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

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
04. April 2019 (04.04.2019)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2019/063256 A1

(51) Internationale Patentklassifikation:
H04L 9/32 (2006.01) *H04W 12/06* (2009.01)
G06K 9/00 (2006.01) *G06Q 20/36* (2012.01)
G06Q 20/22 (2012.01) *G06Q 20/40* (2012.01)
H04L 29/08 (2006.01) *H04L 9/08* (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2018/073966

(22) Internationales Anmeldedatum:
06. September 2018 (06.09.2018)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2017 122 227.8
26. September 2017 (26.09.2017) DE

(71) Anmelder: **INNOGY INNOVATION GMBH** [—/DE]; Lysegang 11, 45139 Essen (DE).

(72) Erfinder: **STÖCKER, Carsten**; Verdistraße 5, 40724 Hilden (DE). **KEMMANN, Harald**; Im Spring 13, 42555 Velbert (DE).

(74) Anwalt: **COHAUSZ & FLORACK PATENT- UND RECHTSANWÄLTE PARTNERSCHAFTSGESELLSCHAFT MBB**; Hendrik Bücker, Bleichstraße 14, 40211 Düsseldorf (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD,

(54) **Title:** SYSTEM, IN PARTICULAR AUTHENTICITY SYSTEM

(54) **Bezeichnung:** SYSTEM, INSBESONDERE AUTHENTIZITÄTSSYSTEM

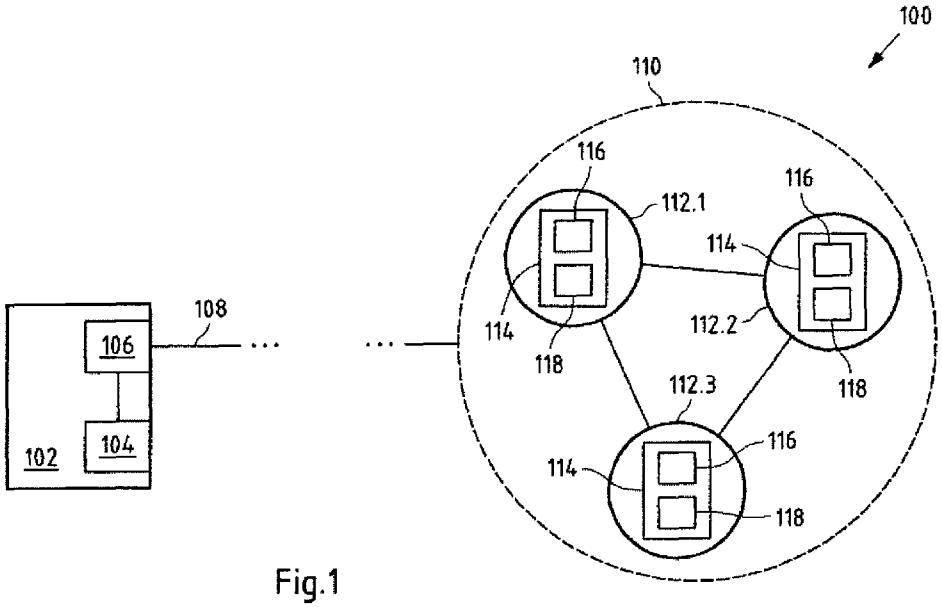


Fig.1

(57) **Abstract:** The invention relates to a system (100, 200, 300, 500) comprising at least one device (102, 202, 302) with at least one output device (106, 206, 306), which is designed to output at least one data set, and with at least one PUF device (104, 204, 304), which is designed to generate at least one key which is uniquely assigned to the device (102, 202, 302), said key being used upon outputting the data set; at least one peer-to-peer network (110, 210, 310, 510) comprising at least one peer-to-peer application (114, 214, 314, 414); and at least one key register (118, 218, 318, 418), which is at least controlled by the peer-to-peer application (114, 214, 314, 414) and which is designed to at least store the key uniquely assigned to the device (102, 202, 302), wherein the peer-to-peer application (114, 214, 314, 414) comprises at least one authenticity module (116, 216, 316, 416) which can be ran by at least one part of the peer computer (112, 212, 312, 502, 512, 564) of the peer-to-peer network (110, 210, 310, 510), and the authenticity module (116, 216, 316, 416) is designed to check the key which is used upon outputting the data set on the basis of the key register (118, 218, 318, 418) after receiving the data set by means of the peer-to-peer application (114, 214, 314, 414).

WO 2019/063256 A1

[Fortsetzung auf der nächsten Seite]

ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Bestimmungsstaaten** *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

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

(57) Zusammenfassung: Die Anmeldung betrifft ein System (100, 200, 300, 500), umfassend mindestens eine Vorrichtung (102, 202, 302) mit mindestens einer Ausgabeeinrichtung (106, 206, 306), eingerichtet zum Ausgeben von mindestens einem Datensatz, und mit mindestens einer PUF-Einrichtung (104, 204, 304), eingerichtet zum Erzeugen mindestens eines der Vorrichtung (102, 202, 302) eindeutig zugeordneten Schlüssels, wobei der Schlüssel beim Ausgeben des Datensatzes verwendet wird, mindestens ein Peer-to-Peer-Netzwerks (110, 210, 310, 510) umfassend mindestens eine Peer-to-Peer-Anwendung (114, 214, 314, 414), und mindestens ein von der Peer-to-Peer-Anwendung (114, 214, 314, 414) zumindest gesteuertes Schlüsselregister (118, 218, 318, 418), eingerichtet zumindest zum Speichern des der Vorrichtung (102, 202, 302) eindeutig zugeordneten Schlüssels, wobei die Peer-to-Peer-Anwendung (114, 214, 314, 414) mindestens ein von mindestens einem Teil der Peer-Computer (112, 212, 312, 502, 512, 564) des Peer-to-Peer-Netzwerks (110, 210, 310, 510) ausführbares Authentizitätsmodul (116, 216, 316, 416) umfasst, und wobei das Authentizitätsmodul (116, 216, 316, 416) zum Überprüfen des bei der Ausgabe des Datensatzes verwendeten Schlüssels basierend auf dem Schlüsselregister (118, 218, 318, 418) nach Empfang des Datensatzes durch die Peer-to-Peer-Anwendung (114, 214, 314, 414) eingerichtet ist.

System, insbesondere Authentizitätssystem

Die Anmeldung betrifft ein System, insbesondere ein Authentizitätssystem, mit mindestens einer Vorrichtung, umfassend mindestens eine Ausgabeeinrichtung, eingerichtet zumindest zum Ausgeben mindestens eines Datensatzes. Darüber hinaus betrifft die Anmeldung ein Verfahren, insbesondere zum Überwachen des Datenaustausches in einem anmeldungsgemäßen System, eine Vorrichtung, insbesondere für ein anmeldungsgemäßes System, und eine Peer-to-Peer-Anwendung für ein anmeldungsgemäßes System.

Sensorvorrichtungen, aber auch andere Vorrichtungen, von Kommunikationssystemen sind eingerichtet, Datensätze, umfassend erfasste Parameterwerte, an mindestens eine zentrale Instanz, insbesondere einen Server, über ein Kommunikationsnetz zu übertragen. Ein stetiges Anliegen besteht in der Sicherstellung, dass ein von einer Sensorvorrichtung durch eine Ausgabeeinrichtung ausgegebener und an den Server übertragener Datensatz nicht manipuliert wird/wurde.

Um eine Manipulation eines Datensatzes zu verhindern, ist die Verwendung von kryptographischen Schlüsseln bekannt. Insbesondere kann das Ausgeben bzw. Aussenden eines Datensatzes unter Verwendung eines kryptographischen Schlüssels erfolgen, der der Vorrichtung zugeordnet ist.

Ein bekannte und als besonders sicher geltende Einrichtung, die als Schlüsselgenerator verwendet werden kann, ist eine sogenannte PUF-Einrichtung (Physical Unclonable Function Einrichtung). Eine PUF-Einrichtung zeichnet sich vorliegend dadurch aus, dass ein (bestimmter) Schlüssel (in Form einer Bit-Folge), auch Response genannt, abhängig von einem Eingangssignal (in Form einer Bit-Folge), auch Challenge genannt, und abhängig von den physikalischen Eigenschaften der PUF-

Einrichtung, durch die PUF-Einrichtung erzeugbar ist. Da die physikalischen Eigenschaften inhärent beim Herstellungsprozess entstehen und eindeutig der hergestellten Vorrichtung zugeordnet sind, ist es nicht möglich, die Vorrichtung zu kopieren.

Die herkömmlichen Lösungen des Standes der Technik haben jedoch verschiedene Nachteile. So ist stets eine zentrale Instanz in Form eines Servers (oder mehrerer Server) erforderlich, in welchem die Schlüssel gespeichert sind. Neben den hohen Transaktionskosten, die durch eine entsprechende Kommunikationsarchitektur entstehen, ist ein weiterer Nachteil dieser Architektur, dass die zentrale Instanz bzw. der zentrale Server Schlüsseldaten, aber auch andere sensible Daten, wie Nutzerdaten (Kontodaten, Zugangsdaten, Verbrauchsdaten, etc.), verwaltet. Ein ständiges Problem der zentralen Instanz ist, diese auf einem oder mehreren Server/n gespeicherten Daten vor einem Zugriff eines unberechtigten Dritten zu schützen. Insbesondere ist ein großer sicherheitstechnischer Aufwand erforderlich, um eine Manipulation beispielsweise der Nutzerdaten, Abrechnungsdaten, erfassten Parameterwerte etc. zu verhindern. Dies führt wiederum zu höheren Transaktionskosten.

Daher liegt der Anmeldung die Aufgabe zugrunde, ein System zum Ausgeben von Datensätzen bereitzustellen, welches manipulationssicher einen Datenaustausch ermöglicht.

Die Aufgabe wird gemäß einem ersten Aspekt der Anmeldung durch ein System, insbesondere Authentizitäts- und/oder Kommunikationssystem, gemäß dem Anspruch 1 gelöst. Das System umfasst mindestens eine Vorrichtung mit mindestens einer Ausgabeeinrichtung, eingerichtet zum Ausgeben von mindestens einem Datensatz, und mit mindestens einer PUF-Einrichtung, eingerichtet zum Erzeugen mindestens eines der Vorrichtung eindeutig zugeordneten (PUF-)Schlüssels. Der Schlüssel wird beim Ausgeben des Datensatzes verwendet. Das System umfasst mindestens ein Peer-to-Peer-Netzwerk, umfassend mindestens eine Peer-to-Peer-Anwendung. Das System umfasst mindestens ein von der Peer-to-Peer-Anwendung

zumindest gesteuertes Schlüsselregister, eingerichtet zumindest zum Speichern des der Vorrichtung eindeutig zugeordneten Schlüssels. Die Peer-to-Peer-Anwendung umfasst mindestens ein von mindestens einem Teil der Peer-Computer des Peer-to-Peer-Netzwerks ausführbares Authentizitätsmodul. Das Authentizitätsmodul ist zum Überprüfen des bei der Ausgabe des Datensatzes verwendeten Schlüssels basierend auf dem Schlüsselregister nach Empfang des Datensatzes durch die Peer-to-Peer-Anwendung eingerichtet.

Im Gegensatz zum Stand der Technik ist anmeldungsgemäß vorgesehen, dass bei der Ausgabe eines Datensatzes durch eine Vorrichtung ein von einer PUF-Einrichtung der Vorrichtung erzeugter Schlüssel verwendet wird und ein derart ausgegebener Datensatz durch ein Authentizitätsmodul einer Peer-to-Peer-Anwendung überwacht bzw. ausgewertet wird. Insbesondere wird die Manipulationssicherheit durch die anmeldungsgemäße Kombination einer PUF-Einrichtung und das durch einen Teil (>1) der Peer-Computer im Wesentlichen gleichzeitig ausführbare Authentizitätsmodul erreicht. Indem anstelle eines zentralen Servers oder einer Plattform ein Peer-to-Peer-Netzwerk (also ein Framework), zumindest ein Teil (>1) der Peer-Computer des Peer-to-Peer-Netzwerks, zumindest die Überwachung bzw. Auswertung durchführt, wird die Sicherheit signifikant und in einfacher Weise verbessert. Bei einem anmeldungsgemäße Peer-to-Peer-Netzwerk werden hohe Sicherheitsstandards dadurch erreicht, indem vorzugsweise sämtliche Peer-Computer (Peer-Knoten bzw. Peers) des Netzwerks, zumindest eine Teilmenge der Peers des Netzwerks, die Korrektheit des verwendeten Schlüssels überwacht/en. Die Transaktionskosten können signifikant reduziert werden. Es ist keine zentrale, übergeordnete Plattform, Server, Cloud, etc. erforderlich. Nur wenn dieser Teil der Peer-Computer zu einem positiven Authentizitätsergebnis gelangt, kann die Echtheit und/oder Authentizität des Datensatzes bzw. der den Datensatz umfassenden Nachricht verifiziert werden. Auf einen zusätzlichen Kryptochip kann verzichtet werden.

Das anmeldungsgemäße System ist insbesondere ein Kommunikationssystem mit mindestens einer (ersten) Vorrichtung, die Datensätze ausgeben bzw. Datensätze aussenden kann. Hierfür weist die anmeldungsgemäße Vorrichtung mindestens eine Ausgabeeinrichtung, eingerichtet zum Ausgeben von mindestens einem Datensatz auf. Die Ausgabeeinrichtung kann beispielsweise eingerichtet sein, eine Nachricht mit dem Datensatz über ein drahtgebundenes und/oder drahtloses Kommunikationsnetzwerk zu übertragen.

Darüber hinaus umfasst die Vorrichtung eine sogenannte PUF-Einrichtung (Physical Unclonable Function Einrichtung). Eine PUF-Einrichtung zeichnet sich vorliegend dadurch aus, dass ein (bestimmter) Schlüssel (in Form einer Bit-Folge), auch Response genannt, abhängig von einem Eingangssignal (in Form einer Bit-Folge), auch Challenge genannt, und abhängig von den physikalischen Eigenschaften der PUF-Einrichtung, durch die PUF-Einrichtung erzeugbar ist. Der Schlüssel kann als PUF-Schlüssel bezeichnet werden. Dieser Schlüssel repräsentiert insbesondere die Identität, insbesondere die PUF-Identität, der Vorrichtung. Da die physikalischen Eigenschaften inhärent beim Herstellungsprozess entstehen und eindeutig der hergestellten Vorrichtung zugeordnet sind, ist es nicht möglich, die Vorrichtung zu kopieren. So kann durch die Challenge beispielsweise ein Chip oder eine andere Einrichtung entsprechend der Bit-Folge der Challenge konfiguriert werden. Mittels eines Messmechanismus der PUF-Einrichtung kann der durch die Konfiguration bewirkte Zustand des Chips oder der anderen Einrichtung gemessen und als Response bzw. Schlüssel (in Form einer Bit-Folge) ausgegeben werden.

Beispielhafte und nicht abschließende PUF-Einrichtungen umfassen nicht-elektronische PUFs (z.B. Paper PUF, CD PUF, Optical PUF, Optical Integrated PUF, RF-DNA PUF, Magnetic PUF, Acoustic PUF, u.a), analoge elektronischen PUFs (z.B. VT PUF, Power Distribution PUF, Coating PUF, LC PUF, u.a.), „delay-based intrinsic" PUFs (z.B. Arbiter PUF, XOR Arbiter PUF , Ring Oscillator PUF, u.a.) und Speicher basierte intrinsische PUFs (z.B. SRAM PUF, Butterfly PUF, Latch PUF, Flip-flop PUF, u.a.).

Beim Ausgeben bzw. beim Versenden des Datensatzes, insbesondere bei jedem Datensatz, wird der mindestens eine erzeugte Schlüssel verwendet. Insbesondere kann der Datensatz bzw. die entsprechende Nachricht mit dem Schlüssel versehen werden. Hierunter ist insbesondere zu verstehen, dass der Datensatz als von der Vorrichtung stammend gekennzeichnet werden kann. Der Schlüssel ist aufgrund der Verwendung einer PUF-Einrichtung eindeutig der aussendenden Vorrichtung zugeordnet. Dies ermöglicht es, den Austausch einer Vorrichtung oder deren Manipulation aufgrund eines anderen Schlüssels zu detektieren und/oder „man-in-the-middle" Angriffe zu verhindern.

Ferner umfasst das anmeldungsgemäße System mindestens ein Peer-to-Peer-Netzwerk mit mindestens einer Peer-to-Peer-Anwendung. Im Vergleich zu einem Client-Server-Netzwerk, bei dem ein Server einen Dienst anbietet und ein Client diesen Dienst nutzt, ist in einem Peer-to-Peer-Netzwerk diese Rollenverteilung aufgehoben. Jeder Teilnehmer des Peer-to-Peer-Netzwerks kann einen Dienst gleichermaßen nutzen und selbst anbieten. Insbesondere ist ein Peer-to-Peer-Netzwerk selbstbestimmt und/oder selbstorganisiert (ohne übergeordnete Einheit). Vorliegend weist vorzugweise jeder Rechner bzw. Peer des Peer-to-Peer-Netzwerks eine Peer-to-Peer-Anwendung auf.

Mindestens ein Schlüsselregister ist anmeldungsgemäß vorgesehen. Das Schlüsselregister ist zumindest zum Speichern des von der mindestens einen PUF-Einrichtung erzeugbaren Schlüssels eingerichtet. Insbesondere kann als Schlüssel mindestens ein Challenge/Response-Paar (CPR) der mindestens einen Vorrichtung und/oder mindestens ein Parameter zum PUF-Authentication-Protokoll der mindestens einen Vorrichtung in dem Schlüsselregister gespeichert sein. Vorzugsweise kann für jede in dem Schlüsselregister registrierte Vorrichtung mit PUF-Einrichtung ein Challenge/Response-Paar, vorzugsweise eine Vielzahl von Challenge/Response-Paaren (mit unterschiedlichen Challenges und entsprechend unterschiedlichen Responses) gespeichert sein. Insbesondere kann (hierdurch) die mindestens eine (PUF-) Vorrichtungs-Identität in dem Schlüsselregister gespeichert

sein. Bevorzugt kann neben der Vorrichtungs-Identität auch weitere Stamm- oder Bewegungsdaten in dem Schlüsselregister oder einem Digitalen Produktgedächtnis (in einem dezentralen Datenspeicher) gespeichert sein.

