(19) Deutsches Patent- und Markenamt

(10) **DE 10 2020 210 810 A1** 2022.03.03

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2020 210 810.2**
(22) Anmeldetag: **27.08.2020**
(43) Offenlegungstag: **03.03.2022**

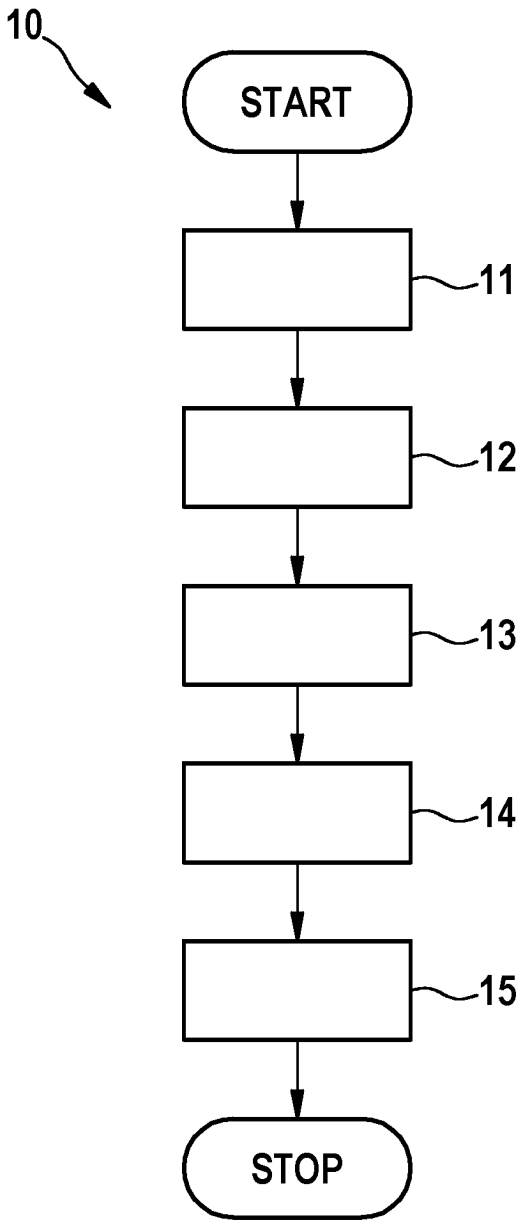
(51) Int Cl.: ***G06Q 30/06*** (2012.01)

(71) Anmelder:
Robert Bosch Gesellschaft mit beschränkter Haftung, 70469 Stuttgart, DE

(72) Erfinder:
Lehenbauer, Cecile, 71665 Vaihingen, DE;
Ververis, Diamantis, 70376 Stuttgart, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Verfahren und Vorrichtung zum gegenseitigen Bewerten von Leistungserbringern und Leistungsempfänger mittels einer dezentralen Transaktionsdatenbank**



(57) Zusammenfassung: Verfahren (10) zum Bewerten eines Erbringers (20) einer Leistung (21) mittels einer dezentralen Transaktionsdatenbank, gekennzeichnet durch folgende Merkmale:
- der Erbringer (20) wird einer Bewertung durch einen Empfänger (22) der Leistung (21) unterzogen (11) oder umgekehrt,
- ein der Transaktionsdatenbank zuletzt hinzugefügter Datensatz (23) wird unter einer Streuwertfunktion auf einen ersten Streuwert abgebildet (12),
- die Bewertung und der erste Streuwert werden in einem neuen Datensatz (23) zusammengefasst (13),
- der neue Datensatz (23) wird der Transaktionsdatenbank hinzugefügt und unter der Streuwertfunktion auf einen zweiten Streuwert abgebildet (14) und
- der neue Datensatz (23) oder der zweite Streuwert werden von einem ausgewählten (28) Dritten (24), der nicht im Interesse der bewerteten Partei handelt, verwaltet und Interessenten (25) an der Leistung (21) auf Anfrage (27) bereitgestellt (15).

Beschreibung

[0001] Die vorliegende Erfindung betrifft ein Verfahren zum Bewerten eines Leistungserbringers mittels einer dezentralen Transaktionsdatenbank. Die vorliegende Erfindung betrifft darüber hinaus eine entsprechende Vorrichtung, ein entsprechendes Computerprogramm sowie ein entsprechendes Speichermedium.

