(19) österreichisches patentamt

(10) **AT 526983 A1 2024-09-15**

(12) Österreichische Patentanmeldung

(21) Anmeldenummer: A 60030/2023
(22) Anmeldetag: 27.02.2023
(43) Veröffentlicht am: 15.09.2024

(51) Int. Cl.:
G06K 7/10 (2006.01)
G06K 19/07 (2006.01)
G06Q 30/018 (2023.01)
H04B 5/77 (2024.01)
H04L 9/32 (2006.01)
H04L 9/00 (2006.01)
H04L 9/40 (2022.01)
H04W 12/06 (2009.01)
H04W 12/47 (2021.01)

(56) Entgegenhaltungen:
US 2018108024 A1
US 10523443 B1
MA, J. et al. "A Blockchain-Based Application System for Product Anti-Counterfeiting" IEEE Access [online]. 6. Februar 2020 (06.02.2020). Bd. 8, Seiten 77642–77652. [ermittelt am 2. Jänner 2024]. <doi:10.1109/ACCESS.2020.2972026>. Ermittelt von <https://ieeexplore.ieee.org/document/8985337>
US 2020364817 A1
US 2021091960 A1
US 2021103938 A1
US 2021248653 A1
US 2021374693 A1
US 2022284447 A1
US 2022405770 A1

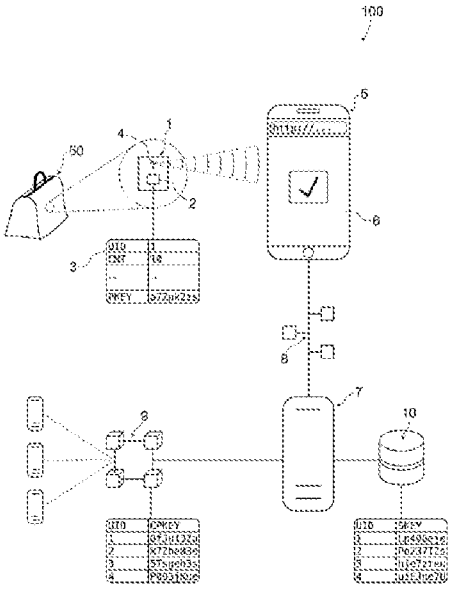
(71) Patentanmelder:
VariusSystems digital solutions GmbH
1220 Wien (AT)

(74) Vertreter:
Schardmüller Gall-Schuhmann Patentanwälte OG
1090 Wien (AT)

(54) Verfahren zur Verifizierung eines elektronischen Etiketts und System hierzu

(57) Die vorliegende Erfindung betrifft ein Verfahren (200, 201, 202) zur Verifizierung eines elektronischen Etiketts (1) zum Anbringen an ein Produkt (50), in welchem auslesbare Daten und ein geheimer Schlüssel gespeichert sind, wobei das elektronische Etikett (1) einen integrierten Schaltkreis (2) aufweist, welcher dazu ausgebildet ist aus den Daten mittels des privaten Schlüssels einen Hashwert zu errechnen.
Zudem betrifft die vorliegende Erfindung ein System (100) umfassend ein elektronisches Etikett (1) mit einem integrierten Schaltkreis (2) zum Anbringen an ein Produkt (50), ein Lesegerät (5) zum Auslesen von Daten aus dem elektronischen Etikett (1) und einen über ein Netzwerk (8) mit dem Lesegerät (5) verbundenen Server (7) zum Austausch von Daten.

Fig. 1



AT 526983 A1 2024-09-15

Zusammenfassung

Die vorliegende Erfindung betrifft ein Verfahren (200, 201, 202) zur Verifizierung eines elektronischen Etiketts (1) zum Anbringen an ein Produkt (50), in welchem auslesbare Daten und ein geheimer Schlüssel gespeichert sind, wobei das elektronische Etikett (1) einen integrierten Schaltkreis (2) aufweist, welcher dazu ausgebildet ist aus den Daten mittels des privaten Schlüssels einen Hashwert zu errechnen.

Zudem betrifft die vorliegende Erfindung ein System (100) umfassend ein elektronisches Etikett (1) mit einem integrierten Schaltkreis (2) zum Anbringen an ein Produkt (50), ein Lesegerät (5) zum Auslesen von Daten aus dem elektronischen Etikett (1) und einen über ein Netzwerk (8) mit dem Lesegerät (5) verbundenen Server (7) zum Austausch von Daten.

Verfahren zur Verifizierung eines elektronischen Etiketts und System hierzu

[0001] Die vorliegende Erfindung betrifft ein Verfahren zur Verifizierung eines elektronischen Etiketts zum Anbringen an ein Produkt, welches einen integrierten Schaltkreis aufweist, sowie ein System aufweisend ein elektronisches Etikett, ein Lesegerät und einen Server.

Stand der Technik

[0002] Verfahren und Systeme zur Fälschungssicherung und Echtheitsverifizierung von Produkten sind in verschiedenen Ausprägungen aus dem Stand der Technik bekannt. Insbesondere die Feststellung der Echtheit eines Produkts ist dabei von großer Bedeutung für sowohl Hersteller als auch Konsumenten, um Originale von Fälschungen unterscheiden zu können.

[0003] So können beispielsweise in Kleidungsstücken Etikette eingenäht sein, welche besondere Sicherheitsmerkmale aufweisen, um die Echtheit des Kleidungsstücks zu verifizieren. Solche Etikette können zudem auch mittels eines Lesegeräts elektronisch auslesbar ausgestaltet sein.

[0004] Aus dem Stand der Technik (US 2021/0103938 A1) sind Verfahren zur Verifizierung von elektronischen Etiketten bekannt, welche an Produkten angebracht sein können. Solche Verfahren führen die Verifizierung eines Etiketts über eine private Datenbank durch, welche beispielsweise vom Hersteller des Etiketts bzw. des Produkts bereitgestellt werden. Diese Verfahren haben jedoch den Nachteil, dass eine Echtheitsprüfung anhand einer privaten Datenbank nicht sicher gegenüber Manipulationen ist, da diese sowohl gewollt vom Eigentümer, als auch ungewollt durch Dritte manipuliert werden kann – beispielsweise in dem Einträge „echter“ Produkte geändert oder gelöscht werden, oder neue Einträge generiert werden, welche nicht einem „echten“ Produkt entsprechen. Gefälschte Produkte können somit mit solchen Etiketten versehen werden und durch Manipulation der entsprechenden Datenbank als „echt“ erscheinen.

Offenbarung der Erfindung

[0005] Die vorliegende Erfindung hat sich daher die Aufgabe gestellt, ein Verfahren der eingangs erwähnten Art fälschungssicherer zu gestalten bzw. ein Verfahren zur Verifizierung zur Verfügung zu stellen, welches die Fälschungssicherheit von Produkten erhöhen kann.

[0006] Die Erfindung löst die gestellte Aufgabe durch die Gegenstände der unabhängigen Patentansprüche. Bevorzugte Ausgestaltungen ergeben sich aus den abhängigen Patentansprüchen und den in weiterer Folge dargestellten Ausführungsvarianten.

[0007] Gemäß einem Aspekt der Erfindung ist ein Verfahren zur Verifizierung eines elektronischen Etiketts gezeigt, welches beispielsweise an einem physischen Produkt angebracht werden kann, um die Fälschungssicherheit des Produkts zu erhöhen. Das elektronische Etikett weist dabei einen integrierten Schaltkreis auf, in welchem auslesbare Daten und ein geheimer Schlüssel gespeichert sind. Der integrierte Schaltkreis ist zudem dazu ausgebildet, aus den Daten mittels des geheimen Schlüssels einen Hashwert zu errechnen.

[0008] Das Verfahren weist dabei folgende Schritte auf:

a) Auslesen von Daten aus dem elektronischen Etikett durch ein Lesegerät, wobei die ausgelesenen Daten zumindest den Hashwert enthalten,

b) Übertragen der ausgelesenen Daten von dem Lesegerät an einen Server,

c) Verifizierung des Hashwerts am Server mittels einer Blockchain,

d) Übertragen des Ergebnisses der Verifizierung von dem Server an das Lesegerät, und

e) Ausgabe und/oder Verarbeitung des Ergebnisses der Verifizierung am Lesegerät.

[0009] Gemäß einem weiteren Aspekt der vorliegenden Erfindung ist ein System, umfassend ein elektronisches Etikett mit einem elektronischen Schaltkreis zum Anbringen an ein Produkt, ein Lesegerät zum Auslesen von Daten aus dem elektronischen Etikett und einen über ein Netzwerk mit dem Lesegerät verbundenen Server zum Austausch von Daten gezeigt.

[0010] Erfindungsgemäß weist der elektronische Schaltkreis in dem Etikett einen Speicher auf, in welchem auslesbare Daten und ein geheimer Schlüssel gespeichert sind, und ist der elektronische Schaltkreis dazu ausgebildet, beim Auslesen durch ein Lesegerät einen Hashwert anhand einer kryptografischen Funktion aus den gespeicherten Daten und dem geheimen Schlüssel zu errechnen und an das Lesegerät zu senden.

[0011] Erfindungsgemäß ist das Lesegerät dazu ausgebildet, den Hashwert von dem elektronischen Etikett zu empfangen und an einen Server zur Verifikation zu senden, sowie ein Ergebnis der Verifizierung vom Server zu empfangen und zu verarbeiten und/oder auszugeben.

[0012] Erfindungsgemäß ist der Server dazu ausgebildet, den Hash-Wert vom Lesegerät zu empfangen und mittels einer Blockchain zu verifizieren und das Ergebnis der Verifizierung an das Lesegerät zu senden.

[0013] Im Rahmen der vorliegenden Erfindung wird unter elektronischem Etikett jede Form eines „Tags“ bezeichnet, welcher Daten beinhalten und zur Anbringung an oder in einem Produkt geeignet ist. Solche Produkte können beispielsweise Kleidungsstücke, Accessoires wie Taschen, Rucksäcke, etc., sowie elektrische bzw. elektronische Geräte sein, in welchen das Etikett angebracht oder integriert sein kann. Des Weiteren können derartige Produkte Sammelkarten, Briefmarken, Spiele, Smartcards oder andere Papierprodukte mit integriertem elektronischem Schaltkreis sein, in welchen das elektronische Etikett direkt integriert ist.

[0014] Es wird im Allgemeinen festgehalten, dass unter einer Blockchain im Sinne der vorliegenden Erfindung sowohl private als auch öffentliche Blockchains verstanden werden können. Private Blockchains können dabei auf einem oder mehreren Servern des Inhabers und/oder auf Recheneinrichtung von Benutzern gespeichert sein. Insbesondere im Falle einer privaten Blockchain kann der Inhaber die Protokolle („smart contracts“) frei definieren und so die Funktionsweise und Regeln der Blockchain bestimmen, während die einzelnen Blocks der Blockchain für alle Benutzer öffentlich und frei einsehbar sind.

[0015] Als Hashwert werden im Allgemeinen Zeichenfolgen bezeichnet, welche durch eine Hashfunktion (ein mathematischer Algorithmus), welche Daten (bzw. eine „Nachricht“) als Eingabe aufnimmt und eine feste Zeichenfolge von Zeichen zurückgibt (der „Hashwert“), generiert werden. Der durch die Hashfunktion erzeugte Hashwert ist dabei jeweils einzigartig für die Eingabe und identische Eingaben liefern immer das gleiche Ergebnis. Kleine Änderungen in der Eingabe führen jedoch zu deutlich unterschiedlichen Hashwerten.