Das Schlüsselregister ist zumindest von der Peer-to-Peer-Anwendung steuerbar bzw. verwaltbar. Bei einer Ausführungsform ist hierunter zu verstehen, dass das Schlüsselregister als Schlüsselregistermodul von der Peer-to-Peer-Anwendung umfasst sein kann. Mit anderen Worten kann zumindest auf einem Teil der Peer-Computer das Schlüsselregistermodul gespeichert sein. Dieser Teil kann insbesondere zumindest den Teil umfassen, der auch das Authentizitätsmodul umfasst. Bei Ausführung des Authentizitätsmodul kann daher auf das Schlüsselregister (unmittelbar) zugegriffen werden. Hierdurch kann die Sicherheit weiter verbessert werden, da für eine erfolgreiche Manipulation sämtliche Schlüsselregister zumindest von diesem Teil der Peer-Computer manipuliert sein müssten.

Alternativ oder zusätzlich ist hierunter zu verstehen, dass die Peer-to-Peer-Anwendung ein Steuermodul aufweist, eingerichtet zum Steuern und/oder Kontrollieren des Zugriffs auf eine, insbesondere dezentralen, Datenspeicheranordnung. Vorzugsweise kann die Speicheranordnung, die eine Vielzahl von dezentralen Speichereinheiten umfassen kann, ein dezentrales Datenbanksystem (wie z. B. IPFS) oder ein dezentraler Objektspeicher (wie z.B. storj) oder eine dezentrale verteilte Datenbank (wie BigchainDB) sein, das/der/die von der Peer-to-Peer-Anwendung gesteuert wird. Beispielsweise kann die Peer-to-Peer-Anwendung ein entsprechend konfiguriertes und von einem Teil der Peer-Computer ausführbares Steuermodul umfassen.

Die Peer-to-Peer-Anwendung, insbesondere ein Softwareanwendung, umfasst mindestens ein Authentizitätsmodul. Das Authentizitätsmodul ist, wenn es ausgeführt wird, eingerichtet, den beim Ausgeben eines Datensatzes verwendeten Schlüssel zu überprüfen. Der Datensatz kann beispielsweise mittelbar oder unmittelbar an die

Peer-to-Peer-Anwendung übertragen werden. Beispielsweise nach einem Empfang und insbesondere vor einer weiteren Verarbeitung des Datensatzes kann die Authentizität des Datensatzes durch eine Authentizitätsüberprüfung des mindestens einen verwendeten Schlüssels basierend auf dem Schlüsselregister, also insbesondere den darin gespeicherten Schlüsseln (z.B. Challenge-Response-Paaren) durchgeführt werden. Dies kann beispielsweise die Durchführung von mindestens einer Vergleichsoperation zwischen empfangenen Schlüssel und gespeicherten Schlüsseln umfassen. Nur wenn eine Korrespondenz zwischen verwendeten Schlüssel und einem gespeicherten Schlüssel von dem Teil der Peer-Computer aufgrund der Ausführung des Authentizitätsmoduls festgestellt wird, kann ein Weiterverarbeitung des entsprechenden Datensatzes zugelassen werden. Andernfalls kann eine Weiterverarbeitung des entsprechenden Datensatzes gesperrt und dieser beispielsweise entsprechend gekennzeichnet werden. Weitere Maßnahmen, z.B. zur Überprüfung der Ursache, können veranlasst werden.

Insbesondere ist mittels des PUF-Schlüssels die ausgebende Vorrichtung in eindeutiger Weise identifizierbar.

Gemäß einer ersten Ausführungsform des anmeldungsgemäßen Systems kann die Vorrichtung als Sensorvorrichtung mit mindestens einer Sensoreinrichtung gebildet sein. Die Sensoreinrichtung kann zum Erfassen von mindestens einem Parameter eingerichtet sein. Der ausgegebene Datensatz kann insbesondere zumindest den erfassten Parameterwert umfassen. Die Sensoreinrichtung kann beispielsweise ein Messfühler zur Aufnahme eines Messwerts (z.B. Wärmemenge, Temperatur, Feuchtigkeit, Druck, Schallfeldgrößen, Helligkeit, Beschleunigung, pH-Wert, Ionenstärke, elektrochemisches Potential etc.) sein. Die erfassten Parameterwerte können von der Sensorvorrichtung durch eine Ausgabeeinrichtung in Form von mindestens einem Datensatz ausgegeben werden. Indem die PUF-Einrichtung in der Sensorvorrichtung integriert ist, kann durch Verwenden des Schlüssels eine Manipulation der ausgegebenen Parameterwerte zumindest signifikant erschwert werden.

Alternativ oder zusätzlich kann die Vorrichtung als Aktorvorrichtung mit mindestens einer Aktoreinrichtung gebildet sein. Die Aktoreinrichtung kann zum Verfahren eines aktuierbaren Elements eingerichtet sein. Der ausgegebene Datensatz kann insbesondere zumindest einen Zustand der Aktoreinrichtung und/oder des aktuierbaren Elements umfassen. Unter einem Verfahren eines aktuierbaren Elements ist vorliegend insbesondere zu verstehen, dass ein Aktor insbesondere einen bereitgestellten Befehlsdatensatz (oder –signal) in mechanische Bewegung und/oder andere physikalische Größe(n) überträgt. Hierdurch kann insbesondere ein aktuierbares Element entsprechend der mechanische Bewegung und/oder einer anderen physikalischen Größe verfahren bzw. eingestellt werden. Beispielsweise Zustandsdaten über den Aktor und/oder das aktuierbare Element können von der Aktorvorrichtung durch eine Ausgabeeinrichtung in Form von mindestens einem Datensatz ausgegeben werden. Indem die PUF-Einrichtung in der Aktorvorrichtung integriert ist, kann durch Verwenden des Schlüssels eine Manipulation der ausgegebenen Datensätze zumindest signifikant erschwert werden.

Alternativ oder zusätzlich kann die Vorrichtung als Verarbeitungsvorrichtung mit mindestens einer Verarbeitungseinrichtung gebildet sein. Die Verarbeitungseinrichtung kann zum Verarbeiten von empfangbaren Daten eingerichtet sein. Der ausgegebene Datensatz kann insbesondere zumindest die verarbeiteten Daten umfassen. Beispielsweise kann ein elektronischer Chip oder dergleichen als Verarbeitungseinrichtung vorgesehen sein. Daten, wie Datensätze, umfassend oben beschriebene Parameterwerte, die durch eine Sensoreinrichtung erfasst wurden, können von der Verarbeitungseinrichtung verarbeitet werden. Die verarbeiteten Daten können von der Verarbeitungsvorrichtung durch eine Ausgabeeinrichtung in Form von mindestens einem Datensatz ausgegeben werden. Indem die PUF-Einrichtung in der Verarbeitungsvorrichtung integriert ist, kann durch Verwenden des Schlüssels eine Manipulation der ausgegebenen Datensätze zumindest signifikant erschwert werden.

Für den Fall, dass es sich bei den verarbeiteten Daten um erfasste Parameterwerte handelt, die zuvor mit einem ersten Schlüssel der entsprechenden Sensorvorrichtung versehen wurden, kann der Datensatz, der von der Verarbeitungsvorrichtung ausgegeben wird, mit mindestens zwei Schlüsseln, insbesondere dem zuvor empfangenen Schlüssel der Sensorvorrichtung, und dem Schlüssel der Verarbeitungsvorrichtung, versehen sein. Bei einer nachfolgenden Authentizitätsprüfung eines derartigen Datensatzes ist das Authentizitätsmodul zum Überprüfen der beiden Schlüssel eingerichtet. Nur wenn bei beiden Schlüsseln ein positives Authentizitätsergebnis festgestellt wird, kann eine Weiterverarbeitung des Datensatzes zugelassen werden. Es versteht sich, dass auch drei oder mehr weitere Vorrichtung zwischengeschaltet sein können. Mit anderen Worten kann vorzugsweise eine Vorrichtung einen mit einem Schlüssel versehenen Datensatz von einer anderen Vorrichtung empfangen. Bei Ausgeben des Datensatzes – beispielsweise um den Datensatz weiterzuleiten – kann die Vorrichtung den mit dem Schlüssel versehenden Datensatz zusätzlich mit dem eigenen Schlüssel entsprechend den vorherigen Ausführungen versehen. Bei der Überprüfung des Datensatzes werden dann beide Schlüssel, allgemein sämtliche Schlüssel eines Datensatzes, von dem Authentizitätsmodul überprüft.

Es versteht sich, dass die verschiedenen Einrichtungen einer Vorrichtung durch eine kompakte Einheit, wie ein Chipset, gebildet sein können. Hierbei kann die Vorrichtung ein Gehäuse umfassen, das bevorzugt sämtliche Einrichtungen einer Vorrichtung umschließt. Eine Manipulation kann weiter erschwert.

Gemäß einer besonders bevorzugten Ausführungsform des anmeldungsgemäßen Systems kann das System mindestens ein Peer-to-Peer-Modul umfassen. Das Peer-to-Peer-Modul kann zumindest zum Übertragen des den Schlüssel verwendeten Datensatzes an die Peer-to-Peer-Anwendung eingerichtet sein. Das Peer-to-Peer-Modul ist insbesondere zum Kommunizieren mit der mindestens einen Peer-to-Peer Anwendung eingerichtet. Das Peer-to-Peer-Modul kann beispielsweise einer Vorrichtung, wie einer Sensor-, Aktor,- und/oder Verarbeitungsvorrichtung,

zugeordnet sein. Auch kann es durch eine separate, mit einer anderen Vorrichtung, wie einer Sensor-, Aktor,- und/oder Verarbeitungsvorrichtung, verbindbare, Vorrichtung gebildet sein.

Beispielsweise kann eine anmeldungsgemäße Vorrichtung ein Peer-to-Peer-Modul umfassen. Beispielsweise kann das Peer-to-Peer-Modul in der mindestens einen Vorrichtung des anmeldungsgemäßen Systems integriert sein. In diesem Fall kann das Peer-to-Peer-Modul durch die Ausgabeeinrichtung der Vorrichtung gebildet sein. Besonders bevorzugt kann in diesem Fall das Peer-to-Peer-Modul die PUF-Einrichtung umfassen.

Es ist auch möglich, dass eine Kommunikationsverbindung zwischen einer Vorrichtung und einem (entfernt angeordneten) Peer-to-Peer-Modul vorgesehen ist, welches insbesondere dieser Vorrichtung zugeordnet ist. Dies bedeutet insbesondere, dass das Peer-to-Peer-Modul zumindest im Namen dieser Vorrichtung kommunizieren und/oder handeln kann. Beispielsweise kann das Peer-to-Peer-Modul teilweise durch eine separate Verarbeitungseinheit, wie beispielsweise ein mobiles Kommunikationsgerät (z. B. Mobiltelefon, mobiler Computer usw.), oder auf einer entfernten, stationären Verarbeitungseinheit (z.B. ein Rechenzentrum) gebildet sein. Im Falle einer mobilen Verarbeitungseinheit oder einer entfernt angeordneten stationären Verarbeitungseinheit kann die mindestens eine Vorrichtung einen sicheren Kommunikationskanal zur Verarbeitungseinheit (oder Mobilkommunikationseinrichtung) des Rechenzentrums aufweisen und die Verarbeitungseinheit selbst kann eine Verbindung zum Peer-to-Peer-Netzwerk bereitstellen. In einer Ausführungsform kann die entfernte Verarbeitungseinheit ein "Gateway" zum Peer-to-Peer-Netzwerk sein. Dies bedeutet, dass die Vorrichtung über das zugeordnete Peer-to-Peer-Modul und das hierdurch gebildete Gateway sicher mit dem Peer-to-Peer-Netzwerk kommunizieren kann.

Vorzugsweise kann die Vorrichtung mindestens eine Signierungseinrichtung umfassen. Besonders bevorzugt kann die Signierungseinrichtung (und die PUF-

Einrichtung) in der Ausgabeeinrichtung der Vorrichtung integriert sein. Hierdurch wird die Manipulationssicherheit noch weiter erhöht. Die Signierungseinrichtung kann zum Signieren des ausgegebenen Datensatzes unter Verwendung des der Vorrichtung eindeutig zugeordneten Schlüssels eingerichtet sein. Unter Signieren ist insbesondere zu verstehen, dass der Datensatz mit einer auf den Schlüssel basierenden Signatur (oder Zertifikat) (insbesondere bildet der Schlüssel die Signatur) versehen wird. Hierdurch kann die Echtheit (bzw. Authentizität) der Daten bestätigt werden.

Alternativ oder zusätzlich kann die Vorrichtung gemäß einer weiteren Ausführungsform mindestens eine Verschlüsselungseinrichtung umfassen. Besonders bevorzugt kann die Verschlüsselungseinrichtung (und/oder die PUF-Einrichtung und/oder die Signierungseinrichtung) in der Ausgabeeinrichtung der Vorrichtung integriert sein. Hierdurch wird die Manipulationssicherheit noch weiter erhöht. Die Verschlüsselungseinrichtung kann zum Verschlüsseln des ausgegebenen Datensatzes unter Verwendung des der Vorrichtung eindeutig zugeordneten Schlüssels eingerichtet sein. Wenn sowohl eine Signierungseinrichtung als auch eine Verschlüsselungseinrichtung vorgesehen ist, kann die PUF-Einrichtung vorzugsweise zwei Schlüssel (basierend auf unterschiedlichen Challenges) generieren. Ein erster Schlüssel kann dann zum Signieren und ein weiterer Schlüssel zum Verschlüsseln genutzt werden. Alternativ können auch andere Verschlüsselungskonzepte eingesetzt werden können.

Alternativ oder zusätzlich kann die Vorrichtung gemäß einer weiteren Ausführungsform mindestens eine Hasheinrichtung umfassen. Die Hasheinrichtung kann in der Ausgabeneinrichtung integriert sein. Die Hasheinrichtung kann eingerichtet sein, dem mindestens einen ausgegebenen Datensatz zu hashen. Mit anderen Worten können die ausgehenden Daten gehasht werden. Deren Hash kann vorzugsweise in dem Schlüsselregister der Peer-to-Peer Anwendung abgespeichert sein. Hierdurch kann insbesondere die Integrität von übermittelten Daten bestätigt

werden kann. Alternativ oder zusätzlich kann ein MAC oder HMAC Protokoll verwendet werden.

Darüber hinaus kann gemäß einer bevorzugten Ausführungsform die Peer-to-Peer-Anwendung mindestens ein Registermodul umfassen. Das Registermodul kann vorzugsweise von zumindest einem Teil der Peer-Computer des Peer-to-Peer-Netzwerks ausführbar sein. Das Registermodul kann zum Registrieren einer (neuen) Vorrichtung in dem Schlüsselregister zumindest durch Speichern des der Vorrichtung eindeutig zugeordneten Schlüssels, beispielsweise zumindest ein Challenge-Response-Paar, eingerichtet sein. Besonders bevorzugt kann die Registrierung während oder unmittelbar nach Herstellung der Vorrichtung durchgeführt werden. Neben dem mindestens einen Schlüssel können weitere, die Vorrichtung betreffende Daten registriert werden (Digitales Produktgedächtnis), wie Hersteller, Besitzer, Installationsort, Zustand, Daten über den Herstellungsprozess (z.B. eingesetzte Materialien, Maschinen etc.), Kennung etc.

Das Registermodul kann konfiguriert sein, eine Registrierungsnachricht einer Vorrichtung, insbesondere eines dieser Vorrichtung zugeordneten Peer-to-Peer-Moduls zu empfangen. Die Registrierungsnachricht kann vorzugsweise zumindest den Schlüssel, insbesondere das zumindest eine (vorzugsweise mehrere) Challenge-Response-Paar, umfassen. Das Registermodul kann konfiguriert sein, zumindest den einen Schlüssel in dem Schlüsselregister zu speichern, um die Vorrichtung zu registrieren.

Vor der Registrierung einer Vorrichtung kann zumindest ein Teil der Peer-Computer des Peer-to-Peer-Netzwerks, insbesondere durch Ausführen des Registermoduls, überprüfen, ob die Registrierungsanforderungen (z. B. spezifische Entitätsspezifikationen oder gültige Schlüssel oder Compliance-Anforderungen), die durch das Peer-to-Peer-Netzwerk vordefiniert sind, von der Vorrichtung, die eine Registrierung anfordert, erfüllt sind. Beispielsweise kann der Schlüssel, insbesondere das mindestens eine Challenge-Response-Paar durch Durchführung eines

Kommunikationstests (z.B. Austausch von Testnachrichten insbesondere in Form von Challenges) überprüft werden.

Alternativ oder zusätzlich kann es notwendig sein, dass eine Vorrichtung vordefinierte, technische Spezifikationen erfüllt. Um die Überprüfung durchzuführen, können vorzugsweise weitere Daten in die Registrierungsnachricht enthalten sein. Insbesondere können die Peer-Computer des Peer-to-Peer-Netzwerks Registrierungsregeln oder Registrierungsanforderungen festlegen, die von einer Vorrichtung erfüllt werden müssen, damit diese insbesondere als eine vertrauenswürdige Vorrichtung angesehen wird. Regeln und/oder Anforderungen können individuell von den Peer-Computern eines Peer-to-Peer-Netzwerks definiert werden. Beispielsweise kann es notwendig sein, dass eine neue Vorrichtung von einer Entität empfohlen werden muss, die bereits Teilnehmer (Peer) des Peer-to-Peer-Netzwerks ist. Darüber hinaus kann es notwendig sein, dass dieser Teilnehmer einen Reputationsfaktor haben muss, der einen vordefinierten Mindestreputationsfaktor übersteigt.

