

Urkunde

über die Erteilung des
Patents Nr. 10 2020 129 468

Bezeichnung:
Sicherheitslabel

IPC:
G09F 3/03


Inhaber/Inhaberin:
BCTSL & Services GmbH, 76227 Karlsruhe, DE

Erfinder/Erfinderin:
Rummel, Matthias, 76137 Karlsruhe, DE; Schäfer, Michael, 76461 Muggensturm, DE

Tag der Anmeldung:
09.11.2020

Tag der Veröffentlichung der Patenterteilung:
14.03.2024

Die Präsidentin des Deutschen Patent- und Markenamts



Eva Schewior

München, 14.03.2024



(19)



Deutsches
Patent- und Markenamt



(10) **DE 10 2020 129 468 B4** 2024.03.14

(12)

Patentschrift

(21) Aktenzeichen: **10 2020 129 468.9**
(22) Anmeldetag: **09.11.2020**
(43) Offenlegungstag: **12.05.2022**
(45) Veröffentlichungstag
der Patenterteilung: **14.03.2024**

(51) Int Cl.: **G09F 3/03 (2006.01)**
G09F 3/02 (2006.01)
E05G 1/00 (2006.01)

Innerhalb von neun Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten (§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 1 Patentkostengesetz).

(73) Patentinhaber:
BCTSL & Services GmbH, 76227 Karlsruhe, DE

(72) Erfinder:
**Rummel, Matthias, 76137 Karlsruhe, DE; Schäfer,
Michael, 76461 Muggensturm, DE**

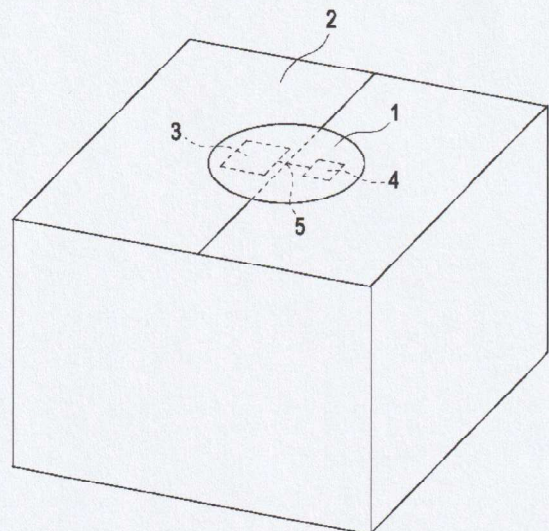
(74) Vertreter:
**Geitz Patentanwälte PartG mbB, 76135 Karlsruhe,
DE**

(56) Ermittelter Stand der Technik:
siehe Folgeseiten

(54) Bezeichnung: **Sicherheitslabel**

(57) Hauptanspruch: Sicherheitslabel zur Sicherung von Wertgegenständen (2) beliebiger Art gegen Fälschung oder unbefugte Öffnung, wobei das Sicherheitslabel (1) irreversibel derart mit dem Wertgegenstand (2) verbunden ist, dass eine Öffnung der Verpackung oder des Wertgegenstandes (2) selbst, ohne Beschädigungen des Sicherheitslabels (1) nicht möglich ist, wobei das Sicherheitslabel (1) eine Siegelfolie mit einem unterseitigen Kleber umfasst, wobei in dem Zwischenbereich zwischen dem von der Siegelfolie überdeckten Bereich des Wertgegenstandes (2) und der Siegelfolie ein NFC-Chip (3), nämlich ein RFID-Chip, angeordnet ist, mit zwei Antennen (4, 4'), welche zum Empfang der von einem autorisierten Transponder übermittelten Daten und/oder zum Auslesen der in dem NFC-Chip (3) gespeicherten Daten geeignet sind, wobei der besagte NFC-Chip (3) mit zwei Antennen (4,4') versehen ist, nämlich wenigstens einer Antenne zum Empfangen von Daten von einem autorisierten Transponder und wenigstens einer anderen Antenne, welche nach entsprechender Aktivierung durch einen autorisierten Transponder ausschließlich zum Senden von gespeicherten Daten geeignet ist, wobei als zusätzliche Sicherung die Daten des Wertgegenstandes im Speicher des besagten Chips abgelegt sind, dadurch gekennzeichnet, dass die Daten des Wertgegenstandes zusätzlich in einer Blockchain, also in einer erweiterbaren Liste von Datensätzen, die mittels kryptographischer Verfahren miteinander verkettet sind, irreversibel gespeichert sind, dass das Sicherheitslabel (1) derart mit den Antennen (4, 4') der NFC-Chips (3) irreversibel verklebt ist, dass das Sicherheitslabel (1) nicht ohne Zerstörung der Antennen (4, 4') von dem zu sichernden Wertgegenstand (2) entfernbar ist,

dass die zwei Antennen (4, 4') des NFC-Chips (3) jeweils mit Sollbruchstellen versehen sind, so dass der Versuch einer unbefugten Entfernung des Sicherheitslabels (1) zwangsläufig mit einer Zerstörung der in dem Zwischenbereich zwischen dem Wertgegenstand (2) und dem Sicherheitslabel (1) angeordneten Antennen (4, 4') verbunden ist, und dass das Sicherheitslabel (1) derart mit einem mehrteiligen Wertgegenstand (2) verbunden ist, dass das Sicherheitslabel (1) die jeweiligen Verbindungsteile der Einzelteile des Wertgegenstandes (2) übergreift, so dass ein Zugriff oder eine Öffnung des Wertgegenstandes (2) nicht ohne Beschädigung des Sicherheitslabels (1) und zumindest einer der angeschlossenen Antennen (4, 4') möglich ist.



