(19) Deutsches Patent- und Markenamt

(10) **DE 10 2018 210 224 A1** 2019.12.24

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2018 210 224.4**
(22) Anmeldetag: **22.06.2018**
(43) Offenlegungstag: **24.12.2019**

(51) Int Cl.: ***G06Q 40/08*** (2012.01)
G06Q 50/30 (2012.01)
B60W 30/02 (2012.01)

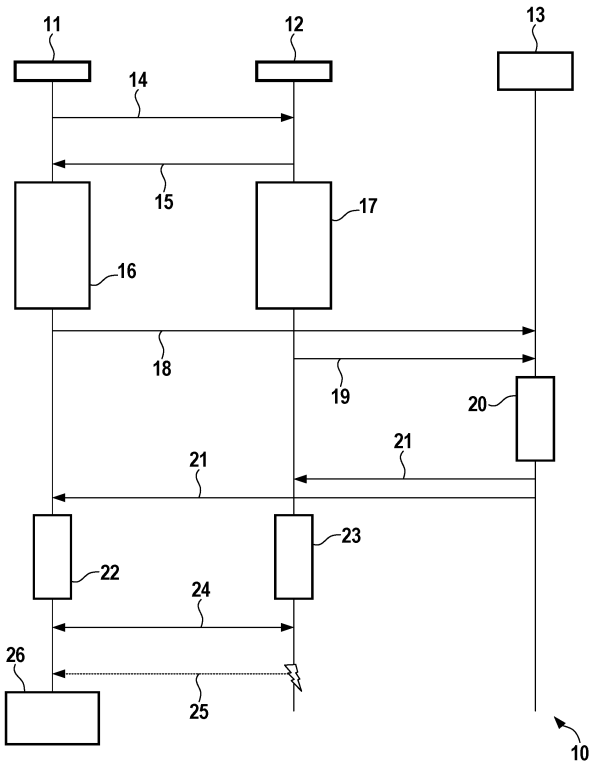
(71) Anmelder:
Robert Bosch GmbH, 70469 Stuttgart, DE

(72) Erfinder:
Amarnath, Rakshith, 71282 Hemmingen, DE; Nordmann, Arne, 70499 Stuttgart, DE; Scharmann, Nik, 74321 Bietigheim-Bissingen, DE; Burton, Simon, 70839 Gerlingen, DE; Munk, Peter, 70195 Stuttgart, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Verfahren und Vorrichtung zum Vereinbaren einer Zusammenarbeit zwischen einem ersten System und einem zweiten System**

(57) Zusammenfassung: Verfahren (10, 30, 40) zum Vereinbaren einer Zusammenarbeit zwischen einem ersten System (11) und einem zweiten System (12),
gekennzeichnet durch folgende Merkmale:
- Annahmen des ersten Systems (11) bezüglich des zweiten Systems (12) und Garantien des ersten Systems (11) an das zweite System (12) werden vom ersten System (11) gesendet (14),
- Annahmen des zweiten Systems (12) bezüglich des ersten Systems (11) und Garantien des zweiten Systems (12) an das erste System (11) werden vom zweiten System (12) gesendet (15),
- falls die wechselseitigen Annahmen und Garantien einander entsprechen, wird ein digitaler Sicherheitsvertrag zwischen dem ersten System (11) und dem zweiten System (12) geschlossen und
- der Sicherheitsvertrag wird in einer Transaktionsdatenbank (13) dokumentiert.



Beschreibung

[0001] Die vorliegende Erfindung betrifft ein Verfahren zum Vereinbaren einer Zusammenarbeit zwischen einem ersten System und einem zweiten System. Die vorliegende Erfindung betrifft darüber hinaus eine entsprechende Vorrichtung, ein entsprechendes Computerprogramm sowie ein entsprechendes Speichermedium.

Stand der Technik

[0002] Als dezentrales Transaktionssystem oder Transaktionsdatenbank (distributed ledger) wird jegliches Protokoll in Rechnernetzen bezeichnet, das eine Übereinkunft (consensus) hinsichtlich der Abfolge bestimmter Transaktionen herbeiführt, die beispielsweise die Aktualisierung von Daten betreffen. Eine häufige Ausprägung eines solchen Systems bedient sich einer Blockkette (blockchain).

[0003] Ein Computersystem, das mit einer Blockchain verbunden ist, wird etwa in US 9,794,074 B2 offenbart. Das Computersystem empfängt Übereinstimmungsdaten für eine Übereinstimmung zwischen einer ersten Datentransaktion, die einer ersten Kennung zugeordnet ist, und einer zweiten Datentransaktion, die einer zweiten Kennung zugeordnet ist. Basierend auf den in der Blockchain gespeicherten Daten wird eine erste Blockchain-Transaktion erzeugt. Es wird mindestens eine weitere Blockchain-Transaktion erzeugt, die die Übereinstimmung in zwei verschiedene Transaktionen aufteilt: eine zwischen der ersten Kennung und einem Vermittler und das zweite zwischen dem Vermittler.

[0004] Diese werden über die weiteren Blockchain-Transaktionen in der Blockchain erfasst.

Offenbarung der Erfindung

[0005] Die Erfindung stellt ein Verfahren zum Vereinbaren einer Zusammenarbeit zwischen einem ersten System und einem zweiten System, eine entsprechende Vorrichtung, ein entsprechendes Computerprogramm sowie ein entsprechendes Speichermedium gemäß den unabhängigen Ansprüchen bereit.

