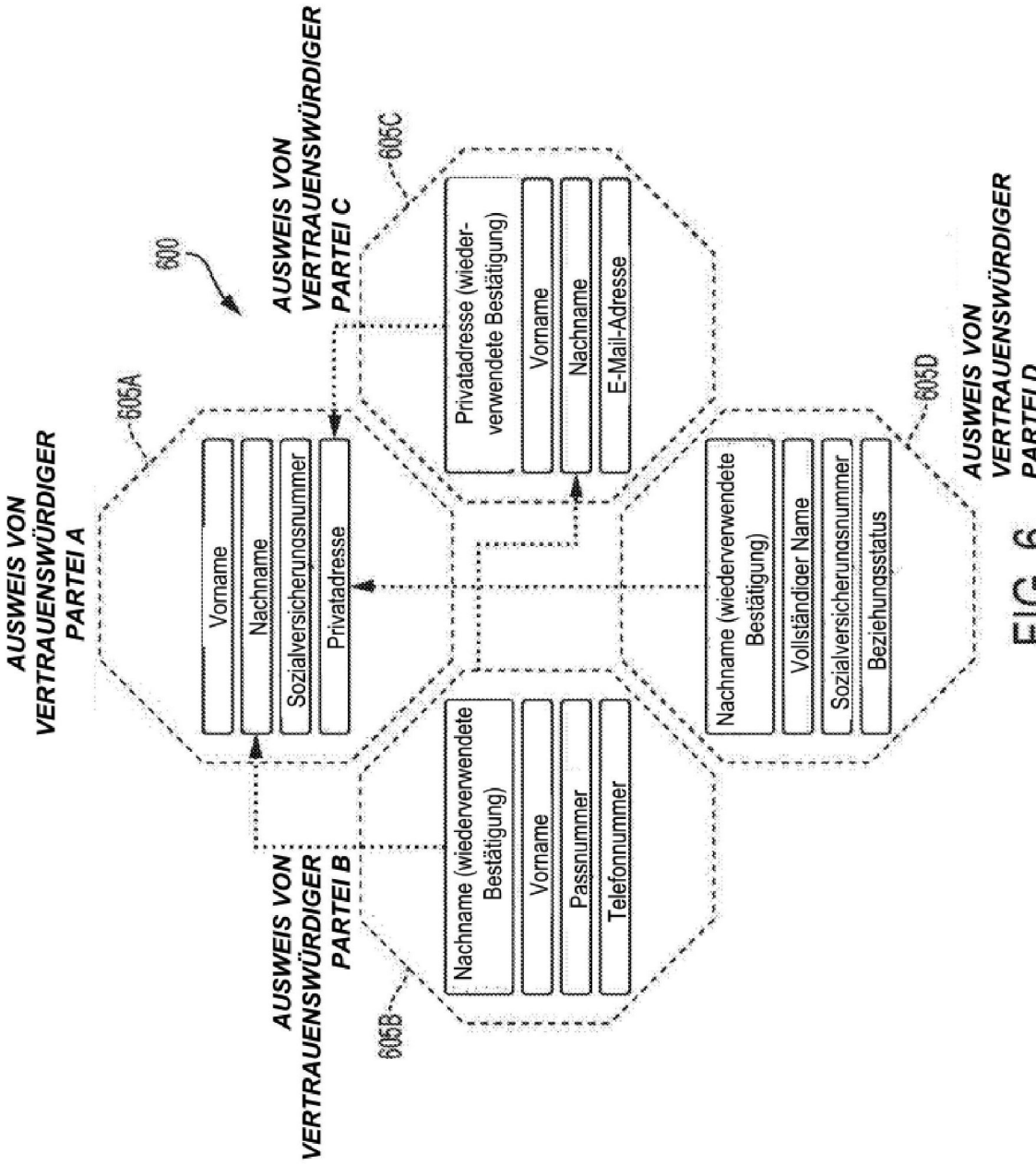

600
AUSWEIS VON VERTRAUENSWÜRDIGER PARTEI A
605A
Vorname
Nachname
Sozialversicherungsnummer
Privatadresse
AUSWEIS VON VERTRAUENSWÜRDIGER PARTEI C
605C
Privatadresse (wieder-verwendete Bestätigung)
Vorname
Nachname
E-Mail-Adresse
AUSWEIS VON VERTRAUENSWÜRDIGER PARTEI B
605B
Nachname (wiederverwendete Bestätigung)
Vorname
Passnummer
Telefonnummer
AUSWEIS VON VERTRAUENSWÜRDIGER PARTEI D
605D
Nachname (wiederverwendete Bestätigung)
Vollständiger Name
Sozialversicherungsnummer
Beziehungsstatus

