(19) Deutsches Patent- und Markenamt

(10) **DE 10 2020 100 863 A1** 2020.07.16

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2020 100 863.5**
(22) Anmeldetag: **15.01.2020**
(43) Offenlegungstag: **16.07.2020**

(51) Int Cl.: ***G06F 21/64*** (2013.01)

(30) Unionspriorität:
16/248,377 **15.01.2019** **US**

(71) Anmelder:
FISHER-ROSEMOUNT SYSTEMS, INC., Round Rock, TX, US

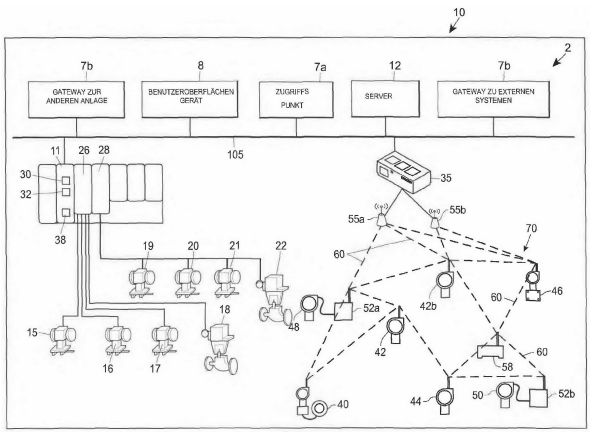
(74) Vertreter:
Meissner Bolte Patentanwälte Rechtsanwälte Partnerschaft mbB, 80538 München, DE

(72) Erfinder:
Cahill, James S., Austin, TX, US

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Blockchain-basierte Automatisierungsarchitektur für Cybersicherheit**

(57) Zusammenfassung: Um eine vertrauenswürdige, sichere und unveränderliche Aufzeichnung von Transaktionen in einer Prozessanlage bereitzustellen, werden Techniken zur Verwendung eines Distributed Ledgers in Prozessleitsystemen beschrieben. Das Distributed Ledger kann von Knoten verwaltet werden, die Transaktionen empfangen, die von Feldgeräten, Steuerungen, Bedienerarbeitsplätze oder anderen in der Prozessanlage arbeitenden Geräten gesendet werden. Die Transaktionen können Prozessanlagendaten wie Prozessparameterdaten, Produktparameterdaten, Konfigurationsdaten, Benutzerinteraktionsdaten, Verwaltungsdaten, Inbetriebnahmedaten, Anlagennetzwerkdaten und Produktverfolgungsdaten umfassen. Die Distributed Ledger können auch zum Ausführen von Smart Contracts verwendet werden, damit Maschinen wie Feldgeräte ohne menschliches Eingreifen selbstständig Transaktionen ausführen können. Auf diese Weise können aufgezeichnete Prozessparameterwerte und Produktparameterwerte abgerufen werden, um die Qualität der Produkte zu überprüfen. Darüber hinaus können regulatorische Daten als Reaktion auf auslösende Ereignisse aufgezeichnet werden, so dass die Aufsichtsbehörden die Daten überprüfen können.



Beschreibung

TECHNISCHES GEBIET

[0001] Die vorliegende Offenbarung bezieht sich allgemein auf Prozessanlagen und Prozessleitsysteme und insbesondere auf die Verwendung von Distributed Ledgers in Prozessleitsystemen zum Aufzeichnen von Daten und Ereignissen.

HINTERGRUND

[0002] Dezentrale Prozessleitsysteme, wie sie in chemischen, petrochemischen oder anderen Prozessanlagen verwendet werden, beinhalten in der Regel eine oder mehrere Prozesssteuerungen, die über analoge, digitale oder kombinierte analoge/digitale Busse oder über eine drahtlose Kommunikationsverbindung oder ein drahtloses Netzwerk kommunikativ mit einem Feldgerät oder mehreren Feldgeräten gekoppelt sind. Die Feldgeräte, die beispielsweise Ventile, Ventilstellungsregler, Schalter und Transmitter (z. B. Temperatur-, Druck-, Füllstands- und Durchflusssensoren) sein können, befinden sich innerhalb der Prozessumgebung und übernehmen im Allgemeinen physische oder prozesssteuernde Funktionen wie das Öffnen oder Schließen von Ventilen, das Messen von Prozessparametern wie beispielsweise Druck, Temperatur usw. und ähnlichem zur Steuerung eines oder mehrerer Prozesse, die in der Prozessanlage oder dem System ausgeführt werden. Intelligente Feldgeräte wie beispielsweise jene, die dem bekannten Feldbus-Protokoll entsprechen, können auch Steuerungsberechnungen, Alarmfunktionen und andere in der Steuerung üblicherweise implementierte Steuerungsfunktionen ausführen. Die Prozesssteuerungen, die in der Regel ebenfalls in der Anlagenumgebung platziert sind, empfangen Signale, die von den Feldgeräten vorgenommene Prozessmessungen und/oder andere zu den Feldgeräten gehörende Informationen anzeigen, und eine Steuerungsanwendung ausführen, die zum Beispiel unterschiedliche Steuerungsmodule laufen lässt, die Entscheidungen über die Prozesssteuerung treffen, Steuersignale auf der Grundlage der empfangenen Informationen generieren und mit den Steuerungsmodulen oder -blöcken, die in Feldgeräten wie beispielsweise HART®, WirelessHART® und FOUNDATION® Feldbus-Feldgeräten ausgeführt werden, koordinieren. Die Steuerungsmodule in der Steuerung senden die Steuersignale über die Kommunikationsleitungen oder -verbindungen zu den Feldgeräten, um dadurch den Betrieb mindestens eines Teils der Prozessanlage oder des Systems zu steuern. Wie vorliegend verwendet, werden Feldgeräte und Steuerungen im Allgemeinen als „Prozesssteuerungsgeräte“ bezeichnet.

[0003] Informationen von den Feldgeräten und der Steuerung werden in der Regel von den Steuerungen über eine Datenautobahn einem Hardwaregerät oder mehreren anderen Hardwaregeräten, wie beispielsweise Bedienerarbeitsplätzen, PCs oder Computergeräten, Data Historians, Berichtgeneratoren, zentralisierten Datenbanken oder anderen zentralisierten administrativen Computergeräten bereitgestellt, die in der Regel in Steuerungsräumen oder an anderen Orten entfernt von der raueren Anlagenumgebung platziert sind. Jedes dieser Hardware-Geräte ist in der Regel über die gesamte Prozessanlage oder einen Teil der Prozessanlage hinweg zentralisiert. Diese Hardwaregeräte führen Anwendungen aus, die es beispielsweise einem Bediener ermöglichen können, Funktionen in Bezug auf die Steuerung eines Prozesses und/oder den Betrieb der Prozessanlage auszuführen, wie z. B. das Ändern der Einstellungen der Prozesssteuerungsroutine, das Ändern des Betriebs der Steuerungsmodule innerhalb der Steuerungen oder der Feldgeräte, das Anzeigen des aktuellen Prozesszustands, das Anzeigen von Alarmen, die von Feldgeräten und Steuerungen generiert werden, das Simulieren des Betriebs des Prozesses zum Zwecke der Schulung von Personal oder das Testen der Prozesssteuerungssoftware, das Halten und Aktualisieren einer Konfigurationsdatenbank usw. Die von den Hardwaregeräten, Steuerungen und Feldgeräten verwendete Datenautobahn kann einen drahtgebundenen Kommunikationsweg, einen drahtlosen Kommunikationsweg oder eine Kombination aus drahtgebundenen und drahtlosen Kommunikationswegen beinhalten.

[0004] Als Beispiel enthält das DeltaV™-Steuerungssystem, das von Emerson Process Management vertrieben wird, mehrere Anwendungen, die in verschiedenen Geräten an verschiedenen Orten in einer Prozessanlage gespeichert und ausgeführt werden. Eine Konfigurationsanwendung, die in einem oder mehreren Arbeitsplätzen oder Computergeräten untergebracht ist, ermöglicht Benutzern das Erstellen oder Ändern von Prozesssteuerungsmodulen und das Herunterladen dieser Prozesssteuerungsmodule über eine Datenautobahn auf dedizierte dezentrale Steuerungen. In der Regel bestehen diese Steuerungsmodule aus kommunikativ miteinander verbundenen Funktionsblöcken, die Objekte in einem objektorientierten Programmierprotokoll sind, die Funktionen innerhalb des Steuerungsschemas auf der Basis von Eingaben ausführen und die Ausgaben an andere Funktionsblöcke innerhalb des Steuerungsschemas bereitstellen. Die Konfigurationsanwendung kann es einem Konfigurationskonstrukteur auch ermöglichen, Bedieneroberflächen zu erstellen oder zu ändern, die einer Anzeigeanwendung dazu dienen, einem Bediener Daten anzuzeigen und es dem Bediener ermöglichen, Einstellungen wie beispielsweise Sollwerte innerhalb der Prozesssteuerungsroutinen zu verändern. Jede dedizierte Steuerung und in einigen Fällen ein oder mehrere Feldgeräte speichern und führen eine entsprechen-

de Steuerungsanwendung aus, welche die ihr zugeordneten und heruntergeladenen Steuerungsmodule ausführt, um die eigentliche Prozesssteuerungsfunktionalität zu implementieren. Die Anzeigeanwendungen, die in einem oder mehreren Bedienerarbeitsplätzen (oder auf einem entfernten Computergerät oder mehreren entfernten Computergeräten in kommunikativer Verbindung mit den Bedienerarbeitsplätzen und der Datenautobahn) ausgeführt werden können, empfangen Daten von der Steuerungsanwendung über die Datenautobahn und zeigen diese Daten den Konstrukteuren, Bedienern oder Benutzern von Prozessleitsystemen über die Benutzeroberflächen an und können eine von mehreren verschiedenen Ansichten bereitstellen, wie beispielsweise eine Bedieneransicht, eine Ingenieursansicht, eine Technikeransicht usw. Eine Data Historian-Anwendung wird in der Regel in einem Data Historian-Gerät gespeichert und ausgeführt, das einige oder alle Daten sammelt und speichert, die über die Datenautobahn bereitgestellt werden, während eine Konfigurationsdatenbankanwendung in noch einem weiteren, an die Datenautobahn angeschlossenen Computer ausgeführt werden kann, um die aktuelle Konfiguration der Prozesssteuerungsroutine und die damit verbundenen Daten zu speichern. Alternativ kann die Konfigurationsdatenbank in demselben Arbeitsplatz wie die Konfigurationsanwendung platziert sein.

[0005] Im Allgemeinen umfasst ein Prozessleitsystem einer Prozessanlage Feldgeräte, Steuerungen, Arbeitsplätze und andere Geräte, die durch einen Satz geschichteter Netzwerke und Busse miteinander verbunden sind. Das Prozessleitsystem kann wiederum mit verschiedenen geschäftlichen und externen Netzwerken verbunden sein, um z. B. Herstellungs- und Betriebskosten zu senken, die Produktivität und Effizienz zu steigern, einen zeitnahen Zugriff auf Prozesssteuerungs- und/oder Prozessanlageninformationen zu ermöglichen usw. Zum anderen erhöht die Verbindung von Prozessanlagen und/oder Prozessleitsystemen mit Unternehmens- und/oder externen Netzwerken und Systemen das Risiko von Cyber-Eingriffen und/oder böswilligen Cyber-Angriffen, die sich aus erwarteten Sicherheitslücken in kommerziellen Systemen und Anwendungen ergeben, wie sie beispielsweise in Unternehmens- und/oder externen Netzwerken verwendet werden. Cyber-Eingriffe und böswillige Cyber-Angriffe auf Prozessanlagen, Netzwerke und/oder Steuerungssysteme können die Vertraulichkeit, Integrität und/oder Verfügbarkeit von Informationsressourcen beeinträchtigen, bei denen es sich im Allgemeinen um Schwachstellen handelt, die denen von Allzweck-Computernetzwerken ähneln. Im Gegensatz zu Allzweck-Computernetzwerken können Cyber-Eingriffe in Prozessanlagen, Netzwerke und/oder Steuerungssysteme jedoch nicht nur zur Beschädigung, Zerstörung und/oder zum Verlust von Anlagenausrüstung, Produkten und anderen physischen Gütern, sondern auch zu Todesfällen führen. Beispielsweise kann ein Cyber-Eingriff dazu führen, dass ein Prozess außer Kontrolle gerät und dadurch Explosionen, Brände, Überschwemmungen, die Exposition gegenüber gefährlichen Materialien usw. verursachen. Daher ist die Sicherung der Kommunikation in Bezug auf Prozesssteuerungsanlagen und -systeme von größter Bedeutung.

ZUSAMMENFASSUNG

[0006] Techniken, Systeme, Apparate, Komponenten, Geräte und Verfahren werden offenbart, um einen Distributed Ledger oder eine Blockchain in Prozessleitsystemen zu verwenden. Die Techniken, Apparate, Geräte, Komponenten, Geräte und Verfahren können auf industrielle Prozessleitsysteme, Umgebungen und/oder Anlagen angewendet werden, die vorliegend austauschbar als „industrielle Steuerung“, „Prozesssteuerung“ oder „Prozess“ - Systeme, Umgebungen und/oder Anlagen bezeichnet werden. In der Regel steuern solche Systeme und Anlagen auf dezentrale Weise einen oder mehrere Prozesse, mit denen physische Materialien oder Produkte hergestellt, veredelt, umgewandelt, generiert oder hergestellt werden.

[0007] Beispielsweise kann in einem Prozessleitsystem ein Distributed Ledger von Knoten verwaltet werden, die hier als „Edge-Gateways“ bezeichnet werden. Die Knoten empfangen Transaktionen, die von Feldgeräten, Steuerungen, Bedienerarbeitsplätzen oder anderen in der Prozessanlage arbeitenden Geräten an ein Distributed-Ledger-Netzwerk gesendet werden. In einigen Szenarien enthalten die Transaktionen Prozessparameterwerte für Prozessparameter, die einer Prozessanlageneinheit entsprechen. Eine Prozessanlageneinheit kann Geräte in einer Prozessanlage zur Verwendung in einem Teil des Prozesses enthalten, die physische Materialien enthalten, umwandeln, generieren oder übertragen, wie beispielsweise ein Ventil, einen Tank, einen Mischer, eine Pumpe, einen Wärmetauscher usw. Die Transaktionen können auch Produktparameterwerte umfassen, wie Eigenschaften eines von der Prozessanlage hergestellten physischen Materials oder Produkts, einschließlich einer Temperatur des Produkts, eines Volumens des Produkts, einer Masse des Produkts, einer Dichte des Produkts, einem Druck des Produkts usw.

[0008] Die aufgezeichneten Prozessparameterwerte und Produktparameterwerte können dann abgerufen werden, um die Qualität eines Produkts zu überprüfen. Beispielsweise kann eine erste Prozessanlage ein Produkt herstellen, veredeln, umwandeln, generieren oder produzieren, das dann einer zweiten Prozessanlage bereitgestellt wird. Die zweite Prozessanlage kann bestimmen, dass das Produkt bestimmte Qualitätsstandards erfüllt, indem sie die auf-

gezeichneten Prozessparameterwerte und Produktparameterwerte aus dem Distributed Ledger abruft. Darüber hinaus können regulatorische Daten im Distributed Ledger erfasst werden. Beispielsweise können als Reaktion auf ein auslösendes Ereignis wie ein Alarm, ein Fehler, ein Leck, ein Reparaturereignis, ein Prozessmeilenstein, eine Korrekturmaßnahme usw. Prozesssteuerungselemente wie Feldgeräte oder Steuerungen Transaktionen einschließlich Daten von dem auslösenden Ereignis, wie der Zeitpunkt, an dem das Ereignis stattfindet, die Dauer des Ereignisses, Prozessparameterwerte für am Ereignis beteiligte Prozessanlageneinheiten, Produktparameterwerte für am Ereignis beteiligte Produkte usw. generieren. Die regulatorischen Daten werden dann im Distributed Ledger aufgezeichnet, damit die Aufsichtsbehörden die Daten überprüfen können.

[0009] Darüber hinaus können Distributed Ledgers zum Ausführen von Smart Contracts verwendet werden, die nachstehend ausführlicher beschrieben werden. Prozessleitsysteme können Smart Contracts für den Distributed Ledger bereitstellen, um den Wert auszutauschen, z. B. nach Erhalt eines Produkts in gutem Zustand. Smart Contracts können auch für den Distributed Ledger bereitgestellt werden, damit Maschinen wie Feldgeräte ohne menschliches Eingreifen selbstständig Transaktionen durchführen können. Beispielsweise kann gemäß den Bedingungen eines Smart Contracts ein Computergerät in einer ersten Prozessanlage einem Computergerät in einer zweiten Prozessanlage automatisch einen vorbestimmten Token-Betrag bereitstellen, wenn Hinweise von einem Feldgerät oder mehreren Feldgeräten in der ersten Prozessanlage empfangen werden, dass ein Produkt aus der zweiten Prozessanlage geliefert wurde und bestimmte Qualitätsstandards erfüllt. Smart Contracts können auch in Prozessanlagen für mehrere andere Anwendungen verwendet werden, die nachstehend ausführlicher beschrieben werden.

[0010] Durch die Verwendung von Distributed Ledgers und in einigen Szenarien von Smart Contracts kann jede Prozessanlage oder ein Netzwerk von Prozessanlagen eine vertrauenswürdige, sichere und unveränderliche Aufzeichnung von Transaktionen in der Prozessanlage bereitstellen. Die Sicherheit, Unveränderlichkeit und Vertrauenswürdigkeit von Distributed Ledgers ist besonders wichtig in Prozessleitsystemen, in denen Cyber-Eingriffe nicht nur zur Beschädigung, Zerstörung und/oder zum Verlust von Anlagenausrüstung, Produkten und anderen physischen Gütern, sondern auch zu Todesfällen führen können. Darüber hinaus ermöglichen Distributed Ledgers den Prozessanlagen, die Produktlinie vom Rohmaterial bis zum fertigen Produkt zu verfolgen und die Produkte nach der Herstellung weiter zu verfolgen. Wenn konkurrierende Einheiten eine gemeinsame Ressource nutzen oder übertragen, können Distributed Ledgers verwendet werden, um die Menge der von einer der Einheiten genutzten Ressource und eine angemessene Vergütung für die Nutzung der Ressource für die konkurrierende Einheit zu bestimmen. Beispielsweise kann eine Ölraffinerie Öl produzieren, das über eine Ölleitung mehreren Unternehmen oder Prozessanlagen bereitgestellt wird. Jede Prozessanlage ist dafür verantwortlich, der Ölraffinerie die Ölmenge zu vergüten, welche die Prozessanlage von der Ölpipeline erhalten hat. Distributed Ledgers können verwendet werden, um die Ölmenge aufzuzeichnen, die jede Prozessanlage von Geräten erhält, welche die Ölmenge zum Zeitpunkt der Bereitstellung des Öls messen. Aufgrund der Schwierigkeit, die aufgezeichneten Daten in den Distributed Ledgers zu ändern, müssen konkurrierende Einheiten nicht darauf vertrauen, dass die Daten zuverlässig sind.

Figurenliste

Fig. 1 ist ein Blockdiagramm einer beispielhaften Prozessanlage oder eines beispielhaften Prozessleitsystems, das unter anderem Verbindungen zwischen verschiedenen beispielhaften Komponenten des Prozessleitsystems, dem Prozessleitsystem selbst und anderen beispielhaften Systemen und/oder Netzwerken darstellt;

Fig. 2 ist ein Blockdiagramm einer beispielhaften Sicherheitsarchitektur für eine Prozessanlage oder ein Prozessleitsystem;

Fig. 3 ist ein beispielhaftes Distributed-Ledger-System zum Aufzeichnen von Transaktionen und zum Ausführen von Smart Contracts in einem Prozessleitsystem;

Fig. 4 zeigt beispielhafte Validierungs-Netzwerkknoten und einen beispielhaften Transaktionsfluss in einem Distributed-Ledger-Netzwerk in einem Prozessleitsystem;

Fig. 5 zeigt beispielhafte Komponenten eines Netzwerkknotens in einem Distributed-Ledger-Netzwerk in einem Prozessleitsystem;

Fig. 6A zeigt einen beispielhaften Distributed Ledger, welcher eine Blockchain einschließt, die Transaktionsblöcke in einem Prozessleitsystem aufweist;

Fig. 6B zeigt ein weiteres Beispiel eines Distributed Ledgers, welches mehrere Sideblockchains oder Sidechains einschließt, die von verschiedenen Prozessanlagen verwaltet werden, und einer Hauptblockchain, die von mehreren Prozessanlagen verwaltet wird, die Transaktionsdaten von den Sidechains enthält;

Fig. 7A zeigt noch ein weiteres Beispiel eines Distributed Ledgers, der mehrere lokale Blockchains einschließt, die jeweils von einer anderen Prozessanlage verwaltet werden;

Fig. 7B zeigt eine globale Blockchain für eine Prozessanlage, die von mehreren Prozessanlagen verwaltet wird und die Blöcke aus der lokalen Blockchain enthält;

Fig. 7C zeigt eine Super-Blockchain, die von mehreren Prozessanlagen verwaltet wird und die Blöcke von jeder der globalen Blockchains für jede Prozessanlage enthält;

Fig. 8 zeigt einen beispielhaften Zustand des Smart Contracts in einem Distributed-Ledger-Netzwerk zum Ausführen sicherer Schreibvorgänge in einer Prozessanlage zum Schreiben eines Prozessparameters in eine SIS-Vorrichtung (Safety Instrumented System);

Fig. 9 zeigt eine beispielhafte Transaktion, die eine Nachweistransaktion darstellt, die von einem Nachweis-Orakel generiert wird, das ein Feldgerät ist, das die von einer Ölpipeline empfangene Ölmenge meldet;

Fig. 10 zeigt eine beispielhafte Transaktion, die eine Nachweistransaktion darstellt, die von einem Nachweis-Orakel generiert wird, bei dem es sich um ein Computergerät handelt, das eine Software- oder Firmware-Aktualisierung meldet;

Fig. 11 zeigt eine beispielhafte Transaktion, die eine Nachweistransaktion darstellt, die durch ein Nachweis-Orakel generiert wird, das eine Prozessanlageneinheit ist, die Prozessparameter- oder Produktparameterdaten meldet;

Fig. 12 zeigt ein Flussdiagramm, das ein beispielhaftes Verfahren zum Aufzeichnen von Daten in einem Prozessleitsystem unter Verwendung eines Distributed Ledgers darstellt;

Fig. 13 zeigt ein Flussdiagramm, das ein beispielhaftes Verfahren zur sicheren Messung nicht vertrauenswürdiger Daten in Prozessleitsystemen unter Verwendung eines Distributed Ledgers darstellt;

Fig. 14 zeigt ein Flussdiagramm, das ein beispielhaftes Verfahren zum Aufzeichnen von Qualitätskontroll-, Produktions- oder regulatorischen Daten in einem Prozesskontrollsystem unter Verwendung eines Distributed Ledgers darstellt;

Fig. 15 zeigt ein Flussdiagramm, das ein beispielhaftes Verfahren zum Aufzeichnen von Software- oder Firmware-Zuständen in einem Prozessleitsystem und einer verbundenen Instrumentierung unter Verwendung eines Distributed Ledgers darstellt;

Fig. 16 zeigt ein Flussdiagramm, das ein beispielhaftes Verfahren zum Erstellen von Smart Contracts in einem Prozessleitsystem unter Verwendung eines Distributed Ledgers darstellt; und

Fig. 17 zeigt ein Flussdiagramm, das ein beispielhaftes Verfahren zur Interaktion mit einem Smart Contract in einem Prozessleitsystem unter Verwendung eines Distributed Ledgers darstellt.

DETAILLIERTE BESCHREIBUNG

[0011] Ein Distributed Ledger ist ein Speichermechanismus für Daten, Ereignisse, Transaktionen usw., der von mehreren Teilnehmern verwaltet wird. Insbesondere ist ein Distributed Ledger ein Weg, um einen dezentralen Konsens bezüglich der Gültigkeit oder Ungültigkeit von Informationen zu erzielen, die im Distributed Ledger aufgezeichnet sind. Mit anderen Worten bietet der Distributed Ledger den Teilnehmern und Beobachtern eine dezentrale Vertrauensbasis. Im Gegensatz zu einer zentralen Autorität ist ein Distributed Ledger eine dezentrale Datenbank, in der von jedem Knoten eines Peer-to-Peer-Netzwerks ein Transaktionsprotokoll über Änderungen am Ledger verwaltet und validiert wird. Ein Typ eines Distributed Ledgers, eine Blockchain, besteht aus Gruppierungen von Transaktionen, die gemeinsam zu einem „Block“ zusammengefasst und nacheinander geordnet sind (daher der Begriff „Blockchain“). Während auf die hier diskutierten Distributed Ledgers im Kontext einer Blockchain Bezug genommen wird, ist dies nur ein Beispiel für einen Distributed Ledger. Distributed Ledgers können auch einen Tangle, ein Blockgitter oder einen anderen gerichteten azyklischen Graphen (DAG) enthalten. In jedem Fall können Knoten im Laufe der Zeit dem Blockchain-Netzwerk beitreten und dieses verlassen und Blöcke von Peer-Knoten erhalten, die während der Abwesenheit des Knotens weitergegeben wurden. Knoten können Adressen anderer Knoten verwalten und Adressen bekannter Knoten miteinander austauschen, um die Weitergabe neuer Informationen über das Netzwerk in einer dezentralen Peer-to-Peer-Weise zu erleichtern.

[0012] Die Knoten, die sich den Ledger teilen, bilden das, was hier als Distributed-Ledger-Netzwerk bezeichnet wird. Die Knoten im Distributed-Ledger-Netzwerk validieren Änderungen an der Blockchain (z. B. wenn eine neue Transaktion und/oder ein neuer Block erstellt wird) gemäß einem Satz von Konsensregeln. Die Konsensregeln hängen von den Informationen ab, die von der Blockchain verfolgt werden, und können Regeln für die Chain selbst enthalten. Beispielsweise kann eine Konsensregel beinhalten, dass der Urheber einer Änderung einen Identitätsnachweis vorlegt, sodass nur genehmigte Einheiten Änderungen an der Chain vornehmen können. Eine Konsensregel kann fordern, dass die Blöcke und Transaktionen Formatanforderungen einhalten und bestimmte Meta-Informationen in Bezug auf die Änderung liefern (z. B. dass Blöcke unterhalb einer Größenbeschränkung sein müssen, Transaktio-

nen eine Reihe von Feldern usw. enthalten müssen). Konsensregeln können einen Mechanismus umfassen, um die Reihenfolge zu bestimmen, in welcher neue Blöcke der Chain hinzugefügt werden (z. B. durch ein Proof-of-Work-System, einen Proof-of-Stake usw.).

[0013] Ergänzungen zur Blockchain, welche die Konsensregeln erfüllen, werden von Knoten weitergegeben, welche die Hinzufügung zu anderen Knoten validiert haben, die dem validierenden Knoten bekannt sind. Wenn alle Knoten, die eine Änderung an der Blockchain erhalten, den neuen Block validieren, spiegelt der Distributed Ledger die auf allen Knoten gespeicherte neue Änderung wider, und es kann gesagt werden, dass ein dezentraler Konsens in Bezug auf den neuen Block und die darin enthaltenen Informationen erzielt wurde. Jede Änderung, welche die Konsensregel nicht erfüllt, wird ignoriert, indem Knoten validiert werden, welche die Änderung erhalten, und die Änderung wird nicht an andere Knoten weitergegeben. Im Gegensatz zu einem herkömmlichen System, das eine zentrale Autorität verwendet, kann eine einzelne Partei den Distributed Ledger nicht einseitig ändern, es sei denn, die einzelne Partei kann dies auf eine Weise tun, die den Konsensregeln entspricht. Die Unfähigkeit, frühere Transaktionen zu ändern, führt dazu, dass Blockchains im Allgemeinen als vertrauenswürdig, sicher und unveränderlich beschrieben werden.

[0014] Die Validierungsaktivitäten von Knoten, die Konsensregeln in einem Blockchain-Netzwerk anwenden, können verschiedene Formen annehmen. In einer Implementierung kann die Blockchain als gemeinsam genutztes Arbeitsblatt betrachtet werden, das Daten, wie beispielsweise den Besitz von Vermögenswerten nachverfolgt. In einer anderen Implementierung werden die Validierungsknoten den in „Smart Contracts“ enthaltenen Code ausführen und der dezentrale Konsens wird als die Netzwerkknoten ausgedrückt, die sich auf die Ausgabe des ausgeführten Codes einigen.

[0015] Ein Smart Contract ist ein Computerprotokoll, das die automatische Ausführung und/oder Durchsetzung einer Vereinbarung zwischen verschiedenen Parteien ermöglicht. Insbesondere kann der Smart Contract ein Computercode sein, der sich an einer bestimmten Adresse in der Blockchain befindet. In einigen Fällen wird der Smart Contract möglicherweise automatisch ausgeführt, wenn ein Teilnehmer der Blockchain Geld (z. B. eine Kryptowährung wie Bitcoin, Ether oder eine andere digitale/virtuelle Währung) an die Adresse sendet, in welcher der Smart Contract gespeichert ist. Darüber hinaus können Smart Contracts einen Saldo des Betrags von Geldern verwalten, der unter ihrer Adresse gespeichert ist. In einigen Szenarien, in denen dieser Saldo Null erreicht, ist der Smart Contract möglicherweise nicht mehr betriebsbereit.

[0016] Der Smart Contract kann eine oder mehrere Auslösebedingungen enthalten, die, wenn sie erfüllt sind, einer Aktion oder mehreren Aktionen entsprechen. Bei einigen Smart Contracts kann die durchgeführte Aktion/können die durchgeführten Aktionen auf der Grundlage einer oder mehrerer Entscheidungsbedingungen bestimmt werden. In einigen Fällen können Datenströme an den Smart Contract weitergeleitet werden, so dass der Smart Contract möglicherweise erkennen kann, dass eine Auslösebedingung stattgefunden hat, und/oder er kann eine Entscheidungsbedingung analysieren.

[0017] Blockchains können auf eine public (öffentliche), dezentralisierte und permissionless (erlaubnislose) Weise bereitgestellt werden. Dies bedeutet, dass jede Partei den Distributed Ledger sehen, neue Informationen zum Ledger hinzufügen oder dem Netzwerk als validierender Knoten beitreten kann. Andere Blockchains sind private (z. B. Permissioned Ledger), welche die Daten einer Chain innerhalb einer Gruppe von Einheiten, die zur Teilnahme am Blockchain-Netzwerk autorisiert sind, geheim halten. Andere Blockchain-Implementierungen können sowohl permissioned als auch permissionless sein, wobei die Teilnehmer möglicherweise validiert werden müssen, aber nur die Informationen, welche die Teilnehmer des Netzwerks veröffentlichen möchten, werden veröffentlicht.

[0018] In einigen Implementierungen enthält ein Distributed Ledger mehrere Blockchains, wie z. B. eine Hauptblockchain, und mehrere Sidechains, die unabhängig von der Hauptblockchain arbeiten. Die Sidechains interagieren dann mit der Hauptblockchain, um einige der Transaktionsdaten von den Sidechains an die Hauptblockchain zu liefern. Auf diese Weise können die Sidechains privat sein, während die Hauptblockchain öffentlich ist oder einer größeren Anzahl von Einheiten als die Sidechains zur Verfügung steht. Nicht vertrauliche Informationen aus den Sidechains können in der Hauptblockchain geteilt werden. In einigen Implementierungen enthält ein Distributed Ledger auch mehrere Schichten oder separate Blockchains, die parallel ausgeführt werden und von denselben Validierungsknoten verwaltet werden. Einige der Transaktionsdaten aus der Blockchain für die erste Schicht können der Blockchain für die zweite Schicht bereitgestellt werden oder umgekehrt.

[0019] In einem Beispiel kann ein Distributed Ledger in einem Prozessleitsystem verwaltet werden, indem Knoten validiert werden, die hier als „Edge-Gateways“ bezeichnet werden, die Daten an entfernte Systeme wie beispielsweise andere Prozessanlagen übermitteln, welche ein öffentliches und/oder privates

Netzwerk oder mehrere öffentliche und/oder private Netzwerke wie z. B. ein privates Unternehmensnetzwerk, das Internet, ein zellularer Router, ein Backhaul-Internet oder eine andere Art von Backhaul-Verbindung verwenden. Die Edge-Gateways empfangen Transaktionen, die beispielsweise von Prozesssteuerungsgeräten wie Feldgeräten oder Steuerungen, die in der Prozessanlage arbeiten, an das Distributed-Ledger-Netzwerk gesendet werden. Andere Computergeräte wie Bedienerarbeitsplätze, Servergeräte oder andere Benutzeroberflächenvorrichtungen in der Prozessanlage können ebenfalls Transaktionen an das Distributed-Ledger-Netzwerk senden. Die Edge-Gateways validieren dann die gesendeten Transaktionen.