(19)



Deutsches
Patent- und Markenamt

(10) **DE 10 2020 129 468 B4** 2024.03.14

(56) Ermittelter Stand der Technik:

DE	29 19 753	A1
DE	31 43 915	A1
DE	10 2007 022 460	A1
DE	10 2012 112 297	A1
DE	10 2017 125 259	A1
DE	10 2018 133 104	A1
DE	10 2019 108 253	A1
US	2005 / 0 284 941	A1
EP	1 420 477	B1
EP	1 470 453	B1
EP	2 015 149	A2
WO	2008/ 151 831	A1

Beschreibung

[0001] Die Erfindung betrifft ein Sicherheitslabel zur Sicherung von Wertgegenständen beliebiger Art gegen Fälschung oder unbefugte Öffnung, wobei das Sicherheitslabel irreversibel derart mit dem Wertgegenstand verbunden ist, dass eine Öffnung der Verpackung oder des Wertgegenstandes selbst, ohne Beschädigungen des Sicherheitslabels nicht möglich ist, wobei das Sicherheitslabel eine Siegelfolie mit einem unterseitigen Kleber umfasst, wobei in dem Zwischenbereich zwischen dem von der Siegelfolie überdeckten Bereich des Wertgegenstandes und der Siegelfolie ein NFC-Chip, nämlich ein RFID-Chip, angeordnet ist, mit zwei Antennen, welche zum Empfang der von einem autorisierten Transponder übermittelten Daten und/oder zum Auslesen der in dem NFC-Chip gespeicherten Daten geeignet sind, wobei der besagte NFC-Chip mit zwei Antennen versehen ist, nämlich wenigstens einer Antenne zum Empfangen von Daten von einem autorisierten Transponder und wenigstens einer anderen Antenne, welche nach entsprechender Aktivierung durch einen autorisierten Transponder ausschließlich zum Senden von gespeicherten Daten geeignet ist, wobei als zusätzliche Sicherung die Daten des Wertgegenstandes, also beispielsweise eine Seriennummer einer Uhr, etwa der sogenannte „Product-Identification-Code“, kurz PIC, im Speicher des besagten Chips abgelegt sind.

[0002] In diesem Zusammenhang ist aus der EP 1 420 477 B1 eine, mittels eines so genannten Tamper-Evident-Etiketts, gesicherte Uhr vorbekannt, wobei es sich bei diesem Sicherheitsetikett um ein so genanntes RFID-Etikett handelt, das bedarfsweise als passiver Transponder oder auch als aktiver Transponder realisiert sein kann bzw. mit einer zusätzlichen Antenne ausgerüstet sein kann. Zusätzlich ist diese Uhr unterseitig gegen deren unbefugte Eröffnung mittels eines Siegels gesichert. Sobald der in die vorbekannte Uhr integrierte Transponder aktiviert wird, übermittelt dieser eine Informationen, betreffend das so genannte Zertifikat der Uhr und gibt damit Auskunft über die Herkunft und den Hersteller der fraglichen Uhr.

[0003] Grundsätzlich ist es bekannt, elektronische Bauteile zur Sicherstellung von deren Originalität, Authentizität und Unversehrtheit mittels eines Zertifikates zu sichern.

[0004] So ist es beispielsweise aus der DE 10 2007 022 460 A1 bekannt, eine elektronische Baugruppe durch ein Zertifikat zu sichern. Hierdurch soll sichergestellt sein, dass sobald die gesicherte äußerer Umhüllung eines Gerätes verletzt ist, die angesprochene Elektronikbaugruppe kein Zertifikat ausgibt. Im Einzelnen wird eine entsprechende Anwendung dieser Lösung in Verbindung mit elektro-

nisch gesicherten Führerscheinen, in die ein derartiger Transponder integriert ist, erläutert. Dabei wird sichergestellt, dass sobald die äußere Umhüllung dieses Führerscheins verletzt ist, kein die Authentizität des Führerscheins repräsentierendes Zertifikat mehr ausgegeben wird.

[0005] Aus der EP 1 470 453 B1 ist ein Uhrengehäuse bekannt, bei dem im Bodenelement der Uhr, also innerhalb des Uhrengehäuses eine Antenne integriert ist. Eine darüber hinaus gehende Sicherung kann dieser Schrift nicht entnommen werden.

[0006] Im Übrigen ist es aus der EP 2 015 149 A2 bekannt, Juwelierwaren mit einem elektronischen Speicher zu bestücken, wobei auch hier in dem besagten Speicher ein elektronisches Zertifikat abgelegt ist, das über eine in die entsprechende Uhr oder besagtes Schmuckstück zusätzlich integrierte Schnittstelle ausgelesen werden kann. Das besagte Zertifikat bestätigt die Echtheit der gesicherten Einheit.

[0007] Außerdem ist es aus der WO 2008/151831 bereits bekannt, die erwähnten Transponder in Uhrengehäusen zu installieren, vermutlich ebenfalls um deren Authentizität überprüfen zu können, wobei sich dieser Stand der Technik vornehmlich mit der Problematik beschäftigt, dass die Leistungsfähigkeit des integrierten Transponder in einem metallischen Uhrengehäuse dadurch beeinträchtigt wird, dass der für die Datenübertragung erforderliche Schwingkreis, bestehend aus einem Transponder, einer Antenne, sowie einer Spule in seiner Kapazität durch das metallische Gehäuse beeinträchtigt bzw. verstimmt wird, so dass die Datenübertragung gegebenenfalls beeinträchtigt oder verhindert ist.