Stand der Technik

[0002] Als dezentrales Transaktionssystem, Transaktionsdatenbank oder verteiltes Hauptbuch (distributed ledger) wird jegliches Protokoll in Rechnernetzen bezeichnet, das eine Übereinkunft (consensus) hinsichtlich der Abfolge bestimmter Transaktionen herbeiführt. Eine häufige Ausprägung eines solchen Systems beruht auf einer Blockkette (blockchain) und bildet die Grundlage zahlreicher sogenannter Kryptowährungen.

[0003] US 2019/0325432 A1 offenbart ein auf einer Blockkette basierendes Reputationssystem.

[0004] Blockketten werden ferner beispielsweise im Rahmen der sogenannten dezentralen Identität (decentralized identity, DID) und insbesondere der selbstsouveränen Identität (self-sovereign identity, SSI) genutzt, mittels derer einzelne Identitätsinhaber eine Identität verwalten und die Nutzung ihrer persönlichen Daten ohne die Mitwirkung eines Vermittlers oder einer Zentralbehörde kontrollieren können. Konkret kann die DID zum Beispiel zum verifizierbaren Nachweis (verifiable credential) behaupteter Eigenschaften dienen, der wiederum durch eine nachprüfbare Darstellung (verifiable presentation) erbracht werden kann.

[0005] DE212019000019U1 offenbart ein System, das den Träger eines Identitätsdokuments autorisiert und Folgendes umfasst: einen Identitäts-Provider zum Bereitstellen einer dezentralen Identität für den Träger; ein Mittel, um dem Träger digital signierte biometrische Daten in Bezug auf das Identitätsdokument bereitzustellen, wobei die biometrischen Daten von einem Vertrauensanker signiert und als an die dezentrale Identität ausgegeben validiert werden, wobei die biometrischen Daten ein Bild des Trägers beinhalten; ein Mittel, um einer Behörde die dezentrale Identität und die biometrischen Daten des Trägers, inkl. des Bildes, vor der Reise des Trägers, die für die Einreiseerlaubnis des Trägers zuständig ist, zur Verifizierung bereitzustellen, wobei der Träger nach der Verifizierung eine Autorisierung von der Behörde empfängt; ein Bilderfassungssystem zum Erfassen eines Bildes des Trägers bei der Ankunft des Trägers; ein Bildabgleichsystem zum Abgleichen des Bildes des Trägers mit Bildern einer Mehrzahl von Trägern, die von der Behörde autorisiert wurden; und ein Kontrollgate zum Erteilen einer Einreiseerlaubnis für den Träger nach erfolgreichem Abgleich.

Offenbarung der Erfindung

[0006] Die Erfindung stellt ein Verfahren zum Bewerten eines Leistungserbringers wie auch des Leistungsempfängers mittels einer dezentralen Transaktionsdatenbank, eine entsprechende Vorrichtung, ein entsprechendes Computerprogramm sowie ein entsprechendes Speichermedium gemäß den unabhängigen Ansprüchen bereit.

[0007] Der erfindungsgemäße Ansatz fußt hierbei auf der Erkenntnis, dass es bei bekannten Reputationssystemen meist ein zentraler Anbieter ist, welcher zum einen die Möglichkeit der Bewertung einer anderen Partei bietet, zum anderen allerdings auch letztlich der Eigentümer der abgegebenen Reputations-Daten ist. Daraus ergibt sich zum einen eine Abhängigkeit der verschiedenen Parteien, welche ihre Interaktionen gegenseitig bewerten wollen, und zum anderen eine Informationsasymmetrie zu Gunsten des Betreibers. Darüber hinaus sind diese Systeme angreifbar, da die Bewertungsfunktion leicht missbraucht werden kann, zumal es zur Erstellung einer Bewertung oft keines Nachweises einer Interaktion, sondern nur eines Accounts auf der jeweiligen Bewertungsplattform bedarf.

[0008] In herkömmlichen Reputationssystemen ist aus den genannten Gründen sowohl eine Verbesserung der Selbstdarstellung als auch eine Verschlechterung der Darstellung eines Mitbewerbers mit geringem Aufwand möglich. Darüber hinaus unterliegen die Bewertungen meist einer enormen Willkür und Subjektivität, sodass sie in zahlreichen Fällen unberechtigt und schwerlich nachvollziehbar sind.

[0009] Die vorgeschlagene Lösung beruht ferner auf der Einsicht, dass ein Reputationssystem für die autonome Interaktion internetfähiger Geräte (machine-to-machine, M2M) in dezentralen Systemen von großer Bedeutung ist, da es keinen Intermediär gibt, der für regelkonformes Verhalten sorgt und im Zweifelsfall die Verantwortung übernimmt. Ein Reputationssystem, welches auf einen Intermediär verzichtet, dient daher dem Vertrauensaufbau zwischen einander unbekannten Parteien.