[0016] Hashfunktionen werden regelmäßig in kryptographischen Protokollen wie digitalen Signaturen und Nachrichtenauthentifizierungscodes (MAC) verwendet. Ein MAC ist ein spezifischer Typ von Hash-Funktion, der eine Nachricht und einen geheimen Schlüssel als Eingabe erhält und eine feste Zeichenfolge von Zeichen zurückgibt. Der geheime Schlüssel wird verwendet, um sicherzustellen, dass nur autorisierte Parteien die Echtheit der Nachricht überprüfen können, da der Sender den MAC an die Nachricht anhängen und der Empfänger den MAC durch Rückrechnung aus der empfangenen Nachricht unter Verwendung des gleichen privaten Schlüssels überprüfen kann, um sicherzustellen, dass die empfangene Nachricht nicht verändert wurde, bzw. aus einer sicheren Quelle stammt.

[0017] Werden Daten aus dem elektronischen Etikett mittels eines Lesegeräts ausgelesen bzw. angefordert, so kann die Echtheitsüberprüfung bzw. Verifizierung besonders einfach und komfortabel erfolgen.

[0018] Die vom Lesegerät ausgelesenen Daten können dabei die im elektronischen Etikett gespeicherten Daten ganz oder teilweise umfassen. Der errechnete Hashwert wird dabei als Teil der ausgelesenen Daten auf das Lesegerät übertragen. Ein solches Auslesen kann dabei kontaktlos oder mittels Herstellung eines elektronischen Kontakts erfolgen. Alternativ kann der Auslesevorgang am elektronischen Etikett auch durch einen Benutzer initiiert werden (bspw. indem das Lesegerät nahe an das Etikett herangebracht wird, oder ein elektronischer Kontakt zwischen Etikett und Lesegerät hergestellt wird).

[0019] Werden weiter die ausgelesenen Daten von dem Lesegerät an einen Server übertragen, so kann die Echtheitsprüfung unabhängig vom Lesegerät erfolgen. Zudem muss der Datenbestand, welcher zur Verifizierung bzw. zur Echtheitsprüfung notwendig ist, nicht auf jedem Lesegerät redundant vorrätig gehalten werden. Hierdurch wird zudem gewährleistet, dass jedes Lesegerät stets auf den aktuellen Datenbestand zugreift und nicht veraltete oder unrichtige Daten abruft.

[0020] Wird der Hashwert am Server mittels einer Blockchain verifiziert, so kann die Verifizierung des Hashwerts in einem hohen Maß fälschungssicher gestaltet werden, da die zur Verifizierung benötigten, in der Blockchain gespeicherten Daten resistent gegenüber Manipulationen sind. In herkömmlichen Verfahren zur Echtheitsverifizierung sind die zur Verifizierung notwendigen Daten in der Regel in (privaten) Datenbanken gespeichert. Hierbei besteht sowohl für den Eigentümer der Datenbank als auch für Hacker bzw. Eindringlinge von außen die Möglichkeit, Datenbankeinträge zu ändern, hinzuzufügen oder zu löschen und somit die Echtheitsprüfung zu manipulieren. Werden die zur Verifizierung notwendigen Daten allerdings in einer Blockchain gespeichert, so kann die Sicherheit gegenüber Manipulationen deutlich erhöht werden.

[0021] Daten, die in Blockchains gespeichert sind, gelten aus mehreren Gründen als sicherer gegenüber Manipulation als Daten, die in traditionellen Datenbanken gespeichert sind. Insbesondere sind folgende Faktoren von Relevanz:

- Unveränderlichkeit: Sobald Daten in eine Blockchain aufgenommen werden, können sie nicht mehr verändert oder gelöscht werden. Das macht es Angreifern sehr viel schwerer, die Daten zu manipulieren;
- Dezentralisierung: In einer traditionellen Datenbank werden die Daten an einem einzigen Ort gespeichert, was Angriffe erleichtert. Im Gegensatz dazu verteilen

Blockchains die Daten auf ein Netzwerk von Computern, was es Angreifern viel schwerer macht, die Kontrolle über alle Kopien zu erlangen;

- Kryptografie: Blockchains nutzen kryptografische Techniken, um die Daten zu sichern, wie etwa digitale Signaturen und Hashing-Algorithmen. Dies bietet eine zusätzliche Sicherheitsschicht, um unbefugtem Zugriff und Manipulation entgegenzuwirken;
- Transparenz: Es ist in der Regel möglich, jeden Transaktionsverlauf in einer Blockchain zu verfolgen, so dass es einfacher ist, verdächtige Aktivitäten zu erkennen; und schließlich
- Konsensualität: In einem Blockchain-Netzwerk müssen mehrere Parteien einen Konsens erreichen, bevor neue Daten der Kette hinzugefügt werden können. Das macht es Angreifern deutlich schwerer, die Daten zu verfälschen.

[0022] Durch Kombination von zumindest einigen der oben genannten Faktoren kann somit die Fälschungssicherheit der elektronischen Etiketten deutlich erhöht werden.

[0023] Erfindungsgemäß wird dann weiter das Ergebnis der Verifizierung von dem Server an das Lesegerät zurückübertragen und schließlich das Ergebnis der Verifizierung am Lesegerät ausgegeben oder weiterverarbeitet. Somit kann eine vom Lesegerät losgelöste Verifizierung der Echtheit des Etiketts anhand einer Blockchain erfolgen, welche die Möglichkeiten zur Fälschung deutlich einschränkt.

[0024] Zusammenfassend kann somit erfindungsgemäß ein Verfahren zur Echtheitsüberprüfung bzw. Verifizierung eines elektronischen Etiketts, welches an einem Produkt angebracht oder integriert sein kann, geschaffen werden.

[0025] Im Folgenden werden weitere Ausführungsvarianten der Erfindung dargestellt. Die dargestellten Ausführungsvarianten, bzw. einzelne Teilaspekte der Ausführungsvarianten, sind, falls nicht anders angegeben, beliebig miteinander kombinierbar.

[0026] Gemäß einer Ausführungsvariante der Erfindung kann das Auslesen der Daten aus dem Etikett durch das Lesegerät anhand einer oder mehrerer der folgenden Methoden erfolgen:

- Drahtlos: Die Übertragung von Daten zwischen Etikett und Lesegerät kann ohne Kontakt elektronisch, also drahtlos, beispielsweise mittels RFID- oder NFC-Technologie, erfolgen. Ein physischer Kontakt zwischen Etikett und Lesegerät ist dabei nicht vonnöten;

- Barcode-Scannen: Beim Scannen von Barcodes wird ein laser- oder kamerabasiertes System im Lesegerät verwendet, um Daten von dem Etikett zu erfassen. Der Barcode kann dabei auf dem Etikett oder dem Produkt aufgedruckt sein, oder durch das Etikett digital angezeigt werden;
- Magnetstreifenlesung: Beim Lesen von Magnetstreifen wird ein Magnetkopf im Lesegerät verwendet, um die auf einem Magnetstreifen kodierten Daten zu lesen. Dabei kann das Etikett etwa einen Magnetstreifen aufweisen oder bspw. in einer Magnetstreifenkarte inkludiert sein;
- Smartcard-Lesen: Beim Lesen von Smartcards bzw. Chipkarten wird eine kontaktlose oder kontaktbasierte Schnittstelle verwendet, um Daten zu lesen, die auf dem Etikett gespeichert sind. Das Etikett kann dabei eine Kontaktzone mit Kontaktflächen aufweisen, die mit den Kontakten eines Lesegeräts in Verbindung gebracht werden können, um die Daten auszulesen;
- Optische Zeichenerkennung (OCR): OCR ist eine Technologie, mit der gedruckter Text aus einem Bild, einem Foto oder einem gescannten Dokument gelesen und in maschinencodierten Text umgewandelt werden kann. Das Lesegerät kann dazu eine Kamera aufweisen, welche auf dem Etikett oder dem Produkt aufgedruckten Text erfassen kann.
- QR-Code-Scannen: QR-Codes sind zweidimensionale Strichcodes, die mit einer Kamera gescannt werden können, um die kodierten Informationen zu extrahieren. Dabei kann das Lesegerät wiederum eine Kamera aufweisen, welche ein Bild von dem QR-Code aufnimmt und diesen entschlüsselt. Der QR-Code kann dabei wiederum auf dem Etikett oder dem Produkt aufgedruckt bzw. angebracht sein.

[0027] Wie zuvor erwähnt, können die oben genannten Methoden auch miteinander kombiniert werden, so dass beispielsweise ein Teil der Daten über RFID vom Etikett ans Lesegerät gesendet wird und ein Teil der Daten als QR-Code oder Schrift bzw. Text auf dem Etikett aufgedruckt ist und durch eine Kamera des Lesegeräts erfasst wird.

[0028] Gemäß einer bevorzugten Ausführungsvariante können die Daten mit einem RFID-Lesegerät, von dem elektronischen Etikett gelesen werden. RFID (Radiofrequenz-Identifikation) nutzt Funkwellen zur Kommunikation zwischen dem Lesegerät und dem Etikett. Das Lesegerät sendet dabei ein Funksignal aus, welches von der Antenne des Tags empfangen wird, wodurch eine Auslesevorgang gestartet wird. Dieser Start des Auslesevorgangs kann etwa dadurch initiiert werden, indem das Lesegerät nahe an das Etikett herangeführt wird. Das Etikett sendet dann Daten zurück, welche vom Lesegerät empfangen und gelesen werden können. Auf diese Weise können Daten elektronisch von

einem elektronischen Etikett gelesen werden, ohne dass ein physischer Kontakt oder eine Sichtverbindung zwischen dem Etikett und dem Lesegerät erforderlich ist.

[0029] Gemäß einer Ausführungsvariante kann das RFID-Lesegerät ein NFC-Lesegerät sein und das elektronische Etikett ein NFC-Tag sein, wobei Lesegerät und Etikett nach dem NFC-Standard arbeiten und so eine Kommunikation zwischen Etikett und Lesegerät lediglich im Nahfeld ermöglichen. Hierdurch wird es insbesondere Angreifern erschwert, die Kommunikation zwischen Etikett und Lesegerät abzuhören.

[0030] Gemäß einer Ausführungsvariante kann die Übertragung der Daten vom Lesegerät an den Server bevorzugt über ein Netzwerk erfolgen, in dem sich Lesegerät und Server befinden. So kann eine physische Trennung zwischen Server und Lesegerät hergestellt werden, wobei der Server zentral Anfragen von verschiedenen Lesegeräten empfangen und verarbeiten kann. Ein solches Netzwerk kann sowohl ein privates LAN- oder WLAN-Netzwerk sein, sowie ein öffentliches Netzwerk, etwa das Internet, sein. Insbesondere bei Übertragungen über ein öffentliches Netzwerk kann zur Verbesserung der Sicherheit die Kommunikation zwischen Lesegerät und Server verschlüsselt erfolgen.

[0031] Gemäß einer weiteren Ausführungsvariante kann der Server am Lesegerät selbst ausgeführt sein, womit die Daten vom Lesegerät intern direkt an den Server übertragen werden. Der Server kann dann dezentral, wie viele gleichartige Server, die Anfragen zur Verifizierung erledigen, wodurch die Anfragezeiten und Serverlasten reduziert werden können und Ausfallszeiten der Server minimiert werden können.

[0032] Für die Übertragung vom Server zurück an das Lesegerät sind die zuvor beschriebenen Ausführungsvarianten analog anwendbar.

[0033] Gemäß einer Ausführungsvariante kann das Lesegerät das Ergebnis der Verifizierung am Lesegerät visuell, auditiv oder haptisch ausgeben. So kann die Ausgabe etwa eine visuelle Indikation für das Verifizierungsergebnis sein, beispielsweise eine farbige LED oder die Ausgabe von Text oder Symbolen auf einem Bildschirm. Alternativ kann auch ein Ton oder eine Tonfolge ausgegeben werden, welche das Verifizierungsergebnis widerspiegelt. Gemäß einer weiteren Möglichkeit kann das Verifizierungsergebnis auch als haptischer Reiz kodiert sein (wie etwa ein Vibrieren).