[0008] Aus der DE 10 2012 112 297 A1 ist darüber hinaus, ein Verschlusselement für ein Gefäß mit einem pharmazeutischen Inhalt vorbekannt, das eine Verschlusskapsel (10) mit einer Mantelfläche, einem geschlossenen Ende und einem offenen Ende aufweist. Dieses Verschlusselement umfasst eine Verschlusskapsel mit einer Mantelfläche, sowie einem geschlossenen und einem offenen Ende, einen Aufreißstreifen mit einer Anfasslasche zum Öffnen der besagten Verschlusskapsel und ein Verschlussetikett mit einem bahnförmigen Substrat, das auf einer Unterseite mit Klebstoff versehen ist, wobei die besagte Verschlusskapsel auf dem Gefäß so angeordnet ist, dass diese Verschlusskapsel eine Öffnung des Gefäßes überdeckt, wobei ein erster Teilbereich des Etiketts derart auf der auf der Verschlusskapsel angeordnet ist, dass die Anfasslasche des Aufreißstreifens nicht von dem Etikett überdeckt ist. Dies stellt sicher, dass die besagte Anfasslasche des Aufreißstreifens nicht von dem Etikett überdeckt ist, also freiliegt und somit leicht mit der Hand abgezogen werden kann.

[0009] Dieses Verschlusselement stellt lediglich sicher, dass eine mögliche unbefugte Öffnung des Gefäßes dokumentiert ist. Eine zerstörungsfreie Prüfung des Inhalts der Verschlusskapsel ist nicht offenbart.

[0010] Aus der DE 10 2019 108 253 A1 ist ein weiteres pharmazeutisches Gefäß vorbekannt, umfassend einen Gefäßkörper mit einem abnehmbaren Verschluss. Dieser Gefäßkörper ist oberseitig, mittels eines dreidimensionalen Formteiles verschlossen, sowie mit einem am Außenumfang des Gefäßes mit einem kennzeichnenden Etikett versehen.

[0011] Darüber hinaus ist das besagte Gefäß ggf. außenseitig mit einem Etikett und/oder Transponder auf der Außenseite bestückt.

[0012] Ebenfalls ist aus der DE 10 2017 125 259 A1, die Verwendung eines Sicherheitsetikettes zum Nachweis missbräuchlicher Manipulationsversuche vorbekannt. Dieses Sicherheitsetikett umfasst einen Chip, insbesondere einen RFID-Chip, sowie einen zerstörungsanfälligen gedruckten Schichtenstapel, der eine Lackschicht und mindestens eine strukturierte Leiterbahnschicht aufweist, die wenigstens eine Leiterbahn des RFID-Chips einschließt. Dabei ist der Schichtenstapel bewusst zerstörungsanfällig ausgebildet, so dass schon ein nur teilweises Ablösen von dem etikettierten Untergrund oder Gegenstand zu einer nachweisbaren irreversiblen Unterbrechung der Leiterbahn des RFID-Chips führt. Etwa in dem RFID-Chip gespeicherte Informationen können dann nicht mehr ausgelesen werden.

[0013] Außerdem ist aus der US 2005/0284941 A1 ein Kommunikationssystem vorbekannt, das sowohl ein elektromagnetisches Kommunikationsgerät als auch ein optisches Kommunikationsgerät darstellt. Dabei kann das elektronische Kommunikationsgerät eine Antenne umfassen, insbesondere einen RFID-Tag. Auch diese Ausführung sieht den Einsatz eines RFID-TAGS vor, wobei die Zerstörung des RFID-Tags zwingend dazu führt, dass die in dem RFID-TAG gespeicherte Information nicht mehr abrufbar ist. Allerdings handelt es sich hier um ein Kommunikationssystem und nicht um Wertverwahrungsobjekt.

[0014] Auch aus der DE 31 43 915 A1 ist eine Chipkarte mit einer integrierten Halbleiterschaltung vorbekannt. Die besagte Chipkarte weist eine Halbleiterschaltung auf und kann mit einer entsprechenden Empfangsantenne ausgelesen werden. Es handelt sich dabei aber nicht um Wertverwahrungsobjekt.

[0015] Ferner ist aus der DE 10 2018 133 104 A1 ein Zahlungsmittel vorbekannt, in das ein RFID-Chip sowie ein Wertgegenstand, beispielsweise ein Diamant, integriert ist, der den Wert des Zahlungsmittels darstellt, wobei weder der RFID-Chip noch der Wert-

gegenstand zerstörungsfrei aus dem Zahlungsmittel entfernbar ist. Der Wert sowie die Eigenschaften des Wertgegenstandes sind in einer Blockchain verschlüsselt dokumentiert.

[0016] Letztlich ist aus der DE 29 19 753 A1 eine Einrichtung zur automatischen Identifizierung von Objekten und/oder Lebewesen vorbekannt. Diese besteht aus einem ortsfesten Abfragegerät und einem am Objekt bzw. Lebewesen befestigten Antwortgerät, wobei das Abfragegerät einen Energiesender, einen Empfänger und eine Auswerteeinheit und das Antwortgerät einen Energieempfänger und -wandler, einen Kennzeichen-Speicher, einen Taktgenerator und einen Kennzeichen-Sender enthaltende Schaltungseinheit und wenigstens eine Antenne enthält.

[0017] Ausgehend hiervon liegt der Erfindung die Aufgabe zugrunde, eine insoweit vergleichbar kostengünstige, aber doch nachvollziehbare und dokumentierte Authentizitätsprüfung vor Ort zu ermöglichen. Dies gelingt in einfacher Weise dadurch, dass der Wertgegenstand mit einem Siegel versehen wird, sodass ein Zugang zu dem Wertgegenstand nicht möglich ist, ohne das Siegel zu beschädigen. So kann schon auf den ersten Blick, angesichts der Beschädigung des Siegels, erkannt werden, dass der Gegenstand entweder beschädigt oder gegebenenfalls sogar ausgetauscht wurde.