[0020] In einem anderen Beispiel führen die Edge-Gateways den Code aus, der in „Smart Contracts“ enthalten ist, und die Feldgeräte fungieren als „Nachweis-Orakel“, die einen Nachweis für die Qualitätskontrolle, die Einhaltung von Vorschriften, die Lieferung oder den Empfang eines Produkts und die gelieferte/empfangene Menge usw. zur Blockchain bereitstellen.

[0021] **Fig. 1** ist ein Blockdiagramm einer beispielhaften Prozessanlage **10**, in der eine oder mehrere der hierin beschriebenen neuartigen Distributed-Ledger-Technologien verwendet werden können. Die Prozessanlage **10** (die hier auch austauschbar als Prozessleitsystem **10** oder Prozesssteuerungsumgebung **10** bezeichnet wird) umfasst eine oder mehrere Prozesssteuerungen, die Signale empfangen, die Prozessmessungen anzeigen, die von Feldgeräten durchgeführt werden, und diese Informationen verarbeiten, um eine Steuerungsroutine zu implementieren und Steuersignale zu generieren, die über drahtgebundene oder drahtlose Kommunikationsverbindungen oder Netzwerke an andere Feldgeräte gesendet werden, um den Betrieb eines Prozesses in der Anlage **10** zu steuern. In der Regel führt mindestens ein Feldgerät eine physische Funktion aus (z. B. Öffnen oder Schließen eines Ventils, Erhöhen oder Verringern einer Temperatur, Vornahme einer Messung, Erfassen einer Bedingung usw.), um den Betrieb eines Prozesses zu steuern. Einige Feldgeräte kommunizieren mit Steuerungen über Ein-/Ausgabegeräte (E/A-Geräte). Prozesssteuerungen, Feldgeräte und E/A-Geräte können drahtgebunden oder drahtlos sein, und jede beliebige Anzahl und Kombination von drahtgebundenen und drahtlosen Prozesssteuerungen, Feldgeräten und E/A-Geräten kann in der Prozessanlagenumgebung oder dem System **10** enthalten sein.

[0022] Zum Beispiel zeigt **Fig. 1** eine Prozesssteuerung **11**, die über Eingabe/Ausgabe-Karten (E/A-Karten) **26** und **28** kommunikativ mit drahtgebundenen Feldgeräten **15-22** verbunden ist und die über ein drahtloses Gateway **35** und eine Prozesssteuerungsdatenautobahn oder ein Backbone **105** kommunikativ mit drahtlosen Feldgeräten **40-46** verbunden ist. Die Prozesssteuerungsdatenautobahn **105** kann eine oder mehrere drahtgebundene und/oder drahtlose Kommunikationsverbindungen enthalten und kann unter Verwendung eines beliebigen gewünschten oder geeigneten Kommunikationsprotokolls, wie z. B. eines Ethernet-Protokolls, implementiert sein. In einigen (nicht dargestellten) Konfigurationen kann die Steuerung **11** kommunikativ mit dem drahtlosen Gateway **35** unter Verwendung eines Kommunikationsnetzwerks oder mehrerer Kommunikationsnetzwerke außer dem Backbone **105** verbunden sein, wie beispielsweise durch Verwenden einer beliebigen Anzahl anderer drahtgebundener oder drahtloser Kommunikationsverbindungen, die ein oder mehrere Kommunikationsprotokolle unterstützen, z. B. Wi-Fi oder andere IEEE 802.11-konforme drahtlose lokale Netzwerkprotokolle, mobile Kommunikationsprotokolle (z. B. WiMAX, LTE oder ein anderes ITU-R-kompatibles Protokoll), das Bluetooth®-Protokoll, das HART®-Protokoll, das WirelessHART®-Protokoll, das Profibus-Protokoll, das FOUNDATION®-Feldbusprotokoll usw.

[0023] Die Steuerung **11**, die beispielsweise die von Emerson Process Management vertriebene DeltaV™-Steuerungen sein kann, kann dazu betrieben werden, einen Batch-Prozess oder einen kontinuierlichen Prozess unter Verwendung von mindestens einigen der Feldgeräte **15-22** und **40-46** zu implementieren. Die Steuerung **11** ist zusätzlich zur kommunikativen Verbindung mit der Prozesssteuerungsdatenautobahn **105** auch kommunikativ mit mindestens einigen der Feldgeräte **15-22** und **40-46** verbunden, unter Verwendung einer beliebigen gewünschten Hard- und Software, die zum Beispiel mit Standard **4-20** mA-Geräten, E/A-Karten **26**, **28** und/oder einem beliebigen intelligenten Kommunikationsprotokoll, wie beispielsweise dem FOUNDATION®-Feldbus-Protokoll, dem HART®-Protokoll, dem WirelessHART®-Protokoll etc., verknüpft ist. In **Fig. 1** sind die Steuerung **11**, die Feldgeräte **15-22** und die E/A-Karten **26**, **28** drahtgebundene Geräte und die Feldgeräte **40-46** sind drahtlose Feldgeräte. Natürlich könnten die drahtgebundenen Feldgeräte **15-22** und die drahtlosen Feldgeräte **40-46** jedem (allen) anderen gewünschten Standard(s) oder Protokollen, wie beispielsweise allen drahtgebundenen oder drahtlosen Protokollen, einschließlich allen künftig entwickelten Standards oder Protokollen, entsprechen.

[0024] Die Prozesssteuerung **11** von **Fig. 1** enthält einen Prozessor **30**, der eine oder mehrere Prozesssteuerungsroutinen **38** implementiert oder überwacht (die z. B. in einem Speicher **32** gespeichert sind). Der Prozessor **30** ist konfiguriert, um mit den Feldgeräten **15-22** und **40-46** und mit anderen mit der Steuerung **11** kommunikativ verbundenen Knoten zu kommunizieren. Zu beachten ist, dass beliebige der hier

beschriebenen Steuerungsroutinen oder Module von verschiedenen Steuerungen oder anderen Geräten implementiert oder ausgeführt werden können, wenn dies gewünscht ist. Ebenso können die hier beschriebenen Steuerungsroutinen oder Steuerungsmodule **38**, die innerhalb des Prozessleitsystems **10** zu implementieren sind, jede Form annehmen, einschließlich Software, Firmware, Hardware usw. Steuerungsroutinen können zudem in jedem beliebigen Softwareformat implementiert werden, wie beispielsweise durch objektorientierte Programmierung, Leiterlogik, sequenzielle Funktionspläne, Funktionsblockdiagramme oder durch Verwendung irgendeiner anderen Softwareprogrammiersprache oder eines Designparadigmas. Die Steuerungsroutinen **38** können in jedem gewünschten Speichertyp **32**, wie beispielsweise Arbeitsspeicher (RAM) oder Festwertspeicher (ROM) gespeichert sein. Ebenso können die Steuerroutinen **38** zum Beispiel in einem oder mehreren EPROMs, EEPROMs, anwendungsspezifischen integrierten Schaltungen (ASICs) oder anderen Hardware- oder Firmware-Elementen fest eingebaut sein. Somit kann die Steuerung **11** dafür konfiguriert sein, eine Steuerungsstrategie oder Steuerungsroutine in jeder gewünschten Weise zu implementieren.

[0025] Die Steuerung **11** implementiert eine Steuerungsstrategie unter Verwendung von dem, was üblicherweise als Funktionsblöcke bezeichnet werden, wobei jeder Funktionsblock ein Objekt oder ein anderer Teil (z. B. ein Unterprogramm) einer Gesamtsteuerungsroutine ist und in Verbindung mit anderen Funktionsblöcken (über Kommunikationen, sogenannte Links) arbeitet, um Prozesssteuerungskreise innerhalb des Prozessleitsystems **10** zu implementieren. Steuerungsbasierte Funktionsblöcke führen in der Regel eine Eingabefunktion aus, wie sie beispielsweise einem Transmitter, einem Sensor oder einer anderen Prozessparameter-Messvorrichtung, einer Steuerfunktion zugeordnet ist, beispielsweise so einer Steuerfunktion, die einer Steuerroutine zugeordnet ist, welche eine PID-, Fuzzy Logik- usw. Steuerung ausführt, oder einer Ausgabefunktion, welche den Betrieb eines beliebigen Geräts, beispielsweise eines Ventils, steuert, um eine physische Funktion innerhalb des Prozessleitsystems **10** auszuführen. Natürlich existieren auch hybride und andere Arten von Funktionsblöcken. Funktionsblöcke können durch die Steuerung **11** gespeichert und ausgeführt werden, was in der Regel der Fall ist, wenn diese Funktionsblöcke für Standard **4-20** mA-Geräte und einige Typen von intelligenten Feldgeräten, wie beispielsweise HART®-Geräten, verwendet werden oder damit verknüpft werden, oder sie können in den Feldgeräten selbst gespeichert und implementiert sein, was bei FOUNDATION®-Feldbus-Geräten der Fall sein kann. Somit kann die Steuerung **11** demnach eine oder mehrere Steuerroutinen **38** enthalten, die eine oder mehrere Regelschleifen implementieren können, die durch Ausführen eines Funktionsblocks oder mehrerer Funktionsblöcke ausgeführt werden.

[0026] Die drahtgebundenen Feldgeräte **15-22** können beliebige Arten von Geräten sein, wie beispielsweise Sensoren, Ventile, Transmitter, Stellungsregler usw., während die E/A-Karten **26** und **28** beliebige Arten von E/A-Geräten sein können, die einem beliebigen gewünschten Kommunikations- oder Steuerungsprotokoll entsprechen. In **Fig. 1** sind Feldgeräte **15-18** Standard **4-20** mA-Geräte oder HART®-Geräte, die über analoge Leitungen oder kombinierte analoge und digitale Leitungen mit der E/A-Karte **26** kommunizieren, während die Feldgeräte **19-22** intelligente Geräte wie FOUNDATION®-Feldbus-Feldgeräte sind, die über einen digitalen Bus mit der E/A-Karte **28** mittels eines FOUNDATION®-Feldbus-Kommunikationsprotokolls kommunizieren. In einigen Ausführungsformen können jedoch mindestens einige der drahtgebundenen Feldgeräte **15**, **16** und **18-21** und/oder mindestens einige der E/A-Karten **26**, **28** zusätzlich oder alternativ mit der Steuerung **11** über die Prozesssteuerungsdatenautobahn **105** und/oder über andere geeignete Steuerungssystemprotokolle (z. B. Profibus, DeviceNet, Foundation Feldbus, ControlNet, Modbus, HART usw.) kommunizieren.

[0027] In **Fig. 1** kommunizieren die drahtlosen Feldgeräte **40-46** über ein drahtloses Prozesssteuerungs-Kommunikationsnetzwerk **70** unter Verwendung eines drahtlosen Protokolls, wie dem WirelessHART®-Protokoll. Solche drahtlosen Feldgeräte **40-46** können direkt mit einem Gerät oder mehreren anderen Geräte oder Knoten des drahtlosen Netzwerks **70** kommunizieren, die ebenfalls für eine drahtlose Kommunikation (zum Beispiel unter Verwendung des drahtlosen Protokolls oder eines anderen drahtlosen Protokolls) konfiguriert sind. Um mit einem oder mehreren anderen Knoten, die nicht für die drahtlose Kommunikation konfiguriert sind zu kommunizieren, können die drahtlosen Feldgeräte **40-46** das drahtlose Gateway **35**, das mit der Prozesssteuerungsdatenautobahn **105** oder einem anderen Prozesssteuerungs-Kommunikationsnetzwerk verbunden ist, verwenden. Ein drahtloses Gateway **35** ermöglicht den Zugriff auf verschiedene drahtlose Geräte **40-58** des drahtlosen Kommunikationsnetzwerkes **70**. Insbesondere stellt das drahtlose Gateway **35** eine kommunikative Kopplung zwischen den drahtlosen Geräten **40-58**, den drahtgebundenen Geräten **15-28** und/oder anderen Knoten oder Geräten der Prozesssteuerungsanlage **10** bereit. Zum Beispiel kann das drahtlose Gateway **35** eine kommunikative Kopplung unter Verwendung der Prozesssteuerungsdatenautobahn **105** und/oder unter Verwendung eines Kommunikationsnetzwerks oder mehrerer anderer Kommunikationsnetzwerke der Prozessanlage **10** bereitstellen.

[0028] Analog zu den drahtgebundenen Feldgeräten **15-22** übernehmen die drahtlosen Feldgeräte **40-16** des drahtlosen Netzwerks **70** physische Steuerungsfunktionen in der Prozessanlage **10**, z. B. Öffnen oder Schließen von Ventilen oder Vornahme von Messungen von Prozessparametern usw. Die drahtlosen Feldgeräte **40 - 46** sind jedoch konfiguriert, um unter Verwendung des drahtlosen Protokolls des Netzwerks **70** zu kommunizieren. Als solche sind die drahtlosen Feldgeräte **40-46**, das drahtlose Gateway **35** und andere drahtlose Knoten **52-58** des drahtlosen Netzwerks **70** Erzeuger und Verbraucher drahtloser Kommunikationspakete.

[0029] In einigen Konfigurationen der Prozessanlage **10** enthält das drahtlose Netzwerk **70** auch nichtdrahtlose Geräte. So wird beispielsweise in **Fig. 1** ein Feldgerät **48** als Legacy-Gerät mit 4-20 mA und ein Feldgerät **50** als drahtgebundenes HART®-Gerät dargestellt. Zur Kommunikation innerhalb des Netzwerks **70** sind die Feldgeräte **48** und **50** über einen drahtlosen Adapter **52A**, **52B** mit dem drahtlosen Kommunikationsnetzwerk **70** verbunden. Die drahtlosen Adapter **52A**, **52B** unterstützen ein drahtloses Protokoll, wie beispielsweise WirelessHART, und können auch ein oder mehrere andere Kommunikationsprotokolle wie Foundation®-Feldbus, PROFIBUS, DeviceNet, etc. unterstützen. Darüber hinaus enthält das drahtlose Netzwerk **70** in einigen Konfigurationen einen oder mehrere Netzwerkzugangspunkte **55A**, **55B**, die separate physische Geräte in drahtgebundener Kommunikation mit dem drahtlosen Gateway **35** sein können oder die in das drahtlose Gateway **35** integriert sein können. Das drahtlose Netzwerk **70** kann auch einen oder mehrere Router **58** enthalten, um Pakete von einem drahtlosen Gerät zu einem anderen drahtlosen Gerät innerhalb des drahtlosen Kommunikationsnetzwerks **70** weiterzuleiten. In **Fig. 1** kommunizieren die drahtlosen Geräte **40-46** und **52-58** miteinander und mit dem drahtlosen Gateway **35** über drahtlose Verbindungen **60** des drahtlosen Kommunikationsnetzwerks **70** und/oder über die Prozesssteuerungsdatenautobahn **105**.

[0030] In **Fig. 1** umfasst das Prozessleitsystem **10** eine oder mehrere Bedienerarbeitsplätze oder Benutzeroberflächenvorrichtungen **8**, die kommunikativ mit der Datenautobahn **105** verbunden sind. Über die Bedienerarbeitsplätze **8** können Bediener Laufzeitvorgänge der Prozessanlage **10** sehen und überwachen sowie alle erforderlichen Diagnose-, Korrektur-, Verwaltungs- und/oder sonstigen Maßnahmen ergreifen. Zumindest einige der Bedienerarbeitsplätze **8** können sich in verschiedenen, geschützten Bereichen in oder nahe der Anlage **10** befinden; und in manchen Situationen können mindestens einige der Bedienerarbeitsplätze **8** entfernt angeordnet sein, jedoch dennoch in kommunikativer Verbindung mit der Anlage **10** stehen. Die Bedienerarbeitsplätze **8** können drahtgebundene oder drahtlose Computergeräte sein.

[0031] Das beispielhafte Prozessleitsystem **10** kann ferner eine Konfigurationsanwendung (nicht gezeigt) und eine Konfigurationsdatenbank (nicht gezeigt) enthalten, von denen jede auch kommunikativ mit der Datenautobahn **105** verbunden ist. Wie oben diskutiert, können verschiedene Instanzen der Konfigurationsanwendung (nicht gezeigt) auf einer oder mehreren Benutzeroberflächenvorrichtungen **8** ausgeführt werden, um es Benutzern zu ermöglichen, Prozesssteuerungsmodule zu erstellen oder zu ändern und diese Module auch über die Datenautobahn **105** auf die Steuerungen **11** herunterzuladen, sowie Benutzern das Erstellen oder Ändern von Bedieneroberflächen ermöglichen, über die ein Bediener Daten sehen und Dateneinstellungen innerhalb von Prozesssteuerungsroutinen ändern kann. In der Konfigurationsdatenbank (nicht gezeigt) sind die erstellten (z. B. konfigurierten) Module und/oder Bedieneroberflächen gespeichert.

[0032] In einigen Konfigurationen enthält das Prozessleitsystem **10** einen oder mehrere andere drahtlose Zugangspunkte **7a**, die mit anderen Geräten unter Verwendung von anderen drahtlosen Protokollen kommunizieren, wie beispielsweise Wi-Fi oder anderen IEEE 802.11-konformen drahtlosen lokalen Netzwerkprotokollen, mobilen Kommunikationsprotokollen, wie z. B. WiMAX (Worldwide Interoperability for Microwave Access), LTE (Long Term Evolution) oder andere ITU-R (International Telecommunication Union Radiocommunication Sector)-kompatiblen Protokollen, kurzwelligen Funkkommunikationen, wie z. B. NFC (Near Field Communications) und Bluetooth, oder anderen drahtlosen Kommunikationsprotokollen. In der Regel ermöglichen solche drahtlosen Zugangspunkte **7a** die Kommunikation von Handheld- oder anderen tragbaren Computergeräten über ein entsprechendes drahtloses Prozesssteuerungskommunikationsnetzwerk, das sich vom drahtlosen Netzwerk **70** unterscheidet und ein anderes drahtloses Protokoll als das drahtlose Netzwerk **70** unterstützt. Beispielsweise kann eine drahtlose oder tragbare Benutzeroberflächenvorrichtung **8** ein mobiler Arbeitsplatz oder ein Diagnosetestgerät sein, das von einem Bediener in der Prozessanlage **10** verwendet wird. In einigen Szenarien kommunizieren neben tragbaren Computergeräten auch ein Prozesssteuerungsgerät oder mehrere Prozesssteuerungsgeräte (z. B. Steuerung **11**, Feldgeräte **15-22**, oder drahtlose Geräte **35**, **40-58**) unter Verwendung des von den Zugangspunkten **7a** unterstützten drahtlosen Protokolls.

[0033] In einigen Konfigurationen umfasst das Prozessleitsystem **10** ein Gateway oder mehrere Gateways **7b**, **7c** für Systeme, die sich außerhalb des unmittelbaren Prozessleitsystems **10** befinden (hierin auch als „Edge-Gateway“ bezeichnet und nachstehend ausführlicher beschrieben). In der Regel sind solche Systeme Kunden oder Lieferanten von Informationen, die vom Prozessleitsystem **10** gene-

riert oder verarbeitet werden. Zum Beispiel kann die Prozesssteuerungsanlage **10** einen Gateway-Knoten **7b** enthalten, um die unmittelbare Prozessanlage **10** kommunikativ mit einer anderen Prozessanlage zu verbinden. Zusätzlich oder alternativ kann die Prozesssteuerungsanlage **10** einen Gateway-Knoten **7c** enthalten, um die unmittelbare Prozessanlage **10** mit einem externen öffentlichen oder privaten System zu verbinden, wie z. B. einem Laborsystem (z. B. Laborinformations-Managementsystem oder LIMS), einer Operator-Rounds-Datenbank, einem Materialflusssystem, einem Verwaltungsmanagementsystem, einem Produktbestandssteuerungssystem, einem Produktionsplanungssystem, einem Witterungsdatensystem, einem Versand- und Handhabungssystem, einem Verpackungssystem, dem Internet, einem Prozessleitsystem eines anderen Lieferanten oder anderen externen Systemen.

[0034] Es wird darauf hingewiesen, dass, obwohl **Fig. 1** nur eine einzelne Steuerung **11** mit einer endlichen Anzahl von Feldgeräten **15-22** und **40-46**, drahtlosen Gateways **35**, drahtlosen Adaptern **52**, Zugangspunkten **55**, Routern **58** und drahtlosen Prozesssteuerungskommunikationsnetzwerken **70**, die in der Beispiel-Prozessanlage **10** enthalten sind, zeigt, dieses Beispiel jedoch nur eine veranschaulichende und nichteinschränkende Ausführungsform ist. Jede beliebige Anzahl von Steuerungen **11** kann in die Prozesssteuerungsanlage oder das System **10** einbezogen werden, und jede der Steuerungen **11** kann mit einer beliebigen Anzahl von drahtgebundenen oder drahtlosen Geräten und Netzwerken **15-22**, **40-46**, **35**, **52**, **55**, **58** und **70** kommunizieren, um einen Prozess in der Anlage **10** zu steuern.

[0035] Ferner wird darauf hingewiesen, dass das Prozessanlagen- bzw. - Steuerungssystem 10 der **Fig. 1** eine Feldumgebung (z. B. „die Prozessanlagenhalle“) und eine Back-End-Umgebung (z. B. einen Server **12**) enthält, die über die Datenautobahn **105** kommunikativ verbunden sind. Wie in **Fig. 1** gezeigt, enthält die Feldumgebung physische Komponenten (z. B. Prozesssteuerungsgeräte, Netzwerke, Netzwerkelemente usw.), die zur Steuerung des Prozesses während der Laufzeit angeordnet, installiert und darin miteinander verbunden sind. Zum Beispiel sind die Steuerung **11**, die E/A-Karten **26**, **28**, die Feldgeräte **15-22** und weitere Geräte und Netzwerkkomponenten **40-46**, **35**, **52**, **55**, **58** und **70** in der Feldumgebung der Prozessanlage **10** platziert, angeordnet oder anderweitig in diese eingeschlossen. Allgemein gesprochen, werden in der Feldumgebung der Prozessanlage **10** Rohstoffe empfangen und mit den darin angeordneten physischen Komponenten verarbeitet, um ein oder mehrere Produkte zu generieren.

[0036] Die Back-End-Umgebung der Prozessanlage **10** enthält verschiedene Komponenten, wie z. B. Server Computergeräte **12**, Bedienerarbeitsplätze **8**, Datenbasen oder Datenbanken usw., die von den rauen Bedingungen und Materialien der Feldumgebung abgeschirmt und/oder vor diesen geschützt werden. Bezugnehmend auf **Fig. 1** umfasst die Back-End-Umgebung zum Beispiel die Bedienerarbeitsplätze **8**, die Server Computergeräte **12** und/oder Funktionen, welche die Laufzeitoperationen der Prozessanlage **10** unterstützen. In einigen Konfigurationen können sich verschiedene in der Back-End-Umgebung der Prozessanlage **10** enthaltene Computergeräte, Datenbanken und andere Komponenten und Ausrüstungen an verschiedenen physischen Standorten befinden, von denen einige lokal in der Prozessanlage **10** und andere entfernt angeordnet sein können.

[0037] **Fig. 2** enthält ein Blockdiagramm einer beispielhaften Sicherheitsarchitektur **200** für die Prozessanlage **10**. Wie in **Fig. 2** gezeigt, sind ein Gerät oder mehrere Geräte **202** kommunikativ mit einem oder mehreren drahtlosen Gateways **205A**, **205B** verbunden, bei denen es sich beispielsweise um Instanzen des drahtlosen Gateways **35** von **Fig. 1** handeln kann. Die Kommunikationsverbindungen zwischen den Gateways **205A**, **205B** und den Geräten **202** sind mit den Bezugszeichen **204A**, **204B** bezeichnet.

[0038] Der Satz von Geräten **202** ist so dargestellt, dass er eine endliche Anzahl von drahtlosen Feldgeräten umfasst. Es versteht sich jedoch, dass die hierin in Bezug auf die Geräte **202** beschriebenen Konzepte und Merkmale leicht auf eine beliebige Anzahl von Feldgeräten der Prozessanlage **10** sowie auf beliebige Arten von Feldgeräten angewendet werden können. Beispielsweise können die Feldgeräte **202** ein drahtgebundenes Feldgerät oder mehrere drahtgebundene Feldgeräte **15-22** enthalten, die über ein oder mehrere drahtgebundene Kommunikationsnetzwerke der Prozessanlage **10** und/oder die Feldgeräte **202** mit den drahtlosen Gateways **205A**, **205B** kommunikativ verbunden sind drahtgebundene Feldgeräte **48**, **50** umfassen, die mit drahtlosen Adaptern **52A**, **52B** gekoppelt sind.

[0039] Ferner versteht es sich, dass der Satz von Geräten **202** nicht nur auf Feldgeräte beschränkt ist, sondern zusätzlich oder alternativ jedes Gerät oder jede Komponente in der Prozessanlage **10** enthalten kann, die Daten als Ergebnis davon generiert, dass die Prozessanlage **10** den Online-Prozess steuert. Beispielsweise kann der Satz von Geräten **202** ein Diagnosegerät oder eine Komponente, die Diagnosedaten generiert, ein Netzwerkroutinggerät oder eine Netzwerkroutingkomponente, die Informationen zwischen verschiedenen Komponenten der Prozessanlage **10** übermittelt, und dergleichen enthalten. In der Tat kann jede der in **Fig. 1** gezeigten Komponenten (z. B. Komponenten **7a-7c**, **8**, **11**, **12**, **15-22**, **26**, **28**, **35**, **40-46**, **52**, **55**, **58**, **60** und **70**) und andere Kom-

ponenten, die nicht gezeigt sind, ein Gerät sein, das Daten zur Lieferung an das entfernte System **210** generiert. Als solches wird der Satz von Geräten **202** hier austauschbar als „Datenquellen 202“ oder „Datenquellengeräte 202“ bezeichnet.

[0040] **Fig. 2** zeigt ferner einen Satz von entfernten Anwendungen oder Diensten **208**, die für die Prozessanlage **10** und/oder die Prozessanlage **10** verwendet werden können. Der Satz von entfernten Anwendungen oder Diensten **208** kann auf einem oder mehreren entfernten Systemen **210** ausgeführt oder gehostet werden. Zumindest einige der Anwendungen oder Dienste **208** arbeiten in Echtzeit mit Echtzeitdaten, da die Echtzeitdaten von der Prozessanlage **10** generiert und von den Anwendungen oder Diensten **208** empfangen werden. Andere Anwendungen oder Dienste **208** können mit von Prozessanlagen generierten Daten mit weniger strengen Zeitsteuerungsanforderungen arbeiten oder diese ausführen. Beispiele von Anwendungen/Diensten **208**, die auf dem entfernten System **210** ausgeführt oder gehostet werden können und die Verbraucher von Daten sind, die von der Prozessanlage **10** generiert werden, umfassen Anwendungen, die Bedingungen und/oder Ereignisse überwachen und/oder erfassen, die in der Prozessanlage **10** stattfinden, und Anwendungen oder Dienste, die zumindest einen Teil des Online-Prozesses selbst überwachen, während dieser in der Prozessanlage **10** ausgeführt wird. Andere Beispiele von Anwendungen/Diensten **208** umfassen beschreibende und/oder vorschreibende Analysen, die mit Daten arbeiten können, die von der Prozessanlage **10** generiert wurden, und in einigen Fällen auch mit Wissen arbeiten können, das aus der Analyse der von der Prozessanlage generierten Daten gewonnen oder entdeckt wurde, wie bei Daten, die von anderen Prozessanlagen generiert und von diesen empfangen werden. Noch andere Beispiele von Anwendungen/Diensten **208** umfassen eine oder mehrere Routinen, die vorgeschriebene Funktionen und/oder Änderungen implementieren, die z. B. als Ergebnis eines anderen Dienstes oder einer anderen Anwendung zurück in die Prozessanlage **10** implementiert werden sollen. Andere Beispiele von Anwendungen und Diensten **208** basieren auf Kenntnissen, die aus der Analyse von historischen Daten, die von der Prozessanlage und/oder anderen Prozessanlagen generiert wurden, oder aus dem Vergleich von Daten für eine Prozessanlageneinheit mit Daten für Prozessanlageneinheiten desselben oder eines ähnlichen Typs gewonnen wurden.

[0041] Das eine oder die mehreren entfernten Systeme **210** können auf jede gewünschte Art und Weise implementiert werden, beispielsweise durch eine entfernte Bank von Netzwerkservern, ein oder mehrere Cloud-Computing-Systeme, ein Netzwerk oder mehrere Netzwerke usw. Zur Vereinfachung der Diskussion wird das eine entfernte System **210** oder werden die mehreren entfernten Systeme **210** hier unter Verwendung der Singularform bezeichnet, d. h. „Fernsystem **210**“, obwohl klar ist, dass sich der Begriff auf ein System, mehr als ein System oder eine beliebige Anzahl von Systemen beziehen kann. In einigen Szenarien kann das Computergerät **250**, welches Prozessanlagendaten analysiert, in dem entfernten System **210** enthalten sein.

[0042] Im Allgemeinen bietet die Sicherheitsarchitektur **200** eine durchgehende Sicherheit von der Feldumgebung der Prozessanlage **10**, in der Geräte **202** installiert sind und betrieben werden, bis zu dem entfernten System **210**, welches Anwendungen und/oder Dienste **208** bereitstellt, welche die von der Prozessanlage **10** generierten Daten verbrauchen und mit diesen Daten arbeiten. Somit können Daten, die von den Geräte **202** und anderen Komponenten der Prozessanlage **10** generiert werden, zur Verwendung durch die entfernten Anwendungen/Dienste **208** sicher zu dem entfernten System **210** transportiert werden, während die Anlage **10** vor Cyber-Angriffen, Cyber-Eingriffen und/oder anderen schädlichen Ereignissen geschützt wird. Insbesondere umfasst die Sicherheitsarchitektur **200** ein Feld-Gateway **212** und ein Edge-Gateway **218**, die zwischen der Prozessanlage **10** (z. B. zwischen den drahtlosen Gateways **205A**, **205B** der Prozessanlage **10**) und dem entfernten System **210** angeordnet sind.

[0043] Daten, die aus der Prozessanlage **10** austreten und vom Eingangsport **220** zum Ausgangsport **222** übermittelt werden, können ferner durch Verschlüsselung gesichert werden. In einem Beispiel verschlüsselt das Feld-Gateway **212** Daten und liefert verschlüsselte Daten an den Eingangsport **220**. Der Datenverkehr, der verschlüsselt und transportiert wird, kann in einem Beispiel UDP-Datenverkehr (User Datagram Protocol) und in einem anderen Beispiel JSON-Datenverkehr oder ein anderes Allzweck-Kommunikationsformat sein.

[0044] Das Feld-Gateway **212** ist kommunikativ mit der Prozesssteuerungsanlage **10** verbunden. Wie in **Fig. 2** gezeigt, ist das Feld-Gateway **212** kommunikativ mit den drahtlosen Gateways **205A**, **205B** verbunden, die in der Feldumgebung der Prozessanlage **10** angeordnet sind und die kommunikativ mit einem Gerät oder mehreren Geräten oder Datenquellen **202** verbunden sind. Wie zuvor besprochen, können die Geräte oder Datenquellen **202** und die drahtlosen Gateways **205A**, **205B** unter Verwendung des industriellen WirelessHART-Protokolls oder eines anderen geeigneten drahtlosen Protokolls kommunizieren, das so aufgebaut ist, dass es eine gesicherte Kommunikation über einen oder mehrere Sicherheitsmechanismen bereitstellt. Beispielsweise stellt das industrielle WirelessHART-Protokoll eine 128-Bit-AES-Verschlüsselung bereit, und die Kommuni-

kationspfade **204A**, **204B** können entsprechend gesichert werden.

[0045] Zusätzlich wird die Kommunikationsverbindung **225** zwischen den drahtlosen Gateways **205A**, **205B** und dem Feld-Gateway **212** jeweils unter Verwendung des gleichen oder eines anderen Sicherheitsmechanismus, wie er für die Kommunikationsverbindungen **204A**, **204B** verwendet wird, gesichert. In einem Beispiel ist die Kommunikationsverbindung **225** durch einen TLS- (Transport Layer Security) -Wrapper gesichert. Beispielsweise generieren die drahtlosen Gateways **205A**, **205B** Pakete im HART-IP-Format, die durch einen TLS-Wrapper für die Übertragung zum Feld-Gateway **212** gesichert sind.

[0046] Somit können, wie oben beschrieben, in einer Ausführungsform Daten oder Pakete, die von den Geräten **202** generiert wurden, für den Transit **204A**, **204B** zu den drahtlosen Gateways **205A**, **205B** unter Verwendung eines ersten Sicherheitsmechanismus gesichert werden und anschließend für den Transit **225** von den drahtlosen Gateways **205A**, **205B** zu dem Feld-Gateway **212** gesichert werden, wobei ein zweiter Sicherheitsmechanismus verwendet wird, und anschließend für den Transit an den Edge-Gateway **218** gesichert werden, wobei ein dritter Sicherheitsmechanismus verwendet wird. Zusätzlich oder alternativ und wie in **Fig. 2** kann das Edge-Gateway **218** durch eine Firewall **228** geschützt sein.

