(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
EIDGENÖSSISCHES INSTITUT FÜR GEISTIGES EIGENTUM

(11) **CH 720 457 A2**

(51) Int. Cl.: **G06K 1/12** (2006.01)
G09C 5/00 (2006.01)
G09F 3/02 (2006.01)
H04L 9/32 (2006.01)
G04B 47/00 (2006.01)

Patentanmeldung für die Schweiz und Liechtenstein
Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(12) PATENTANMELDUNG

(21) Anmeldenummer: 000078/2024

(22) Anmeldedatum: 23.01.2024

(43) Anmeldung veröffentlicht: 15.08.2024

(30) Priorität: 26.01.2023 CH 000086/2023

(71) Anmelder:
Frank Ziemer Holding AG,
c/o Ziemer Group AG Allmendstrasse 11
2562 Port (CH)

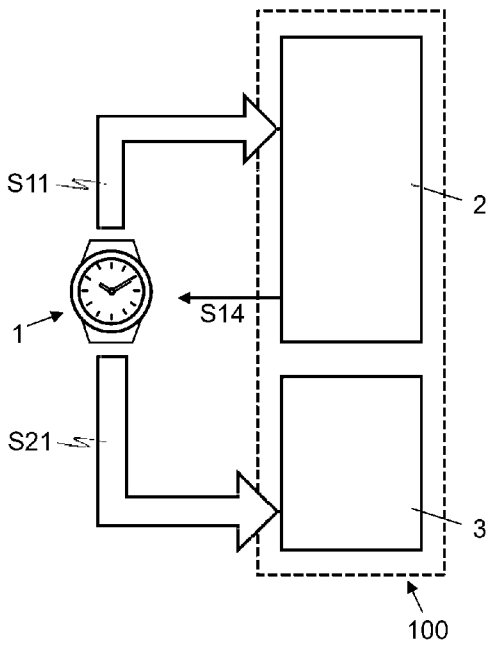
(72) Erfinder:
Christian Rathjen, 28197 Bremen (DE)
Frank Ziemer, 2562 Port (CH)
Michael Steinlechner, 8006 Zürich (CH)
Robert Chodelka, 2562 Port (CH)

(74) Vertreter:
RENTSCH PARTNER AG, Kirchenweg 8 Postfach
8034 Zürich (CH)

(54) VERFAHREN UND SYSTEM ZUR BESTIMMUNG DER AUTHENTIZITÄT EINER UHR

(57) Die Erfindung betrifft ein Verfahren (100) zur Bestimmung der Authentizität einer Uhr (1) mittels einem computergestützen Zertifizierungssystem (2) und einem computergestützten Authentifizierungssystem (3). Das computergestützte Zertifizierungssystem (2) ist so konfiguriert, dass es eine Uhr (1) durch Erzeugen (S11) von Referenzmerkmalen der Uhr unter Verwendung eines oder mehrerer physikalischer Eigenschaften der Uhr (1), die während einer Zertifizierungsphase gemessen wurden, und durch Aufzeichnen (S14) eines visuellen Codes in oder auf der Uhr (1) unter Verwendung eines Strahlschreibsystems zertifiziert. Das computergestützte Authentifizierungssystem (3) ist so konfiguriert, dass es die Uhr (1) durch Erzeugen (S21) von Uhrenverifizierungsmessungen unter Verwendung einer oder mehrerer physikalischer Eigenschaften der Uhr (1), die während einer Authentifizierungsphase gemessen wurden, durch Erfassen des visuellen Codes der Uhr (1) und durch Vergleichen der Uhrenverifizierungsmessungen und der Referenzmerkmale der Uhr unter Verwendung des von der Uhr (1) erfassten visuellen Codes authentifiziert.

Die Erfindung betrifft zudem das computergestützte Authentifizierungssystem (3).



Beschreibung

GEBIET DER OFFENBARUNG

[0001] Die vorliegende Offenbarung bezieht sich auf ein Verfahren und ein System zur Bestimmung der Authentizität einer Uhr. Insbesondere bezieht sich die vorliegende Offenbarung auf ein Verfahren zur Bestimmung der Authentizität einer Uhr und ein computergestütztes Authentifizierungssystem zur Verifizierung der Authentizität der Uhr.

HINTERGRUND DER OFFENBARUNG

[0002] In den letzten Jahren ist die Aufgabe der Authentizität von Uhren, insbesondere von wertvollen Luxusuhren und limitierten Auflagen, immer komplexer geworden. Mit der steigenden Nachfrage nach diesen exklusiven Zeitmessern nimmt auch die Zahl der Fälschungen und Nachahmungen zu. Gefälschte Uhren täuschen nicht nur ahnungslose Verbraucher, sondern fügen auch dem Ruf und den finanziellen Interessen der betroffenen Marken erheblichen Schaden zu. Die immer raffinierteren Fälscher, die fortschrittliche Fertigungstechniken anwenden und authentische Markenzeichen nachahmen, stellen eine erhebliche Bedrohung sowohl für die Verbraucher als auch für die Luxusuhrenindustrie dar. Daher besteht ein dringender Bedarf an wirksamen Verfahren und Technologien zur Echtheitsprüfung, um Fälschungen aufzuspüren und die Authentizität dieser begehrten Zeitmesser zu bewahren. Darüber hinaus wäre es von grossem Vorteil, ein zuverlässiges Verfahren zur Authentizität einer bestimmten Uhr zu entwickeln. Dazu gehört die Verknüpfung der Uhr mit ihrem Hersteller, dem Produktionsdatum, der Produktionszeit, dem Produktionsort, dem Material/der Herkunft der Komponenten, dem Eigentümer und der Provenienz (d. h. der chronologischen Geschichte des Eigentums). Eine solche Authentizität würde nicht nur eine genaue Identifizierung der echten Uhr ermöglichen, sondern auch das Aufspüren von Fälschungen oder Fälschungen erleichtern.

[0003] US 2021/158118 A1 offenbart ein gesichertes Verfahren zur Produktidentifizierung für Produkte wie Edelsteine, um Fälschungen zu verhindern, indem ein markiertes Produkt mit einer gefälschten Markierung (ID) oder einem gefälschten Strichcode versehen wird. Laut US 2021/158118 A1 erfordert das Authentifizierungsverfahren mindestens zwei identifizierende Datensätze, eine offene Markierung oder offene Daten und verdeckte Daten. Bei den offenen Daten kann es sich um einen eindeutigen Produktidentifizierer wie einen Barcode handeln. Bei den verdeckten Daten kann es sich um beliebige zusätzliche Daten handeln, die von dem jeweiligen Produkt abgeleitet sind. Bei den zusätzlichen Daten handelt es sich um einen neuen Datenpunkt, der ursprünglich nicht Teil des Produkts war, oder um einen eindeutigen Datenpunkt, der bereits im Produkt vorhanden ist, aber in keinem anderen ähnlichen Produkt. Das Produkt wird mit zentralen oder dezentralen Datenbanken authentifiziert, wenn die Kombination der Datensätze im Vergleich zu den ursprünglichen Datensätzen positiv ist. Es kann ein teilautomatisiertes oder nichtautomatisiertes Verfahren angewandt werden, bei dem z. B. ein Strichcode mit der Datenbank verknüpft wird. Die Authentizität, die sich auf zentrale oder dezentrale Datenbanken stützt, ist beeinträchtigt, wenn auf diese Datenbanken nicht zugegriffen werden kann, z. B. wegen mangelnder Netzwerkverbindungen oder Netzwerkproblemen, oder wenn die Datenbanken nicht verfügbar sind, z. B. wegen Wartungsarbeiten.

[0004] US 7,655,882 B2 offenbart eine Vorrichtung und ein Verfahren zur Erstellung einer Authentizität-Zertifizierung für einen Edelstein, mit einem Prozessor, einer mit dem Prozessor gekoppelten Datenbank, in der Daten gespeichert sind, die Laser-Mikroeinschriften und physikalische Eigenschaften einer Vielzahl von Edelsteinen definieren. Eine grafische Benutzeroberfläche (GUI) stellt in menschenlesbarer Form Informationen aus der Datenbank dar, die für einen jeweiligen Edelstein die Laser-Mikroeinschrift und die physikalischen Eigenschaften beschreiben. Die Ausgabe wird zur Authentifizierung eines vermuteten Edelsteins verwendet. In einer Ausführungsform wird die Lasermarkierung auf dem Edelstein nicht mit den in der Datenbank gespeicherten metrischen Daten verglichen, sondern es wird eine verschlüsselte Nachricht eingeschossen, die Daten über die Merkmale des Steins enthält. Ein so genanntes Public-Key/Private-Key-Verschlüsselungsprotokoll wird verwendet, um den Edelstein mit einer „digitalen Signatur" zu versehen. Die codierende Partei verschlüsselt die Daten mit einem privaten Schlüssel. Die Nachricht wird mit dem zugehörigen öffentlichen Schlüssel entschlüsselt. Die Daten in der entschlüsselten Nachricht schliessen eine Reihe eindeutiger oder quasi eindeutiger Merkmale des Edelsteins ein. Um die Herkunft des Edelsteins und seine Authentizität zu überprüfen, werden die Informationen aus der entschlüsselten Nachricht mit dem Edelstein verglichen. Diese „selbst-authentifizierende" Ausführungsform ermöglicht zwar die Verifizierung des Edelsteins ohne Zugang zu einer Datenbank, aber sie ermöglicht es auch einer böswilligen Partei, den Edelstein zu kopieren, indem sie die Merkmale des Edelsteins mit Hilfe des öffentlichen Schlüssels entschlüsselt und einen Edelstein mit denselben Merkmalen herstellt, einschliesslich einer Kopie der Lasermarkierung, die auf dem Original-Edelstein eingraviert ist.

ZUSAMMENFASSUNG DER OFFENBARUNG

[0005] Ein Gegenstand dieser Offenbarung ist es, ein Verfahren zur Bestimmung der Authentizität einer Uhr und ein computergestütztes Authentifizierungssystem zur Verifizierung der Authentizität der Uhr bereitzustellen.

[0006] Gemäss der vorliegenden Offenbarung wird der Gegenstand dieser Offenbarung durch die Merkmale der unabhängigen Ansprüche adressiert. Darüber hinaus ergeben sich weitere vorteilhafte Ausführungsformen aus den abhängigen Ansprüchen und der Beschreibung.

[0007] Gemäss der vorliegenden Offenbarung wird der oben genannte Gegenstand dieser Offenbarung insbesondere dadurch erreicht, dass zur Bestimmung der Authentizität einer Uhr ein computergestütztes Zertifizierungssystem Referenzmerkmale der Uhr durch Erfassen von Messungen einer oder mehrerer physikalischer Eigenschaften der Uhr während einer Zertifizierungsphase erzeugt. Das computergestützte Zertifizierungssystem erzeugt einen Hash der Referenzmerkmale der Uhr durch Anwendung einer kryptographischen Hash-Funktion auf die Referenzmerkmale der Uhr. Das computergestützte Zertifizierungssystem erzeugt einen visuellen Code für die Uhr unter Verwendung des Hashs der Referenzmerkmale der Uhr. Mit Hilfe eines Strahlschreibsystems wird der visuelle Code in oder auf ein oder mehrere Teile der Uhr geschrieben. Ein computergestütztes Authentifizierungssystem verifiziert die Authentizität der Uhr durch Erzeugen von Uhrenverifizierungsmessungen durch Erfassen von Messungen der einen oder mehreren physikalischen Eigenschaften der Uhr während einer Authentifizierungsphase. Das computergestützte Authentifizierungssystem erzeugt einen Hash der Uhrenverifizierungsmessungen durch Anwendung der kryptographischen Hash-Funktion auf die Uhrenverifizierungsmessungen. Das computergestützte Authentifizierungssystem erfasst den visuellen Code der Uhr und vergleicht den Hash der Uhrenverifizierungsmessungen mit dem Hash des Referenzmerkmals der Uhr unter Verwendung des von der Uhr erfassten visuellen Codes. In Abhängigkeit von dem Vergleich bestätigt oder verkennt das computergestützte Authentifizierungssystem die Authentizität der Uhr. Das Strahlschreibsystem ist zum Beispiel ein Laserstrahl-Schreibsystem, ein Ionenstrahl-Schreibsystem oder ein Elektronenstrahl-Schreibsystem.

[0008] Der Begriff „visueller Code" bezieht sich auf einen optisch erkennbaren Code. Dementsprechend ist ein Lesegerät für visuelle Codes so konfiguriert, dass der Code optisch erfasst werden kann.

[0009] In einer Ausführungsform umfasst das Erzeugen des Hashs der Referenzmerkmale der Uhr („Referenz-Hash") während der Zertifizierungsphase eine Diskretisierung (oder Rundung) der Referenzmerkmale der Uhr vor der Anwendung der kryptographischen Funktion, insbesondere der kryptographischen Hash-Funktion. Ebenso umfasst das Erzeugen des Hashs der Uhrenverifizierungsmessungen („Verifikations-Hash") während der Authentifizierungsphase eine Diskretisierung (oder Rundung) der Uhrenverifizierungsmessungen der Uhr vor der Anwendung der kryptographischen Funktion, insbesondere der kryptographischen Hash-Funktion.

[0010] In einer Ausführungsform speichert das computergestützte Zertifizierungssystem die Referenzmerkmale der Uhr, die einem eindeutigen Uhrenidentifizierer zugeordnet sind, in einem Datenspeichersystem; das computergestützte Zertifizierungssystem bestimmt den eindeutigen Uhrenidentifizierer im visuellen Code; das computergestützte Authentifizierungssystem bestimmt den Uhrenidentifizierer aus dem visuellen Code; und das computergestützte Authentifizierungssystem vergleicht die Uhrenverifizierungsmessungen mit mindestens einigen der Referenzmerkmale der Uhr, die in dem Datenspeichersystem gespeichert und dem Uhrenidentifizierer zugeordnet sind.

[0011] In einer Ausführungsform umfasst der Vergleich der Uhrenverifizierungsmessungen mit den Referenzmerkmalen der Uhr das Abrufen mindestens einiger der Referenzmerkmale der Uhr über ein Netzwerk aus dem Datenspeichersystem und/oder die Übertragung mindestens einiger der Uhrenverifizierungsmessungen und des Uhrenidentifizierers über das Netzwerk an einen Verifizierungsserver.

[0012] In einer Ausführungsform umfasst das Erzeugen des visuellen Codes das Einschliessen von Adressierungsinformationen des Datenspeichersystems und/oder des Verifizierungsservers in den visuellen Code; und das Vergleichen der Uhrenverifizierungsmessungen mit den Referenzmerkmalen der Uhr umfasst das Verwenden der in dem visuellen Code enthaltenen Adressierungsinformationen zum Abrufen von mindestens einigen der Referenzmerkmale der Uhr aus dem Datenspeichersystem und/oder das Übertragen von mindestens einigen der Uhrenverifizierungsmessungen und des Uhrenidentifizierers an den Verifizierungsserver.

[0013] In einer Ausführungsform speichert das computergestützte Zertifizierungssystem den Hash der Referenzmerkmale der Uhr in einem Blockchain-Datenspeichersystem; und das computergestützte Authentifizierungssystem vergleicht den Hash der Uhrenverifizierungsmessungen mit dem Hash der im Blockchain-Datenspeichersystem gespeicherten Referenzmerkmale der Uhr.

[0014] In einer Ausführungsform werden die Markierungen in oder auf einem oder mehreren Teilen der Uhr mit einem Strahlschreibsystem erzeugt. Das Strahlschreibsystem ist zum Beispiel ein Laserstrahlschreibsystem, ein Ionenstrahlschreibsystem oder ein Elektronenstrahlschreibsystem.

[0015] In verschiedenen Ausführungsformen umfasst das Erzeugen der Markierungen in oder auf einem oder mehreren Teilen der Uhr das Variieren des Energieniveaus des Strahlschreibsystems, das Variieren des Grades der Überlappung der Impulse des Strahlschreibsystems, das Variieren der Projektionsrichtung eines Strahls des Strahlschreibsystems und/oder das Variieren der Fokusposition des Strahls des Strahlschreibsystems.