Das System kann zumindest teilweise in einem Fahrzeug integriert sein. Beispielhafte und nicht abschließende Fahrzeuge sind Autos, Lastwagen, Schiffe, Schienenfahrzeuge, Flugzeuge, Fahrräder, Motorräder, Drohnen, mobile Maschinen, Boote, Flugzeuge, U-Boote, Raumfahrzeuge, Satelliten usw.

Das System kann zumindest teilweise durch das Bordnetz eines derartigen Fahrzeugs gebildet sein. Insbesondere können die in einem Fahrzeugbordnetz (oder in mehreren Fahrzeugbordnetzen) eingesetzten Sensoren, Aktoren und/oder Verarbeitungseinheiten (z.B. ECU) durch zuvor beschriebene Sensorvorrichtungen, Aktorvorrichtungen und/oder Verarbeitungsvorrichtungen gebildet sein. Hierdurch kann beispielsweise die Manipulation von Fahrzeugparameterwerten, wie Geschwindigkeitsdaten, Beschleunigungsdaten, Verbrauchsdaten etc., zumindest erschwert werden. Entsprechende Datensätze können beispielsweise für eine weitere

Auswertung an die Peer-to-Peer-Anwendung und/oder eine weitere Entität übertragen werden.

Vorzugsweise kann das Bordnetz eines Fahrzeugs selbst in Form eines internen Peer-to-Peer-Netzwerks organisiert sein (z.B. Peer-to-Peer Module in den unterschiedlichen ECUs eines Fahrzeugs oder anderen elektronischen Systemkomponenten). Dieses Peer-to-Peer-Netzwerk kann mit einem externen Peer-to-Peer-Netzwerk kommunizieren. Beide Peer-to-Peer-Netzwerke können jeweils eine zuvor beschriebene Peer-to-Peer-Anwendung, umfassend zumindest ein Authentizitätsmodul, aufweisen. Vorzugsweise kann eine Mehrzahl von Bordnetzen jeweils in Form eines anmeldungsgemäßen Peer-to-Peer-Netzwerks mit einem externen Peer-to-Peer-Netzwerk kommunizieren. Beispielsweise kann zumindest eine Vorrichtung des internen Peer-to-Peer-Netzwerks auch ein Peer-Computer des externen Peer-to-Peer-Netzwerks sein.

Darüber hinaus kann das System zumindest teilweise in einem Hausautomationssystem integriert sein. Insbesondere können die in einem Hausautomationssystem eingesetzten Sensoren, Aktoren und/oder Verarbeitungseinheiten (z.B. Hausautomationscontroller) durch zuvor beschriebene Sensorvorrichtungen, Aktorvorrichtungen und/oder Verarbeitungsvorrichtungen gebildet sein. Hierdurch kann beispielsweise die Manipulation von Hausparameterwerte, wie Temperaturdaten, Anwesenheitsdaten, Verbrauchsdaten etc., zumindest erschwert werden. Entsprechende Datensätze können beispielsweise für eine weitere Auswertung an die Peer-to-Peer-Anwendung und/oder eine weitere Entität übertragen werden.

Entsprechend den obigen Ausführungen zu einem Bordnetz kann auch das Hausautomationssystem bzw. -netz als Peer-to-Peer-Netzwerk organisiert und beispielsweise mit einem weiteren externen Peer-to-Peer-Netzwerk kommunizieren.

Darüber hinaus kann das System zumindest teilweise in einem Infrastrukturnetz oder deren einzelnen Komponenten integriert sein, z.B. Komponenten von Versorgungsnetzen, Überwachungsnetzen, Verkehrssteuerungsnetzen, Messnetzen (z.B. meteorologische Messnetze), Logistiknetze, Produktionsnetze, usw.

Darüber hinaus kann gemäß einer weiteren Ausführungsform das System mindestens ein Authentifizierungsgerät mit mindestens einem Authentizitätsmodul umfassen. Das Authentifizierungsgerät (z.B. Handgerät) kann insbesondere eingerichtet sein, bei einer nicht vorhandenen augenblicklichen Verbindung zu dem Peer-to-Peer-Netzwerk (beispielsweise aufgrund eines Netzwerkfehlers) des bei der Ausgabe des Datensatzes verwendeten Schlüssels basierend auf einem in dem Authentifizierungsgerät gespeicherten weiteren Schlüsselregister nach Empfang des Datensatzes durchzuführen. Auch in einem Offline Fall kann die Authentifizierung einer Vorrichtung mit einer PUF-Einrichtung durchgeführt werden. Vorzugsweise können bei einem Authentifizierungsgerät Obfuscating-PUF Protokolle eingesetzt werden, um die Datenmenge auf dem Authentifizierungsgerät klein zu halten.

Gemäß einer Ausführungsform des Systems gemäß der vorliegenden Anmeldung kann die Peer-to-Peer-Anwendung ein dezentrales Register, eine verteilte Ledger oder eine geteilte Datenbank sein. Das dezentrale Register kann zumindest von jedem Teilnehmer des Peer-to-Peer-Netzwerks lesbar sein. Insbesondere können sämtliche Peer-to-Peer-Module und sämtliche Peer-Computer des Peer-to-Peer-Netzwerks vorzugsweise sämtliche Informationen in der als Register gebildeten Peer-to-Peer-Anwendung (oder der von der Peer-to-Peer-Anwendung kontrollierten Speicheranordnung) lesen. Bevorzugt können auch sämtliche Peer-to-Peer-Module und sämtliche weitere Rechner bzw. Peer-Computer des Peer-to-Peer-Netzwerks Nachrichten bzw. Datensätze an die Peer-to-Peer-Anwendung senden oder in diese schreiben. In einfacher Weise können Informationen bevorzugt sämtlichen Teilnehmern des Peer-to-Peer-Netzwerks zugänglich gemacht werden. Dies erlaubt die Durchführung einer Überprüfung der in dem dezentralen Register gespeicherten Informationen, wie zuvor beschrieben Datensätze, Schlüsselregistereinträge etc.

Insbesondere kann vorzugsweise jeder Peer-Computer des Peer-to-Peer-Netzwerks eingerichtet sein, eine Überprüfung einer neuen Information, insbesondere basierend auf älteren in der Peer-to-Peer-Anwendung abgespeicherten Informationen, durchzuführen.

Darüber hinaus kann gemäß einer weiteren Ausführungsform des anmeldungsgemäßen Systems jeder Peer (Teilnehmer) des Peer-to-Peer-Netzwerks die Peer-to-Peer-Anwendung aufweisen. Vorzugsweise kann jeder Rechner, zumindest ein Teil der Peers, jeweils den kompletten Dateninhalt, zumindest jedoch einem Teil des Dateninhalts der Peer-to-Peer-Anwendung, insbesondere des dezentralen Registers, umfassen. Beispielsweise kann vorgesehen sein, dass nach einer positiven Verifizierung einer neuen, in die Peer-to-Peer-Anwendung geschriebenen Information diese von sämtlichen Peer-Computern, zumindest von einem Teil der Peer-Computer, abgespeichert wird. Die Manipulationssicherheit kann hierdurch weiter verbessert werden.

Um neue Informationen manipulationssicher zu speichern, kann die Peer-to-Peer-Anwendung Verschlüsslungsmittel und/oder Signaturmittel und/oder Verifikationsmittel, beispielsweise geeignete Hash-Funktionen, umfassen. Mindestens ein Mittel der vorgenannten Mittel kann zum Speichern von insbesondere zumindest jedem generierten Datensatz eingerichtet sein. Insbesondere kann vorgesehen sein, dass durch die Hash-Funktion eine Verknüpfung mit mindestens einer vorherigen im dezentralen Register gespeicherten Information hergestellt wird. Es können weitere Daten, wie Anfragen, Stamm-, Kontext- und/oder Transaktionsdaten einer Vorrichtung oder eines Nutzers gespeichert werden.

Bei einer besonders bevorzugten Ausführungsform kann die Peer-to-Peer-Anwendung eine Blockchain oder eine dezentrale Ledger sein, umfassend mindestens zwei miteinander verknüpfte Blöcke. Die Blockchain-Technologie bzw. „decentral ledger technology“ wird bereits bei der Bezahlung mittels einer Cryptowährung, wie Bitcoin, eingesetzt. Es ist erkannt worden, dass durch eine spezielle Konfiguration

eine Blockchain eingerichtet werden kann, zumindest einen Datenaustausch besonders manipulationssicher zu steuern.

Die Blockchain gemäß der vorliegenden Ausführungsform ist insbesondere ein dezentralisiertes, Peer-to-Peer-basiertes Register, in dem vorzugsweise eine Mehrzahl von Datensätzen und/oder Modulen und sonstigen Nachrichten von Vorrichtung/en protokolliert werden können. Eine Blockchain ist als technisches Mittel besonders geeignet, eine zentrale Instanz in einfacher und gleichzeitig sicherer Weise zu ersetzen.

Wie bereits beschrieben wurde, kann die mindestens eine Peer-to-Peer-Anwendung ein dezentralisiertes Register, ein verteiltes Ledger oder eine gemeinsam genutzte Datenbank sein, die konfiguriert ist, um Daten zu speichern, z.B. die zuvor beschriebenen Datensätze, Kennung(en), Schlüssel, usw. mit bestimmten Beweisen (proofs) und/oder Signaturen. Zusätzlich zu z.B. Schlüsseln von registrierten Vorrichtungen, kann das dezentrale Register Computercode speichern, wie z.B. das Authentizitätsmodul zum Überwachen bzw. Verifizieren der Echtheit bzw. Authentizität eines Datensatzes oder ein Registermodul zum Registrieren einer Vorrichtung oder ein Steuermodul zum Steuern des Zugriffs auf eine durch das Steuermodul kontrollierte Datenspeicheranordnung.

Insbesondere kann der Code durch eine Transaktion an die Adresse des Codes in dem so genannten "smart contract" aufgerufen werden. Dieser Code kann auf der Mehrzahl von Peer-Computern des Peer-to-Peer-Netzwerks verarbeitet werden.

Es versteht sich, dass ein/e (smart contract-) Code- oder Verarbeitungslogik in sogenannten „Krypto-Bedingungen“ („crypto condictions") des Interledger-Protokolls (ILP) gespeichert und ausgeführt werden kann. Dies bedeutet, dass nicht unbedingt sämtlicher Code in einem smart contract, wie Ethereum smart contract, gespeichert sein muss.

In einer weiteren Ausführungsform kann der (smart contract-) Code auf einem dezentralen Berechnungsmarktplatz (z. B. Ethereum Computation Market, Trubit, Golem, Cryplets Microsoft) gespeichert und ausgeführt werden.

In einer weiteren Ausführungsform können Computercodes einer externen Rechenvorrichtung, die durch die Peer-to-Peer-Anwendung gesteuert werden, Algorithmen für dezentrale kognitive Analysen, künstliche Intelligenz oder maschinelles Lernen umfassen. Analytik und Lernen können mit anderen Geräten geteilt und über die Peer-to-Peer-Anwendung gemeinsam genutzt, aggregiert und weiter analysiert werden. Zum Beispiel können diese Algorithmen angewendet werden, um einen Austauschvorgang zu optimieren.

Ein dezentrales Register kann zumindest von einem Teil der Teilnehmer des Peer-to-Peer-Netzwerks lesbar sein. Insbesondere kann jeder Rechnerknoten (Peer-Computer) und jede registrierte Entität/Vorrichtung (mittels des jeweiligen Peer-to-Peer-Moduls) die Peer-to-Peer-Anwendung umfassen. Das dezentrale Register, zumindest der öffentliche Teil (d.h. ohne private contracts), kann zumindest von jedem Teilnehmer des Peer-to-Peer-Netzwerks gelesen werden. Insbesondere können alle Peer-to-Peer-Module und alle anderen Peer-Computer des Peer-to-Peer-Netzwerks vorzugsweise sämtliche Informationen in der Peer-to-Peer-Anwendung lesen, die als Register ausgebildet ist. Vorzugsweise ist es auch möglich, dass alle Peer-to-Peer-Module und alle anderen Peer-Computer des Peer-to-Peer-Netzwerks Nachrichten/Datensätze an die Peer-to-Peer-Anwendung senden oder empfangen können. Eine Nachricht oder Transaktion, die an einen smart contract gesendet wird, kann die Ausführung eines Codes des smart contracts (z. B. Authentizitätsmodul, Registermodul, usw.) starten, während Daten verwendet werden, die in dem smart contract gespeichert sind. Zum Beispiel kann das Empfangen eines Datensatzes die Ausführung des Authentizitätsmoduls starten, wie oben beschrieben wurde. Auch kann eine Registrierungsnachricht die Ausführung des Registermoduls starten.

Die Peer-to-Peer-Anwendung kann auf folgenden Elementen aufgebaut werden: Peer-

to-Peer-Netzwerk mit Consensus System/Protocol, Data Structure, Merkle Trees, Public Key Signatures und/oder Byzantinische Fehlertoleranz. Es kann Daten nach einem Consensus Prinzip replizieren. Es kann auditierbar und nachvollziehbar sein.

Auf einfache Weise können Informationen vorzugsweise allen Teilnehmer zur Verfügung gestellt werden. Dies kann eine Überprüfung der im dezentralen Register gespeicherten Informationen oder der im dezentralen Register ausgeführten Codes ermöglichen. Besonders bevorzugt kann jeder Rechner (Peer-Computer) im Peer-to-Peer-Netzwerk konfiguriert sein, um neue Informationen zu überprüfen, insbesondere auf der Grundlage älterer Informationen, die in der Peer-to-Peer-Anwendung gespeichert sind. Zusätzlich kann das mindestens eine Authentizitätsmodul und/oder das mindestens eine Steuermodul und/oder das mindestens eine Registermodul durch mindestens einen Teil der Peers des Peer-to-Peer-Netzwerks, vorzugsweise durch alle Peers, überwacht werden. Eine Manipulation eines derartigen Moduls kann somit verhindert werden.

Darüber hinaus kann zumindest ein Peer-Computer, vorzugsweise jeder Peer-Computer, jeweils den kompletten Dateninhalt umfassen, aber zumindest einen Teil des Dateninhalts der Peer-to-Peer-Anwendung, insbesondere des dezentralen Registers, umfassen. Beispielsweise kann vorgesehen sein, dass nach einer positiven Authentifizierung eines Datensatzes oder z.B. nach einer positiven Registrierung einer Vorrichtung in der Peer-to-Peer-Anwendung diese Information von allen Peer-Computern, zumindest von einem Teil der Peer-Computer, gespeichert wird. Beispielsweise können nach der nach einer erfolgreichen Registrierung einer Vorrichtung der mindestens eine (neue) Schlüssel zumindest durch einen Teil der Peer-Computer, vorzugsweise durch sämtliche Peer-Computer des Peer-to-Peer-Netzwerks, gespeichert werden. Die Manipulationssicherheit für die in der Peer-to-Peer-Anwendung gespeicherten Daten kann dadurch weiter verbessert werden. Ein Datenaustauschvorgang und/oder ein Registrierungsprozess kann sicher gesteuert werden.

Die Peer-to-Peer-Anwendung kann durch eine Directed Acyclic Graph (DAG) gebildet sein. Ein gerichteter azyklischer Graph, wie IOTA oder Tangle, bedeutet, dass Blöcke (oder Knoten des Graphen) über gerichtete Kanten miteinander gekoppelt sind. Dabei bedeutet „direct", dass die (alle) Kanten (immer) eine gleiche Richtung in der Zeit haben. Mit anderen Worten, es ist nicht möglich, zurückzugehen. Schließlich bedeutet azyklisch, dass Schleifen nicht existieren.

In weiteren Ausführungsformen der Peer-to-Peer-Anwendung kann die Blockchain eine „permissionless" oder „permissioned" Blockchain sein. In einem Fall kann die Blockchain eine öffentliche, Konsortium oder private Blockchain sein.

In einer weiteren Ausführungsform können mehrere Peer-to-Peer-Netzwerke, insbesondere Blockchains, vorgesehen sein, die über Mechanismen wie „side chains" oder smart contracts verbunden sind. Insbesondere kann hierdurch mindestens ein oben beschriebenes externes Peer-to-Peer-Netzwerk mit mindestens einem oben beschriebenen internen Peer-to-Peer-Netzwerks eines Fahrzeugs oder eines Gebäudes verbindbar sein. Ein Peer-to-Peer-Knoten bzw. Peer-Computer kann einen oder mehrere Blockchain-Client(s) ausführen.

Die Daten der Peer-to-Peer-Anwendung können auf der "dezentralen Ledger-Technologie" und/oder der „dezentralen Ledger-Steers (verschlüsselte) Datenspeicherung" über das Internet und vorzugsweise im dezentralen Datenspeicher, Objektspeicher bzw. Datenbank gespeichert sein, wie z. B. ein Interplanetary File System (IPFS) oder storj oder in einer verteilten Blockchain-Datenbank (z.B. BigChainDB oder mit Cryptowerk-Funktionen gehashte Datenbank). Der Zugriff auf verschlüsselte Daten an Drittanbieter kann über ein zuvor beschriebenes Steuermodul verwaltet werden, das als ein oder mehrere smart contract(s) in der Blockchain gebildet sein kann/können.