[0034] Das Lesegerät kann gemäß einer Ausführungsvariante ein Smartphone bzw. ein tragbarer Computer sein. Bevorzugt weist das Smartphone einen RFID- bzw. NFC-Leser auf, mit welchem das elektronische Etikett ausgelesen wird. Die empfangenen Daten werden dann auf den Server übertragen und das vom Server erhaltene Ergebnis kann auf einem Display des Smartphones angezeigt werden.

[0035] Gemäß einer Ausführungsvariante der Erfindung kann zur Verifizierung des Hashwerts ein Verifizierungsparameter anhand der vom Lesegerät empfangenen Daten von der Blockchain angefordert werden. Der Verifizierungsparameter kann dabei bspw. ein Vergleichswert sein, anhand dessen eine Verifizierung des Hashwerts durchgeführt wird. Alternativ kann der Verifizierungsparameter auch dazu dienen einen Vergleichswert am Server zu errechnen, welcher zur Verifizierung des Hashwerts herangezogen werden kann.

[0036] Gemäß einer Ausführungsvariante der Erfindung können die auslesbaren Daten eine Kennung zur eindeutigen Identifizierung des Etiketts und einen inkrementellen Zähler umfassen. Die Kennung zur eindeutigen Identifizierung des Etiketts kann dabei beispielsweise eine UID oder eine fortlaufende Nummerierung des Etiketts oder dergleichen sein. Der inkrementelle Zähler kann dabei einen aktuellen Zählerwert aufweisen, welcher durch den integrierten Schaltkreis inkrementiert, also erhöht werden kann. Bevorzugt ist der Zähler von außerhalb des Etiketts nicht änderbar, sondern ausschließlich im Zuge entsprechender Programmabläufe im integrierten Schaltkreis, wobei der Zählerwert nicht erniedrigt werden kann.

[0037] Gemäß einer weiteren Ausführungsvariante der Erfindung kann das Lesegerät beim Auslesen der Daten aus dem elektronischen Etikett die Kennung zur eindeutigen Identifizierung des Etiketts und den Zählerwert empfangen. Gemäß weiteren Ausführungsvarianten der Erfindung können ebenso weitere, auf dem elektronischen Etikett gespeicherte Daten oder Informationen (beispielsweise Identifizierungscodes, Zeichenfolgen, etc.), empfangen werden.

[0038] Gemäß einer Ausführungsvariante können diese auslesbaren Daten durch das Lesegerät in Form einer Nachricht von dem elektronischen Etikett erhalten werden. Die Nachricht kann dabei sämtliche ausgelesenen Daten enthalten. Der Hashwert wird dabei als Prüfsumme aus der Nachricht errechnet und beim Senden der Nachricht vom elektronischen Etikett ans Lesegerät der Nachricht angehängt, so dass das gesamte Paket die ausgelesenen Daten als Nachricht und den Hashwert als Prüfsumme enthält.

[0039] Gemäß einer Ausführungsvariante können die auslesbaren Daten in Form einer Zeichenkette von dem elektronischen Etikett erhalten werden. Bevorzugt stellt die Zeichenkette dabei eine URL oder eine URI (Uniform Ressource Identifier) dar, wobei ein Öffnen bzw. Abfragen der URL/URI am Lesegerät die Daten auf den Server überträgt und das Ergebnis der Verifizierung ausgegeben wird. Auf diese Weise können technisch besonders einfach eine Vielzahl von Lesegeräten zum Auslesen der elektronischen Etiketten eingesetzt werden, ohne dass spezielle Software bzw. Programme auf den Lesegeräten bereitgestellt werden müssen.

[0040] Hierzu können die vom Etikett ans Lesegerät übertragenen Daten bzw. die übertragene Nachricht in der URL/URI enthalten sein (etwa in Form von Abfrage-Zeichenketten, bzw. „Query-Strings"). Der Server kann dabei etwa als http-Server betrieben werden, welcher die URL/URI auflöst und die Daten daraus extrahiert. Das ans Lesegerät zurückübertragene Ergebnis kann dabei in Form eines http-Response erhalten werden.

[0041] Gemäß einer Ausführungsvariante der Erfindung kann der integrierte Schaltkreis des elektronischen Etiketts dazu programmiert sein, beim Auslesen von Daten den inkrementellen Zähler zu erhöhen. Der Zählerwert kann somit die Anzahl der Auslesevorgänge des elektronischen Etiketts widerspiegeln.

[0042] Gemäß einer Ausführungsvariante der Erfindung kann der integrierte Schaltkreis des elektronischen Etiketts dazu programmiert sein, automatisch bei jedem Auslesen der Daten einen Hashwert aus den ausgelesenen Daten zu berechnen und zusammen mit den Daten an das Lesegerät zu senden. Der Hashwert kann dabei als Prüfsumme (Checksum) oder digitale Signatur dienen und so durch Einbindung des geheimen Schlüssels ein fälschungssicheres Zertifikat für die Echtheit des Etiketts darstellen.

[0043] Wird zudem der Hashwert aus den Daten errechnet, welche den inkrementellen Zähler umfassen, so kann bei jedem Auslesen ein eindeutiger Hashwert generiert werden, was die Fälschungssicherheit des elektronischen Etiketts weiter erhöht.

[0044] Gemäß einer Ausführungsvariante kann das Lesegerät aus dem elektronischen Etikett dabei eine Nachricht enthaltend die Daten auslesen, wobei die Nachricht bevorzugt eine Kennung zur eindeutigen Identifizierung und den aktuellen Zählerwert aufweist. Die gesamte Nachricht wird dann zur Berechnung des Hashwerts herangezogen, wobei der Hashwert ein Nachrichtenauthentifizierungscodes (MAC) ist, welcher anhand einer kryptografischen Hashfunktion oder anhand eines Blockverschlüsselungsverfahrens aus der Nachricht und dem geheimen Schlüssel berechnet wird. Bevorzugt ist der Hashwert ein „One-Key MAC" (OMAC), wobei die Nachricht mit dem, auf dem elektronischen Etikett gespeicherten, geheimen Schlüssel verschlüsselt wird.

[0045] Gemäß einer weiteren Ausführungsvariante kann der Hashwert auch durch ein Verschlüsselungsverfahren mit mehr als einem Schlüssel generiert werden. So können auf dem elektronischen Etikett auch mehr als ein geheimer Schlüssel gespeichert sein; gemäß einer Ausführungsvariante etwa ein primärer geheimer Schlüssel und ein sekundärer geheimer Schlüssel. Die Verschlüsselung der auszulesenden Daten zur Erzeugung des Hashwerts kann dann zunächst mit dem primären Schlüssel und danach nochmals mit dem

sekundären Schlüssel erfolgen. Auf diese Weise können entweder zwei Hashwerte oder ein doppelt verschlüsselter Hashwert erzeugt werden.

[0046] Gemäß einer weiteren Ausführungsvariante kann zur Verifizierung des Hashwerts, dieser mit in der Blockchain gespeicherten Vergleichs-Hashwerten verglichen werden. Die Blockchain kann somit als Verifizierungsparameter direkt Vergleichs-Hashwerte enthalten, mit welchen die vom Lesegerät empfangenen Hashwerte verglichen werden können, um die Verifizierung des elektronischen Etiketts durchzuführen. Die in der Blockchain gespeicherten Hashwerte sind somit unveränderlich und können nicht manipuliert werden. Dabei können die möglichen Hashwerte etwa für ein bestimmtes elektronisches Etikett vorberechnet werden und vorab in der Blockchain gespeichert werden. Ein besonders einfaches und auch sicheres Verifizierungsverfahren kann so geschaffen werden, da die Verifizierung ausschließlich anhand bzw. mittels der Blockchain erfolgen kann.

[0047] Gemäß einer Ausführungsvariante können weiter die in der Blockchain gespeicherten Vergleichs-Hashwerte für mehre mögliche Zählerwerte vorberechnet sein. So können die in der Blockchain gespeicherten Hashwerte etwa für eine gewisse Anzahl von unterschiedlichen Zählerwerten für jeweils einen Datensatz des elektronischen Etiketts (etwa der eindeutigen Kennung) unter Verwendung des privaten Schlüssels errechnet sein. Da für den Hersteller der elektronischen Etiketten der private Schlüssel und die darauf gespeicherten Daten bekannt sind, können diese bei der Fertigung erstmalig zur Berechnung der unterschiedlichen Hashwerte herangezogen werden. Da zu einem späteren Zeitpunkt insbesondere der private Schlüssel nicht mehr aus dem elektronischen Etikett auslesbar ist, kann nach der erstmaligen Vorbefüllung der Blockchain keine Errechnung der Hashwerte ohne Kenntnis des privaten Schlüssels mehr erfolgen. Indem lediglich die vorberechneten Hashwerte in der Blockchain gespeichert werden, ist eine aktive Kenntnis des privaten Schlüssels am Server nicht notwendig, um eine Echtheitsprüfung des elektronischen Etiketts durchführen zu können.

[0048] Gemäß einer weiteren Ausführungsvariante können die gespeicherten Vergleichs-Hashwerte als trunkierte Vergleichs-Hashwerte in der Blockchain gespeichert sein. Solche trunkierte Vergleichs-Hashwerte können etwa durch ein Abschneiden bzw. Beschneiden der errechneten Hashwerte erhalten werden. Dabei können in der Blockchain nicht die gesamten Hashwerte, sondern beispielsweise lediglich die ersten/letzten 10/20/30, etc. Zeichen des errechneten Hashwerts gespeichert werden. Ein Rückrechnen auf den privaten Schlüssel bzw. ein durch viele Versuche zufälliges Erraten der Nachricht bzw. des Geheimnisses, wird somit deutlich erschwert. Es werden zur Verifizierung dann lediglich die ersten Zeichen des vom Lesegerät empfangenen Hashwerts mit den in der Blockchain gespeicherten Vergleichs-Hashwerten verglichen.

[0049] Gemäß einer weiteren Ausführungsvariante können die Vergleichs-Hashwerte in einem auf der Blockchain ausgeführten Programm, gespeichert sein und der Vergleich zwischen Hashwert und gespeicherten Vergleichs-Hashwerten beim Ausführen des Programms erfolgen. Ein solches Programm bzw. Protokoll kann vorzugsweise ein sogenannter „Smart Contract" sein, welcher auf der Blockchain durch einen Benutzer ausgeführt werden kann. Die Speicherung der Verifizierungsparameter direkt in dem Programm bzw. dem Smart Contract, hat den Vorteil, dass die Kontrolle über die gespeicherten Werte im Einflussbereich des Betreibers der Blockchain bleibt.

[0050] Gemäß einer weiteren Ausführungsvariante kann zur Verifizierung des Hashwerts, der Server aus der Blockchain einen Vergleichs-Schlüssel abrufen, aus den empfangenen Daten und dem Vergleichs-Schlüssel einen Vergleichs-Hashwert mittels einer kryptografischen Funktion errechnen und den Hashwert mit dem Vergleichs-Hashwert vergleichen. Auf der Blockchain sind dabei eine Anzahl von Vergleichs-Schlüssel gespeichert, welche jeweils einem elektronischen Etikett zugeordnet sind und so zur Überprüfung des vom elektronischen Etikett gesendeten Hashwerts herangezogen werden. Der Vergleichs-Schlüssel kann vom Server aus der Blockchain in Abhängigkeit der empfangenen Daten abgerufen werden. So können die empfangenen Daten beispielsweise eine Kennung zur eindeutigen Identifizierung des elektronischen Etiketts enthalten und der Vergleichs-Schlüssel aus der Blockchain für die jeweilige Kennung abgerufen werden. Am Server wird der Vergleichs-Schlüssel nun verwendet um aus den vom Lesegerät erhaltenen Daten einen Vergleichs-Hashwert zu errechnen, wobei der Server dabei vorzugsweise dieselbe kryptografische Hashfunktion bzw. den selben Verschlüsselungsalgorithmus wie der im elektronischen Etikett integrierte Schaltkreis verwendet. Der errechnete Vergleichs-Hashwert kann somit zur Verifizierung der Echtheit den errechneten Vergleichs-Hashwert mit dem empfangenen Hashwert vergleichen.