[0006] Das erfindungsgemäße Verfahren fußt auf der Erkenntnis, dass immer mehr sicherheitskritische Systeme im Betrieb zusammenarbeiten müssen. Diese Systeme werden mitunter von verschiedenen Herstellern entwickelt. Daher müssen sie mit anderen Systemen kooperieren, deren Verhalten und Eigenschaften zum Zeitpunkt ihres Entwurfes unbekannt sind. Beispiele für solche Systeme sind heterogene Fahrzeuge, die sich z. B. zur Verkehrsberuhigung oder -regelung oder für Notdienste miteinander austauschen, hochautomatisierte Lastwagen, die eine Kolonne bilden und automatisch einem führenden Lastwagen mit einem menschlichen Fahrer folgen, bedingt automatisierte Lastwagen, die eine Kolonne bilden und automatisch einem führenden hochautomatisierten Lastwagen folgen, Schneepflüge, die automatisch einem seitlich versetzten, von einem Menschen gelenkten Pflug auf einem Flugfeld oder einer Skipiste folgen, Autos, die mit einem Lotsensystem auf einem Parkplatz kooperieren, Landwirtschaftsroboter, die gleich einem Schwarm ein Feld düngen oder abernten, oder Herstellungsroboter, die sich auf einer Fahrfläche bewegen und mit anderen Robotern oder sogar Menschen zusammenarbeiten, um eine gemeinsame Aufgabe zu erfüllen.

[0007] Aufgrund der möglichen Gefährdungen sind an die Betriebssicherheit dieser „Systeme von Systemen“ hohe Anforderungen zu stellen. Um solch dynamische Konfigurationen unter Berücksichtigung der Sicherheitsanforderungen zu bewältigen, wurden in der Literatur sogenannte Sicherheitsverträge (safety contracts) vorgeschlagen. Zum Zeitpunkt seines Entwurfes wird nach diesem Ansatz für jedes System eine Reihe von (formell beschriebenen) Annahmen und Garantien definiert. Die Garantien jedes Systems unter den gegebenen Annahmen können mit bekannten Sicherheitsanalysetechniken ebenfalls im Rahmen des Entwurfes analysiert werden. Zur Laufzeit tauschen potenziell kooperierende Systeme ihre Annahmen und Garantien untereinander aus. Jedes System entscheidet dann, ob die Garantien des anderen Systems seinen Annahmen entsprechen. Wenn sie übereinstimmen, wird ein Sicherheitsvertrag geschlossen, was bedeutet, dass, solange die Annahmen jedes Systems erfüllt sind, auch die eigenen Garantien erfüllt werden. Die Annahmen und Garantien können auch Parameter enthalten, um mehr Flexibilität zu ermöglichen.

[0008] Betrachtet seien zum Beispiel zwei hochautomatisierte Lastwagen, die eine Kolonne bilden sollen. Dabei sei angenommen, die Fahrzeuge würden von verschiedenen Herstellern stammen, aber das Sicherheitsvertragsformat und das Austauschprotokoll seien zur Entwurfszeit vereinbart worden. Die Annahme eines Lastwagens könnte darin bestehen, dass er innerhalb einer vorgegebenen Zeitspanne **X** informiert wird, wenn der Lastwagen, dem er folgt, bremst. Eine Garantie indes könnte darin bestehen, dass der Lastwagen, die ihrerseits ihm folgen, innerhalb einer vorgegebenen Zeitspanne **Y** informiert, wenn er selbst bremst. Offensichtlich können die Sicherheitsverträge nur dann geschlossen und daher die Kolonne nur dann gebildet werden, wenn $Y < X$ ist, was beide Lastwagen prüfen müssen.

[0009] Der vorgeschlagene Ansatz trägt ferner dem Umstand Rechnung, dass im Allgemeinen das Risiko eines Systemausfalls besteht. Wenn ein System ausfällt, kann es gegen seine Garantien verstoßen und wenn es zum Zeitpunkt des Ausfalls mit ande-

ren Systemen zusammenarbeitet, bricht es seinen Sicherheitsvertrag. Obwohl der Sicherheitsvertrag einen technischen Ursprung hat, können solche Situationen rechtliche Probleme verursachen oder eine Klärung möglicher Versicherungsansprüche erfordern, insbesondere da kein Mensch an der Schließung des Sicherheitsvertrags beteiligt war und wenn verschiedene Hersteller beteiligt sind.

[0010] Das grundlegende Merkmal eines erfindungsgemäßen Ansatzes besteht hierbei darin, dass jedes System, das erfolgreich einen Sicherheitsvertrag mit einem anderen System geschlossen hat, einen Datensatz erstellt, der diese Informationen enthält, und diese an die Transaktionsdatenbank übermittelt.

[0011] Wenn das andere System versagt und den Sicherheitsvertrag verletzt, indem es die abgegebenen Garantien bricht, kann es das Zustandekommen des Vertrages nicht bestreiten. Auf diese Weise wird Rechtssicherheit für den Hersteller erreicht. Hersteller müssen nicht einer einzigen Einheit vertrauen, die die Sicherheitsverträge speichert, doch sie müssen dem vorgeschlagenen Protokoll zustimmen und es umsetzen.

[0012] Durch die in den abhängigen Ansprüchen aufgeführten Maßnahmen sind vorteilhafte Weiterbildungen und Verbesserungen des im unabhängigen Anspruch angegebenen Grundgedankens möglich. So kann vorgesehen sein, dass die beteiligten Systeme nach dem Aufnehmen der Zusammenarbeit jeweils wiederholt ein Umgebungsmodell an die Transaktionsdatenbank senden und letztere die Umgebungsmodelle der Blockkette hinzufügt. Im Falle eines Fehlers können diese Daten nicht abgestritten werden und helfen, die Situation zu rekonstruieren. Falls eines der teilnehmenden Systeme versagt, wird seinem Hersteller auf diese Weise der Nachweis erleichtert, dass ein Sicherheitsvertrag nicht nur bestand, sondern auch, dass ein anderes System dagegen verstoßen hat.