Auch können Token aus einem Peer-to-Peer-Netzwerk eingefroren und z.B. an eine Blockchainifizierte Datenbank übertragen werden. D.h. Nutzer können ein zweites

‚Wallet' in dieser Datenbank aufweisen. Transaktionen zwischen den Nutzern bzw. deren Wallets können als performante Datenbanktransaktionen durchgeführt werden. Nach Ablauf einer bestimmten Zeit oder der Beendigung der Gesamttransaktion kann das Ergebnis auf das ursprüngliche Peer-to-Peer-Netzwerk zurückgeschrieben werden. Als Beispiel für die Ausführung mehrerer Blockchains kann eine IoT Blockchain, wie DAT tangle, dazu benutzt werden, sicher IoT Daten zu erfassen, und diese in einem zweiten Peer-to-Peer-Netzwerk, wie z.B. BigchainDB, als Input für die Durchführung von Transaktionen zu speichern.

Darüber hinaus können Daten-Feeds (data feeds) von der Peer-to-Peer-Anwendung (sogenannte "smart oracles") bereitgestellt werden. Daten-Feeds können weitere Daten über eine Vorrichtung aus mindestens einer weiteren Quelle bereitstellen. Daten können aus vertrauenswürdigen Quellen empfangen und in der Peer-to-Peer-Anwendung gespeichert oder über die Peer-to-Peer-Anwendung auf einer dezentralen Datenspeicheranordnung gespeichert werden.

Informationen zwischen Peer-Computern können durch ein Peer-to-Peer-Messaging-System ausgetauscht werden. Dies bedeutet, dass ein Peer-Computer eine Nachricht an einen anderen Peer-Computer senden kann, um eine Information zu übermitteln oder eine Aktion auszulösen. Nachrichten bzw. Datensätze können als Klartext, signiert, hashed, zeitgestempelt und/oder verschlüsselt werden. Dies bedeutet, dass nicht alle Daten, die zwischen Peers ausgetauscht werden, auf der Peer-to-Peer Anwendung gespeichert werden müssen.

In einer weiteren Ausführungsform kann das mindestens eine Peer-to-Peer-Netzwerk durch mehrere Peer-Computer und ein Peer-to-Peer-Modul gebildet sein. Ein Peer-to-Peer-Modul kann nur so konfiguriert sein, dass es mit der Vielzahl von Peer-Computern kommunizieren kann. Mit anderen Worten, das Peer-to-Peer-Modul ist kein Peer-Computer des Peer-to-Peer-Netzwerks, sondern nur ein Teilnehmer. Ein solches Peer-to-Peer-Modul umfasst nicht die Peer-to-Peer-Anwendung, sondern stellt nur ein Schnittstellenmodul, wie eine Anwendungsprogrammierschnittstelle

(API), und eine dezentrale Applikation zur Kommunikation mit den Peer-Computern des Peer-to-Peer-Netzwerks bzw. mit der Peer-to-Peer-Anwendung, wie eine Blockchain oder ein smart contract einer Peer-to-Peer-Anwendung, bereit. Beispielsweise kann ein solches Peer-to-Peer-Modul entweder Klartext- oder verschlüsselte Informationen senden oder eine sichere Verbindung (z.B. Tunnel) zu einem weiteren Peer-to-Peer Modul erzeugen, um mit dem Peer-to-Peer-Modul oder dem Peer-to-Peer-Netzwerk zu kommunizieren. Dies ermöglicht eine Verringerung der erforderlichen Rechenleistung des Peer-to-Peer-Moduls.

In einer Ausführungsform des Peer-to-Peer-Netzwerks kann es nur einen validierenden Peer-Computer oder einen vollständigen Knoten geben, z.B. kann nur ein Knoten konfiguriert werden, um einen Validierungsprozess durchzuführen und einen oder mehrere Beobachtungs- (oder Überwachungs-) Peers. Ein Beobachtungspeer kann einige Transaktionen validieren, um eine Vertrauensstufe zu etablieren, aber er validiert nicht alle Transaktionen, die durch den validierenden Peer durchgeführt werden.

In einer weiteren Ausführungsform kann das Peer-to-Peer-Modul einer der Peer-Computer sein. In diesem Fall umfasst das Peer-to-Peer-Modul zumindest einen Teil der Peer-to-Peer-Anwendung. Insbesondere kann das Peer-to-Peer-Modul vorzugsweise den gesamten Dateninhalt der Peer-to-Peer-Anwendung umfassen oder auf die in einem anderen Peer gespeicherten Informationen zugreifen. Beispielsweise kann das Peer-to-Peer-Modul ein sogenannter "light node" oder eine dezentrale Anwendung (DAPP) sein, die mit einem entfernten Peer (fest) verbunden ist.

Es wird angemerkt, dass im vorliegenden Fall gemäß einer Ausführungsform das Peer-to-Peer-Modul mindestens eine API umfasst, die konfiguriert ist, um mit der Peer-to-Peer-Anwendung zu kommunizieren. Zusätzlich zu der API umfasst das Peer-to-Peer-Modul eine dezentrale Software-Anwendung, die lokale Algorithmen umfasst, die zumindest konfiguriert sind, um Datensätze, wie z.B. Messdaten, zu erzeugen und über die API an die Peer-to-Peer-Anwendung zu übertragen. Die dezentrale

Anwendung "Dapp" ist zumindest so konfiguriert, dass sie die Daten verarbeitet und überträgt.

Vorzugsweise werden die Daten signiert oder verschlüsselt oder können über einen kryptographisch gesicherten Tunnel oder eine gesicherte Internetverbindung an einen Peer oder ein weiteres Peer-to-Peer-Modul übertragen werden. In einer weiteren Ausführungsform ist auch die Peer-to-Peer-Anwendung selbst im Peer-to-Peer-Modul implementiert, d.h. das Peer-to-Peer-Modul ist ein Peer des Peer-to-Peer-Netzwerks, der die dezentrale Applikation, die API und die Peer-to-Peer-Anwendung umfasst.

Daten und Transaktionen, die auf der Blockchain gespeichert sind, stellen keine "transaktionale Privatsphäre" zur Verfügung. Transaktionen zwischen Pseudonymen können (oft) in Klartext auf der Blockchain gespeichert werden. In manchen Fällen werden die auf der Blockchain gespeicherten Daten verschlüsselt und die Schlüssel können über die Blockchain gehandhabt werden. Transaktionen zwischen Pseudonymen werden in Klartext auf der Blockchain gespeichert. Sichere Transaktionen oder Ausführungen von Computer-Codes können mit kryptografischen Werkzeugen, wie z. B. „zero knowledge“ (zk) Proofs oder „zk Succinct Non-interactive Arguments“ (zk-SNARK) erreicht werden. Transaktionen oder Algorithmen sind in zwei Teile unterteilt: ein Smart contract über die Blockchain und ein private contract. Ein Datenschutzbewahrungsprotokoll sorgt für die Privatsphäre der Daten und die Richtigkeit der Codeausführung (SNARK-Überprüfung erfolgt über den Smart-Vertrag auf Kette). Die private Auftragsberechnung kann durch einen Satz von Peers, Off-Chain-Computern oder in einer „measured launch environment“ oder einer sicheren Hardware-Enklave für die Bescheinigung und Abdichtung (sealing) durchgeführt werden, die nicht durch einen anderen Softwarecode, der auf den Geräten ausgeführt wird, manipuliert werden können. In einer alternativen Ausführungsform können sichere Multi-Party-Computing (sMPC) -Systeme für die Transaktions-Privatsphäre genutzt werden. Beispiele für Datenschutzbewahrungsprotokolle und Berechnungen sind HAWK und MIT Enigma.

Mit „zero knowledge“ (zk Proofs) können die Parteien sehen, dass der Algorithmus in einem privaten Vertrag korrekt ausgeführt wird, aber die Eingabedaten werden nicht an die Parteien weitergegeben. Darüber hinaus kann eine selektive Privatsphäre durch die Freigabe von Schlüsseln zur Entschlüsselung von Transaktionen für Berichts- und Prüfungszwecke bereitgestellt werden.

Zur sicheren Bereitstellung von Codes und/oder Daten in ein Gerät kann eine vertrauenswürdige Ausführungsumgebung (Trusted Execution Environments) wie Intel SGX oder TPM oder Direct Anonymous Attestation Modul mit einem Peer-to-Peer-Modul integriert werden. In weiteren Ausführungsformen kann eine PUF-Einrichtung in einer vertrauenswürdige Ausführungsumgebung integriert sein.

Auch können weitere kryptographische Verfahren zur Herstellung einer transaktionalen Privatsphäre genutzt werden (z.B. Ring Signatures, Stealth Addresses oder Pedersen Commitments).

Ähnlich kann in einer weiteren Ausführungsform ein besonders großes Peer-to-Peer-Netzwerk in zwei oder mehr (physikalische oder logische oder dynamisch virtuelle) Cluster aufgeteilt werden. In einem entsprechenden Peer-to-Peer-Netzwerk kann beispielsweise eine Validierung (einer Teilmenge von Transaktionen) nur von den Mitgliedern eines Clusters durchgeführt werden (eine Teilmenge von Peers, z. B. das Aufteilen einer Blockchain zur Verbesserung der Skalierbarkeit). In einer weiteren Ausführungsform kann die Peer-to-Peer-Anwendung unter Verwendung mehrerer Blockchains gebildet werden. Diese Blockchains sind über Frameworks, wie beispielsweise „sidechains“ oder smart contracts oder Interledger Protokolle, verbunden.

Ein weiterer Aspekt der Anmeldung ist ein Verfahren, umfassend:

- Ausgeben von mindestens einem Datensatz durch eine Ausgabeeinrichtung einer Vorrichtung unter Verwendung mindestens eines der Vorrichtung zugeordneten Schlüssels,
- wobei der Schlüssel durch mindestens eine in der Vorrichtung integrierte PUF-Einrichtung erzeugt wird,
- Bereitstellen einer Peer-to-Peer-Anwendung eines Peer-to-Peer-Netzwerks,
- Bereitstellen eines zumindest von der Peer-to-Peer-Anwendung gesteuerten Schlüsselregisters, eingerichtet zumindest zum Speichern des der Vorrichtung eindeutig zugeordneten Schlüssels, und
- Überprüfen des ausgegebenen und durch die Peer-to-Peer-Anwendung empfangenen Datensatzes durch Ausführen mindestens eines Authentizitätsmoduls durch mindestens einen Teil der Peer-Computer des Peer-to-Peer-Netzwerks,
- wobei das Überprüfen das Auswerten des bei der Ausgabe des Datensatzes verwendeten Schlüssels basierend auf dem Schlüsselregister umfasst.

Das Verfahren kann insbesondere auf einem zuvor beschriebenen System durchgeführt werden. Der Überprüfungsschritt umfasst insbesondere das Verifizieren der Authentizität eines erhaltenen Datensatzes anhand des mindestens einen verwendeten Schlüssels und den gespeicherten Schlüsseln.

In der vorliegend Anmeldung ist unter einem Schlüssel, der bei Ausgeben eines Datensatzes verwendet wird, ein von der ausgebenden Vorrichtung erzeugter PUF-Schlüssel zu verstehen.

Ein weiter Aspekt der Anmeldung ist eine Vorrichtung. Die Vorrichtung umfasst mindestens eine Ausgabeeinrichtung, eingerichtet zum Ausgeben von mindestens einem Datensatz. Die Vorrichtung umfasst mindestens eine PUF-Einrichtung, eingerichtet zum Erzeugen mindestens eines der Vorrichtung eindeutig zugeordneten Schlüssels. Der Schlüssel wird beim Ausgeben des Datensatzes verwendet. Die Ausgabeeinrichtung ist durch ein (zuvor beschriebenes) Peer-to-Peer-Modul gebildet,

eingerichtet zumindest zum Übertragen des den Schlüssel verwendeten Datensatzes an eine Peer-to-Peer-Anwendung eines Peer-to-Peer-Netzwerks, derart, dass mindestens ein von mindestens einem Teil der Peer-Computer des Peer-to-Peer-Netzwerks ausführbares Authentizitätsmodul der Peer-to-Peer-Anwendung den bei der Ausgabe des Datensatzes verwendeten Schlüssels basierend auf einem Schlüssel speichernden Schlüsselregisters überprüft.

Die Vorrichtung kann insbesondere in einem zuvor beschriebenen System implementiert sein. Insbesondere kann die Vorrichtung eine zuvor beschriebene Sensorvorrichtung, eine zuvor beschriebene Aktorvorrichtung und/oder eine zuvor beschriebene Verarbeitungsvorrichtung sein.

Ein noch weiterer Aspekt der Anmeldung ist eine Peer-to-Peer-Anwendung, insbesondere eine zuvor beschriebene Peer-to-Peer-Anwendung, für ein (zuvor beschriebenes) Peer-to-Peer-Netzwerk, umfassend:

- mindestens ein von mindestens einem Teil der Peer-Computer des Peer-to-Peer-Netzwerks ausführbares Authentizitätsmodul, eingerichtet zum Überprüfen eines durch die Peer-to-Peer-Anwendung empfangenen und unter Verwendung eines durch eine PUF-Einrichtung erzeugten Schlüssels ausgegebenen Datensatzes,
- wobei das Überprüfen ein Auswerten des bei der Ausgabe des Datensatzes verwendeten Schlüssels basierend auf einem von der Peer-to-Peer-Anwendung zumindest gesteuerten Schlüsselregister, eingerichtet zumindest zum Speichern des einer Vorrichtung eindeutig zugeordneten Schlüssels, umfasst.

Die Peer-to-Peer-Anwendung kann insbesondere ein auf einem Prozessor ausführbares Computerprogramm sein.

Das anmeldungsgemäße System kann beispielsweise für Software-Lizensierungsanwendungen oder anonyme Rechenanwendungen verwendet werden. Das anmeldungsgemäße System kann weiter auch für Software-Updates von

Systemen und / oder deren Parametrisierung verwendet werden. Eine bevorzugte Anwendung können die Over-the-Air Updates von Systemen sein (Fahrzeuge, Gebäude, Infrastrukturnetz etc.).

Ferner kann zwischen so genannten schwachen und starken PUF-Einrichtungen unterschieden werden. Eine starke PUF-Einrichtung kann sich (u.a.) von einer schwachen PUF-Einrichtung durch eine höhere Anzahl von Challenge-Response Paaren (CPR) unterscheiden. In bevorzugten Ausführungen der Anmeldung können starke PUF-Einrichtung verwendet werden.

Ferner kann eine PUF-Einrichtung mit einem Krypto-Hardware Prozessor kombiniert werden. Zum Beispiel kann diese Kombination eingerichtet sein, um aus einem schwachen Schlüssel einen stärkeren Schlüssel zu generieren, und/oder für Keyed-Hash Message Authentication Code Generierung (HMAC), um eine ausreichende Authentifizierungsfähigkeit zur Authentifizierung von Nachrichten einer Vorrichtung an einen Dritten zu etablieren (und damit Man-in-the-middle Attacken zu verhindern), und/oder zum Signieren, Hashen und / oder Verschlüsseln von Nachrichten.

Bevorzugt kann sogenannte Hardware Entangled Cryptography angewendet werden, bei der eine PUF-Einrichtung in den Krypto-Hardware Prozessor integriert sein kann (oder umgekehrt).

Auch kann eine PUF-Einrichtung auch mit einem Error-Correction Module kombiniert sein, der Varianzen in der Antwortverhalten (z.B. aufgrund von Temperaturabhängigkeiten von Bauelementen) bei CPRs korrigieren kann. Um Wiederholungen zu vermeiden, ist insbesondere vorliegend eine PUF-Einrichtung eine Einrichtung mit oder ohne Crypto-Hardware Prozessor und/oder mit oder ohne Error Correction Module.

Unter einer eine PUF-Einrichtung ist ferner eine Einrichtung zu verstehen, die eine so genannte „physical one-way" Function darstellen, die aus einer oder vorzugsweise

mehrere Challenge(s) eine oder mehrere Response/s generiert, die von den individuellen, besonderen physikalischen Eigenschaften einer Vorrichtung abhängen. Ein derartiger Mechanismus kann eingerichtet sein, um one-way Functions zu produzieren, günstig herzustellen, extrem aufwendig (oder gar unmöglich) zu duplizieren, primär nicht auf mathematischen Algorithmen basierend und tamper-resistant. Diese Funktionen können für ein Authentifizierungsprotokoll genutzt werden. Es können Funktionen eingesetzt werden, die einen großen Adressraum bzw. eine große Menge von CPRs ermöglichen. Weitere Beispiele von PUF-Einrichtungen sind Physical One-Way Functions, Physical Random Functions oder Continuous-variable Quantum Authentication of Physical Unclonable Keys. Diese Methoden können in einer PUF-Einrichtung zumindest teilweise implementiert sein und insbesondere unter dem Begriff PUF zusammengefasst werden. Des Weiteren gibt es Varianzen von PUFs, z.B. t-PUFs.

Auch die Methode der Obfuscating PUFs, bei denen nicht eine größere Menge an CPRs auf in einem Schlüsselregister, sondern ein nur ein verhältnismäßig kleinerer Datensatz gespeichert werden muss und dafür für dieses Protokolle Rechenoperationen auf der Vorrichtung durchgeführt werden müssen, können in einer anmeldungsgemäßen PUF-Einrichtung zumindest teilweise implementiert sein. Neben der Authentifizierung können PUFs noch für Secret Key Generation und Schlüssel-Speicherung genutzt werden.

Unter einer PUF-Einrichtung ist auch so genannte Physically obfuscated keys (POK) und physically obfuscated algorithms Einrichtungen zu verstehen. Schlüssel können hierbei nicht elektronisch sondern physikalisch gespeichert sein.

Bei so geannten gesteuerten (controlled) PUF (CPUF)-Einrichtungen kann eine PUF-Einrichtung in Kombination mit kryptographischen Primitives verwendet werden. Auf ein solches CPUF kann insbesondere nur über einen physikalisch mit dem PUF verbundenen Algorithmus zugegriffen werden.

Reconfiguarbale PUF (rPUF) –Einrichtungen können so rekonfiguriert werden, dass in einem Rekonfigurationsprozess das CRP Verhalten sich zufällig und irreversibel ändert. Weitere PUF Konzepte sind Quantum Readout PUFs, SIMPL Systems und PPUFs.