FIG. 6

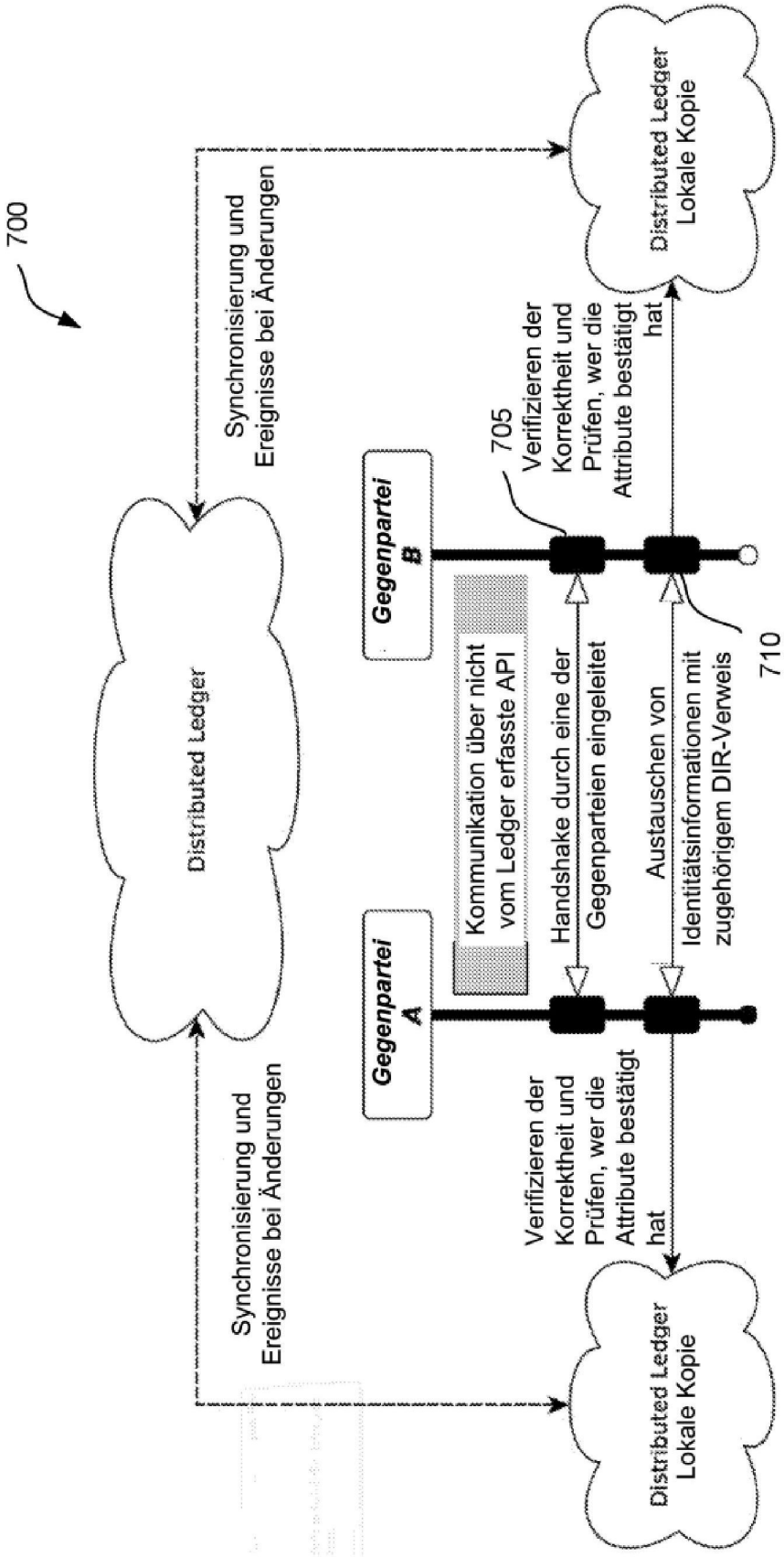

700
Distributed Ledger
Synchronisierung und Ereignisse bei Änderungen
Synchronisierung und Ereignisse bei Änderungen
Distributed Ledger Lokale Kopie
Distributed Ledger Lokale Kopie
Gegenpartei A
Gegenpartei B
Kommunikation über nicht vom Ledger erfasste API
Handshake durch eine der Gegenparteien eingeleitet
Austauschen von Identitätsinformationen mit zugehörigem DIR-Verweis
705
Verifizieren der Korrektheit und Prüfen, wer die Attribute bestätigt hat
Verifizieren der Korrektheit und Prüfen, wer die Attribute bestätigt hat
710