[0016] In einer Ausführungsform werden Markierungen in oder auf einem oder mehreren Teilen der Uhr mittels Kaliumnitrat, Plasmaätzung in Kombination mit Maskierungsmaterialien, Gasphasenätzung in trockenem Sauerstoff, Gasphasenätzung in einer Mischung aus Sauerstoff und Wasserdampf und/oder Flüssigätzung in geschmolzenem Kaliumnitrat erzeugt. Das Maskierungsmaterial bzw. die Maske(n) wird/werden z. B. durch Druck auf die Oberfläche der Uhr aufgebracht.

[0017] In verschiedenen Ausführungsformen umfasst das Messen der einen oder mehreren physikalischen Eigenschaften der Uhr das Messen eines Gewichts der Uhr, das Messen einer dreidimensionalen geometrischen Form der Uhr, das Messen einer dreidimensionalen geometrischen Form eines oder mehrerer Teile der Uhr, das Messen eines Farbspektrums

eines oder mehrerer Teile der Uhr, das Messen einer chemischen Zusammensetzung eines oder mehrerer Teile der Uhr, das Messen von Markierungen in oder auf einem oder mehreren Teilen der Uhr, das Messen von Einschlüssen in einem oder mehreren Teilen der Uhr und/oder das Messen eines Hologramms in einem oder mehreren Teilen der Uhr.

[0018] Die physikalischen Eigenschaften der Uhr, die als Referenzmerkmale der Uhr verwendet werden, und die Uhrenverifizierungsmessungen umfassen eine oder mehrere physikalische Eigenschaften der Uhr, die deterministische Eigenschaften der Uhr sind. In Abhängigkeit von der Ausführungsform umfassen die deterministischen physikalischen Eigenschaften der Uhr, die als Referenzmerkmale und Uhrenverifizierungsmessungen verwendet werden, das Gewicht der Uhr, die dreidimensionale geometrische Form der Uhr, die dreidimensionale geometrische Form eines oder mehrerer Teile der Uhr, das Farbspektrum eines oder mehrerer Teile der Uhr, die chemische Zusammensetzung eines oder mehrerer Teile der Uhr, Markierungen in oder auf einem oder mehreren Teilen der Uhr und/oder Einschlüsse in einem oder mehreren Teilen der Uhr. Die Markierungen in oder auf einem oder mehreren Teilen der Uhr und/oder Einschlüsse in einem oder mehreren Teilen der Uhr werden durch relative Positionsdaten und/oder Dimensionsdaten, die die Markierungen und/oder Einschlüsse beschreiben, dargestellt. In einer Ausführungsform werden die Markierungen und/oder Einschlüsse durch eine Markierungskarte, ein dreidimensionales Markierungsmodell, eine Einschlusskarte und/oder ein dreidimensionales Einschlussmodell definiert.

[0019] In einer Ausführungsform umfassen die deterministischen physikalischen Eigenschaften der Uhr, die als Referenzmerkmale und Uhrenverifizierungsmessungen verwendet werden, ausserdem den Brechungsindex und den Leitwert der Uhr. Dies ermöglicht die Unterscheidung der Uhr von anderen Materialien.

[0020] In einer Ausführungsform umfasst das Erzeugen der Referenzmerkmale der Uhr, dass das computergestützte Zertifizierungssystem einen geheimen Uhrencode in die Referenzmerkmale der Uhr einschliesst; und das Erzeugen der Uhrenverifizierungsmessungen umfasst, dass das computergestützte Authentifizierungssystem von einem Benutzer den geheimen Uhrencode empfängt und den vom Benutzer empfangenen geheimen Uhrencode in die Uhrenverifizierungsmessungen einschliesst.

[0021] In einer Ausführungsform umfasst das Erzeugen des visuellen Codes das Erzeugen eines QR-Codes (Quick Response), und das Aufzeichnen des visuellen Codes in oder auf einem oder mehreren Teilen der Uhr umfasst das Aufzeichnen des QR-Codes in oder auf einem oder mehreren Teilen der Uhr unter Verwendung des Strahlschreibsystems.

[0022] In einer Ausführungsform besteht die Bestätigung der Authentizität der Uhr darin, dass das computergestützte Authentifizierungssystem eine Authentifizierungsnachricht erzeugt. In einer Ausführungsform schliesst die Authentifizierungsnachricht eine digitale Signatur ein, die von einer vertrauenswürdigen dritten Partei verifizierbar ist.

[0023] In einer Ausführungsform umfasst das Erzeugen des visuellen Codes, dass das computergestützte Zertifizierungssystem in den visuellen Code Adressierungsinformationen der vertrauenswürdigen dritten Partei einschliesst.

[0024] In einer Ausführungsform umfasst das Erzeugen des visuellen Codes, dass das computergestützte Zertifizierungssystem in den visuellen Code Adressierungsinformationen des Datenspeichersystems einschliesst.

[0025] In einer Ausführungsform umfasst das Erzeugen des visuellen Codes, dass das computergestützte Zertifizierungssystem in den visuellen Code Blockchain-Adressierungsinformationen einschliesst.

[0026] Neben dem Verfahren zur Bestimmung der Authentizität einer Uhr bezieht sich die vorliegende Offenbarung auch auf ein computergestütztes Authentifizierungssystem zur Verifizierung der Authentizität einer Uhr, die einen visuellen Code umfasst. Das computergestützte Authentifizierungssystem umfasst eine Verarbeitungseinheit und ein Sensorsystem, das mit der Verarbeitungseinheit verbunden ist. Die Verarbeitungseinheit ist konfiguriert, um eine oder mehrere physikalische Eigenschaften der Uhr zu erfassen, die von dem Sensorsystem während einer Authentifizierungsphase gemessen werden, und um Uhrenverifizierungsmessungen unter Verwendung der einen oder mehreren physikalischen Eigenschaften der Uhr zu erzeugen, die während der Authentifizierungsphase gemessen wurden. Die Verarbeitungseinheit ist ferner konfiguriert, um einen Hash der Uhrenverifizierungsmessungen zu erzeugen, indem eine kryptographische Hash-Funktion auf die Uhrenverifizierungsmessungen angewendet wird, und um den visuellen Code der Uhr zu erfassen. Unter Verwendung des von der Uhr erfassten visuellen Codes ist die Verarbeitungseinheit ferner so konfiguriert, dass sie den Hash der Verifikationsmessungen der Uhr mit einem Hash eines Referenzmerkmals der Uhr vergleicht, der von einem computergestützten Zertifizierungssystem aus einer oder mehreren physikalischen Eigenschaften der Uhr während einer Zertifizierungsphase erzeugt wurde, und dass sie die Authentizität der Uhr in Abhängigkeit von dem Vergleich bestätigt oder aberkennt.

[0027] Zusätzlich zu dem Verfahren und dem System zur Bestimmung der Authentizität einer Uhr bezieht sich die vorliegende Offenbarung auch auf ein Computerprogrammprodukt, das einen Computerprogrammcode zur Steuerung einer Verarbeitungseinheit eines computergestützten Authentifizierungssystems zur Verifizierung der Authentizität einer Uhr umfasst, der einen visuellen Code enthält. Insbesondere bezieht sich die vorliegende Offenbarung auf ein Computerprogrammprodukt, das ein computerlesbares Medium umfasst, auf dem der Computerprogrammcode gespeichert ist. Insbesondere bezieht sich die vorliegende Offenbarung auf ein Computerprogrammprodukt, das ein nichtflüchtiges computerlesbares Medium umfasst, auf dem der Computerprogrammcode gespeichert ist. Der Computerprogrammcode ist konfiguriert, um die Verarbeitungseinheit des computergestützten Authentifizierungssystems zu steuern, um die Authentizität der Uhr zu verifizieren, indem er die folgenden Schritte durchführt: Erfassen einer oder mehrerer physikalischer Eigenschaften der Uhr, die von einem Sensorsystem des computergestützten Authentifizierungssystems während einer

Authentifizierungsphase gemessen wurden; Erzeugen von Uhrenverifizierungsmessungen unter Verwendung der einen oder mehreren physikalischen Eigenschaften der Uhr, die während der Authentifizierungsphase gemessen wurden; Erzeugen eines Hashs der Uhrenverifizierungsmessungen durch Anwendung einer kryptographischen Hash-Funktion auf die Uhrenverifizierungsmessungen; Erzeugen eines Hashs der Uhr-Verifizierungsmessungen durch Anwenden einer kryptographischen Hash-Funktion auf die Uhr-Verifizierungsmessungen; Erzeugen eines Hashs der Uhr-Verifizierungsmessungen durch Anwenden einer kryptographischen Hash-Funktion auf die Uhrenverifizierungsmessungen; Erzeugen eines Hashs der Uhrenverifizierungsmessungen durch Anwenden einer kryptographischen Hash-Funktion auf die Uhrenverifizierungsmessungen; Erfassen des visuellen Codes der Uhr; Verwenden des von der Uhr erfassten visuellen Codes, um den Hash der Uhrenverifizierungsmessungen mit einem Hash eines Referenzmerkmals der Uhr zu vergleichen, der durch ein computergestütztes Zertifizierungssystem aus einem oder mehreren physikalischen Eigenschaften der Uhr während einer Zertifizierungsphase erzeugt wird; und Bestätigen oder Aberkennen der Authentizität der Uhr in Abhängigkeit von dem Vergleich.

KURZBESCHREIBUNG DER ZEICHNUNGEN

[0028] Die vorliegende Offenbarung wird unter Bezugnahme auf die Zeichnungen, in denen sie dargestellt ist, beispielhaft näher erläutert:

Figure 1 zeigt ein Blockdiagramm, das schematisch ein System zur Bestimmung der Authentizität einer Uhr darstellt, wobei das System ein computergestütztes Zertifizierungssystem und ein computergestütztes Authentifizierungssystem umfasst.

Figure 2 zeigt ein Blockdiagramm, das schematisch ein computergestütztes Zertifizierungssystem mit einer Verarbeitungseinheit, einem Sensorsystem, einem Strahlschreibsystem und einem Datenspeichersystem darstellt.

Figure 3 zeigt ein Blockdiagramm, das schematisch ein computergestütztes Zertifizierungssystem mit einer Verarbeitungseinheit, einem Sensorsystem und einem Strahlschreibsystem darstellt.

Figure 4 zeigt ein Blockdiagramm, das schematisch ein computergestütztes Authentifizierungssystem veranschaulicht, das ein Sensorsystem und eine Verarbeitungseinheit umfasst, die über ein Netzwerk mit einem Datenspeichersystem verbunden sind.

Figure 5 zeigt ein Blockdiagramm, das schematisch ein computergestütztes Authentifizierungssystem illustriert, das ein Sensorsystem, eine Verarbeitungseinheit und einen Verifizierungsserver umfasst, der über ein Datenspeichersystem verfügt und über ein Netzwerk mit der Verarbeitungseinheit verbunden ist.

Figure 6 zeigt ein Blockdiagramm zur schematischen Darstellung eines computergestützten Authentifizierungssystems, das ein Sensorsystem und eine Verarbeitungseinheit umfasst.

Figure 7 zeigt ein Blockdiagramm, das schematisch ein computergestütztes Authentifizierungssystem illustriert, das als mobiles Gerät implementiert ist und ein Sensorsystem und eine Verarbeitungseinheit umfasst, wobei das mobile Gerät optional über ein Netzwerk mit einem Datenspeichersystem verbunden ist.

Figure 8 zeigt ein Flussdiagramm, das eine beispielhafte Abfolge von Schritten zum Bestimmen der Authentizität einer Uhr veranschaulicht, einschliesslich des Zertifizierens der Uhr in einer Zertifizierungsphase und des Verifizierens der Authentizität der Uhr in einer Authentifizierungsphase.

Figure 9 zeigt ein Flussdiagramm, das eine beispielhafte Abfolge von Schritten zur Zertifizierung einer Uhr durch Erzeugen von Referenzmerkmalen einer Uhr während einer Zertifizierungsphase veranschaulicht, wobei die Referenzmerkmale der Uhr vor dem Aufzeichnen eines visuellen Codes in oder auf der Uhr bestimmt werden.

Figure 10 zeigt ein Flussdiagramm, das eine beispielhafte Abfolge von Schritten zur Zertifizierung einer Uhr durch Erzeugen von Referenzmerkmalen einer Uhr während einer Zertifizierungsphase veranschaulicht, wobei vor dem Bestimmen von Referenzmerkmalen der Uhr ein visueller Code in oder auf die Uhr aufgezeichnet wird.

Figure 11 zeigt ein Flussdiagramm, das eine beispielhafte Abfolge von Schritten zur Zertifizierung einer Uhr durch Erzeugen von Referenzmerkmalen einer Uhr während einer Zertifizierungsphase veranschaulicht, wobei Referenzmerkmale der Uhr vor dem Aufzeichnen eines visuellen Codes in oder auf der Uhr bestimmt werden und weitere Referenzmerkmale der Uhr bestimmt werden, nachdem der visuelle Code in oder auf der Uhr aufgezeichnet wurde.

Figure 12 zeigt ein Flussdiagramm, das eine beispielhafte Abfolge von Schritten zur Authentifizierung einer Uhr während einer Authentifizierungsphase veranschaulicht, einschliesslich des Bestimmens von Uhrenverifizierungsmessungen, des Erfassens eines visuellen Codes der Uhr und des Beurteilens der Übereinstimmung der Uhrenverifizierungsmessungen mit Uhrenreferenzmerkmalen der Uhr.

Figure 13 zeigt ein Flussdiagramm, das eine beispielhafte Abfolge von Schritten zur Bewertung der Übereinstimmung von Uhrenverifizierungsmessungen mit Referenzmerkmalen der Uhr veranschaulicht, einschliesslich des Bestimmens eines Uhrenidentifizierers aus einem visuellen Code und des Abrufens der Referenzmerkmale der Uhr aus einem Datenspeichersystem.

Figure 14 zeigt ein Flussdiagramm, das eine beispielhafte Abfolge von Schritten zur Bewertung der Übereinstimmung von Uhrenverifizierungsmessungen mit Referenzmerkmalen der Uhr veranschaulicht, einschliesslich des Bestimmens eines Uhrenidentifizierers aus einem visuellen Code und des Übertragens der Uhrenverifizierungsmessungen an einen Verifizierungsserver.

Figure 15 zeigt ein Flussdiagramm, das eine beispielhafte Abfolge von Schritten zur Bewertung der Übereinstimmung von Uhrenverifizierungsmessungen mit Referenzmerkmalen der Uhr veranschaulicht, einschliesslich des Bestimmens von Referenzmerkmalen der Uhr anhand eines visuellen Codes.

Figure 16 zeigt ein Flussdiagramm, das eine beispielhafte Abfolge von Schritten zur Bewertung der Übereinstimmung von Uhrenverifizierungsmessungen mit Referenzmerkmalen der Uhr veranschaulicht, einschliesslich des Erzeugens von transformierten Uhrenverifizierungsmessungen und des Bestimmens von transformierten Referenzmerkmalen der Uhr aus einem visuellen Code.

Figure 17 zeigt ein Flussdiagramm, das eine beispielhafte Abfolge von Schritten zur Bewertung der Übereinstimmung von Uhrenverifizierungsmessungen mit Referenzmerkmalen der Uhr veranschaulicht, einschliesslich des Erzeugens transformierter Uhrenverifizierungsmessungen, des Bestimmens von Blockchain-Adressierungsinformationen aus einem visuellen Code und des Bestimmens transformierter Referenzmerkmale der Uhr in einer Blockchain.

Figure 18 zeigt ein Flussdiagramm, das eine beispielhafte Abfolge von Schritten zur Bewertung der Übereinstimmung von Uhrenverifizierungsmessungen mit Referenzmerkmalen von Uhren veranschaulicht, einschliesslich des Erzeugens von transformierten Uhrenverifizierungsmessungen, des Bestimmens einer Blockchain-Kontoadresse aus einem visuellen Code und des Übermittelns der transformierten Uhrenverifizierungsmessungen an das Blockchain-Konto.