[0013] Gemäß einem weiteren Aspekt kann vorgesehen sein, dass die beteiligten Systeme nach dem Aufnehmen der Zusammenarbeit jeweils wiederholt einen Streuwert (hash) des Umgebungsmodells an die Transaktionsdatenbank senden und letztere lediglich diese Streuwerte der Blockkette hinzufügt. Der Hash des Umgebungsmodells hat eine erheblich geringere Größe als das gesamte Modell und kann daher viel schneller an die Transaktionsdatenbank gesendet werden. Bei einem Unfall kann der Hersteller nachweisen, dass die in der Systemdatenbank aufgezeichnete Umgebung nicht verändert wurde.

[0014] Gemäß einem weiteren Aspekt kann vorgesehen sein, dass die Systeme einen wechselseitigen Transaktionskanal etablieren, über welchen sie nach dem Empfangen des Blockes mit dem Sicherheitsvertrag Informationen und unterschriebene Mitteilungen austauschen. Dieses Konzept reduziert den Umfang der Kommunikation mit der Transaktionsdatenbank, wodurch typischerweise Transaktionsgebühren (in einer Kryptowährung) reduziert werden. Außerdem kann im Fehlerfall automatisch erkannt werden, welches System den Sicherheitsvertrag tatsächlich verletzt hat, und es kann automatisch eine Geldstrafe (in einer Kryptowährung) mit einer Kaution verrechnet werden, die beide Systeme bei der Erstellung des digitalen Vertrages aufbringen mussten. Die besagte Ausführungsform verbessert auch die Rechtssicherheit bei einem Unfall, da die zuletzt vereinbarten Informationen und deren Zeitstempel bekannt und in der Transaktionsdatenbank gespeichert sind.

[0015] Gemäß einem weiteren Aspekt kann vorgesehen sein, dass die Blockkette der Transaktionsdatenbank auf zahlreiche Endgeräte verteilt ist und die am Sicherheitsvertrag beteiligten Systeme eine digitale Geldbörse verwalten, aus welcher sie die Endgeräte für das Hinzufügen von Blöcken vergüten. Mit einer solchen Geldbörse werden Zahlungen an die „Schürfer“ (miners) möglich, bei denen die teilnehmenden Systeme ihnen einen Betrag zahlen könnten, der umgekehrt proportional zu der Zeit ist, die benötigt wird, um die für die Rechtssicherheit relevanten Informationen zu verifizieren und der Blockkette hinzuzufügen. Ferner wird eine echte „Wirtschaft der Dinge“ (economy of things, EoT) ermöglicht, wenn teilnehmende Systeme auf diese Weise für die bezogene Leistung zahlen oder dafür bezahlt werden, wenn sie selbst einen Dienst für andere Systeme erbringen - etwa im Falle eines vorausfahrenden Fahrzeuges, das dem nachfolgenden Fahrzeug hilft, die Möglichkeit eines Überholmanövers jenseits einer vorausliegenden Kurve einzuschätzen.

Figurenliste

[0016] Ausführungsbeispiele der Erfindung sind in den Zeichnungen dargestellt und in der nachfolgenden Beschreibung näher erläutert. Es zeigt:

Fig. 1 ein Verfahren, gemäß dem zwei Systeme mittels einer Blockkette eine rechtssichere Zusammenarbeit vereinbaren.

Fig. 2 eine Variante des Verfahrens, bei welcher die Transaktionsdatenbank mit Rechenfunktionen ausgestattet und so in der Lage ist, den Sicherheitsvertrag aufzusetzen.

Fig. 3 eine Variante des Verfahrens, bei welcher die Systeme einen intelligenten Kanal einrichten, um Informationen auszutauschen. Ein System sendet hierbei Informationen, die vom anderen System als fehlerhaft angesehen werden. Dank der Rechenfunktion des digitalen Vertrages in der Transaktionsdatenbank kann überprüft wer-

den, welches System im Recht ist und welches die letzte überstimmende Information war.

Fig. 4 schematisch ein erfindungsgemäßes Steuergerät.

Ausführungsformen der Erfindung

[0017] **Fig. 1** zeigt die Zeitachsen von zwei Systemen (**11**, **12**) von verschiedenen Herstellern einer verteilten Transaktionsdatenbank (**13**). Die Systeme (**11**, **12**) kommunizieren über eine Internetverbindung mit der verteilten Transaktionsdatenbank (**13**); die Kommunikation zwischen den Systemen (**11**, **12**) erfolgt unmittelbar von Fahrzeug zu Fahrzeug (car to car, C2C) oder ebenfalls über eine Internetverbindung. Zunächst tauschen beide Systeme (**11**, **12**) ihre Annahmen und Garantien (**14**, **15**) aus, und jedes System prüft (**16**, **17**), ob sie übereinstimmen, d. h. ob ein Sicherheitsvertrag unterzeichnet werden kann. Wenn dies der Fall ist, sendet jedes System (**11**, **12**) einen Datensatz (**18**, **19**) an die Transaktionsdatenbank (**13**). Der jeweilige Datensatz (**18**, **19**) kann die grundlegende Information, dass ein Sicherheitsvertrag geschlossen wurde, sowie die Eigenschaften oder die Gesamtheit der vereinbarten Annahmen und Garantien enthalten. Da beide Systeme (**11**, **12**) einen Datensatz (**18**, **19**) erstellen, kann jeder Datensatz (**18**, **19**) die Kennung (identifier, ID) der „Gegenseite“ (**12** bzw. **11**) enthalten.