Alle die oben genannten Konzepte/Einrichtungen sind in der vorliegenden Anmeldung insbesondere unter dem Begriff PUF zusammen.

Die Merkmale der Systeme, Verfahren, Vorrichtungen, Peer-to-Peer Anwendungen und Computerprogramme sind frei miteinander kombinierbar. Insbesondere können Merkmale der Beschreibung und/oder der abhängigen Ansprüche, auch unter vollständiger oder teilweiser Umgehung von Merkmalen der unabhängigen Ansprüche, in Alleinstellung oder frei miteinander kombiniert eigenständig erfinderisch sein.

Es gibt nun eine Vielzahl von Möglichkeiten, das anmeldungsgemäße System, das anmeldungsgemäße Verfahren, die anmeldungsgemäße Vorrichtung und die anmeldungsgemäße Peer-to-Peer-Anwendung auszugestalten und weiterzuentwickeln. Hierzu sei einerseits verwiesen auf die den unabhängigen Patentansprüchen nachgeordneten Patentansprüche, andererseits auf die Beschreibung von Ausführungsbeispielen in Verbindung mit der Zeichnung. In der Zeichnung zeigt:

Fig. 1 eine schematische Ansicht eines Ausführungsbeispiels eines Systems gemäß der vorliegenden Anmeldung,

Fig. 2 eine schematische Ansicht eines weiteren Ausführungsbeispiels eines Systems gemäß der vorliegenden Anmeldung,

Fig. 3 eine schematische Ansicht eines weiteren Ausführungsbeispiels eines Systems gemäß der vorliegenden Anmeldung,

Fig. 4 eine schematische Ansicht eines Ausführungsbeispiels einer Peer-to-Peer-Anwendung gemäß der vorliegenden Anmeldung;

Fig. 5 eine schematische Ansicht eines weiteren Ausführungsbeispiels eines Systems gemäß der vorliegenden Anmeldung;

Fig. 6 ein Diagramm eines Ausführungsbeispiels eines Verfahrens gemäß der vorliegenden Anmeldung;

In den Figuren werden für gleiche Elemente gleiche Bezugszeichen verwendet.

Die Figur 1 zeigt eine schematische Ansicht eines Ausführungsbeispiels eines Systems 100, insbesondere eines Kommunikationssystems 100, gemäß der vorliegenden Anmeldung. Das System 100 umfasst mindestens eine Vorrichtung 102 und mindestens ein Peer-to-Peer-Netzwerk 110.

Die Vorrichtung 102 umfasst mindestens eine Ausgabeeinrichtung 106. Die Ausgabeeinrichtung 106 ist zumindest zum Ausgeben, insbesondere Aussenden, von Datensätzen über ein Kommunikationsdatennetz 108 eingerichtet. Das Kommunikationsdatennetz 108 kann ein drahtloses und/oder drahtgebundenes Kommunikationsdatennetz 108 sein. Vorzugsweise kann die Ausgabeeinrichtung 106 eine Sende-/Empfangseinrichtung 106 sein und insbesondere zum Aussenden und Empfangen von Datensätzen, beispielsweise in Form von Datensatznachrichten, konfiguriert sein.

Daneben umfasst die Vorrichtung 102 mindestens eine PUF-Einrichtung 104. Die PUF-Einrichtung 104 kann insbesondere durch ohnehin in der Vorrichtung 102 implementierte elektronische Komponenten, Schaltkreise etc. gebildet sein. Die PUF-Einrichtung 104 zeichnet sich vorliegend dadurch aus, dass ein (bestimmter) Schlüssel (in Form einer Bit-Folge), auch Response genannt, abhängig von einem

Eingangssignal (in Form einer Bit-Folge), auch Challenge genannt, und abhängig von den physikalischen Eigenschaften der PUF-Einrichtung, also den elektronischen Komponenten, Schaltkreisen, erzeugt wird. Da die physikalischen Eigenschaften inhärent beim Herstellungsprozess entstehen und eindeutig der hergestellten Vorrichtung zugeordnet sind, kann ein entsprechender PUF-Schlüssel eindeutig der Vorrichtung 102 zugeordnet werden.

Durch ein Challenge-Signal werden beispielsweise die elektronische Komponenten, Schaltkreise etc. entsprechend konfiguriert. Mittels eines (nicht dargestellten) Messmechanismus kann der durch die Konfiguration bewirkte Zustand der elektronischen Komponenten, Schaltkreise etc. von der PUF-Einrichtung 104 gemessen und als Response bzw. Schlüssel (in Form einer Bit-Folge) bereitgestellt werden.

Dieser mindestens eine PUF-Schlüssel wird beim Ausgeben eines Datensatzes von der Ausgabeeinrichtung 106 verwendet. Hierunter ist insbesondere zu verstehen, dass der Datensatz mit dem PUF-Schlüssel derart versehen wird, dass hierdurch die Echtheit bzw. Authentizität der in dem Datensatz bzw. der Datensatznachricht enthaltenen Daten belegt wird.

Bevorzugt können die Einrichtungen 104 und 106 von einem (nicht gezeigten) Gehäuse und/oder einer (nicht gezeigten) geeigneten Verkapselung umschlossen sein, um die Manipulationssicherheit weiter zu erhöhen.

Ein wesentlicher Unterschied zu einem Stand der Technik System besteht darin, dass in dem System 100 keine zentrale Instanz vorgesehen ist. Vorliegend weist das System 100 mindestens ein Peer-to-Peer-Netzwerk 110 bzw. ein Rechner-Rechner-Netzwerk 110 auf. Das Peer-to-Peer-Netzwerk 100 umfasst eine Vielzahl von Peer-Computern 112.1 bis 112.3 (auch Knoten bzw. Rechner genannt). Es versteht sich, dass mehr als die dargestellten drei Peer-Computer 112.1 bis 112.3 vorgesehen sein können. Ein Peer-to-Peer-Netzwerk 122 zeichnet sich vorliegend dadurch aus, dass vorzugsweise

jeder Knoten und/oder Teilnehmer mit jedem anderen Knoten und/oder Teilnehmer verbunden ist. Dies kann über ein drahtloses oder drahtgebundenes Netzwerk erfolgen. Beispielsweise kann das Internet verwendet werden. Dieses Netzwerk kann zumindest teilweise identisch mit dem Kommunikationsdatennetz 108 sein.

Zudem sind die Peer-Computer 112.1 bis 112.3 als gleichberechtigte Peer-Computer 112.1 bis 112.3 konfiguriert, wodurch sie sich von einer herkömmlichen Server-Client-Struktur unterscheiden.

Die dargestellten drei Peer-Computer 112.1 bis 112.3 umfassen (jeweils) eine Peer-to-Peer-Anwendung 114. Wie zu erkennen ist, ist auf jedem Peer-Computer 112.1 bis 112.3 die gleiche Peer-to-Peer-Anwendung 114 implementiert. Vorzugsweise kann die Peer-to-Peer-Anwendung 114 ein von insbesondere allen Teilnehmern (nicht nur den Peer-Computer 112.1 bis 112.3) des Peer-to-Peer-Netzwerks 110 einsehbares öffentliches Register 114 sein. Jeder Peer-Computer 112.1 bis 112.3 weist vorzugweise das (gesamte) öffentliche Register 114 auf. Auch kann vorgesehen sein, dass auf einem Peer nur ein Teil des Registers vorgesehen ist. In einer besonders bevorzugten Ausgestaltung kann die Peer-to-Peer-Anwendung 114 eine Blockchain 114 sein.

Ferner ist in der Figur 1 angedeutet, dass ein von der Vorrichtung 102 ausgegebener Datensatz von dem Peer-to-Peer-Netzwerk 110 bzw. der Peer-to-Peer-Anwendung 114 empfangen werden kann. Beispielsweise kann das System 100 ein (nicht gezeigtes) Peer-to-Peer-Modul aufweisen, welches beispielsweise den mit dem Schlüssel versehenen Datensatz von der Vorrichtung 102 empfangen und insbesondere an das Peer-to-Peer-Netzwerk 110 bzw. die Peer-to-Peer-Anwendung 114 zumindest weiterleiten kann.

Vorliegend kann mittels der Peer-to-Peer-Anwendung 124 ein Datenaustauschvorgang von mindestens einem Teil (>1) der Peer-Computer 112.1 bis 112.3, vorzugsweise von sämtlichen Peer-Computern 112.1 bis 112.3, überwacht

werden. Die Peer-to-Peer-Anwendung 114 weist hierfür im vorliegenden Ausführungsbeispiel ein Authentizitätsmodul 116 und ein Schlüsselregister 118 auf.

Das Schlüsselregister 118 ist zumindest auf den drei dargestellten Peer-Computern 112.1 bis 112.3 implementiert. In dem Schlüsselregister 118 sind zumindest die Schlüssel der in dem System 100 registrierten Vorrichtungen 102 gespeichert. Beispielsweise kann für jede registrierte Vorrichtung 102 mindestens ein Challenge-Response-Paar der registrierten Vorrichtung 102 gespeichert sein. Es versteht sich, dass in dem Schlüsselregister 118 weitere Daten der Vorrichtung 102, wie Vorrichtungstyp (Sensor-, Aktor- und/oder Verarbeitungsvorrichtung), Installationsort, Aufgabe, Hersteller, letzte Wartung, Reputationsfaktor, Kommunikationsadresse etc., gespeichert sein können.

Das Authentizitätsmodul 116 ist vorliegend eingerichtet, die Authentizität eines Datensatzes zu überprüfen. Das anmeldungsgemäße System 100 erlaubt hierbei insbesondere eine Überprüfung der Authentizität der in dem Datensatz enthaltenen Daten. Mit anderen Worten kann mit dem Authentizitätsmodul 116 überprüft werden, ob der Datensatz und/oder die darin enthaltenen Daten manipuliert sein könnten.

Um die Authentizität zu prüfen, ist das Authentizitätsmodul 116 zum Überprüfen des bei der Ausgabe des Datensatzes verwendeten Schlüssels basierend auf dem Schlüsselregister 118, insbesondere den in dem Schlüsselregister 118 gespeicherten Schlüsseln, eingerichtet. Vorzugsweise kann die Ausführung des Authentizitätsmoduls 116 automatisch nach einem Empfang eines Datensatzes durch die Peer-to-Peer-Anwendung 114 gestartet werden. Insbesondere wird die Ausführung des Authentizitätsmoduls 116 auf zumindest einem Teil der Peer-Computer 112.1 bis 112.3, also einer Mehrzahl von Peer-Computern 112.1 bis 112.3, zumindest nahezu parallel gestartet. Insbesondere kann jedes Authentizitätsmodul 116 den bei der Ausgabe des Datensatzes verwendeten Schlüssels überprüfen, indem insbesondere ausgewertet wird, ob dieser Schlüssel zu einem der in dem Schlüsselregister 118 gespeicherten Schlüssel korrespondiert. Nur wenn jedes Authentizitätsmodul 116 des

Teils der Peer-Computer 112.1 bis 112.3 zu einem positiven Authentizitätsergebnis gelangt, also eine zuvor beschriebene Korrespondenz feststellt, wird der Datensatz insgesamt als authentisch bzw. echt bewertet. In diesem Fall kann der Datensatz anschließend gespeichert, weiterverarbeitet und/oder weitergeleitet werden. Andernfalls wird die Weiterverarbeitung gesperrt und der Datensatz beispielsweise als nicht ausreichend authentisch gekennzeichnet. Weitere Maßnahmen können folgen.

Die Figur 2 zeigt eine schematische Ansicht eines weiteren Ausführungsbeispiels eines Systems 200 gemäß der vorliegenden Anmeldung. Zur Vermeidung von Wiederholungen werden nachfolgend im Wesentlichen nur die Unterschiede zu dem Ausführungsbeispiel nach Figur 1 beschrieben. Für die anderen Komponenten des Systems 200 wird insbesondere auf die obigen Ausführungen verwiesen.

Das System 200 ist vorliegend zumindest teilweise in einem Fahrzeug 250, insbesondere ein Auto 250, integriert. Insbesondere kann das System 200 zumindest teilweise das Bordnetz 252 des Fahrzeugs 250 bilden. Insbesondere können die anmeldungsgemäßen Vorrichtungen 202.1, 202.2, 202.3 des Systems 200 Bestandteil des Bordnetzes 252 (oder mehrere Bordnetze eines Fahrzeugs) sein.

Eine erste beispielhafte Vorrichtung 202.1 kann eine Sensorvorrichtung 202.1 mit einer Sensoreinrichtung 222, insbesondere einem Messfühler 222, sein. Beispielsweise kann die Vorrichtung 202.1 ein Geschwindigkeitsmesser 202.1 sein. Es versteht sich, dass die nachfolgenden Ausführungen zu einem Geschwindigkeitsmesser 202.1 in einfacher Weise auf andere Sensorvorrichtungen des Fahrzeugs 250 übertragen werden können.

Der Geschwindigkeitsmesser 202.1 kann die Geschwindigkeit des Fahrzeugs 250 erfassen. Diese erfassten Parameterwerte können in Form von Datensätzen bzw. Nachrichten durch eine Ausgabeeinrichtung 206.1 ausgegeben werden. Vorliegend ist in der Ausgabeeinrichtung 206.1eine (zuvor beschriebene) PUF-Einrichtung 204 und

insbesondere eine Signierungseinrichtung 232 integriert. Die Signierungseinrichtung 232 ist eingerichtet, insbesondere jeden ausgegebenen Datensatz zu signieren. Hierzu wird der PUF-Schlüssel von der PUF-Einrichtung 204 der Signierungseinrichtung 232 (z.B. Message Authentication Einrichtung) zur Verfügung gestellt.

Der Datensatz kann vorliegend über ein internes Kommunikationsnetz 208.1 an eine Verarbeitungsvorrichtung 202.3, beispielsweise eine Motorsteuerung 202.3 (ECU), gesendet werden. Es versteht sich, dass die nachfolgenden Ausführungen zu einer Motorsteuerung 202.3 in einfacher Weise auf andere Verarbeitungsvorrichtungen des Fahrzeugs 250 übertragen werden können.

Ferner ist beispielhaft eine Aktorvorrichtung 202.2 dargestellt. Die Aktorvorrichtung 202.2 weist eine Aktoreinrichtung 224 auf, um ein aktuierbares Element 226 entsprechend einem bereitgestellten Befehlsdatensatz und/oder -signal zu verfahren. Das Befehlssignal und/oder Befehlsdatensatz kann beispielsweise über das interne Kommunikationsnetz 208.1 empfangen werden. Beispielsweise kann eine Sende-/Empfangseinrichtung 236 der Motorsteuerung 202.3 einen entsprechenden Befehlsdatensatz aussenden. Auch dieser Befehlsdatensatz kann mittels einer PUF-Einrichtung 204 mit einem Schlüssel versehen sein.

Auch kann die Aktorvorrichtung 202.2 Datensätze, wie Zustandsdatensätze, insbesondere an die Motorsteuerung 202.3 ausgeben. Hierzu weist die Aktorvorrichtung 202.2 eine Ausgabeeinrichtung 206.2, eine PUF-Einrichtung 204 und beispielhaft eine Verschlüsselungseinrichtung 230 auf. Die Verschlüsselungseinrichtung 230 ist zum Verschlüsseln des ausgegebenen Datensatzes unter Verwendung des der Vorrichtung 202.2 eindeutig zugeordneten PUF-Schlüssels eingerichtet. Es versteht sich, dass alternativ oder zusätzlich eine zuvor beschriebene Signierungseinrichtung 232 vorgesehen sein kann. Verschlüsselungseinrichtung 230 und PUF-Einrichtung 204 sind vorzugsweise in der Ausgabeeinrichtung 206.2 integriert. Hierbei kann die Ausgabeeinrichtung 206.2 insbesondere eine Sende-/Empfangseinrichtung sein.

Die Motorsteuerung 202.3 kann über eine weitere Ausgabeeinrichtung 206 verfügen. Die weitere Ausgabeeinrichtung 206 der Motorsteuerung 202.3 kann insbesondere als Peer-to-Peer-Modul 240 mit einer PUF-Einrichtung 204 gebildet sein. Das Peer-to-Peer-Modul 240 ist der Motorsteuerung 202.3 zugeordnet. Insbesondere ist im vorliegenden Ausführungsbeispiel das Peer-to-Peer-Modul 240 in der Motorsteuerung 202.3 integriert.

Ein Peer-to-Peer-Modul 240 ist vorliegend dazu eingerichtet, zumindest mit dem Peer-to-Peer-Netzwerk 210, also der Mehrzahl von Peer-Computern 212.1, 212.2 (vorliegend sind zu Gunsten einer besseren Übersicht nur zwei dargestellt) des Peer-to-Peer-Netzwerks 210, zu kommunizieren. Mit anderen Worten ist ein Peer-to-Peer-Modul 240 bzw. die zu diesem Peer-to-Peer-Modul 240 korrespondierende Vorrichtung 202.3 zumindest Teilnehmer des Peer-to-Peer-Netzwerks 210. Hierbei sind jedem Teilnehmer des Peer-to-Peer-Netzwerks 210 vorzugsweise sämtliche Teilnehmer des Peer-to-Peer-Netzwerks 210 bekannt.

Beispielsweise kann das Peer-to-Peer-Modul 240 einen von dem Geschwindigkeitsmesser 202.1 erhaltenen Sensordatensatz an die Peer-to-Peer-Anwendung 214 senden. Der Sensordatensatz ist mit dem PUF-Schlüssel des Geschwindigkeitsmessers 202.1 versehen. Vorliegend ist der Sensordatensatz insbesondere entsprechend signiert. Dieser Sensordatensatz umfassend den PUF-Schlüssel des Geschwindigkeitsmessers 202.1 wird von dem Peer-to-Peer-Modul 240 der Motorsteuerung 202.3 in Form eines weiteren Datensatzes, der zusätzlich mit dem PUF-Schlüssels der Motorsteuerung 202.3 versehen wird, an die Peer-to-Peer-Anwendung 214 gesendet.