DETAILLIERTE BESCHREIBUNG DER AUSFÜHRUNGSFORMEN

[0029] In Figur 1 bezieht sich die Bezugsziffer 100 auf ein computergestütztes System zur Bestimmung der Authentizität einer Uhr 1, insbesondere einer Uhr 1. Wie in Figur 1 dargestellt, umfasst das System 100 ein computergestütztes Zertifizierungssystem 2 und ein computergestütztes Authentifizierungssystem 3. Das computergestützte Zertifizierungssystem 2 ist konfiguriert, um eine Uhr 1 in einer Zertifizierungsphase zu zertifizieren. Das computergestützte Authentifizierungssystem 3 ist konfiguriert, um eine Uhr 1 in einer Authentifizierungsphase zu authentifizieren.

[0030] Wie in den Figuren 2 und 3 dargestellt, umfasst das computergestützte Zertifizierungssystem 2 eine Verarbeitungseinheit 20, ein Sensorsystem 21 und ein Strahlschreibsystem 22. Das Strahlschreibsystem 22 ist zum Beispiel ein Laserstrahlschreibsystem, ein Ionenstrahlschreibsystem oder ein Elektronenstrahlschreibsystem. Die Verarbeitungseinheit 20 ist über drahtgebundene oder drahtlose Kommunikationsverbindungen oder Netzwerke 201, 202 mit dem Sensorsystem 21 und dem Strahlschreibsystem 22 verbunden. Alternativ kann die Datenkommunikation zwischen der Verarbeitungseinheit 20 und dem Sensorsystem 21 und/oder zwischen der Verarbeitungseinheit 20 und dem Strahlschreibsystem 22 von einem menschlichen Benutzer über Benutzerschnittstellen und/oder ein übertragbares Datenspeichermedium, wie ein Flash-Speichermodul, durchgeführt werden.

[0031] In den Figuren 2 und 3 bezieht sich die Referenznummer 200 auf ein Datenspeichersystem. In Abhängigkeit von der Ausführungsform umfasst das Datenspeichersystem 200 einen Datenspeicherspeicher, Datenspeicherplatten und einen oder mehrere Computer für die Verwaltung von Datenspeichern, Datenbanken und/oder verteilten Ledger-Systemen, wie z. B. Blockchain-Systeme. In der Ausführungsform von Figur 2 ist das Datenspeichersystem 200 Teil des computergestützten Zertifizierungssystems 2, das über eine drahtgebundene oder drahtlose Kommunikationsverbindung oder ein Netzwerk 203 mit der Verarbeitungseinheit 20 verbunden ist.

[0032] Zu den drahtgebundenen oder drahtlosen Kommunikationsverbindungen oder Netzwerken 201, 202, 203 gehören Kommunikationsbusse, LANs (Local Area Network) oder WLANs (Wireless Local Area Network) oder andere drahtlose Kommunikationsverbindungen wie Bluetooth oder RFID (Radio Frequency Identifier).

[0033] In der Ausführungsform der Figur 3 ist das Datenspeichersystem 200 entfernt vom computergestützten Zertifizierungssystem 2 angeordnet und mit dem computergestützten Zertifizierungssystem 2 und seiner Verarbeitungseinheit über ein Telekommunikationsnetzwerk 204, einschliesslich eines mobilen Funknetzwerks, wie z. B. ein GSM- (Global System for Mobile Communication) oder UMTS- (Universal Mobile Telephone System) Funknetzwerk, und/oder das Internet verbunden.

[0034] Die Verarbeitungseinheit 20 umfasst einen Computer, einen Prozessor und/oder eine elektronische Schaltung, die so konfiguriert ist, dass sie das Sensorsystem 21 und/oder das Strahlschreibsystem 22 steuert und Daten mit dem

Sensorsystem 21 und/oder dem Strahlschreibsystem 22 sowie dem Datenspeichersystem 200 austauscht, wie später noch näher beschrieben wird.

[0035] Das Strahlschreibsystem 22 ist konfiguriert, um einen visuellen Code, d. h. einen optisch erkennbaren Code, z. B. einen QR-Code (Quick Response), einen Strichcode und/oder einen alphanumerischen Code in oder auf die Uhr 1 zu schreiben. Das Strahlschreibsystem 22 umfasst eine Strahlquelle, z.B. eine Laserquelle, die zum Erzeugen eines Laserstrahls konfiguriert ist, z.B. eine Laserquelle zum Erzeugen eines gepulsten Laserstrahls, wie ein Nano-, Piko- oder Femtosekundenlaser. Alternativ dazu umfasst das Strahlschreibsystem 22 eine Strahlquelle, die zum Erzeugen eines Ionen- oder Elektronenstrahls konfiguriert ist. Das Strahlschreibsystem 22 umfasst ferner ein Scannersystem und ein Fokussierungssystem, die so konfiguriert sind, dass sie den Strahl so lenken und fokussieren, dass der visuelle Code in oder auf die Uhr 1 geschrieben wird.

[0036] Wie in den Figuren 4-7 dargestellt, besteht das computergestützte Authentifizierungssystem 3 aus einer Verarbeitungseinheit 30 und einem Sensorsystem 31. Die Verarbeitungseinheit 30 und das Sensorsystem 31 sind separate Geräte mit eigenem Gehäuse oder in einem Gerät mit einem Gehäuse integriert. Figur 7 zeigt ein Beispiel für eine Vorrichtung, die sowohl die Verarbeitungseinheit 30 als auch das Sensorsystem 31 umfasst. Das Gerät der Figur 7 ist beispielsweise als mobiles Gerät, z. B. ein Smartphone, ein Tablet oder ein Notebook, ausgeführt.

[0037] In den Figuren 4, 5 und 7 bezieht sich die Bezugsziffer 200' auf ein Datenspeichersystem. In Abhängigkeit von der Ausführungsform entspricht das in den Figuren 4, 5 und 7 gezeigte Datenspeichersystem 200' dem oben erörterten und in den Figuren 2 und 3 gezeigten Datenspeichersystem 200 (d. h. ist dasselbe), oder das in den Figuren 4, 5 und 7 gezeigte Datenspeichersystem 200' ist ein separates Datenspeichersystem mit demselben oder einer Teilmenge des Dateninhalts des oben erörterten und in den Figuren 2 und 3 gezeigten Datenspeichersystems 200.

[0038] In der Ausführungsform der Figur 4 und optional in der Ausführungsform der Figur 7 ist das computergestützte Authentifizierungssystem 3 bzw. dessen Verarbeitungseinheit 30 mit dem Datenspeichersystem 200' über ein Telekommunikationsnetz 5, einschliesslich eines Mobilfunknetzes, wie z. B. ein GSM- (Global System for Mobile Communication) oder UMTS-Funknetz (Universal Mobile Telephone System), und/oder das Internet verbunden.

[0039] In der Ausführungsform der Figur 5 umfasst das computergestützte Authentifizierungssystem 3 ausserdem einen Verifizierungsserver 4, der über ein Telekommunikationsnetzwerk 5 mit der Verarbeitungseinheit 30 verbunden ist. Der Verifizierungsserver 4 umfasst einen oder mehrere Computer mit einem oder mehreren Prozessoren, die mit dem Datenspeichersystem 200' über eine Kommunikationsverbindung oder ein Netzwerk 401, einschliesslich Kommunikationsbussen, LANs (Local Area Network) oder WLANs (Wireless Local Area Network), verbunden sind.

[0040] Wie in den Figuren 4-7 dargestellt, ist die Verarbeitungseinheit 30 über eine verdrahtete oder drahtlose Kommunikationsverbindung oder ein Netzwerk 301 mit dem Sensorsystem 31 verbunden. In Abhängigkeit von der Ausführungsform schliesst die drahtgebundene oder drahtlose Kommunikationsverbindung oder das Netzwerk 301 optische Schnittstellen, Kommunikationsbusse, LANs oder WLANs oder andere drahtlose Kommunikationsverbindungen, wie Bluetooth oder RFID, ein. Alternativ kann die Datenkommunikation zwischen der Verarbeitungseinheit 30 und dem Sensorsystem 31 von einem menschlichen Benutzer über Benutzerschnittstellen und/oder ein übertragbares Datenspeichermedium, wie z. B. ein Flash-Speichermodul, durchgeführt werden.

[0041] Die Verarbeitungseinheit 30 umfasst einen Computer, einen Prozessor und/oder eine elektronische Schaltung, die für die Kommunikation von Daten mit dem Datenspeichersystem 200' konfiguriert ist, wie später noch näher beschrieben wird. In Abhängigkeit von der Ausführungsform und/oder der Konfiguration ist der Computer, der Prozessor und/oder die elektronische Schaltung der Verarbeitungseinheit 30 ferner konfiguriert, um das Sensorsystem 31 zu steuern und Daten mit dem Sensorsystem 31 zu übermitteln. Die Sensorsysteme 21, 31 umfassen ein oder mehrere Geräte mit einem oder mehreren Sensoren, die konfiguriert sind, um physikalische Eigenschaften der Uhr 1 zu messen. Die Sensorsysteme 21, 31 umfassen beispielsweise eine Waage zum Messen des Gewichts der Uhr 1, ein Spektrometer zum Messen des Farbspektrums eines oder mehrerer Teile der Uhr 1, ein Massenspektrometer zum Messen der chemischen Zusammensetzung eines oder mehrerer Teile der Uhr 1, einen oder mehrere visuelle Sensoren, z.B. Kameras zum Erfassen von Bildern der Uhr 1, von Markierungen in oder auf einem oder mehreren Teilen der Uhr 1 und/oder von Einschlüssen in einem oder mehreren Teilen der Uhr 1 und/oder Tiefen- oder Abstandssensoren zum Messen dreidimensionaler Topographien der Uhr 1 oder eines oder mehrerer Teile der Uhr 1, ein oder mehrere tomographische Systeme, wie ein optisches Kohärenztomographiesystem (OCT) oder ein konfokales Mikroskop, zum Erfassen von tomografischen Daten von Einschlüssen und/oder Markierungen und deren Positionen in der Uhr 1 oder in einem oder mehreren Teilen der Uhr, und/oder ein kombiniertes Laser- und Kamerasystem, das zum Lesen eines Hologramms konfiguriert ist, das von einem Strahl des Lasers erzeugt wird, der auf Strukturen in der Uhr 1 oder in einem oder mehreren Teilen der Uhr 1 gerichtet ist und von diesen reflektiert wird. Die Sensorsysteme 21, 31 umfassen ferner Mikroskope, die optisch mit Kameras verbunden sind, um vergrösserte Bilder der Uhr 1 oder eines oder mehrerer Teile der Uhr 1, Markierungen in oder auf der Uhr 1 oder einem oder mehreren Teilen der Uhr 1 und/oder Einschlüsse in der Uhr 1 oder in einem oder mehreren Teilen der Uhr 1 zu erfassen. In einer Ausführungsform umfassen die Sensorsysteme 21, 31 ferner Messgeräte, z. B. ein Refraktometer und/oder ein Impedanzmessgerät, zum Messen des Brechungsindexes und/oder des Leitwertes des vorderen oder hinteren Glases der Uhr 1 oder von Edelsteinen, wie natürlichen und/oder hergestellten Diamanten, die in die Uhr 1 eingeschlossen und/oder an ihr befestigt sind. Das Sensorsystem 31 des computergestützten Authentifizierungssystems 3 umfasst ein Lesegerät

für visuelle Codes, das so konfiguriert ist, dass es den visuellen Code von der Uhr 1 oder von einem oder mehreren Teilen der Uhr 1 abliest. In Abhängigkeit von der Ausführungsform umfasst der Leser des visuellen Codes eine Kamera und/oder einen Scanner, der beispielsweise optisch mit einem optischen Vergrösserungssystem, wie einem Mikroskop oder einer Vergrösserungslinse, verbunden ist und so konfiguriert ist, dass er den in oder auf der Uhr 1 oder in oder auf einem oder mehreren Teilen der Uhr 1 aufgezeichneten visuellen Code vergrössert.

[0042] Die in den Figuren 6 und 7 gezeigten Ausführungsformen oder Konfigurationen des computergestützten Authentifizierungssystems 3 (ohne optionalen Zugriff auf das Datenspeichersystem 200') eignen sich besonders für die Offline-Überprüfung der Uhr 1, bei der die Bewertung der Übereinstimmung der Uhrenverifizierungsmessungen und der Referenzmerkmale der Uhr 1 keinen Zugriff auf das Datenspeichersystem 200' oder den Verifizierungsserver 4 erfordert, wie später unter Bezugnahme auf die Figuren 15 und 16 beschrieben wird.

[0043] In den folgenden Abschnitten werden unter Bezugnahme auf die Figuren 8-18 mögliche Schrittfolgen beschrieben, die vom computergestützten Zertifizierungssystem 2 oder seiner Verarbeitungseinheit 20 zur Zertifizierung einer Uhr 1 in Schritt S1 während einer Zertifizierungsphase und vom computergestützten Authentifizierungssystem 3 zur Authentifizierung der Uhr 1 in Schritt S2 während einer Authentifizierungsphase durchgeführt werden (siehe Figur 8).

[0044] Wie in Figur 9 dargestellt, erzeugt das computergestützte Zertifizierungssystem 2 zur Zertifizierung der Uhr 1 in Schritt S1 während der Zertifizierungsphase in Schritt S11 Referenzmerkmale der Uhr 1. Genauer gesagt steuert die Verarbeitungseinheit 20 des computergestützten Zertifizierungssystems 2 das Sensorsystem 21 des computergestützten Zertifizierungssystems 2, um eine oder mehrere physikalische Eigenschaften der Uhr 1 zu messen. Die Verarbeitungseinheit 20 des computergestützten Zertifizierungssystems 2 erzeugt die Referenzmerkmale der Uhr 1, indem sie einen Datensatz oder einen Datensatz bildet, der die gemessenen physikalischen Eigenschaften der Uhr 1 einschliesst. Die gemessenen physikalischen Eigenschaften der Uhr 1 stellen deterministische Eigenschaften der Uhr 1 dar. Wie oben beschrieben, umfassen Beispiele für die gemessenen physikalischen Eigenschaften der Uhr 1 das Gewicht der Uhr 1, das Farbspektrum eines oder mehrerer Teile der Uhr 1 oder eines oder mehrerer Teile der Uhr 1, die chemische Zusammensetzung eines oder mehrerer Teile der Uhr 1, ein oder mehrere Bilder der Uhr 1, Messungen und/oder Bilder von Markierungen in oder auf der Uhr 1 oder in oder auf einem oder mehreren Teilen der Uhr 1, Messungen und/oder Bilder von Einschlüssen in oder auf der Uhr 1 oder in oder auf einem oder mehreren Teilen der Uhr 1, dreidimensionale Topographien der Uhr 1 oder eines oder mehrerer Teile der Uhr 1, tomographische Daten von Einschlüssen und/oder Markierungen und deren Lage in der Uhr 1 oder in einem oder mehreren Teilen der Uhr 1 und/oder ein Hologramm in der Uhr 1 oder in einem oder mehreren Teilen der Uhr 1. In einer Ausführungsform umfassen die gemessenen physikalischen Eigenschaften der Uhr 1 ferner den Brechungsindex und/oder den Leitwert eines oder mehrerer Teile der Uhr 1, z. B. des vorderen oder hinteren Glases der Uhr 1 oder von Edelsteinen, wie natürlichen und/oder hergestellten Diamanten, die in die Uhr 1 eingeschlossen und/oder an ihr befestigt sind.

[0045] In einer Ausführungsform wird in Schritt S11 von der Verarbeitungseinheit 20 des computergestützten Zertifizierungssystems 2 ferner ein geheimer Uhrencode, z.B. ein Code mit mehreren Ziffern, z.B. 10, 20 oder mehr alphanumerischen und/oder Sonderzeichen-Ziffern (z.B. „+“, „*“, „&“, usw.), erzeugt und in die Referenzmerkmale der Uhr 1 eingeschlossen.