FIG. 7

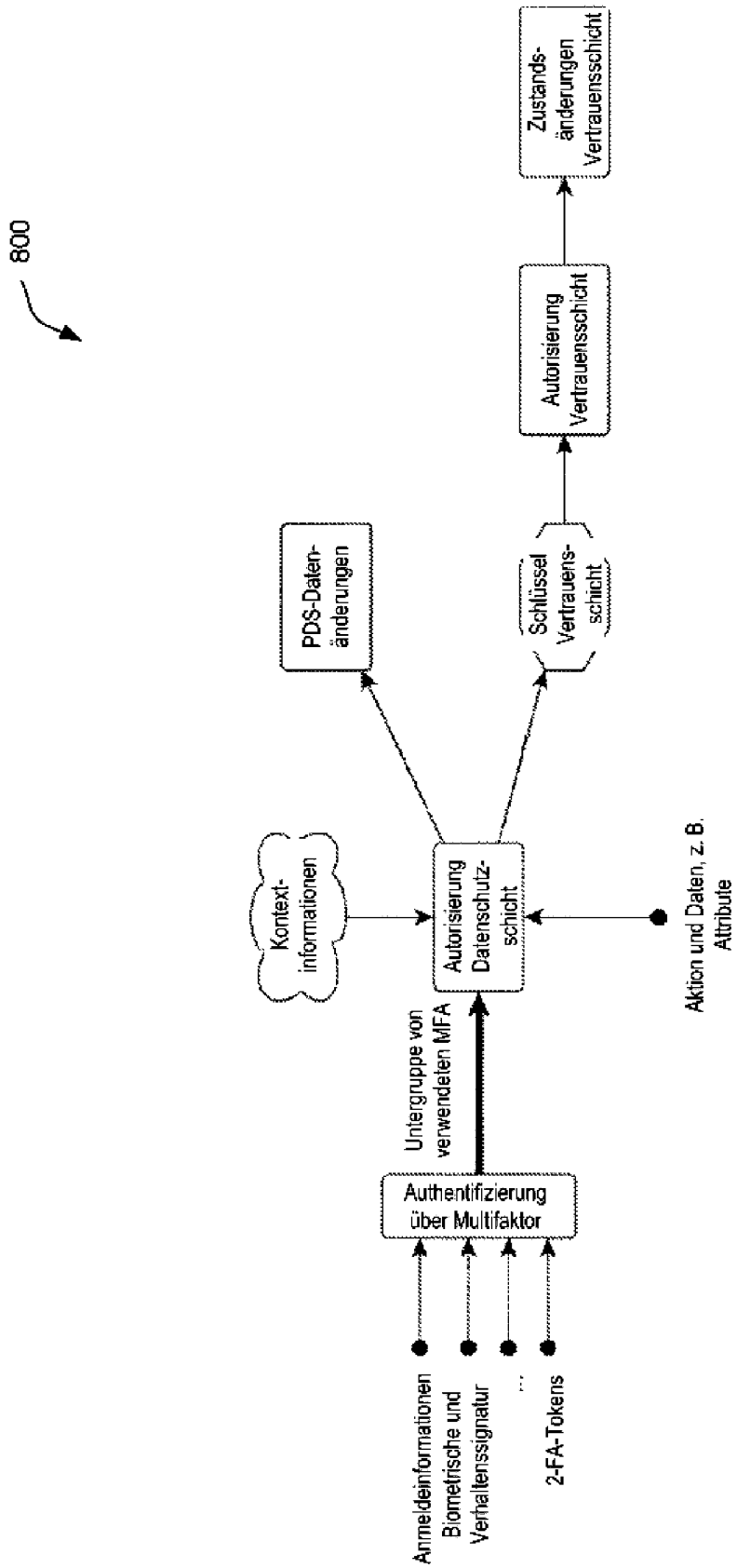

800
Zustands-
änderungen
Vertrauensschicht
Autorisierung
Vertrauensschicht
Schlüssel
Vertrauens-
schicht
PDS-Daten-
änderungen
Kontext-
informationen
Autorisierung
Datenschutz-
schicht
Aktion und Daten, z. B.
Attribute
Untergruppe von
verwendeten MFA
Authentifizierung
über Multifaktor
Anmeldeinformationen
Biometrische und
Verhaltenssignatur
...
2-FA-Tokens