[0018] Diese ID sollte in der verteilten Transaktionsdatenbank (**13**) eindeutig sein und ist der sogenannten Wallet-ID einer Kryptowährung vergleichbar.

[0019] Für die Zeitspanne, die bis zur Aufnahme des Datensatzes (**18**, **19**) in die verteilte Transaktionsdatenbank (**13**) benötigt wird, bieten sich zwei mögliche Verfahrensweisen an: Entweder nehmen die Systeme (**11**, **12**) die Zusammenarbeit auf und verzichten auf abschließende Rechtssicherheit, bis der Datensatz (**18**, **19**) der Blockkette hinzugefügt wird, oder warten, bis der Datensatz (**18**, **19**) hinzugefügt wurde, bevor sie mit der Zusammenarbeit beginnen (**23**). In der Ausführungsform gemäß **Fig. 1** warten beide Systeme (**11**, **12**), bis sie eine Bestätigung von der Transaktionsdatenbank (**13**) darüber erhalten, dass der Block erfolgreich hinzugefügt wurde.

[0020] Sobald die Datensätze (**18**, **19**) in der Transaktionsdatenbank (**13**) abgelegt und die neuen Blöcke (**21**) von beiden Systemen (**11**, **12**) empfangen wurden, kann jedes System (**11**, **12**) prüfen (**22**, **23**), ob die jeweils andere Partei (**12** bzw. **11**) einen übereinstimmenden Datensatz (**19** bzw. **18**) erstellt hat. Wenn kein Datensatz hinzugefügt wurde, ist die ID des Gegenübers falsch; wenn zwar ein Datensatz hinzugefügt wurde, dessen ID jedoch nicht übereinstimmt, ist ein Fehler oder Angriff wahrscheinlich und die Zusammenarbeit wird aufgegeben. In **Fig. 1** stimmen die Datensätze (**18**, **19**) beider Systeme (**11**, **12**) überein und letztere nehmen die Zusammenarbeit auf (23).

[0021] Betrachtet sei nun der Fall, dass ein System (**11**, **12**) ausfällt und seine Garantie bzw. den Sicherheitsvertrag verletzt, wie im Falle des zweiten, abbildungsgemäß rechten Systems (**12**) in **Fig. 1** dargestellt. Wenn möglich, überwacht das erste System (**11**) die vom zweiten System (**12**) empfangenen Daten und prüft, ob dieses die vereinbarten Garantien erfüllt. Wenn die entsprechende Überwachungskomponente eine Verletzung (**25**) des Sicherheitsvertrags feststellt, beendet sie die Zusammenarbeit (**26**) und versucht, das System (**11**) in einen sicheren Zustand zu versetzen. Dies mag im Einzelfall nicht möglich sein, da komplexe Garantien gar nicht erst überwacht werden können. In jedem Fall haben beide Hersteller Zugang zu dem Sicherheitsvertrag, den beide Systeme (**11**, **12**) geschlossen haben, und keiner der beiden kann den Vertragsschluss daher bestreiten. Daher hat jeder Hersteller im Falle einer Garantieverletzung oder eines Unfalls nachzuweisen, dass sein System (**11**, **12**) diesen Sicherheitsvertrag erfüllt hat. Man beachte, dass dieses Vorgehen im Wesentlichen dem üblichen Verfahren nach einem Unfall zwischen herkömmlichen Fahrzeugen entspricht, wobei die Straßenverkehrsordnung dem Sicherheitsvertrag entspricht.

[0022] Eine erste Variante des Verfahrens (**10**) nimmt sich des Problems an, dass, falls die teilnehmenden Systeme (**11**, **12**) versagen, deren Hersteller zwar nachweisen können, dass ein Sicherheitsvertrag bestand, aber nicht beweisen können, dass das jeweils andere System (**12**, **11**) gegen diesen verstoßen hat. Eine Möglichkeit, diesen Nachweis zu erleichtern, besteht darin, dass der Sicherheitsvertrag eine Klausel enthält, wonach beide Systeme (**11**, **12**) eine Darstellung ihres Systemzustandes einschließlich ihres Umgebungsmodells (Kamerabild, Position in der Karte etc.) wie im Sicherheitsvertrag definiert periodisch an die verteilte Transaktionsdatenbank (**13**) senden müssen.

[0023] Eine zweite Variante ähnelt der ersten, wobei jedoch jedes System (**11**, **12**) einen kryptografischen Hash seines gesamten Umgebungsmodells erstellt und das Modell und den Hash in einer lokalen Datenbank speichert.

[0024] Eine dritte Variante (**30** - **Fig. 2**) nutzt die Möglichkeit einiger verteilter Transaktionsdatenbanken, in einem Datensatz enthaltene ausführbare Anweisungen auf mehreren Endgeräten verteilt zu berechnen. Ein bekanntes Beispiel für eine für eine solche Transaktionsdatenbank ist die Kryptowährung „Ethereum“, welche entsprechende Funktionen für digitale Verträge erfüllt. Daher ist es auch möglich, dass beide Systeme (**11**, **12**) ihre Annahmen und Garantien an eine verteilte Transaktionsdatenbank (**13**)

mit Berechnungsfähigkeit senden, wie in **Fig. 2** gezeigt. Die verteilte Transaktionsdatenbank (**13**) bewertet die Annahmen und Garantien und speichert im Erfolgsfall den Sicherheitsvertrag (**31**). Die Systeme (**11**, **12**) beginnen mit der Zusammenarbeit (**23**), sobald sie jeweils den Block mit ihrem Sicherheitsvertrag (**32**) erhalten haben.