[0046] In einer Ausführungsform erzeugt die Verarbeitungseinheit 20 des computergestützten Zertifizierungssystems 2 in Schritt S11 ausserdem Markierungen in oder auf der Uhr oder in oder auf einem oder mehreren Teilen der Uhr 1, bevor die eine oder mehreren physikalischen Eigenschaften der Uhr 1 gemessen werden. Genauer gesagt steuert die Verarbeitungseinheit 20 des computergestützten Zertifizierungssystems 2 ein Strahlschreibsystem 22, um die Markierungen in oder auf der Uhr oder in oder auf einem oder mehreren Teilen der Uhr 1 zu erzeugen. Beispielsweise werden die Markierungen mit variierendem Energieniveau des Strahlschreibsystems 22, variierendem Grad der Überlappung der Impulse des Strahlschreibsystems 22, variierender Projektionsrichtung des Strahls des Strahlschreibsystems 22 und/oder variierender Fokusposition des Strahls des Strahlschreibsystems 22 erzeugt. In einer Ausführungsform werden zusätzlich oder alternativ Markierungen auf der Uhr oder auf einem oder mehreren Teilen der Uhr 1 unter Verwendung von Kaliumnitrat, Plasmaätzung in Kombination mit Maskierungsmaterialien, Gasphasenätzung in trockenem Sauerstoff, Gasphasenätzung in einer Mischung aus Sauerstoff und Wasserdampf und/oder Flüssigätzung in geschmolzenem Kaliumnitrat erzeugt. Das Maskierungsmaterial bzw. die Maske(n) wird (werden) z. B. durch Druck auf die Oberfläche der Uhr oder von Teilen davon aufgebracht. Die Markierungen werden zum Beispiel im oder auf dem vorderen Glas der Uhr 1, einem hinteren Glas der Uhr 1 und/oder einem oder mehreren Edelsteinen, wie natürlichen und/oder hergestellten Diamanten, die in die Uhr 1 eingeschlossen und/oder an ihr befestigt sind, erzeugt. In einer Ausführungsform werden hergestellte Einschlüsse in dem vorderen Glas der Uhr 1, einem hinteren Glas der Uhr 1 und/oder einem oder mehreren hergestellten Edelsteinen, wie natürlichen und/oder hergestellten Diamanten, die in die Uhr 1 eingeschlossen und/oder an ihr befestigt sind, erzeugt.

[0047] Die Messungen der Markierungen in oder auf der Uhr 1 oder in oder auf einem oder mehreren Teilen der Uhr 1 umfassen die Form, die Abmessungen sowie die Position und Ausrichtung in oder auf der Uhr 1 oder in oder auf einem oder mehreren Teilen der Uhr 1. Dasselbe gilt für Messungen des visuellen Codes als Markierung, wenn die Messungen nach dem Aufzeichnen des visuellen Codes in oder auf der Uhr 1 oder in oder auf einem oder mehreren Teilen der Uhr 1 vorgenommen werden, wie später unter Bezugnahme auf die Figuren 10 und 11 beschrieben wird.

[0048] In Schritt S12 verknüpft das computergestützte Zertifizierungssystem 2 bzw. dessen Verarbeitungseinheit 20 die Referenzmerkmale der Uhr mit der Uhr 1. Genauer gesagt, erzeugt die Verarbeitungseinheit 20 des computergestützten Zertifizierungssystems 2 einen eindeutigen Identifizierer für die Uhr 1 und speichert die dem eindeutigen Uhrenidentifizierer zugeordneten Referenzmerkmale der Uhr im Datenspeichersystem 200. Alternativ oder zusätzlich erzeugt die Verarbeitungseinheit 20 des computergestützten Zertifizierungssystems 2 transformierte Referenzmerkmale der Uhr durch Anwendung einer kryptographischen Funktion auf die Referenzmerkmale der Uhr, insbesondere einer kryptographischen Hash-Funktion, und speichert die transformierten Referenzmerkmale der Uhr, insbesondere den dem eindeutigen Uhrenidentifizierer zugeordneten kryptographischen Hash-Wert der Referenzmerkmale der Uhr („Referenz-Hash"), in einem Datenspeichersystem 200 einer Blockchain, z.B. einer Ethereum Blockchain. Eine kryptographische Hash-Funktion ist mit einer Einwegfunktion verwandt und erzeugt einen digitalen Fingerabdruck aus einer Eingabe, z. B. einem Datensatz oder einer Nachricht. Die kryptographische Hash-Funktion erzeugt aus der Eingabe m einen Hash-Wert h in der Weise, dass es für einen gegebenen Hash-Wert h schwierig ist, eine beliebige Eingabe m so zu finden, dass h = hash(m) ist, wobei sich „schwierig" auf die Rechenkomplexität bezieht. Ausserdem ist es bei einer Eingabe m_1 schwierig, eine andere Eingabe m_2 zu finden, bei der hash(m_1) = hash(m_2) ist. Beispiele für kryptographische Hash-Funktionen sind Message Digest 5 (MD5), die Secure Hash Algorithms (SHA), eine Familie von kryptographischen Hash-Funktionen, die vom National Institute of Standards and Technology (NIST) veröffentlicht wurden und SHA-1, SHA-2 und SHA-3 einschliessen, sowie BLAKE2 oder BLAKE3. Der eindeutige Uhrenidentifizierer schliesst eine Seriennummer, eine Herstellungsnummer, ein Herstellungsdatum, eine Herstellungszeit und/oder einen Materialreferenzcode ein. In Abhängigkeit von der Ausführungsform oder Konfiguration ist der Materialreferenzcode im Datenspeichersystem 200 mit Quelleninformationen über die spezifische Quelle von zumindest einem Teil des zum Erzeugen der Uhr 1 verwendeten Materials verknüpft. Die Quelleninformationen können eine Behälterreferenz eines Behälters, der eine Probe des für die Herstellung der Uhr 1 verwendeten Originalmaterials enthält, Multimediainformationen, wie Video-, Bild- und/oder Audioaufnahmen, die sich auf die Quelle und/oder das für die Herstellung der Uhr 1 verwendete Material beziehen, und/oder Adressierungsinformationen, wie URL oder andere Verknüpfungsinformationen, die zu solchen Multimediainformationen im Internet führen, einschliessen.

[0049] In einer Ausführungsform umfasst das Erzeugen der transformierten Referenzmerkmale der Uhr („Referenz-Hash") während der Zertifizierungsphase eine Diskretisierung der Referenzmerkmale der Uhr 1 vor der Anwendung der kryptographischen Funktion, insbesondere der kryptographischen Hash-Funktion. Mit anderen Worten werden die verschiedenen Referenzmerkmale der Uhr diskretisiert oder gerundet, indem sie durch diskrete oder „körnige" Werte dargestellt werden, mit einer definierten Genauigkeit oder Auflösung der spezifischen physikalischen Eigenschaften. Ebenso umfasst das Erzeugen von transformierten Uhrenverifizierungsmessungen („Verifikations-Hash") während der Authentifizierungsphase eine Diskretisierung der Uhrenverifizierungsmessungen der Uhr 1 vor der Anwendung der kryptographischen Funktion, insbesondere der kryptographischen Hash-Funktion. Durch die Diskretisierung oder Rundung der physikalischen Eigenschaften der Uhr 1 werden die verschiedenen physikalischen Eigenschaften der Uhr 1 in die kryptographische Funktion, insbesondere die kryptographische Hash-Funktion, mit ihrer jeweiligen Genauigkeit und Präzision eingegeben. Auf diese Weise können unterschiedliche Genauigkeiten und Präzisionen beim Messen der physikalischen Eigenschaften der Uhr 1 als Referenzmerkmale der Uhr in der Zertifizierungsphase und als Uhrenverifizierungsmessungen in der Authentifizierungsphase berücksichtigt werden. Zum Beispiel werden vor der Anwendung der kryptographischen Funktion, insbesondere der kryptographischen Hash-Funktion, die Messungen des Abstands der Uhr 1 auf eine Genauigkeit von 10 µm, vorzugsweise 5 µm, diskretisiert oder gerundet, und die Messungen des Gewichts der Uhr 1 werden auf eine Genauigkeit von 10 mg, vorzugsweise 5 mg, gerundet. Dies führt zu Toleranzschwellen von weniger als 10 µm, vorzugsweise weniger als 5 µm, für Messungen des Abstands und zu Toleranzschwellen von weniger als 10 mg, vorzugsweise weniger als 5 mg, für Messungen des Gewichts. Dies ermöglicht es beispielsweise einem Juwelier oder Uhrenhändler, für die Bestimmung der Verifizierungsmessungen in der Authentifizierungsphase Messgeräte mit einer geringeren Genauigkeit oder Präzision zu verwenden als die Messgeräte, die für die Messung der Referenzmerkmale der Uhr in der Zertifizierungsphase verwendet werden.

[0050] In Schritt S13 erzeugt das computergestützte Zertifizierungssystem 2 bzw. dessen Verarbeitungseinheit 20 einen visuellen Code für die Uhr 1, z. B. einen QR-Code oder einen Strichcode. In einer Ausführungsform schliesst der visuelle Code den eindeutigen Uhrenidentifizierer ein. Alternativ oder zusätzlich schliesst der visuelle Code Adressierungsinformationen einer vertrauenswürdigen dritten Partei (z. B. einer PKI-vertrauenswürdigen dritten Partei), des Verifizierungsservers 4 und/oder des Datenspeichersystems 200, 200', z. B. einen Hyperlink oder einen anderen Uniform Resource Locator (URL), und/oder Blockchain-Adressierungsinformationen wie eine Blockchain-Kontoadresse oder eine Blockchain-Transaktionskennung eines Blockchain-Datensatzes ein. Alternativ oder zusätzlich verwendet das computergestützte Zertifizierungssystem 2 bzw. dessen Verarbeitungseinheit 20 die Referenzmerkmale der Uhr zum Erzeugen des visuellen Codes. Zum Beispiel, wie oben beschrieben, erzeugt das computergestützte Zertifizierungssystem 2 bzw. seine Verarbeitungseinheit 20 transformierte Referenzmerkmale der Uhr durch Anwendung einer kryptographischen Funktion auf die Referenzmerkmale der Uhr, insbesondere einer kryptographischen Hash-Funktion, und schliesst die transformierten Referenzmerkmale der Uhr, insbesondere den kryptographischen Hash-Wert der Referenzmerkmale der Uhr („Referenz-Hash"), in den visuellen Code ein.

[0051] Im Schritt S14 steuert das computergestützte Zertifizierungssystem 2 bzw. dessen Verarbeitungseinheit 20 das Strahlschreibsystem 22, um den visuellen Code in oder auf die Uhr 1 zu schreiben. Genauer gesagt wird das Strahl-

schreibsystem 22 gesteuert, um den visuellen Code in oder auf einen oder mehrere Teile der Uhr 1 zu schreiben. In Abhängigkeit von der Ausführungsform und/oder der Konfiguration wird der visuelle Code in oder auf die Glasvorderseite oder die Glasrückseite der Uhr 1, auf das Zifferblatt der Uhr 1, auf das Gehäuse der Uhr 1, das Uhrwerk der Uhr 1 und/oder auf andere Teile oder Komponenten der Uhr 1 geschrieben. Der visuelle Code ist in oder auf einem oder mehreren Teilen der Uhr 1 aufgezeichnet, die einem Sensorsystem zur Verifizierung/Authentizität zugänglich sind oder zugänglich gemacht werden können.

[0052] Figur 10 zeigt eine alternative Abfolge der Schritte S11-S14 zur Zertifizierung der Uhr 1 in Schritt S1 während der Zertifizierungsphase. Insbesondere werden die Schritte S13 und S14 zum Erzeugen und Aufzeichnen des visuellen Codes in oder auf der Uhr 1 vor den Schritten S11 und S12 zum Erzeugen der Referenzmerkmale der Uhr und zur Verknüpfung der Referenzmerkmale der Uhr mit der Uhr 1 ausgeführt. Im Wesentlichen werden bei dieser alternativen Abfolge die physikalischen Parameter der Uhr 1 gemessen, nachdem der visuelle Code in oder auf die Uhr 1 geschrieben wurde. Dabei spiegeln die Referenzmerkmale der Uhr gemäss Figur 10 den visuellen Code wider, der in oder auf die Uhr 1 geschrieben wurde, jedoch schliesst der visuelle Code die Referenzmerkmale der Uhr nicht ein, wie es bei der Sequenz gemäss Figur 9 möglich wäre.

[0053] Figur 11 zeigt eine kombinierte Ausführungsform der Abläufe der Figuren 9 und 10 zur Zertifizierung der Uhr 1 in Schritt S1 während der Zertifizierungsphase. Insbesondere wird in den Schritten S11 und S12 ein erster Satz von Referenzmerkmalen der Uhr erzeugt und mit der Uhr 1 verknüpft. In den Schritten S13 und S14 wird unter Verwendung des ersten Satzes von Referenzmerkmalen der Uhr der visuelle Code erzeugt und in oder auf die Uhr 1 aufgezeichnet. In einem weiteren Schritt S11* erzeugt das computergestützte Zertifizierungssystem 2 einen zweiten Satz von Referenzmerkmalen für die Uhr 1. Der zweite Satz von Referenzmerkmalen der Uhr 1 wird wie oben mit Bezug auf die Figuren 9 oder 10 beschrieben erzeugt. In einem weiteren Schritt S12* verknüpft das computergestützte Zertifizierungssystem 2 den zweiten Satz von Referenzmerkmalen der Uhr mit der Uhr 1. Der zweite Satz von Referenzmerkmalen wird mit der Uhr 1 verknüpft, wie oben unter Bezugnahme auf die Figuren 9 oder 10 beschrieben. Im Wesentlichen wird bei dieser kombinierten Ausführungsform ein erster Satz physikalischer Parameter der Uhr 1 gemessen, bevor der visuelle Code in oder auf die Uhr 1 oder Teile davon geschrieben wurde, und ein zweiter Satz physikalischer Parameter der Uhr 1 wird gemessen, nachdem der visuelle Code in oder auf die Uhr 1 oder Teile davon geschrieben wurde. Dabei spiegelt der erste Satz der Referenzmerkmale der Uhr den visuellen Code wider, der in oder auf die Uhr 1 oder Teile davon geschrieben wurde, während der zweite Satz der Referenzmerkmale der Uhr den visuellen Code widerspiegelt, der in oder auf die Uhr 1 oder Teile davon geschrieben wurde.

[0054] Wie in Figur 12 dargestellt, bestimmt das computergestützte Authentifizierungssystem 3 zur Authentifizierung der Uhr 1 in Schritt S2 während einer Authentifizierungsphase in Schritt S21 die Uhrenverifizierungsmessungen der Uhr 1. Genauer gesagt erfasst die Verarbeitungseinheit 30 des computergestützten Authentifizierungssystems 3 Messungen von einer oder mehreren physikalischen Eigenschaften der Uhr 1. Beispielsweise steuert die Verarbeitungseinheit 30 des computergestützten Authentifizierungssystems 3 das Sensorsystem 31 des computergestützten Authentifizierungssystems 3, um die eine oder mehreren physikalischen Eigenschaften der Uhr 1 zu messen. Alternativ dazu empfängt die Verarbeitungseinheit 30 des computergestützten Authentifizierungssystems 3 die Messungen einer oder mehrerer physikalischer Eigenschaften der Uhr 1 über eine Benutzerschnittstelle von einem Benutzer, der das Sensorsystem 31 zum Messen der einen oder mehreren physikalischen Eigenschaften der Uhr 1 verwendet hat.

[0055] Wie oben beschrieben, gehören zu den gemessenen physikalischen Eigenschaften der Uhr 1 beispielsweise das Gewicht der Uhr 1, das Farbspektrum eines oder mehrerer Teile der Uhr 1, die chemische Zusammensetzung eines oder mehrerer Teile der Uhr 1, ein oder mehrere Bilder der Uhr 1, Messungen und/oder Bilder von Markierungen in oder auf der Uhr 1 oder in oder auf einem oder mehreren Teilen der Uhr 1, Messungen und/oder Bilder von Einschlüssen in der Uhr 1 oder in oder auf einem oder mehreren Teilen der Uhr 1 und/oder dreidimensionale Topografien der Uhr 1 oder eines oder mehrerer Teile der Uhr 1, tomografische Daten von Einschlüssen und/oder Markierungen und ihrer Lage in der Uhr 1 oder in einem oder mehreren Teilen der Uhr 1 und/oder ein Hologramm in der Uhr oder in einem oder mehreren Teilen der Uhr 1. In einer Ausführungsform umfassen die gemessenen physikalischen Eigenschaften der Uhr 1 ferner den Brechungsindex und/oder den Leitwert eines oder mehrerer Teile der Uhr 1, wie oben erwähnt. Wie oben in Verbindung mit Schritt S11 beschrieben, umfassen die Referenzmerkmale der Uhr in einer Ausführungsform einen geheimen Uhrencode; dementsprechend umfasst das Erzeugen der Uhrenverifizierungsmessungen in Schritt S21 ferner, dass das computergestützte Authentifizierungssystem über eine Benutzerschnittstelle von einem Benutzer den geheimen Uhrencode anfordert und empfängt und den vom Benutzer empfangenen geheimen Uhrencode in die Uhrenverifizierungsmessungen einschliesst.