[0010] Ein Vorzug des erfindungsgemäßen Verfahrens liegt vor diesem Hintergrund in seiner Eignung, sowohl die Datensouveränität der bewerteten Parteien als auch die Korrektheit der Bewertungen zu gewährleisten.

[0011] Durch die in den abhängigen Ansprüchen aufgeführten Maßnahmen sind vorteilhafte Weiterbildungen und Verbesserungen des im unabhängigen

Anspruch angegebenen Grundgedankens möglich. So kann ein Nachweis über die Berechtigung zur Bewertung des jeweiligen Leistungserbringers vorgesehen sein. Auf diese Weise kann das willkürliche Ausstellen von Bewertungen durch Akteure verhindert werden, die niemals mit der bewerteten Partei interagiert haben.

Figurenliste

[0012] Ausführungsbeispiele der Erfindung sind in den Zeichnungen dargestellt und in der nachfolgenden Beschreibung näher erläutert. Es zeigt:

Fig. 1 das Flussdiagramm eines Verfahrens zum Bewerten eines Leistungserbringers gemäß einer ersten Ausführungsform.

Fig. 2 die Sicherstellung der Integrität der Bewertungen.

Fig. 3 die Überprüfung der Korrektheit der Bewertungen.

Fig. 4 die Rollenverteilung zwischen den Akteuren des Verfahrens.

Fig. 5 schematisch ein Steuergerät gemäß einer zweiten Ausführungsform.

Ausführungsformen der Erfindung

[0013] Fig. 1 illustriert die grundlegenden Schritte eines erfindungsgemäßen Verfahrens (10), dessen Ablauf nunmehr anhand der nachfolgenden Abbildungen erläutert sei. Nach einer erfolgreich abgeschlossenen Interaktion, welche etwa den Austausch von Geld-, Sach- oder Dienstleistungen zwischen zwei Parteien zum Gegenstand hat, können diese sich gegenseitig eine Bewertung zukommen lassen (Prozess 11). Bewertungen werden als einzelne atomare Datensätze erzeugt und können in Form von Verifiable Reputation Credentials (VRC) ausgestellt werden, ähnlich einem Zeugnis. Die Datensätze können auch einer anderen Form entsprechen. Die Bewertung wird dabei nur der bewerteten Partei übermittelt, wodurch diese Partei auch der alleinige Eigentümer dieser Bewertungsdaten ist.

[0014] Diese VRCs werden vom Adressaten der Bewertung gesammelt und können einem potenziellen nächsten Interaktionspartner in Form einer Darstellung zur Verfügung gestellt werden, deren Korrektheit vom neuen Interaktionspartner überprüft werden kann.

[0015] Um dies zu ermöglichen, wird stets bei der Ausstellung einer Bewertung vom jeweils bewertenden Leistungsempfänger (im Folgenden kurz: „Empfänger“) ein Streuwert (hash) des letzten VRCs erzeugt (Prozess 12), der vom zu bewertenden Leistungserbringer (im Folgenden kurz: „Erbringer“) als Teil der Darstellung übermittelt wurde. Dieser Streuwert wird, wie **Fig. 2** veranschaulicht, nun vom Empfänger (22) in seinen neu erstellten Bewertungsdatensatz (VRC) (23) eingetragen (Prozess 13 - **Fig. 1**) und mit seiner DID signiert. Somit ist es dem Erbringer (20) nach der Hinzufügung des Datensatzes (23) zu einer Transaktionsdatenbank nicht möglich, eine eventuell vorherige negative Bewertung aus dieser Datenbank zu entfernen, da jeder Datensatz (23) mit seinem Vorgänger kryptographisch verkettet ist.

[0016] Ohne weitere Maßnahmen könnte der Erbringer (20) den Datensatz (23) jedoch vor der Hinzufügung zur Transaktionsdatenbank verwerfen, falls ihm die enthaltene Bewertung nicht zusagt und er diese nicht präsentieren möchte. Um dies zu verhindern, ist ein vertrauenswürdiger Dritter (24) vorgesehen, welcher dazu dient, den Streuwert des neuesten Datensatzes (23) vorzuhalten, dem potenziellen neuen Interaktionspartner zur Verfügung zu stellen und somit die Nachprüfbarkeit des Datensatzes (23) zu gewährleisten. Alternativ kann auch der Datensatz (23) selbst vom Dritten (24) verwaltet werden; die Preisgabe lediglich des Streuwertes bürgt jedoch für einen besseren Datenschutz (privacy), da der Dritte (24) auf diese Weise keine Kenntnis von der im Datensatz (23) enthaltenen Bewertung erlangt.