FIG. 8

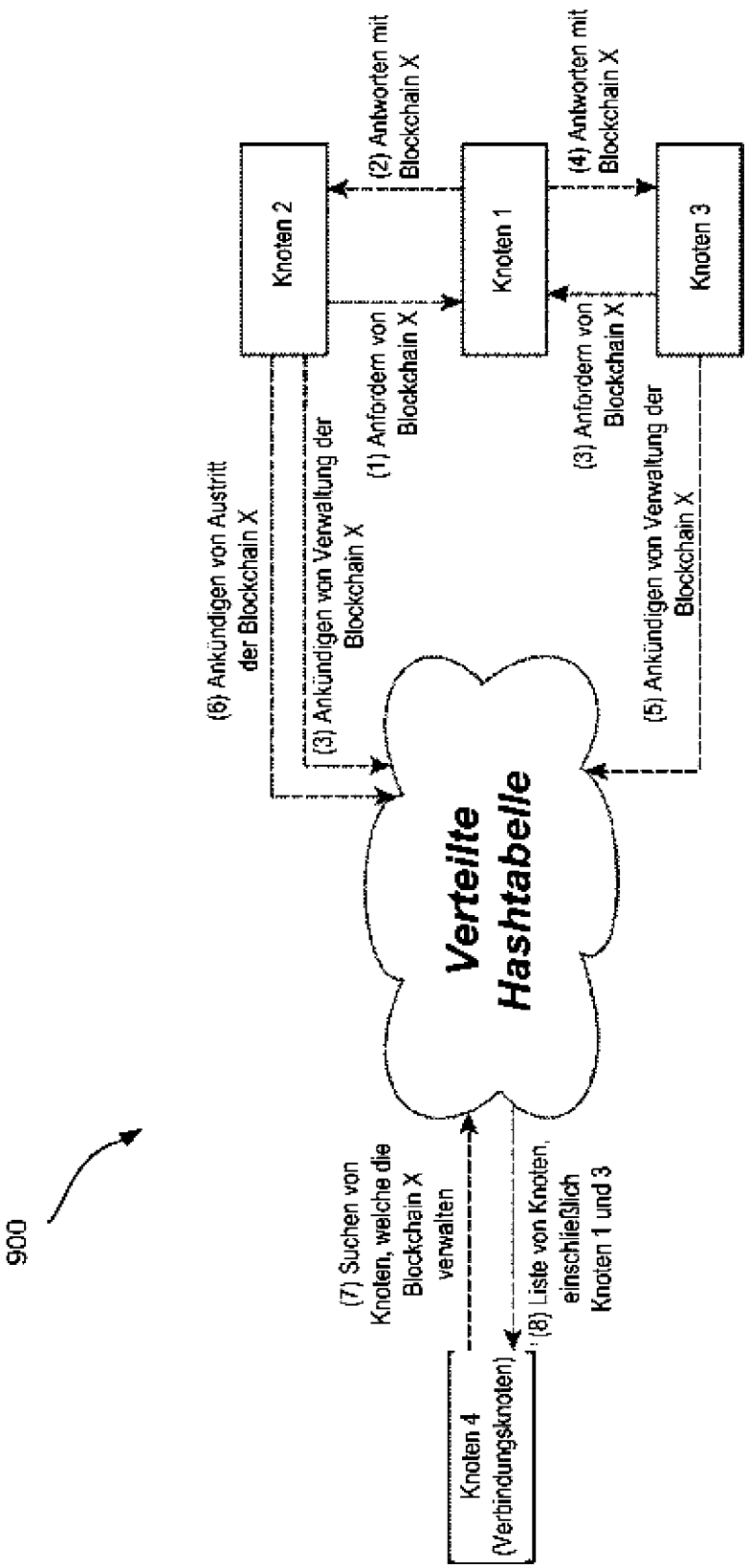

900
Knoten 2
Knoten 1
Knoten 3
Knoten 4
(Verbindungsknoten)
Verteilte Hashtabelle
(1) Anfordern von Blockchain X
(2) Antworten mit Blockchain X
(3) Anfordern von Blockchain X
(4) Antworten mit Blockchain X
(3) Ankündigen von Verwaltung der Blockchain X
(5) Ankündigen von Verwaltung der Blockchain X
(6) Ankündigen von Austritt der Blockchain X
(7) Suchen von Knoten, welche die Blockchain X verwalten
(8) Liste von Knoten, einschließlich Knoten 1 und 3