[0056] In Schritt S22 wird der visuelle Code, der in oder auf der Uhr 1 aufgezeichnet ist, im computergestützten Authentifizierungssystem 3 erfasst. In einer Ausführungsform liest das computergestützte Authentifizierungssystem 3 den visuellen Code, der in oder auf der Uhr 1 aufgezeichnet ist. Genauer gesagt, steuert die Verarbeitungseinheit 30 des computergestützten Authentifizierungssystems 3 das Sensorsystem 31 des computergestützten Authentifizierungssystems 3, um den visuellen Code von der Uhr 1 zu lesen. Beispielsweise steuert die Verarbeitungseinheit 30 des computergestützten Authentifizierungssystems 3 den visuellen Code-Leser des Sensorsystems 31, um den visuellen Code von der Uhr 1 abzulesen. Alternativ dazu empfängt das computergestützte Authentifizierungssystem 3 den visuellen Code über eine Benutzerschnittstelle von einem Benutzer, der den visuellen Code von der Uhr 1 abgelesen hat.

[0057] Der Fachmann wird verstehen, dass die Reihenfolge der Schritte S21 und S22 auch umgekehrt werden kann, ohne dass sich das Ergebnis ändert.

[0058] In Schritt S23 bewertet das computergestützte Authentifizierungssystem 3 die Übereinstimmung der für die Uhr 1 in Schritt S21 bestimmten Uhrenverifizierungsmessungen und der Referenzmerkmale der Uhr 1. In Abhängigkeit von dem Ergebnis dieser Bewertung bestätigt das computergestützte Authentifizierungssystem 3 bzw. seine Verarbeitungseinheit 30 in Schritt S24 die Authentizität der Uhr 1, falls eine positive Übereinstimmung der Uhrenverifizierungsmessungen und der Referenzmerkmale der Uhr vorliegt (d.h. (d.h. die Uhrenverifizierungsmessungen und die Referenzmerkmale der Uhr stimmen innerhalb einer definierten Toleranz überein), oder erkennt die Authentizität der Uhr 1 in Schritt S25 an, falls es keine positive Übereinstimmung der Uhrenverifizierungsmessungen und der Referenzmerkmale der Uhr gibt (d.h. die Uhrenverifizierungsmessungen und die Referenzmerkmale der Uhr stimmen nicht innerhalb der definierten Toleranz überein). Verschiedene Ausführungsformen des Schritts S23 zur Beurteilung dieser Übereinstimmung werden im Folgenden unter Bezugnahme auf die Figuren 13-18 erläutert.

[0059] In Schritt S24 bestätigt das computergestützte Authentifizierungssystem 3 bzw. dessen Verarbeitungseinheit 30 die Authentizität der Uhr 1 durch Erzeugen einer Authentifizierungsnachricht. Das computergestützte Authentifizierungssystem 3 bzw. seine Verarbeitungseinheit 30 teilt dem Benutzer die Authentifizierungsnachricht über eine Benutzerschnittstelle des computergestützten Authentifizierungssystems 3, z.B. ein Display und/oder einen Lautsprecher, mit. In einer Ausführungsform schliesst die Authentifizierungsnachricht eine digitale Signatur ein, die von einer vertrauenswürdigen dritten Partei verifizierbar ist, z. B. unter Verwendung der Public Key Infrastructure (PKI). In einer Ausführungsform schliesst die Authentifizierungsnachricht den oben im Zusammenhang mit Schritt S12 beschriebenen Materialreferenzcode oder die Quellinformationen ein. Dementsprechend kann das computergestützte Authentifizierungssystem 3 bzw. seine Verarbeitungseinheit 30 bei positiver Bestätigung der Authentizität der Uhr 1 dem Benutzer auf der Benutzeroberfläche des computergestützten Authentifizierungssystems 3 zumindest einige der multimedialen Informationen in Bezug auf die Quelle und/oder das zur Herstellung der Uhr 1 verwendete Material anzeigen.

[0060] In der Ausführungsform oder Konfiguration der Figur 13 bestimmt das computergestützte Authentifizierungssystem 3 bzw. seine Verarbeitungseinheit 30 in Schritt S231 den Uhrenidentifizierer der Uhr 1 anhand des von der Uhr 1 erfassten visuellen Codes. In Schritt S232 ruft das computergestützte Authentifizierungssystem 3 bzw. dessen Verarbeitungseinheit 30 die Referenzmerkmale der Uhr 1 aus einem Datenspeichersystem 200' ab, wobei der Uhrenidentifizierer der Uhr 1 verwendet wird. In einer Ausführungsform wird die Adressierungsinformation für das Datenspeichersystem 200' aus dem von der Uhr 1 erfassten visuellen Code bestimmt. In Schritt S233 bestimmt das computergestützte Authentifizierungssystem 3 bzw. dessen Verarbeitungseinheit 30 die Authentizität der Uhr 1 durch Vergleich der Uhrenverifizierungsmessungen der Uhr 1 mit den Referenzmerkmalen der Uhr 1.

[0061] In der Ausführungsform bzw. Konfiguration der Figur 14 bestimmt das computergestützte Authentifizierungssystem 3 bzw. dessen Verarbeitungseinheit 30 in Schritt S231 den Uhrenidentifizierer der Uhr 1 aus dem von der Uhr 1 erfassten visuellen Code. Im Schritt S234 überträgt das computergestützte Authentifizierungssystem 3 bzw. dessen Verarbeitungseinheit 30 den Uhrenidentifizierer der Uhr 1 und die für die Uhr 1 bestimmten Uhrenverifizierungsmessungen an den Verifizierungsserver 4 des computergestützten Authentifizierungssystems 3. In einer Ausführungsform wird die Adressierungsinformation für den Verifizierungsserver 4 aus dem von der Uhr 1 erfassten visuellen Code bestimmt. In Schritt S235 bestimmt der Verifizierungsserver 4 des computergestützten Authentifizierungssystems 3 die Authentizität der Uhr 1, indem er die empfangenen Uhrenverifizierungsmessungen mit den Referenzmerkmalen der Uhr vergleicht, die dem empfangenen Uhrenidentifizierer der Uhr 1 im Datenspeichersystem 200' zugeordnet sind.

[0062] In der Ausführungsform oder Konfiguration der Figur 15 bestimmt das computergestützte Authentifizierungssystem 3 bzw. seine Verarbeitungseinheit 30 in Schritt S236 die Referenzmerkmale der Uhr anhand des von der Uhr 1 erfassten visuellen Codes. In Schritt S237 bestimmt das computergestützte Authentifizierungssystem 3 bzw. dessen Verarbeitungseinheit 30 die Authentizität der Uhr 1, indem es die Uhrenverifizierungsmessungen der Uhr 1 mit den aus dem visuellen Code ermittelten Referenzmerkmalen der Uhr vergleicht.

[0063] In der Ausführungsform bzw. Konfiguration der Figur 16 erzeugt das computergestützte Authentifizierungssystem 3 bzw. dessen Verarbeitungseinheit 30 in Schritt S238 transformierte Uhrenverifizierungsmessungen. Beispielsweise erzeugt das computergestützte Authentifizierungssystem 3 bzw. seine Verarbeitungseinheit 30 die transformierten Uhrenverifizierungsmessungen durch Anwendung einer kryptographischen Funktion auf die Uhrenverifizierungsmessungen der Uhr 1, insbesondere einer kryptographischen Hash-Funktion. Wie oben beschrieben, umfasst in einer Ausführungsform das Erzeugen der transformierten Uhrenverifizierungsmessungen („Verifikations-Hash") eine Diskretisierung der Uhrenverifizierungsmessungen der Uhr 1 vor der Anwendung der kryptographischen Funktion, insbesondere der kryptographischen Hash-Funktion.

[0064] In Schritt S239 bestimmt das computergestützte Authentifizierungssystem 3 bzw. dessen Verarbeitungseinheit 30 aus dem von der Uhr 1 erfassten visuellen Code transformierte Referenzmerkmale der Uhr („Referenz-Hash").

[0065] In Schritt S240 bestimmt das computergestützte Authentifizierungssystem 3 bzw. dessen Verarbeitungseinheit 30 die Authentizität der Uhr 1, indem es die transformierten Uhrenverifizierungsmessungen („Verifikations-Hash") der Uhr

1 mit den transformierten Referenzmerkmalen der Uhr („Referenz-Hash“) vergleicht, die aus dem visuellen Code ermittelt wurden.

[0066] In der Ausführungsform oder Konfiguration von Figur 17 erzeugt das computergestützte Authentifizierungssystem 3 bzw. seine Verarbeitungseinheit 30 in Schritt S238 transformierte Uhrenverifizierungsmessungen, wie oben unter Bezugnahme auf Figur 16 beschrieben. In Schritt S241 bestimmt das computergestützte Authentifizierungssystem 3 bzw. seine Verarbeitungseinheit 30 anhand des von der Uhr 1 erfassten visuellen Codes Blockchain-Adressierungsinformationen für das Blockchain-Datenspeichersystem 200', z. B. eine Blockchain-Kontoadresse oder einen Blockchain-Transaktionsidentifizierer eines Blockchain-Eintrags. In Schritt S242 bestimmt das computergestützte Authentifizierungssystem 3 bzw. dessen Verarbeitungseinheit 30 transformierte Referenzmerkmale der Uhr aus dem Blockchain-Datenspeichersystem 200' unter Verwendung der Blockchain-Adressierungsinformationen. In Schritt S243 bestimmt das computergestützte Authentifizierungssystem 3 bzw. seine Verarbeitungseinheit 30 die Authentizität der Uhr 1, indem es die transformierten Uhrenverifizierungsmessungen („Verifikations-Hash“) der Uhr 1 mit den transformierten Referenzmerkmalen der Uhr („Referenz-Hash“) vergleicht, die im Blockchain-Datenspeichersystem 200' ermittelt wurden.

[0067] In der Ausführungsform oder Konfiguration von Figur 18 erzeugt das computergestützte Authentifizierungssystem 3 bzw. seine Verarbeitungseinheit 30 in Schritt S238 transformierte Uhrenverifizierungsmessungen, wie oben unter Bezugnahme auf die Figuren 16 und 17 beschrieben. In Schritt S244 bestimmt das computergestützte Authentifizierungssystem 3 bzw. seine Verarbeitungseinheit 30 anhand des von der Uhr 1 erfassten visuellen Codes eine Blockchain-Kontoadresse für das Blockchain-Datenspeichersystem 200'. In Schritt S245 übermittelt das computergestützte Authentifizierungssystem 3 bzw. seine Verarbeitungseinheit 30 die transformierten Uhrenverifizierungsmessungen an das Blockchain-Konto des Blockchain-Datenspeichersystems 200' unter Verwendung der Blockchain-Kontoadresse. In Schritt S246 wird die Authentizität der Uhr 1 bestimmt, indem der Code eines Smart Contracts des Blockchain-Kontos ausgeführt wird, um die transformierten Uhrenverifizierungsmessungen („Verifikations-Hash“) der Uhr 1 mit den transformierten Referenzmerkmalen der Uhr („Referenz-Hash“) zu vergleichen, die im Blockchain-Datenspeichersystem 200', insbesondere im adressierten Konto des Blockchain-Datenspeichersystems 200', gespeichert sind. Der Code des Smart Contracts wird beispielsweise durch das computergestützte Authentifizierungssystem 3 bzw. dessen Verarbeitungseinheit 30 ausgeführt, die einen Knoten des Blockchain-Datenspeichersystems 200' implementiert.

[0068] Es sollte beachtet werden, dass in der Beschreibung die Abfolge der Schritte in einer bestimmten Reihenfolge dargestellt wurde, ein Fachmann wird jedoch verstehen, dass die Reihenfolge zumindest einiger der Schritte geändert werden könnte, ohne vom Umfang der Offenbarung abzuweichen.

Patentansprüche

1. Verfahren zum Bestimmen der Authentizität einer Uhr (1), umfassend:
   Erzeugen (S11) von Referenzmerkmalen der Uhr durch ein computergestütztes Zertifizierungssystem (2), das Messungen von einer oder mehreren physikalischen Eigenschaften der Uhr (1) während einer Zertifizierungsphase erfasst;
   Erzeugen, durch das computergestützte Zertifizierungssystem (2), eines Hashs der Referenzmerkmale der Uhr durch Anwendung einer kryptographischen Hash-Funktion auf die Referenzmerkmale der Uhr;
   Erzeugen (S13), durch das computergestützte Zertifizierungssystem (2), eines visuellen Codes für die Uhr (1) unter Verwendung des Hashs der Referenzmerkmale der Uhr;
   Aufzeichnen (S14) des visuellen Codes in oder auf einem oder mehreren Teilen der Uhr (1) unter Verwendung eines Strahlschreibsystems (22); und
   Verifizierung (S2) der Authentizität der Uhr (1) durch:
   Erzeugen (S21) von Uhrenverifizierungsmessungen durch ein computergestütztes Authentifizierungssystem (3), das während einer Authentifizierungsphase Messungen der einen oder mehreren physikalischen Eigenschaften der Uhr (1) erfasst;
   Erzeugen eines Hashs der Uhrenverifizierungsmessungen durch das computergestützte Authentifizierungssystem (3), wobei die kryptographische Hash-Funktion auf die Uhrenverifizierungsmessungen angewendet wird;
   Erfassen (S22), in dem computergestützten Authentifizierungssystem (3), des visuellen Codes der Uhr (1);
   Vergleichen, durch das computergestützte Authentifizierungssystem (3), des Hashs der Uhrenverifizierungsmessungen mit dem Hash des Referenzmerkmals der Uhr, unter Verwendung des erfassten visuellen Codes der Uhr (1); und
   Bestätigen (S24) oder Aberkennen (S25) der Authentizität der Uhr (1) durch das computergestützte Authentifizierungssystem (3), in Abhängigkeit von dem Vergleich.
2. Verfahren nach Anspruch 1, wobei das Verfahren ferner umfasst, dass das computergestützte Zertifizierungssystem (2) die Referenzmerkmale der Uhr, die einem eindeutigen Uhrenidentifizierer zugeordnet sind, in einem Datenspeichersystem (200) speichert; dass das computergestützte Zertifizierungssystem (2) den eindeutigen Uhrenidentifizierer in den visuellen Code einschliesst; dass das computergestützte Authentifizierungssystem (3) den Uhrenidentifizierer aus dem visuellen Code bestimmt; und dass das computergestützte Authentifizierungssystem (3) die Messungen zur Verifizierung der Uhr mit mindestens einigen der Referenzmerkmale der Uhr vergleicht (S233), die in dem Datenspeichersystem (200) gespeichert und dem Uhrenidentifizierer zugeordnet sind.

3. Verfahren nach Anspruch 2, wobei der Vergleich (S233) der Uhrenverifizierungsmessungen mit den Referenzmerkmalen der Uhr mindestens einen der folgenden Schritte umfasst: Abrufen (S232) mindestens einiger der Referenzmerkmale der Uhr über ein Netzwerk (5) aus dem Datenspeichersystem (200), oder Übertragen (S234) mindestens einiger der Uhrenverifizierungsmessungen und des Uhrenidentifizierers über das Netzwerk (5) an einen Verifizierungsserver (4).