[0017] Im Detail läuft das Verfahren (10 - **Fig. 1**) folgendermaßen ab: Der Empfänger (22) bildet den der in der Darstellung/Sammlung von Bewertungsdatensätzen (Verifiable Presentation) des Leistungserbringers zuletzt hinzugefügten VRC auf einen Streuwert ab (Prozess 12 - **Fig. 1**) und fasst diesen mit seiner Bewertung zu einem neuen Datensatz (23) zusammen (Prozess 13 - **Fig. 1**). Anschließend bildet er wiederum den Streuwert dieses Datensatzes (Prozess 14 - **Fig. 1**) und übermittelt letzteren in Form einer signierten Nachricht an den Dritten (24).

[0018] Wenn nun, wie in **Fig. 3** dargestellt, ein neuer Interessent (25) an der angebotenen Leistung (21) die Bewertungen des Erbringers (20) einsehen möchte, kann er die Korrektheit und Vollständigkeit der Bewertungen mithilfe des Dritten (24) überprüfen, indem er den Streuwert des neuesten Datensatzes (23) mit jenem vergleicht, den der Dritte (24) verwahrt (Prozess 15 - **Fig. 1**). Im Falle einer Übereinstimmung sind die Bewertungen korrekt und der Interessent (25) weiß, dass er dem Erbringer (20) vertrauen kann.

[0019] Die Zusammenhänge sowie die Rollen dieses Bewertungsszenarios werden in **Fig. 4** veranschaulicht. Der vom Erbringer (20) ausgewählte Dritte (24) dient in der vorliegenden Ausführungsform nicht nur dem Empfänger (22), indem er die Integrität der im neuen Datensatz (23) enthaltenen Bewertung bezeugt (30), sondern verwaltet ferner

einen vom Empfänger (22) erbrachten Nachweis (26), die Leistung (21) des Erbringers (20) überhaupt in Anspruch genommen zu haben und somit zu dessen Bewertung berechtigt zu sein. Der Erbringer (20) kann sich diese Berechtigung vor dem Hinzufügen des neuen Datensatzes (23) durch den Dritten (24) bestätigen lassen. Der diesbezügliche Nachweis (26) mag dem Empfänger (22) durch den Erbringer (20) der Leistung (21) bereitgestellt worden sein oder die Inanspruchnahme der Leistung (21) durch den Empfänger (22) anderweitig belegen. Somit wird, falls eine der Parteien (20, 22) die Bewertung verhindern möchte, gewährleistet, dass stattdessen die andere Partei den Nachweis (26) erbringen kann.

[0020] Ein weiterer Aspekt des Verfahrens (10) besteht darin, autonome und objektive Bewertungen zu ermöglichen, da im Kontext des Internet der Dinge (Internet of things, IoT) Produkte und Leistungen größtenteils standardisiert und neutral beurteilt werden können. Eine bevorzugte Ausführungsform sieht daher messbare Eigenschaften zur Evaluation einer Ware oder Dienstleistung vor. So kann gewährleistet werden, dass keine Willkür bei der Bewertung vorliegt.

[0021] Um das zu veranschaulichen, soll die autonome Beurteilung eines digitalen Service wie beispielsweise die Bereitstellung einer Datenbank betrachtet werden. Hierbei könnten Kriterien wie Verfügbarkeit, Verarbeitungsdauer, Konsistenz sowie Ausfalltoleranz (partition tolerance) eine Rolle spielen. All dies sind messbare Kriterien, die eine objektive Bewertung gestatten. Entsprechendes gilt in den meisten Anwendungsfällen des IoT, in denen Maschinen autonom handeln und eigenständig Transaktionen abschließen. Eine optionale weitere Sicherheitsmaßnahme besteht darin, dass die Evaluationen keiner einheitlichen Berechnungsmethodik unterliegen, sondern von jedem Marktteilnehmer auf seine eigenen Weise interpretiert werden. Dadurch ist es nicht zielführend, den Berechnungsvorgang anzugreifen oder zu manipulieren.