[0047] Daten, die vom Edge-Gateway **218** zum entfernten System **210** übertragen werden, können unter Verwendung eines öffentlichen und/oder privaten Netzwerkes oder mehrerer öffentlicher und/oder privater Netzwerke wie eines privaten Unternehmensnetzwerks, des Internets, eines zellularen Routers, eines Backhaul-Internets oder einer Backhaul-Verbindung eines anderen Typs übermittelt werden. Bezeichnenderweise werden die Daten, die vom Edge-Gateway **218** zum entfernten System **210** übertragen werden, unter Verwendung eines vierten Sicherheitsmechanismus oder unter Verwendung eines der oben diskutierten Sicherheitsmechanismen gesichert. **Fig. 2** zeigt den vom Edge-Gateway **218** an das entfernte System **210** gelieferten Datenverkehr als über ein SAS- (Shared Access Signature) -Token gesichert an, das über einen Token-Dienst **230** verwaltet werden kann, der am entfernten System **210** bereitgestellt wird. Das Edge-Gateway **218** authentifiziert sich gegenüber dem Token-Dienst **230** und fordert ein SAS-Token an, das nur für einen begrenzten Zeitraum gültig sein kann, z. B. zwei Minuten, fünf Minuten, dreißig Minuten, nicht mehr als eine Stunde usw. Das Edge-Gateway **218** empfängt und verwendet das SAS-Token, um eine AMQP- (Advanced Message Queuing Protocol)-Verbindung zum entfernten System **210** zu sichern und zu authentifizieren, über welche Inhaltsdaten vom Edge-Gateway **218** zum entfernten System **210** übermittelt werden.

[0048] In dem entfernten System **210** wird Sicherheit über einen Domänenauthentifizierungsdienst **232** bereitgestellt. Somit können nur Benutzeroberflächenvorrichtungen **235**, die über den Domänenauthentifizierungsdienst **232** authentifiziert und autorisiert sind, auf mindestens einige der Daten zugreifen, die auf dem fernen System **210** verfügbar sind, zu denen unter anderem die von den Geräten **202** generierten Daten gehören.

[0049] Somit stellt die Sicherheitsarchitektur **200**, wie oben beschrieben, eine Ende-zu-Ende-Sicherheit für Daten bereit, die von Geräten oder Datenquellen **202** generiert werden, während sie in der Prozessanlage **10** arbeiten, um einen Prozess zu steuern, z. B. von der Aufnahme der Daten durch die Datenquellen **202** bis zu deren Übertragung an das entfernte System **210**, um von einer oder mehreren entfernten Anwendungen oder Diensten **208** bearbeitet zu werden. Es ist wichtig, dass die Sicherheitsarchitektur **200** diese Ende-zu-Ende-Sicherheit bereitstellt, während verhindert wird, dass böswillige Angriffe auf die Prozessanlage **10** auftreten.

[0050] Es wird angemerkt, dass, obwohl **Fig. 2** drahtlose Gateways **205A**, **205B** zeigt, welche die Geräte oder Datenquellen **202** kommunikativ mit dem Feld-Gateway **212** verbinden, wobei in einigen Anordnungen eines oder mehrere der drahtlosen Gateways **205A**, **205B** weggelassen werden und Quelldaten von den Datenquellen **202** direkt an das Feld-Gateway **212** übermittelt werden. Beispielsweise können die Datenquellen **202** Quelldaten über ein Big-Data-Netzwerk der Prozessanlage **10** direkt an das Feld-Gateway **212** übermitteln. Im Allgemeinen ist ein Big-Data-Netzwerk der Prozessanlage **10** weder das Backbone-Anlagennetzwerk **105** noch das Big-Data-Netzwerk ein industrielles Protokollnetzwerk, das zur Übermittlung von Steuersignalen zwischen Geräten unter Verwendung eines industriellen Kommunikationsprotokolls (z. B. Profibus, DeviceNet, Foundation Feldbus, ControlNet, Modbus, HART usw.) verwendet wird. Vielmehr kann ein Big-Data-Netzwerk der Prozessanlage **10** ein für die Prozessanlage **10** implementiertes Overlay-Netzwerk sein, das beispielsweise Daten für Datenverarbeitungs- und Analysezwecke zwischen Knoten überträgt. Die Knoten eines Big-Data-Netzwerks können beispielsweise die Datenquellen **202**, die drahtlosen Gateways **205A**, **205B** und das Feld-Gateway **212** sowie eine oder mehrere der Komponenten **7a-7c**, **8**, **11**, **12**, **15-22**, **26**, **28**, **35**, **40-46**, **52**, **55**, **58**, **60** und **70**, die in **Fig. 1** gezeigt sind und andere Komponenten umfassen. Dementsprechend umfassen viele Knoten eines Prozessanlagendatennetzwerks jeweils eine festgelegte Schnittstelle für Prozessanlagenvorgänge, die in der Regel ein industrielles Kommunikationsprotokoll verwendet, und eine andere festgelegte Schnittstelle für Datenvcrarbeitungs-/Analysevorgänge, die beispielsweise ein Streaming-Protokoll verwenden kann.

[0051] Es wird ferner mit Bezug auf **Fig. 2** angemerkt, dass in einigen Ausführungsformen ein drahtgebundenes Gateway (nicht gezeigt) anstelle eines der drahtlosen Gateways **205A**, **205B** verwendet werden kann. Weiterhin können das Feld-Gateway **212** und das Edge-Gateway **218** physisch nebeneinander angeordnet sein, wie dies durch den in **Fig. 2** gezeigten Kasten **235** angegeben ist oder die Komponenten **212** und **218** können sich physisch über mehrere Standorte verteilt befinden. Beispielsweise kann ein Feld-Gateway **212** oder mehrere Feld-Gateways **212** oder das Edge-Gateway **218** in der Prozessanlage **10** angeordnet sein. Zusätzlich oder alternativ können ein Feld-Gateway **212** oder mehrere Feld-Gateways **212** oder das Edge-Gateway **218** entfernt von der Prozessanlage **10** angeordnet sein.

[0052] Die Prozessanlage **10** kann, falls gewünscht, von mehr als einem Feld-Gateway **212** bedient werden, und eine beliebige Anzahl von Feld-Gateways **210** kann von einem einzelnen Edge-Gateway **218** bedient werden. In einigen Ausführungsformen wird das entfernte System **210**, falls gewünscht, von mehr als einem Edge-Gateway **218** bedient.

[0053] Während sich das obige Beispiel auf das Computergerät **250** zum Analysieren von Prozessanlagendaten als eine Komponente des entfernten Systems **210** bezieht, kann das Computergerät **250** Prozessanlagendaten durch Kommunikation mit einer beliebigen geeigneten Kommunikationskomponente auf sichere Weise empfangen. Beispielsweise kann das Computergerät **250** kommunikativ mit den drahtlosen Gateways **205A**, **205B**, dem Feld-Gateway **212** oder dem Edge-Gateway **218** verbunden sein. Die Kommunikationspfade können von den Geräten **202** zu dem Computergerät **250** über Verschlüsselungstechniken, Firewalls, eine Datendiode oder mit einem anderen geeigneten Sicherheitsmechanismus gesichert werden.

[0054] Sobald die Prozessanlagendaten an dem Computergerät **250** empfangen wurden, analysiert das Computergerät die Prozessanlagendaten, um Bedingungen in entsprechenden Prozessanlageneinheiten zu identifizieren. Hinweise auf die Bedingungen werden dann beispielsweise über einen Domänenauthentifizierungsdienst an die Benutzeroberflächenvorrichtung **235** übermitteln. Auf diese Weise kann ein Bediener die Bedingungen sehen, die an verschiedenen Prozessanlageneinheiten in der Prozessanlage stattfinden. Der Bediener kann dann die geeigneten Maßnahmen ergreifen, um durch diese Bedingungen verursachte Probleme zu lösen.

Distributed-Ledger-Architektur
in einem Prozessleitsystem

[0055] Während in **Fig. 2** gezeigt wird, dass die Prozessanlage **10** einen einzelnen Edge-Gateway **218** einschließt, kann die Prozessanlage **10** mehrere Edge-Gateways enthalten, die jeweils als Validierungsknoten in einem Distributed-Ledger-Netzwerk fungieren. **Fig. 3** zeigt ein beispielhaftes Distributed-Ledger-System **300** zum Aufzeichnen von Prozessanlagendaten. Prozessanlagendaten können Prozessparameterdaten, Produktparameterdaten, Konfigurationsdaten, Benutzerinteraktionsdaten, Verwaltungsdaten, Inbetriebnahmedaten, Anlagennetzdaten, Produktverfolgungsdaten, Ereignisdaten in Bezug auf Ereignisse in der Prozessanlage **10** wie Warnungen, Lecks, Ausfälle, Fehler usw. oder andere geeignete Daten sein, die in einer oder mehreren Prozessanlagen generiert wurden oder sich auf diese beziehen.

[0056] Das System **300** enthält ein Distributed Ledger **312** und mehrere Knoten **302**, **304**, **306**, **308** und **310**, die Edge-Gateways in der Prozessanlage **10** sein können, wie das Edge-Gateway **218**, sie können Feldgeräte sein oder können beliebige geeignete Computergeräte sein, die in der Prozessanlage **10** oder anderen Prozessanlagen betrieben werden. Jeder Knoten verwaltet eine Kopie des Distributed Ledgers **312**. Wenn Änderungen an dem Distributed Ledger **312** vorgenommen werden, empfängt jeder Knoten die Änderung über das Netzwerk **314** und aktualisiert seine jeweilige Kopie des Distributed Ledgers **312**. Ein Konsensmechanismus kann von den Knoten **302-310** in dem Distributed-Ledger-System **300** verwendet werden, um zu entscheiden, ob es angebracht ist, empfangene Änderungen an dem Distributed Ledger **312** vorzunehmen.

[0057] Jeder Knoten im System hat daher eine eigene Kopie des Distributed Ledgers **312**, die mit jeder anderen Kopie des Distributed Ledgers **312** identisch ist, die von den anderen Knoten gespeichert wird. Das Distributed-Ledger-System **300** kann aufgrund der Dezentralität des Distributed Ledgers robuster sein als ein Datenbanksystem einer zentralen Autorität. Als solches gibt es auf dem Distributed-Ledger-System **300** keine einzelne Fehlerstelle, wie dies in einem zentralisierten System der Fall wäre.

[0058] **Fig. 4** zeigt beispielhafte Validierungs-Netzwerkknoten und einen beispielhaften Transaktionsfluss **400** in einem Distributed-Ledger-Netzwerk zum Auflösen von Transaktionen. **Fig. 4** umfasst zwei Zeitrahmen **420** und **422**, welche durch die linke und rechte Seite der gepunkteten Linie, jeweils Knoten A **402** und Knoten B **404** (die zwei Edge-Gateways in einer Prozessanlage **10** sein können, zwei Edge-Gateways in zwei verschiedenen Prozessanlagen, zwei Feldgeräte in derselben Prozessanlage oder in verschiedenen Prozessanlagen usw. sein können), eine Gruppe von Transaktionen **408A-408D**, eine Gruppe von Blöcken von Transaktionen **409A-409D**, einen Distributed Ledger **410** und eine Blockchain **418**.

[0059] Der Blockverbreitungsfluss **400** kann mit dem Knoten A **402** beginnen, der die Transaktion **406** zum Zeitpunkt **420** empfängt. Wenn der Knoten A **402** bestätigt, dass die Transaktion **406** gültig ist, kann der Knoten A **402** die Transaktion einem neu generierten Block **408** hinzufügen. Als Teil des Hinzufügens der Transaktion **406** zu Block **408** kann der Knoten A **402** ein kryptographisches Puzzle lösen und die Lösung in den neu generierten Block **408** als Nachweis für die zum Generieren des Blocks **408** geleistete Arbeit aufnehmen. Alternativ kann ein Proof-of-Stake-Algorithmus verwendet werden, um den Block **408** zu generieren, wobei der Knoten A **402** eine Menge eines im Netzwerk verwendeten digitalen Tokens „staket“, das Netzwerk jedoch selbst den Knoten bestimmt, der den neuen Block prägt. In anderen Ausführungsformen kann die Transaktion **406** zu einem Pool von Transaktionen hinzugefügt werden, bis eine ausreichende Anzahl von Transaktionen in dem Pool existiert, um einen Block zu bilden. Der Knoten A **402** kann den neu generierten Block **408** zum Zeitpunkt **412** an das Netzwerk übermitteln. Vor oder nach der Weitergabe des Blocks **408** kann der Knoten A **402** den Block **408** zu seiner Kopie der Blockchain **418** hinzufügen.

[0060] Während der Proof-of-Work und der Proof-of-Stake hierin als Konsensalgorithmen zum Auswählen eines Knotens zum Prägen eines neuen Blocks beschrieben sind, sind diese lediglich einige beispielhafte Konsensalgorithmen und sollen nicht einschränkend sein. Zusätzliche Konsensalgorithmen können verwendet werden, wie beispielsweise ein delegierter Proof-of-Stake, bei dem Knoten eine Teilmenge von Knoten auswählen, die als Delegierte bezeichnet werden, um eine Validierung durchzuführen, und die Delegierten abwechselnd neue Blöcke prägen. Konsensalgorithmen können auch den Proof-of-Authority, den Proof-of-Weight, die byzantinische Fehlertoleranz, die Konsensalgorithmen für den Tangle, das Blockgitter usw. einschließen.

[0061] In jedem Fall können die Transaktionen **409A-409D** Aktualisierungen einer Zustandsdatenbank **416** enthalten. Die Zustandsdatenbank **416** kann aktuelle Werte von Variablen enthalten, die durch in der Blockchain **418** bereitgestellte Smart Contracts erstellt wurden. Validierte Blöcke, wie beispielsweise der Block **408**, können Transaktionen enthalten, die Zustandsvariablen in der Zustandsdatenbank **416** bewirken. Zum Zeitpunkt **422** kann der Knoten B **404** den neu erstellten Block **408** über das Netzwerk bei **412** empfangen. Der Knoten B **404** kann überprüfen, ob der Transaktionsblock **408** gültig ist, indem die Lösung des im Block **408** bereitgestellten kryptographischen Puzzles überprüft wird. Wenn die Lösung genau ist, kann der Knoten B **404** den Block **408** zu seiner Blockchain **418** hinzufügen und Aktualisierungen an der Zustandsdatenbank **416** vornehmen, wie sie von den Transaktionen in Block **408** abgelehnt wurden. Der Knoten B **404** kann dann den Block **408** zum Zeitpunkt **314** an den Rest des Netzwerks übermitteln.

[0062] **Fig. 5** zeigt beispielhafte Komponenten eines Validierungs-Netzwerkknotens **500** in einem Distributed-Ledger-Netzwerk zum Aufzeichnen von Prozessanlagendaten. Der Knoten **500** kann mindestens einen Prozessor **502**, einen Speicher **504**, ein Kommunikationsmodul **506**, einen Satz von Anwendungen **508**, externe Ports **510**, einen Blockchain-Manager **514**, Smart Contracts **516** und ein Betriebssystem **518** enthalten. In einigen Ausführungsformen kann der Knoten **500** einen neuen Transaktionsblock generieren oder Transaktionen unter Verwendung des Blockchain-Managers **514** an andere Netzwerkknoten senden. In ähnlicher Weise kann der Knoten **500** den Blockchain-Manager **514** in Verbindung mit den in dem Speicher **504** gespeicherten Smart Contracts **516** verwenden, um die hier offenbarte Funktionalität auszuführen. Der Speicher **504** kann ferner Kettendaten **524** enthalten, die beispielsweise eine Zustandsdatenbank der Blockchain zum Speichern von Zuständen von darauf bereitgestellten Smart Contracts enthalten.

[0063] In anderen Ausführungsformen arbeiten die Smart Contracts **516** unabhängig von dem Blockchain-Manager **514** oder anderen Anwendungen. In einigen Ausführungsformen verfügt der Knoten **500** nicht über einen Blockchain-Manager **514** oder Smart Contracts **516**, die auf dem Knoten gespeichert sind. In einigen Ausführungsformen kann der Knoten **500** zusätzliche oder weniger Komponenten als beschrieben aufweisen. Die Komponenten des Knotens **500** werden nachstehend ausführlicher beschrieben.

[0064] Der Knoten **500** kann als Teil eines dezentralen Ledger-Systems **300** oder eines anderen dezentralen oder zentralen Netzwerks als Teil von Systemen verwendet werden, die mit Transaktionen interagieren und/oder diese manipulieren, welche Daten oder Ereignissen zugeordnet sind, die in einer oder mehreren Prozessanlagen stattfinden.

[0065] **Fig. 6A** zeigt ein beispielhaftes Distributed Ledger **600** einschließend einer Blockchain, welche die Blöcke **602-608** von Transaktionen in einem Prozessleitsystem aufweist. In einigen Ausführungsformen enthält die Blockchain **600** mehrere Blöcke **602-608**, die miteinander verbunden sind, um eine Chain von Blöcken **602-608** von Transaktionen zu bilden. Um Blöcke und Transaktionen kryptographisch miteinander zu verbinden, organisiert jeder Block in der Blockchain **600** seine Transaktionen in einem Merkle-Tree. In einem Merkle-Tree wird jede Transaktion gemäß einem kryptographischen Hashing-Algorithmus (z. B. SHA-256) gehasht, und der resultierende Ausgabe-Hash wird dann mit dem Hash einer anderen Transaktion kombiniert. Dann wird

das kombinierte Ergebnis auch gemäß dem kryptographischenkryptographischen Hashing-Algorithmus gehasht. Diese Ausgabe wird dann mit dem Hash von zwei anderen Transaktionen kombiniert und dieser Prozess wird wiederholt, bis alle Transaktionen in dem Block kombiniert und gehasht wurden, um eine Merkle-Wurzel zu generieren, die in dem Header für einen Block **602-608** verwendet wird. Wenn eine einzelne Transaktion in dem Block manipuliert wird, wird eine andere Merkle-Wurzel generiert, da die Merkle-Wurzel eine Kombination der Hashes aller Transaktionen in dem Block ist.

[0066] Mit anderen Worten können die Transaktionen unter Verwendung eines kryptographischen Hash-Algorithmus, wie die oben diskutierten Algorithmen, gehasht werden, und der Hash jeder Transaktion kann in dem Baum gespeichert werden. Wenn der Baum aufgebaut ist, kann der Hash jedes benachbarten Knotens auf derselben Ebene zusammen gehasht werden, um einen neuen Knoten zu generieren, der auf einer höheren Ebene im Baum existiert. Daher hängt der Knoten am oberen Ende des Baums oder der Merkle-Wurzel vom Hash jeder Transaktion ab, die unten im Baum gespeichert ist. Jede Transaktion kann einen Datensatz enthalten. Der Datensatz kann das Identifizieren von Daten für die Transaktion und Transaktionsdaten enthalten, welche die Art der Transaktion identifizieren und was die Transaktion beinhaltet (z. B. Eingabe- und Ausgabeadressen, einen Transaktionswert, einen Dokumenten-Hashwert, einen Zeitstempel, einen Transaktionsgebührenwert, usw.).

[0067] Um zu überprüfen, ob ein Block gültig ist, kann ein Knoten die Merkle-Wurzel des Blocks mit der Merkle-Wurzel desselben Blocks vergleichen, der in den Kopien der Blockchain anderer Knoten enthalten ist. Somit kann die Merkle-Wurzel als Nachweis für die im Block enthaltenen Transaktionen und als Nachweis dafür verwendet werden, dass der Inhalt des Blocks nicht manipuliert wurde, wenn die Merkle-Wurzel in der Kopie jedes Knotens des Blocks dieselbe ist.

[0068] In einer Implementierung sind Dokumente, die „auf" einer Blockchain gespeichert sind, Dokumente, die gemäß einem kryptographischen Hashing-Algorithmus (z. B. SHA-256) gehasht wurden, und der resultierende Ausgabe-Hash wurde in eine Transaktion in einem Block aufgenommen, der von den Netzwerkknoten akzeptiert wurde, welche die Konsensregeln der Blockchain erfüllen. Als solches können die Dokumente später verifiziert oder validiert werden, indem der Hash der Dokumente mit dem in der Blockchain gespeicherten Hash verglichen wird. Wenn beispielsweise ein Satz von Dokumenten zu einem SHA-256-Hash führt, der an einem bestimmten Datum in einer Blockchain aufgezeichnet wurde, stellt die Blockchain einen kryptographischen Nachweis dafür bereit, dass die Dokumente zu diesem Datum vorhanden waren.

[0069] Eine Möglichkeit zum Speichern eines Dokuments in einer Blockchain besteht darin, eine Transaktion mit einem Hash des Dokuments an das Netzwerk zu senden, das in einem Block enthalten ist, wenn die Transaktion alle Konsensregeln des Netzwerks erfüllt. In einigen Implementierungen ist die Blockchain ein Permissioned Ledger, d. h. nur autorisierte Netzwerkteilnehmer dürfen Transaktionen senden. In anderen Implementierungen können nur einige autorisierte Netzwerkteilnehmer bestimmte Transaktionen durchführen. Beispielsweise können Produktparameterdaten, die Eigenschaften eines in einer Prozessanlage **10** generierten Produkts angeben, von einem Feldgerät in die Blockchain **600** hochgeladen werden, wenn das Feldgerät die Produkteigenschaften bestimmt (z. B. eine Temperatur des Produkts, ein Volumen des Produkts, eine Masse des Produkts, eine Dichte des Produkts, einen Druck des Produkts usw.). Nur ein kryptographischer Hash der Daten kann in der Blockchain **600** enthalten sein, so dass die Daten unter Verwendung der Blockchain verifiziert werden können, selbst wenn sie von einer Partei außerhalb der Chain erhalten werden.

[0070] Das Validieren von Netzwerkknoten kann überprüfen, ob die signierte Transaktion oder signierte Nachricht mit dem privaten kryptographischen Schlüssel signiert wurde, der dem veröffentlichten öffentlichen kryptographischen Schlüssel entspricht, der dem Feldgerät gehört, das die Messungen sammelt. In mindestens einer Implementierung kann ein gültiger Identitätsnachweis als Konsensregel vom Blockchain-Netzwerk angewendet werden. Daher wird jede Transaktion, die versucht, neue Produktparameterdaten ohne einen kryptographischen Identitätsnachweis hinzuzufügen, der mit einer Identität übereinstimmt, die zum Hinzufügen neuer Produktparameterdaten autorisiert ist, vom Netzwerk als nicht konform mit der Konsensregel zurückgewiesen. Jedem Feldgerät in einer Prozessanlage **10** kann ein Paar aus öffentlichem Schlüssel und privatem Schlüssel zugewiesen werden, das im Blockchain-Netzwerk als dem Feldgerät entsprechend identifiziert wird. Zusätzlich kann jedes Feldgerät autorisiert sein, bestimmte Arten von Messungen zu erfassen. Beispielsweise kann ein erstes Feldgerät autorisiert sein, Temperaturmessungen für ein Produkt zu erfassen, während ein zweites Feldgerät autorisiert sein kann, Volumenmessungen zu erfassen, die das Volumen des hergestellten Produkts anzeigen. Wenn die validierenden Netzwerkknoten eine Transaktion bezüglich Produktparameterdaten empfangen, die nicht von einem autorisierten Feldgerät stammen oder eine Art von Messung enthalten, zu deren Erfassung das Feldgerät nicht autorisiert ist, lehnen die validierenden Netzwerkknoten die Transaktion ab.

[0071] Fig. 6B zeigt einen anderen beispielhaften Distributed Ledger **650**, der eine andere Architektur als die in **Fig. 6A** beschriebene Architektur aufweist. Der Distributed Ledger **650** in **Fig. 6B** enthält eine Blockchain **660**, welche die Blöcke **662-668** von Transaktionen in einem Prozessleitsystem aufweist, ähnlich dem Distributed Ledger **600** in **Fig. 6A**. Die Blockchain **660** kann in dem Distributed Ledger **650** als die Hauptblockchain bezeichnet werden. Zusätzlich zu der Hauptblockchain **660** enthält der Distributed Ledger **650** mehrere Sideblockchains **670**, **680** oder Sidechains, die von verschiedenen Prozessanlagen, welche die Transaktionsblöcke **672-676**, **682-686** aufweisen, verwaltet werden. Beispielsweise kann die Sidechain **670** von zwei Prozessanlagen verwaltet werden: Anlage A und Anlage B, um Transaktionen aufzuzeichnen, die sich auf Ereignisse beziehen, die innerhalb oder zwischen den beiden Prozessanlagen stattfinden. Diese Transaktionen können einschließen, dass die Anlage B eine Zahlung in Form eines Tokenwerts an die Anlage A sendet, wenn die Anlage A ein Produkt an die Anlage B versendet. Die Sidechain **680** kann auch von zwei Prozessanlagen verwaltet werden: Anlage C und Anlage D, um Transaktionen aufzuzeichnen, die sich auf Ereignisse beziehen, die innerhalb oder zwischen der Anlage C und der Anlage D stattfinden. Diese Transaktionen können beinhalten, dass die Anlage D die von der Anlage C innerhalb eines bestimmten Zeitraums erhaltene Ölmenge aufzeichnet.

[0072] In einigen Ausführungsformen wird die Hauptblockchain **660** von mehreren Prozessanlagen einschließlich der Anlagen A-D zusammen mit mehreren anderen Prozessanlagen verwaltet. In einigen Ausführungsformen interagieren die Sidechains **670**, **680** auch mit der Hauptblockchain **660**, um der Hauptblockchain **660** mindestens einige der Transaktionen in ihren jeweiligen Blöcken **672-676**, **682-686** bereitzustellen. Auf diese Weise können die Sidechains **670**, **680** Daten von Transaktionen enthalten, die sich auf die Prozessanlagen beziehen, welche sie verwalten. Die Hauptblockchain **660** kann Daten von Transaktionen enthalten, die sich auf jede der Prozessanlagen beziehen. Zusätzlich können die Sidechains **670**, **680** private oder sensible Daten enthalten, die nicht außerhalb der Prozessanlagen, die eine bestimmte Sidechain verwalten, gemeinsam genutzt werden sollen. Daten von der Sidechain **670**, die nicht privat oder vertraulich sind, können der Hauptblockchain **660** bereitgestellt werden, während die privaten oder vertraulichen Daten nicht der Hauptblockchain **660** bereitgestellt werden. Beispielsweise kann die Sidechain **670** einen Smart Contract zwischen der Anlage A und der Anlage B ausführen, der einen Tokenwert von der Anlage A an die Anlage B überträgt, wenn die Anlage A ein Produkt von der Anlage B erhält, das bestimmte Qualitätsstandards erfüllt. Die Anlagen A und B möchten möglicherweise nicht alle Bedingungen des Smart Contracts der Öffentlichkeit oder einer großen Gruppe von Prozessanlagen offenlegen, indem sie den Smart Contract in der Hauptblockchain **660** bereitstellen, oder möchten möglicherweise nicht, dass jede Messung der Produkteigenschaften der Öffentlichkeit oder einer großen Gruppe von Prozessanlagen zur Verfügung gestellt wird. Zusätzlich erhöht sich der Speicherbedarf für die Hauptblockchain **660**, wenn der Hauptblockchain **660** mehr Transaktionen hinzugefügt werden. Dementsprechend kann es den Speicherbedarf zum Validieren von Knoten in dem Distributed-Ledger-Netzwerk reduzieren, um einige Transaktionen außerhalb der Hauptblockchain **660** zu speichern. In jedem Fall kann, wenn der Smart Contract feststellt, dass die Anlage A ein Produkt von der Anlage B erhalten hat, das die erforderlichen Qualitätsstandards erfüllt, die Transaktion, die den Tokenwert von der Anlage A an die Anlage B überträgt, der Hauptblockchain **660** bereitgestellt werden.

[0073] In einigen Ausführungsformen ist die Hauptblockchain **660** eine Public Blockchain, was bedeutet, dass jede Partei den Distributed Ledger sehen, neue Informationen zum Ledger hinzufügen oder dem Netzwerk als Validierungsknoten beitreten kann. Die Sidechains **670**, **680** sind Private oder Permissioned Blockchains, die Chain-Daten unter einer Gruppe von Einheiten, die zur Teilnahme an dem Sidechain-Netzwerk autorisiert sind, privat halten (z. B. kann die Sidechain **670** zwischen der Anlage A und der Anlage B privat sein). In anderen Ausführungsformen ist die Hauptblockchain **660** auch eine Permissioned Blockchain, aber die Hauptblockchain weist eine größere Anzahl von Einheiten auf, die autorisiert sind, an dem Blockchain-Netzwerk teilzunehmen, als die Sidechains **670**, **680**. Beispielsweise kann die Hauptblockchain **660** zwischen einer großen Anzahl von Prozessanlagen einschließlich den Anlagen A-D und mehreren anderen Prozessanlagen privat sein, wohingegen die Sidechain **670** zwischen der Anlage A und der Anlage B privat ist.

[0074] Zusätzlich oder als Alternative zu Sidechains kann der Distributed Ledger **650** andere Formen von Transaktionen enthalten, die außerhalb der Chain stattfinden und nicht Teil der Hauptblockchain **660** sind. Beispielsweise können zwei Parteien wie die Anlage A und die Anlage B einen Zahlungskanal eröffnen, in dem eine anfängliche Transaktion, die einen Schwellenwertbetrag eines Tokens zwischen der Anlage A und der Anlage B austauscht, der Hauptblockchain **660** bereitgestellt wird. Dann können die Anlage A und die Anlage B miteinander Transaktionen durchführen, ohne irgendetwas in der Hauptblockchain **660** aufzuzeichnen, solange sie Teile des Schwellenwertbetrags einander hin und her senden, und keine der Transaktionen dazu führt, dass eine der Prozessanlagen mehr als den Schwellenwertbetrag aufweist. Wenn die beiden Prozessanlagen eine Transaktion miteinander abgeschlossen haben,

können sie den Zahlungskanal schließen und die endgültigen Tokenbeträge für jede Prozessanlage in der Hauptblockchain **660** bereitstellen. Beispielsweise können die Anlage A und die Anlage B einen Zahlungskanal eröffnen, wenn die Anlage A zwei Token an die Anlage B sendet. Die Anlage B kann dann einen Token an die Anlage A zurücksenden, sodass jede Prozessanlage einen Token aufweist, die Anlage B kann 0,5 Token zu der Anlage A zurücksenden und so weiter, solange keine der Prozessanlagen mehr als zwei Token hat. In anderen Ausführungsformen kann der Distributed Ledger **650** mehrere Blockchain-Schichten umfassen, einschließlich separater Blockchain-Schichten, die unabhängig voneinander arbeiten. Beispielsweise kann eine erste Blockchain-Schicht Transaktionen in Bezug auf die Lieferkette aufzeichnen, während eine zweite Blockchain-Schicht Transaktionen in Bezug auf den Token-Austausch aufzeichnen kann. Die erste Blockchain-Schicht kann öffentlich sein, während die zweite Blockchain-Schicht privat ist oder umgekehrt.

[0075] Zusätzlich zum Datenschutz über Sidechains oder Off-Chain-Transaktionen kann in einigen Ausführungsformen der Datenschutz in einer öffentlichen Blockchain, wie der Blockchain **600**, wie sie in **Fig. 6A** gezeigt ist, erhalten bleiben. Beispielsweise können die Transaktionen in der Blockchain **600** die Identitäten der Parteien der Transaktion und die Transaktionsbeträge durch verschiedene Verschlüsselungstechniken verschleiern.

[0076] Fig. 7A-7C zeigen einen anderen beispielhaften Distributed Ledger **700**, der eine andere Architektur als die in **Fig. 6A** beschriebene Architektur aufweist. Der Distributed Ledger **700** in **Fig. 7A-7C** enthält mehrere lokale Blockchains **710**, **720**, wobei jede lokale Blockchain **710**, **720** von einer anderen Partei oder einer anderen Prozessanlage verwaltet wird. Jede lokale Blockchain **710**, **720** enthält einen Transaktionsblock **712-716**, **722-726** in einem Prozessleitsystem. Beispielsweise können sich mehrere Prozessanlagen eine Ressource teilen, z. B. Öl aus einer Ölpipeline, Strom aus einem Stromerzeugungssystem, ein Produkt über die Schiene, ein Automobil, ein Schiff oder einen Lufttransport, ein Produkt über eine Flüssigkeits-, Gas-, Dampf-, Kraftstoff- oder Materialleitung oder Wasser aus einem Wasserverteilungssystem. Feldgeräte in der Anlage A können Messungen in Bezug auf die gemeinsam genutzte Ressource wie beispielsweise eine aus der Pipeline gewonnene Ölmenge erfassen und die Messdaten in Transaktionen an die lokale Blockchain für die Anlage A senden. In ähnlicher Weise können Feldgeräte in der Anlage B Messungen in Bezug auf die geteilte Ressource sammeln und die Messdaten in Transaktionen an die lokale Blockchain für die Anlage B senden.