4. Verfahren nach Anspruch 3, wobei das Erzeugen (S13) des visuellen Codes das Einschliessen von Adressierungsinformationen des Datenspeichersystems (200) und/oder des Verifizierungsservers (4) in den visuellen Code umfasst; und das Vergleichen (S233) der Uhrenverifizierungsmessungen mit den Referenzmerkmalen der Uhr das Verwenden der in dem visuellen Code enthaltenen Adressierungsinformationen zum Abrufen (S232) mindestens einiger der Referenzmerkmale der Uhr aus dem Datenspeichersystem (200) oder zum Übertragen (S234) mindestens einiger der Uhrenverifizierungsmessungen und des Uhrenidentifizierers an den Verifizierungsserver (4) umfasst.

5. Verfahren nach einem der Ansprüche 1 bis 4, wobei das Verfahren ferner umfasst, dass das computergestützte Zertifizierungssystem (2) den Hash der Referenzmerkmale der Uhr in einem Blockchain-Datenspeichersystem (200) speichert; und dass das computergestützte Authentifizierungssystem (3), das den Hash der Uhrenverifizierungsmessungen mit dem Hash der Referenzmerkmale der Uhr vergleicht (S240), die im Blockchain-Datenspeichersystem gespeichert sind.

6. Das Verfahren nach einem der Ansprüche 1 bis 5, ferner umfassend das Erzeugen von Markierungen in oder auf einem oder mehreren Teilen der Uhr (1), unter Verwendung eines Strahlschreibsystems (22).

7. Verfahren nach Anspruch 6, wobei das Erzeugen von Markierungen in oder auf einem oder mehreren Teilen der Uhr (1) mindestens eines der folgenden umfasst: Variieren eines Energieniveaus des Strahlschreibsystems (22), Variieren eines Grades der Überlappung von Impulsen des Strahlschreibsystems (22), Variieren einer Projektionsrichtung eines Strahls des Strahlschreibsystems (22) oder Variieren einer Fokusposition des Strahls des Strahlschreibsystems (22).

8. Das Verfahren nach einem der Ansprüche 1 bis 7, ferner umfassend das Erzeugen von Markierungen auf einem oder mehreren Teilen der Uhr unter Verwendung von mindestens einem der folgenden: Kaliumnitrat, Plasmaätzung in Kombination mit Maskierungsmaterialien, Gasphasenätzung in trockenem Sauerstoff, Gasphasenätzung in einer Mischung aus Sauerstoff und Wasserdampf oder Flüssigätzung in geschmolzenem Kaliumnitrat.

9. Verfahren nach einem der Ansprüche 1 bis 8, wobei das Messen der einen oder mehreren physikalischen Eigenschaften der Uhr (1) mindestens eines der folgenden umfasst: Messen eines Gewichts der Uhr (1), Messen einer dreidimensionalen geometrischen Form der Uhr (1), Messen einer dreidimensionalen geometrischen Form eines oder mehrerer Teile der Uhr (1), Messen eines Farbspektrums eines oder mehrerer Teile der Uhr (1), Messen einer chemischen Zusammensetzung eines oder mehrerer Teile der Uhr (1), Messen von Markierungen in oder auf einem oder mehreren Teilen der Uhr (1), Messen von Einschlüssen in einem oder mehreren Teilen der Uhr (1), oder Messen eines Hologramms in einem oder mehreren Teilen der Uhr (1).

10. Verfahren nach einem der Ansprüche 1 bis 9, wobei das Erzeugen (S11) der Referenzmerkmale der Uhr umfasst, dass das computergestützte Zertifizierungssystem (2) einen geheimen Uhrencode in die Referenzmerkmale der Uhr einschliesst; und das Erzeugen (S21) der Uhrenverifizierungsmessungen umfasst, dass das computergestützte Authentifizierungssystem (3) von einem Benutzer den geheimen Uhrencode empfängt und den von dem Benutzer empfangenen geheimen Uhrencode in die Uhrenverifizierungsmessungen einschliesst.

11. Verfahren nach einem der Ansprüche 1 bis 10, wobei das Erzeugen (S13) des visuellen Codes das Erzeugen eines QR-Codes umfasst, und das Aufzeichnen (S14) des visuellen Codes in oder auf einem oder mehreren Teilen der Uhr (1) das Aufzeichnen des QR-Codes in oder auf einem oder mehreren Teilen der Uhr (1) unter Verwendung des Strahlschreibsystems (22) umfasst.

12. Verfahren nach einem der Ansprüche 1 bis 11, wobei das Bestätigen (S24) der Authentizität der Uhr (1) das Erzeugen einer Authentifizierungsnachricht umfasst, wobei die Authentifizierungsnachricht eine digitale Signatur einschliesst, die von einer vertrauenswürdigen dritten Partei verifizierbar ist.

13. Verfahren nach Anspruch 12, wobei das Erzeugen (S13) des visuellen Codes das Einschliessen von Adressierungsinformationen der vertrauenswürdigen dritten Partei in den visuellen Code umfasst.

14. Computergestütztes Authentifizierungssystem (3) zum Verifizieren der Authentizität einer Uhr (1), wobei die Uhr (1) einen visuellen Code umfasst, wobei das computergestützte Authentifizierungssystem (3) eine Verarbeitungseinheit (30) und ein Sensorsystem (31) umfasst, das mit der Verarbeitungseinheit (30) verbunden ist, wobei die Verarbeitungseinheit (30) konfiguriert ist zum:
Erfassen einer oder mehrerer physikalischer Eigenschaften der Uhr (1), gemessen durch das Sensorsystem (31) während einer Authentifizierungsphase,
Erzeugen von Uhrenverifizierungsmessungen unter Verwendung der einen oder mehreren physikalischen Eigenschaften der Uhr (1), die während der Authentifizierungsphase gemessen wurden,
Erzeugen eines Hashs der Uhrenverifizierungsmessungen durch Anwendung einer kryptographischen Hash-Funktion auf die Uhrenverifizierungsmessungen;
Erfassen des visuellen Codes der Uhr (1),

Verwenden des von der Uhr erfassten visuellen Codes, um den Hash der Uhrenverifizierungsmessungen mit einem Hash eines Referenzmerkmals der Uhr zu vergleichen, der von einem computergestützten Zertifizierungssystem (2) aus einer oder mehreren physikalischen Eigenschaften der Uhr (1) während einer Zertifizierungsphase erzeugt wird, und

Bestätigen oder Aberkennen der Authentizität der Uhr (1) in Abhängigkeit von dem Vergleich.

15. Computerprogrammprodukt, das ein nichtflüchtiges computerlesbares Medium umfasst, auf dem Computerprogrammcode gespeichert ist, der konfiguriert ist, um eine Verarbeitungseinheit (30) eines computergestützten Authentifizierungssystems (3) zu steuern, um die Authentizität einer Uhr (1) zu verifizieren, wobei die Uhr (1) einen visuellen Code umfasst, indem die folgenden Schritte durchgeführt werden:
Erfassen einer oder mehrerer physikalischer Eigenschaften der Uhr (1), gemessen durch ein Sensorsystem (31) des computergestützten Authentifizierungssystems (3) während einer Authentifizierungsphase,
Erzeugen von Uhrenverifizierungsmessungen unter Verwendung der einen oder mehreren physikalischen Eigenschaften der Uhr (1), die während der Authentifizierungsphase gemessen wurden,
Erzeugen eines Hashs der Uhrenverifizierungsmessungen durch Anwendung einer kryptographischen Hash-Funktion auf die Uhrenverifizierungsmessungen;
Erfassen des visuellen Codes der Uhr (1),
Verwenden des von der Uhr erfassten visuellen Codes, um den Hash der Uhrenverifizierungsmessungen und einen Hash eines Referenzmerkmals der Uhr zu vergleichen, der von einem computergestützten Zertifizierungssystem (2) aus einer oder mehreren physikalischen Eigenschaften der Uhr (1) während einer Zertifizierungsphase erzeugt wird, und
Bestätigen oder Aberkennen der Authentizität der Uhr (1) in Abhängigkeit von dem Vergleich.