[0022] Dieses Verfahren (10) kann beispielsweise in Software oder Hardware oder in einer Mischform aus Software und Hardware beispielsweise in einem Steuergerät (50) implementiert sein, wie die schematische Darstellung der **Fig. 5** verdeutlicht.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Zitierte Patentliteratur

- US 2019/0325432 A1 [0003]
- DE 212019000019 U1 [0005]

Patentansprüche

1. Verfahren (10) zum Bewerten eines Erbringers (20) einer Leistung (21) mittels einer dezentralen Transaktionsdatenbank, **gekennzeichnet durch** folgende Merkmale:
- der Erbringer (20) wird einer Bewertung durch einen Empfänger (22) der Leistung (21) unterzogen (11),
- ein der Transaktionsdatenbank in der Darstellung/-Sammlung von Bewertungsdatensätzen zuletzt hinzugefügter Datensatz (23) wird unter einer Streuwertfunktion auf einen ersten Streuwert abgebildet (12),
- die Bewertung und der erste Streuwert werden in einem neuen Datensatz (23) zusammengefasst (13),
- der neue Datensatz (23) wird der Transaktionsdatenbank hinzugefügt und unter der Streuwertfunktion auf einen zweiten Streuwert abgebildet (14) und
- der neue Datensatz (23) oder der zweite Streuwert werden von einem ausgewählten (28) Dritten (24) verwaltet und Interessenten (25) an der Leistung (21) auf Anfrage (27) bereitgestellt (15).

2. Verfahren (10) nach Anspruch 1, **gekennzeichnet durch** folgende Merkmale:
- vom Dritten (24) wird ferner ein Nachweis (26) des Empfängers (22) über eine Berechtigung zur Bewertung des Erbringers (20) verwaltet und
- vor dem Hinzufügen des neuen Datensatzes (23) wird dem Erbringer (20) die Berechtigung durch den Dritten (24) bestätigt (29).

3. Verfahren (10) nach Anspruch 2, **gekennzeichnet durch** mindestens eines der folgenden Merkmale:
- der Nachweis (26) wird dem Empfänger (22) durch den Erbringer (20) der Leistung (21) bereitgestellt oder
- der Nachweis (26) belegt eine Inanspruchnahme der Leistung (21) durch den Empfänger (22).

4. Verfahren (10) nach Anspruch 2 oder 3, **gekennzeichnet durch** mindestens eines der folgenden Merkmale:
- der neue Datensatz (23) wird vom Empfänger (22) der Leistung (21) signiert,
- der zweite Streuwert wird vom Empfänger (22) der Leistung (21) signiert oder
- der Nachweis (26) über die Berechtigung wird vom Empfänger (22) der Leistung (21) signiert.

5. Verfahren (10) nach einem der Ansprüche 1 bis 4, **gekennzeichnet durch** folgende Merkmale:
- die Bewertungen definieren eine dezentrale Identität des Erbringers (20) in der Transaktionsdatenbank und
- die Interessenten (25) fordern bezugnehmend auf die Identität bedarfsweise eine mittels der Transaktionsdatenbank nachprüfbare Darstellung (28) der Bewertungen an.

6. Verfahren (10) nach Anspruch 5, **gekennzeichnet durch** folgende Merkmale:
- die dezentrale Identität ist eine selbstsouveräne Identität des Erbringers (20) und
- die Darstellung (28) erfolgt durch den Erbringer (20).

7. Verfahren (10) nach einem der Ansprüche 1 bis 6, **gekennzeichnet durch** folgende Merkmale:
- die Transaktionsdatenbank umfasst eine Blockkette und
- das Hinzufügen der Datensätze umfasst ein Angliedern entsprechender Datenblöcke an die Blockkette.