In einer bevorzugten (nicht dargestellten) Ausführungsform kann das Peer-to-Peer-Modul 240 mit einer Kommunikationsvorrichtung zu einer Fahrzeug-internen oder Fahrzeug-externen Peer-to-Peer-Anwendung 214 eingerichtet. Bespiele sind ECU der

Fahrzeugsteuerung, ECU der Motorsteuerung, ECU des Entertainmentsystems, Telematics-Vorrichtung, eCall-Vorrichtung oder OBD-Vorrichtung, u,a..

Hierbei sei angemerkt, dass die Motorsteuerung 202.3 über eine Verarbeitungseinrichtung 234 (z.B. Prozessor, Mikrocontroller etc.) verfügt, um erhaltene Daten zu verarbeiten und beispielsweise entsprechend den vorherigen Ausführungen auszugeben. So können beispielsweise die Sensordaten verarbeitet werden, um einen Befehlsdatensatz zu generieren.

Wie ferner zu erkennen ist, ist vorliegend eine Datenspeicheranordnung 242 vorgesehen. Vorzugsweise kann die Datenspeicheranordnung 242, die eine Vielzahl von (nicht gezeigten) dezentralen Speichereinheiten umfassen kann, ein dezentrales Datenbanksystem (wie z. B. IPFS) oder ein dezentraler Objektspeicher (wie z.B. storj) oder eine dezentrale verteilte Datenbank (wie BigchainDB) sein, das/der/die von der Peer-to-Peer-Anwendung 214, insbesondere durch ein Steuermodul 217, gesteuert und/oder verwaltet wird. Das Steuermodul 217 kann insbesondere zum Steuern und/oder Kontrollieren des Zugriffs auf die Datenspeicheranordnung 242 eingerichtet sein.

Insbesondere nach einem Empfang eines Datensatzes durch die Peer-to-Peer-Anwendung 214 kann der eine oder die mehreren Schlüssel des Datensatzes in zuvor beschriebener Weise überprüft werden.

Bei einer besonderen Variante eines Fahrzeugsystems gemäß der vorliegenden Anmeldung kann zumindest ein Teil der Vorrichtungen des Bordnetzes ein internes Peer-to-Peer-Netzwerk bilden. Dieses interne Peer-to-Peer-Netzwerk kann mit dem dargestellten externen Peer-to-Peer-Netzwerk 210 verbunden sein. Beispielsweise kann die Motorsteuerung 202.3 sowohl ein Peer-Computer des internen Peer-to-Peer-Netzwerks als auch des externen Peer-to-Peer-Netzwerks 210 sein.

Die Figur 3 zeigt eine schematische Ansicht eines weiteren Ausführungsbeispiels eines Systems 300 gemäß der vorliegenden Anmeldung. Zur Vermeidung von Wiederholungen werden nachfolgend im Wesentlichen nur die Unterschiede zu den Ausführungsbeispielen nach Figur 1 und 2 beschrieben. Für die anderen Komponenten des Systems 300 wird insbesondere auf die obigen Ausführungen verwiesen. Zudem wurde zu Gunsten einer besseren Übersicht das Peer-to-Peer-Netzwerk mit nur einem Peer-Computer 312 dargestellt. Es versteht sich, dass eine Mehrzahl von Peer-Computern vorgesehen sein kann.

Im vorliegenden Ausführungsbeispiel ist das System 300 zumindest teilweise in einem Gebäude 354 integriert. Insbesondere kann das System 300 zumindest teilweise durch die Vorrichtungen 302.1, 302.2, 302.3 eines Hausautomationsnetzes 356 gebildet sein.

Die beispielhaft dargestellten Vorrichtungen 302.1, 302.2, 302.3 umfassen insbesondere eine Sensorvorrichtung 302.1, beispielsweise einen Temperatursensor zur Erfassung einer Raumtemperatur, eine Aktoreinrichtung 302.2, beispielsweise eingerichtet zum Verfahren eines Ventils 326 einer Heizungsanlage, und eine Verarbeitungsvorrichtung 302.3, beispielsweise einen Hausautomationscontroller 302.3.

In zuvor beschriebener Weise (siehe insbesondere Fig. 2) können Datensätze ausgegeben und/oder empfangen werden. Ferner kann insbesondere nach einem Empfang eines Datensatzes durch die Peer-to-Peer-Anwendung 314 der eine oder die mehreren Schlüssel des Datensatzes in zuvor beschriebener Weise überprüft werden.

Darüber hinaus umfasst im vorliegenden Ausführungsbeispiel das System 300 eine durch die Peer-to-Peer-Anwendung 314 gesteuerte Offchain-Rechenvorrichtung 358. Eine derartige Off -Chain-Rechenvorrichtung 358 kann ein Rechenmodul 360 zur Ausführung von Algorithmen, kognitiver Analytik, maschinellem Lernen und/oder

künstlicher Intelligenz (KI) bereitstellen, um beispielsweise den Austauschvorgang und/oder Prozesse des Hausautomationsnetzes 356 zu optimieren.

Auch kann ein (nicht gezeigtes) Authentifizierungsgerät (z.B. Handgerät) mit einem weiteren Authentizitätsmodul und einem weiteren Schlüsselregister vorgesehen sein, um bei einem Netzwerkfehler die Überprüfung von ausgegebenen Datensätzen zu übernehmen. Ein solches Gerät kann mit dem Peer-to-Peer-Netzwerk verbunden sein. Benötigte CPRs oder Bitsrings können dann im On-line Fall automatisch auf dieses Authentifizierungsgerät synchronisiert werden. Diese Synchronisation kann über ein Registry auf der Peer-to-Peer-Anwendung gesteuert werden.

Figur 4 zeigt eine schematische Ansicht eines Ausführungsbeispiels einer Peer-to-Peer-Anwendung 414 gemäß der vorliegenden Anmeldung. Die Peer-to-Peer-Anwendung 414 ist insbesondere ein für die Teilnehmer eines Peer-to-Peer-Netzwerks einsehbares bzw. lesbares Register, in welches Nachrichten/Datensätze von Vorrichtungen bzw. Teilnehmern des Peer-to-Peer-Netzwerks geschrieben und/oder aus dem Nachrichten/Datensätze ausgelesen werden können. Bei einem bevorzugten Ausführungsbeispiel kann die Peer-to-Peer-Anwendung 414 eine Blockchain 414 sein.

Nachfolgend wird bei der näheren Beschreibung des vorliegenden Ausführungsbeispiels davon ausgegangen, dass es sich bei der Peer-to-Peer-Anwendung 414 um eine Blockchain 414 handelt. Jedoch lassen sich die nachfolgenden Ausführungen problemlos auf andere Peer-to-Peer-Anwendungen übertragen.

Die Blockchain 414 wird aus mindestens einem Block 451 bis 455, vorzugsweise einer Vielzahl von miteinander verknüpften Blöcken 451 bis 455, gebildet. Der erste Block 451 kann auch Genesis-Block 451 genannt werden. Wie zu erkennen ist, bezieht sich ein Block 453, 455 (außer dem ersten Block 451) auf den jeweils vorherigen Block 451, 453. Ein neuer Block kann durch einen rechenintensiven Prozess (zum Beispiel

so genanntes „Mining" oder durch einen entsprechenden Prozess) erschaffen werden und insbesondere allen Teilnehmern des Peer-to-Peer-Netzwerks bereitgestellt werden.

Die vorliegende Blockchain 414 ist insbesondere dazu eingerichtet Nachrichten bzw. Datensätze von einem Peer-to-Peer Modul eines Teilnehmers des Peer-to-Peer-Netzwerks, wie einem Peer-to-Peer-Modul einer zuvor beschriebenen Vorrichtung, zu empfangen und diese Nachricht bzw. diesen Datensatz in der Blockchain 414 zu speichern. Insbesondere kann eine neue Nachricht in dem aktuellen Block 455 der Blockchain 414 gespeichert und veröffentlicht werden. Aufgrund der Ausgestaltung einer Blockchain 414 als öffentliches Register 414, kann die Nachricht eines Peer-to-Peer Moduls von bevorzugt sämtlichen Teilnehmern des Peer-to-Peer-Netzwerks gelesen und somit insbesondere überprüft werden.

In der vorliegenden Blockchain 414 können unterschiedliche Arten von Nachrichten bzw. Datensätze, beispielsweise innerhalb eines Smart Contracts (Algorithmus und/oder Speicher auf der Blockchain) (und/oder außerhalb der Blockchain 414), verarbeitet und/oder gespeichert werden. Wie bereits beschrieben wurde, kann die Blockchain 414 ein Authentizitätsmodul 416 umfassen. Das Authentizitätsmodul 416 ist insbesondere ein Softwaremodul in Form eines Smart Contracts, der von dem jeweiligen Computer-Peer ausführbar ist. Die Ausführung kann insbesondere nach Erhalt eines Datensatzes gestartet und entsprechend den obigen Ausführungen durchgeführt werden. Alternativ kann ein solches Modul auch in einer vertrauenswürdige Ausführungsumgebung eingerichtet sein, die über ein Peer-to-Peer Modul an die Peer-to-Peer Anwendung angeschlossen und insbesondere von dieser steuerbar sein kann.

Neben einem Authentizitätsmodul 416 kann die Blockchain 414 ein Schlüsselregister 418 (auch CPR-Register genannt) und/oder ein Steuermodul 417 zum Steuern des Zugriffs auf ein Schlüsselregister, das durch eine Offchain-Datenspeicheranordnung bereitgestellt wird, verfügen, wie zuvor beschrieben wurde.

Darüber hinaus ist vorliegend ein Registermodul 460 vorgesehen. Das Registermodul 460 ist zum Registrieren einer Vorrichtung in dem Schlüsselregister 418 zumindest durch Speichern des der Vorrichtung eindeutig zugeordneten Schlüssels (und/oder mehrerer CPRs) eingerichtet ist. Ein Registrierungsprozess kann das Durchführen eines Kommunikationstests sowie die Überprüfung weiterer, vorgebbarer Registrierungsregeln umfassen.

Ein Registrierungsprozess kann auch das Anlegen eines (dezentralen) Digitalen Produktgedächtnisses bewirken. Zudem können in dem Registrierungsprozess Einzel-Komponenten einem zugehörigen System (z.B. Auto, Gebäude, Netz) zugeordnet werden (z.B. Registrierung der Komponenten in einem Konfigurationsbaum). Damit kann die Identität einzelner Vorrichtungen z.B. zu der Identität eines Fahrzeuges zugordnet werden.

Ferner kann eine Peer-to-Peer-Anwendung 414 grundsätzlich zur Generierung von (nicht gezeigten) Datensatzaustauschvorgangsvereinbarungsmodulen eingerichtet sein. In einem Datensatzaustauschvorgangsvereinbarungsmodul kann beispielsweise festgelegt sein, welche Bedingungen für einen zulässigen Datensatzaustausch zu erfüllen sind und zwischen welchen Entitäten (z.B. Fahrzeug eines Nutzers, Versicherungsanbieter) ein Austausch erfolgen kann. Hierzu können die Entitäten, beispielsweise ein Peer-to-Peer-Modul einer Entität, die Generierung eines Datensatzaustauschvorgangsvereinbarungsmodul initiieren. Basierend auf den in dem Datensatzaustauschvorgangsvereinbarungsmodul generierten und gespeicherten Datenelementen kann anschließend der Austauschvorgang durchgeführt werden. Die Generierung kann insbesondere durch Senden mindestens einer Anfragenachricht an die Peer-to-Peer-Anwendung 414 initiiert werden.

Eine Anfragenachricht kann beispielsweise Kennung/en der involvierten Entität/en, mindestens ein Austauschkriterium, welches während oder nach dem Austauschvorgang erfüllt oder eingehalten werden muss, und/oder Angaben über den

Dateninhalt umfassen. Es versteht sich, dass eine Anfragenachricht weniger Datenelemente oder mehr Datenelemente aufweisen kann.

Ferner kann/können mindestens ein Austauschkriterium, vorzugsweise mehrere Austauschkriterien, angegeben sein. Beispielsweise kann als Austauschkriterium ein Transaktionskriterium angegeben sein. Hierbei kann es sich um ein Kriterium handeln, welches von einer Entität erfüllt werden muss, um ein Datensatzaustauschvorgangsvereinbarungsmodul zu generieren. Beispielsweise kann das Transaktionskriterium eine Tokenmenge (die einem bestimmten Geldwert entsprechen kann) angeben, die eine weitere Entität für den Empfang der Daten entrichten muss.

Es versteht sich, dass anderen Austauschkriterien festgelegt sein können. Weitere Angaben können beispielsweise ein Zeitstempel, eine Kennung der Nachricht und weitere Transaktionskriterien, wie eine Angabe über die gewünschte Datenart etc., sein.

Eine weitere Nachricht kann eine Annahmenachricht sein. Die Annahmenachricht kann von einem weiteren Peer-to-Peer-Modul der weiteren Entität generiert und insbesondere an die Peer-to-Peer-Anmeldung 414 übertragen werden. Dies kann insbesondere nach einem Lesen der Anfragenachricht erfolgen.

Eine Annahmenachricht kann gleiche oder zumindest ähnliche Datenelemente wie eine zugehörige Anfragenachricht aufweisen. Zusätzlich kann die Annahmenachricht beispielsweise eine Bezugsangabe auf eine vorherige Anfrage, wie die Kennung der Anfragenachricht, umfassen.

Auch können Anfragenachrichten und/oder Annahmenachrichten direkt zwischen den Entitäten ausgetauscht werden. Vorzugsweise über ein Peer-to-Peer-Kommunikationsprotokoll.

Bei dem Austauschkriterium kann in einer Annahmenachricht ein geringeres/höheres Transaktionskriterium angegeben sein. Falls eine Annahmenachricht ein geringeres/höheres/anderes Transaktionskriterium oder dergleichen umfasst, kann die Annahmenachricht als Gegenangebotsnachricht bezeichnet werden. Diese kann von der ersten Entität durch eine weitere Annahmenachricht angenommen werden. Basierend hierauf kann mindestens ein Peer-to-Peer-Modul die Generierung eines Datensatzaustauschvorgangsvereinbarungsmodul durch die Peer-to-Peer-Anwendung veranlassen.

Insbesondere kann es mehrere Anfragenachrichten und/oder Annahmenachrichten geben. Jede Entität kann Vorgaben geben, nach denen mindestens ein Datensatzaustauschvorgangsvereinbarungsmodul generiert werden kann. In einem vorzugsweise automatischen, beispielsweise iterativen, Prozess kann vorzugsweise jeder Anfragenachricht eine möglichst optimal korrespondierende Annahmenachricht zugeordnet werden.

Ein (nicht gezeigtes) Datensatzaustauschvorgangsvereinbarungsmodul kann innerhalb eines Smart Contracts in einem Block gespeichert sein.

Ein Smart-Contract kann vorliegend Computerprogrammcode (kurz Code) umfassen. In dem Datensatzaustauschvorgangsvereinbarungsmodul kann insbesondere der Austausch von Datensätzen zwischen den zumindest zwei Entitäten vereinbart sein.

Insbesondere ist die Peer-to-Peer-Anwendung 414 dazu eingerichtet, die gespeicherten Datensätze/Nachrichten in manipulationssicherer Weise zu speichern. Dies erfolgt im Wesentlichen dadurch, dass durch das gesamte Peer-to-Peer-Netzwerk zum Beispiel ein Datensatzaustauschvorgangsvereinbarungsmodul durch die kumulierte Rechenleistung des gesamten Peer-to-Peer-Netzwerks verifiziert werden kann.

Vorzugsweise können zumindest die zuvor beschriebenen Nachrichten/Datensätze in einem Block 453, 455 der Blockchain 424 durch einen Merkle-Baum paarweise miteinander gehasht werden. Insbesondere kann nur der letzte Hashwert, der so genannte Root-Hash, als Prüfsumme in dem Header eines Blocks vermerkt werden. Dann kann der Block mit dem vorherigen Block verkettet werden. Das Verketten der Blöcke kann mithilfe dieses Root-Hashes durchgeführt werden. Jeder Block kann im Header den Hash des gesamten vorherigen Blockheaders umfassen. Dies erlaubt es, die Reihenfolge der Blöcke eindeutig festzulegen. Außerdem kann dadurch auch das nachträgliche Modifizieren vorangegangener Blöcke bzw. der in den vorherigen Blöcken gespeicherten Nachrichten (praktisch) ausgeschlossen werden, da insbesondere die Hashes aller nachfolgenden Blöcke in kurzer Zeit ebenfalls neu berechnet werden müssten.

Es versteht sich, dass die zuvor genannten Module/Datensätze etc. zumindest teilweise auch miteinander kombiniert werden können. Auch versteht es sich, dass zumindest teilweise die Daten in einer zuvor beschriebenen Datenspeicheranordnung gespeichert werden können.

Auch kann anstelle einer linearen Blockchain ein DAG tangle oder eine Blockchain Datenbank oder ein Lightning oder State Channel Netzwerk oder eine Blockchain Integrationstechnologie, wie Interledger Protocol oder eine Kombination der genannten Peer-to-Peer Technologien, zum Einsatz kommen.

Figur 5 zeigt eine schematische Ansicht eines weiteren Ausführungsbeispiels eines Systems 500 gemäß der vorliegenden Anmeldung. Zur Vermeidung von Wiederholungen werden nachfolgend im Wesentlichen nur die Unterschiede zu den Ausführungsbeispielen nach Figur 1, 2 und 3 beschrieben.