[0077] Wie in **Fig. 7B** gezeigt, werden Transaktionen von jeder lokalen Blockchain **710**, **720** einer globalen Blockchain **730** für die jeweilige Partei oder Prozessanlage bereitgestellt, wobei die globale Blockchain **730** von mehreren Prozessanlagen und/oder über Cloud-Dienste, welche mehrere Cloud-Computing-Systeme aufweisen, verwaltet wird. Beispielsweise werden Blöcke von der lokalen Blockchain **710** für die Anlage A der globalen Blockchain **730** für die Anlage A bereitgestellt, Blöcke aus der lokalen Blockchain **720** für die Anlage B werden der globalen Blockchain für die Anlage B bereitgestellt, usw. Die Transaktionsblöcke können von lokalen Blockchains entsprechenden globalen Blockchains nach einem Schwellenwertzeitraum oder einer Schwellenwertepoche bereitgestellt werden. Auf diese Weise kann das Validieren von Knoten in einer bestimmten Prozessanlage, die jede lokale Blockchain verwaltet, Blöcke aus der lokalen Blockchain entfernen oder Blöcke aus der lokalen Blockchain beschneiden, welche der globalen Blockchain bereitgestellt wurden, wenn es sich nicht um den letzten Block handelt, um den Speicherbedarf zu verringern.

[0078] Wie in **Fig. 7B** gezeigt, werden Block N (Ref. Nr. **742**), Block N+1 (Ref. Nr. **746**) und Block N+2 (Ref. Nr. **748**) zu der lokalen Blockchain **710** für Anlage A während der Zeitepoche E hinzugefügt (Ref. Nr. **740**). Nachdem der Schwellenwertzeitraum für die Zeitepoche E abgelaufen ist, stellen die Validierungsknoten, welche die lokale Blockchain **710** für die Anlage A verwalten, der globalen Blockchain **730** für die Anlage A die Blöcke N-N+2 (Ref. Nr. **742-746**) zur Verfügung. Anschließend entfernen die Validierungsknoten, welche die lokale Blockchain **710** für die Anlage A verwalten, Block N (Ref. Nr. **742**) und Block N+1 (Ref. Nr. **744**) von der lokalen Blockchain **710** oder beschneiden diese, um den Speicherbedarf zu verringern. Die lokale Blockchain **710** enthält zu diesem Zeitpunkt nur den letzten Block, Block N+2 (Ref. Nr. **746**). Dann werden während der Zeitepoche E+1 (Ref. Nr. **750**) Block N+3 (Ref. Nr. **752**) und Block N+4 (Ref. Nr. **754**) zu der lokalen Blockchain **710** hinzugefügt. Nachdem der Schwellenwertzeitraum für die Zeitepoche E+1 abgelaufen ist, stellen die Validierungsknoten, welche die lokale Blockchain **710** für Anlage A verwalten, die Blöcke N+3-N+4 (Ref. Nr. **752-754**) für die globale Blockchain **730** für Anlage A bereit. Dann entfernen oder beschneiden die Validierungsknoten, welche die lokale Blockchain **710** für Anlage A verwalten, die Blöcke N+2-N+3 (Ref. Nr. **746**, **752**) aus der lokalen Blockchain **710**. Die lokale Blockchain **710** enthält zu diesem Zeitpunkt nur den neuesten Block, Block N+4 (Ref. Nr. **754**).

[0079] Wie in **Fig. 7C** gezeigt, kombinieren die Validierungsknoten, welche die globalen Blockchains wie die globale Blockchain für die Anlage A **730** und die globale Blockchain für die Anlage B **770** verwalten, die globalen Blockchains **730**, **770**, um eine Super-

blockchain **760** mit Zustandsblöcken **762**, **764** zu generieren. Jeder Zustandsblock **762**, **764** enthält jeden der Blöcke aus den globalen Blockchains **730**, **770** für einen bestimmten Zeitraum. Beispielsweise enthält der Zustandsblock K (Ref. Nr. **762**) den jeweiligen Block N, den Block N+1 und den Block N+2 von jeder globalen Blockchain **730**, **770**. Der Zustandsblock K+1 (Ref. Nr. **764**) enthält den jeweiligen Block N+3, den Block N+4 und den Block N+5 aus jeder globalen Blockchain **730**, **770**.

[0080] Um Blöcke und Transaktionen kryptographisch miteinander zu verbinden, organisiert jeder Zustandsblock **762**, **764** in der Superblockchain **760** seine Transaktionen in einem Merkle-Tree. Wenn eine einzelne Transaktion in dem Zustandsblockblock manipuliert wird, würde eine andere Merkle-Wurzel generiert, da die Merkle-Wurzel eine Kombination der Hashes aller Transaktionen in dem Block ist. Die Merkle-Wurzel für jeden Zustandsblock **762**, **764** ist in dem Header für den Zustandsblock **762**, **764** enthalten.

[0081] Die in den **Fig. 7A-7C** beschriebene Distributed-Ledger-Architektur **700**, welche lokale Blockchains, globale Blockchains und eine Superblockchain aufweist, ermöglicht es konkurrierenden Einheiten, die Genauigkeit von Messdaten zu überprüfen. Wenn beispielsweise die Anlage A der Anlage B meldet, dass die Anlage A 30.000 Gallonen Öl aus einer Ölpipeline entnommen hat, die von beiden Einheiten gemeinsam genutzt wird, kann die Anlage B Messdaten aus der Superblockchain abrufen, um die Genauigkeit dieser Messung zu überprüfen. Die Messdaten können auch innerhalb der Superblockchain **760** kryptographisch überprüft werden, indem eine erwartete Merkle-Wurzel für den Header des Zustandsblocks berechnet wird, der die Messdaten enthält, und die tatsächliche Merkle-Wurzel im Header des Zustandsblocks mit der erwarteten Merkle-Wurzel verglichen wird. Dies ermöglicht es konkurrierenden Einheiten, welche die Superblockchain **760** analysieren, zu validieren, dass die Zustandsblöcke **762**, **764** in der Superblockchain **760** nicht manipuliert wurden.

Smart Contracts in einem Prozessleitsystem

[0082] Wie oben beschrieben können Prozessleitsysteme Smart Contracts für den Distributed Ledger bereitstellen, um den Wert auszutauschen, beispielsweise nach Erhalt eines Produkts in gutem Zustand. Smart Contracts können auch für den Distributed Ledger bereitgestellt werden, damit Maschinen wie Feldgeräte ohne menschliches Eingreifen selbstständig Transaktionen durchführen können.

[0083] **Fig. 8** zeigt einen beispielhaften Zustand **806** des Smart Contracts in einem Distributed-Ledger-Netzwerk in einem Prozessleitsystem. **Fig. 8** enthält eine Blockchain **802**, einen Transaktionsblock **804** und einen Zustand **806** des Smart Contracts für Aufforderungen zum sicheren Schreiben. Ein Smart Contract kann von jedem Teilnehmer des Distributed-Ledger-Netzwerks oder des Blockchain-Netzwerks (z. B. Anlagenbedienern, Konfigurationsingenieuren, Prozessleitsystemkonstrukteuren usw.) bereitgestellt werden, um beispielsweise einen Zustand **806** des Contracts für eine Aufforderung zum sicheren Schreiben festzulegen. Der bereitgestellte Smart Contract kann anderen Teilnehmern im Blockchain-Netzwerk Verfahren und Daten zur Verfügung stellen. Einige der Daten im Zustand des Smart Contracts können private Daten sein, die nur durch Aufrufen eines Verfahrens des Smart Contracts oder nur durch autorisierte Blockchain-Teilnehmer geändert werden können. Eine Möglichkeit zum Ändern des Zustands des Smart Contracts besteht darin, eine Transaktion an das Distributed-Ledger-Netzwerk zu senden. Wenn die gesendete Transaktion die Konsensregeln erfüllt, können Netzwerkvalidierer die Transaktion in einen Block einschließen. Die Aufnahme einer Transaktion in die Blockchain, die Daten an den Smart Contract sendet, kann dazu führen, dass Validierungsknoten eine Zustandsdatenbank für den Smart Contract aktualisieren und auf diese Weise Netzwerkteilnehmern den Zugriff auf einen Rich-State-Mechanismus ermöglichen, mit dem sie die Aufforderung zum sicheren Schreiben verwalten und letztendlich Parameterdaten an ein SIS-(Safety Instrumented System)-Gerät schreiben können.

[0084] Der Zustand **806** des Smart Contracts für eine Aufforderung zum sicheren Schreiben kann Datenelemente enthalten, um den Bediener, der die Aufforderung zum sicheren Schreiben absendet, das Computergerät, mit dem der Bediener die Aufforderung zum sicheren Schreiben absendet, und/oder das SIS-Gerät, welches das Ziel der Aufforderung zum sicheren Schreiben ist, zu identifizieren. In einigen Ausführungsformen kann der Bediener durch kryptographische öffentliche Schlüssel identifiziert werden, die der elektronischen Geldbörse des Bedieners zugewiesen sind. Das Computergerät des Bedieners kann durch dieselben öffentlichen kryptographischen Schlüssel wie der Bediener identifiziert werden, wenn die elektronische Geldbörse des Bedieners das Computergerät des Bedieners bedient. In anderen Ausführungsformen kann das Computergerät des Bedieners durch andere kryptographische öffentliche Schlüssel identifiziert werden, von denen bekannt ist, dass sie von den anderen Netzwerkteilnehmern zum Computergerät des Bedieners gehören.

[0085] In einigen Ausführungsformen kann ein Inhaber des Contracts eine eindeutige ID für das SIS-Gerät auswählen, sodass nachfolgende Transaktionen und Daten, die an den Smart Contract gesendet werden, das SIS-Gerät anhand der ID-Nummer identifizieren können. Beispielsweise kann jedes SIS-Ge-

rät im Smart Contract eine andere eindeutige Kennung haben. Der Inhaber des Contracts kann auch Kennungen von Bedienern und/oder Computergeräten angeben, die zum Ausführen sicherer Schreibvorgänge autorisiert sind. Nachfolgende Daten, die an den Smart Contract gesendet werden, können eine Nachricht enthalten, die von privaten Schlüsseln signiert ist, die den öffentlichen Schlüsseln entsprechen, die den Bediener und/oder das Computergerät in dem Smart Contract identifizieren, wodurch ein kryptographischer Nachweis erbracht wird, dass die Transaktion von einem autorisierten Bediener und/oder einem autorisierten Computergerät initiiert wurde. Die privaten und die öffentlichen Schlüssel können ausschließlich von den Bedienern/Computergeräten verwaltet werden, um die Angriffsfläche für Angreifer zu minimieren, die versuchen könnten, eine Transaktion zu fälschen (z. B. generieren die Bediener/Computergeräte öffentliche/private kryptographische Schlüsselpaare offline und stellen lediglich den öffentlichen Schlüssel für andere Netzwerkteilnehmer zur Verfügung). Die privaten Schlüssel eines Bedieners und/oder eines Computergeräts können gemäß einem sicher gespeicherten Startwert (z. B. auf einem Stück physischem Papier oder mehreren Kopien eines Stück Papiers) generiert werden, so dass die privaten Schlüssel im Fall von einem Datenverlust wiederhergestellt werden können.

[0086] Um Parameterdaten in ein SIS-Gerät zu schreiben, kann der Zustand **806** des Smart Contracts für Aufforderungen zum sicheren Schreiben Nachweise für die Aufforderung zum sicheren Schreiben erhalten. Der Nachweis für die Aufforderung zum sicheren Schreiben kann den Namen des zu ändernden Parameters im SIS-Gerät und/oder Pfadinformationen für den Parameter enthalten. Der Nachweis kann auch einen neuen Parameterwert enthalten, und in einigen Ausführungsformen kann der Nachweis einen CRC-(Cyclical Redundancy Check)-Wert oder einen anderen Fehlerprüfwert zusammen mit dem neuen Parameterwert enthalten, um sicherzustellen, dass die Parameterinformationen intakt sind und nicht verfälscht wurden. In einigen Ausführungsformen kann der Smart Contract als Reaktion auf den Empfang der Parameterinformationen einen Bestätigungsdialog für das Computergerät des Bedieners bereitstellen, der den Namen des SIS-Geräts, den Namen und/oder den Pfad für den in dem SIS-Gerät zu ändernden Parameter, den neuen Parameterwert und eine Bestätigungstaste enthält, mit welcher der Bediener die Aufforderung zum sicheren Schreiben bestätigen kann. In diesem Szenario kann der Nachweis eine Angabe enthalten, ob der Bediener die Bestätigungsschaltfläche ausgewählt hat.

[0087] Der Bediener und/oder das Computergerät des Bedieners können Transaktionen an die Blockchain **802** senden, welche den Nachweis enthält. Der Nachweis kann kryptographisch signiert sein, um einen kryptographischen Identitätsnachweis zu erbringen, dass der Nachweis von einem Bediener und/oder einem Computergerät des Bedieners stammt, der zur Ausführung einer Aufforderung zum sicheren Schreiben autorisiert ist. Dementsprechend kann der Smart Contract die bereitgestellte Identität mit einer Liste von Bedienern und/oder Computergeräten vergleichen, die autorisiert sind, Aufforderungen zum sicheren Schreiben auszuführen. In einigen Ausführungsformen kann der Smart Contract die bereitgestellte Identität mit einer Liste von Bedienern und/oder Computergeräten vergleichen, die autorisiert sind, Aufforderungen zum sicheren Schreiben für das bestimmte SIS-Gerät auszuführen, welches das Ziel der Aufforderung zum sicheren Schreiben ist.

[0088] Ein weiterer Aspekt des Zustands **806** des Smart Contracts für Aufforderungen zum sicheren Schreiben sind die Daten des Smart Contracts. Daten des Smart Contracts können als private und öffentliche Daten in einem Objekt betrachtet werden, das gemäß einem objektorientierten Programmierparadigma erstellt wurde, indem die Daten des Smart Contracts direkt von außerhalb des Objekts aktualisiert werden können, oder die Daten des Smart Contracts nur begrenzt aktualisiert werden können, so wie beispielsweise durch Aufrufen eines Verfahrens des Smart Contracts. Die Daten des Smart Contracts können den Namen und/oder den Pfad für den im SIS-Gerät zu ändernden Parameter und den neuen Parameterwert enthalten. In einigen Ausführungsformen können die Daten des Smart Contracts eine Angabe enthalten, ob die Parameterinformationen intakt empfangen wurden. Beispielsweise kann die Transaktion, welche den zu ändernden Parameter und Parameterinformationen enthält, auch einen CRC-Wert oder einen anderen Fehlerprüfwert enthalten. Der Smart Contract kann einen erwarteten CRC-Wert auf der Grundlage des zu ändernden Parameters und der Parameterinformationen generieren und den erwarteten CRC-Wert mit dem empfangenen CRC-Wert vergleichen. Wenn der erwartete CRC-Wert mit dem empfangenen CRC-Wert übereinstimmt, kann der Smart Contract feststellen, dass die Parameterinformationen intakt empfangen wurden. In einigen Ausführungsformen können die Daten des Smart Contracts auch eine Angabe enthalten, ob die Aufforderung zum sicheren Schreiben bestätigt wurde. Wenn der Smart Contract beispielsweise eine Transaktion durch den Bediener und/oder das Computergerät des Bedieners empfängt, die angibt, dass der Bediener die Bestätigungsschaltfläche ausgewählt hat, kann der Smart Contract bestimmen, dass die Aufforderung zum sicheren Schreiben bestätigt wurde.

[0089] Zum Beispiel können die Daten des Smart Contracts, wie in **Fig. 8** gezeigt, einen Parameter zum Sperren/Entsperren des SIS-Geräts, einen Parameterwert von ‘1‘ oder ’Sperren‘, der angibt, dass

der Parameter zum Sperren des SIS-Geräts eingestellt werden soll, einen bestätigten Wert von ‚1', 'ja' oder ‚wahr', der angibt, dass die Aufforderung zum sicheren Schreiben bestätigt wurde, und einen intakten Wert für empfangene Daten von '1', 'ja' oder 'wahr', der angibt, dass die Parameterinformationen nicht beschädigt wurden, enthalten. Dementsprechend kann der Smart Contract bestimmen, dass der neue Parameterwert dem SIS-Gerät bereitgestellt werden soll. Dann kann der Smart Contract die Parameterinformationen an das SIS-Gerät oder an eine mit dem SIS-Gerät kommunikativ gekoppelte Steuerung liefern, um das sichere Schreiben von Daten durchzuführen.

[0090] In einigen Ausführungsformen kann der Smart Contract für Aufforderungen zum sicheren Schreiben Parameterinformationen an ein Ziel-SIS-Gerät oder eine mit dem Ziel-SIS-Gerät kommunikativ gekoppelte Steuerung liefern, wenn der Bediener und/oder das Computergerät, welches die Aufforderung zum sicheren Schreiben sendet, autorisiert sind, das sichere Schreiben von Daten für das Ziel-SIS-Gerät durchzuführen, die Parameterinformationen nicht beschädigt sind, und die Aufforderung zum sicheren Schreiben bestätigt wird. In anderen Ausführungsformen bestimmt der Smart Contract für Aufforderungen zum sicheren Schreiben nicht, ob die Parameterinformationen intakt empfangen werden. Stattdessen stellt der Smart Contract für Aufforderungen zum sicheren Schreiben eine erste Instanz der Parameterinformationen, einschließlich des Parameternamens und/oder -pfads, des neuen Parameterwerts und des CRC-Werts, an das Ziel-SIS-Gerät oder die Ziel-SIS-Steuerung als Reaktion auf den Empfang der Aufforderung zum sicheren Schreiben bereit. Der Smart Contract für Aufforderungen zum sicheren Schreiben stellt dem Ziel-SIS-Gerät oder der -Steuerung auch eine zweite Instanz der Parameterinformationen als Reaktion auf den Empfang einer Bestätigung der Aufforderung zum sicheren Schreiben zur Verfügung. Die Steuerung oder das Ziel-SIS-Gerät bestimmt dann, ob die Parameterinformationen in beiden Fällen gleich sind und ob die Parameterinformationen intakt empfangen wurden. Wenn die Parameterinformationen in beiden Fällen identisch sind und die Parameterinformationen intakt empfangen wurden, schreibt die Steuerung oder das Ziel-SIS-Gerät den neuen Parameterwert für den Parameter in das Ziel-SIS-Gerät.

[0091] Während **Fig. 8** einen Zustand **806** des Smart Contracts für eine Aufforderung zum sicheren Schreiben zeigt, ist dies lediglich ein beispielhafter Smart Contract, um die Darstellung zu vereinfachen. Teilnehmer am Distributed-Ledger-Netzwerk (z. B. Anlagenbediener, Konfigurationsingenieure, Konstrukteure von Prozessleitsystemen usw.) können alle geeigneten Smart Contracts im Zusammenhang mit der Prozesssteuerung einsetzen.

[0092] In einem anderen Beispiel kann ein Smart Contract bereitgestellt werden, der Geräteinformationen für ein Gerät in der Prozessanlage **10** abruft, bei dem ein Fehler aufgetreten ist, und die Geräteinformationen einem Gerätelieferanten als Reaktion auf den Empfang einer Aufforderung zum Teilen der Geräteinformationen bereitstellt. Genauer gesagt, wenn bei einem Gerät in der Prozessanlage **10**, wie beispielsweise einer Prozessanlageneinheit, ein Fehler auftritt, kann das Gerät eine Transaktion an eine Adresse für den Smart Contract übermitteln, der in dem Distributed Ledger gespeichert ist. Die Transaktion kann kryptographisch signiert sein, um einen kryptographischen Identitätsnachweis zu liefern, dass die Transaktion vom Gerät stammt. In anderen Ausführungsformen kann die Prozessanlageneinheit eine Angabe des Fehlers an eine Steuerung, ein Feldgerät oder ein anderes Prozesssteuerungsgerät übermitteln, das als Nachweis-Orakel fungiert und die Transaktion generiert. In jedem Fall kann die Transaktion Geräteinformationen für das Gerät enthalten, wie beispielsweise Identifikationsinformationen für das Gerät, Marke, Modell und Jahr des Geräts, Wartungsverlauf für das Gerät, Art des Fehlers, beschädigte Teile im Gerät, etc.

[0093] In einigen Ausführungsformen übermittelt der Smart Contract die Geräteinformationen an ein Computergerät des Verwaltungspersonals in der Prozessanlage **10**, damit das Verwaltungspersonal die Geräteinformationen überprüfen kann. Nach Überprüfung der Geräteinformationen kann das Verwaltungspersonal feststellen, dass die Geräteinformationen vom Gerätelieferanten überprüft werden müssen, um den Fehler weiter zu untersuchen und/oder ein Ersatzgerät oder Ersatzteile bereitzustellen. Dementsprechend kann das Computergerät des Verwaltungspersonals eine Transaktion generieren, die den Smart Contract auffordert, die Geräteinformationen an den Gerätelieferanten weiterzuleiten. Die Transaktion kann kryptographisch signiert sein, um einen kryptographischen Identitätsnachweis zu liefern, dass die Transaktion vom Verwaltungspersonal stammt. In Reaktion auf die Feststellung, dass die Aufforderung zur Bereitstellung der Geräteinformationen an den Gerätelieferanten von autorisiertem Verwaltungspersonal stammt, kann der Smart Contract die Geräteinformationen an ein Computergerät des Gerätelieferanten weiterleiten.

[0094] Ein weiterer beispielhafter Smart Contract ist ein Smart Contract, der einen Tokenwert von einer ersten Prozessanlage erhält, feststellt, dass ein Produkt bestimmte Qualitätsstandards erfüllt, die von einer zweiten Prozessanlage auf die erste Prozessanlage übertragen wurden, und der zweiten Prozessanlage den Tokenwert bereitstellt. In einigen Ausführungsformen kann der Smart Contract einen Hinweis erhalten, dass das Produkt in der ersten Prozessanlage von einem Nachweis-Orakel wie einem Feldgerät

in der ersten Prozessanlage empfangen wurde. Das Feldgerät kann auch Parameterdaten in Bezug auf das Produkt bereitstellen, die der Smart Contract mit einer Reihe von Qualitätsmetriken vergleicht, um zu bestimmen, ob die Produkte die Qualitätsstandards erfüllen. Wenn das Produkt die Qualitätsstandards erfüllt, stellt der Smart Contract der zweiten Prozessanlage den Tokenwert bereit. Andernfalls kann der Smart Contract den Tokenwert an die erste Prozessanlage zurückgeben.

Arten von Transaktionen, die in Distributed Ledgers in einem Prozessleitsystem erfasst werden

[0095] Die Distributed Ledgers des Prozessleitsystems können viele verschiedene Arten von Transaktionen enthalten, die sich auf die Prozesssteuerung beziehen. Diese Transaktionen können umfassen: 1) Transaktionen in Bezug auf die Lieferung oder den Empfang eines Produkts in einer Prozessanlage **10** und die gelieferte/erhaltene Menge; 2) Transaktionen im Zusammenhang mit Software- oder Firmware-Upgrades an Geräten in der Prozessanlage **10**, wie z. B. Bedienerarbeitsplätze, Servergeräte, Steuerungen, E/A-Geräte, Netzwerkgeräte, Feldgeräte usw.; 3) Transaktionen im Zusammenhang mit der Qualitätskontrolle, der Produktion oder dem behördlichen Berichtswesen in der Prozessanlage **10**; **4**) Transaktionen, die Prozessanlagendaten aufzeichnen; und 5) Transaktionen, welche die Produktüberwachungskette über Produktverfolgungsdaten aufzeichnen.

[0096] In einigen Szenarien werden die Transaktionen für Smart Contracts bereitgestellt, um beispielsweise einen Zustand des Smart Contracts zu ändern. In anderen Szenarien werden die Transaktionen nicht für Smart Contracts bereitgestellt und lediglich als sichere, unveränderliche und vertrauenswürdigen Aufzeichnung von Informationen, die sich auf eine Prozessanlage oder mehrere Prozessanlagen im Distributed Ledger beziehen, erfasst.

Transaktionen im Zusammenhang mit der Lieferung oder dem Erhalt eines Produkts und der gelieferten/erhaltenen Menge

[0097] Fig. 9 zeigt eine beispielhafte Transaktion **906**, die eine Nachweistransaktion darstellt, welche die in einer Prozessanlage **10** von einer Ölpipeline erhaltene Ölmenge meldet. Während die beispielhafte Transaktion **906** in **Fig. 9** die Ölmenge aus einer Ölpipeline angibt, ist dies nur ein Beispiel, um die Darstellung zu vereinfachen. Andere Materialien oder Produkte aus anderen Quellen können ebenfalls gemeldet werden, z. B. Elektrizität aus einem Stromerzeugungssystem, einem Produkt, das über die Schiene, ein Kraftfahrzeug, ein Schiff oder die Luft transportiert wird, ein Produkt, das über eine Flüssigkeits-, Gas-, Dampf-, Kraftstoff- oder Materialleitung oder Wasser aus einem Wasserverteilungssystem transportiert wird. In jedem Fall kann die Transaktion **906** durch ein Feldgerät generiert werden, das als Nachweis-Orakel fungiert. Wenn das Feldgerät Öl erkennt, das durch ein Ventil fließt, sendet das Feldgerät eine Transaktion **906** an die Blockchain **902**, um in einem Block wie dem Block **904** enthalten zu sein.

[0098] Die Transaktion **906** kann eine Transaktions-ID und einen Urheber wie das Feldgerät **456** in Anlage A (identifiziert durch einen kryptographischen Identitätsnachweis) enthalten. Die Transaktion **906** kann auch Identifikationsinformationen in Bezug auf das Produkt, den Anbieter des Produkts (z. B. einen Ölproduzenten) und Informationen in Bezug auf die Menge des erhaltenen Produkts enthalten. Beispielsweise kann das Feldgerät ein Durchflusssensor sein, der das in der Anlage A über einen bestimmten Zeitraum (z. B. eine Stunde, einen Tag usw.) erhaltene Ölvolumen bestimmt und das Volumen in die Transaktion einbezieht. In anderen Ausführungsformen kann das Feldgerät mehrere Flussraten zu verschiedenen Zeitperioden in einer Reihe von Transaktionen enthalten, und die Flussraten als eine Funktion der Zeit können verwendet werden, um die in Anlage A empfangene Ölmenge zu bestimmen. Des Weiteren kann die Transaktion **906** einen kryptographischen Hash der Informationen bezüglich des Ereignisses, der Produktkennung und der Produktanbieterkennung enthalten. In einer anderen Implementierung werden die Informationen bezüglich des Ereignisses, der Produktkennung und der ProduktanbieterKennung nicht als kryptographischer Hash gespeichert, sondern es kann ein Beobachter oder ein anderer Netzwerkteilnehmer direkt auf die Informationen in Block **904** zugreifen.

[0099] Während in diesem Beispiel das Feldgerät für die Prozessanlage **10**, die das Produkt empfängt, eine Transaktion generiert, kann ein Feldgerät für eine Prozessanlage **10** oder eine andere Einheit, die das Produkt bereitstellt, eine Transaktion generieren. Diese Transaktion kann zusätzlich oder alternativ zu der Transaktion durch das Feldgerät für die Prozessanlage **10** generiert werden, welche das Produkt empfängt.

Transaktionen im Zusammenhang mit Software- oder Firmware-Upgrades auf Geräten in der Prozessanlage

[0100] Um zu verhindern, dass nicht autorisierte Software oder Firmware in eine Prozessanlage **10** eingeführt wird, können Software- und Firmware-Upgrades für Geräte in der Prozessanlage **10** in einem Distributed Ledger, wie den oben beschriebenen Distributed Ledgers, digital aufgezeichnet werden. Das Distributed Ledger kann Aufzeichnungen über jede Software- und Firmware-Upgrade eines Geräts in der Prozessanlage **10** verwalten, einschließlich der Zeit und des Datums der Aktualisierung, der

Identität des Benutzers, der das Upgrade durchführt (über einen kryptographischen Identitätsnachweis), und Änderungen an der vorherigen Version der Software und/oder der neuen Version der Software. Ein Servergerät **12** oder ein anderes Computergerät in der Prozessanlage **10** kann kontinuierlich oder periodisch (z. B. einmal pro Sekunde, einmal pro Minute, einmal pro Stunde, einmal pro Tag usw.) aktuelle Versionen von Software und Firmware erhalten, die in Geräten in der Prozessanlage **10** ausgeführt werden. Die Servergerät **12** kann auch die Transaktionen aus dem Distributed Ledger abrufen und die aktuelle Software oder Firmware in einem Gerät mit der neuesten Version der Software oder Firmware vergleichen, die in dem Distributed Ledger aufgezeichnet ist. In einigen Ausführungsformen speichert der Distributed Ledger einen kryptographischen Hash der neuen Version der Software oder Firmware und vergleicht die aktuelle Software oder Firmware, die in dem Gerät ausgeführt wird, mit dem kryptographischen Hashwert, um sicherzustellen, dass die Software oder Firmware nicht manipuliert wurde.

[0101] Wenn die aktuelle Software oder Firmware im Gerät nicht mit der neuesten Version der Software oder Firmware übereinstimmt, die im Distributed Ledger aufgezeichnet ist, kann das Servergerät **12** verhindern, dass das Gerät die aktuelle Software oder Firmware ausführt. In einigen Ausführungsformen kann das Servergerät **12** bewirken, dass die Software oder Firmware in dem Gerät auf eine vorherige Version zurückgesetzt wird, beispielsweise durch Herunterladen der vorherigen Version auf das Gerät. Auf diese Weise können nicht autorisierte Benutzer die in der Prozessanlage **10** ausgeführte Software oder Firmware nicht manipulieren.

[0102] Fig. 10 zeigt eine beispielhafte Transaktion **1006**, die eine Nachweistransaktion darstellt, die eine Software- oder Firmware-Aktualisierung in einem Gerät in einer Prozessanlage **10** meldet. Die Transaktion **1006** kann durch das Gerät generiert werden, das die Upgrades empfängt, wie beispielsweise einen Bedienerarbeitsplatz, eine andere Benutzeroberflächenvorrichtung **8**, ein Servergerät **12**, eine Steuerung **11**, ein E/A-Gerät **26**, **28**, ein Netzwerkgerät, ein Feldgerät **15-22**, **40-46** usw. Ein Netzwerkgerät in der Prozessanlage **10** kann beispielsweise ein drahtloses Gateway **35**, einen Router **58**, einen drahtlosen Zugangspunkt **7a**, **55**, ein Edge-Gateway, einen drahtlosen Adapter **52** usw. enthalten.

[0103] Die Transaktion **1006** kann eine Transaktions-ID und einen Urheber enthalten, der die Software oder Firmware modifiziert, wie beispielsweise John Doe (identifiziert durch einen kryptographischen Identitätsnachweis). Die Transaktion **1006** kann auch Identifikationsinformationen (Bedienerarbeitsplatz **1234**) für das Gerät, das die Software oder Firmware ausführt (identifiziert durch einen kryptographischen Identitätsnachweis), eine Beschreibung einschließlich einer Versionsnummer und einer Zeit und eines Datums des Upgrades („Aktualisierung auf Version 10.3.1.4 am 15. Januar 2019 um 6: 02 Uhr morgens“). Weiterhin kann die Transaktion **1006** einen kryptographischen Hash der Softwareanweisungen für die neue Version der Software enthalten. In einer anderen Implementierung wird die neue Version der Software nicht als kryptographischer Hash gespeichert, sondern ist in Block **1004** für einen Beobachter oder einen anderen Netzwerkteilnehmer direkt zugänglich. In einigen Ausführungsformen geben die Konsensregeln an, dass nur autorisierte Benutzer Software- oder Firmware-Aktualisierungen auf dem Distributed Ledger aufzeichnen dürfen. Wenn dementsprechend die Transaktion **1006** an den Distributed Ledger gesendet wird, validieren die Validierungsknoten die Transaktion **1006**, wenn der Urheber ein autorisierter Benutzer ist. Wenn der Urheber kein autorisierter Benutzer ist, ist die Transaktion **1006** nicht im Distributed Ledger enthalten, und die Aktualisierung der Software stimmt nicht mit der neuesten Version der Software überein, die im Distributed Ledger aufgezeichnet ist.

[0104] In einem beispielhaften Szenario erhält eine Servergerät **12** in der Prozessanlage **10** am 15. Januar 2019 um 6: 03 Uhr morgens den Zustand der in dem Bedienerarbeitsplatz **1234** ausgeführten Software und vergleicht die Software mit dem kryptographischen Hash der Softwareanweisungen für die neue Version der Software in dem Distributed Ledger, indem beispielsweise ein kryptographischer Hash der Softwareanweisungen ausgeführt wird, die in dem Bedienerarbeitsplatz **1234** ausgeführt werden. Wenn die kryptographischen Hashes gleich sind, stellt das Servergerät **12** fest, dass die Software nicht manipuliert wurde. Wenn sich andererseits die kryptographischen Hashes unterscheiden, stellt das Servergerät fest, dass die Software manipuliert wurde, und verhindert, dass der Bedienerarbeitsplatz **1234** die Software in ihrem aktuellen Zustand ausführt. Das Servergerät **12** lädt dann den vorherigen Zustand der Software auf den Bedienerarbeitsplatz **1234** herunter, und der Bedienerarbeitsplatz **1234** setzt die Ausführung der Software in ihrem vorherigen Zustand fort.