[0051] Gemäß einer weiteren Ausführungsvariante können zur Berechnung des Vergleichs-Hashwerts am Server alle oder ein Teil der vom elektronischen Etikett empfangenen Daten verwendet werden. Bevorzugt umfassen die Daten die Kennung zur eindeutigen Identifizierung und den aktuellen Zählerwert, welche mit dem Vergleichs-Schlüssel verschlüsselt werden. Alternativ können andere oder weitere Daten zur Berechnung des Hashwerts herangezogen werden.

[0052] Gemäß einer weiteren Ausführungsvariante kann zur Berechnung des Hashwerts im integrierten Schaltkreis des elektronischen Etiketts eine geheime Zeichenfolge bzw. ein sekundärer Schlüssel miteinbezogen werden, welche/r beim Auslesen der Daten vom elektronischen Etikett nicht an das Lesegerät gesendet wird. Diese geheime Zeichenfolge kann zudem am Server, beispielsweise in einer privaten Datenbank, gespeichert sein, und

bei der Berechnung des Vergleichs-Hashwerts am Server mit dem Vergleichs-Schlüssel einbezogen werden. Durch die Einbeziehung eines weiteren Geheimnisses bzw. eines sekundären Schlüssels, kann eine Verifizierung alleine anhand der Blockchain ohne Kenntnis des Geheimnisses nicht erfolgen. Ein Umgehen des Servers bei der Verifizierung ist somit nicht möglich, wodurch die Fälschungssicherheit weiter erhöht wird.

[0053] Gemäß einer Ausführungsvariante der Erfindung kann in der Blockchain pro Kennung zur eindeutigen Identifizierung des Etiketts jeweils ein Vergleichs-Schlüssel gespeichert sein. Der Server kann somit nach Erhalt der Daten vom Lesegerät, welche insbesondere die Kennung enthalten, den passenden Vergleichs-Schlüssel aus der Blockchain abrufen.

[0054] Gemäß weiterer Ausführungsvarianten können die Vergleichs-Schlüssel auch zu anderen Daten des elektronischen Etiketts verknüpft in der Blockchain gespeichert sein.

[0055] Gemäß einer weiteren Ausführungsvariante können die Vergleichs-Schlüssel in einem auf der Blockchain ausgeführten Programm gespeichert sein und das Programm in Abhängigkeit von einem elektronischen Etikett zugeordneten Daten einen Vergleichs-Schlüssel zurückgeben. Ein solches Programm bzw. Protokoll kann vorzugsweise ein sogenannter „Smart Contract“ sein, welcher auf der Blockchain durch einen Benutzer ausgeführt werden kann. Die Speicherung der Verifizierungsparameter direkt in dem Programm bzw. dem Smart Contract, hat den Vorteil, dass die Kontrolle über die gespeicherten Werte im Einflussbereich des Betreibers der Blockchain bleibt. Wie zuvor beschrieben, können die Vergleichs-Schlüssel in dem Programm mit Daten des Etiketts, wie etwa der Kennung zur eindeutigen Identifizierung oder anderen Eigenschaften, verknüpft sein. So kann das Programm etwa als Übergabeparameter die Kennung des Etiketts aufnehmen und hierfür den passenden Vergleichs-Schlüssel zurückgeben.

[0056] Gemäß einer weiteren Ausführungsvariante können die in der Blockchain gespeicherten Vergleichs-Schlüssel verschlüsselt sein. Da die in der Blockchain gespeicherten Daten in der Regel für alle Benutzer frei zugänglich und öffentlich einsehbar sind, kann durch Verschlüsselung der gespeicherten Vergleichs-Schlüssel eine weitere Sicherheitsebene eingezogen werden. Die verschlüsselten Vergleichs-Schlüssel können somit ohne Sicherheitsverlust direkt in einer öffentlichen Blockchain gespeichert werden, ohne dass eine Gefahr für ein Umgehen der Verifizierung am Server besteht.

[0057] Gemäß einer weiteren Ausführungsvariante kann der aus der Blockchain abgerufene Vergleichs-Schlüssel am Server entschlüsselt werden, und so der

entschlüsselte Vergleichs-Schlüssel zur Berechnung des Vergleichs-Hashwerts herangezogen werden.

[0058] Die Verschlüsselung der Vergleichs-Schlüssel kann dabei mit einem oder mehreren Sicherheitsschlüsseln erfolgen, wobei die Sicherheitsschlüssel insbesondere nur am Server oder nur beim Benutzer selbst zur Verfügung stehen, so dass eine unbefugte Verifizierung durch Dritte effektiv unterbunden werden kann.

[0059] Die Verschlüsselung kann dabei anhand gängiger Verschlüsselungs-Algorithmen erfolgen, wobei sowohl symmetrische als auch asymmetrische Verschlüsselungen möglich sind. Im Falle einer symmetrischen Verschlüsselung wird der Vergleichs-Schlüssel beim Eintragen in die Blockchain mit dem gleichen Sicherheitsschlüssel verschlüsselt, welcher zur Entschlüsselung der verschlüsselten Vergleichs-Schlüssel am Server verwendet wird. Im Falle einer asymmetrischen Verschlüsselung kann zur Verschlüsselung der Vergleichs-Schlüssel eine anderer Sicherheitsschlüssel als zur Entschlüsselung der verschlüsselten Vergleichs-Schlüssel am Server verwendet werden.

[0060] Gemäß einer Ausführungsvariante der Erfindung kann ein erster Teil der in der Blockchain gespeicherten Vergleichs-Schlüssel mit einem ersten Sicherheitsschlüssel verschlüsselt sein.

[0061] Zudem kann gemäß einer weiteren Ausführungsvariante ein zweiter Teil der in der Blockchain gespeicherten Vergleichs-Schlüssel mit einem zweiten Sicherheitsschlüssel verschlüsselt sein.

[0062] Auf diese Weise kann durch die Verwendung unterschiedlicher Sicherheitsschlüssel zur Verschlüsselung der Vergleichs-Schlüssel, die Sicherheit des Verfahrens weiter erhöht werden. So können beispielsweise Teile der Vergleichs-Schlüssel in der Blockchain durch Verwendung eigener Sicherheitsschlüssel nur für eine bestimmte Gruppe an Teilnehmern, welche den jeweiligen Sicherheitsschlüssel kennen, verfügbar sein, wobei andere Gruppen an Teilnehmern keinen Zugriff auf den so verschlüsselten Teil der Vergleichs-Schlüssel haben und somit die Verifizierung der Etiketten nicht durchführen können. Unter Teilnehmer können dabei etwa Server, welche die Verifizierung durchführen, Geräte, Lesegeräte, Hersteller (von Etiketten oder Produkten) oder Benutzer verstanden werden.

[0063] Gemäß einer Ausführungsvariante können mehrere Server aus einer Blockchain zur Verifizierung von Etiketten Vergleichs-Schlüssel abrufen, wobei jedem Server ein Satz an Vergleichs-Schlüssel zugeordnet ist und wobei die Server jeweils über einen Sicherheitsschlüssel, zur Entschlüsselung der zugeordneten Vergleichs-Schlüssel, verfügen. So kann eine zentrale Blockchain geschaffen werden, welche zur Verifizierung

unterschiedlicher Etiketten bzw. Produkte verschiedener Hersteller zugleich dient, ohne dass die Hersteller in der Lage sind, gegenseitig den Verifizierungs-Vorgang der Etiketten zu beeinflussen bzw. zu fälschen. Durch die zentrale Blockchain wird ein von den einzelnen Herstellern unabhängiger und durch alle Teilnehmer bestätigter „wahrer" Datenbestand geschaffen („Single Source of Truth" SSOT).

[0064] In anderen Worten werden so Partitionen von Vergleichs-Schlüsseln in der Blockchain geschaffen, welche jeweils einem Teilnehmer (Besitzer, Herausgeber oder Hersteller von Etiketten oder Produkten) zugeordnet sein können.

[0065] Sind mehrere Server dazu eingerichtet, eine Verifizierung der Etiketten anhand der Blockchain durchzuführen, so können die Server zudem zur dezentralen Speicherung der Blockchain verwendet werden. Die Server können dabei zudem als Validatoren neuer Blöcke fungieren und so den Konsensmechanismus der Blockchain erfüllen, indem die Server neue Blöcke über ein Konsensverfahren (Proof of Work, Proof of Stake, etc.) erschaffen und anschließend an die Blockchain anhängen.

[0066] Gemäß einer Ausführungsvariante der Erfindung wird jede Anfrage eines Servers an die Blockchain zur Verifizierung eines Etiketts als Transaktion in einem Block der Blockchain gespeichert. So kann jede Verifizierung bzw. jeder Verifizierungsversuch eines Etiketts lückenlos in der Blockchain aufgezeichnet werden, wodurch eine Überwachung auf Fälschungsversuche oder Angriffe erreicht werden kann und etwa schadhafte Angriffe entdeckt werden können.

[0067] Gemäß einer Ausführungsvariante kann der Sicherheitsschlüssel am Lesegerät von einem Benutzer manuell eingegeben werden; etwa indem der Benutzer aufgefordert wird, den Sicherheitsschlüssel von dem Etikett oder dem Produkt abzulesen und am Lesegerät einzugeben. So kann eine zusätzliche Sicherheitsebene eingeführt werden, wobei eine Echtheitsprüfung bzw. Verifizierung nur dann durchgeführt werden kann, wenn der Benutzer in physischem Besitz des Produkts bzw. Etiketts ist.

[0068] Gemäß einer Ausführungsvariante kann der Sicherheitsschlüssel auf einem sekundären elektronischen Schaltkreis gespeichert sein. Ein solcher sekundärer Schaltkreis kann beispielsweise ein in einer Smartcard integrierter Chip sein (Schlüsselkarte) oder in bzw. an einem Produkt angebracht sein. Der sekundäre Schaltkreis kann dabei bevorzugt von dem Lesegerät ausgelesen werden. Alternativ kann auch ein sekundäres Lesegerät verwendet werden, um den sekundären elektronischen Schaltkreis auszulesen.

[0069] Gemäß der zuvor genannten Ausführungsvarianten kann der Sicherheitsschlüssel zur Verifizierung vom Lesegerät an den Server übertragen werden. Gemäß einer alternativen Ausführungsvariante kann ein Teilergebnis der Verifizierung am Server berechnet werden und

dieses Teilergebnis zur vollständigen Verifizierung zurück auf das Lesegerät übertragen werden, wobei die Verifizierung schlussendlich am Lesegerät stattfindet.

[0070] Gemäß einer weiteren Ausführungsvariante kann als Sicherheitsschlüssel auch eine Geräteeigenschaft bzw. ein Geräteparameter des Lesegeräts herangezogen werden. So kann als Sicherheitsschlüssel beispielsweise die MAC-Adresse oder eine Seriennummer des Lesegeräts verwendet werden.

[0071] Gemäß einer weiteren Ausführungsvariante können in einem Block der Blockchain die Eigentumsverhältnisse des Etiketts bzw. eines Produkts, auf dem ein Etikett angebracht ist, gespeichert sein. So kann das erfindungsgemäße Verfahren neben einer Echtheitsprüfung auch eine Besitzstandsprüfung durchführen und in Abhängigkeit des Benutzers und/oder des Lesegeräts das Eigentum am Etikett bzw. Produkt überprüfen. So kann beispielsweise durch das Scannen des Etiketts zugleich die Echtheit des Produkts festgestellt werden und überprüft werden, ob der Benutzer, welcher das Etikett scannt, der Eigentümer des Etiketts bzw. des Produkts mit dem Etikett ist.