[0025] Eine in **Fig. 3** dargestellte vierte Variante (**40**) erweitert die dritte Variante wie folgt: Blockchains wie „Lightning“ und „Raiden“ haben ein als Transaktions- oder Zustandskanal (state Channel) bezeichnetes Konzept eingeführt. Ein Zustandskanal ist ein direkter Kommunikationskanal zwischen den Systemen (**11**, **12**) und ein digitaler Vertrag in der Blockchain, der von diesen Systemen (**11**, **12**) geschlossen wird. Die Systeme (**11**, **12**) tauschen über diesen Kanal Informationen direkt aus. Das Empfängersystem (**11**, **12**) quittiert die jeweils empfangene Information (**42**, **44**, **46**) mit einer kryptografisch signierten Mitteilung (**43**, **45**), wenn es der empfangenen Nachricht zustimmt. Falls beide Systeme (**11**, **12**) die Zusammenarbeit beenden wollen oder eines der Systeme (**11**, **12**) feststellt, dass die empfangene Information (hier: **46**) den Sicherheitsvertrag verletzt, z. B. die Bremskraft eines entsprechend ausgerüsteten Fahrzeuges den im Sicherheitsvertrag definierten Maximalwert übersteigt, kann es im digitalen Vertrag in der Blockchain eine Abrechnungsfunktion ausführen (**47**). Beide Systeme (**11**, **12**) müssen dann den digitalen Vertrag vom letzten einvernehmlichen Zustand gewissermaßen „überzeugen“, indem sie ihre Zustimmungsmitteilungen absenden.

[0026] Den Schwerpunkt der bisher erläuterten Ausführungsformen stellt die Rechtssicherheit für die zusammenarbeitenden Systeme (**11**, **12**) aufgrund der Manipulationssicherheit der Blockchain dar. Da jedoch Rechenleistung aufgewendet wird, um Blöcke zu pflegen und zu aktualisieren, ist auch eine Belohnung für den hierzu erbrachten Arbeitsnachweis (proof of work, PoW) wünschenswert. Daher sieht eine fünfte Variante des Verfahrens (**10**) vor, dass die teilnehmenden Systeme mit Mechanismen ausgestattet sind, um zum Beispiel mittels digitaler Geldbörsen Transaktionen durchzuführen, um Einheiten einer virtuellen Währung als Werteinheit für die Zusammenarbeit zu speichern.

[0027] Gemäß einer sechsten Variante kann die Einbeziehung der von früheren Kollaborationspartnern bewerteten Vertrauenswürdigkeit eines Systems die Auswahl des Partners für eine spätere Zusammenarbeit einschränken. Im Hinblick auf einen solchen Anwendungsfall kann eine virtuelle Krypto-Wallet auch die besagte Vertrauenswürdigkeit speichern. Dies würde beispielsweise ermöglichen, dass ein Produkt für die Verwendung in bestimmten Interaktionsszenarien zertifiziert (und ihm dadurch eine Vertrauenswürdigkeit zugewiesen) wird, wodurch die Zusammenarbeit auf Produkte beschränkt wird, die grundsätzlich kompatibel sein sollten. Das Vertrauen, das dem anderen System entgegengebracht wird, kann sich im Laufe der Zeit abhängig von der Quantität und Qualität seiner Zusammenarbeit erhöhen. Die resultierende Bewertung kommt nicht nur den an der Blockkette beteiligten Endgeräten, sondern auch Zertifizierungsstellen und anderen Treuhändern zugute.

[0028] Gemäß einer siebten Variante schließlich können die Sicherheitsverträge von den Systemen anstelle der Blockchain an einen zentralen Server oder eine Datenbank gesendet werden, dem bzw. der die Hersteller der Systeme vertrauen.

[0029] Dieses Verfahren 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. 4** verdeutlicht.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- US 9794074 B2 [0003]

Patentansprüche

1. Verfahren (10, 30, 40) zum Vereinbaren einer Zusammenarbeit zwischen einem ersten System (11) und einem zweiten System (12), **gekennzeichnet durch** folgende Merkmale:
- Annahmen des ersten Systems (11) bezüglich des zweiten Systems (12) und Garantien des ersten Systems (11) an das zweite System (12) werden vom ersten System (11) gesendet (14),
- Annahmen des zweiten Systems (12) bezüglich des ersten Systems (11) und Garantien des zweiten Systems (12) an das erste System (11) werden vom zweiten System (12) gesendet (15),
- falls die wechselseitigen Annahmen und Garantien einander entsprechen, wird ein digitaler Sicherheitsvertrag zwischen dem ersten System (11) und dem zweiten System (12) geschlossen und
- der Sicherheitsvertrag wird in einer Transaktionsdatenbank (13) dokumentiert.

2. Verfahren (10, 30, 40) nach Anspruch 1, **gekennzeichnet durch** folgende Merkmale:
- die Annahmen des ersten Systems (11) bezüglich des zweiten Systems (12) und Garantien des ersten Systems (11) an das zweite System (12) werden vom zweiten System (12) empfangen,
- die Annahmen des zweiten Systems (12) bezüglich des ersten Systems (11) und Garantien des zweiten Systems (12) an das erste System (11) werden vom ersten System (11) empfangen,
- das erste System (11) prüft (16), ob die Garantien des zweiten Systems (12) den Annahmen des ersten Systems (11) entsprechen und sendet gegebenenfalls einen ersten Eintrag (18) mit dem Sicherheitsvertrag und einer Kennung des zweiten Systems (12) an die Transaktionsdatenbank (13),
- das zweite System (12) prüft (17), ob die Garantien des ersten Systems (11) den Annahmen des zweiten Systems (12) entsprechen und sendet gegebenenfalls einen zweiten Eintrag (19) mit dem Sicherheitsvertrag und einer Kennung des ersten Systems (11) an die Transaktionsdatenbank (13),
- die Transaktionsdatenbank (13) fügt die Einträge einer Blockkette hinzu (20),
- die Transaktionsdatenbank (13) sendet die hinzugefügten Einträge der Blockkette (21) an das erste System (11) und das zweite System (12),
- das erste System (11) prüft (22) den zweiten Eintrag,
- das zweite System (12) prüft (23) den ersten Eintrag,
- wenn die Einträge übereinstimmen, nehmen das erste System (11) und das zweite System (12) die Zusammenarbeit auf (24) und
- wenn eines der Systeme (11, 12) eine Verletzung (25) des Sicherheitsvertrages durch das andere System (12, 11) feststellt, beendet es die Zusammenarbeit (26).