Transaktionen im Zusammenhang mit der Qualitätskontrolle, Produktion oder dem behördlichen Berichtswesen in der Prozessanlage

[0105] In Prozessanlagen gelten Berichterstattungs- und Aufzeichnungspflichten, um die Anforderungen von Aufsichtsbehörden wie beispielsweise der Environmental Protection Agency (EPA) zu erfüllen. Zum Beispiel die von der EPA erlassenen Vorschriften zur Lecksuche und -behebung (Leak Detection and Repair, LDAR), um die Emission entweichender flüchtiger organischer Verbindungen und gefährlicher Luft-

schadstoffe von zum Beispiel undichten Geräten wie Ventilen, Pumpen und Anschlüssen in Prozessanlagen zu minimieren. Zur Einhaltung der Vorschriften und zur Bereitstellung einer sicheren, unveränderlichen und vertrauenswürdigen Aufzeichnung können die regulatorischen Daten in einem Distributed Ledger aufgezeichnet werden. Beispielsweise können als Reaktion auf ein auslösendes Ereignis wie ein Alarm, ein Fehler, ein Leck, ein Reparaturereignis, ein Prozessmeilenstein, eine Korrekturmaßnahme usw. Prozesssteuerungselemente wie Feldgeräte, Steuerungen oder Prozessanlageneinheiten Transaktionen generieren, die Daten aus dem auslösenden Ereignis enthalten, wie beispielsweise den Zeitpunkt, an dem das Ereignis stattfand, die Dauer des Ereignisses, Prozessparameterwerte für am Ereignis beteiligte Prozessanlageneinheiten, Produktparameterwerte für am Ereignis beteiligte Produkte usw. Die regulatorischen Daten werden dann im Distributed Ledger erfasst, sodass die Aufsichtsbehörden die Daten überprüfen können.

[0106] In einigen Ausführungsformen wird, wenn ein auslösendes Ereignis stattfindet, das auslösende Ereignis von einem der Prozesssteuerungselemente erfasst. Das Prozesssteuerungselement benachrichtigt dann andere Prozesssteuerungselemente über das auslösende Ereignis und weist dem auslösenden Ereignis eine eindeutige Kennung zu. Auf diese Weise kann jedes der Prozesssteuerungselemente Messungen in Bezug auf das auslösende Ereignis erfassen und Transaktionen an den Distributed Ledger senden, wobei jede Transaktion dieselbe eindeutige Kennung für das auslösende Ereignis enthält.

[0107] In einigen Ausführungsformen werden regulatorische Daten in einer öffentlichen Blockchain aufgezeichnet, so dass jeder die regulatorischen Daten einer Prozessanlage **10** sehen kann. In anderen Ausführungsformen werden die regulatorischen Daten in einer Private oder Permissioned Blockchain aufgezeichnet, auf welche die Prozessanlage **10** und die Aufsichtsbehörde zugreifen können. In noch anderen Ausführungsformen werden die regulatorischen Daten in einer Private oder Permissioned Blockchain aufgezeichnet, auf die mehrere Prozessanlagen in einem Prozessanlagen-Netzwerk zusammen mit der Aufsichtsbehörde zugreifen können.

[0108] **Fig. 11** zeigt eine beispielhafte Transaktion **1106**, die Prozessparameter oder Produktparameterdaten zur Meldung von Nachweistransaktionen darstellt. Die Transaktion **1106** kann von einer Prozessanlageneinheit generiert werden, die ein Gerät in einer Prozessanlage **10** zur Verwendung in einem Teil des Prozesses sein kann, der physische Materialien enthält, umwandelt, generiert oder überträgt, wie z. B. ein Ventil, ein Tank, ein Mischer, eine Pumpe, eine Heizung usw.

[0109] Die Transaktion **1106** kann eine Transaktions-ID und einen Urheber (Heater Y-001) umfassen, welche die Produkt- oder Prozessparameter-Messung (identifiziert durch einen kryptographischen Identitätsnachweis) sammeln. Die Transaktion **1106** kann auch Identifikationsinformationen in Bezug auf das Produkt, Produktparameterdaten (z. B. die Produkttemperatur wurde 2 Stunden lang auf 100°C gehalten) und Prozessparameterdaten (z. B. die Temperatur in der Heizung Y-001 beträgt 120°C) enthalten. Wenn die Transaktion **1106** als Reaktion auf ein auslösendes Ereignis generiert wird, kann die Transaktion **1106** auch Identifikationsinformationen für das auslösende Ereignis und Ereignisdaten aus dem auslösenden Ereignis enthalten, wie beispielsweise den Zeitpunkt des auslösenden Ereignisses, eine Dauer des auslösenden Ereignisses und/oder eine Beschreibung des auslösenden Ereignisses. In einigen Szenarien generieren mehrere Prozessanlageneinheiten Transaktionen als Reaktion auf dasselbe auslösende Ereignis und kommunizieren miteinander, um dem auslösenden Ereignis eine eindeutige Kennung zuzuweisen. Auf diese Weise kann eine Partei, beispielsweise eine Aufsichtsbehörde, die den Distributed Ledger prüft, jede der Transaktionen sehen, die mit demselben auslösenden Ereignis verbunden sind.

[0110] Darüber hinaus kann die Transaktion **1106** einen kryptographischen Hash der Produkt- und/oder Prozessparameterdaten zusammen mit Daten enthalten, die sich auf ein auslösendes Ereignis beziehen. In einer anderen Implementierung werden die Produktparameterdaten, Prozessparameterdaten und andere Daten, die sich auf ein auslösendes Ereignis beziehen, nicht als ein kryptographischer Hash gespeichert, sondern sind in Block **1104** für einen Beobachter oder einen anderen Netzwerkteilnehmer direkt zugänglich.

[0111] Wie oben beschrieben, können auslösende Ereignisse Alarme, Fehler, Lecks, Reparaturereignisse, Korrekturmaßnahmen usw. umfassen. In einem beispielhaften Szenario kann das auslösende Ereignis ein Leck in der Prozessanlage **10** sein, das durch das Öffnen eines Überdruckventils verursacht wird. Das Überdruckventil kann sich öffnen, wenn der Druck in dem Prozessleitsystem einen Schwellenwertbetrag für den Druck überschreitet oder das Überdruckventil sich proportional zu dem am Ventil erfassten Druckbetrag öffnen kann. Wenn sich das Überdruckventil öffnet, kann das Überdruckventil oder ein oder mehrere andere Feldgeräte den Zeitpunkt des Öffnens, die Dauer des Öffnens, die Größe des Öffnens, den Druck im Überdruckventil beim Öffnen, die Durchflussmenge von aus dem Überdruckventil austretenden Fluid und/oder Eigenschaften des Fluids wie die Temperatur des Fluids, die Art des Fluids usw. erfassen. In einigen Ausführungsformen kann die Menge des aus dem Überdruckventil aus-

tretenden Fluids auch auf der Grundlage der Durchflussmenge, der Größe des Öffnens und der Dauer des Öffnens des Überdruckventils bestimmt werden. Dann können das Überdruckventil und/oder ein oder mehrere andere Feldgeräte Transaktionen generieren, ähnlich der Transaktion **1106**, welche dieselbe eindeutige Kennung für das auslösende Ereignis und/oder dieselbe Beschreibung für das auslösende Ereignis eines Lecks enthalten, das durch das Öffnen des Überdruckventils verursacht wird. Jede der Transaktionen kann auch Prozessparameterdaten enthalten, wie den Zeitpunkt des Öffnens, die Größe des Öffnens, den Druck im Überdruckventil, die Durchflussrate des aus dem Überdruckventil austretenden Fluids usw. Die Transaktionen können auch Produktparameterdaten, wie z. B. die Eigenschaften des Fluids umfassen. Die Geräte, welche die Transaktionen generieren, leiten die Transaktionen dann an das Distributed-Ledger-Netzwerk weiter, um Knoten zu validieren, z. B. Edge-Gateways, um zu bestätigen, dass die Transaktionen gültig sind, und um die Transaktionen in den Distributed Ledger aufzunehmen.

[0112] Eine Aufsichtsbehörde, die den Vorfall prüft, kann Ereignisdaten vom Distributed Ledger anfordern und abrufen, die in Transaktionen, welche die auslösende Ereigniskennung aufweisen, enthalten sind. Das Computergerät der Aufsichtsbehörde, wie beispielsweise das Computergerät **235**, wie in **Fig. 2** gezeigt, kann dann die Ereignisdaten auf einer Benutzeroberfläche präsentieren. In anderen Ausführungsformen enthält der Distributed Ledger kryptographische Hashes der Ereignisdaten, die dem Computergerät **235** der Aufsichtsbehörde als Reaktion auf eine Aufforderung zur Authentifizierung der Ereignisdaten bereitgestellt werden. Die Ereignisdaten werden aus anderen Datenquellen wie beispielsweise einer Datenbank erhalten, die mit einem Servergerät **12** in der Prozessanlage **10** kommunikativ gekoppelt ist. Das Computergerät **235** der Aufsichtsbehörde berechnet dann einen kryptographischen Hash der erhaltenen Ereignisdaten und vergleicht den kryptographischen Hash der erhaltenen Ereignisdaten mit dem kryptographischen Hash der Ereignisdaten aus dem Distributed Ledger. Wenn die kryptographischen Hashes gleich sind, stellt das Computergerät **235** der Aufsichtsbehörde fest, dass die Ereignisdaten aus der Datenbank nicht manipuliert wurden. Andernfalls stellt das Computergerät **235** der Aufsichtsbehörde fest, dass die Ereignisdaten aus der Datenbank unzuverlässig sind.

Transaktionen zeichnen Prozessanlagendaten auf

[0113] Zusätzlich zum Aufzeichnen von Prozessparameterdaten und Produktparameterdaten in Transaktionen, die sich auf ein auslösendes Ereignis beziehen, können Prozess- und Produktparameterdaten in Transaktionen enthalten sein, die sich nicht auf ein auslösendes Ereignis beziehen, um beispielsweise genaue Aufzeichnungen der Operationen einer Prozessanlage **10** zu verwalten. Andere Arten von Prozessanlagendaten können ebenfalls in Transaktionen enthalten sein, wie beispielsweise Konfigurationsdaten, Benutzerinteraktionsdaten, Verwaltungsdaten, Inbetriebnahmedaten, Anlagennetzwerkdaten, Produktverfolgungsdaten oder andere geeignete Daten, die in einer Prozessanlage oder mehreren Prozessanlagen generiert werden oder damit zusammenhängen. Benutzerinteraktionsdaten können Operationen umfassen, die von einem Bediener oder einem Konfigurationstechniker beispielsweise an einem Bedienerarbeitsplatz ausgeführt werden. Der Bediener kann Sollwerte einstellen, auf Alarme reagieren usw., und zwar über Benutzersteuerungen an dem Bedienerarbeitsplatz, die in Transaktionen als Benutzerinteraktionsdaten enthalten sein können. Auf diese Weise kann die Prozessanlage **10**, wenn eine konkurrierende Einheit die Qualität eines in der Prozessanlage **10** hergestellten Produkts in Frage stellt, Prozessanlagendaten aus dem Distributed Ledger abrufen, die sich auf das Produkt beziehen. Die Prozessanlage **10** kann dann Aufzeichnungen von jeder der Prozessanlageneinheiten, die an der Herstellung des Produkts beteiligt sind, Parameterwerte für die Prozessanlageneinheiten bei der Herstellung des Produkts, Parameterwerte für das Produkt in verschiedenen Phasen des Herstellungsprozesses überprüfen, was Ereignisse auslöst, die während der Herstellung des Produkts usw. stattgefunden haben. Dementsprechend kann die Prozessanlage **10** bestimmen, ob das Produkt ordnungsgemäß hergestellt wurde, um bestimmte Qualitätsstandards zu erfüllen, oder ob eine Abnormalität während der Produktion auftrat, die dazu führte, dass das Produkt die Qualitätsstandards nicht erfüllte.

[0114] Die Prozessanlagendaten können auch verwendet werden, um eine Ursachenanalyse an Produkten durchzuführen. Beispielsweise können Produkte eine vorhergesagte Haltbarkeit aufweisen, wie beispielsweise Benzin, dessen Halbwertszeit weniger als einen Monat betragen kann. In einigen Ausführungsformen kann ein Computergerät die Haltbarkeit eines Produkts auf der Grundlage der Eigenschaften des Produkts vorhersagen, einschließlich Prozessparameterdaten und Produktparameterdaten, die im Distributed Ledger aufgezeichnet wurden, während das Produkt hergestellt wurde. Das Computergerät kann auch die Haltbarkeit des Produkts auf der Grundlage von historischen Daten für ähnliche Produkte mit ähnlichen Komponenten und/oder Prozessparameterdaten und Produktparameterdaten während der Herstellung vorhersagen. Insbesondere kann das Computergerät die Haltbarkeit eines Produkts auf der Grundlage der durchschnittlichen Haltbarkeit desselben Produkttyps (z. B. Benzin) vorhersagen.

[0115] Das Computergerät kann dann die vorhergesagte Haltbarkeit von der durchschnittlichen Haltbarkeit auf der Grundlage der Qualität der Komponenten in dem Produkt erhöhen oder verringern. Beispielsweise können Komponenten als überdurchschnittlich, durchschnittlich oder unterdurchschnittlich eingestuft werden. Komponentenangaben können in einer Datenbank mit zugehörigen Rangfolgen oder Qualitätsbewertungen gespeichert werden. Komponenten mit einem Qualitätsfaktor unter einem ersten Schwellenwert oder einem Rang unter einem ersten Schwellenwert können als unterdurchschnittlich eingestuft werden. Komponenten mit einer Qualitätsbewertung über einer ersten Schwellenwertbewertung und unter einer zweiten Schwellenwertbewertung oder die über dem ersten Schwellenwert und unter einem zweiten Schwellenwert liegen, können als durchschnittlich eingestuft werden. Komponenten mit einer Qualitätsbewertung über der zweiten Schwellenwertbewertung oder die über dem zweiten Schwellenwert liegen, können als überdurchschnittlich eingestuft werden.

[0116] Das Computergerät kann die vorhergesagte Haltbarkeit in Abhängigkeit von den Eigenschaften des Produkts, wie beispielsweise einer Temperatur des Produkts, einem Volumen des Produkts, einer Masse des Produkts, einer Dichte des Produkts, einem Druck des Produkts, einer Viskosität des Produkts, einer chemischen Zusammensetzung des Produkts usw. weiter erhöhen oder verringern. Beispielsweise kann das Computergerät jeder Eigenschaft eine Qualitätsbewertung zuweisen und die vorhergesagte Lagerfähigkeit auf der Grundlage von jeder der Qualitätsbewertungen anpassen.

[0117] In einigen Ausführungsformen kann das Computergerät ein maschinelles Lernmodell generieren, um die Haltbarkeit eines Produkts auf der Grundlage der tatsächlichen Haltbarkeit vorheriger Produkte, der Komponenten in den vorherigen Produkten und der Eigenschaften der vorherigen Produkte vorherzusagen.

[0118] Wenn die tatsächliche Haltbarkeit eines Produkts von der vorhergesagten Haltbarkeit abweicht, kann das Computergerät außerdem Prozessanlagendaten, die sich auf das Produkt beziehen, aus dem Distributed Ledger abrufen, um die Ursache zu identifizieren. Beispielsweise kann die tatsächliche Haltbarkeit aufgrund von Komponenten mit schlechter Qualität im Produkt geringer sein als die vorhergesagte Haltbarkeit. In einem anderen Beispiel kann die tatsächliche Haltbarkeit geringer als die vorhergesagte Haltbarkeit sein, da eine Heizung in der Prozessanlage **10** das Produkt auf eine unerwünschte Temperatur erwärmt.

Transaktionen welche die Produktüberwachungskette über Produktverfolgungsdaten aufzeichnet

[0119] Um genaue Aufzeichnungen der Produktüberwachungskette von Produkten in einer Lieferkette zu erhalten, können Transaktionen generiert werden, die Identifikationsinformationen für die Quelle oder den Lieferanten eines Produkts und die mit dem Produkt befassten Einheiten wie Hersteller, Händler, Vertriebseinrichtungen, Einzelhändler und den Kunden, der das Produkt kauft, umfassen. Insbesondere können die Transaktionen Produktverfolgungsdaten, welche Identifikationsinformationen für das Produkt, Identifikationsinformationen für den Lieferanten/Hersteller des Produkts, Identifikationsinformationen für Hersteller/Anbieter jeder der Komponenten des Produkts, Identifikationsinformationen für Einheiten in der Lieferkette enthalten, die das Produkt erhalten und handhaben, Identifikationsinformationen für Einzelhändler, die das Produkt verkaufen, und/oder Identifikationsinformationen für Kunden, die das Produkt kaufen, enthalten. Wenn das Produkt von einer Einheit (z. B. einer Prozessanlage) an eine andere Einheit (z. B. ein Lagerhaus) geliefert wird, kann die liefernde Einheit eine Transaktion generieren, die Identifikationsinformationen für die liefernde Einheit, Identifikationsinformationen für die empfangende Einheit und eine Angabe umfasst, dass das Produkt an die empfangende Einheit übertragen wird.

[0120] Dementsprechend kann ein Benutzer wie beispielsweise ein Kunde über eine Benutzeroberflächenvorrichtung jede der Transaktionen, die ein bestimmtes Produkt betreffen, aus dem Distributed Ledger unter Verwendung der Identifikationsinformationen für das Produkt abrufen. Die Benutzeroberflächenvorrichtung kann dann über eine Benutzeroberfläche Angaben des Lieferanten oder die Herkunft des Produkts und der Einheiten, die das Produkt gehandhabt haben, wie Hersteller, Händler, Vertriebseinrichtungen, Einzelhändler und den Kunden, der das Produkt kauft, anzeigen. Die Benutzeroberflächenvorrichtung kann auch Angaben der Komponenten des Produkts über die Benutzeroberfläche anzeigen. Der Benutzer kann dann jede der Transaktionen, die eine bestimmte Komponente des Produkts betreffen, aus dem Distributed Ledger unter Verwendung von Identifikationsinformationen für die Komponente abrufen. Dann kann die Benutzeroberflächenvorrichtung über die Benutzeroberfläche Angaben des Lieferanten oder der Herkunft der Komponente und der Einheiten, welche die Komponente gehandhabt haben, wie Hersteller, Händler, Vertriebseinrichtungen usw., anzeigen.

[0121] In einigen Ausführungsformen kann die Produktverpackung eine Produktkennung enthalten, wie beispielsweise einen Barcode oder ein RFID- (Radio Frequency Identification)-Tag, der beim Scannen Da-

ten aus dem Distributed Ledger für das Produkt bereitstellt. Beispielsweise kann ein Benutzer den Barcode oder das RFID-Tag über ein Mobilgerät scannen, das dann Angaben zum Lieferanten oder zur Herkunft des Produkts sowie zu den Einheiten, die das Produkt auf dem Mobilgerät gehandhabt haben, anzeigt.

[0122] **Fig. 12** zeigt ein Flussdiagramm, das ein beispielhaftes Verfahren **1200** zum Aufzeichnen von Daten in einem Prozessleitsystem unter Verwendung eines Distributed Ledgers darstellt. Das Verfahren **1200** kann von einem Feldgerät **15-22**, **40-46** in der Prozessanlage **10**, einer Steuerung **11** in der Prozessanlage **10** oder einem anderen Computergerät in der Prozessanlage **10**, wie einem Bedienerarbeitsplatz, einem Servergerät **12**, einer Benutzeroberflächenvorrichtung **8**, einem E/A-Gerät **26**, **28**, einem Netzwerkgerät **35** usw. ausgeführt werden.

[0123] Bei Block **1202** werden Daten, die sich auf ein Prozesssteuerungselement beziehen, von einem Feldgerät erhalten. Das Prozesssteuerungselement kann ein Feldgerät, eine Steuerung oder eine Prozessanlageneinheit wie ein Ventil, ein Tank, ein Mischer, eine Pumpe, ein Wärmetauscher usw. sein. Die Daten können Prozessanlagendaten wie beispielsweise Prozessparameterdaten für Parameter des Prozesssteuerungselements (z. B. ein Tankfüllstand, eine Pumpendrehzahl, die Temperatur in einem Wärmetauscher) und Produktparameterdaten für ein Produkt, das in das Prozesssteuerungselement eintritt, aus diesem austritt und/oder von diesem gesteuert wird (z. B. die Temperatur eines Fluids in einem Tank, die Durchflussrate des aus einem Ventil austretenden Fluids) sein. Dann wird bei Block **1204** eine Transaktion generiert, welche die Prozessanlagendaten enthält, die sich auf das Prozesssteuerungselement beziehen. Die Einheit (z. B. ein Feldgerät), welche die Transaktion generiert, signiert die Transaktion mit einer für die Einheit eindeutigen kryptographischen Signatur (Block **1206**) und ergänzt die Transaktion mit Identitätsdaten für die Einheit, wie beispielsweise einem öffentlichen kryptographischen Schlüssel, welcher der Einheit gehört (Block **1208**). Beispielsweise kann die Transaktion durch einen privaten kryptographischen Schlüssel signiert werden, der dem öffentlichen kryptographischen Schlüssel entspricht, welcher der Einheit gehört.

[0124] Bei Block **1210** wird die Transaktion an einen Teilnehmer in dem Distributed-Ledger-Netzwerk übermitteln. Beispielsweise kann ein Feldgerät die Transaktion an das Distributed-Ledger-Netzwerk senden. Ein Validierungsknoten wie ein Edge-Gateway kann dann bestätigen, dass die Transaktion gültig ist, die Transaktion einem Transaktionsblock hinzufügen, ein kryptographisches Puzzle lösen und die Lösung in den neu generierten Block als Nachweis für die zum Generieren des Blocks geleistete Arbeit aufnehmen. Der Validierungsknoten kann dann den neu generierten Block an jeden der anderen Validierungsknoten in dem Distributed-Ledger-Netzwerk liefern, um den neu generierten Block in deren jeweilige Kopien des Distributed Ledgers aufzunehmen.

[0125] In einigen Ausführungsformen bestätigt der Validierungsknoten die Transaktion anhand eines Satzes von Konsensregeln und fügt die Transaktion einem Block hinzu, wenn die Transaktion jede der Konsensregeln erfüllt. Beispielsweise kann eine Konsensregel beinhalten, dass der Urheber einer Transaktion einen Identitätsnachweis vorlegt, so dass nur genehmigte Einheiten Transaktionen in dem Distributed Ledger verursachen können. Eine Konsensregel kann erfordern, dass die Blöcke und Transaktionen Formatanforderungen erfüllen und bestimmte Meta-Informationen in Bezug auf die Transaktion liefern (z. B. müssen Blöcke unterhalb einer Größenbeschränkung sein, Transaktionen müssen eine Reihe von Feldern usw. enthalten). Jede Transaktion, welche die Konsensregel nicht erfüllt, wird ignoriert, indem Knoten überprüft werden, welche die Transaktion empfangen, und die Transaktion wird nicht an andere Knoten weitergegeben.

[0126] Der Validierungsknoten umfasst einen Transceiver zur Kommunikation mit Feldgeräten, Steuerungen oder anderen Computergeräten in der Prozessanlage **10**, die Transaktionen, welche Daten des Distributed Ledgers wie Prozessanlagendaten aufweisen, senden. Zusätzlich kann der Validierungsknoten einen Speicher zum Speichern einer Kopie des Distributed Ledgers enthalten, einschließlich einer Zustandsdatenbank zum Speichern von Zuständen von Smart Contracts, die auf dem Distributed Ledger bereitgestellt sind. Ferner kann der Validierungsknoten Anwendungen enthalten, wie beispielsweise einen Prozessdatenvalidierer, der einen Satz von Konsensregeln auf die dezentralen Ledgerdaten anwendet und die Daten des Distributed Ledgers an die Kopie des Validierungsknotens des Distributed Ledgers anfügt, wenn die Daten des Distributed Ledgers die Konsensregeln erfüllen.

[0127] **Fig. 13** zeigt ein Flussdiagramm, das ein beispielhaftes Verfahren **1300** zum sicheren Messen nicht vertrauenswürdiger Daten in einem Prozessleitsystem unter Verwendung eines Distributed Ledgers darstellt. Das Verfahren **1300** kann von einem Feldgerät **15-22**, **40-46** in der Prozessanlage **10**, einer Steuerung **11** in der Prozessanlage **10** oder einem anderen Computergerät in der Prozessanlage **10**, wie einem Bedienerarbeitsplatz, einem Servergerät **12**, einer Benutzeroberflächenvorrichtung **8**, einem E/A-Gerät **26**, **28**, einem Netzwerkgerät **35** usw. ausgeführt werden. Das Verfahren **1300** kann auch von einem Validierungsknoten wie einem Edge-Gateway oder einer Kombination aus einem Feldgerät und einem Validierungsknoten ausgeführt werden.

[0128] Bei Block **1302** werden Daten, die sich auf ein Prozesssteuerungselement beziehen, von einem Feldgerät erhalten. Das Prozesssteuerungselement kann ein Feldgerät, eine Steuerung oder eine Prozessanlageneinheit wie ein Ventil, ein Tank, ein Mischer, eine Pumpe, ein Wärmetauscher usw. sein. Die Daten können Prozessanlagendaten wie beispielsweise Prozessparameterdaten für Parameter des Prozesssteuerungselements (z. B. ein Tankfüllstand, eine Pumpendrehzahl, die Temperatur in einem Wärmetauscher) und Produktparameterdaten für ein Produkt, das in das Prozesssteuerungselement eintritt, aus diesem austritt und/oder von diesem gesteuert wird (z. B. die Temperatur eines Fluids in einem Tank, die Durchflussrate des aus einem Ventil austretenden Fluids) sein. Dann wird in Block **1304** eine Transaktion generiert, welche die Prozessanlagendaten enthält, die sich auf das Prozesssteuerungselement beziehen. Die die Transaktion generierende Einheit (z. B. ein Feldgerät) signiert die Transaktion mit einer für die Einheit eindeutigen kryptographischen Signatur und ergänzt die Transaktion mit Identitätsdaten für die Einheit, z. B. einem öffentlichen kryptographischen Schlüssel, welcher der Einheit gehört. Beispielsweise kann die Transaktion durch einen privaten kryptographischen Schlüssel signiert werden, der dem öffentlichen kryptographischen Schlüssel entspricht, welcher der Einheit gehört.

[0129] Bei Block **1306** wird die Transaktion an einen Teilnehmer in einem lokalen Distributed-Ledger-Netzwerk übermitteln. Es kann mehrere lokale Distributed Ledger geben, wobei jedes lokale Distributed Ledger von einer anderen Partei oder einer anderen Prozessanlage verwaltet wird. Beispielsweise kann ein lokales Distributed-Ledger-Netzwerk für die Anlage A aus Edge-Gateways in der Anlage A bestehen. Die Edge-Gateways können Transaktionen aufzeichnen, die Prozessanlagendaten enthalten, die sich auf Ereignisse und Geräte in der Anlage A beziehen. Transaktionen werden für einen bestimmten Zeitraum oder eine bestimmte Epoche dann zu dem lokalen Distributed-Ledger-Netzwerk hinzugefügt. Nachdem der Schwellenwertzeitraum abgelaufen ist (Block **1308**), stellen die Validierungsknoten, die den lokalen Distributed Ledger verwalten, die Transaktionen oder Transaktionsblöcke, die während des Schwellenwertzeitraums generiert wurden, einem globalen Distributed-Ledger-Netzwerk (Block **1310**) zur Verfügung. Das globale Distributed-Ledger-Netzwerk kann das Validieren von Knoten über mehrere Prozessanlagen hinweg umfassen, beispielsweise einen Cloud-Dienst mit mehreren Cloud-Computing-Systemen. Die Validierungsknoten können für jede Prozessanlage einen globalen Distributed Ledger (z. B. eine globale Blockchain) verwalten. Dann können die Validierungsknoten im lokalen Distributed-Ledger-Netzwerk Blöcke aus dem lokalen Distributed Ledger entfernen oder beschneiden, die dem globalen Distributed Ledger bereitgestellt wurden, das nicht der letzte Block ist. Die Validierungsknoten für den lokalen Distributed Ledger können weiterhin Blöcke generieren, die Blöcke nach Ablauf jeder Zeitepoche an das globale Distributed-Ledger-Netzwerk senden und lokale Kopien der Blöcke entfernen, wenn die Blöcke der globalen Blockchain hinzugefügt wurden.

[0130] In einigen Ausführungsformen wird auch jede der globalen Blockchains für die jeweiligen Einheiten oder Prozessanlagen kombiniert, um eine Superblockchain, welche Zustandsblöcke aufweist, zu generieren. Jeder Zustandsblock enthält jeden der Blöcke aus den globalen Blockchains, die einem bestimmten Zeitraum oder einer bestimmten Epoche entsprechen.

[0131] **Fig. 14** zeigt ein Flussdiagramm, das ein beispielhaftes Verfahren **1400** zum Aufzeichnen von Qualitätskontroll-, Produktions- oder regulatorischen Daten in einem Prozesskontrollsystem unter Verwendung eines Distributed Ledgers darstellt. Das Verfahren **1400** kann von einem Feldgerät **15-22**, **40-46** in der Prozessanlage **10**, einer Steuerung **11** in der Prozessanlage **10** oder einem anderen Computergerät in der Prozessanlage **10**, wie einem Bedienerarbeitsplatz, einem Servergerät **12**, einer Benutzeroberflächenvorrichtung **8**, einem E/A-Gerät **26**, **28**, einem Netzwerkgerät **35** usw. ausgeführt werden.

[0132] Bei Block **1402** wird ein auslösendes Ereignis in Bezug auf die Qualitätskontrolle durch ein Prozesssteuerungselement erfasst. Das auslösende Ereignis kann ein Alarm, ein Fehler, ein Leck, ein Reparaturereignis, ein Prozessmeilenstein, eine Korrekturmaßnahme usw. sein. In einigen Ausführungsformen wird eine Angabe des auslösenden Ereignisses einem Feldgerät, einer Steuerung oder einem anderen Computergerät in der Prozessanlage **10** bereitgestellt. In anderen Ausführungsformen erfasst das Feldgerät, die Steuerung oder ein anderes Computergerät das auslösende Ereignis.

[0133] In jedem Fall werden bei Block **1404** Ereignisdaten für das auslösende Ereignis erhalten. Die Ereignisdaten können eine eindeutige Kennung für das auslösende Ereignis, einen Zeitpunkt des auslösenden Ereignisses, eine Dauer des auslösenden Ereignisses, eine Beschreibung des auslösenden Ereignisses, Identifikationsinformationen für die am auslösenden Ereignis beteiligten Prozesssteuerungselemente, Identifikationsinformationen für ein Produkt enthalten, das von den Prozesssteuerungselementen während des ausgelösten Ereignisses usw. hergestellt wird. Dann wird bei Block **1406** eine Transaktion generiert, welche die Ereignisdaten und/oder einen kryptographischen Hash der Ereignisdaten für das auslösende Ereignis enthält. Die Transaktion kann auch Identifikationsinformationen für den Urhe-

ber der Transaktion, Produktparameterdaten für das Produkt, als das auslösende Ereignis stattfand, Prozessparameterdaten für Prozesssteuerungselemente während des auslösenden Ereignisses oder andere geeignete Informationen enthalten. In einigen Ausführungsformen können mehrere Feldgeräte, Steuerungen oder andere Computergeräte in der Prozessanlage **10** Transaktionen generieren, die sich auf das auslösende Ereignis beziehen. Beispielsweise kann ein erstes Feldgerät eine Transaktion generieren, welche die Temperatur in einer Heizung zum Zeitpunkt des auslösenden Ereignisses enthält, während ein zweites Feldgerät eine Transaktion generieren kann, welche die Drehzahl einer Pumpe zum Zeitpunkt des auslösenden Ereignisses enthält.

[0134] Bei Block **1408** wird die Transaktion an einen Teilnehmer in dem Distributed-Ledger-Netzwerk übermitteln. Beispielsweise kann ein Feldgerät die Transaktion an das Distributed-Ledger-Netzwerk senden. Ein Validierungsknoten wie ein Edge-Gateway kann dann bestätigen, dass die Transaktion gültig ist, die Transaktion einem Transaktionsblock hinzufügen, ein kryptographisches Puzzle lösen und die Lösung in den neu generierten Block als Nachweis für die zum Generieren des Blocks geleistete Arbeit aufnehmen. Der Validierungsknoten kann dann den neu generierten Block an jeden der anderen Validierungsknoten in dem Distributed-Ledger-Netzwerk liefern, um den neu generierten Block in deren jeweilige Kopien des Distributed Ledgers aufzunehmen.

[0135] Wie oben beschrieben, kann die Transaktion einen kryptographischen Hash der Ereignisdaten für das auslösende Ereignis und/oder eine Kombination der Ereignisdaten für das auslösende Ereignis und anderer Prozessanlagendaten in Bezug auf das auslösende Ereignis enthalten. Zusätzlich zum Generieren der Transaktion kann das Feldgerät die Ereignisdaten oder andere Prozessanlagendaten, die sich auf das auslösende Ereignis beziehen, einem Servergerät **12** bereitstellen, um sie beispielsweise in einer Datenbank zu speichern (Block **1410**).