[0072] Gemäß einer Ausführungsvariante kann zur Besitzstandsprüfung eine Benutzerkennung vom Lesegerät an den Server übertragen werden, wobei die Benutzerkennung mit dem Lesegerät des Benutzers verknüpft ist.

[0073] Gemäß einer Ausführungsvariante kann die Benutzerkennung ein Benutzername oder eine Identifikationsnummer einer digitalen Brieftasche (Wallet) sein und das Etikett in der Blockchain mit einem NFT (Non fungible Token) verknüpft sein. Das Eigentum am Etikett bzw. Produkt kann somit mit einem Eigentum an dem zugeordneten NFT verbunden sein, wobei der Server zur Besitzstandsprüfung den Eigentümer des NFT mit dem Benutzer des Lesegeräts vergleicht.

[0074] Gemäß einer Ausführungsvariante kann das elektronische Etikett in einer Schlüsselkarte integriert sein und das Lesegerät ein Türschloss sein. Hierbei kann insbesondere auch ein Berechtigungsattribut in der Blockchain oder in einer Datenbank gespeichert sein, welches etwa den Zugriff bzw. das Sperren des Türschlosses erlaubt.

[0075] So kann etwa jeder Lesevorgang durch das Türschloss in einem Block der Blockchain, insbesondere zusammen mit einem Zeitstempel (Timestamp), gespeichert werden. So kann ein lückenloser Verlauf der Öffnungsanfragen an das Türschloss dokumentiert werden.

[0076] Insbesondere bei elektronischen Geräten kann das Etikett gemäß einer Ausführungsvariante in einem elektronischen Schaltkreis des Geräts integriert sein.

[0077] In dem erfindungsgemäßen System, wie zuvor beschrieben, können insbesondere elektronisches Etikett und/oder Lesegerät und/oder Server entsprechend programmiert sein, um das Verfahren gemäß einem der Ansprüche 1 bis 16 auszuführen.

Kurzbeschreibung der Figuren

[0078] Im Folgenden werden bevorzugte Ausführungsvarianten der Erfindung anhand der Zeichnungen näher dargestellt. Es zeigen:

Fig. 1 eine schematische Darstellung eines Systems gemäß einer ersten Ausführungsvariante der Erfindung,

Fig. 2 schematische Darstellung eines Verfahrens gemäß einer ersten Ausführungsvariante der Erfindung,

Fig. 3 ein schematisches Ablaufdiagramm eines Verfahrens gemäß einer zweiten Ausführungsvariante der Erfindung, und

Fig. 4 ein schematisches Ablaufdiagramm eines Verfahrens gemäß einer dritten Ausführungsvariante der Erfindung.

Wege zur Ausführung der Erfindung

[0079] Das erfindungsgemäße System 100 wird im Folgenden anhand der in den Figuren gezeigten Ausführungsvarianten exemplarisch beschrieben.

[0080] Gemäß Fig. 1 ist eine schematische Darstellung eines Systems 100 gemäß einer ersten Ausführungsvariante der Erfindung gezeigt.

[0081] Das System 100 weist dabei ein elektronisches Etikett 1 auf, welches in einem Produkt 50 integriert ist. Das Etikett 1 kann dabei in dem Produkt 50 fest eingebaut sein, oder an dem Produkt 50 angebracht ist. Das Produkt 50 ist in Fig. 1 exemplarisch als Handtasche 51 dargestellt, wobei das Etikett 1 in einem Innenfutter der Handtasche 51 integriert, bzw. eingenäht ist. Das System 100, wie in weiterer Folge beschrieben, ist jedoch unabhängig von der Art des Produkts 50 realisierbar und das elektronische Etikett 1 kann dabei in beliebige physische Produkte integriert oder an diesen angebracht werden.

[0082] Das elektronische Etikett 1 weist wiederum einen integrierten Schaltkreis 2 auf, in welchem Daten 3 gespeichert sind. Wie exemplarisch dargestellt umfassen die Daten 3 eine Kennung zur eindeutigen Identifizierung des Etiketts UID, einen inkrementellen Zähler CNT und einen privaten Schlüssel PKEY; es können allerdings auch noch weitere, nicht dargestellte Daten gespeichert sein. Der private Schlüssel PKEY kann nicht aus dem

elektronischen Etikett ausgelesen werden, sondern ist als geheime Information gespeichert, welche nur dem integrierten Schaltkreis 2 selbst zugänglich ist.

[0083] Der integrierte Schaltkreis 2 ist insbesondere dazu programmiert, bei einem Auslesevorgang den Zählerwert CNT um eins zu erhöhen und so jeweils die aktuelle Anzahl an bisherigen Auslesevorgängen als Zählerwert CNT zu übergeben.

[0084] Zudem ist der integrierte Schaltkreis 2 im elektronischen Etikett 1 dazu programmiert, bei einem Auslesevorgang aus den Daten 3 einen Hashwert zu errechnen. Dabei werden insbesondere die auslesbaren Daten, also die Kennung UID, der Zählerwert CNT und ggf. weitere, mit dem privaten Schlüssel PKEY zu dem Hashwert HASH „verschlüsselt". Die dabei verwendete kryptografische Hashfunktion ist vorzugsweise ein OMAC-Algorithmus. Zur näheren Beschreibung wird auf die obige Darstellung der Erfindung verwiesen.

[0085] Zum Auslesen der Daten 3, weist das elektronische Etikett 1 eine Sendeeinrichtung 4 zur Datenübertragung an ein Lesegerät 5 auf. Gemäß der in Fig. 1 dargestellten Ausführungsvariante ist die Sendeeinrichtung 4 als RFID-Transponder ausgeführt, wobei das Lesegerät 5 eine Ausleseanfrage mittels Radiowellen an das elektronische Etikett 1 aussendet und dieses als Antwort die auslesbaren Daten 3 in Form einer Nachricht an das Lesegerät 5 sendet.

[0086] Die Nachricht ist dabei gemäß der dargestellten Ausführungsvariante eine Zeichenkette, welche einen URI (Uniform Ressource Identifier) darstellt, welcher vom Lesegerät empfangen und als Webadresse geöffnet werden kann. In dem URI sind die ausgelesenen Daten aus dem elektronischen Etikett 1 direkt enthalten. Die ausgelesenen Daten umfassen dabei bevorzugt die eindeutige Kennung UID, den Zählerwert CNT und den vom integrierten Schaltkreis errechneten Hashwert HASH.

[0087] Am Lesegerät 5, welches in Fig. 1 als Smartphone 6 dargestellt ist, kann die URI beispielsweise über einen Browser oder über ein entsprechendes Programm (App) aufgelöst werden. Durch das Aufrufen der URI werden die in der Nachricht an das Lesegerät 5 übertragenen Daten weiter an einen Server 7 übertragen.

[0088] Die Übertragung bzw. Kommunikation zwischen Lesegerät 5 und Server 7 erfolgt dabei über ein Netzwerk 8. Das Netzwerk 8 ist dabei bevorzugt mit dem Internet verbunden und kann vom Smartphone 6 beispielsweise über WLAN (Wireless LAN) oder über ein Funknetz (bspw. GPRS, UMTS, LTE, bzw. 2G, 3G, 4G, 5G, etc.) erreicht werden. Der Server 7 kann somit an einem anderen Standort als das Lesegerät 5 situiert sein, bzw. kann Anfragen von unterschiedlichen Lesegeräten 5 empfangen und verarbeiten.

[0089] Der Server 7 dient zur Verifizierung der gesendeten Daten; insbesondere führt der Server 7 hierzu eine Echtheitsprüfung durch, welche die übertragenen Daten, die aus dem elektronischen Etikett 1 ausgelesen wurden, mithilfe einer Blockchain 9 abgleicht. Die Blockchain 9 kann dabei in ihrer Gesamtheit auf dem Server 7 gespeichert sein. Zugleich kann die Blockchain 9 auch auf weiteren Servern gespeichert sein, was in Fig. 1 schematisch angedeutet wurde.

[0090] In der Blockchain 9 sind gemäß der ersten Ausführungsvariante zu jeder UID verschlüsselte private Schlüssel CPKEY gespeichert, wobei zur Errechnung des CPKEY der PKEY eines elektronischen Etiketts mit einem Sicherheitsschlüssel SKEY verschlüsselt wird. Diese Verschlüsselung ist voll reversibel und dient dazu, die öffentlichen Daten in der Blockchain abzusichern.

[0091] Der Server 7 ist weiters mit einer Datenbank 10 verbunden, in welcher zu jeder UID die SKEYs gespeichert sind. Damit kann der Server 7 die in der Blockchain 9 gespeicherten CPKEYs mit dem jeweiligen SKEY entschlüsseln, um den PKEY zu einer UID zu erhalten.

[0092] Mit dem errechneten PKEY am Server 7 kann somit aus den übertragenen Daten, insbesondere aus der UID und COUNT, unter Verwendung derselben kryptografischen Hashfunktion wie im elektronischen Etikett 1, ein Vergleichs-Hashwert errechnet werden. Der Vergleichs-Hashwert kann dann mit dem übertragenen Hashwert verglichen werden, wodurch bei Übereinstimmung die Echtheit des elektronischen Etiketts 1 bzw. des Produkts 50 verifiziert werden kann.

[0093] Der Server 7 kann dann wiederum das Ergebnis der Echtheitsprüfung bzw. der Verifikation an das Lesegerät 5 zurückübertragen, wo dieses Ergebnis vom Lesegerät 5 verarbeitet bzw. ausgegeben werden kann. Insbesondere wenn das Lesegerät 5 die URI in einem Browser oder Programm öffnet, so kann das Ergebnis vom Server direkt im Browser bzw. dem Programm, bevorzugt als HTML-Dokument, angezeigt werden.

[0094] Das Lesegerät 5 und der Server 7 sind gemäß der ersten Ausführungsvariante dazu programmiert, die oben genannten Schritte auszuführen.

[0095] Alternativ können gemäß einer weiteren Ausführungsvariante, welche in den Figuren nicht näher dargestellt wurde, in der Blockchain 9 zu jeder UID Vergleichs-Hashwerte für unterschiedliche Zählerwerte gespeichert sein. Der Server 7 kann dabei durch direkten Abruf der Vergleichs-Hashwerte aus der Blockchain und Vergleich mit dem übertragenen Hashwert eine Verifikation bzw. Echtheitsprüfung durchführen.

[0096] In weiterer Folge wird das erfindungsgemäße Verfahren 200, 201, 202 anhand verschiedener Ausführungsvarianten exemplarisch dargestellt.

[0097] Die im Nachfolgenden beschriebene Verfahren 200, 201, 202 können mittels des erfindungsgemäßen Systems 100 ausgeführt werden, wobei elektronisches Etikett 1 bzw. integrierter Schaltkreis 2, Lesegerät 5 und Server 7 derart programmiert sind, um die Schritte des Verfahrens 200. 201, 202 auszuführen.

[0098] Gemäß Fig. 2 ist eine schematische Darstellung des Verfahrens 200 gemäß einer ersten Ausführungsvariante gezeigt. Das Verfahren 200 weist dabei die nachfolgend beschriebenen Schritte in chronologischer Reihenfolge auf.

[0099] In Schritt 210 werden mittels einem Lesegerät 5 aus einem elektronischen Etikett 1 Daten 3 und ein Hashwert ausgelesen. Das elektronische Etikett 1 weist dabei, wie zuvor beschrieben, einen integrierten Schaltkreis 2 auf, welcher aus den im elektronischen Etikett 1 gespeicherten (auslesbaren) Daten 3 bei einem Auslesevorgang einen Hashwert erzeugt.