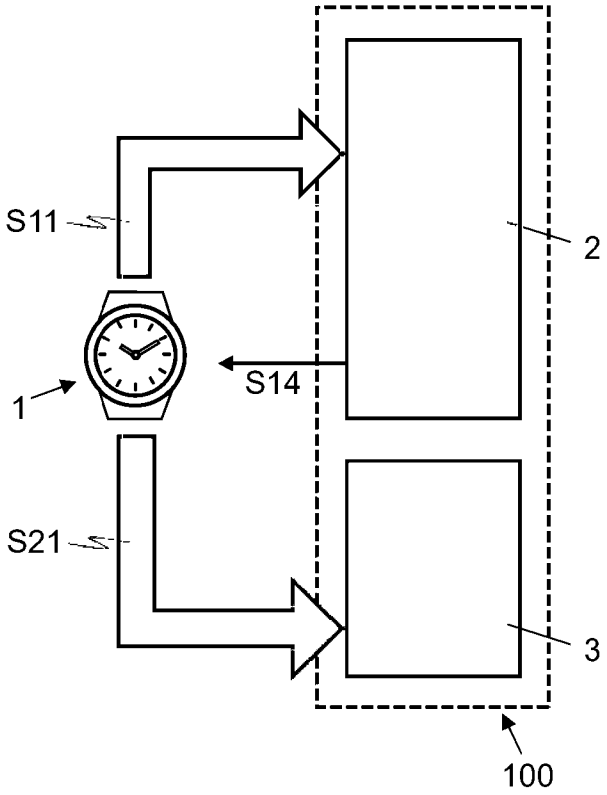


Fig. 1

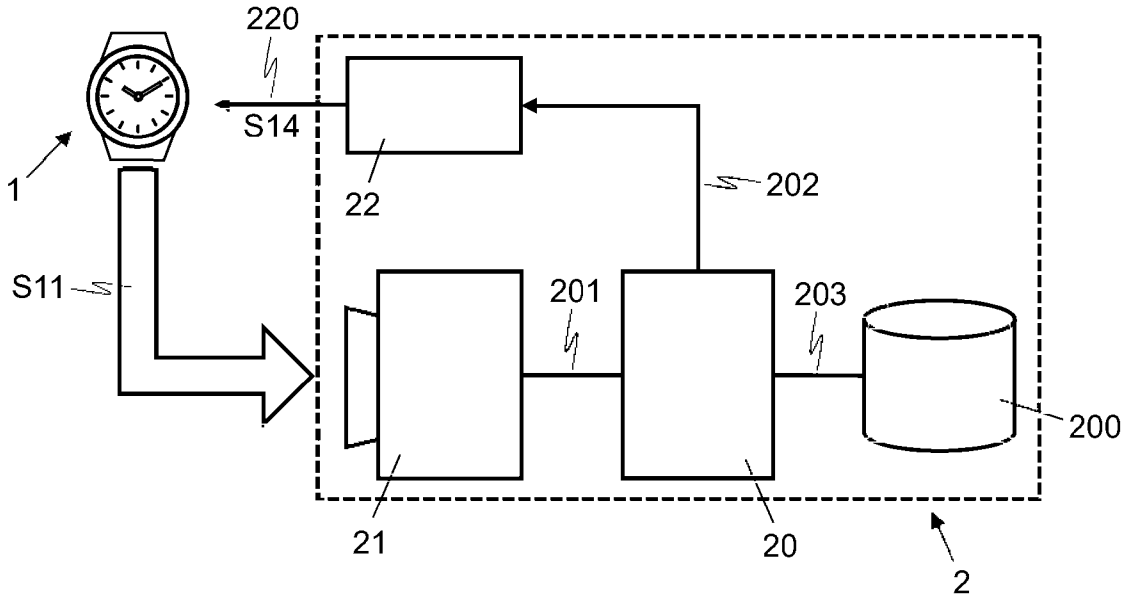


Fig. 2

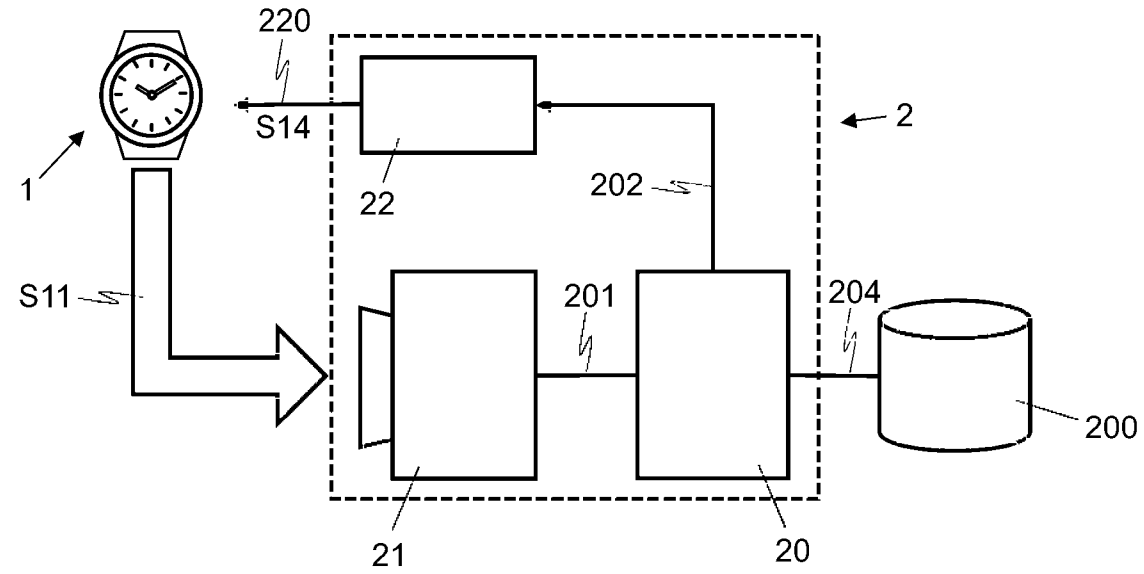


Fig. 3

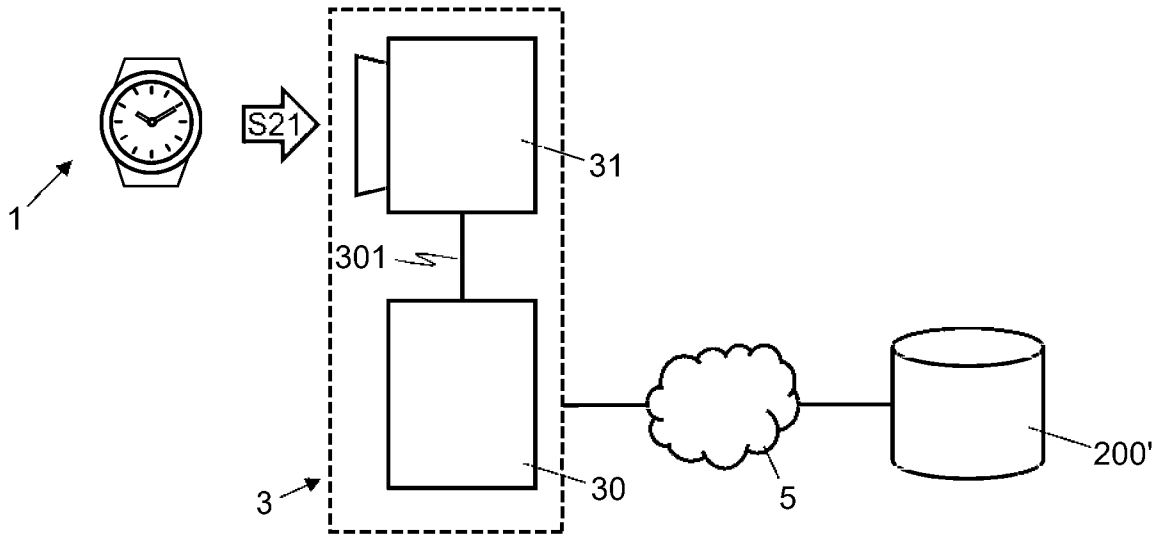


Fig. 4

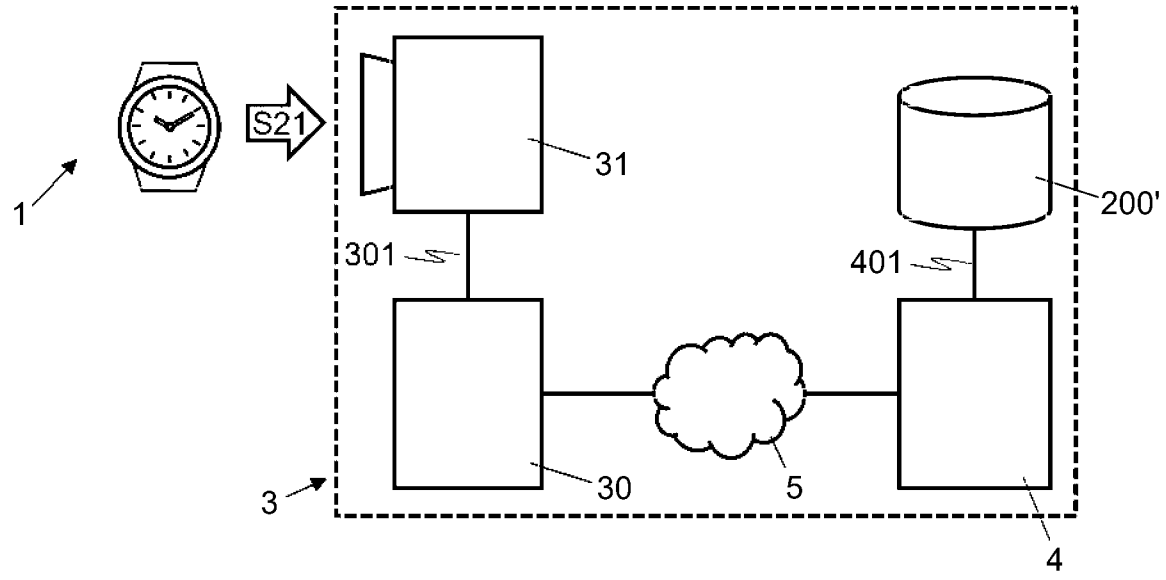


Fig. 5

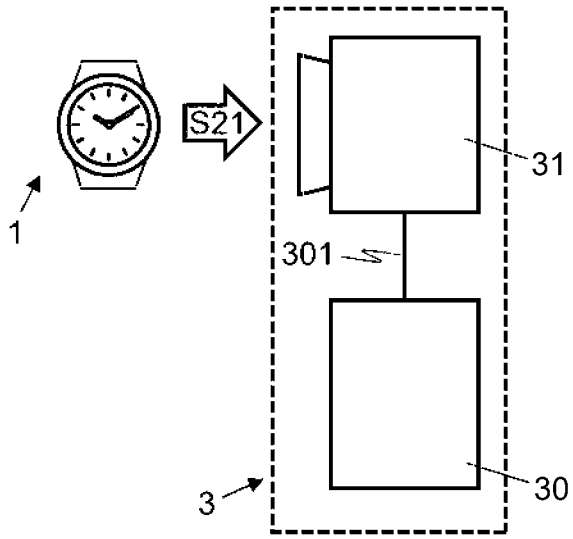


Fig. 6

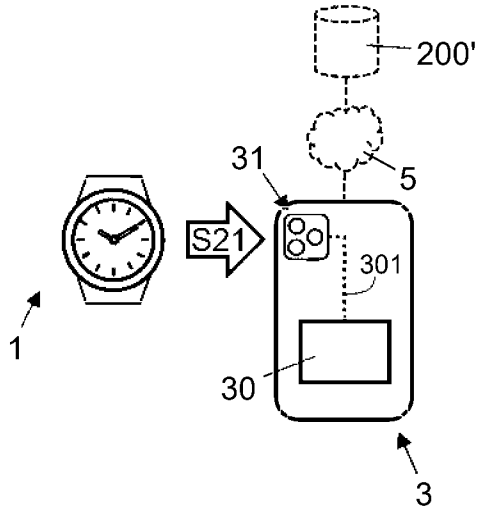


Fig. 7

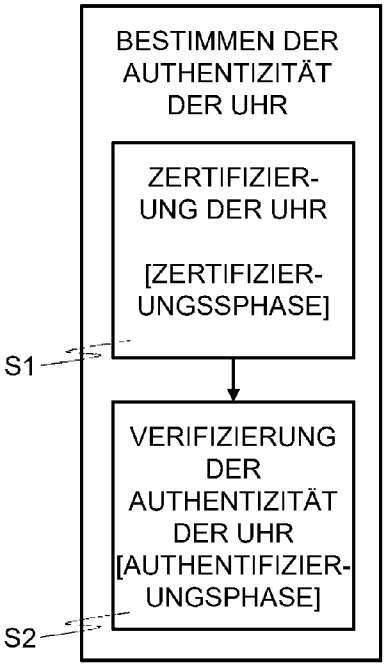


Fig. 8

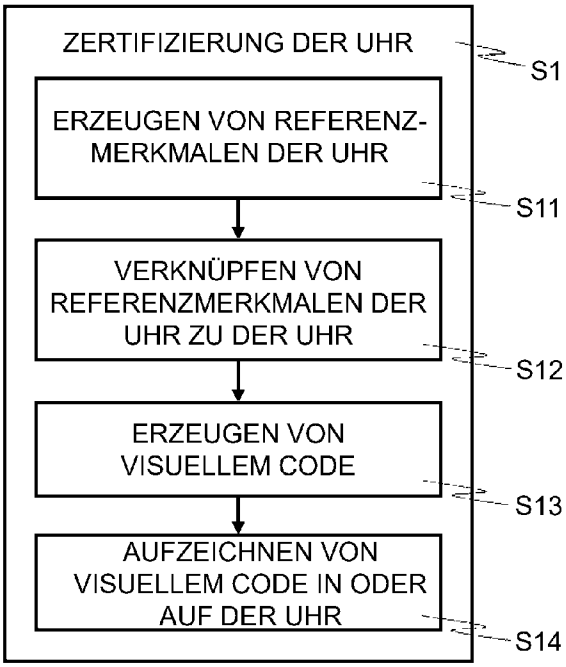


Fig. 9

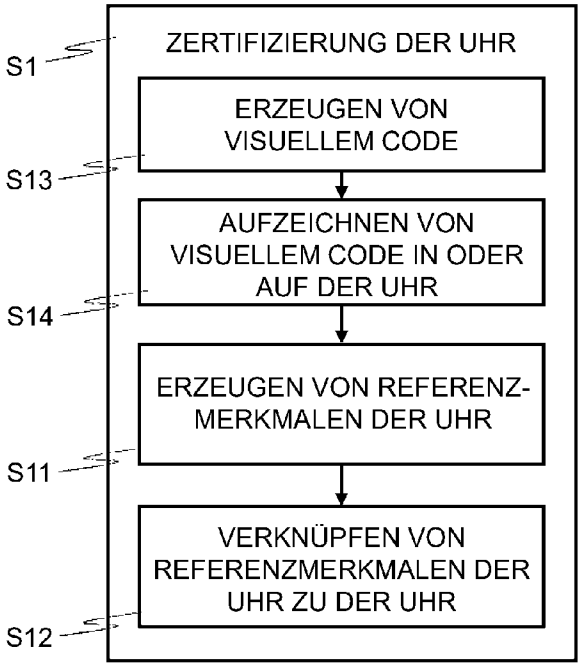


Fig. 10

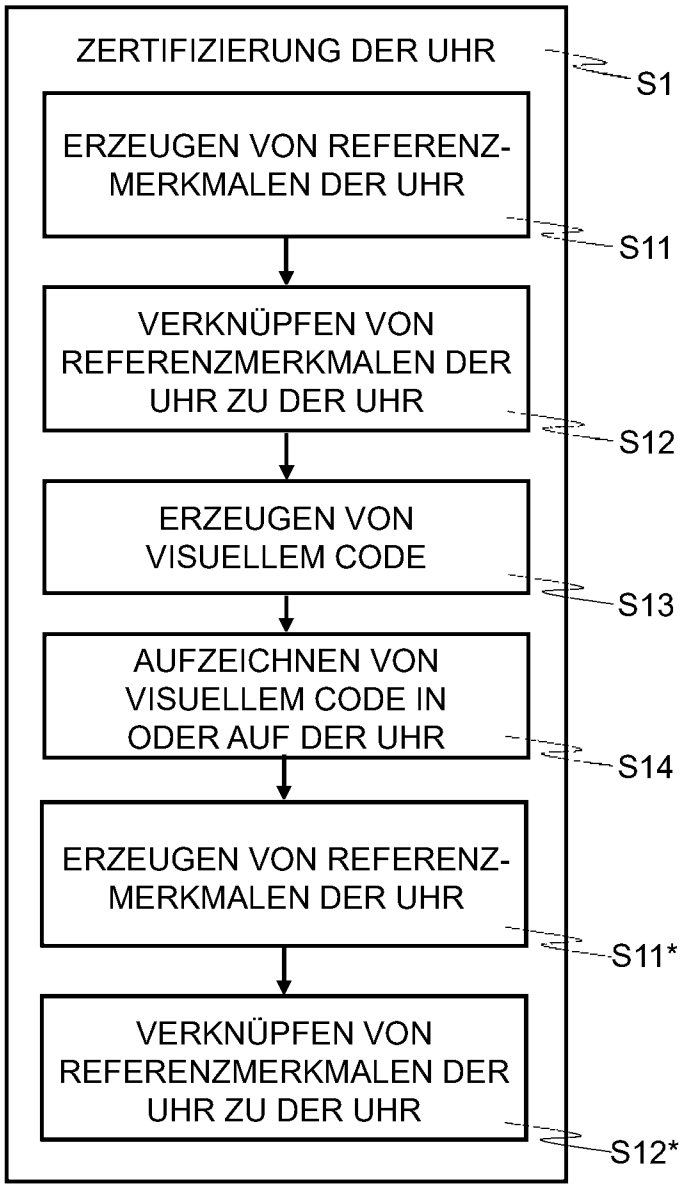

ZERTIFIZIERUNG DER UHR
S1
ERZEUGEN VON REFERENZ-MERKMALEN DER UHR
S11
VERKNÜPFEN VON REFERENZMERKMALEN DER UHR ZU DER UHR
S12
ERZEUGEN VON VISUELLEM CODE
S13
AUFZEICHNEN VON VISUELLEM CODE IN ODER AUF DER UHR
S14
ERZEUGEN VON REFERENZ-MERKMALEN DER UHR
S11*
VERKNÜPFEN VON REFERENZMERKMALEN DER UHR ZU DER UHR
S12*

Fig. 11

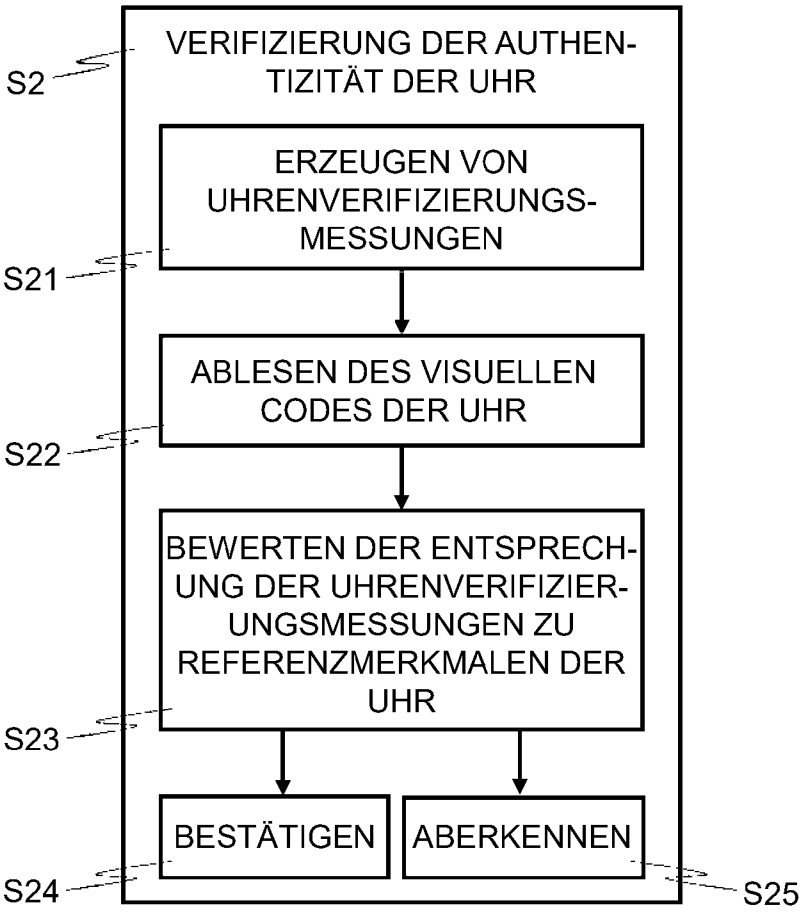

S2
VERIFIZIERUNG DER AUTHEN-TIZITÄT DER UHR
S21
ERZEUGEN VON UHRENVERIFIZIERUNGS-MESSUNGEN
S22
ABLESEN DES VISUELLEN CODES DER UHR
S23
BEWERTEN DER ENTSPRECH-UNG DER UHRENVERIFIZIER-UNGSMESSUNGEN ZU REFERENZMERKMALEN DER UHR
S24
BESTÄTIGEN
ABERKENNEN
S25

Fig. 12

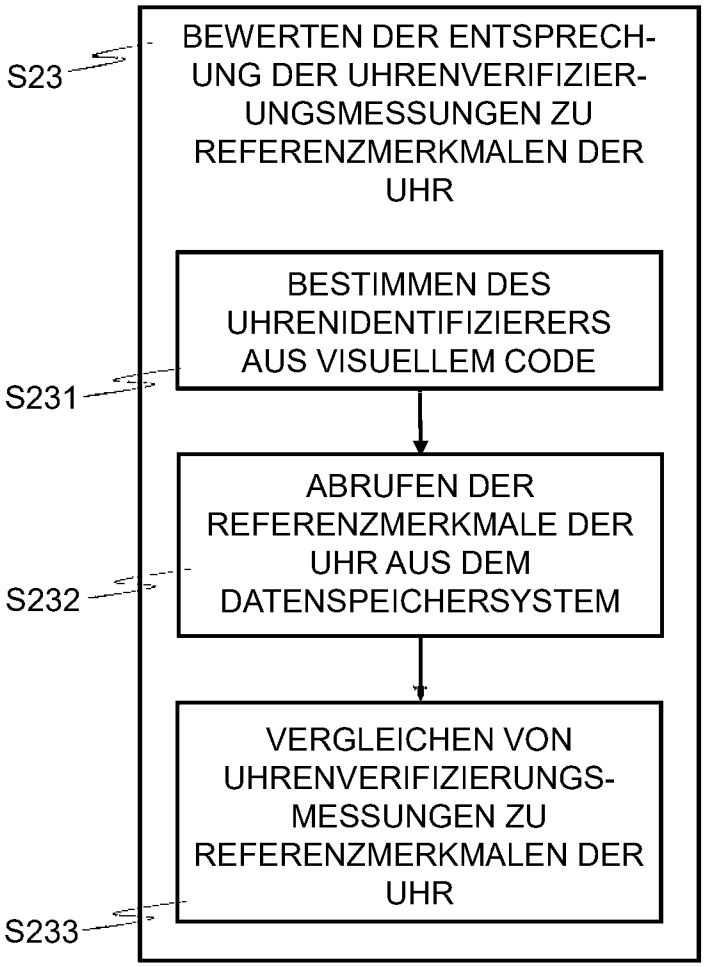

S23
BEWERTEN DER ENTSPRECH-UNG DER UHRENVERIFIZIER-UNGSMESSUNGEN ZU REFERENZMERKMALEN DER UHR
S231
BESTIMMEN DES UHRENIDENTIFIZIERERS AUS VISUELLEM CODE
S232
ABRUFEN DER REFERENZMERKMALE DER UHR AUS DEM DATENSPEICHERSYSTEM
S233
VERGLEICHEN VON UHRENVERIFIZIERUNGS-MESSUNGEN ZU REFERENZMERKMALEN DER UHR