Das stark vereinfacht dargestellte System 500 umfasst vorliegend sieben Entitäten 502.1, 502.2, 512.1, 512.2 die insbesondere Peer-Computer eines Peer-to-Peer-Netzwerkes 510 umfassen und/oder diese bilden. Jeder Peer-Computer kann eine

(nicht dargestellte) Peer-to-Peer-Anwendung, z.B. die Blockchain 414 gemäß Figur 4, bereitstellen bzw. umfassen.

Vorliegend sind Peer-Computer durch Vorrichtungen 502.1, 502.2, beispielsweise Sensorvorrichtungen, und durch Recheneinrichtungen 512.1, 512.2 gebildet.

Ferner sind vorliegend insbesondere zwei unterschiedliche Arten von Peer-Computern bzw. Knotenrechnern 502.1, 512.1 bzw. 502.2, 512.2 dargestellt. Sämtliche Peer-Computer 502.1 bis 512.2 sind von dem Peer-to-Peer-Netzwerk 510 umfasst. Beim vorliegenden Ausführungsbeispiel überprüft jedoch nur ein Teil der Peer-Computer 502.1 bis 512.2, vorliegend die Peer-Computer 502.1, 512.1 die Validität eines empfangenen Datensatzes anhand des mindestens einen verwendeten Schlüssels und der gespeicherten, zulässigen Schlüssel. Insbesondere ist nur ein Teil der Peer-Computer 502.1, 512.1 eingerichtet, das (nicht gezeigte) Authentizitätsmodul auszuführen.

Auch kann vorgesehen sein, dass nur ein Teil der Peer-Computer die gesamte Peer-to-Peer-Anwendung speichert und/oder nur ein Teil der Peer-Computer die Algorithmen der (weiteren) Smart Contracts ausführt. Da mit der Validierung/Überprüfung ein erheblicher Rechenaufwand einhergehen kann, kann es aus Effizienzgründen von Vorteil sein, wenn nur ein Teil der Peer-Computer 502.1, 512.1, insbesondere besonders leistungsstarke Peer-Computer 502.1, 512.1, die Validierung bzw. Überprüfung der Datensätze vornehmen. Leistungsstark meint insbesondere eine hohe Rechenleistung. Mit anderen Worten wird vorliegend von einem validen Datensatz in der Peer-to-Peer-Anwendung, wie einer Blockchain, ausgegangen, wenn (nur) ein Teil der Peer-Computer 502.1, 512.1 zu einem positiven Ergebnis eines Überprüfungsvorgangs gelangt ist. Es versteht sich, dass auch nur ein einzelner, insbesondere besonders leistungsstarker Peer, die Validierung durchführen kann. In diesem Fall können die anderen Peer-Computer als Beobachtungs-Computer ausgeführt sein, die eingerichtet sind, zumindest die Korrektheit des Überprüfungsprozesses zu bestätigen.

Ebenso kann bei einer alternativen (nicht gezeigten) Ausführungsform vorgesehen sein, dass ein insbesondere großes Peer-to-Peer-Netzwerk in zwei oder mehr Cluster aufgeteilt sein kann. Bei einem entsprechenden Peer-to-Peer-Netzwerk kann beispielsweise eine Validierung nur von den Mitgliedern eines Clusters durchgeführt werden.

Weiterhin kann bei einer (nicht gezeigten) Ausführungsform vorgesehen sein, dass eine Steuervorrichtung des Anbieters, Nutzers von Flottenbetreibern, Fahrzeugherstellern, Gebäudeverwaltern oder des Netzbetreibers oder zentrale Steuerungssysteme für Austauschmodulinfrastrukturen mit dem Peer-to-Peer Netzwerk verbunden sind.

Die Figur 6 zeigt ein Diagramm eines Ausführungsbeispiels eines Verfahrens gemäß der vorliegenden Anmeldung. In einem ersten Schritt 601 kann, beispielsweise entsprechend den vorherigen Ausführungen (siehe z.B. Figur 2, 3 und/oder 4), ein zuvor generierter Datensatz mit einem PUF-Schlüssel versehen werden. Hierzu kann die PUF-Einrichtung den PUF-Schlüssel abhängig von einer Challenge generieren. Beispielsweise kann der Datensatz mit dem PUF-Schlüssel signiert werden. Dieser Datensatz wird dann in Schritt 601 ausgegeben, insbesondere durch eine Ausgabeeinrichtung der Vorrichtung, zu dem der PUF-Schlüssel eindeutig zugeordnet ist, ausgesendet.

Vor einer erstmaligen Ausgabe eines Datensatzes kann ein (nicht dargestellter) Registrierungsschritt durchgeführt werden, um die Vorrichtung in dem anmeldungsgemäßen System zu registrieren.

In Schritt 602 wird eine Peer-to-Peer-Anwendung eines Peer-to-Peer-Netzwerks bereitgestellt. In Schritt 603 wird ein zumindest von der Peer-to-Peer-Anwendung steuerbares Schlüsselregisters, eingerichtet zumindest zum Speichern des der Vorrichtung eindeutig zugeordneten Schlüssels, bereitgestellt.

Dann wird, insbesondere nach einem Empfang eines Datensatzes durch die Peer-to-Peer-Anwendung dieser Datensatz überprüft. Insbesondere wird der ausgegebene und durch die Peer-to-Peer-Anwendung empfangene Datensatz durch Ausführen mindestens eines Authentizitätsmoduls durch mindestens einen Teil der Peer-Computer des Peer-to-Peer-Netzwerks überprüft. Das Überprüfen umfasst insbesondere das Auswerten des bei der Ausgabe des Datensatzes verwendeten Schlüssels basierend auf dem Schlüsselregister (wie zuvor beschrieben wurde).

Patentansprüche

1. System (100, 200, 300, 500), umfassend:
   - mindestens eine Vorrichtung (102, 202, 302) mit mindestens einer Ausgabeeinrichtung (106, 206, 306), eingerichtet zum Ausgeben von mindestens einem Datensatz, und mit mindestens einer PUF-Einrichtung (104, 204, 304), eingerichtet zum Erzeugen mindestens eines der Vorrichtung (102, 202, 302) eindeutig zugeordneten Schlüssels,
   - wobei der Schlüssel beim Ausgeben des Datensatzes verwendet wird,
   - mindestens ein Peer-to-Peer-Netzwerks (110, 210, 310, 510), umfassend mindestens eine Peer-to-Peer-Anwendung (114, 214, 314, 414), und
   - mindestens ein von der Peer-to-Peer-Anwendung (114, 214, 314, 414) zumindest gesteuertes Schlüsselregister (118, 218, 318, 418), eingerichtet zumindest zum Speichern des der Vorrichtung (102, 202, 302) eindeutig zugeordneten Schlüssels,
   - wobei die Peer-to-Peer-Anwendung (114, 214, 314, 414) mindestens ein von mindestens einem Teil der Peer-Computer (112, 212, 312, 502, 512, 564) des Peer-to-Peer-Netzwerks (110, 210, 310, 510) ausführbares Authentizitätsmodul (116, 216, 316, 416) umfasst, und
   - wobei das Authentizitätsmodul (116, 216, 316, 416) zum Überprüfen des bei der Ausgabe des Datensatzes verwendeten Schlüssels basierend auf dem Schlüsselregister (118, 218, 318, 418) nach Empfang des Datensatzes durch die Peer-to-Peer-Anwendung (114, 214, 314, 414) eingerichtet ist.

2. System (100, 200, 300, 500) nach Anspruch 1, **dadurch gekennzeichnet, dass** die Vorrichtung (102, 202, 302) gebildet ist als:
   - Sensorvorrichtung (202.1, 302.1) mit mindestens einer Sensoreinrichtung (222, 322), eingerichtet zum Erfassen von mindestens einem Parameter,

wobei der ausgegebene Datensatz insbesondere zumindest den erfassten Parameterwert umfasst,

und/oder

- Aktorvorrichtung (202.2, 302.2) mit mindestens einer Aktoreinrichtung (224, 324), eingerichtet zum Verfahren eines aktuierbaren Elements (226, 326), wobei der ausgegebene Datensatz insbesondere zumindest einen Zustand der Aktoreinrichtung (224, 324) und/oder des aktuierbaren Elements (226, 326) umfasst,

und/oder

- Verarbeitungsvorrichtung (202.3, 302.3) mit mindestens einer Verarbeitungseinrichtung (234, 334), eingerichtet zum Verarbeiten von empfangbaren Daten, wobei der ausgegebene Datensatz insbesondere zumindest die verarbeiteten Daten umfasst.

3. System (100, 200, 300, 500) nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass**

- das System (100, 200, 300, 500) mindestens ein Peer-to-Peer-Modul (240, 340) umfasst,
- wobei das Peer-to-Peer-Modul (240, 340) zumindest zum Übertragen des den Schlüssel verwendeten Datensatzes an die Peer-to-Peer-Anwendung (114, 214, 314, 414) eingerichtet ist.

4. System (100, 200, 300, 500) nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet, dass**

- die Vorrichtung (102, 202, 302) mindestens eine Signierungseinrichtung (232) umfasst,
- wobei die Signierungseinrichtung (232) zum Signieren des ausgegebenen Datensatzes unter Verwendung des der Vorrichtung (102, 202, 302) eindeutig zugeordneten Schlüssels eingerichtet ist.

5. System (100, 200, 300, 500) nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet, dass**
   - die Vorrichtung (102, 202, 302) mindestens eine Verschlüsselungseinrichtung (230) umfasst,
   - wobei die Verschlüsselungseinrichtung (230) zum Verschlüsseln des ausgegebenen Datensatzes unter Verwendung des der Vorrichtung (102, 202, 302) eindeutig zugeordneten Schlüssels eingerichtet ist.

6. System (100, 200, 300, 500) nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet, dass**
   - die Peer-to-Peer-Anwendung (114, 214, 314, 414) mindestens ein Registermodul (460) umfasst,
   - wobei das Registermodul (460) zum Registrieren einer Vorrichtung (102, 202, 302) in dem Schlüsselregister (118, 218, 318, 418) zumindest durch Speichern des der Vorrichtung (102, 202, 302) eindeutig zugeordneten Schlüssels eingerichtet ist.

7. System (100, 200, 300, 500) nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet, dass**
   - das System (100, 200, 300, 500) zumindest teilweise in einem Fahrzeug (350) integriert ist,

   oder
   - das System (100, 200, 300, 500) zumindest teilweise in einem Hausautomationssystem (354) integriert ist.

8. System (100, 200, 300, 500) nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass
   - die Peer-to-Peer-Anwendung (114, 214, 314, 414) ein dezentrales Register oder eine verteilte Datenbank ist, und
   - die Peer-to-Peer-Anwendung (114, 214, 314, 414) insbesondere eine Blockchain oder eine dezentrale Ledger ist.

9. Verfahren, umfassend:

- Ausgeben von mindestens einem Datensatz durch eine Ausgabeeinrichtung (106, 206, 306) einer Vorrichtung (102, 202, 302) unter Verwendung mindestens eines der Vorrichtung (102, 202, 302) zugeordneten Schlüssels,
- wobei der Schlüssel durch mindestens eine in der Vorrichtung (102, 202, 302) integrierte PUF-Einrichtung (104, 204, 304) erzeugt wird,
- Bereitstellen einer Peer-to-Peer-Anwendung (114, 214, 314, 414) eines Peer-to-Peer-Netzwerks (110, 210, 310, 510),
- Bereitstellen eines zumindest von der Peer-to-Peer-Anwendung (114, 214, 314, 414) gesteuerten Schlüsselregisters (118, 218, 318, 418), eingerichtet zumindest zum Speichern des der Vorrichtung (102, 202, 302) eindeutig zugeordneten Schlüssels, und
- Überprüfen des ausgegebenen und durch die Peer-to-Peer-Anwendung (114, 214, 314, 414) empfangenen Datensatzes durch Ausführen mindestens eines Authentizitätsmoduls (116, 216, 316, 416) durch mindestens einen Teil der Peer-Computer (112, 212, 312, 502, 512, 564) des Peer-to-Peer-Netzwerks (110, 210, 310, 510),
- wobei das Überprüfen das Auswerten des bei der Ausgabe des Datensatzes verwendeten Schlüssels basierend auf dem Schlüsselregister (118, 218, 318, 418) umfasst.

10. Vorrichtung (102, 202, 302), umfassend:

- mindestens eine Ausgabeeinrichtung (106, 206, 306), eingerichtet zum Ausgeben von mindestens einem Datensatz,
- mindestens eine PUF-Einrichtung (104, 204, 304), eingerichtet zum Erzeugen mindestens eines der Vorrichtung (102, 202, 302) eindeutig zugeordneten Schlüssels,
- wobei der Schlüssel beim Ausgeben des Datensatzes verwendet wird,
- wobei die Ausgabeeinrichtung (106, 206, 306) durch ein Peer-to-Peer-Modul (240, 340) gebildet ist, eingerichtet zumindest zum Übertragen des den

Schlüssel verwendeten Datensatzes an eine Peer-to-Peer-Anwendung (114, 214, 314, 414) eines Peer-to-Peer-Netzwerks (110, 210, 310, 410), derart, dass mindestens ein von mindestens einem Teil der Peer-Computer (112, 212, 312, 502, 512, 564) des Peer-to-Peer-Netzwerks (110, 210, 310, 410) ausführbares Authentizitätsmodul (116, 216, 316, 416) der Peer-to-Peer-Anwendung (114, 214, 314, 414) den bei der Ausgabe des Datensatzes verwendeten Schlüssels basierend auf einem Schlüssel speichernden Schlüsselregisters (118, 218, 318, 418) überprüft.

11. Peer-to-Peer-Anwendung (114, 214, 314, 414) für ein Peer-to-Peer-Netzwerk (110, 210, 310, 510), umfassend:

- mindestens ein von mindestens einem Teil der Peer-Computer (112, 212, 312, 502, 512, 564) des Peer-to-Peer-Netzwerks (110, 210, 310, 510) ausführbares Authentizitätsmodul (116, 216, 316, 416), eingerichtet zum Überprüfen eines durch die Peer-to-Peer-Anwendung (114, 214, 314, 414) empfangenen und unter Verwendung eines durch eine PUF-Einrichtung (104, 204, 304) erzeugten Schlüssels durch eine Vorrichtung (102, 202, 302) ausgegebenen Datensatzes,
- wobei das Überprüfen ein Auswerten des bei der Ausgabe des Datensatzes verwendeten Schlüssels basierend auf einem von der Peer-to-Peer-Anwendung (114, 214, 314, 414) zumindest gesteuerten Schlüsselregister (118, 218, 318, 418), eingerichtet zumindest zum Speichern des der Vorrichtung (102, 202, 302) eindeutig zugeordneten Schlüssels, umfasst.