[0100] Das Auslesen 210 kann beispielsweise durch Halten des Lesegeräts 5 in der Nähe des Etiketts 1 initiiert werden, insbesondere wenn elektronisches Etikett 1 und Lesegerät 5 über RFID/NFC miteinander kommunizieren. Das Lesegerät 5 sendet dabei kontinuierlich Radiowellen aus, welche von dem RFID-Transponder des Etiketts 1 empfangen werden und einen Lesevorgang starten. Das Etikett 1 sendet dabei die angeforderten Daten direkt zurück an das Lesegerät 5.

[0101] Eine RFID- bzw. NFC-Kommunikation zwischen Lesegerät 5 und Etikett 1 hat den Vorteil, dass die Kommunikation nur im Nahfeld funktioniert, was das Abhören der Kommunikation zwischen Lesegerät 5 und Etikett 1 erschwert bzw. verunmöglicht.

[0102] Im nachfolgenden Schritt 220 werden die aus dem elektronischen Etikett 1 ausgelesenen Daten an einen Server 7 übertragen, um eine Verifizierung der Echtheit des elektronischen Etiketts durchzuführen. Diese Übertragung kann, wie anhand der Fig. 1 weiter oben beschrieben, besonders einfach erfolgen, wenn die aus dem elektronischen Etikett 1 ausgelesenen Daten in Form einer URI vorliegen, welche am Lesegerät aufgelöst und aufgerufen werden kann. Die URI verweist dann auf eine Netzwerkadresse des Servers 7 und beinhält alle an den Server 7 zu übertragenden Daten, insbesondere den Hashwert und die ausgelesenen Daten, wie UID und COUNT.

[0103] In Schritt 230 wird nun am Server 7 eine Verifizierung der Daten, insbesondere des Hashwerts durchgeführt, um festzustellen, ob das elektronische Etikett 1, bzw. das damit

etikettierte Produkt 50, echt ist und keine Fälschung vorliegt. Hierzu versucht der Server 7 den vom Etikett 1 errechneten Hashwert nachzuvollziehen bzw. zu bestätigen.

[0104] Erfindungsgemäß erfolgt diese Verifizierung des elektronischen Etiketts 1 anhand einer Blockchain 9. Hierzu wird vom Server 7 aus der Blockchain 9 ein Verifizierungsparameter abgerufen, anhand dem eine Verifizierung des Hashwerts erfolgen kann. Ein solcher Verifizierungsparameter kann beispielsweise gemäß einer Ausführungsvariante ein Vergleichs-Hashwert sein; gemäß einer weiteren Ausführungsvariante kann dies auch ein Vergleichs-Schlüssel sein, welcher zur Berechnung des Vergleichs-Hashwerts am Server 7 herangezogen wird.

[0105] In Schritt 240 wird das Ergebnis der Verifizierung vom Server 7 zurück an das Lesegerät 5 übertragen. Dies kann, wenn die Übertragung der Daten in Form einer URI erfolgte, als Ergebnis des Abrufs der URI geschehen. Das Lesegerät 5 ruft dabei die URI ab und wartet bis der Server 7 eine Antwort liefert.

[0106] In Schritt 250 kann das abgerufene Ergebnis der Verifizierung am Lesegerät 5 nun entsprechend verarbeitet werden. So kann das Ergebnis direkt ausgegeben werden, beispielsweise als Indikator, ob das elektronische Etikett echt ist oder nicht.

[0107] Gemäß Fig. 3 ist ein schematisches Ablaufdiagramm des Verfahrens 201 gemäß einer zweiten Ausführungsvariante gezeigt. Das Verfahren 201 weist dabei die zuvor anhand der Fig. 2 beschriebenen Schritte 210 bis 250 auf, mit den nachfolgend angeführten Besonderheiten.

[0108] Wie in Fig. 3 gezeigt, wird in Schritt 210 von dem Lesegerät 5 aus dem elektronischen Etikett 1 eine UID und der errechnete Hashwert HASH ausgelesen und vom Lesegerät 5 weiter in Schritt 220 an den Server 7 übertragen.

[0109] Die Verifizierung 230 des Hashwerts HASH am Server 7 erfolgt dann gemäß der gezeigten Ausführungsvariante anhand der Schritte 231 bis 233 wie nachfolgend beschrieben.

[0110] In Schritt 231 wird die UID an die Blockchain 9 übertragen und anhand eines Programms in der Blockchain 9 zu der UID ein zugeordneter Vergleichs-Hashwert CHASH abgerufen.

[0111] In Schritt 232 wird der CHASH zurück zum Server 7 übertragen, wo dieser in dem nachfolgenden Schritt 233 mit dem vom Lesegerät übertragenen HASH verglichen wird und

bei Übereinstimmung die Verifizierung bzw. Echtheit des elektronischen Etiketts 1 festgestellt wird.

[0112] Das Ergebnis der Verifizierung wird dann wieder in Schritt 240 zurück zum Lesegerät übertragen.

[0113] Gemäß einer weiteren Ausführungsvariante, welche in den Figuren nicht näher dargestellt ist, ist der in der Blockchain 9 gespeicherte Vergleichs-Hashwert CHASH ein trunkierter Hashwert, enthält also nur eine bestimmte Anzahl von Zeichen des Hashwerts, nicht aber den gesamten Hashwert. In Schritt 233 am Server 7 wird der (trunkierte) CHASH dann mit dem entsprechenden Teil des übertragenen HASH verglichen um die Verifizierung des elektronischen Etiketts 1 festzustellen.

[0114] Gemäß Fig. 4 ist ein schematisches Ablaufdiagramm des Verfahrens 202 gemäß einer dritten Ausführungsvariante gezeigt. Das Verfahren 202 weist dabei die zuvor anhand der Fig. 2 beschriebenen Schritte 210 bis 250 auf, mit den nachfolgend angeführten Besonderheiten.

[0115] Wie in Fig. 4 gezeigt, werden in Schritt 210 von dem Lesegerät 5 aus dem elektronischen Etikett 1 die UID, der CNT und der errechnete Hashwert HASH als Daten ausgelesen und vom Lesegerät 5 weiter in Schritt 220 an den Server 7 übertragen.

[0116] Die Verifizierung 230 des Hashwerts am Server 7 erfolgt dann gemäß der gezeigten Ausführungsvariante anhand der Schritte 231.1, 232.1, 234, 235, 236, 237 und 233.1 wie nachfolgend beschrieben.

[0117] In Schritt 231.1 wird, wie schon zuvor für Fig. 3 beschrieben, die UID an die Blockchain 9 übertragen. Allerdings wird nun anhand eines Programms in der Blockchain 9 zu der UID ein zugeordneter verschlüsselter Vergleichs-Schlüssel CPKEY abgerufen. Der CPKEY wird dann in Schritt 232.1 zurück an den Server 7 übertragen.

[0118] Im nachfolgenden Schritt 234 wird die UID nun an eine mit dem Server 7 verbundene Datenbank 10 übertragen und dort anhand der UID ein Sicherheitsschlüssel SKEY abgerufen. Dieser SKEY wird in Schritt 235 wieder zurück an den Server 7 übertragen.

[0119] Nachfolgend wird in Schritt 236 der CPKEY mit dem SKEY entschlüsselt, um einen Vergleichs-Schlüssel CKEY zu erhalten. Die Entschlüsselung des CPKEY kann dabei anhand einer definierten Verschlüsselungsfunktion erfolgen, welche ebenso zur initialen Erstellung der CPKEYs in der Blockchain 9 verwendet wird. Der entschlüsselte CKEY sollte

dabei dem privaten Schlüssel PKEY auf dem elektronischen Etikett 1 entsprechen, welcher zur Generierung des HASH aus den Daten im integrierten Schaltkreis 2 verwendet wird.

[0120] In Schritt 237 wird schließlich aus den übertragenen Daten, insbesondere UID und CNT, mittels einer kryptografischen Hashfunktion unter Einbeziehung des CKEY ein Vergleichs-Hashwert CHASH errechnet. Nachdem CKEY und PKEY aus dem elektronischen Etikett 1 identisch sein sollten, sollte bei echtem Etikett der so erzeugte CHASH mit dem vom Etikett 1 übertragenen HASH übereinstimmen.

[0121] In Schritt 233.1 wird schließlich überprüft, ob der CHASH mit dem HASH übereinstimmt und bei Übereinstimmung wird die Verifizierung bzw. Echtheit des elektronischen Etiketts 1 festgestellt.

[0122] Die oben beschriebenen Ausführungsvarianten können miteinander kombiniert werden, soweit nichts anderes angegeben ist. Zudem können die oben beschriebenen Ausführungsvarianten mit jenen in der Darstellung der Erfindung beschriebenen Ausführungsvarianten kombiniert werden.

Patentansprüche

1. Verfahren zur Verifizierung eines elektronischen Etiketts (1) zum Anbringen an ein Produkt (50), in welchem auslesbare Daten und ein geheimer Schlüssel gespeichert sind, wobei das elektronische Etikett (1) einen integrierten Schaltkreis (2) aufweist, welcher dazu ausgebildet ist aus den Daten mittels des privaten Schlüssels einen Hashwert zu errechnen, das Verfahren aufweisend die Schritte:

- Auslesen (210) der Daten und des Hashwerts aus dem elektronischen Etikett (1) durch ein Lesegerät (5),
- Übertragen (220) der Daten und des Hashwerts von dem Lesegerät (5) an einen Server (7),
- Verifizieren (230) des Hashwerts am Server (7) mittels einer Blockchain (9),
- Übertragen (240) des Ergebnisses der Verifizierung (230) von dem Server (7) an das Lesegerät (5), und
- Ausgabe und/oder Verarbeitung (250) des Ergebnisses der Verifizierung (230) am Lesegerät (5).

2. Verfahren gemäß Anspruch 1, dadurch gekennzeichnet, dass zur Verifizierung (230) des Hashwerts ein Verifizierungsparameter anhand der Daten von der Blockchain (9) angefordert wird.

3. Verfahren gemäß Anspruch 1 oder 2, dadurch gekennzeichnet, dass die auslesbaren Daten eine Kennung zur eindeutigen Identifizierung des Etiketts (1) und einen inkrementellen Zähler umfassen.

4. Verfahren gemäß Anspruch 3, dadurch gekennzeichnet, dass das Lesegerät (5) beim Auslesen der Daten aus dem elektronischen Etikett (1) die Kennung zur eindeutigen Identifizierung des Etiketts und den Zählerwert des inkrementellen Zählers empfängt.

5. Verfahren gemäß einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass zur Verifizierung des Hashwerts, dieser mit in der Blockchain (9) gespeicherten Vergleichs-Hashwerten verglichen wird.

6. Verfahren gemäß Anspruch 5, dadurch gekennzeichnet, dass die in der Blockchain (9) gespeicherten Vergleichs-Hashwerte für mehre Zählerwerte vorberechnet sind.

7. Verfahren gemäß Anspruch 5 oder 6, dadurch gekennzeichnet, dass die gespeicherten Vergleichs-Hashwerte als trunkierte Vergleichs-Hashwerte in der Blockchain (9) gespeichert sind.

8. Verfahren gemäß einem der Ansprüche 5 bis 7, dadurch gekennzeichnet, dass die Vergleichs-Hashwerte in einem auf der Blockchain (9) ausgeführten Programm, insbesondere einem Smart Contract, gespeichert sind und dass der Vergleich zwischen Hashwert und gespeicherten Vergleichs-Hashwerten beim Ausführen des Programms erfolgt.

9. Verfahren gemäß einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass zur Verifizierung (230) des Hashwerts, der Server aus der Blockchain einen Vergleichs-Schlüssel abruft, aus den empfangenen Daten und dem Vergleichs-Schlüssel einen Vergleichs-Hashwert mittels einer kryptografischen Funktion errechnet und den Hashwert mit dem Vergleichs-Hashwert vergleicht.