FIG. 9

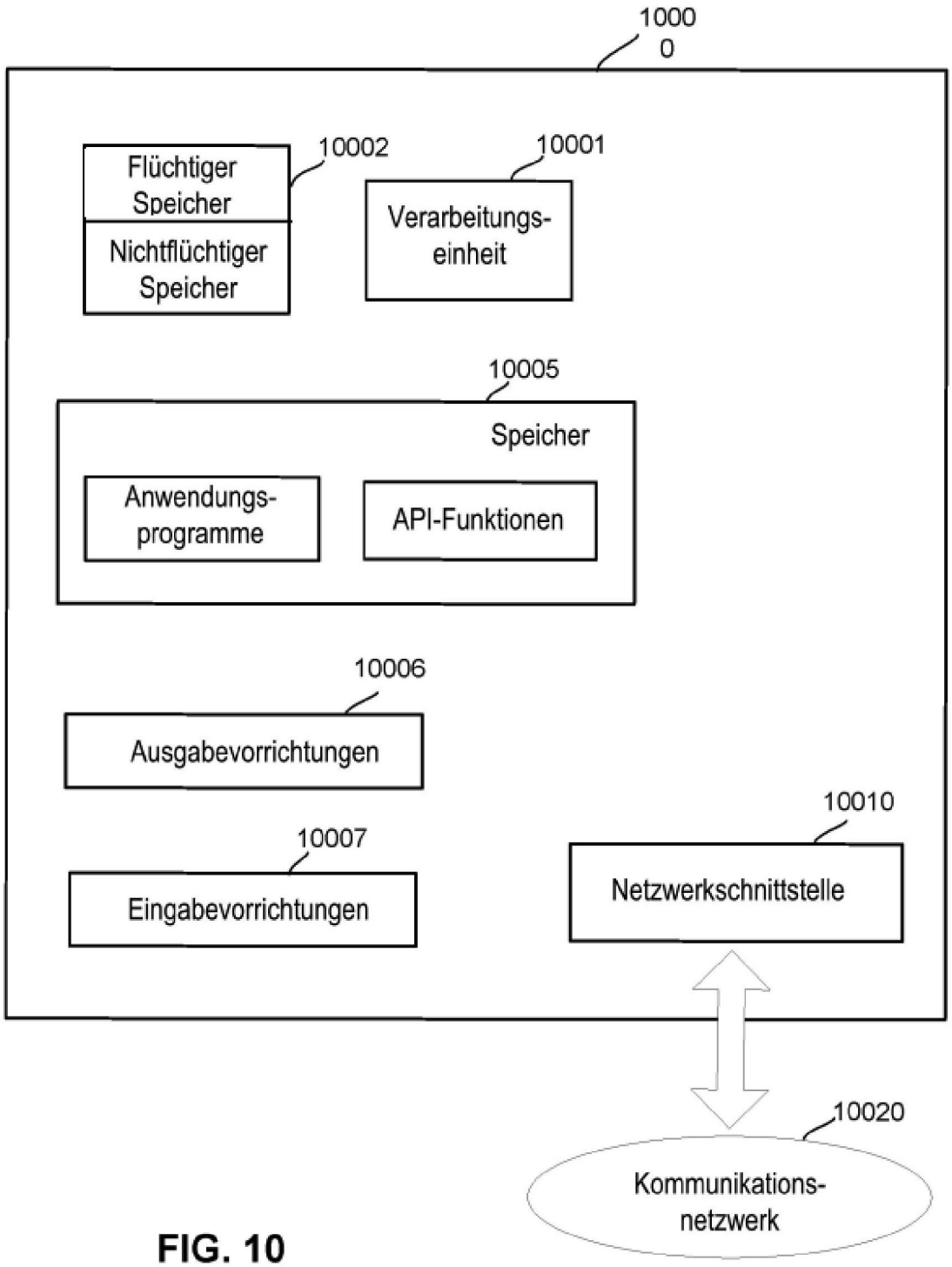

10000
Flüchtiger Speicher
10002
Nichtflüchtiger Speicher
Verarbeitungs-einheit
10001
10005
Speicher
Anwendungs-programme
API-Funktionen
10006
Ausgabevorrichtungen
10007
Eingabevorrichtungen
10010
Netzwerkschnittstelle
10020
Kommunikations-netzwerk

FIG. 10