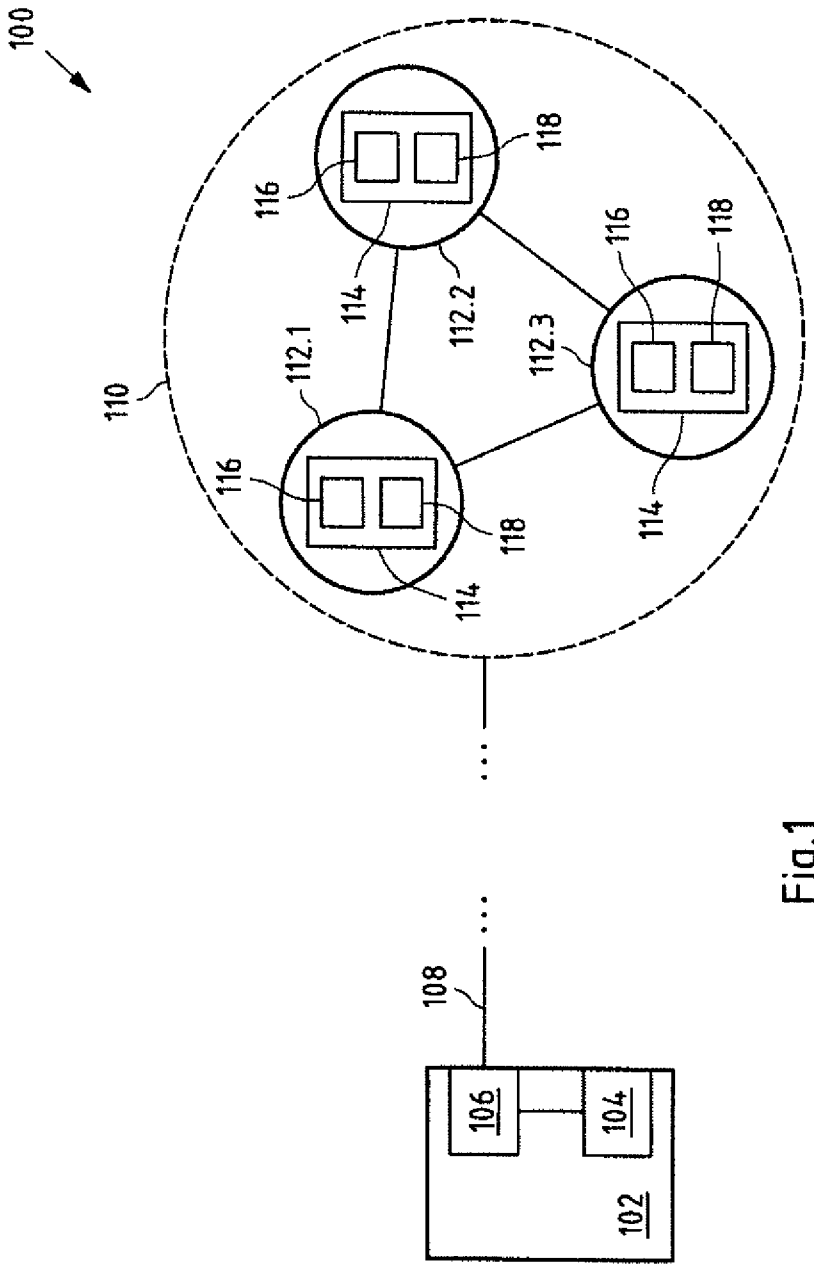


Fig.1

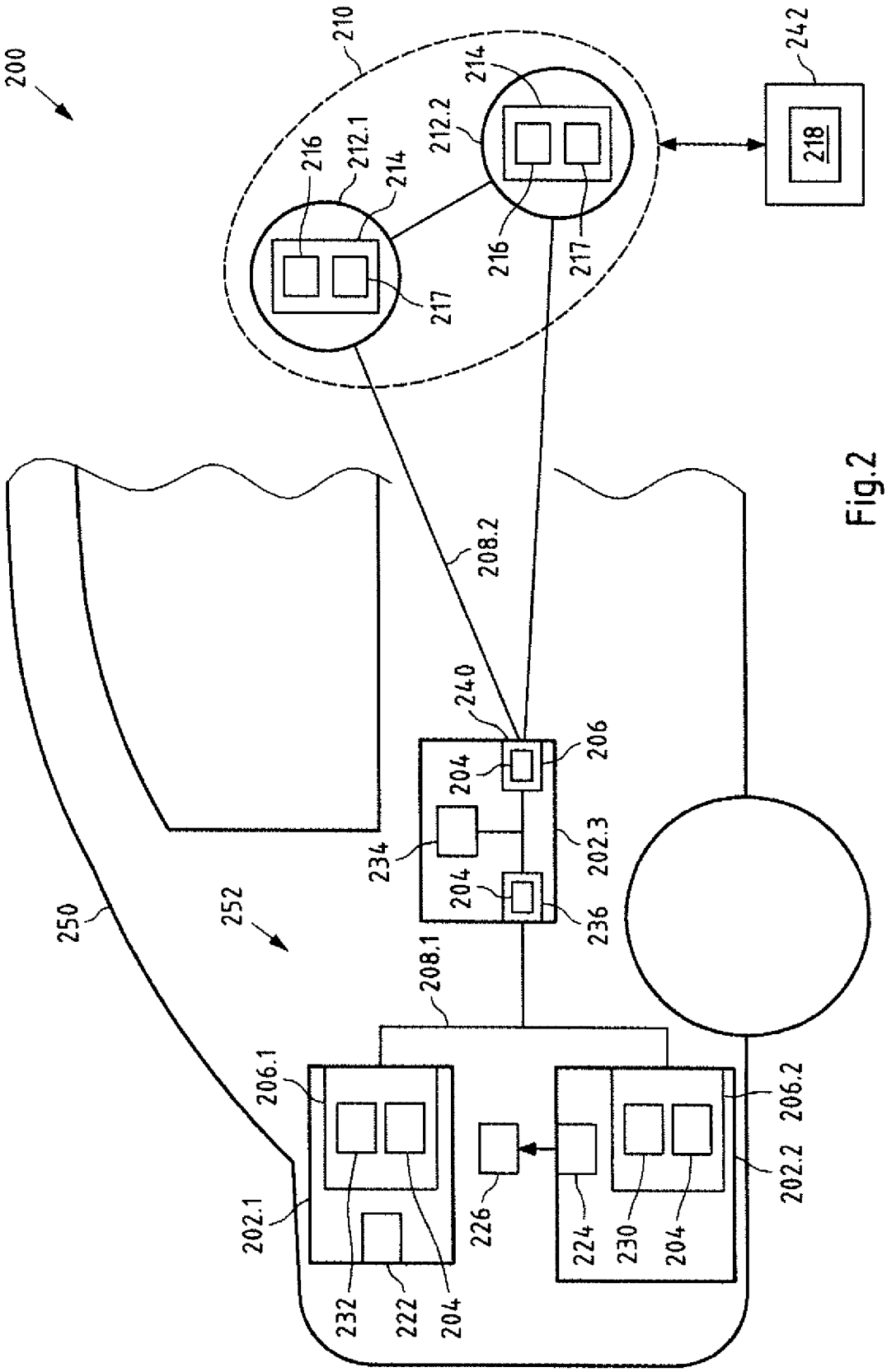

200
210
214
212.2
212.1
216
214
217
216
217
242
218
208.2
240
206
204
234
202.3
204
236
250
252
208.1
206.1
206.2
202.1
202.2
226
224
230
204
232
222
204

Fig.2

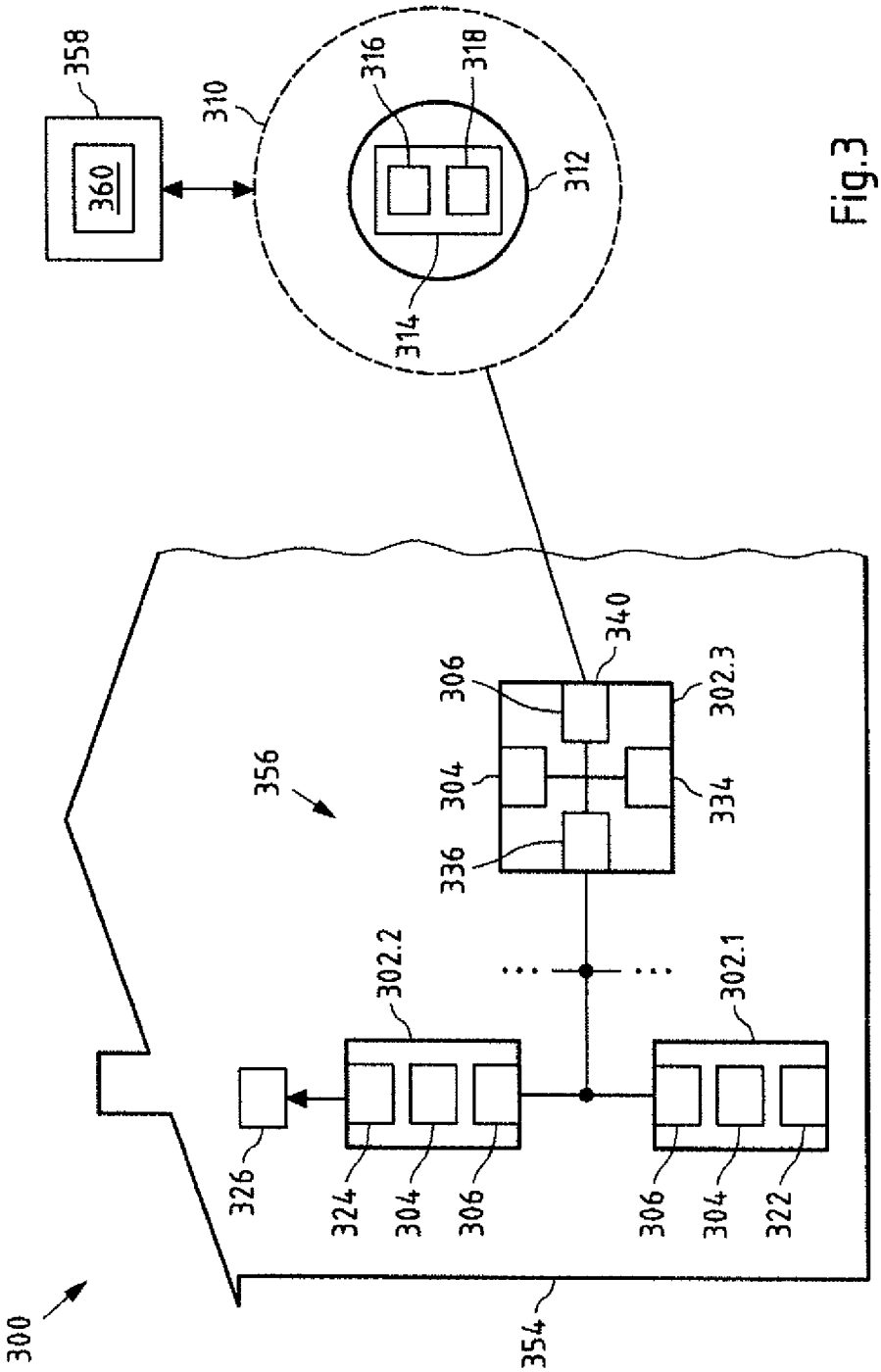

358
360
310
316
318
312
314
340
306
302.3
304
334
336
356
302.2
302.1
326
324
304
306
306
304
322
300
354

Fig.3

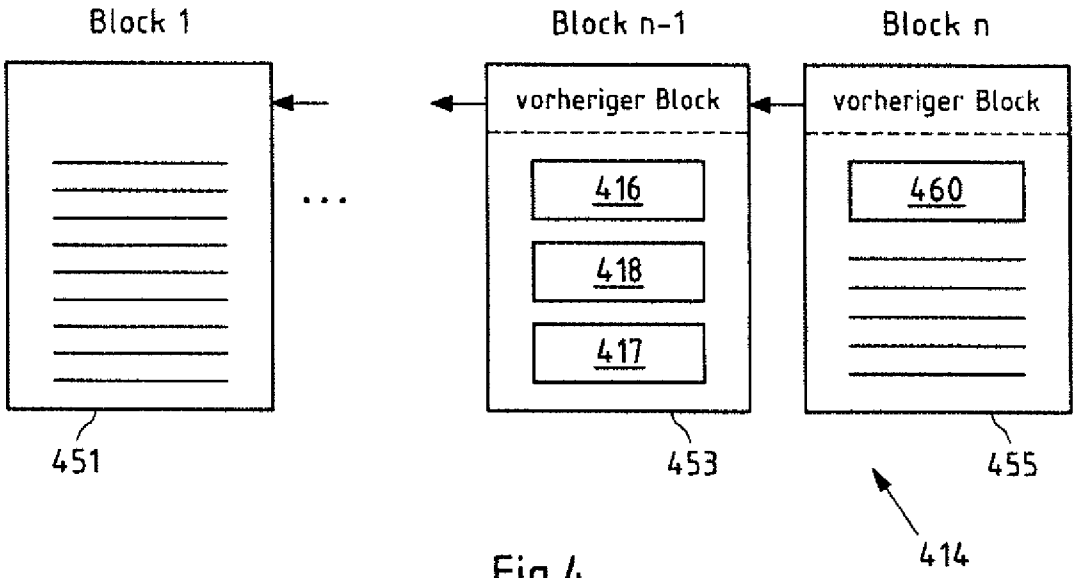

Block 1
Block n-1
Block n
vorheriger Block
vorheriger Block
416
418
417
460
451
453
455
414

Fig.4

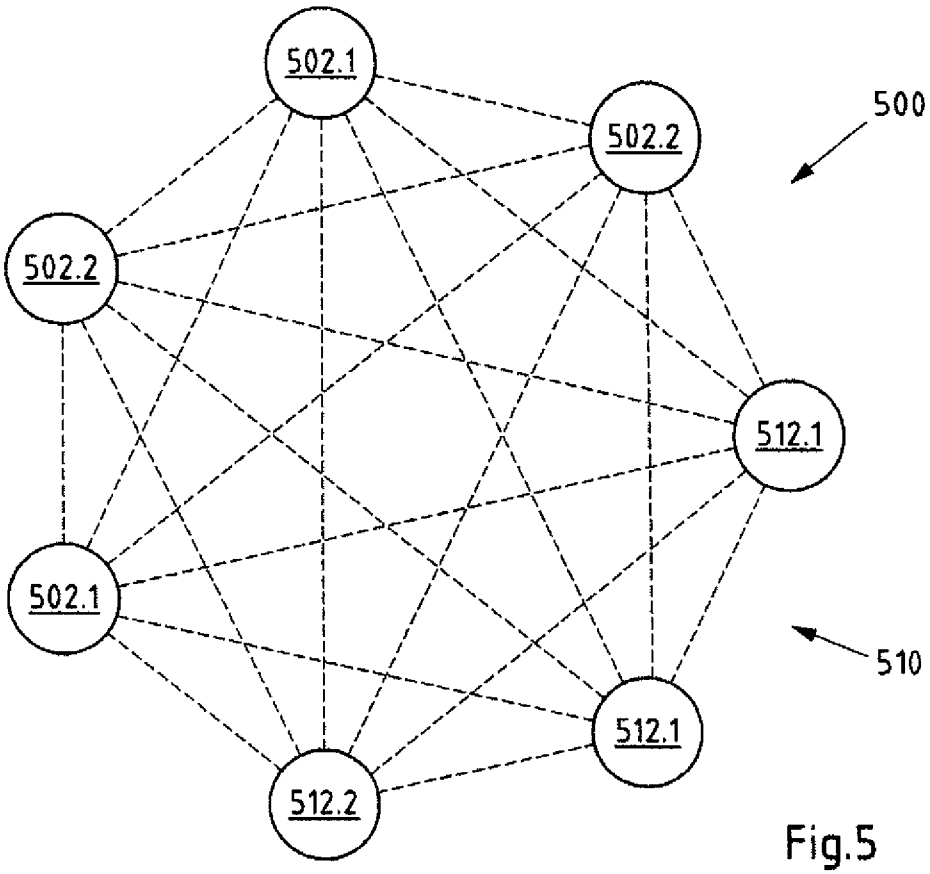

502.1
502.2
500
502.2
512.1
502.1
510
512.1
512.2

Fig.5

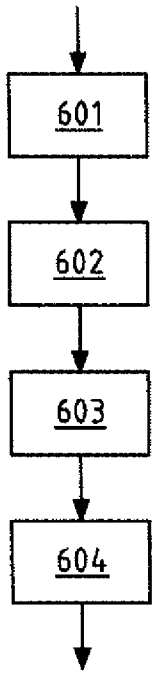


Fig.6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2018/073966

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i; ***G06K 9/00***(2006.01)i; ***G06Q 20/22***(2012.01)i; ***H04L 29/08***(2006.01)i; ***H04W 12/06***(2009.01)i; ***G06Q 20/36***(2012.01)i; ***G06Q 20/40***(2012.01)i; ***H04L 9/08***(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04W; G06K; G06Q

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Guardtime. "Internet of Things Authentication: A Blockchain solution using SRAM Physical Unclonable Functions In cooperation with" 01 May 2017 (2017-05-01), Retrieved from the Internet: https://www.intrinsic-id.com/wp-content/uploads/2017/05/gt_KSI-PUF-web-1611.pdf [retrieved on 2018-11-20] XP055525349 figures 1-8 pages 9, 11 - page 13	1-11
X	US 9716595 B1 (T-CENTRAL INC [US]) 25 July 2017 (2017-07-25) figures 4, 6, 7 column 12, lines 34-67 column 13, line 30 - column 14, line 14	1-11
X A	US 2016300234 A1 (MOSS-PULTZ SEAN [US] ET AL) 13 October 2016 (2016-10-13) figures 1, 2, 10 paragraphs [0017], [0058] - [0066], [0087] paragraphs [0105] - [0117]	1,9-11 2-8

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 November 2018	**28 November 2018**
Name and mailing address of the ISA/EP **European Patent Office** **p.b. 5818, Patentlaan 2, 2280 HV Rijswijk** **Netherlands** Telephone No. **(+31-70)340-2040** Facsimile No. **(+31-70)340-3016**	Authorized officer **Madzharova, Violeta** Telephone No.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	VICTOR COSTAN ET AL. "Intel SGX Explained" *INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,* Vol. 20170115:005718, 15 January 2017 (2017-01-15), pages 1-118 XP061022408	1,9-11
A	Sections 4.6 and 6.6.	2-8

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/EP2018/073966

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 9716595 B1	25 July 2017	NONE	
US 2016300234 A1	13 October 2016	CA 2981952 A1	13 October 2016
		CN 107851284 A	27 March 2018
		EP 3281171 A1	14 February 2018
		JP 2018515048 A	07 June 2018
		SG 11201708295X A	29 November 2017
		US 2016300234 A1	13 October 2016
		WO 2016164496 A1	13 October 2016

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2018/073966

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L9/32 G06K9/00 G06Q20/22 H04L29/08 H04W12/06
G06Q20/36 G06Q20/40 H04L9/08
ADD.
Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L H04W G06K G06Q

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

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

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	Guardtime: "Internet of Things Authentication: A Blockchain solution using SRAM Physical Unclonable Functions In cooperation with", , 1. Mai 2017 (2017-05-01), XP055525349, Gefunden im Internet: URL:https://www.intrinsic-id.com/wp-content/uploads/2017/05/gt_KSI-PUF-web-1611.pdf [gefunden am 2018-11-20] Abbildungen 1-8 Seiten 9, 11 - Seite 13 -----	1-11
X	US 9 716 595 B1 (T-CENTRAL INC [US]) 25. Juli 2017 (2017-07-25) Abbildungen 4, 6, 7 Spalte 12, Zeilen 34-67 Spalte 13, Zeile 30 - Spalte 14, Zeile 14 -----	1-11

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] Siehe Anhang Patentfamilie

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

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
20. November 2018	28/11/2018

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

1

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2018/073966

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2016/300234 A1 (MOSS-PULTZ SEAN [US] ET AL) 13. Oktober 2016 (2016-10-13)	1,9-11
A	Abbildungen 1, 2, 10 Absätze [0017], [0058] - [0066], [0087] Absätze [0105] - [0117] -----	2-8
X	VICTOR COSTAN ET AL: "Intel SGX Explained", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, Bd. 20170115:005718, 15. Januar 2017 (2017-01-15), Seiten 1-118, XP061022408, [gefunden am 2017-01-15]	1,9-11
A	Sections 4.6 and 6.6. -----	2-8

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2018/073966

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 9716595 B1	25-07-2017	KEINE	
US 2016300234 A1	13-10-2016	CA 2981952 A1	13-10-2016
		CN 107851284 A	27-03-2018
		EP 3281171 A1	14-02-2018
		JP 2018515048 A	07-06-2018
		SG 11201708295X A	29-11-2017
		US 2016300234 A1	13-10-2016
		WO 2016164496 A1	13-10-2016