8. Computerprogramm, welches eingerichtet ist, das Verfahren (10) nach einem der Ansprüche 1 bis 7 auszuführen.

9. Maschinenlesbares Speichermedium, auf dem das Computerprogramm nach Anspruch 8 gespeichert ist.

10. Vorrichtung (50), die eingerichtet ist, das Verfahren (10) nach einem der Ansprüche 1 bis 7 auszuführen.

Es folgen 4 Seiten Zeichnungen

Anhängende Zeichnungen

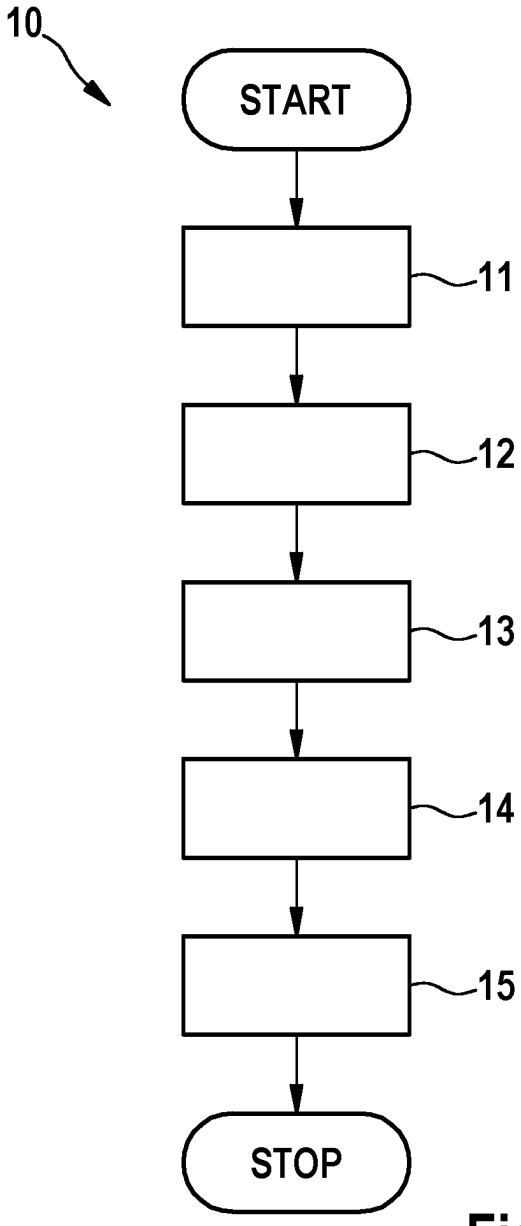


Fig. 1

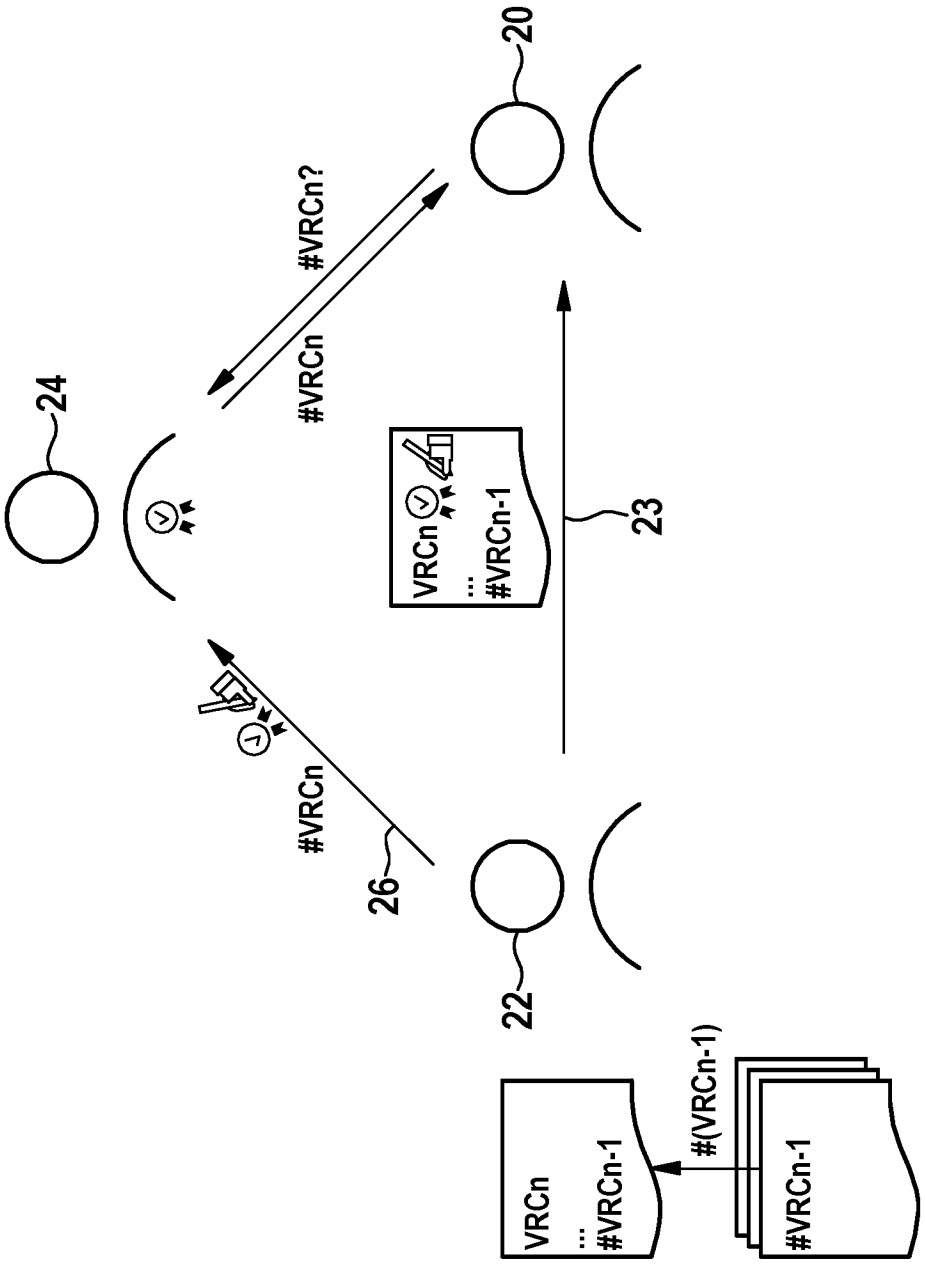

20
#VRCn?
#VRCn
24
VRCn
...
#VRCn-1
23
#VRCn
26
22
VRCn
...
#VRCn-1
#(VRCn-1)
#VRCn-1