[0018] Die Lösung dieser Aufgabe gelingt durch ein Sicherheitslabel gemäß dem geltenden Anspruch 1. Vorteilhafte Ausgestaltungen der Erfindung können den abhängigen Ansprüchen entnommen werden.

[0019] Gemäß den geltenden Anspruch 1 betrifft die Erfindung ein Sicherheitslabel zur Sicherung von Wertgegenständen beliebiger Art, gegen Fälschungen oder deren Öffnung. Dabei ist das entsprechende Sicherheitslabel irreversibel mit dem zu sichernden Wertgegenstand verbunden bzw. derart, dass eine Öffnung der Verpackung oder des Wertgegenstandes ohne Beschädigung des Sicherheitslabels nicht möglich ist. Hierdurch ist sichergestellt, dass eine Beschädigung eines Wertgegenstandes oder von deren Verpackung auf den 1. Blick erkennbar ist, sodass eine Beschädigung des Wertgegenstandes sowie auch dessen Austausch erkennbar ist.

[0020] Dabei kann ein Wertgegenstand auch ein Gegenstand sein, der zunächst einmal einen geringen Geldwert aufweist, wie beispielsweise ein Speicherelement. Allerdings können die gespeicherten Daten auf diesen Speicher einen erheblichen Wert besitzen, sodass auch die Überprüfbarkeit der Authentizität von einfachsten Gegenständen gegebenenfalls von erheblicher finanzieller Bedeutung sein kann.

[0021] Die Sicherheit ist gemäß den geltenden Anspruch 1 dadurch weiter erhöht, dass in die Verpackung des Wertgegenstands ein NFC-Chip integriert ist, der zwei Antennen, aufweist, wobei eine erste Antenne zum Empfang, von einem autorisierten Transponder übermittelter Daten, sowie eine zweite Antenne zum Auslesen der in dem besagte NFC-Chip gespeicherten Daten geeignet ist. Dadurch, dass die besagte Siegelfolie, den NFC-Chip, als auch dessen Antennen vollständig überdeckt, ist die hiermit verbundene zusätzliche elektronische Sicherung des Wertgegenstandes von außen nicht erkennbar.

[0022] Wird gleichwohl ein Versuch, die Siegelfolie zu entfernen, unternommen, so führt dies zwangsläufig zu einer von außen, sichtbaren Beschädigung des Sicherheitslabels. Zusätzlich wird aber dabei auch wenigstens eine Antenne, mit der der NFC-Chip versehen ist, beschädigt, sodass dann, die in dem NFC-Chip gespeicherten Daten, wegen der mit der Öffnung des Wertgegenstandes zwangsläufig verbundenen Zerstörung wenigstens einer Antenne, der NFC-Chip nicht mehr ausgelesen werden kann, selbst wenn dies mit einem autorisierten Transponder versucht wird.

[0023] Dies ist dann ein sicheres Indiz, dass der auf diesem Weg gesicherte Wertgegenstand entweder ausgetauscht, unbefugt geöffnet oder beschädigt wurde. Anders ausgedrückt, das Sicherheitslabel kann nicht ohne Beschädigung wenigstens einer Antenne, mit denen der Wertgegenstand irreversibel verbunden ist, entfernt werden. Der potenziell missbräuchliche Versuch, sich Zugang, zu dem jeweiligen Wertgegenstand zu verschaffen, ist somit sowohl äußerlich als auch über die nicht mehr abrufbaren Daten des NFC-Chips unübersehbar dokumentiert.

[0024] Zur weiteren Erhöhung der Sicherheit sind, ist die in Verbindung mit den von dem Sicherheitslabel überdeckten NFC-Chip, ebenfalls überklebte wenigstens eine Antenne des NFC-Chips mit einer oder mehreren Sollbruchstellen versehen, sodass auch schon sehr vorsichtige Versuche, sich durch die Entfernung des Sicherheitslabels, Zugang zu dem jeweiligen Wertgegenstand zu verschaffen, in einfachster Weise dadurch dokumentiert werden, da dies wiederum, zwangsläufig mit der Zerstörung des wenigstens einen der in dem Zwischenbereich zwischen dem Wertgegenstand und dem Sicherheitslabel angeordneten Antenne des ebenfalls von dem Sicherheitslabel überklebten NFC-Chips verbunden ist.

[0025] Der insoweit unbefugte Zugriff, sofern er nicht unmittelbar von außen sichtbar ist, kann also in einfacher Weise auch mit einem autorisierten Transponder erkannt bzw. dokumentiert werden.

[0026] Ein besonderer Vorteil der Sicherung von Wertgegenständen durch das fragliche Sicherheitslabel liegt darin, dass die entsprechende Sicherung des Wertgegenstandes nicht von außen erkennbar ist. Dementsprechend ist es sinnvoll, dass das entsprechende Sicherheitslabel einigermassen unauffällig ist, insbesondere seine innere Ausstattung mit dem abfragbaren NFC-Chip nicht sofort von außen erkennbar ist. Vor diesem Hintergrund ist es sinnvoll, das Sicherheitslabel mit den neuesten Mikro-NFC-Chips der neuesten Generation mit kleinsten Abmessungen auszustatten, welche insbesondere unterhalb eines Sicherheitslabels als solche mit dem bloßen Auge nicht erkennbar sind.

[0027] In besonders bevorzugter Ausgestaltung der Erfindung sind unterhalb des Sicherheitslabels im Einbauzustand Mikro-NFC-Chips mit Abmessungen von 1,25 x 1,25 x 0,55 mm verbaut.