[0136] Dann werden zum Authentifizieren der Ereignisdaten die in der Datenbank gespeicherten Ereignisdaten mit dem kryptographischen Hash verglichen, der in dem Distributed Ledger enthalten ist (Block **1412**). Wenn eine Übereinstimmung vorliegt, wurden die Ereignisdaten nicht manipuliert. Beispielsweise kann eine Aufsichtsbehörde, die einen Vorfall prüft, kryptographische Hashes von Ereignisdaten von dem Distributed Ledger anfordern und abrufen, das in Transaktionen mit der auslösenden Ereigniskennung enthalten ist. Die Ereignisdaten werden aus anderen Datenquellen wie beispielsweise einer Datenbank erhalten, die mit einem Servergerät **12** in der Prozessanlage **10** kommunikativ gekoppelt ist. Das Computergerät der Aufsichtsbehörde berechnet dann einen kryptographischen Hash der erhaltenen Ereignisdaten und vergleicht den kryptographischen Hash der erhaltenen Ereignisdaten mit dem kryptographischen Hash der Ereignisdaten aus dem Distributed Ledger. Wenn die kryptographischen Hashes identisch sind, stellt das Computergerät der Aufsichtsbehörde fest, dass die Ereignisdaten aus der Datenbank nicht manipuliert wurden. Andernfalls stellt das Computergerät der Aufsichtsbehörde fest, dass die Ereignisdaten aus der Datenbank unzuverlässig sind. In anderen Ausführungsformen ruft ein Computergerät in der Prozessanlage **10** die in der Datenbank gespeicherten Ereignisdaten und den kryptographischen Hash der Ereignisdaten aus dem Distributed Ledger ab und vergleicht die Ereignisdaten mit dem kryptographischen Hash, um die Ereignisdaten zu authentifizieren.

[0137] **Fig. 15** zeigt ein Flussdiagramm, das ein beispielhaftes Verfahren **1500** zum Aufzeichnen von Software- oder Firmware-Zuständen in einem Prozessleitsystem und einer verbundenen Instrumentierung unter Verwendung eines Distributed Ledgers darstellt. Das Verfahren **1500** kann von einem Feldgerät **15-22**, **40-46** in der Prozessanlage **10**, einer Steuerung **11** in der Prozessanlage **10** oder einem anderen Computergerät in der Prozessanlage **10**, wie einem Bedienerarbeitsplatz, einem Servergerät **12**, einer Benutzeroberflächenvorrichtung **8**, einem E/A-Gerät **26**, **28**, einem Netzwerkgerät **35** usw. ausgeführt werden.

[0138] Bei Block **1502** wird ein aktueller Zustand von Software oder Firmware erhalten, die auf einem Gerät in der Prozessanlage **10** ausgeführt werden. Beispielsweise kann ein Gerät in der Prozessanlage **10**, das ein Software- oder Firmware-Upgrade erhält, die neue Version der Software oder Firmware erhalten. Das Gerät kann einen Bedienerarbeitsplatz, eine andere Benutzeroberflächenvorrichtung **8**, ein Servergerät **12**, eine Steuerung **11**, ein E/A-Gerät **26**, **28**, ein Netzwerkgerät **35**, ein Feldgerät **15-22**, **40-46** usw. sein. Dann kann das Gerät bei Block **1504** eine Transaktion generieren, die eine Angabe des aktuellen Zustands der Software oder Firmware enthält. Beispielsweise kann die Angabe ein kryptographischer Hash der Softwareanweisungen für die neue Version der Software sein. Die Transaktion kann auch einen Urheber, der die durch einen kryptographischen Identitätsnachweis identifizierte Software oder Firmware ändert, Identifikationsinformationen für das Gerät, das die Software oder Firmware ausführt, eine Beschreibung des Upgrades, eine Uhrzeit und ein Datum des Upgrades usw. enthalten.

[0139] Bei Block **1506** wird die Transaktion an einen Teilnehmer in dem Distributed-Ledger-Netzwerk übermitteln. Beispielsweise kann ein Computergerät die Transaktion an das Distributed-Ledger-Netzwerk senden. Ein Validierungsknoten wie ein Edge-Gateway kann dann bestätigen, dass die Transaktion gül-

tig ist, die Transaktion einem Transaktionsblock hinzufügen, ein kryptographisches Puzzle lösen und die Lösung in den neu generierten Block als Nachweis für die zum Generieren des Blocks geleistete Arbeit aufnehmen. Der Validierungsknoten kann dann den neu generierten Block an jeden der anderen Validierungsknoten in dem Distributed-Ledger-Netzwerk liefern, um den neu generierten Block in deren jeweilige Kopien des Distributed Ledgers aufzunehmen.

[0140] In einigen Ausführungsformen bestätigt der Validierungsknoten die Transaktion anhand eines Satzes von Konsensregeln und fügt die Transaktion einem Block hinzu, wenn die Transaktion jede der Konsensregeln erfüllt. In einigen Ausführungsformen geben die Konsensregeln auch an, dass nur autorisierte Benutzer Software- oder Firmware-Aktualisierungen auf dem Distributed Ledger aufzeichnen dürfen. Dementsprechend validieren die Validierungsknoten die Transaktion, wenn die Transaktion an den Distributed Ledger gesendet wird, wenn der Urheber ein autorisierter Benutzer ist. Wenn der Urheber kein autorisierter Benutzer ist, ist die Transaktion nicht im Distributed Ledger enthalten und die Aktualisierung der Software stimmt nicht mit der neuesten Version der Software überein, die im Distributed Ledger aufgezeichnet ist.

[0141] In jedem Fall wird bei Block **1508** ein Software- oder Firmware-Zustand erhalten, der auf dem Gerät in der Prozessanlage **10** ausgeführt wird. Beispielsweise kann eine Servergerät **12** oder ein anderes Computergerät in der Prozessanlage **10** kontinuierlich oder periodisch (z. B. einmal pro Sekunde, einmal pro Minute, einmal pro Stunde, einmal pro Tag usw.) aktuelle Versionen von Software und Firmware erhalten, die auf Geräten in der Prozessanlage **10** läuft. Der Zustand der Software oder Firmware, der an dem Servergerät **12** erhalten wird, wird dann mit dem kryptographischen Hashwert für die Software oder Firmware verglichen, der in dem Distributed Ledger gespeichert ist, um sicherzustellen, dass die Software oder Firmware nicht manipuliert wurde (Block **1510**). Wenn der Zustand der Software oder Firmware mit dem kryptographischen Hashwert für die Software oder Firmware übereinstimmt, der im Distributed Ledger gespeichert ist, wird die Software oder Firmware auf dem Gerät weiter ausgeführt (Block **1514**). Andernfalls stellt das Servergerät **12** fest, dass die Software manipuliert wurde, und verhindert, dass das Gerät die Software in ihrem aktuellen Zustand ausführt (Block **1512**). In einigen Ausführungsformen lädt das Servergerät **12** dann den vorherigen Zustand der Software auf das Gerät herunter, und das Gerät nimmt die Ausführung der Software in ihrem vorherigen Zustand wieder auf.

[0142] **Fig. 16** zeigt ein Flussdiagramm, das ein beispielhaftes Verfahren **1600** zum Erstellen von Smart Contracts in einem Prozessleitsystem unter Verwendung eines Distributed Ledgers darstellt. Das Verfahren **1600** kann von einem Feldgerät **15-22**, **40-46** in der Prozessanlage **10**, einer Steuerung **11** in der Prozessanlage **10** oder einem anderen Computergerät in der Prozessanlage **10**, wie einem Bedienerarbeitsplatz, einem Servergerät **12**, einer Benutzeroberflächenvorrichtung **8**, einem E/A-Gerät **26**, **28**, einem Netzwerkgerät **35** usw. ausgeführt werden.

[0143] Bei Block **1602** wird ein Smart Contract generiert, der sich auf eine oder mehrere Prozessanlagen bezieht. Beispielsweise kann der Smart Contract einen Tokenwert von der Anlage A an die Anlage B übertragen, wenn die Anlage A ein Produkt von der Anlage B erhält, das bestimmte Qualitätsstandards erfüllt. Ein anderer beispielhafter Smart Contract in einem Prozessleitsystem kann einen Smart Contract für eine Aufforderung zum sicheren Schreiben enthalten, der es dem Anlagenpersonal ermöglicht, Parameterdaten in ein SIS-Gerät in der Prozessanlage **10** zu schreiben. Noch ein weiteres Beispiel für einen Smart Contract in einem Prozessleitsystem kann einen Smart Contract für Geräteinformationen enthalten, der Geräteinformationen von einem Gerät erhält, bei dem ein Fehler aufgetreten ist, und die Geräteinformationen einem Gerätelieferanten als Reaktion auf den Empfang einer Aufforderung zum Teilen der Geräteinformationen bereitstellt.

[0144] Bei Block **1604** wird der Smart Contract einer Adresse bereitgestellt, die im Distributed Ledger gespeichert ist. Der verteilte Smart Contract kann anderen Teilnehmern Verfahren und Daten im Distributed-Ledger-Netzwerk offenbaren. Einige der Daten im Zustand des Smart Contract können private Daten sein, die nur durch Aufrufen eines Verfahrens des Smart Contracts oder nur durch autorisierte Distributed Ledger-Teilnehmer geändert werden können. Eine Möglichkeit zum Ändern des Zustand des Smart Contracts besteht darin, eine Transaktion an das Distributed-Ledger-Netzwerk zu senden. Wenn die gesendete Transaktion den Konsensregeln entspricht, können Netzwerkvalidierer die Transaktion in den Distributed Ledger aufnehmen.

[0145] In einigen Ausführungsformen führen Validierungsknoten, wie z. B. Edge-Gateways den in dem Smart Contract enthaltenen Code aus, und die Feldgeräte fungieren als Nachweis-Orakel und stellen Nachweistransaktionen bereit, die den Zustand des Smart Contracts ändern.

[0146] **Fig. 17** zeigt ein Flussdiagramm, das ein beispielhaftes Verfahren **1700** zum Interagieren mit einem Smart Contract in einem Prozessleitsystem unter Verwendung eines Distributed Ledgers darstellt. Das Verfahren **1700** kann von einem Feldgerät **15-22**, **40-46** in der Prozessanlage **10**, einer Steuerung **11** in der Prozessanlage **10** oder einem anderen Computergerät in der Prozessanlage **10**, wie ei-

nem Bedienerarbeitsplatz, einem Servergerät **12**, einer Benutzeroberflächenvorrichtung **8**, E/A-Gerät **26**, **28**, einem Netzwerkgerät **35** usw. ausgeführt werden.

[0147] Bei Block **1702** werden Ereignisdaten von einem Ereignis erhalten, das in der Prozessanlage **10** stattfindet. Ein Ereignis kann ein Produkt sein, das von einer Prozessanlage **10** geliefert oder empfangen wird, die Fertigstellung eines in der Prozessanlage **10** hergestellten Produkts, eine Änderung der Eigenschaften eines Produkts, eine Änderung eines Prozessparameterwerts, ein auslösendes Ereignis B. ein Alarm, ein Fehler, ein Leck, ein Reparaturereignis, eine Korrekturmaßnahme, eine Benutzerinteraktion, z. B. eine Aufforderung zum Schreiben auf ein SIS-Gerät, eine Aufforderung zum Bereitstellen von Geräteinformationen an einen Gerätelieferanten oder eine Aufforderung zum Übertragen eines Tokenwerts, wenn ein bestimmtes Produkt empfangen wird, oder ein anderes geeignetes Ereignis, das in der Prozessanlage **10** stattfindet. Die Ereignisdaten können Prozessparameterdaten, Produktparameterdaten, Konfigurationsdaten, Benutzerinteraktionsdaten, Verwaltungsdaten, Inbetriebnahmedaten, Anlagennetzwerkdaten, Produktverfolgungsdaten oder andere geeignete Daten in Bezug auf das Ereignis, wie z. B. Datum und Uhrzeit des Ereignisses, die Dauer des Ereignisses, eine Beschreibung des Ereignisses usw. enthalten.

[0148] Dann wird bei Block **1704** eine Transaktion generiert, welche die Ereignisdaten und Identifikationsinformationen für die Einheit enthält, welche die Transaktion generiert, wie beispielsweise einen kryptographischen öffentlichen Schlüssel, welcher der Einheit zugewiesen ist. Die Transaktion kann kryptographisch signiert sein, um einen kryptographischen Identitätsnachweis der die Transaktion generierenden Einheit bereitzustellen. Bei Block **1706** wird die Transaktion an die Adresse in dem Distributed Ledger übermitteln, in dem der Smart Contract implementiert ist. Auf diese Weise ändern Validierungsknoten wie z. B. Edge-Gateways, den Zustand des Smart Contracts gemäß den in der Transaktion enthaltenen Ereignisdaten.

[0149] Beispielsweise kann ein Smart Contract einen Tokenwert von der Anlage A an die Anlage B übertragen, wenn die Anlage A ein Produkt von der Anlage B erhält, das bestimmte Qualitätsstandards erfüllt. Ein Feldgerät in der Anlage A kann eine Transaktion generieren, die Ereignisdaten enthält, die sich auf die Qualität des Produkts beziehen, z. B. Identifikationsinformationen für die Anlage A, Identifikationsinformationen für das Produkt, einen Hinweis darauf, dass das Produkt von der Anlage B empfangen wurde, und Produktparameterdaten, welche Eigenschaften des Produkts beschreiben (z. B. die Temperatur des Produkts, das Volumen des Produkts, die Dichte des Produkts, die Viskosität des Produkts oder die chemische Zusammensetzung des Produkts). Das Feldgerät kann die Transaktion einer Adresse für den Smart Contract bereitstellen, und die Validierungsknoten können den Zustand des Smart Contracts so ändern, dass er die Produktparameterdaten enthält. In einigen Ausführungsformen vergleicht der Smart Contract die Eigenschaften des Produkts, die in den Produktparameterdaten enthalten sind, mit einem Satz von Mindestschwellenwertanforderungen für das Produkt, um die entsprechenden Qualitätsstandards zu erfüllen. Wenn das Produkt die Qualitätsstandards erfüllt, kann der Smart Contract den Tokenwert an die Anlage B übertragen. In einigen Ausführungsformen kann ein Feldgerät in der Anlage B eine Transaktion generieren, die Ereignisdaten enthält, die sich auf die Qualität des Produkts beziehen, wie z. B. Prozessparameterdaten, die Parameterwerte für Prozessanlageneinheiten in der Anlage B beschreiben, die an der Herstellung des Produkts beteiligt sind, wobei die Parameterwerte während der Herstellung des Produkts erfasst werden.

[0150] Die Ausführungsformen der in der vorliegenden Offenbarung beschriebenen Techniken können eine beliebige Anzahl der folgenden Aspekte - entweder allein oder in Kombination - enthalten:

1. Validierungs-Netzwerkknoten in einer Prozessanlage in einem Distributed-Ledger-Netzwerk, umfassend: einen Transceiver, der konfiguriert ist, um mit einem oder mehreren Feldgeräten zu kommunizieren, die jeweils eine physische Funktion ausführen, um einen industriellen Prozess in der Prozessanlage zu steuern und Daten des Distributed Ledgers mit Peer-Netzwerkknoten auszutauschen, wobei die Daten des Distributed Ledgers Transaktionen umfassen, welche Prozessanlagendaten aufweisen; ein Speichermedium, das zum Speichern einer Kopie des Distributed Ledgers konfiguriert ist; und einen Prozessdatenvalidierer, der konfiguriert ist, um einen Satz von Konsensregeln auf die von den Peer-Netzwerkknoten empfangenen Daten des Distributed Ledgers anzuwenden, wobei der Prozessdatenvalidierer ferner konfiguriert ist, um die von den Peer-Netzwerkknoten erhaltenen Daten des Distributed Ledgers an die Kopie des Distributed Ledgers anzuhängen, wenn die Daten des Distributed Ledgers den Konsensregeln entsprechen.

2. Validierungs-Netzwerkknoten nach Aspekt 1, wobei die Daten des Distributed Ledgers, die von den Peer-Knoten erhalten wurden, einen Identitätsnachweis einer Einheit enthalten, welche eine Transaktion generiert, welche Prozessanlagendaten aufweist.

3. Validierungs-Netzwerkknoten nach einem der vorhergehenden Aspekte, wobei Daten des Distributed Ledgers, die von den Peer-Knoten erhalten wurden, anzuhängen sind, wobei der

Transaktionsvalidierer konfiguriert ist, um: ein kryptographisches Puzzle zu lösen, das auf einem Transaktionsblock basiert; die Lösung des kryptographischen Puzzles zum Transaktionsblock hinzuzufügen; den Transaktionsblock an die Kopie des Distributed Ledgers anzuhängen; und den Transaktionsblock an mindestens einen der Peer-Netzwerkknoten im Distributed-Ledger-Netzwerk zu übermitteln.

4. Validierungs-Netzwerkknoten nach einem der vorhergehenden Aspekte, wobei der Satz von Konsensregeln mindestens eines der Folgenden enthält: Formatierungsanforderungen für Transaktionen oder Transaktionsblöcke; einen Mechanismus zum Bestimmen, welcher der Peer-Netzwerkknoten eine nächste Transaktion oder einen nächsten Transaktionsblock zum Distributed Ledger hinzufügt; oder ein kryptographischer Hashing-Algorithmus zum Hashing der in jeder der Transaktionen enthaltenen Prozessanlagendaten.

5. Validierungs-Netzwerkknoten nach einem der vorhergehenden Aspekte, wobei der Prozessdatenvalidierer ferner dafür konfiguriert ist, Code in Smart Contracts auszuführen und Datenbanken für den Zustand des Smart Contracts zu aktualisieren.

6. Validierungs-Netzwerkknoten nach einem der vorhergehenden Aspekte, wobei der Prozessdatenvalidierer ferner dafür konfiguriert ist, um die Daten des Distributed Ledgers, welche von den Peer-Netzwerkknoten empfangen wurden, nicht zu berücksichtigen, wenn die Daten des Distributed Ledgers die Konsensregeln nicht erfüllen.

7. Validierungs-Netzwerkknoten nach einem der vorhergehenden Aspekte, wobei der Validierungs-Netzwerkknoten und die Peer-Netzwerkknoten Vorrichtungen innerhalb einer gleichen Prozessanlage sind.

8. Validierungs-Netzwerkknoten nach einem der vorhergehenden Aspekte, wobei der Validierungs-Netzwerkknoten und die Peer-Netzwerkknoten Geräte innerhalb von mehreren Prozessanlagen sind.

9. Verfahren zum Aufzeichnen von Daten in einem Prozessleitsystem unter Verwendung eines Distributed Ledgers, der durch mehrere Teilnehmer verwaltet wird, wobei das Verfahren umfasst: das Erhalten durch ein Computergerät, von Prozessanlagendaten, welche sich auf ein Prozesssteuerungselement in einer Prozessanlage beziehen; Generieren einer Transaktion einschließlich der Prozessanlagendaten, wobei die Transaktion in dem Distributed Ledger gespeichert ist; und Übermitteln der Transaktion an mindestens einen anderen Teilnehmer in einem Distributed-Ledger-Netzwerk von Teilnehmern, die den Distributed Ledger verwalten.

10. Verfahren nach Aspekt 9, wobei das Generieren der Transaktion einschließt: Generieren einer kryptographischen Signatur auf der Grundlage der Transaktion; und Ergänzen der Transaktion mit der kryptographischen Signatur.

11. Verfahren nach einem der Aspekte 9 oder 10, wobei die Daten von einem Feldgerät in der Prozessanlage erhalten werden, und wobei das Generieren der Transaktion ferner einschließt: Erhalten von Identitätsdaten für das Feldgerät; und Ergänzen der Transaktion mit den Identitätsdaten.

12. Verfahren nach einem der Aspekte 9-11, ferner umfassend: Hinzufügen der Transaktion zu einem Transaktionsblock; Lösen eines kryptographischen Puzzles auf der Grundlage des Transaktionsblocks; Hinzufügen der Lösung des kryptographischen Puzzles zu dem Transaktionsblock; und Übermitteln des Transaktionsblocks an mindestens einen anderen Teilnehmer in dem Distributed-Ledger-Netzwerk.

13. Verfahren nach einem der Aspekte 9-12, wobei es sich bei den Daten um Produktverfolgungsdaten handelt und das Generieren einer Transaktion das Generieren einer Transaktion enthält, die angibt, dass ein Produkt von einer Prozessanlage zu einer anderen Einheit übertragen wurde.

14. Verfahren nach einem der Aspekte 9-13, wobei die Daten Produktparameterdaten sind, die mindestens eines von Folgendem umfassen: eine Temperatur eines Produkts, ein Volumen des Produkts oder eine chemische Zusammensetzung des Produkts, und wobei die Produktparameterdaten im Distributed Ledger gespeichert werden, um die Echtheit der Parameterdaten für das Produkt zu überprüfen, wenn das Produkt einer anderen Einheit bereitgestellt wird.

15. Verfahren nach einem der Aspekte 9-14, wobei das Distributed-Ledger-Netzwerk mehrere Schichten einschließt und ferner umfasst: in einer ersten Instanz Generieren einer Transaktion, die in einer ersten Schicht des Distributed Ledgers gespeichert werden soll; und in einer zweiten Instanz Generieren einer Transaktion, die in einer zweiten Schicht des Distributed Ledgers gespeichert werden soll.

16. Verfahren nach einem der Aspekte 9-15, wobei die erste Schicht des Distributed Ledgers öffentlich ist und die zweite Schicht der dezentralen Schicht privat ist.

17. Verfahren nach einem der Aspekte 9-16, wobei der Distributed Ledger mindestens eines von: einer Blockchain, einem Tangle, ei-

nem Blockgitter oder anderen gerichteten azyklischen Graphen ist.

18. Verfahren nach einem der Aspekte 9-17, wobei die Prozessanlagendaten zumindest eines von Produktparameterdaten, Konfigurationsdaten, Produktverfolgungsdaten oder Prozessparameterdaten einschließen.

19. Verfahren nach einem der Aspekte 9-18, wobei das Generieren einer Transaktion das Generieren einer Transaktion, welche einen kryptographischen Hashwert einschließt, der den Prozessanlagendaten entspricht, umfasst.

20. System zum Aufzeichnen von Daten in einem Prozessleitsystem unter Verwendung eines Distributed Ledgers, der durch mehrere Teilnehmer verwaltet wird, welches umfasst: ein Gerät oder mehrere Geräte, welche in einer Prozessanlage angeordnet sind, wobei jedes Gerät eine physische Funktion ausführt, um einen industriellen Prozess zu steuern; und ein Computergerät, welches in der Prozessanlage ausgeführt wird und Folgendes umfasst: einen Prozessor oder mehrere Prozessoren; eine Kommunikationseinheit; und ein nichtvorübergehendes computerlesbares Medium, das mit dem einen Prozessor oder den mehreren Prozessoren und der Kommunikationseinheit gekoppelt ist und darauf Anweisungen speichert, die, wenn sie von dem einen Prozessor oder den mehreren Prozessoren ausgeführt werden, das Computergerät veranlassen, Prozessanlagendaten zu erhalten, die sich auf das eine Gerät oder die mehreren Geräte in der Prozessanlage beziehen; Generieren einer Transaktion, welche die Prozessanlagendaten enthält; und Übermitteln der Transaktion an mindestens einen anderen Teilnehmer in einem Distributed-Ledger-Netzwerk von Teilnehmern, welche den Distributed Ledger verwalten, um die Transaktion im Distributed Ledger zu validieren und aufzuzeichnen.

21. System nach Aspekt 20, wobei, um die Transaktion zu generieren, die Anweisungen das Computergerät veranlassen, eine kryptographische Unterschrift auf Grundlage der Transaktion zu generieren; und die Transaktion mit der kryptographischen Signatur zu ergänzen.

22. System nach einem der Aspekte 20 oder 21, wobei die Daten von einem Feldgerät in der Prozessanlage erhalten werden, und die Anweisungen das Computergerät, um die Transaktion zu generieren, veranlassen, Identitätsdaten für das Feldgerät zu erhalten; und die Transaktion mit den Identitätsdaten zu ergänzen.

23. System nach einem der Aspekte 20-22, wobei die Anweisungen ferner das Computergerät veranlassen: die Transaktion zu einem Transaktionsblock hinzuzufügen; ein kryptographisches Puzzle auf der Grundlage des Transaktionsblocks zu lösen; die Lösung des kryptographischen Puzzles zum Transaktionsblock hinzuzufügen; und den Transaktionsblock an mindestens einen anderen Teilnehmer in dem Distributed-Ledger-Netzwerk zu übermitteln.

24. System nach einem der Aspekte 20-23, wobei das Distributed-Ledger-Netzwerk mehrere Schichten einschließt, und die Anweisungen ferner das Computergerät veranlassen: in einer ersten Instanz eine Transaktion zu generieren, welche in einer ersten Schicht des Distributed Ledgers gespeichert werden soll; und in einer zweiten Instanz eine Transaktion zu generieren, die in einer zweiten Schicht des Distributed Ledgers gespeichert werden soll.

25. System nach einem der Aspekte 20-24, wobei die erste Schicht des Distributed Ledgers eine Public Blockchain und die zweite Schicht der dezentralen Schicht eine Private Blockchain ist.

26. System nach einem der Aspekte 20-25, wobei der Distributed Ledger mindestens eines von: einer Blockchain, einem Tangle, einem Blockgitter oder anderen gerichteten azyklischen Graphen ist.

27. System nach einem der Aspekte 20-26, wobei die Prozessanlagendaten mindestens eines von: Produktparameterdaten, Konfigurationsdaten, Produktverfolgungsdaten oder Prozessparameterdaten ist.

28. System nach einem der Aspekte 20-27, wobei das Generieren einer Transaktion das Generieren einer Transaktion einschließend einen kryptographischen Hashwert, welcher den Prozessanlagendaten entspricht, einschließt.

29. Nichtvorübergehender computerlesbarer Speicher, der mit einem Prozessor oder mehreren Prozessoren gekoppelt ist und Anweisungen darauf speichert, die, wenn sie von einem Prozessor oder mehreren Prozessoren ausgeführt werden, den einen Prozessor oder die mehreren Prozessoren veranlassen, Transaktionen zu empfangen, die Prozessanlagendaten einschließen, die durch ein Feldgerät oder mehrere Feldgeräte generiert sind, die jeweils eine physische Funktion zur Steuerung eines industriellen Prozesses in einer Prozessanlage ausführen; eine Kopie eines Distributed Ledgers speichern; eine Reihe von Konsensregeln auf die erhaltenen Transaktionen anwenden; eine der erhaltenen Transaktionen an die Kopie des Distributed Ledgers anhängen, wenn die erhaltene Transaktion den Konsensregeln entspricht; und die angehängte Transaktion an mindestens einen Peer-Netzwerkknoten übermitteln, der eine Kopie des Distributed Ledgers speichert.

30. Computerlesbarer Speicher nach Aspekt 29, wobei die erhaltene Transaktion einen Identitätsnachweis einer Einheit, welche die Transaktion generiert, enthält.

31. Computerlesbarer Speicher nach einem der Aspekte 29 oder 30, wobei um eine der erhaltenen Transaktionen anzuhängen, die Anweisungen den einen Prozessor oder die mehreren Prozessoren veranlassen: ein kryptographisches Puzzle zu lösen, das auf einem Transaktionsblock basiert, welcher die erhaltene Transaktion einschließt; die Lösung des kryptographischen Puzzles zum Transaktionsblock hinzuzufügen; den Transaktionsblock an die Kopie des Distributed Ledgers anzuhängen; und den Transaktionsblock an den Peer-Netzwerkknoten zu übermitteln.

32. Computerlesbarer Speicher nach einem der Aspekte 29-31, wobei der Satz von Konsensregeln mindestens eines der Folgenden umfasst: Formatierungsanforderungen für Transaktionen oder Transaktionsblöcke; einen Mechanismus zum Bestimmen, welcher der Peer-Netzwerkknoten eine nächste Transaktion oder einen nächsten Transaktionsblock zum Distributed Ledger hinzufügt; oder ein kryptographischer Hashing-Algorithmus zum Hashing der in jeder der Transaktionen enthaltenen Prozessanlagendaten.

33. Computerlesbarer Speicher nach einem der Aspekte 29 bis 32, wobei die Anweisungen ferner den einen Prozessor oder die mehreren Prozessoren veranlassen, die von den Peer-Netzwerkknoten empfangenen Daten des Distributed Ledgers zu ignorieren, wenn die Daten des Distributed Ledgers die Konsensregeln nicht erfüllen.

34. Computerlesbarer Speicher nach einem der Aspekte 29 bis 33, wobei die Peer-Netzwerkknoten Geräte innerhalb derselben Prozessanlage sind.

35. Computerlesbarer Speicher nach einem der Aspekte 29 bis 34, wobei die Peer-Netzwerkknoten Geräte innerhalb von mehreren Prozessanlagen sind.

36. Verfahren zur sicheren Messung von nicht vertrauenswürdigen Daten in Prozessleitsystemen, welche einen Distributed Ledger verwenden, das durch mehrere Teilnehmer verwaltet wird, wobei das Verfahren umfasst: das Durchführen einer Messung eines Parameters in der Prozessanlage durch ein Feldgerät, das eine physische Funktion durchführt, um einen industriellen Prozess in einer Prozessanlage zu steuern; Erhalten der Messung des Parameters durch ein Computergerät; Generieren einer Transaktion, welche die Messung einschließt; und Übermitteln der Transaktion an mindestens einen anderen Teilnehmer in einem lokalen Distributed-Ledger-Netzwerk von Teilnehmern, die ein lokales Distributed Ledger verwalten; nach einem Schwellenwertzeitraum Übermitteln von mehreren Transaktionen, die während des Schwellenwertzeitraums generiert wurden, an mindestens einen Teilnehmer in einem globalen Distributed-Ledger-Netzwerk von Teilnehmern, die einen globalen Distributed Ledger verwalten.

37. Verfahren nach Aspekt 36, ferner umfassend: Hinzufügen der Transaktion zu einem lokalen Transaktionsblock; Lösen eines kryptographischen Puzzles auf der Grundlage des lokalen Transaktionsblocks; Hinzufügen der Lösung des kryptographischen Puzzles zum lokalen Transaktionsblock; und Übermitteln des lokalen Transaktionsblocks an mindestens einen anderen Teilnehmer in dem lokalen Distributed-Ledger-Netzwerk.

38. Verfahren nach einem der Aspekte 36 oder 37, ferner umfassend: nach dem Ablauf des Schwellenwertzeitraums, Übermitteln eines oder mehrerer lokaler Transaktionsblöcke, welche während dem Schwellenwertzeitraum generiert wurden, an mindestens einen Teilnehmer in dem globalen Distributed-Ledger-Netzwerk.

39. Verfahren nach einem der Aspekte 36-38, ferner umfassend: nach dem Ablauf des Schwellenwertzeitraums, Beschneiden von mindestens einigen der mehreren Transaktionen, die während des Schwellenwertzeitraums vom lokalen Distributed-Ledger-Netzwerk generiert wurden.

40. Verfahren nach einem der Aspekte 36-39, wobei der globale Distributed Ledger eine Permissioned Blockchain ist, welche durch mehrere Einheiten, die mehrere Prozessanlagen betreiben, sichtbar ist.

41. Verfahren nach einem der Aspekte 36-40, wobei sich der Parameter auf eine Ressource bezieht, welche von den mehreren Einheiten, welche die mehreren Prozessanlagen betreiben, gemeinsam genutzt wird.

42. Verfahren nach einem der Aspekte 36-41, wobei der globale Distributed Ledger mehrere globale Distributed Ledgers einschließt, welche den mehreren Einheiten entsprechen, wobei jeder globale Distributed Ledger Transaktionen einschließt, welche in dem lokalen Distributed Ledger für dieselbe jeweilige Einheit wie der globale Distributed Ledger gespeichert sind.

43. Verfahren nach einem der Aspekte 36-42, ferner umfassend: für Transaktionen, die während des Schwellenwertzeitraums generiert wurden, Hinzufügen der Transaktion von jedem der mehreren globalen Distributed Ledgers

zu einem Zustandstransaktionsblock; Lösen eines kryptographischen Puzzles auf der Grundlage des Zustandstransaktionsblocks; Hinzufügen der Lösung des kryptographischen Puzzles zum Zustandstransaktionsblock; und Übermitteln des Zustandstransaktionsblocks an mindestens einen anderen Teilnehmer in einem Superblockchain-Netzwerk von Teilnehmern, die eine Superblockchain verwalten.

44. Verfahren nach einem der Aspekte 36-43, wobei der lokale Distributed Ledger eine private Blockchain ist, die von einer Einheit gesehen werden kann, welche die Prozessanlage betreibt.

45. Verfahren nach einem der Aspekte 36-44, wobei das Generieren einer Transaktion, welche die Messung umfasst, das Generieren der Transaktion einschließlich eines der Messung entsprechenden kryptographischen Hashwerts einschließt.