Fig. 2

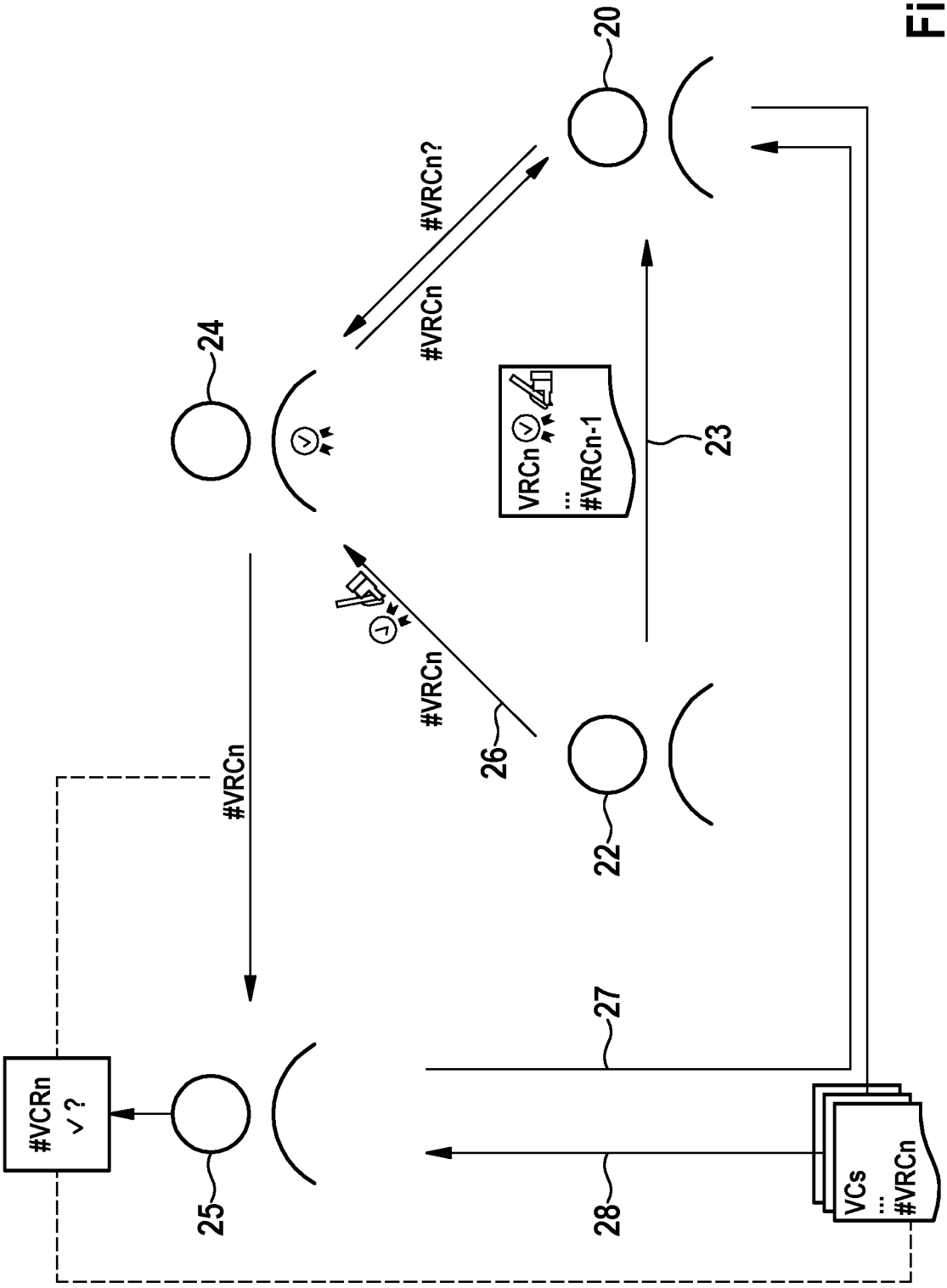

20
#VRCn?
#VRCn
24
VRCn
...
#VRCn-1
23
#VRCn
26
#VRCn
22
27
#VCRn
v ?
25
28