10. Verfahren gemäß Anspruch 9, dadurch gekennzeichnet, dass in der Blockchain (9) pro Kennung zur eindeutigen Identifizierung des Etiketts ein Vergleichs-Schlüssel gespeichert ist.

11. Verfahren gemäß Anspruch 10, dadurch gekennzeichnet, dass die Vergleichs-Schlüssel in einem auf der Blockchain (9) ausgeführten Programm gespeichert sind und dass das Programm in Abhängigkeit von einem Etikett zugeordneten Daten einen Vergleichs-Schlüssel ausgibt.

12. Verfahren gemäß einem der Ansprüche 9 bis 11, dadurch gekennzeichnet, dass die in der Blockchain (9) gespeicherten Vergleichs-Schlüssel verschlüsselt sind.

13. Verfahren gemäß Anspruch 12, dadurch gekennzeichnet, dass am Server (7) der aus der Blockchain (9) abgerufene Vergleichs-Schlüssel entschlüsselt wird, und der entschlüsselte Vergleichs-Schlüssel zur Berechnung des Vergleichs-Hashwerts herangezogen wird.

14. Verfahren gemäß Anspruch 12 oder 13, dadurch gekennzeichnet, dass ein erster Teil der in der Blockchain (9) gespeicherten Vergleichs-Schlüssel mit einem ersten Sicherheitsschlüssel verschlüsselt ist.

15. Verfahren gemäß Anspruch 14, dadurch gekennzeichnet, dass ein zweiter Teil der in der Blockchain (9) gespeicherten Vergleichs-Schlüssel mit einem zweiten Sicherheitsschlüssel verschlüsselt ist.

16. Verfahren gemäß einem der Ansprüch 12 bis 15, dadurch gekennzeichnet, dass zur Verschlüsselung und Entschlüsselung der Vergleichs-Schlüssel ein Sicherheitsschlüssel verwendet wird, welcher insbesondere in einer Datenbank (10) am Server (7) gespeichert ist.

17. System umfassend ein elektronisches Etikett (1) mit einem integrierten Schaltkreis (2) zum Anbringen an ein Produkt (50), ein Lesegerät (5) zum Auslesen von Daten aus dem elektronischen Etikett (1) und einen über ein Netzwerk (8) mit dem Lesegerät (5) verbundenen Server (7) zum Austausch von Daten, wobei der integrierte Schaltkreis (2)

- einen Speicher aufweist, in welchem auslesbare Daten und ein geheimer Schlüssel gespeichert sind, und
- dazu ausgebildet ist, beim Auslesen durch ein Lesegerät (5) einen Hashwert anhand einer kryptografischen Funktion aus den gespeicherten Daten und dem geheimen Schlüssel zu errechnen und an das Lesegerät (5) zu senden,

und wobei das Lesegerät (5)

- dazu ausgebildet ist, den Hashwert von dem elektronischen Etikett (1) zu empfangen und an einen Server (7) zur Verifikation zu senden, und
- dazu ausgebildet ist, ein Ergebnis der Verifizierung vom Server (7) zu empfangen und zu verarbeiten und/oder auszugeben,

und wobei der Server (7)

- dazu ausgebildet ist, den Hashwert vom Lesegerät (5) zu empfangen und mittels einer Blockchain (9) zu Verifizieren und
- dazu ausgebildet ist, das Ergebnis der Verifizierung an das Lesegerät (5) zu senden.

18. System gemäß Anspruch 17, dadurch gekennzeichnet, dass das elektronische Etikett (1) derart ausgebildet ist, dass der geheime Schlüssel durch ein Lesegerät (1) nicht ausgelesen werden kann.

19. System gemäß Anspruch 17 oder 18, dadurch gekennzeichnet, dass der integrierte Schaltkreis (2) im Speicher einen inkrementellen Zähler aufweist und dazu ausgebildet ist, bei einem Lesevorgang den inkrementellen Zähler zu erhöhen und aus dem Zählerwert, optional weiteren Daten und dem geheimen Schlüssel mittels einer kryptografischen Funktion den Hashwert zu errechnen.

20. System gemäß eines der Ansprüche 17 bis 19, dadurch gekennzeichnet, dass das Lesegerät (5) ein Smartphone (6), ein RFID-Lesegerät, ein Türschloss oder ein smartes Schloss ist.

Fig. 1

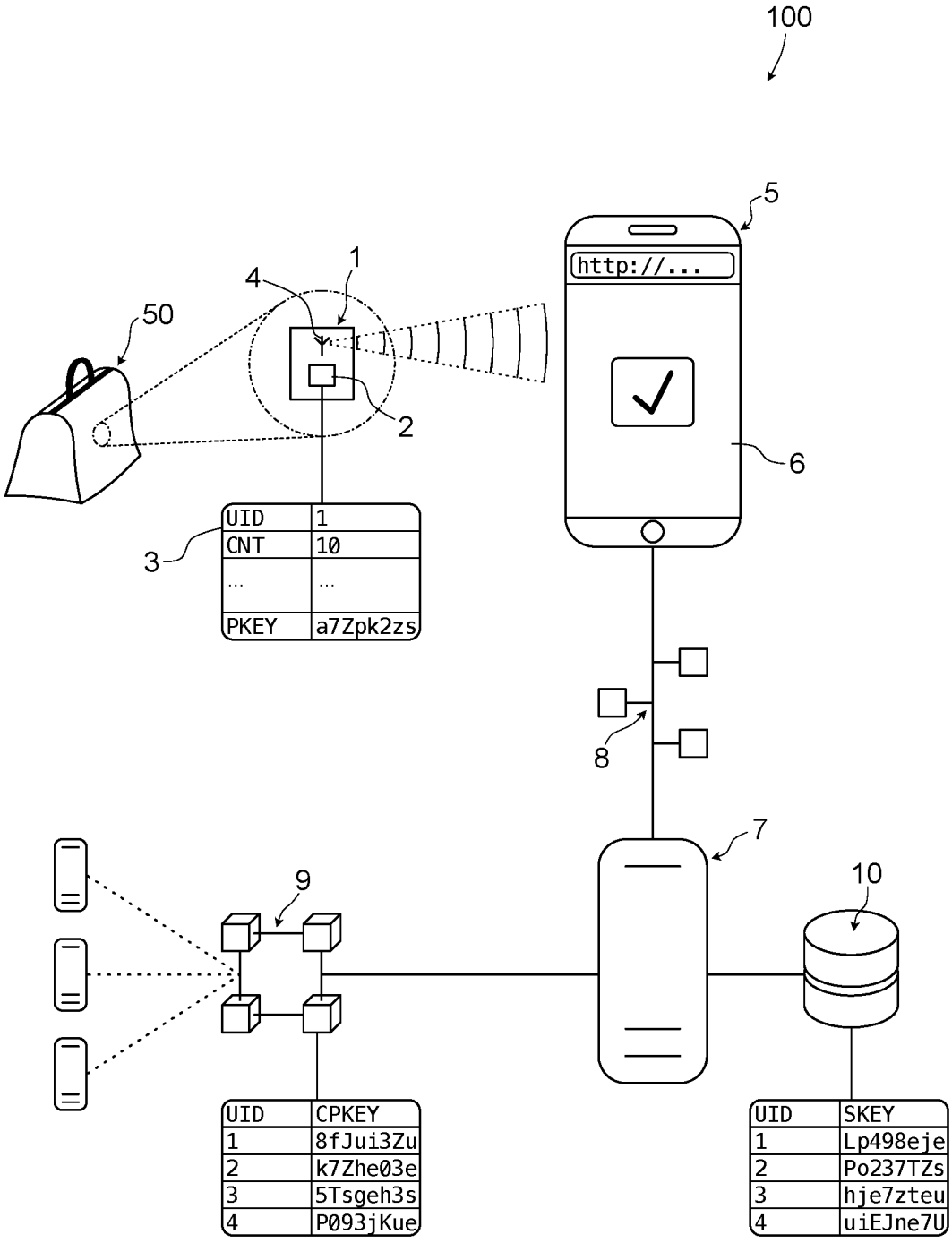

100
5
http://...
1
4
50
2
6
3
UID 1
CNT 10
... ...
PKEY a7Zpk2zs
8
7
9
10
UID CPKEY
1 8fJui3Zu
2 k7Zhe03e
3 5Tsgeh3s
4 P093jKue
UID SKEY
1 Lp498eje
2 Po237TZs
3 hje7zteu
4 uiEJne7U