[0028] In weiterer Ausgestaltung des Erfindungsgegenstandes ist in dem Bereich zwischen dem zu sichernden Wertobjekt und dem Sicherheitslabel wenigstens zwei separate Antennen des NFC-Chips verbaut, wobei wenigstens einer der beiden Antennen zum Empfangen von Daten von einem autorisierten Transponder einsetzbar ist, während die wenigstens eine andere Antenne nach entsprechender Aktivierung durch einen autorisierten Transponder ausschließlich zum Senden von gespeicherten Daten auf eine autorisierte Abfrage einsetzbar ist, beispielsweise betreffend Daten, die den Wertgegenstand beschreiben, also etwa Wertangaben oder aber auch Daten betreffend die Inhaberschaft an dem Wertgegenstand oder aber die Dokumentation von Wartungsintervallen, die den Wertgegenstand betreffen. Dabei stellt die Verwendung von wenigstens zwei separaten Antennen, wobei einer der Antennenkreise lediglich zum Senden und der andere Antennenkreis lediglich zum Empfangen von Daten einsetzbar ist, eine zusätzliche Sicherheitsstufe dar.

[0029] In abermals verbesserter Ausgestaltung der Erfindung ist das Sicherheitslabel hinsichtlich seiner Größe und seines Umfangs so dimensioniert, dass das fragliche Sicherheitslabel jeweils derart mit dem jeweiligen Wertgegenstand verbunden werden kann, dass im Falle eines zu sichernden, mehrteiligen Wertgegenstandes, die jeweilige Verbindungsstelle der Einzelteile dieses Wertgegenstandes von dem Sicherheitslabel übergriffen ist, sodass ein Zugriff oder eine Öffnung des Wertgegenstandes wiederum nicht ohne Beschädigung des Sicherheitslabels möglich. Dies wiederum in Verbindung mit der damit zwangsläufig verbundenen Dokumentation der Beschädigung.

[0030] In abermals verbesserter Ausführung des Erfindungsgegenstandes, ist auch das Sicherheitsla-

bel selbst, mit weiteren Sicherheitsmerkmalen versehen, sodass schon der Versuch der Beschädigung oder Zerstörung des Sicherheitslabels selbst, dadurch dokumentiert wird, dass etwa durch den Einsatz von Tamper-Evident-Etiketten, die die Zerstörung des Sicherheitslabels auf den ersten Blick erkennbar machen, nach außen sichtbar dokumentiert. Auch hier kann es sinnvoll sein, zusätzliche Sicherheitsmerkmale einzusetzen, die nur mit entsprechenden Geräten sichtbar zu machen sind, wie etwa Hologramme oder Prägehologramme.

[0031] Als zusätzliches Sicherheitsmerkmal werden die Daten des Wertgegenstandes also beispielsweise eine Seriennummer einer Uhr, etwa der sogenannte „Product-Identification-Code“, kurz PIC, im Speicher des besagten Chips abgelegt und zusätzlich beispielsweise in der Blockchain irreversibel gespeichert, also in einer erweiterbaren Liste von Datensätzen, die mittels kryptographischer Verfahren miteinander verkettet sind. Jeder Block enthält dabei typischerweise einen kryptographisch sicheren Hash des vorhergehenden Blocks, einen Zeitstempel und Transaktionstag. So können in diesem Zusammenhang beispielsweise Uhren des Herstellers Rolex ein-eindeutig durch die Referenz- und Seriennummer identifiziert werden.

[0032] Der Gegenstand der Erfindung wird anhand zweier in der Zeichnung dargestellten Ausführungsbeispiele näher erläutert:

[0033] Es zeigen:

Fig. 1: die Verwendung eines Ausführungsbeispiels eines Sicherheitslabels zur Sicherung eines Wertgegenstands, sowie

Fig. 2: ein weiteres Ausführungsbeispiel eines Sicherheitslabels.

[0034] Fig. 1 zeigt einen Wertgegenstand 2, der mit einem Sicherheitslabel 1 gegen eine unbefugte Öffnung des Wertgegenstandes 2 gesichert ist. Im vorliegenden Beispiel handelt es sich bei dem Wertgegenstand 2 schlicht und ergreifend um eine entsprechend gesicherte Verpackung, wie sie beispielsweise zum Versand von Medikamenten, Wertgegenständen, aber auch zum Versand von Bargeld, Schmuck, Uhren usw. einsetzbar ist.

[0035] Dabei kann im Rahmen der Erfindung allerdings nicht nur die Verpackung eines Wertgegenstandes 2, sondern beispielsweise auch ein Wertgegenstand 2 selbst, mit einem Sicherheitslabel 1 gesichert werden. Dies ist insbesondere dann möglich, wenn die Wertgegenstände 2 aus mehreren, miteinander verbundenen Teilen bestehen, sodass gegebenenfalls eine unbefugte Öffnung des Wertgegenstandes 2 denkbar ist, etwa i.V.m. einer möglichen Manipulation oder einem Austausch des Wert-

gegenstandes 2. Ein denkbar einfaches Beispiel ist in diesem Zusammenhang eine Armbanduhr mit einem mehrteiligen Gehäuse, bei der beispielsweise die untere Abdeckung des Uhrengehäuse entfernt werden könnte, um die Uhr zu reparieren oder aber auch zu manipulieren. Sinn und Zweck des Sicherheitslabels 1, ist es also, wenn schon nicht der unbefugte Zugriff auf den Wertgegenstand 2 verhindert werden kann, dann zumindest sicherzustellen, dass dieser Zugriff zweifellos und leicht erkennbar dokumentiert ist.