VCs
...
#VRCn

Fig. 3

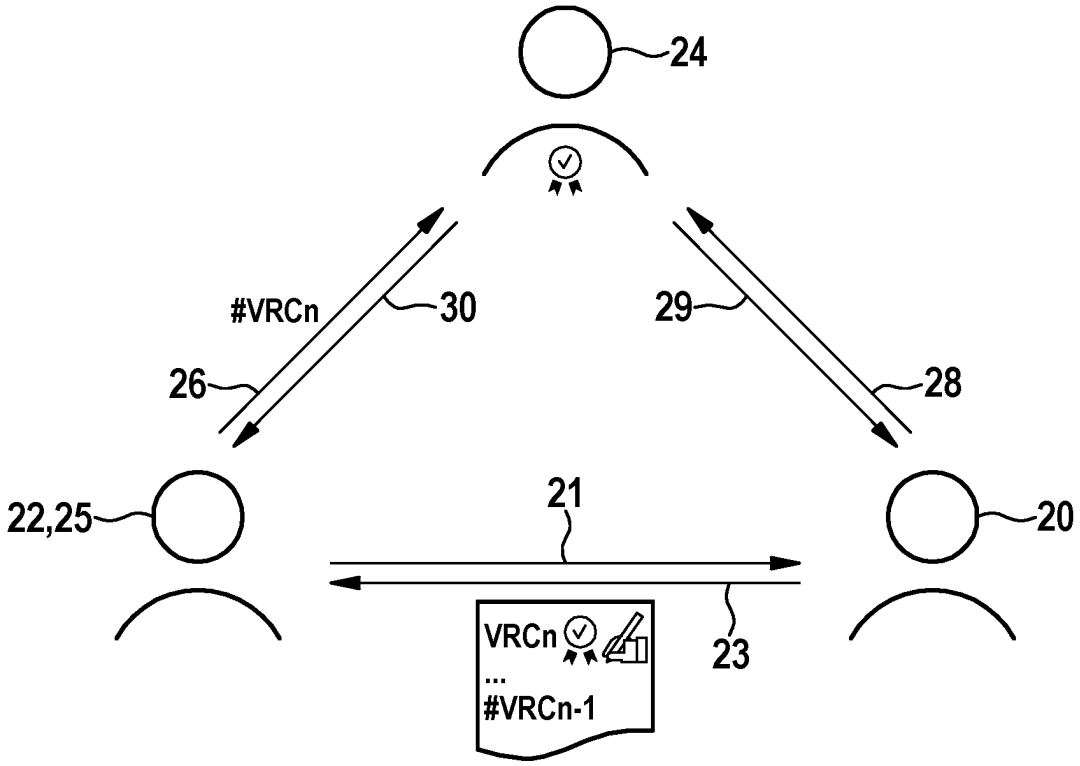


Fig. 4

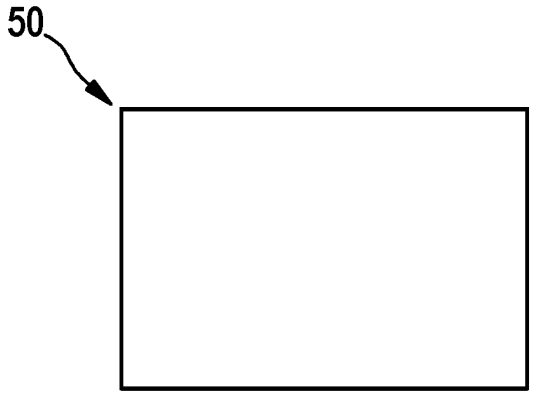


Fig. 5