46. Verfahren nach einem der Aspekte 36-45, wobei die Ressource, welche von mehreren Einheiten gemeinsam genutzt wird, welche die mehreren Prozessanlagen betreiben, ein Fluid in einer Fluidrohrleitung ist und die Parametermessung eine Fluidmenge ist, die durch eine Einheit der mehreren Einheiten von der Fluidleitung erhalten wird.

47. System zur sicheren Erfassung nicht vertrauenswürdiger Daten in Prozessleitsystemen unter Verwendung eines Distributed Ledgers, der von mehreren Teilnehmern verwaltet wird, umfassend: ein Feldgerät oder mehrere Feldgeräte, die in einer Prozessanlage angeordnet sind und jeweils eine physische Funktion zur Steuerung eines industriellen Prozesses ausführen, wobei das eine Feldgerät oder die mehreren Feldgeräte konfiguriert sind, um Messungen von Parametern in der Prozessanlage durchzuführen und die Parametermessungen einem Edge-Gateway-Gerät oder mehreren Edge-Gateway-Geräten bereitzustellen; und wobei das eine Edge-Gateway-Gerät oder die mehreren Edge-Gateway-Geräte, die in der Prozessanlage ausgeführt werden, jeweils einschließen: einen Prozessor oder mehrere Prozessoren; eine Kommunikationseinheit; und ein nichtvorübergehendes computerlesbares Medium, das mit dem einen Prozessor oder den mehreren Prozessoren und der Kommunikationseinheit gekoppelt ist und Anweisungen darauf speichert, die, wenn sie von dem einen Prozessor oder den mehreren Prozessoren ausgeführt werden, das Edge-Gateway-Gerät veranlassen, mindestens eine der Parametermessungen zu erhalten; eine Transaktion, welche die Messung einschließt, zu generieren; und die Transaktion an mindestens ein anderes Edge-Gateway in einem lokalen Distributed-Ledger-Netzwerk von Edge-Gateways zu übermitteln, die ein lokales Distributed Ledger verwalten; und nach Ablauf eines Schwellenwertzeitraums mehrere Transaktionen, die während des Schwellenwertzeitraums generiert wurden, an mindestens einen Teilnehmer in einem globalen Distributed-Ledger-Netzwerk von Teilnehmern zu übermitteln, die einen globalen Distributed Ledger verwalten.

48. System nach Aspekt 47, wobei die Anweisungen ferner den Edge-Gateway veranlassen: die Transaktion zu einem lokalen Transaktionsblock hinzuzufügen; ein kryptographisches Puzzle auf der Grundlage des lokalen Transaktionsblocks zu lösen; die Lösung des kryptographischen Puzzles zum lokalen Transaktionsblock hinzuzufügen; und den lokalen Transaktionsblock an mindestens ein anderes Edge-Gateway in dem lokalen Distributed-Ledger-Netzwerk zu übermitteln.

49. System nach einem der Aspekte 47 oder 48, wobei die Anweisungen ferner das Edge-Gateway veranlassen, nach dem Schwellenwertzeitraum einen oder mehrere lokale Transaktionsblöcke, die während des Schwellenwertzeitraums generiert wurden, an mindestens einen Teilnehmer am globalen Distributed-Ledger-Netzwerk zu übermitteln.

50. System nach einem der Aspekte 47-49, wobei die Anweisungen ferner das Edge-Gateway veranlassen, nach dem Schwellenwertzeitraum mindestens einige der mehreren Transaktionen zu beschneiden, die während des Schwellenwertzeitraums von dem lokalen Distributed-Ledger-Netzwerk generiert wurden.

51. System nach einem der Aspekte 47-50, wobei der globale Distributed Ledger eine Permissioned Blockchain ist, welche durch mehrere Einheiten gesehen werden kann, welche mehrere Prozessanlagen betreiben.

52. System nach einem der Aspekte 47-51, wobei sich der Parameter auf eine Ressource bezieht, welche von den mehreren Einheiten geteilt werden kann, welche die mehreren Prozessanlagen betreiben.

53. System nach einem der Aspekte 47-52, wobei der globale Distributed Ledger mehrere globale Distributed Ledger einschließt, welche den mehreren Einheiten entsprechen, wobei jeder globale Distributed Ledger Transaktionen einschließt, welche in dem lokalen Distributed Ledger für jeweils dieselbe Einheit wie der globale Distributed Ledger gespeichert werden.

54. System nach einem der Aspekte 47-53, ferner umfassend: ein Computergerät in einem globalen Distributed-Ledger-Netzwerk, das einen globalen Distributed Ledger verwaltet, um-

fassend: einen Prozessor oder mehrere Prozessoren; eine Kommunikationseinheit; und ein nichtvorübergehendes computerlesbares Medium, das mit dem einen Prozessor oder den mehreren Prozessoren und der Kommunikationseinheit gekoppelt ist und Anweisungen darauf speichert, die, wenn sie von dem einen Prozessor oder den mehreren Prozessoren ausgeführt werden, das Computergerät veranlassen, für Transaktionen, die während des Schwellenwertzeitraums generiert werden, die Transaktion aus jedem der mehreren globalen Distributed Ledgers zu einem Zustandstransaktionsblock hinzuzufügen; ein kryptographisches Puzzle auf der Grundlage des Zustandstransaktionsblocks zu lösen; die Lösung des kryptographischen Puzzles zum Zustandstransaktionsblock hinzuzufügen; und die Zustandstransaktionsblöcke an mindestens einen anderen Teilnehmer in einem Superblockchain-Netzwerk von Teilnehmern, die eine Superblockchain verwalten, zu übermitteln.

55. System nach einem der Aspekte 47-54, wobei der lokale Distributed Ledger eine private Blockchain ist, die von einer Einheit gesehen werden kann, welche die Prozessanlage betreibt.

56. System nach einem der Aspekte 47-55, wobei die Transaktion einen kryptographischen Hashwert enthält, welcher der Messung entspricht.

57. System nach einem der Aspekte 47-56, wobei die gemeinsam genutzte Ressource zwischen den mehreren Einheiten, welche die mehreren Prozessanlagen betreiben, ein Fluid in einer Fluidrohrleitung ist und die Parametermessung eine Fluidmenge ist, die durch eine der mehreren Einheiten aus der Fluidleitung erhalten wird.

58. Validierungs-Netzwerkknoten in einer Prozessanlage auf einem lokalen Distributed-Ledger-Netzwerk, umfassend: einen Transceiver, der konfiguriert ist, um (i) mit einem Feldgerät oder mehreren Feldgeräten zu kommunizieren, die jeweils eine physische Funktion ausführen, um einen industriellen Prozess in der Prozessanlage zu steuern und Messungen von Parametern in der Prozessanlage zu sammeln und (ii) lokale Daten des Distributed Ledgers mit Peer-Netzwerkknoten auszutauschen, wobei die lokalen Daten des Distributed Ledgers Transaktionen aufweisend Parametermessungen enthalten; ein Speichermedium, das zum Speichern einer Kopie des lokalen Distributed Ledgers konfiguriert ist; und einen Prozessdatenvalidierer, der konfiguriert ist, um einen Satz von Konsensregeln auf die von den Peer-Netzwerkknoten empfangenen Daten des Distributed Ledgers anzuwenden, wobei der Prozessdatenvalidierer ferner konfiguriert ist, um die von den Peer-Netzwerkknoten empfangenen Daten des Distributed Ledgers an die Kopie der Distributed Ledger anzuhängen, wenn die Daten des Distributed Ledgers die Konsensregeln erfüllen, wobei der Transceiver nach einem Schwellenwertzeitraum so konfiguriert ist, dass er mehrere Transaktionen, die während des Schwellenwertzeitraums generiert wurden, an mindestens einen Teilnehmer in einem globalen Distributed-Ledger-Netzwerk von Teilnehmern übermittelt, die einen globalen Distributed Ledger verwalten.

59. Validierungs-Netzwerkknoten nach Aspekt **58**, wobei nach der Schwellenwertzeitperiode, der Validierungs-Netzwerkknoten konfiguriert ist, um mindestens einige der mehreren Transaktionen zu beschneiden, welche während der Schwellenwertzeitperiode von der Kopie des lokalen Distributed Ledgers generiert werden.

60. Validierungs-Netzwerkknoten nach Aspekt 58 oder Aspekt 59, wobei der globale Distributed Ledger eine Permissioned Blockchain ist, die von mehreren Einheiten gesehen werden kann, die mehrere Prozessanlagen betreiben.

61. Validierungs-Netzwerkknoten nach einem der Aspekte 58-60, wobei sich mindestens einer der Parameter auf eine der Ressourcen bezieht, welche von den mehreren Einheiten gemeinsam genutzt werden, welche die mehreren Prozessanlagen betreiben.

62. Validierungs-Netzwerkknoten nach einem der Aspekte 58-61, wobei der globale Distributed Ledger mehrere globale Distributed Ledger enthält, welche den mehreren Einheiten entsprechen, wobei jeder globale Distributed Ledger Transaktionen enthält, die in dem lokalen Distributed Ledger für dieselbe jeweilige Einheit gespeichert sind, wie der globale Distributed Ledger.

63. Validierungs-Netzwerkknoten nach einem der Aspekte 58-62, wobei der lokale Distributed Ledger eine private Blockchain ist, welche durch eine Einheit gesehen werden kann, welche die Prozessanlage betreibt.

64. Validierungs-Netzwerkknoten nach einem der Aspekte 58-63, wobei eine Transaktion einen kryptographischen Hashwert enthält, der einer Parametermessung entspricht.

65. Verfahren zum Aufzeichnen der Qualitätskontrolle, Produktion oder regulatorischen Daten in einem Prozessleitsystem, das einen Distributed Ledger verwendet, der durch mehrere Teilnehmer verwaltet wird, wobei das Verfahren umfasst: über ein Feldgerät oder mehrere Feldgeräte, welche jeweils eine physische Funktion durchführen, um einen industriellen Prozess

zu steuern, Detektieren eines auslösenden Ereignisses, das sich auf die Qualitätskontrolle in einer Prozessanlage bezieht; Erhalten von Ereignisdaten von dem auslösenden Ereignis, einschließlich mindestens eines von: einem Zeitpunkt des auslösenden Ereignisses, einer Dauer des auslösenden Ereignisses, Produktparameterdaten, die sich auf das auslösende Ereignis beziehen, oder Prozessparameterdaten, die sich auf das auslösende Ereignis beziehen; Generieren einer Transaktion einschließlich der Ereignisdaten, wobei die Transaktion in dem Distributed Ledger gespeichert ist; und Übermitteln der Transaktion an mindestens einen anderen Teilnehmer in einem Distributed-Ledger-Netzwerk von Teilnehmern, welche den Distributed Ledger verwalten.

66. Verfahren nach Aspekt 65, wobei das auslösende Ereignis mindestens eines von Folgendem ist: ein Alarm, ein Fehler, ein Leck, ein Reparaturereignis, ein Prozessmeilenstein oder eine Korrekturmaßnahme.

67. Verfahren nach einem von Aspekt 65 oder Aspekt 66, ferner umfassend: Erhalten einer Aufforderung für Ereignisdaten von einem bestimmten auslösenden Ereignis; Erhalten der Ereignisdaten von dem Distributed Ledger; und Präsentieren der Ereignisdaten von dem bestimmten auslösenden Ereignis auf einer Benutzeroberfläche.

68. Verfahren nach einem der Aspekte 65-67, wobei das Generieren einer Transaktion einschließlich der Ereignisdaten das Generieren der Transaktion einschließlich einem kryptographischen Hashwert umfasst, welche mindestens einigen der Ereignisdaten entsprechen.

69. Verfahren nach einem der Aspekte 65-68, ferner umfassend: Speichern der Ereignisdaten in einer Datenbank; und als Reaktion auf eine Aufforderung zur Authentifizierung der Ereignisdaten Bereitstellen des kryptographischen Hashwerts, der mindestens einigen der Ereignisdaten aus dem Distributed Ledger zusammen mit den Ereignisdaten aus der Datenbank entspricht, um die Authentizität der Ereignisdaten zu überprüfen.

70. Verfahren nach einem der Aspekte 65-69, wobei das auslösende Ereignis eine Öffnung in einem Überdruckventil ist und die Ereignisdaten von dem auslösenden Ereignis mindestens eines von Folgendem umfassen: einen Zeitpunkt, zu dem das Überdruckventil geöffnet wurde; eine Dauer, in der das Überdruckventil geöffnet war, ein Druckwert, als das Überdruckventil geöffnet war, oder eine Menge an Fluid, die entfernt wurde, während das Überdruckventil geöffnet war.

71. Verfahren nach einem der Aspekte 65-70, wobei der Distributed Ledger eine private Blockchain ist, auf welche die Prozessanlage und eine Aufsichtsbehörde zugreifen können.

72. Verfahren nach einem der Aspekte 65-71, wobei der Distributed Ledger eine Public Blockchain ist.

73. Verfahren nach einem der Aspekte 65-72, wobei die Transaktion ferner eine eindeutige Kennung für das auslösende Ereignis enthält.

74. Verfahren nach einem der Aspekte 65-73, ferner umfassend: Übermitteln einer Angabe des detektierten auslösenden Ereignisses einschließlich der eindeutigen Kennung für das auslösende Ereignis zu einem Prozesssteuerungselement oder mehreren anderen Prozesssteuerungselementen in der Prozessanlage für die anderen Prozesssteuerungselemente zum Generieren von Transaktionen einschließlich zusätzlicher Ereignisdaten in Bezug auf das auslösende Ereignis.

75. System zum Aufzeichnen der Qualitätskontrolle, Produktion oder regulatorischen Daten in einem Prozessleitsystem, das einen Distributed Ledger verwendet, der durch mehrere Teilnehmer verwaltet wird, umfassend: ein Gerät oder mehrere Geräte, welche in einer Prozessanlage angeordnet sind, die jeweils eine physische Funktion durchführen, um einen industriellen Prozess zu steuern; und ein Computergerät, das in der Prozessanlage ausgeführt wird und Folgendes umfasst: einen Prozessor oder mehrere Prozessoren; eine Kommunikationseinheit; und ein nichtvorübergehendes computerlesbares Medium, das mit dem einen Prozessor oder den mehreren Prozessoren und der Kommunikationseinheit gekoppelt ist und Anweisungen darauf speichert, die, wenn sie von dem einen Prozessor oder den mehreren Prozessoren ausgeführt werden, das Computergerät zu Folgendem veranlassen: Detektieren über das eine Gerät oder die mehreren Geräte eines auslösendes Ereignisses im Zusammenhang mit der Qualitätskontrolle in einer Prozessanlage; Erhalten von Ereignisdaten aus dem auslösenden Ereignis, einschließlich mindestens eines von: einem Zeitpunkt des auslösenden Ereignisses, einer Dauer des auslösenden Ereignisses, Produktparameterdaten, die sich auf das auslösende Ereignis beziehen, oder Prozessparameterdaten, die sich auf das auslösende Ereignis beziehen; Generieren einer Transaktion einschließlich der Ereignisdaten, wobei die Transaktion in dem Distributed Ledger gespeichert ist; und Übermitteln der Transaktion an mindestens einen anderen Teilnehmer in einem Distributed-Ledger-Netzwerk von Teilnehmern, welche den Distributed Ledger verwalten, um die Transaktion im

Distributed Ledger zu validieren und aufzuzeichnen.

76. System nach Aspekt 75, wobei das auslösende Ereignis mindestens eines von Folgendem ist: ein Alarm, ein Fehler, ein Leck, ein Reparaturereignis, ein Prozessmeilenstein oder eine Korrekturmaßnahme.

77. System nach einem der Aspekte 75 oder 76, wobei die Anweisungen das Computergerät ferner veranlassen: eine Anforderung nach Ereignisdaten von einem bestimmten auslösenden Ereignis zu empfangen; die Ereignisdaten von dem Distributed Ledger zu erhalten; und die Ereignisdaten von dem bestimmten auslösenden Ereignis auf einer Benutzeroberfläche zu zeigen.

78. System nach einem der Aspekte 75-77, wobei die Transaktion einen kryptographischen Hashwert einschließt, welcher mindestens einigen der Ereignisdaten entspricht.

79. System nach einem der Aspekte 75-78, wobei die Anweisungen das Computergerät ferner veranlassen, die Ereignisdaten in einer Datenbank zu speichern; und als Reaktion auf eine Aufforderung zur Authentifizierung der Ereignisdaten den kryptographischen Hashwert, der mindestens einigen der Ereignisdaten von dem Distributed Ledger entspricht, zusammen mit den Ereignisdaten aus der Datenbank bereitzustellen, um die Authentizität der Ereignisdaten zu überprüfen.

80. System nach einem der Aspekte 75-79, wobei das auslösende Ereignis eine Öffnung in einem Überdruckventil ist und die Ereignisdaten von dem auslösenden Ereignis mindestens eines von Folgendem umfassen: einen Zeitpunkt, zu dem das Überdruckventil geöffnet wurde; eine Dauer, in der das Überdruckventil geöffnet war, ein Druckwert, als das Überdruckventil geöffnet war, oder eine Menge an Fluid, die entfernt wurde, während das Überdruckventil geöffnet war.

81. System nach einem der Aspekte 75-80, wobei der Distributed Ledger eine private Blockchain ist, welche durch die Prozessanlage und eine Aufsichtsbehörde zugänglich ist.

82. System nach einem der Aspekte 75-81, wobei der Distributed Ledger eine Public Blockchain ist.

83. System nach einem der Aspekte 75-82, wobei die Transaktion ferner eine eindeutige Kennung für das auslösende Ereignis enthält.

84. System nach einem der Aspekte 75-83, wobei die Anweisungen ferner das Computergerät veranlassen: eine Angabe des detektierten auslösenden Ereignisses, welches die eindeutige Kennung für das auslösende Ereignis einschließt, an das eine Gerät oder die mehreren Geräte in der Prozessanlage für das eine Gerät oder die mehreren Geräte zum Generieren von Transaktionen einschließlich zusätzlicher Ereignisdaten, die sich auf das auslösende Ereignis beziehen, zu übermitteln.

85. Validierungs-Netzwerkknoten in einer Prozessanlage auf einem Distributed-Ledger-Netzwerk, umfassend: einen Transceiver, welcher konfiguriert ist, mit einem Feldgerät oder mehreren Feldgeräten zu kommunizieren, das/die jeweils eine physische Funktion ausführen, um einen industriellen Prozess in der Prozessanlage zu steuern und Daten des Distributed Ledgers mit Peer-Netzwerkknoten auszutauschen, wobei die Daten des Distributed Ledgers Transaktionen enthalten, die Ereignisdaten von einem auslösenden Ereignis aufweisen; ein Speichermedium, das zum Speichern einer Kopie des Distributed Ledgers konfiguriert ist; und einen Prozessdatenvalidierer, der konfiguriert ist, um einen Satz von Konsensregeln auf die von den Peer-Netzwerkknoten empfangenen Daten des Distributed Ledgers anzuwenden, wobei der Prozessdatenvalidierer ferner konfiguriert ist, um die von den Peer-Netzwerkknoten empfangenen Daten des Distributed Ledgers an die Kopie des Distributed Ledgers anzuhängen, wenn die Daten des Distributed Ledgers den Konsensregeln entsprechen.

86. Validierungs-Netzwerkknoten nach Aspekt 85, wobei die Ereignisdaten mindestens eines von Folgendem umfassen: einen Zeitpunkt des auslösenden Ereignisses, eine Dauer des auslösenden Ereignisses, Produktparameterdaten, die sich auf das auslösende Ereignis beziehen, oder Prozessparameterdaten, die sich auf das auslösende Ereignis beziehen.

87. Validierungs-Netzwerkknoten nach Aspekt 85 oder Aspekt 86, wobei das auslösende Ereignis mindestens eines von Folgendem ist: ein Alarm, ein Fehler, ein Leck, ein Reparaturereignis oder eine Korrekturmaßnahme.

88. Validierungs-Netzwerkknoten nach einem der Aspekte 85-87, wobei die Daten des Distributed Ledgers, die von den Peer-Knoten empfangen wurden, einen Identitätsnachweis von einem des einen Feldgeräts oder der mehreren Feldgeräte einschließen, welche eine Transaktion generieren, die Ereignisdaten aufweist.

89. Validierungs-Netzwerkknoten nach einem der Aspekte 85-88, wobei Daten des Distributed Ledgers, welche von den Peer-Knoten empfangen wurden, anzuhängen sind, wobei der Transaktionsvalidierer konfiguriert ist, um: ein kryptographisches Puzzle zu lösen, das auf einem Transaktionsblock basiert; die Lösung des kryptographischen Puzzles zum Transaktions-

block hinzuzufügen; den Transaktionsblock an die Kopie des Distributed Ledgers anzuhängen; und den Transaktionsblock an mindestens einen der Peer-Netzwerkknoten im Distributed-Ledger-Netzwerk zu übermitteln.

90. Validierungs-Netzwerkknoten nach einem der Aspekte 85-89, wobei der Satz von Konsensregeln mindestens eines der Folgenden umfasst: Formatierungsanforderungen für Transaktionen oder Transaktionsblöcke; einen Mechanismus zum Bestimmen, welcher der Peer-Netzwerkknoten eine nächste Transaktion oder einen nächsten Transaktionsblock zum Distributed Ledger hinzufügt; oder ein kryptographischer Hashing-Algorithmus zum Hashing der in jeder der Transaktionen enthaltenen Prozesssteuerungsdaten.

91. Validierungs-Netzwerkknoten nach einem der Aspekte 85-90, wobei der Distributed Ledger eine Private Blockchain ist, welche durch die Prozessanlage und eine Aufsichtsbehörde zugänglich ist.

92. Validierungs-Netzwerkknoten nach einem der Aspekte 85-91, wobei der Distributed Ledger eine Public Blockchain ist.

93. Validierungs-Netzwerkknoten nach einem der Aspekte 85-92, wobei die Transaktion ferner eine eindeutige Kennung für das auslösende Ereignis enthält.

94. Verfahren zum Aufzeichnen von Software- oder Firmware-Zuständen in einem Prozessleitsystem und einer angeschlossenen Instrumentierung unter Verwendung eines Distributed Ledgers, der von mehreren Teilnehmern verwaltet wird, wobei das Verfahren umfasst: Erhalten, durch ein Computergerät, eines aktuellen Software- oder Firmware-Zustands, der in einer Prozessanlage ausgeführt wird, welche ein Feldgerät oder mehrere Feldgeräte aufweist, die jeweils eine physische Funktion zur Steuerung eines industriellen Prozesses aufweisen, wobei die Software oder Firmware in einem Netzwerk oder einer Prozesssteuerungsvorrichtung in der Prozessanlage ausgeführt wird; Generieren einer Transaktion, die den aktuellen Zustand der Software oder Firmware enthält, die in der Prozessanlage ausgeführt wird, wobei die Transaktion in dem Distributed Ledger gespeichert ist; und Übermitteln der Transaktion an mindestens einen anderen Teilnehmer in einem Distributed-Ledger-Netzwerk von Teilnehmern, welche den Distributed Ledger verwalten.

95. Verfahren nach Aspekt 94, wobei der aktuelle Zustand der Software oder Firmware, die in der Prozessanlage ausgeführt wird, von einem Computergerät eines Benutzers erhalten wird, der den aktuellen Zustand aktualisiert hat, und das Generieren der Transaktion ferner umfasst: Erhalten von Identitätsdaten für den Benutzer; Ergänzen der Transaktion mit den Identitätsdaten für den Benutzer bei dem einen Prozessor oder den mehreren Prozessoren; Generieren einer kryptographischen Signatur auf der Grundlage der Transaktion an dem einen Prozessor oder den mehreren Prozessoren; und Ergänzen der Transaktion mit der kryptographischen Signatur an dem einen Prozessor oder den mehreren Prozessoren.

96. Verfahren nach einem der Aspekte 94 oder 95, wobei das Generieren einer Transaktion, die den aktuellen Zustand der Software oder Firmware enthält, die in der Prozessanlage ausgeführt wird, das Generieren der Transaktion enthält, die einen kryptographischen Hashwert enthält, der dem aktuellen Zustand der Software oder Firmware entspricht, die in der Prozessanlage ausgeführt wird.

97. Verfahren nach einem der Aspekte 94-96, ferner umfassend: Erhalten eines Zustands der Software oder Firmware, die in der Prozessanlage ausgeführt wird, von dem Netzwerk oder der Prozesssteuerungsvorrichtung, welche die Software oder Firmware ausführen; und Vergleichen des Zustands der Software oder Firmware, die in der Prozessanlage ausgeführt wird, mit dem kryptographischen Hashwert von dem Distributed Ledger, um sicherzustellen, dass die Software oder Firmware nicht manipuliert wurde.

98. Verfahren nach einem der Aspekte 94-97, ferner umfassend: als Reaktion auf das Bestimmen, dass der Zustand der Software oder Firmware, die in der Prozessanlage ausgeführt wird, nicht mit dem aktuellen Zustand der Software oder Firmware übereinstimmt, die in dem Distributed Ledger entsprechend dem kryptographischen Hashwert gespeichert ist, wodurch verhindert wird, dass die Software oder Firmware in der Prozessanlage ausgeführt wird.

99. Verfahren nach einem der Aspekte 94-98, ferner umfassend: Veranlassen, dass die Software oder Firmware zu einem vorherigen Zustand zurückkehrt.

100. Verfahren nach einem der Aspekte 94-99, ferner umfassend: als Reaktion auf das Bestimmen, dass der Zustand der Software oder Firmware, die in der Prozessanlage ausgeführt wird, mit dem aktuellen Zustand der Software oder Firmware übereinstimmt, die in dem Distributed Ledger gemäß dem kryptographischem Hashwert gespeichert ist, und das Netzwerk oder das Prozesssteuerungsgerät veranlasst, die Software oder Firmware auszuführen.

101. Verfahren nach einem der Aspekte 94-100, ferner umfassend: Hinzufügen der Trans-

aktion zu einem Transaktionsblock; Lösen eines kryptographischen Puzzles auf der Grundlage des Transaktionsblocks; Hinzufügen der Lösung des kryptographischen Puzzles zu dem Transaktionsblock; und Übermitteln des Transaktionsblocks an mindestens einen anderen Teilnehmer in dem Distributed-Ledger-Netzwerk.

102. Verfahren nach einem der Aspekte 94-101, ferner umfassend: Vergleichen der Identitätsdaten in der Transaktion mit mehreren Sätzen von Identitätsdaten, die Benutzern entsprechen, die autorisiert sind, den Zustand der Software oder Firmware zu aktualisieren, die in der Prozessanlage ausgeführt wird; und Hinzufügen der Transaktion zu dem Transaktionsblock, wenn die Identitätsdaten in den mehreren Sätzen von Identitätsdaten enthalten sind.

103. Verfahren nach einem der Aspekte 94-102, wobei der Distributed Ledger eine Permissioned Blockchain ist.

104. System zum Aufzeichnen von Software- oder Firmware-Zuständen in einem Prozessleitsystem und einer angeschlossenen Instrumentierung unter Verwendung eines Distributed Ledgers, der von mehreren Teilnehmern verwaltet wird, umfassend: ein Gerät oder mehrere in einer Prozessanlage angeordnete Geräte, die jeweils eine physische Funktion zur Steuerung eines industriellen Prozesses ausführen; und ein Computergerät, das in der Prozessanlage ausgeführt wird und Folgendes umfasst: einen Prozessor oder mehrere Prozessoren; eine Kommunikationseinheit; und ein nichtvorübergehendes computerlesbares Medium, das mit dem einen Prozessor oder den mehreren Prozessoren und der Kommunikationseinheit gekoppelt ist und Anweisungen darauf speichert, die, wenn sie von dem einen Prozessor oder den mehreren Prozessoren ausgeführt werden, das Computergerät veranlassen, einen aktuellen Zustand der Software oder Firmware zu erhalten, die in der Prozessanlage ausgeführt werden, die in mindestens einem Gerät der in der Prozessanlage angeordneten Geräte oder einem Netzwerkgerät in der Prozessanlage ausgeführt wird; Generieren einer Transaktion, die den aktuellen Zustand der Software oder Firmware enthält, die in der Prozessanlage ausgeführt wird, wobei die Transaktion in dem Distributed Ledger gespeichert ist; und Übermitteln der Transaktion an mindestens einen anderen Teilnehmer in einem Distributed-Ledger-Netzwerk von Teilnehmern, die den Distributed Ledger verwalten, um die Transaktion im Distributed Ledger zu validieren und aufzuzeichnen.

105. System nach Aspekt 104, wobei der aktuelle Zustand der Software oder Firmware, die in der Prozessanlage ausgeführt wird, von einem Computergerät eines Benutzers erhalten wird, der den aktuellen Zustand aktualisiert hat, und um die Transaktion zu generieren, veranlassen die Anweisungen das Computergerät: Identitätsdaten für den Benutzer zu erhalten; die Transaktion mit den Identitätsdaten für den Benutzer zu ergänzen; eine kryptographische Signatur auf der Grundlage der Transaktion zu generieren; und die Transaktion mit der kryptographischen Signatur zu ergänzen.

106. System nach einem der Aspekte 104 oder 105, wobei die Transaktion mit einem kryptographischen Hashwert generiert wird, der dem aktuellen Zustand der Software oder Firmware entspricht, die in der Prozessanlage ausgeführt wird.

107. System nach einem der Aspekte 104 bis 106, ferner umfassend: ein Servergerät einschließend: einen Prozessor oder mehrere Prozessoren; eine Kommunikationseinheit; und ein nichtvorübergehendes computerlesbares Medium, das mit dem einen Prozessor oder den mehreren Prozessoren und der Kommunikationseinheit gekoppelt ist und Anweisungen darauf speichert, die, wenn sie von dem einen Prozessor oder den mehreren Prozessoren ausgeführt werden, das Servergerät veranlassen: von dem Netzwerk oder der Prozesssteuerungsvorrichtung, welche Software oder Firmware in der Prozessanlage ausführen, einen Zustand der Software oder Firmware, die in der Prozessanlage ausgeführt wird, zu erhalten; und den Zustand der Software oder Firmware, die in der Prozessanlage ausgeführt werden, mit dem kryptographischen Hashwert von dem Distributed Ledger zu vergleichen, um sicherzustellen, dass die Software oder Firmware nicht manipuliert wurde.

108. System nach einem der Aspekte 104-107, wobei die Anweisungen ferner das Servergerät veranlassen: als Reaktion auf das Bestimmen, dass der Zustand der Software oder Firmware, die in der Prozessanlage ausgeführt werden, nicht mit dem aktuellen Zustand der Software oder Firmware übereinstimmt, die im Distributed Ledger gemäß dem kryptographischen Hashwert gespeichert ist, die Software oder Firmware daran zu hindern, in der Prozessanlage ausgeführt zu werden.

109. System nach einem der Aspekte 104-108, wobei die Anweisungen ferner das Servergerät veranlassen: die Software oder Firmware in einen vorherigen Zustand zurückzuversetzen.

110. System nach einem der Aspekte 104-109, wobei die Anweisungen ferner das Servergerät veranlassen: als Reaktion auf das Bestimmen, dass der Zustand der Software oder Firmware, die in der Prozessanlage ausgeführt werden, mit dem aktuellen Zustand der Software oder Firm-

ware übereinstimmt, welche im Distributed Ledger gemäß dem kryptographischen Hashwert gespeichert werden, das Netzwerk oder die Prozesssteuerungsvorrichtung zu veranlassen, die Software oder Firmware auszuführen.

111. System nach einem der Aspekte 104 bis 110, wobei die Anweisungen das Computergerät ferner veranlassen: die Transaktion zu einem Transaktionsblock hinzuzufügen; ein kryptographisches Puzzle auf der Grundlage des Transaktionsblocks zu lösen; die Lösung des kryptographischen Puzzles zum Transaktionsblock hinzuzufügen; und den Transaktionsblock an mindestens einen anderen Teilnehmer in dem Distributed-Ledger-Netzwerk zu übermitteln.

112. System nach einem der Aspekte 104-111, wobei die Anweisungen das Computergerät ferner veranlassen: die Identitätsdaten in der Transaktion mit mehreren Sätzen von Identitätsdaten zu vergleichen, die Benutzern entsprechen, die autorisiert sind, den Zustand der Software oder Firmware zu aktualisieren, die in der Prozessanlage ausgeführt werden; und die Transaktion zu dem Transaktionsblock hinzuzufügen, wenn die Identitätsdaten in den mehreren Sätzen von Identitätsdaten enthalten sind.

113. System nach einem der Aspekte 104-112, wobei der Distributed Ledger eine Permissioned Blockchain ist.

114. Validierungs-Netzwerkknoten in einer Prozessanlage auf einem Distributed-Ledger-Netzwerk, umfassend: einen Transceiver, der konfiguriert ist, um mit einem Feldgerät oder mehreren Feldgeräten zu kommunizieren, die jeweils eine physische Funktion ausführen, um einen industriellen Prozess in der Prozessanlage zu steuern und Daten des Distributed Ledgers mit Peer-Netzwerkknoten auszutauschen, wobei die Daten des Distributed Ledgers Transaktionen enthalten, deren Daten den aktuellen Zustand der Software oder Firmware anzeigen, die in der Prozessanlage ausgeführt werden; ein Speichermedium, das zum Speichern einer Kopie des Distributed Ledgers konfiguriert ist; und einen Prozessdatenvalidierer, der konfiguriert ist, um einen Satz von Konsensregeln auf die von den Peer-Netzwerkknoten empfangenen Daten des Distributed Ledgers anzuwenden, wobei der Prozessdatenvalidierer ferner konfiguriert ist, um die von den Peer-Netzwerkknoten empfangenen Daten des Distributed Ledgers an die Kopie des Distributed Ledgers anzuhängen, wenn die Daten des Distributed Ledgers den Konsensregeln entsprechen.