[0036] Dies gelingt dadurch, dass die Verbindungsstelle im Falle eines mehrteiligen zu sichernden Wertgegenstandes 2 oder aber auch die Verpackung des Wertgegenstandes 2 mit einem Sicherheitslabel 1 irreversibel verklebbar ist, was so zu verstehen ist, dass eine Öffnung der Verpackung oder des Wertgegenstandes 2 selbst, ohne eine sichtbare Beschädigung des Sicherheitslabels 1 nicht möglich ist.

[0037] Dies gelingt beispielsweise dadurch, dass die in Fig. 1 dargestellte Öffnungsnaht 5 der Verpackung des zu sichernden Wertgegenstandes 2 mit einer Siegelfolie des Sicherheitslabels 1 irreversibel überklebt ist. Dies ist so zu verstehen, dass die Siegelfolie nicht zerstörungsfrei lösbar ist. Dies ist beispielsweise dadurch sichergestellt, dass das Sicherheitslabel 1 selbst, mit weiteren Sicherheitsmerkmalen versehen ist, so dass schon der Versuch der Beschädigung oder Zerstörung des Sicherheitslabels 1 irreversibel dokumentiert wird, etwa durch den Einsatz von Tamper-Evident-Etiketten, die die Zerstörung des Sicherheitslabels 1 auf den ersten Blick erkennbar, nach außen sichtbar dokumentieren, etwa durch eine, aufgrund der Beschädigung einsetzende irreversible Verfärbung des Sicherheitslabels 1, oder der Sichtbarmachung einer Schrift, die einen Hinweis enthält, der sofort erkennbar auf die Beschädigung des Sicherheitslabels 1 hinweist. In diesem Zusammenhang kann es sinnvoll sein, zusätzliche Sicherheitsmerkmale einzusetzen, die nur mit entsprechenden Geräten sichtbar zu machen sind, wie etwa Hologrammen oder Prägehologrammen. Dies kann sinnvoll sein, wenn der unbefugte Zugriff auf den Wertgegenstand 2 nur für bestimmte bzw. befugte Personen ersichtlich sein soll.

[0038] In weiterer Ausgestaltung des Erfindungsgegenstandes ist es denkbar, den Wertgegenstand nicht nur durch das Sicherheitslabel 1, als solches zu schützen, sondern zusätzlich weitere Sicherheitsmerkmale vorzusehen.

[0039] In diesem Sinne schlägt die Erfindung vor, entweder mittels des Sicherheitslabels 1 oder unabhängig davon, den Wertgegenstand 2 mit einem oder mehreren NFC-Chips 3 zu verbinden, wobei in dem oder den NFC-Chips 3, beispielsweise Informationen

über den Wert des zu sichernden Gegenstandes und dessen Zustandes bzw. dessen Wertes gespeichert sein können, die über einen Transponder, vorzugsweise kontaktfrei, auslesbar sind. Dabei kann wiederum das Auslesen des Transponders durch eine spezielle Frequenz oder andere Sicherheitsmerkmale, wie etwa ein Passwort gesichert sein, so dass nur befugten Personen und/oder Autoritäten in der Lage sind, mit dem entsprechenden NFC-Chip 3 zu kommunizieren, bzw. diesen auszulesen oder zu programmieren.

[0040] Um die entsprechende Kommunikation zwischen dem oder den erwähnten NFC-Chips 3 und einem zugelassenen Transponder zu ermöglichen, müssen die entsprechenden NFC-Chips 3 mit wenigstens einer oder mehreren Antennen 4,4' zum Aufbau einer drahtlosen Verbindung versehen sein. Ein solches Ausführungsbeispiel ist in **Fig. 2** gezeigt. In dieser Ausführungsform werden die Antennen 4,4' jeweils irreversibel beschädigt, wenn entweder die besagte Verpackung oder der Wertgegenstand 2 als solcher unbefugt geöffnet wird. Um dies sicherzustellen, sind die Antennen 4,4' so angeordnet, dass mit der Öffnung des Wertgegenstandes 2 oder der Verpackung zwingend die Antennen 4,4' unterbrochen bzw. zerstört werden. In einer weiteren vorteilhaften Ausgestaltung kann dies zu einer automatischen Speicherung dieses Vorfalles in dem oder den NFC-Chips 3 führen.

[0041] Bei den erwähnten NFC-Chips 3 handelt es sich in besonders vorteilhafter Ausgestaltung um die neueste Generation der sogenannten Micro-NFC-Chips.

[0042] Im Ergebnis offenbart die Erfindung eine vergleichsweise kostengünstige Realisierung der Sicherung von Wertgegenständen, die so weitgehend perfektioniert ist, dass der unbefugte Zugriff auf entsprechende Wertgegenstände keinen Sinn mehr macht, weil die auf diesem Wege beschädigten oder entwendeten Gegenstände zumindest einen erheblichen Anteil ihres Wertes verlieren, weil deren Beschädigung zumindest für eine autorisierte Person ohne weiteres sichtbar und erkennbar ist, so dass beispielsweise eine Weiterveräußerung des entwendeten Wertgegenstandes mehr oder minder sinnlos ist.