Fig. 2

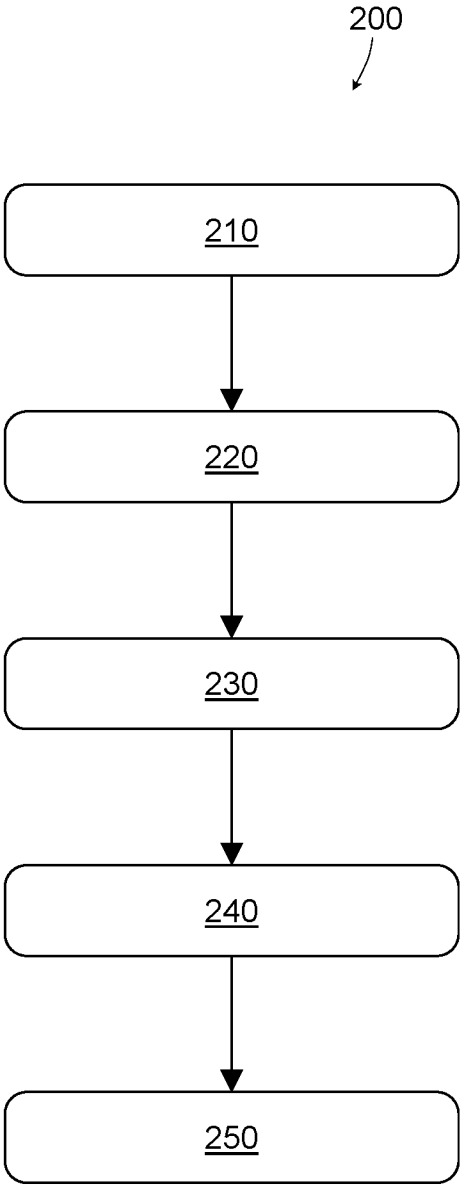


Fig. 3

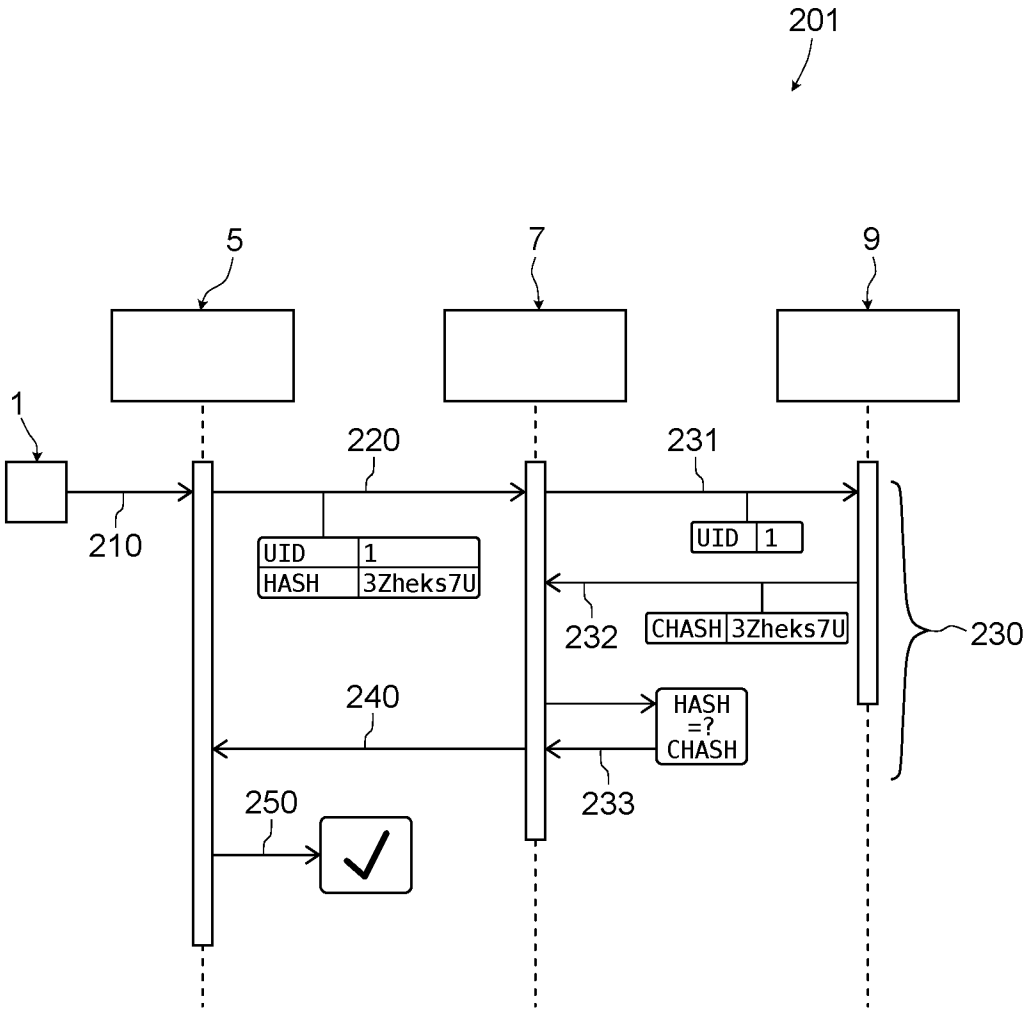
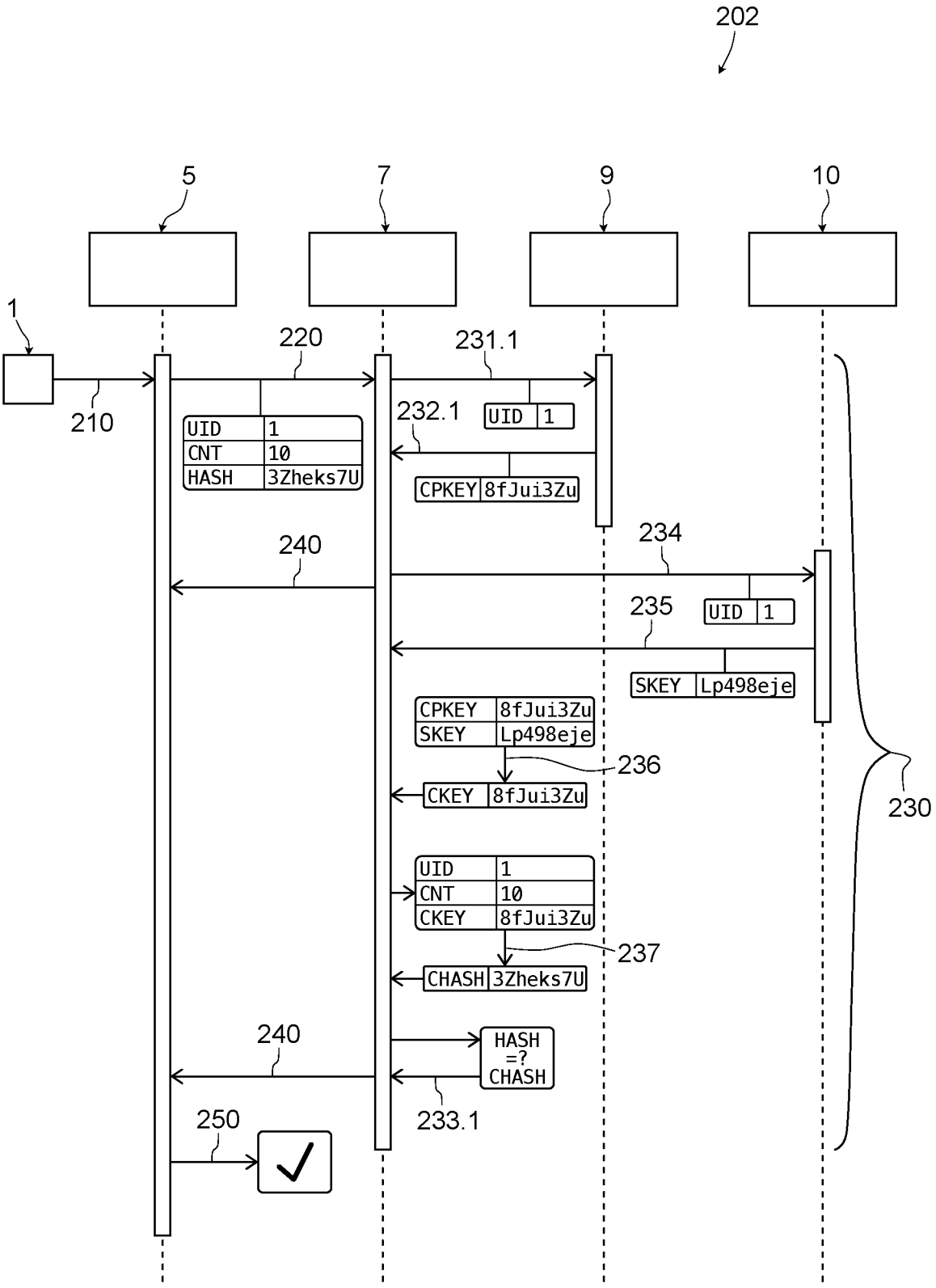

201
5
7
9
1
220
231
210
UID 1
HASH 3Zheks7U
UID 1
232
CHASH 3Zheks7U
230
240
HASH =? CHASH
233
250

Fig. 4


202
5
7
9
10
1
210
220
231.1
UID 1
CNT 10
HASH 3Zheks7U
232.1
UID 1
CPKEY 8fJui3Zu
240
234
UID 1
235
SKEY Lp498eje
CPKEY 8fJui3Zu
SKEY Lp498eje
236
CKEY 8fJui3Zu
230
UID 1
CNT 10
CKEY 8fJui3Zu
237
CHASH 3Zheks7U
240
HASH =? CHASH
233.1
250

Klassifikation des Anmeldungsgegenstands gemäß IPC:
G06K 7/10 (2006.01); ***G06K 19/07*** (2006.01); ***G06Q 30/018*** (2023.01); ***H04B 5/77*** (2024.01); ***H04L 9/32*** (2006.01); ***H04L 9/00*** (2006.01); ***H04L 9/40*** (2022.01); ***H04W 12/06*** (2009.01); ***H04W 12/47*** (2021.01)

Klassifikation des Anmeldungsgegenstands gemäß CPC:
G06K 7/10257 (2013.01); ***G06K 19/0723*** (2013.01); ***G06Q 30/0185*** (2023.01); ***H04B 5/77*** (2024.01); ***H04L 9/3236*** (2013.01); ***H04L 9/50*** (2022.05); ***H04L 63/0853*** (2022.02); ***H04L 63/126*** (2022.02); ***H04W 12/06*** (2021.01); ***H04W 12/47*** (2021.01); *H04L 2209/805* (2018.01)

Recherchierter Prüfstoff (Klassifikation):
G06K, G06Q, H04B, H04L, H04W

Konsultierte Online-Datenbank:
WPIAP, EPODOC, PATENW, PATDEW, IEEEXplore, ScienceDirect

Dieser Recherchenbericht wurde zu den am **27.02.2023** eingereichten Ansprüchen **1-20** erstellt.

Kategorie*)	Bezeichnung der Veröffentlichung: Ländercode, Veröffentlichungsnummer, Dokumentart (Anmelder), Veröffentlichungsdatum, Textstelle oder Figur soweit erforderlich	Betreffend Anspruch
X	US 2018108024 A1 (GRECO et al.) 19. April 2018 (19.04.2018) Figuren; Zusammenfassung; Abs. 0005, 0048, 0049	1, 5, 17, 18, 20
X	US 10523443 B1 (KLEINMAN BRUCE) 31. Dezember 2019 (31.12.2019) Figuren; Zusammenfassung; Spalte 1, Zeile 27 - Spalte 2, Zeile 44	1, 5, 17, 18, 20
X	MA, J. et al. "A Blockchain-Based Application System for Product Anti-Counterfeiting" IEEE Access [online]. 6. Februar 2020 (06.02.2020). Bd. 8, Seiten 77642-77652. [ermittelt am 2. Jänner 2024]. <doi:10.1109/ACCESS.2020.2972026>. Ermittelt von <https://ieeexplore.ieee.org/document/8985337>	1, 5, 17, 18, 20
X	US 2020364817 A1 (LIU et al.) 19. November 2020 (19.11.2020) Figuren; Zusammenfassung; Abs. 0080, 0081, 0107-0109	1, 5, 17, 18, 20
X	US 2021091960 A1 (WERNER et al.) 25. März 2021 (25.03.2021) Figuren; Zusammenfassung; Abs. 0047-0052	1, 5, 17, 18, 20
X	US 2021103938 A1 (BULAWSKI et al.) 08. April 2021 (08.04.2021) Figuren; Zusammenfassung; Abs. 0004, 0028	1, 5, 17, 18, 20
X	US 2021248653 A1 (MCKENZIE et al.) 12. August 2021 (12.08.2021) Figuren; Zusammenfassung; Abs. 0005	1, 5, 17, 18, 20
X	US 2021374693 A1 (LA SALLE DEREK NORMAN) 02. Dezember 2021 (02.12.2021) Figuren; Zusammenfassung; Abs. 0002, 0031	1, 5, 17, 18, 20

Datum der Beendigung der Recherche:	Seite 1 von 2	Prüfer(in):
04.01.2024		MESA PASCASIO Johannes

*) **Kategorien** der angeführten Dokumente:
- **X** Veröffentlichung **von besonderer Bedeutung**: der Anmeldungsgegenstand kann allein aufgrund dieser Druckschrift nicht als neu bzw. auf erfinderischer Tätigkeit beruhend betrachtet werden.
- **Y** Veröffentlichung **von Bedeutung**: der Anmeldungsgegenstand kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren weiteren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese **Verbindung für einen Fachmann naheliegend** ist.
- **A** Veröffentlichung, die den allgemeinen **Stand der Technik** definiert.
- **P** Dokument, das von **Bedeutung** ist (Kategorien **X** oder **Y**), jedoch **nach dem Prioritätstag** der Anmeldung veröffentlicht wurde.
- **E** Dokument, das **von besonderer Bedeutung** ist (Kategorie **X**), aus dem ein „**älteres Recht**“ hervorgehen könnte (früheres Anmeldedatum, jedoch nachveröffentlicht, Schutz ist in Österreich möglich, würde Neuheit in Frage stellen).
- **&** Veröffentlichung, die Mitglied der selben **Patentfamilie** ist.

österreichisches patentamt

Kategorie*)	Bezeichnung der Veröffentlichung: Ländercode, Veröffentlichungsnummer, Dokumentart (Anmelder), Veröffentlichungsdatum, Textstelle oder Figur soweit erforderlich	Betreffend Anspruch
X	US 2022284447 A1 (BULAWSKI et al.) 08. September 2022 (08.09.2022) Figuren; Zusammenfassung; Abs. 0004, 0028	1, 5, 17, 18, 20
X	US 2022405770 A1 (SUN et al.) 22. Dezember 2022 (22.12.2022) Figuren; Zusammenfassung; Abs. 0018	1, 5, 17, 18, 20