3. Verfahren (10, 30, 40) nach Anspruch 2, **gekennzeichnet durch** folgendes Merkmal:
- das erste System (11) und das zweite System (12) senden nach dem Aufnehmen der Zusammenarbeit (24) jeweils wiederholt ein Umgebungsmodell an die Transaktionsdatenbank (13) und
- die Transaktionsdatenbank (13) fügt der Blockkette die Umgebungsmodelle hinzu.

4. Verfahren (10, 30, 40) nach Anspruch 2, **gekennzeichnet durch** folgende Merkmale:
- das erste System (11) und das zweite System (12) senden nach dem Aufnehmen der Zusammenarbeit (24) jeweils wiederholt einen Streuwert eines Umgebungsmodells an die Transaktionsdatenbank (13) und
- die Transaktionsdatenbank (13) fügt der Blockkette die Streuwerte hinzu.

5. Verfahren (10, 30, 40) nach Anspruch 1, **gekennzeichnet durch** folgende Merkmale:
- die Annahmen des ersten Systems (11) bezüglich des zweiten Systems (12), Garantien des ersten Systems (11) an das zweite System (12), Annahmen des zweiten Systems (12) bezüglich des ersten Systems (11) und Garantien des zweiten Systems (12) an das erste System (11) werden von der Transaktionsdatenbank (13) empfangen (14, 15),
- die Transaktionsdatenbank (13) prüft, ob die Garantien des zweiten Systems (12) den Annahmen des ersten Systems (11) und die Garantien des ersten Systems (11) den Annahmen des zweiten Systems (12) entsprechen, setzt gegebenenfalls den Sicherheitsvertrag auf (31) und fügt der Blockkette einen entsprechenden Block hinzu,
- die Transaktionsdatenbank (13) sendet den Block mit dem Sicherheitsvertrag (32) an das erste System (11) und das zweite System (12) und
- wenn sie den Block empfangen, nehmen das erste System (11) und das zweite System (12) die Zusammenarbeit auf (23).

6. Verfahren (10, 30, 40) nach Anspruch 5, **gekennzeichnet durch** folgende Merkmale:
- das erste System (11) und das zweite System (12) etablieren einen wechselseitigen Transaktionskanal,
- nach dem Empfangen des Blockes mit dem Sicherheitsvertrag (41) tauschen die Systeme (11, 12) Informationen (42, 44, 46) und unterschriebene Mitteilungen (43, 45) über den Transaktionskanal aus,
- wenn eines der Systeme (11, 12) eine den Sicherheitsvertrag verletzende Information (46) empfängt, ersucht es die Transaktionsdatenbank (13) um eine Schlichtung (47),
- die Transaktionsdatenbank (13) setzt das andere System (12, 11) von der Schlichtung in Kenntnis (48), fordert von diesem die vermeintlich den Sicherheitsvertrag verletzende Information (46) an, und prüft diese Information (49) anhand des Sicherheitsvertrags.

7. Verfahren (10, 30, 40) nach einem der Ansprüche 2 bis 6, **gekennzeichnet durch** folgende Merkmale:
- die Blockkette ist auf zahlreiche Endgeräte verteilt,
- die Systeme (11, 12) verwalten eine digitale Geldbörse und
- die Endgeräte werden aus der Geldbörse für das Hinzufügen der Blöcke vergütet.