BEZUGSZEICHENLISTE

1	Sicherheitslabel
2	Wertgegenstand
3	NFC-Chip
4,4'	Antenne
5	Öffnungsnaht

Patentansprüche

1. Sicherheitslabel zur Sicherung von Wertgegenständen (2) beliebiger Art gegen Fälschung oder unbefugte Öffnung, wobei das Sicherheitslabel (1) irreversibel derart mit dem Wertgegenstand (2) verbunden ist, dass eine Öffnung der Verpackung oder des Wertgegenstandes (2) selbst, ohne Beschädigungen des Sicherheitslabels (1) nicht möglich ist, wobei das Sicherheitslabel (1) eine Siegelfolie mit einem unterseitigen Kleber umfasst, wobei in dem Zwischenbereich zwischen dem von der Siegelfolie überdeckten Bereich des Wertgegenstandes (2) und der Siegelfolie ein NFC-Chip (3), nämlich ein RFID-Chip, angeordnet ist, mit zwei Antennen (4, 4'), welche zum Empfang der von einem autorisierten Transponder übermittelten Daten und/oder zum Auslesen der in dem NFC-Chip (3) gespeicherten Daten geeignet sind, wobei der besagte NFC-Chip (3) mit zwei Antennen (4,4') versehen ist, nämlich wenigstens einer Antenne zum Empfangen von Daten von einem autorisierten Transponder und wenigstens einer anderen Antenne, welche nach entsprechender Aktivierung durch einen autorisierten Transponder ausschließlich zum Senden von gespeicherten Daten geeignet ist, wobei als zusätzliche Sicherung die Daten des Wertgegenstandes im Speicher des besagten Chips abgelegt sind,

dadurch gekennzeichnet,

dass die Daten des Wertgegenstandes zusätzlich in einer Blockchain,

also in einer erweiterbaren Liste von Datensätzen, die mittels kryptographischer Verfahren miteinander verkettet sind, irreversibel gespeichert sind,

dass das Sicherheitslabel (1) derart mit den Antennen (4, 4') der NFC-Chips (3) irreversibel verklebt ist, dass das Sicherheitslabel (1) nicht ohne Zerstörung der Antennen (4, 4') von dem zu sichernden Wertgegenstand (2) entfernbar ist,

dass die zwei Antennen (4, 4') des NFC-Chips (3) jeweils mit Sollbruchstellen versehen sind, so dass der Versuch einer unbefugten Entfernung des Sicherheitslabels (1) zwangsläufig mit einer Zerstörung der in dem Zwischenbereich zwischen dem Wertgegenstand (2) und dem Sicherheitslabel (1) angeordneten Antennen (4, 4') verbunden ist, und dass das Sicherheitslabel (1) derart mit einem mehrteiligen Wertgegenstand (2) verbunden ist, dass das Sicherheitslabel (1) die jeweiligen Verbindungsteile der Einzelteile des Wertgegenstandes (2) übergreift, so dass ein Zugriff oder eine Öffnung des Wertgegenstandes (2) nicht ohne Beschädigung des Sicherheitslabels (1) und zumindest einer der angeschlossenen Antennen (4, 4') möglich ist.

2. Sicherheitslabel nach Anspruch 1, **dadurch gekennzeichnet,** dass es sich bei den eingesetzten NFC-Chip (3) um Chips der neuesten Micro-NFC-

Chips mit Abmessungen von 1,25 x 1,25 x 0,55 mm und weniger handelt.

3. Sicherheitslabel nach einem der Ansprüche 1 oder 2, **dadurch gekennzeichnet**, dass wenigstens eine Antenne (4,4') irreversibel derart mit der Öffnungsstelle oder Öffnungsnaht (5) des Wertgegenstandes (2) verklebt ist, dass zwangsläufig mit Öffnung des Wertgegenstandes (2) ein Bruch und damit eine Zerstörung wenigstens einer Antenne (4,4') verbunden ist.

4. Sicherheitslabel nach einem oder mehrerer der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass das Sicherheitslabel (1) nicht zerstörungsfrei lösbar, auf dem jeweiligen Wertgegenstand (2) befestigt ist.

5. Sicherheitslabel gemäß einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass das Sicherheitslabel (1) mehrere Sicherheitsmerkmale aufweist, die visuell erkennbar sind.

6. Sicherheitslabel gemäß Anspruch 5, **dadurch gekennzeichnet**, dass die Sicherheitsmerkmale des Sicherheitslabels (1) durch diffraktive Elemente, nämlich mittels Hologrammen oder Prägehologrammen sichtbar sind.