Fig. 13

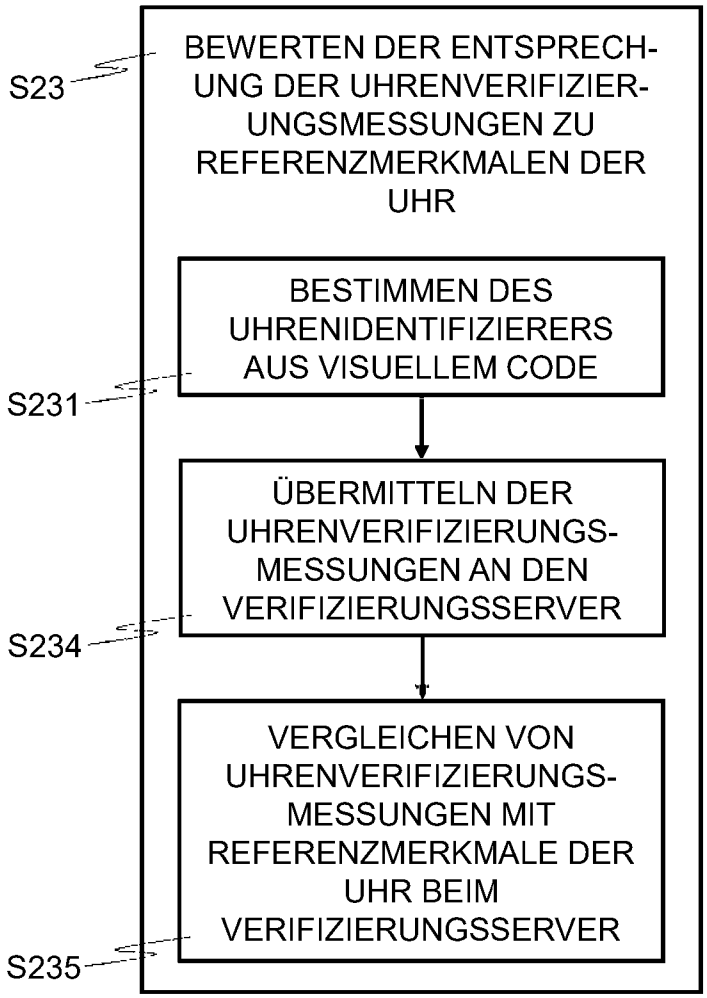

S23
BEWERTEN DER ENTSPRECH-UNG DER UHRENVERIFIZIER-UNGSMESSUNGEN ZU REFERENZMERKMALEN DER UHR
S231
BESTIMMEN DES UHRENIDENTIFIZIERERS AUS VISUELLEM CODE
S234
ÜBERMITTELN DER UHRENVERIFIZIERUNGS-MESSUNGEN AN DEN VERIFIZIERUNGSSERVER
S235
VERGLEICHEN VON UHRENVERIFIZIERUNGS-MESSUNGEN MIT REFERENZMERKMALE DER UHR BEIM VERIFIZIERUNGSSERVER

Fig. 14

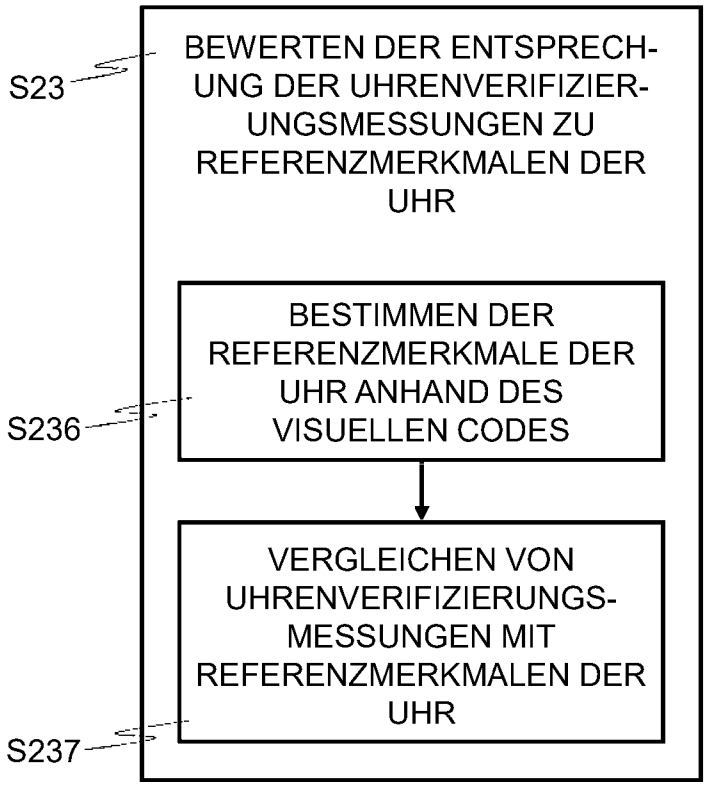

S23
BEWERTEN DER ENTSPRECH-UNG DER UHRENVERIFIZIER-UNGSMESSUNGEN ZU REFERENZMERKMALEN DER UHR
S236
BESTIMMEN DER REFERENZMERKMALE DER UHR ANHAND DES VISUELLEN CODES
S237
VERGLEICHEN VON UHRENVERIFIZIERUNGS-MESSUNGEN MIT REFERENZMERKMALEN DER UHR

Fig. 15

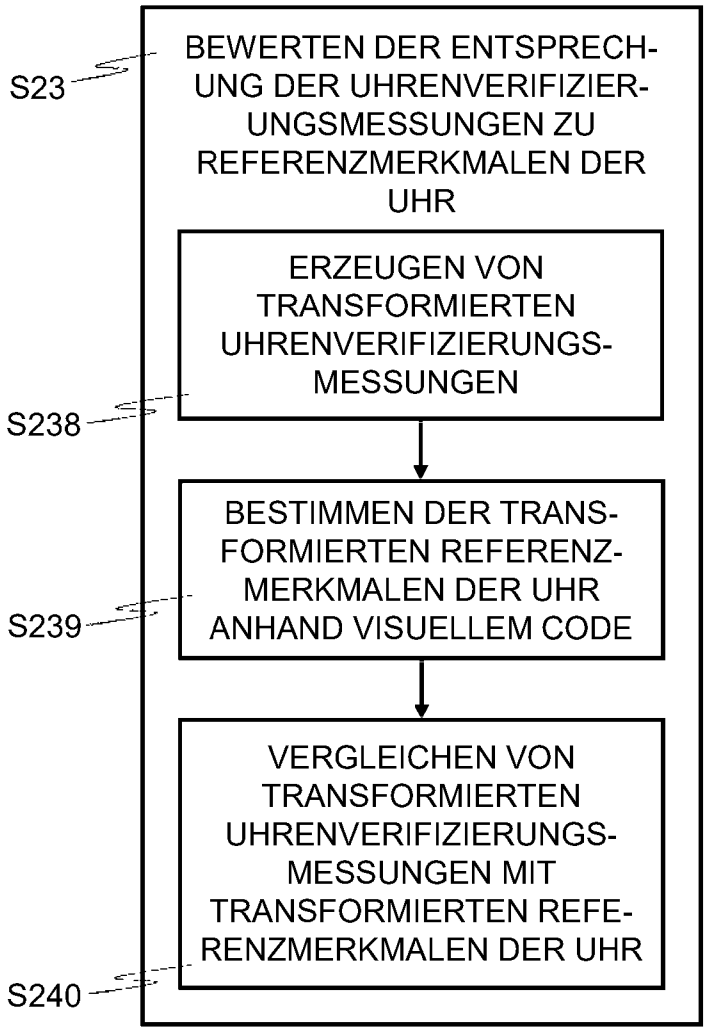

S23
BEWERTEN DER ENTSPRECHUNG DER UHRENVERIFIZIERUNGSMESSUNGEN ZU REFERENZMERKMALEN DER UHR
S238
ERZEUGEN VON TRANSFORMIERTEN UHRENVERIFIZIERUNGSMESSUNGEN
S239
BESTIMMEN DER TRANSFORMIERTEN REFERENZMERKMALEN DER UHR ANHAND VISUELLEM CODE
S240
VERGLEICHEN VON TRANSFORMIERTEN UHRENVERIFIZIERUNGSMESSUNGEN MIT TRANSFORMIERTEN REFERENZMERKMALEN DER UHR

Fig. 16

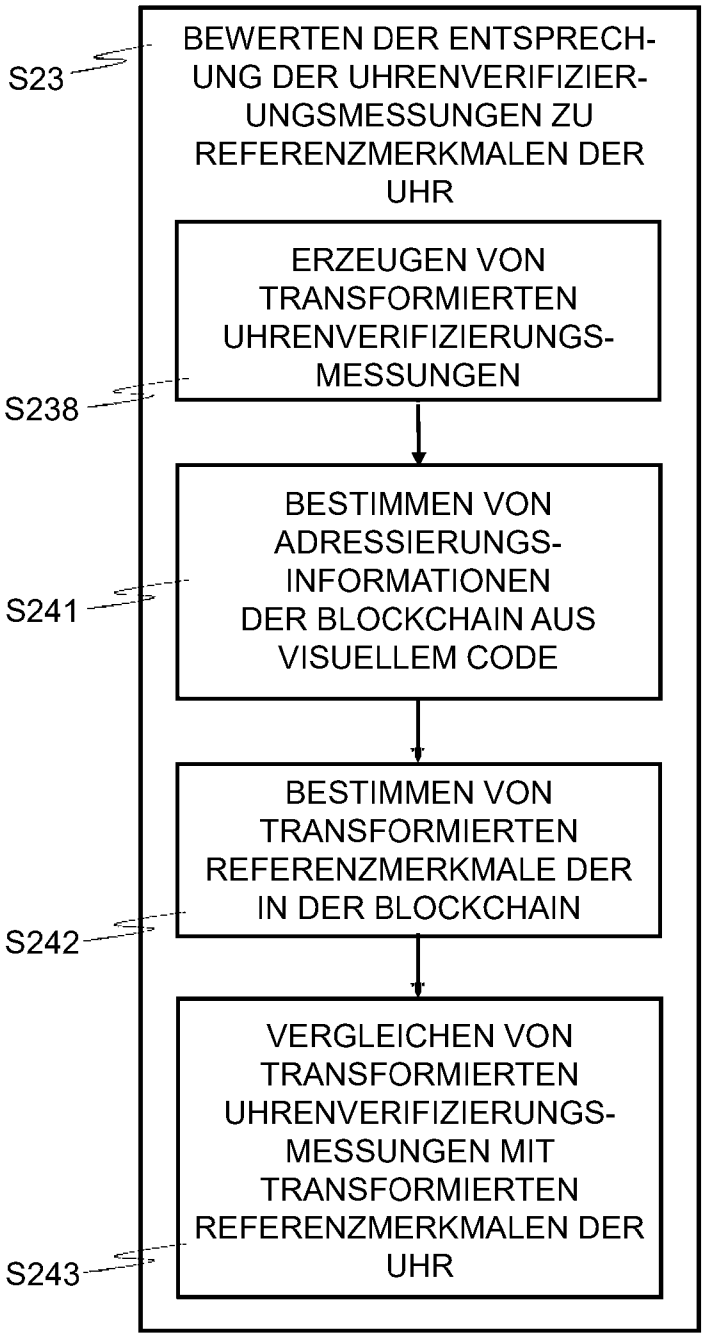

S23
BEWERTEN DER ENTSPRECHUNG DER UHRENVERIFIZIERUNGSMESSUNGEN ZU REFERENZMERKMALEN DER UHR
S238
ERZEUGEN VON TRANSFORMIERTEN UHRENVERIFIZIERUNGSMESSUNGEN
S241
BESTIMMEN VON ADRESSIERUNGSINFORMATIONEN DER BLOCKCHAIN AUS VISUELLEM CODE
S242
BESTIMMEN VON TRANSFORMIERTEN REFERENZMERKMALE DER IN DER BLOCKCHAIN
S243
VERGLEICHEN VON TRANSFORMIERTEN UHRENVERIFIZIERUNGSMESSUNGEN MIT TRANSFORMIERTEN REFERENZMERKMALEN DER UHR

Fig. 17

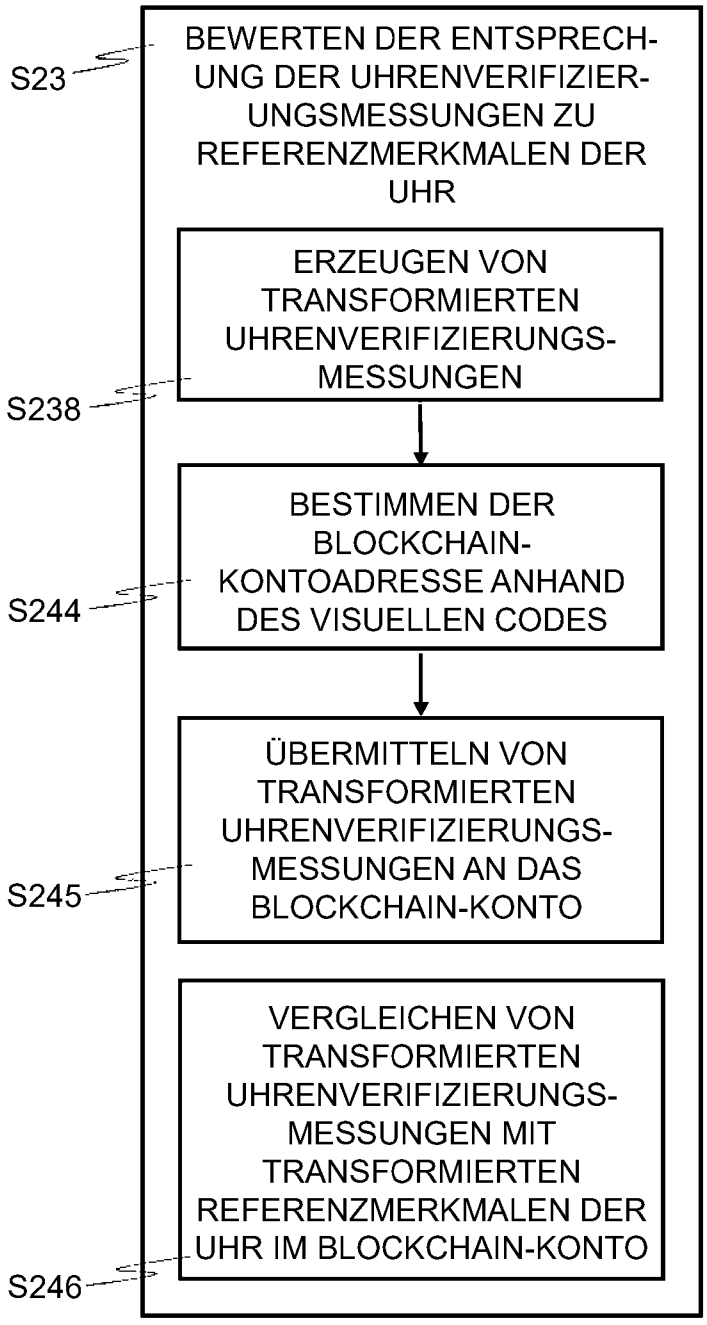

S23
BEWERTEN DER ENTSPRECHUNG DER UHRENVERIFIZIERUNGSMESSUNGEN ZU REFERENZMERKMALEN DER UHR
S238
ERZEUGEN VON TRANSFORMIERTEN UHRENVERIFIZIERUNGSMESSUNGEN
S244
BESTIMMEN DER BLOCKCHAIN-KONTOADRESSE ANHAND DES VISUELLEN CODES
S245
ÜBERMITTELN VON TRANSFORMIERTEN UHRENVERIFIZIERUNGSMESSUNGEN AN DAS BLOCKCHAIN-KONTO
S246
VERGLEICHEN VON TRANSFORMIERTEN UHRENVERIFIZIERUNGSMESSUNGEN MIT TRANSFORMIERTEN REFERENZMERKMALEN DER UHR IM BLOCKCHAIN-KONTO

Fig. 18