8. Computerprogramm, welches eingerichtet ist, das Verfahren (10, 30, 40) nach einem der Ansprüche 1 bis 7 auszuführen.

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

10. Vorrichtung, die eingerichtet ist, das Verfahren (10, 30, 40) nach einem der Ansprüche 1 bis 7 auszuführen.

Es folgen 3 Seiten Zeichnungen

Anhängende Zeichnungen

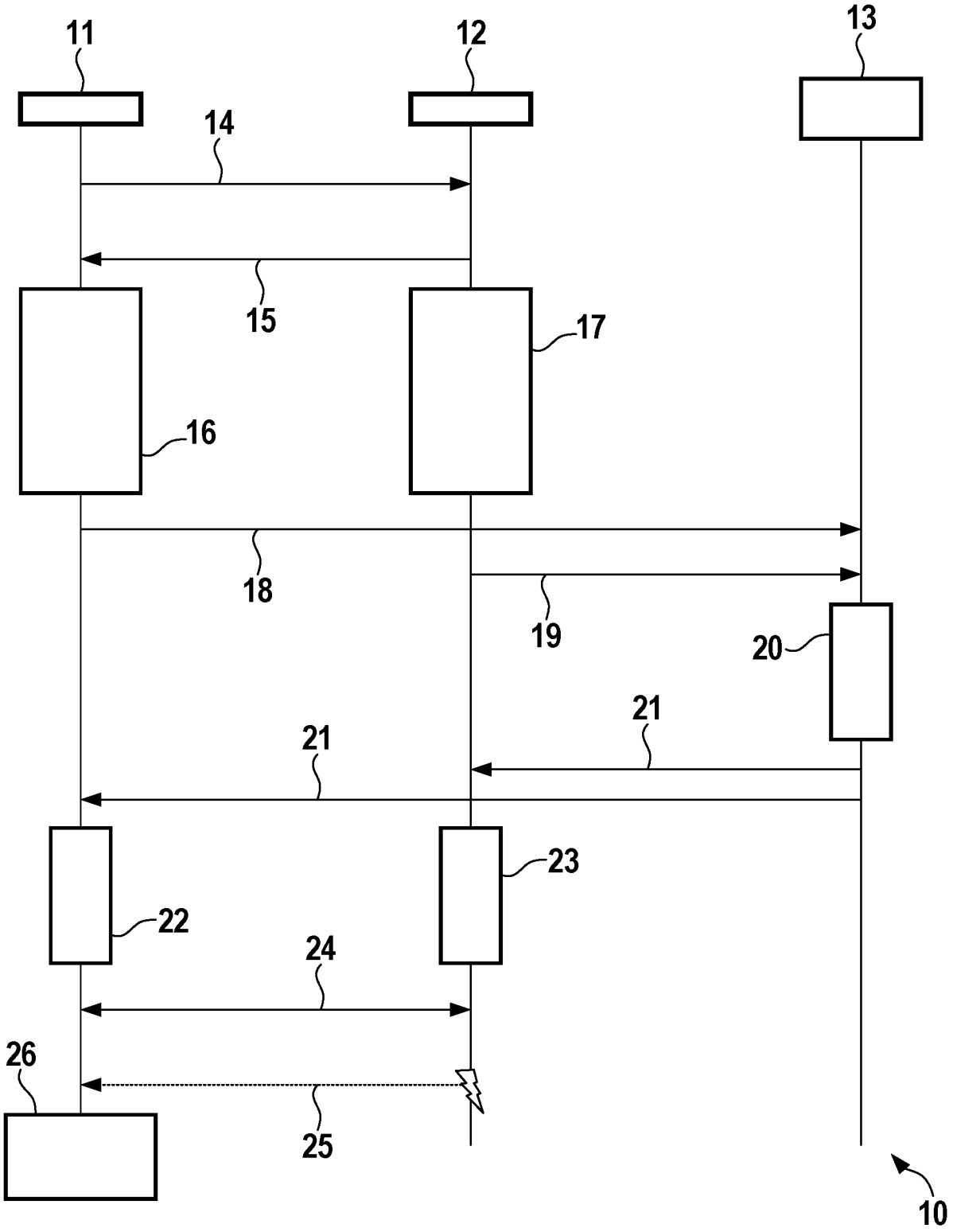


Fig. 1

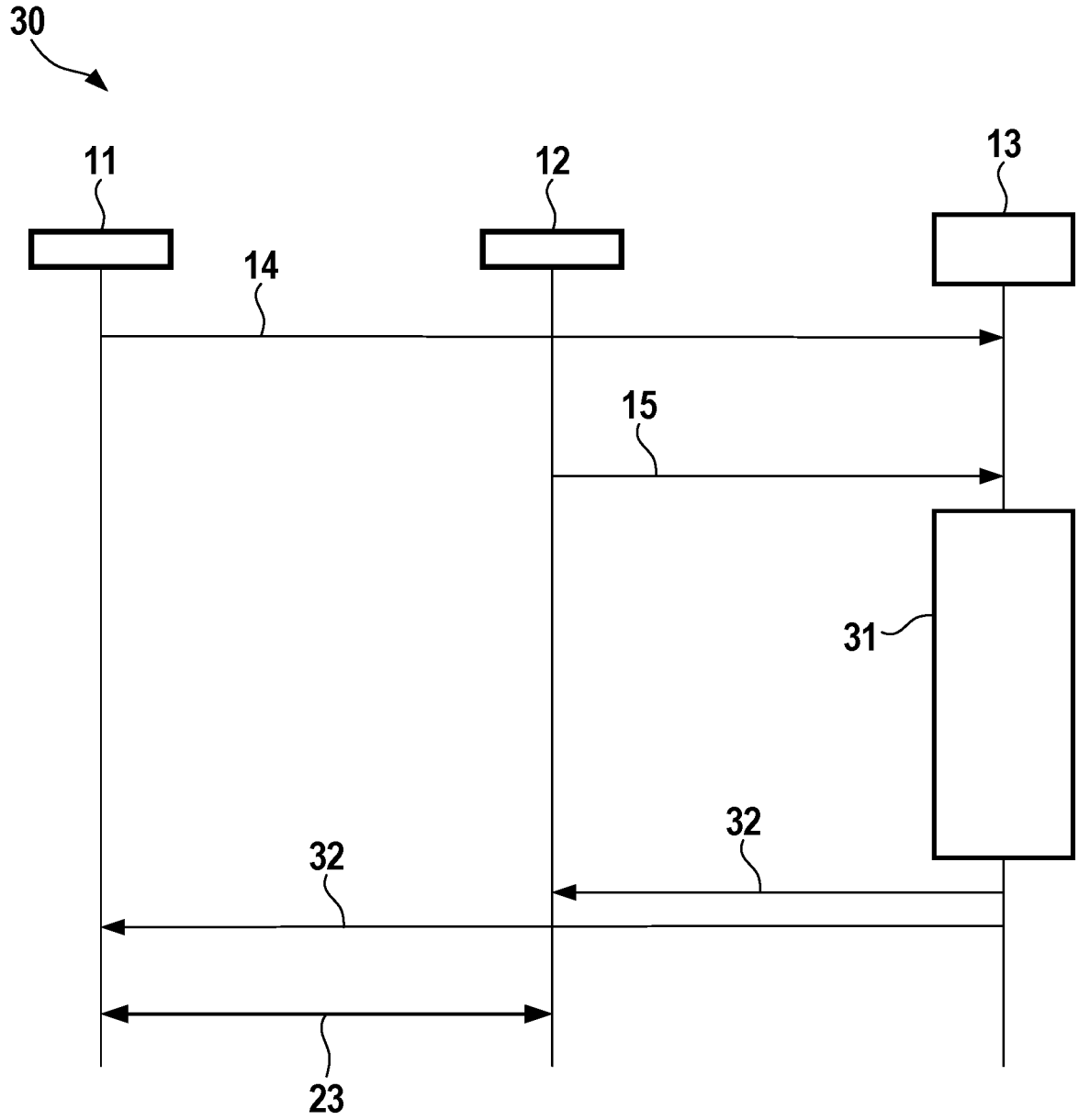


Fig. 2

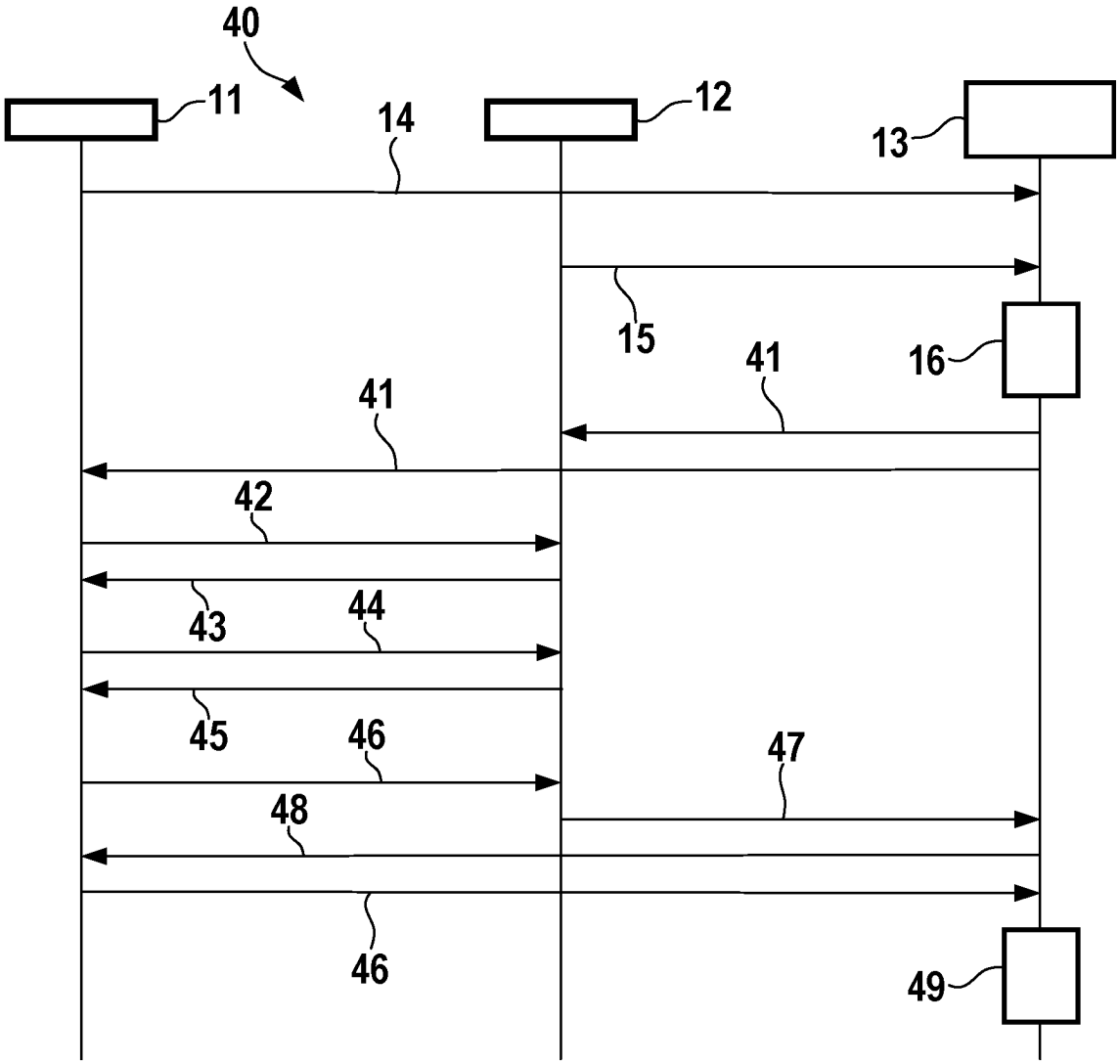


Fig. 3

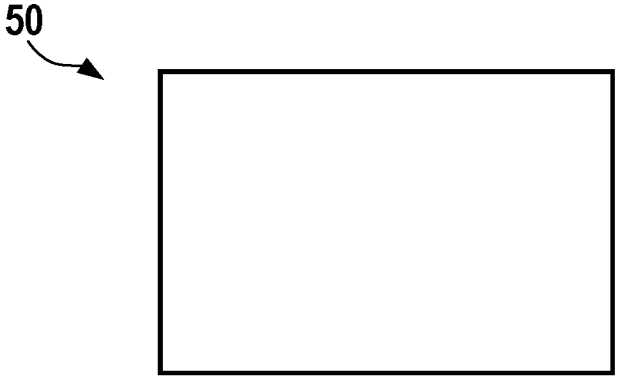


Fig. 4