Es folgen 2 Seiten Zeichnungen

Anhängende Zeichnungen

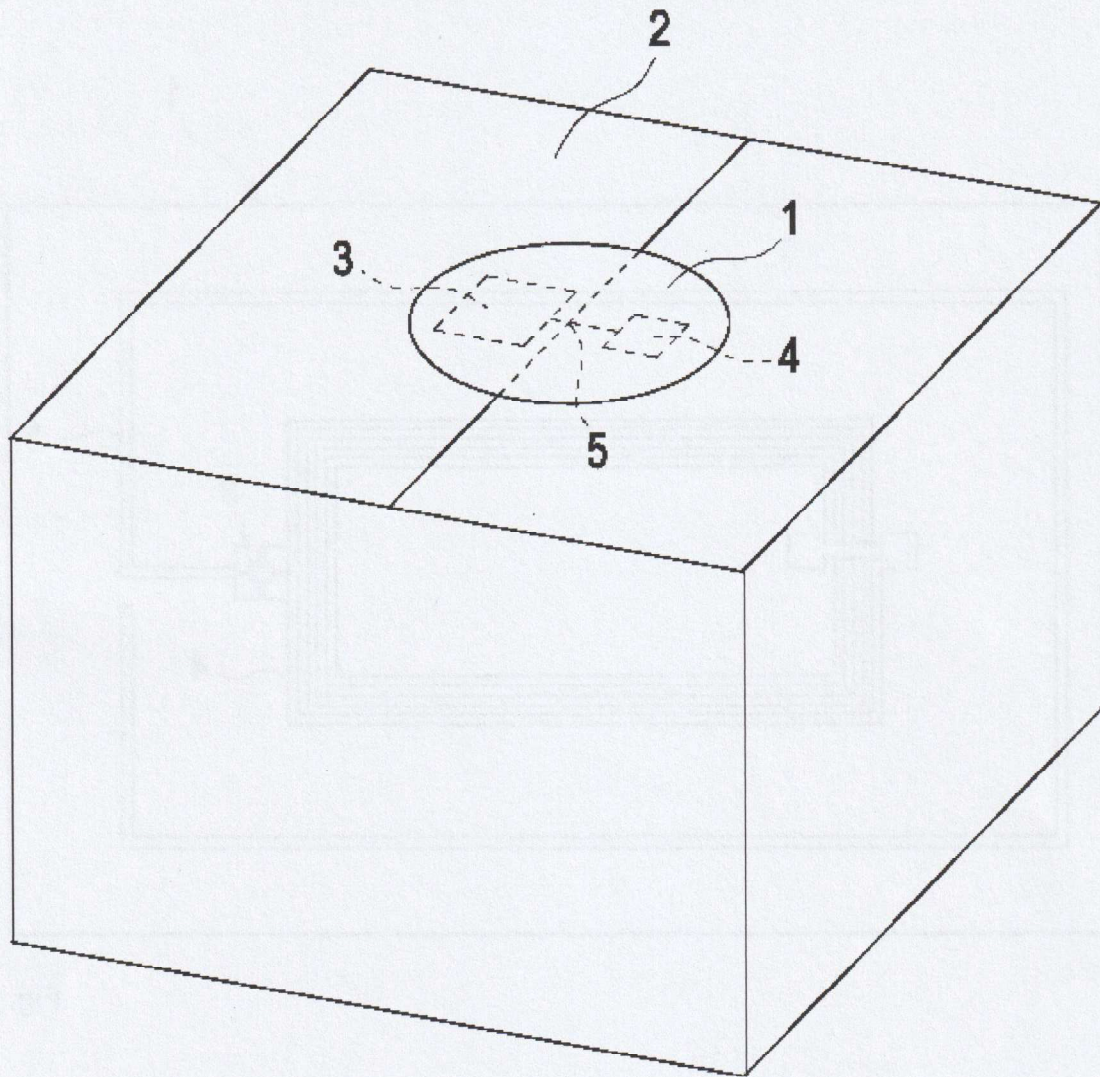


Fig. 1

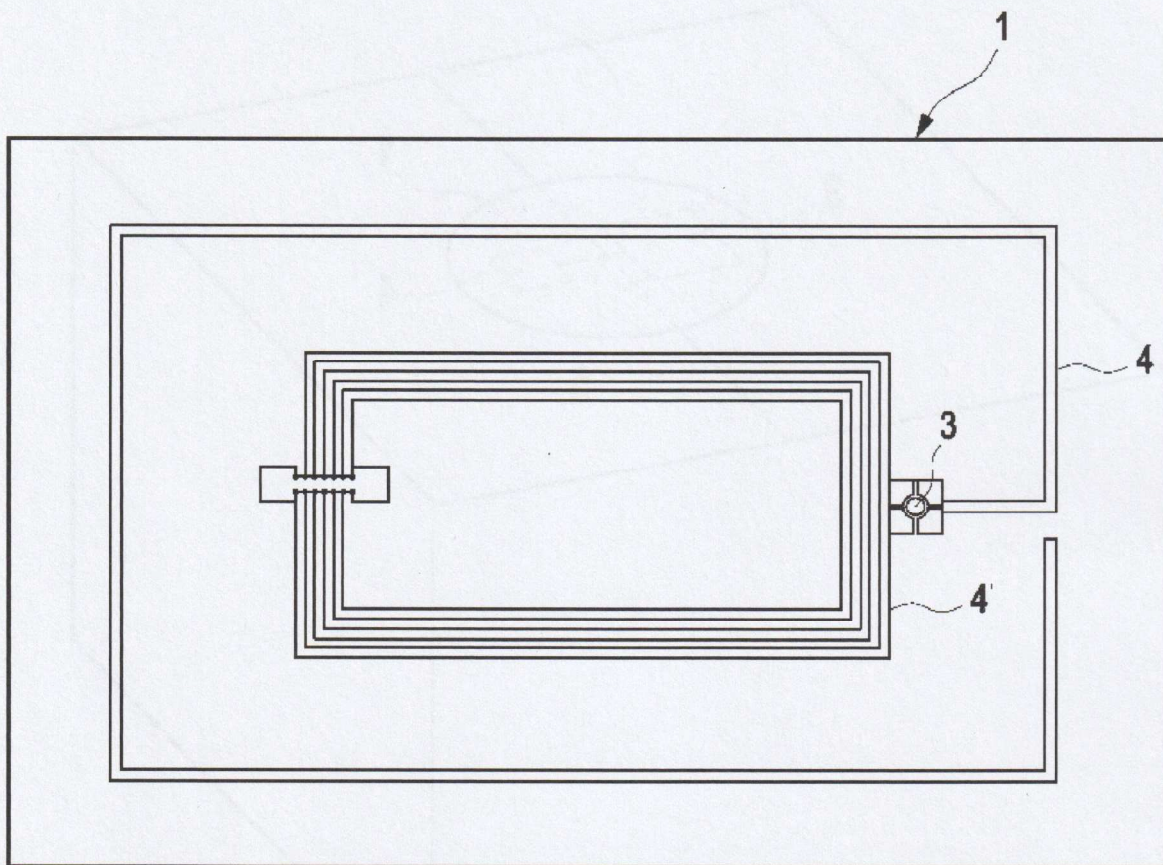


Fig. 2