115. Validierungs-Netzwerkknoten nach Aspekt 114, wobei der Transaktionsvalidierer zum Anhängen von Daten des Distributed Ledgers, die von Peer-Knoten empfangen wurden, konfiguriert ist, um: ein kryptographisches Puzzle auf der Grundlage eines Transaktionsblocks zu lösen; die Lösung des kryptographischen Puzzles zum Transaktionsblock hinzuzufügen; den Transaktionsblock an die Kopie des Distributed Ledgers anzuhängen; und den Transaktionsblock an mindestens einen der Peer-Netzwerkknoten im Distributed-Ledger-Netzwerk zu übermitteln.

116. Validierungs-Netzwerkknoten nach Aspekt 114 oder Aspekt 115, wobei der Satz von Konsensregeln mindestens eines der Folgenden umfasst:

Formatierungsanforderungen für Transaktionen oder Transaktionsblöcke; einen Mechanismus zum Bestimmen, welcher der Peer-Netzwerkknoten eine nächste Transaktion oder einen nächsten Transaktionsblock zum Distributed Ledger hinzufügt; oder ein kryptographischer Hashing-Algorithmus zum Hashing von Software- oder Firmware-Zustandsdaten, die in jeder der Transaktionen enthalten sind.

117. Validierungs-Netzwerkknoten nach einem der Aspekte 114-116, wobei die von den Peer-Knoten empfangenen Daten des Distributed Ledgers einen Identitätsnachweis eines Benutzers eines Geräts enthalten, der eine Transaktion mit Daten generiert, die den aktuellen Zustand der Software oder Firmware anzeigen, die in der Prozessanlage ausgeführt wird.

118. Verfahren zum Erstellen von Smart Contracts in einem Prozessleitsystem unter Verwendung eines Distributed Ledgers, der von mehreren Teilnehmern verwaltet wird, wobei das Verfahren umfasst: Generieren eines Smart Contracts, der sich auf eine Prozessanlage bezieht, die ein Feldgerät oder mehrere Feldgeräte aufweist, die jeweils durch einen Prozessor oder mehrere Prozessoren, eine physische Funktion zur Steuerung eines industriellen Prozesses ausführen; und Bereitstellen des Smart Contracts durch den einen Prozessor oder die mehreren Prozessoren an eine Adresse, die auf dem Distributed Ledger gespeichert ist, das von den mehreren Teilnehmern in einem Distributed-Ledger-Netzwerk verwaltet wird.

119. Verfahren nach Aspekt 118, wobei der Smart Contract einen Tokenwert in Übereinstimmung mit einem Ereignis empfängt oder bereitstellt, das in der Prozessanlage stattfindet.

120. Verfahren nach einem der Aspekte 118 oder 119, wobei das Generieren eines Smart Contracts in Bezug auf eine Prozessanlage das Generieren eines Smart Contracts umfasst, der einen Tokenwert von einer ersten Prozessanlage erhält, der bestimmt, dass ein Produkt von einer zweiten Prozessanlage an die erste Pro-

zessanlage übertragen wurde und der zweiten Prozessanlage den Tokenwert bereitstellt.

121. Verfahren nach einem der Aspekte 118-120, wobei der Smart Contract bestimmt, dass ein Produkt von der zweiten Prozessanlage an die erste Prozessanlage übertragen wurde, indem eine Transaktion von einem Nachweis-Orakel empfangen wird, die anzeigt, dass das Produkt in der ersten Prozessanlage empfangen wurde.

122. Verfahren nach einem der Aspekte 118-121, wobei das Generieren eines Smart Contracts, der sich auf eine Prozessanlage bezieht, ferner das Generieren eines Smart Contracts einschließt, der bestimmt, dass das Produkt eine Qualitätsmetrik oder mehrere Qualitätsmetriken erfüllt oder übertrifft, und der zweiten Prozessanlage den Tokenwert als Reaktion auf das Bestimmen, dass das Produkt eine oder mehrere Qualitätsmetriken erfüllt oder übertrifft, bereitstellt.

123. Verfahren nach einem der Aspekte 118-122, wobei der Smart Contract bestimmt, dass das Produkt eine Qualitätsmetrik oder mehrere Qualitätsmetriken erfüllt oder übertrifft, indem eine Transaktion oder mehrere Transaktionen von dem Nachweis-Orakel empfangen werden, die jeweils einen Produktparameterwert oder einen Prozessparameterwert enthalten und Vergleichen des Produktparameterwerts oder des Prozessparameterwerts mit einem Produkt- oder Prozessparameterschwellenwert, der in der einen oder den mehreren Qualitätsmetriken enthalten ist.

124. Verfahren nach einem der Aspekte 118-123, wobei das Generieren eines Smart Contracts, der sich auf eine Prozessanlage bezieht, das Generieren eines Smart Contracts umfasst, der Geräteinformationen für ein Gerät in der Prozessanlage erhält, bei dem ein Fehler auftritt, und die Geräteinformationen einem Gerätelieferanten als Reaktion auf die Anforderung, die Geräteinformationen weiterzugeben, bereitstellt.

125. Verfahren nach einem der Aspekte 118-124, wobei der Smart Contract Geräteinformationen durch Empfangen einer Transaktion von einem Nachweis-Orakel erhält, das die Geräteinformationen enthält.

126. Verfahren nach einem der Aspekte 118-125, wobei der Smart Contract eine Anfrage zum Teilen der Geräteinformationen durch Empfangen einer Transaktion empfängt, welche die Anfrage zusammen mit Identitätsdaten für einen Benutzer enthält, der die Anfrage ausgestellt hat, und der Smart Contract die Identitätsdaten in der Transaktion mit mehreren Sätzen von Identitätsdaten vergleicht, die Benutzern entsprechen, die autorisiert sind, anzufordern, dass das Distributed-Ledger-Netzwerk die Geräteinformationen teilt, und die Geräteinformationen an den Gerätelieferanten bereitstellen, wenn die Identitätsdaten in den mehreren Sätzen von Identitätsdaten enthalten sind.

127. Verfahren nach einem der Aspekte 118-126, wobei das Generieren eines Smart Contracts, der sich auf eine Prozessanlage bezieht, das Generieren eines Smart Contracts umfasst, der einen Parameter empfängt, der einer SIS-Vorrichtung (Safety Instrumented System) zugeordnet ist, und den Parameter in die SIS-Vorrichtung schreibt als Reaktion auf die Feststellung, dass ein Bediener, der den Parameter bereitgestellt hat, ein autorisierter Bediener ist.

128. Verfahren nach einem der Aspekte 118-127, wobei der Smart Contract einen Parameter empfängt, der einem SIS-Gerät zugeordnet ist, indem eine Transaktion empfangen wird, die den Parameter zusammen mit Identitätsdaten für den Bediener enthält, der die Transaktion bereitgestellt hat, und wobei bestimmt wird, dass ein Bediener, welcher den Parameter bereitstellt, ein autorisierter Bediener ist, schließt das Vergleichen der Identitätsdaten in der Transaktion mit mehreren Sätzen von Identitätsdaten ein, die Bedienern entsprechen, die autorisiert sind, dem SIS-Gerät zugeordnete Parameter anzupassen.

129. Verfahren nach einem der Aspekte 118-128, wobei der dem SIS-Gerät zugeordnete Parameter eine Aufforderung zum Sperren des SIS-Geräts ist.

130. Verfahren zur Interaktion mit einem Smart Contract in einem Prozessleitsystem unter Verwendung eines Distributed Ledgers, der von mehreren Teilnehmern verwaltet wird, wobei das Verfahren umfasst: Erhalten von Ereignisdaten von einem Ereignis, das in einer Prozessanlage stattfindet, die ein Feldgerät oder mehrere Feldgeräte aufweist, die jeweils eine physische Funktion ausführen, um einen industriellen Prozess zu steuern; als Reaktion auf die Bereitstellung eines Smart Contracts an eine Adresse, die im Distributed Ledger gespeichert ist, Generieren einer Transaktion, welche die Ereignisdaten enthält, durch ein Computergerät; und Übermitteln der Transaktion an den Smart Contract, der in dem Distributed Ledger gespeichert ist, das von den mehreren Teilnehmern in einem Distributed-Ledger-Netzwerk verwaltet wird.

131. Verfahren nach Aspekt 130, ferner umfassend: Erhalten von Identitätsdaten für das Computergerät; Ergänzen der Transaktion mit den Identitätsdaten für das Computergerät an dem

einen Prozessor oder den mehreren Prozessoren; Generieren einer kryptographischen Signatur auf der Grundlage der Transaktion bei dem einen Prozessor oder den mehreren Prozessoren; und Ergänzen der Transaktion mit der kryptographischen Signatur bei dem einen Prozessor oder den mehreren Prozessoren.

132. Verfahren nach einem der Aspekte 130 oder 131, ferner umfassend: Hinzufügen der Transaktion zu einem Transaktionsblock; Lösen eines kryptographischen Puzzles auf der Grundlage des Transaktionsblocks; Hinzufügen der Lösung des kryptographischen Puzzles zu dem Transaktionsblock; und Übermitteln des Transaktionsblocks an mindestens einen anderen Teilnehmer in dem Distributed-Ledger-Netzwerk.

133. Verfahren nach einem der Aspekte 130-132, wobei der Smart Contract einen Tokenwert von einer ersten Prozessanlage erhält und bestimmt, dass ein Produkt von einer zweiten Prozessanlage an die erste Prozessanlage übertragen wurde, und der zweiten Prozessanlage den Tokenwert bereitstellt, und wobei das Erhalten von Ereignisdaten von einem Ereignis, das in einer Prozessanlage stattfindet, umfasst: Erhalten einer Angabe, dass das Produkt in der ersten Prozessanlage empfangen wurde; und Generieren der Transaktion einschließlich der Identifikationsinformationen für die erste Prozessanlage, Identifikationsinformationen für das Produkt und einer Angabe, dass das Produkt in der ersten Prozessanlage von der zweiten Prozessanlage empfangen wurde.

134. Verfahren nach einem der Aspekte 130-133, wobei das Erhalten einer Angabe, dass das Produkt in der ersten Prozessanlage empfangen wurde, ferner Folgendes umfasst: Erhalten eines Produktparameterwertes oder mehrerer Produktparameterwerte für das Produkt oder eines Prozessparameterwertes oder mehrerer Prozessparameterwerte für Prozessanlageneinheiten, die an der Herstellung des Produkts beteiligt sind; und Generieren der Transaktion, die einen Produktparameterwert oder mehrere Produktparameterwerte oder einen Prozessparameterwert oder mehrere Prozessparameterwerte enthält.

135. Verfahren nach einem der Aspekte 130-134, wobei der Smart Contract Geräteinformationen für ein Gerät in der Prozessanlage erhält, bei welcher ein Fehler auftritt, und die Geräteinformationen einem Gerätelieferanten als Reaktion auf den Empfang einer Aufforderung zum Teilen der Geräteinformationen bereitstellt, und wobei das Erhalten von Ereignisdaten von einem Ereignis, das in einer Prozessanlage stattfindet, umfasst: Erhalten von Geräteinformationen für das Gerät; und Generieren der Transaktion, welche Identifikationsinformationen für das Gerät und die Geräteinformationen einschließt.

136. Verfahren nach einem der Aspekte 130-135, wobei der Smart Contract einen Parameter empfängt, der einem Sicherheitsinstrumentensystemgerät (SIS) zugeordnet ist, und den Parameter als Reaktion auf die Bestimmung, dass es sich um einen Bediener handelt, der den Parameter bereitgestellt hat, ein autorisierter Bediener ist, in das SIS-Gerät schreibt und wobei das Erhalten von Ereignisdaten von einem Ereignis, das in einer Prozessanlage stattfindet, Folgendes einschließt: Erhalten einer Aufforderung zum Ändern Parameters, der einem SIS-Gerät zugeordnet ist; und Generieren der Transaktion, welche Identifikationsinformationen für das SIS-Gerät, den geänderten Parameter und einem neuen Parameterwert für den geänderten Parameter einschließt.

137. Computergerät zum Erstellen von Smart Contracts in einem Prozessleitsystem unter Verwendung eines Distributed Ledgers, der von mehreren Teilnehmern verwaltet wird, umfassend: einen Prozessor oder mehrere Prozessoren; eine Kommunikationseinheit; und ein nichtvorübergehendes computerlesbares Medium, das mit dem einen Prozessor oder den mehreren Prozessoren und der Kommunikationseinheit gekoppelt ist und Anweisungen darauf speichert, die, wenn sie von dem einen Prozessor oder den mehreren Prozessoren ausgeführt werden, das Computergerät veranlassen, einen Smart Contract in Bezug auf eine Prozessanlage zu generieren, welche ein Feldgerät oder mehrere Feldgeräte aufweist, die jeweils eine physische Funktion zur Steuerung eines industriellen Prozesses ausführen; und Bereitstellen des Smart Contracts an eine Adresse, die in dem Distributed Ledger gespeichert ist, das von den mehreren Teilnehmern in einem Distributed-Ledger-Netzwerk verwaltet wird.

138. Computergerät nach Aspekt 137, wobei der Smart Contract einen Tokenwert in Übereinstimmung mit einem Ereignis empfängt oder bereitstellt, das in der Prozessanlage stattfindet.

139. Computergerät nach einem der Aspekte 137 oder 138, wobei der Smart Contract einen Tokenwert von einer ersten Prozessanlage erhält, feststellt, dass ein Produkt von einer zweiten Prozessanlage an die erste Prozessanlage übertragen wurde, und der zweiten Prozessanlage den Tokenwert bereitstellt.

140. Computergerät nach einem der Aspekte 137-139, wobei der Smart Contract bestimmt, dass ein Produkt von der zweiten Prozessanlage an die erste Prozessanlage übertragen wurde, indem eine Transaktion von einem Nachweis-

Orakel empfangen wird, das anzeigt, dass das Produkt bei der ersten Prozessanlage empfangen wurde.

141. Computergerät nach einem der Aspekte 137-140, wobei der Smart Contract bestimmt, dass das Produkt eine Qualitätsmetrik oder mehrere Qualitätsmetriken erfüllt oder übertrifft, und der zweiten Prozessanlage den Tokenwert als Reaktion auf das Bestimmen bereitstellt, dass das Produkt die eine Qualitätsmetrik oder die mehreren Qualitätsmetriken erfüllt oder übertrifft.

142. Computergerät nach einem der Aspekte 137-141, wobei der Smart Contract bestimmt, dass das Produkt eine Qualitätsmetrik oder mehrere Qualitätsmetriken erfüllt oder übertrifft, indem eine Transaktion oder mehrere Transaktionen von dem Nachweis-Orakel empfangen werden, die jeweils einen Produktparameterwert oder einen Prozessparameterwert enthalten und Vergleichen des Produktparameterwerts oder des Prozessparameterwerts mit einem Produkt- oder Prozessparameterschwellenwert, der in der einen Qualitätsmetrik oder den mehreren Qualitätsmetriken enthalten ist.

143. Computergerät nach einem der Aspekte 137-142, wobei der Smart Contract Geräteinformationen für ein Gerät in der Prozessanlage erhält, bei dem ein Fehler auftritt, und die Geräteinformationen einem Gerätelieferanten als Reaktion auf den Empfang einer Aufforderung zum Teilen der Geräteinformationen bereitstellt.

144. Computergerät nach einem der Aspekte 137-143, wobei der Smart Contract Geräteinformationen durch Empfangen einer Transaktion von einem Nachweis-Orakel erhält, das die Geräteinformationen einschließt.

145. Computergerät nach einem der Aspekte 137-144, wobei der Smart Contract eine Aufforderung zum Teilen der Geräteinformationen durch Empfangen einer Transaktion empfängt, welche die Aufforderung zusammen mit Identitätsdaten für einen Benutzer enthält, der die Aufforderung ausgegeben hat, und der Smart Contract die Identitätsdaten in der Transaktion mit mehreren Sätzen von Identitätsdaten vergleicht, die Benutzern entsprechen, die autorisiert sind, aufzufordern, dass das Distributed-Ledger-Netzwerk die Geräteinformationen teilt, und die Geräteinformationen an den Gerätelieferanten bereitstellen, wenn die Identitätsdaten in den mehreren Sätzen von Identitätsdaten enthalten sind.

146. Computergerät nach einem der Aspekte 137-145, wobei der Smart Contract einen Parameter empfängt, der einer SIS-Vorrichtung (Safety Instrumented System) zugeordnet ist, und den Parameter als Reaktion auf das Bestimmen, dass ein Bediener, der den Parameter bereitgestellt hat, ein autorisierter Bediener ist, in die SIS-Vorrichtung schreibt.

147. Computergerät nach einem der Aspekte 137-146, wobei der Smart Contract einen Parameter empfängt, der einer SIS-Vorrichtung zugeordnet ist, indem eine Transaktion empfangen wird, welche den Parameter zusammen mit Identitätsdaten für den Bediener enthält, der die Transaktion bereitgestellt hat, und wobei bestimmt wird, dass ein Bediener, der den Parameter bereitgestellt hat, ein autorisierter Bediener ist, schließt das Vergleichen der Identitätsdaten in der Transaktion mit mehreren Sätzen von Identitätsdaten ein, welche den Bedienern entsprechen, die zum Anpassen von Parametern autorisiert sind, welche dem SIS-Gerät zugeordnet sind.

148. Computergerät nach einem der Aspekte 137-147, wobei der dem SIS-Gerät zugeordnete Parameter eine Aufforderung zum Sperren des SIS-Geräts ist.

149. System zur Interaktion mit Smart Contracts in einem Prozessleitsystem, das einen Distributed Ledger verwendet, der von mehreren Teilnehmern verwaltet wird, umfassend: ein Gerät oder mehrere Geräte, die in einer Prozessanlage angeordnet sind und jeweils eine physische Funktion zur Steuerung eines industriellen Prozesses ausführen; und ein Computergerät, das in der Prozessanlage ausgeführt wird, einschließend einen Prozessor oder mehrere Prozessoren; eine Kommunikationseinheit; und ein nichtvorübergehendes computerlesbares Medium, das mit dem einen Prozessor oder den mehreren Prozessoren und der Kommunikationseinheit gekoppelt ist und Anweisungen darauf speichert, die, wenn sie von dem einen Prozessor oder den mehreren Prozessoren ausgeführt werden, das Computergerät veranlassen, über das eine Gerät oder die mehreren Geräte Folgendes zu erhalten: Ereignisdaten von einem Ereignis, das in der Prozessanlage stattfindet; Generieren einer Transaktion, welche die Ereignisdaten enthält, als Reaktion auf die Bereitstellung eines Smart Contracts an eine im Distributed Ledger gespeicherte Adresse; und Übermitteln der Transaktion an den Smart Contract, der auf dem Distributed Ledger gespeichert ist, das von den mehreren Teilnehmern in einem Distributed-Ledger-Netzwerk verwaltet wird.

150. System nach Aspekt 149, wobei die Anweisungen das Computergerät ferner veranlassen, Identitätsdaten für das Computergerät zu erhalten; die Transaktion mit den Identitätsdaten für das Computergerät zu ergänzen; eine kryptographische Signatur auf der Grundlage der Trans-

aktion zu generieren; und die Transaktion mit der kryptographischen Signatur zu ergänzen.

151. System nach einem der Aspekte 149 oder 150, wobei die Anweisungen das Computergerät ferner veranlassen: die Transaktion zu einem Transaktionsblock hinzuzufügen; ein kryptographisches Puzzle auf der Grundlage des Transaktionsblocks zu lösen, die Lösung des kryptographischen Puzzles zum Transaktionsblock hinzuzufügen; und den Transaktionsblock an mindestens einen anderen Teilnehmer in dem Distributed-Ledger-Netzwerk zu übermitteln.

152. System nach einem der Aspekte 149-151, wobei der Smart Contract einen Tokenwert von einer ersten Prozessanlage erhält, feststellt, dass ein Produkt von einer zweiten Prozessanlage an die erste Prozessanlage übertragen wurde, und der zweiten Prozessanlage den Tokenwert bereitstellt, und wobei, um Ereignisdaten von einem Ereignis zu erhalten, das in der Prozessanlage stattfindet, die Anweisungen das Computergerät veranlassen: eine Angabe zu erhalten, dass das Produkt in der ersten Prozessanlage empfangen wurde; und die Transaktion, welche Identifikationsinformationen für die erste Prozessanlage, Identifikationsinformationen für das Produkt und eine Angabe, dass das Produkt in der ersten Prozessanlage von der zweiten Prozessanlage empfangen wurde, einschließt.

153. System nach einem der Aspekte 149-152, wobei zum Erhalten einer Angabe, dass das Produkt in der ersten Prozessanlage empfangen wurde, die Anweisungen das Computergerät veranlassen: einen Produktparameterwert oder mehrere Produktparameterwerte für das Produkt oder einen Prozessparameterwert oder mehrere Prozessparameterwerte für Prozessanlageneinheiten zu erhalten, die an der Herstellung des Produkts beteiligt sind; und die Transaktion zu generieren, welche einen Produktparameterwert oder mehrere Produktparameterwerte oder einen Prozessparameterwert oder mehrere Prozessparameterwerte enthält.

154. System nach einem der Aspekte 149-153, wobei der Smart Contract Geräteinformationen für ein Gerät in der Prozessanlage erhält, bei dem ein Fehler auftritt, und die Geräteinformationen einem Gerätelieferanten als Reaktion auf den Empfang einer Aufforderung zum Teilen der Geräteinformationen bereitstellt, und wobei, um Ereignisdaten von einem Ereignis zu erhalten, das in einer Prozessanlage stattfindet, die Anweisungen das Computergerät veranlassen: Geräteinformationen für das Gerät zu erhalten; und die Transaktion zu generieren, welche Identifikationsinformationen für das Gerät und die Geräteinformationen enthält.

155. System nach einem der Aspekte 149-154, wobei der Smart Contract einen Parameter empfängt, der einem Sicherheitsinstrumentensystemgerät (SIS) zugeordnet ist, und den Parameter als Reaktion auf die Feststellung, dass ein Bediener, der den Parameter bereitgestellt hat, ein autorisierter Bediener ist, auf das SIS-Gerät schreibt, und wobei, um die Ereignisdaten eines Ereignisses zu erhalten, das in einer Prozessanlage stattfindet, die Anweisungen das Computergerät veranlassen: eine Aufforderung zum Ändern eines Parameters, der einem SIS-Gerät zugeordnet ist, zu erhalten; und die Transaktion zu generieren, welche Identifikationsinformationen für das SIS-Gerät, den geänderten Parameter und einen neuen Parameterwert für den geänderten Parameter einschließt.

[0151] Wenn sie in Software implementiert sind, können beliebige der vorliegend beschriebenen Anwendungen, Dienste und Antriebe in jedem materiellen, nichtvorübergehenden computerlesbaren Speicher, beispielsweise auf einer Magnetplatte, einer Laserplatte, einer Festkörper-Speichervorrichtung, einer molekularen Speichervorrichtung oder einem anderen Speichermedium, in einem RAM oder ROM eines Computers oder Prozessors usw. gespeichert werden. Obwohl die vorliegend offenbarten beispielhaften Systeme als Systeme offenbart werden, welche unter anderem Komponenten, Software und/oder Firmware einschließen, welche auf Hardware ausgeführt wird, ist festzustellen, dass diese Systeme lediglich der Veranschaulichung dienen und nicht als einschränkend betrachtet werden sollten. Zum Beispiel wird in Betracht gezogen, dass beliebige oder alle dieser Hardware-, Software- und Firmware-Komponenten ausschließlich in Hardware, ausschließlich in Software oder in beliebiger Kombination von Hardware und Software ausgeführt werden können. Während die vorliegend beschriebenen beispielhaften Systeme als in Software implementiert beschrieben werden, die auf einem Prozessor eines Computergeräts oder mehrerer Computergeräte ausgeführt wird, werden Durchschnittsfachleute leicht erkennen, dass die bereitgestellten Beispiele nicht die einzige Möglichkeit sind, solche Systeme zu implementieren.

[0152] Während die vorliegende Erfindung unter Bezugnahme auf spezifische Beispiele beschrieben wurde, die nur veranschaulichend sein sollen und die Erfindung nicht beschränken sollen, ist es für den Durchschnittsfachmann offensichtlich, dass Änderungen, Hinzufügungen oder Streichungen zu den offenbarten Ausführungsformen möglich sind, ohne vom Geist und Umfang der Erfindung abzuweichen.

Patentansprüche

1. Verfahren für das Aufzeichnen von Zuständen von Software oder Firmware in einem Prozessleitsys-

tem und der verbundenen Instrumentierung, welche einen Distributed Ledger verwendet, welcher durch mehrere Teilnehmer verwaltet wird, das Verfahren umfassend:
Erhalten, durch ein Computergerät, eines aktuellen Zustands von Software oder Firmware, die in einer Prozessanlage ausgeführt werden, welche ein Feldgerät oder mehrere Feldgeräte aufweist, die jeweils eine physische Funktion zur Steuerung eines industriellen Prozesses ausführen, wobei die Software oder Firmware in einem Netzwerk oder einer Prozesssteuerungsvorrichtung in der Prozessanlage ausgeführt werden;
Generieren einer Transaktion, die den aktuellen Zustand der Software oder Firmware einschließt, die in der Prozessanlage ausgeführt wird, wobei die Transaktion in dem Distributed Ledger gespeichert ist; und
Übermitteln der Transaktion an mindestens einen anderen Teilnehmer in einem Distributed-Ledger-Netzwerk von Teilnehmern, die den Distributed Ledger verwalten.

2. Verfahren nach Anspruch 1, wobei der aktuelle Zustand der Software oder Firmware, welche in der Prozessanlage ausgeführt werden, von einem Computergerät eines Benutzers erhalten wird, der den aktuellen Zustand aktualisiert hat, und das Generieren der Transaktion ferner Folgendes umfasst:
Erhalten von Identitätsdaten für den Benutzer;
Ergänzen der Transaktion mit den Identitätsdaten für den Benutzer bei dem einen Prozessor oder den mehreren Prozessoren;
Generieren einer kryptographischen Signatur auf der Grundlage der Transaktion bei dem einen Prozessor oder den mehreren Prozessoren; und
Ergänzen der Transaktion mit der kryptographischen Signatur bei dem einen Prozessor oder den mehreren Prozessoren, und/oder
wobei das Generieren einer Transaktion, welche den aktuellen Zustand der Software oder Firmware einschließt, welche in der Prozessanlage ausgeführt wird, das Generieren der Transaktion einschließlich einem kryptographischen Hashwert einschließt, welcher dem aktuellen Zustand der Software oder Firmware entspricht, welche in der Prozessanlage ausgeführt werden, und/oder
ferner umfassend:
Erhalten eines Zustands der Software oder Firmware, die in der Prozessanlage ausgeführt werden, von dem Netzwerk oder der Prozesssteuerungsvorrichtung, welche die Software oder Firmware ausführen; und
Vergleichen des Zustands der Software oder Firmware, die in der Prozessanlage ausgeführt werden, mit dem kryptographischen Hashwert von dem Distributed Ledger, um sicherzustellen, dass die Software oder Firmware nicht manipuliert wurden, und/oder
ferner umfassend:
als Reaktion auf das Feststellen, dass der Zustand der Software oder Firmware, die in der Prozessanlage ausgeführt werden, nicht mit dem aktuellen Zustand der Software oder Firmware übereinstimmt, die in dem Distributed Ledger gemäß dem kryptographischen Hashwert gespeichert ist, wird verhindert, dass die Software oder Firmware in der Prozessanlage ausgeführt wird, und/oder
ferner umfassend:
Veranlassen, dass die Software oder Firmware zu einem vorherigen Zustand zurückkehrt, und/oder
ferner umfassend:
als Reaktion auf das Bestimmen, dass der Zustand der Software oder Firmware, die in der Prozessanlage ausgeführt werden, mit dem aktuellen Zustand der Software oder Firmware übereinstimmt, der in dem Distributed Ledger gemäß dem kryptographischen Hashwert gespeichert ist, veranlassen, dass das Netzwerk oder die Prozesssteuerungsvorrichtung die Software oder Firmware ausführen.

3. Verfahren nach Anspruch 1 oder 2, insbesondere nach Anspruch 2, ferner umfassend:
Hinzufügen der Transaktion zu einem Transaktionsblock;
Lösen eines kryptographischen Puzzles auf der Grundlage des Transaktionsblocks;
Hinzufügen der Lösung des kryptographischen Puzzles zu dem Transaktionsblock; und
Übermitteln des Transaktionsblocks an mindestens einen anderen Teilnehmer im Distributed-Ledger-Netzwerk, und/oder
ferner umfassend:
Vergleichen der Identitätsdaten in der Transaktion mit mehreren Sätzen von Identitätsdaten, die Benutzern entsprechen, die autorisiert sind, den Zustand der Software oder Firmware zu aktualisieren, die in der Prozessanlage ausgeführt werden; und
Hinzufügen der Transaktion zu dem Transaktionsblock, wenn die Identitätsdaten in den mehreren Sätzen von Identitätsdaten enthalten sind.

4. Verfahren nach einem der Ansprüche 1 bis 3, insbesondere nach Anspruch 1, , wobei der Distributed Ledger eine Permissioned Blockchain ist.

5. System für das Aufzeichnen von Zuständen von Software oder Firmware in einem Prozessleitsystem und der verbundenen Instrumentierung, unter Verwendung eines Distributed Ledgers, welcher durch mehrere Teilnehmer verwaltet wird und Folgendes umfasst:
ein Gerät oder mehrere Geräte, die in einer Prozessanlage angeordnet sind und jeweils eine physische Funktion zur Steuerung eines industriellen Prozesses ausführen; und
ein Computergerät, das in der Prozessanlage ausgeführt wird und Folgendes umfasst:
einen Prozessor oder mehrere Prozessoren;
eine Kommunikationseinheit; und
ein nichtvorübergehendes computerlesbares Medium, das mit dem einen Prozessor oder den mehre-

ren Prozessoren und der Kommunikationseinheit gekoppelt ist und Anweisungen darauf speichert, die, wenn sie von dem einen Prozessor oder den mehreren Prozessoren ausgeführt werden, das Computergerät veranlassen:
einen aktuellen Zustand von Software oder Firmware zu erhalten, die in der Prozessanlage ausgeführt werden, wobei die Software oder Firmware in mindestens einem Gerät der in der Prozessanlage angeordneten Geräte oder einem Netzwerkgerät in der Prozessanlage ausgeführt wird;
eine Transaktion zu generieren, die den aktuellen Zustand der Software oder Firmware enthält, die in der Prozessanlage ausgeführt wird, wobei die Transaktion in dem Distributed Ledger gespeichert ist; und
die Transaktion an mindestens einen anderen Teilnehmer in einem Distributed-Ledger-Netzwerk von Teilnehmern zu übermitteln, welche den Distributed Ledger verwalten, um die Transaktion im Distributed Ledger zu validieren und aufzuzeichnen.

6. System nach Anspruch 5, wobei der aktuelle Zustand der Software oder Firmware, die in der Prozessanlage ausgeführt werden, von einem Computergerät eines Benutzers erhalten wird, der den aktuellen Zustand aktualisiert hat, und die Transaktion zu generieren, wobei die Anweisungen das Computergerät veranlassen:
Identitätsdaten für den Benutzer zu erhalten;
die Transaktion mit den Identitätsdaten für den Benutzer zu ergänzen;
eine kryptographische Signatur auf der Grundlage der Transaktion zu generieren; und
die Transaktion mit der kryptographischen Signatur zu ergänzen, und/oder
wobei die Transaktion mit einem kryptographischen Hashwert generiert wird, welcher dem aktuellen Zustand der Software oder Firmware entspricht, welche in der Prozessanlage ausgeführt werden, und/oder
ferner umfassend:
ein Servergerät, welches Folgendes einschließt:
einen Prozessor oder mehrere Prozessoren;
eine Kommunikationseinheit; und
ein nichtvorübergehendes computerlesbares Medium, das mit dem einen Prozessor oder den mehreren Prozessoren und der Kommunikationseinheit gekoppelt ist und Anweisungen darauf speichert, die, wenn sie von dem einen oder den mehreren Prozessoren ausgeführt werden, das Servergerät veranlassen:
einen Zustand der Software oder Firmware, die in der Prozessanlage ausgeführt werden, von dem Netzwerk oder dem Prozesssteuerungsgerät, welche die Software oder Firmware ausführen, zu erhalten; und
den Zustand der Software oder Firmware, die in der Prozessanlage ausgeführt werden, mit dem kryptographischen Hashwert von dem Distributed Ledger zu vergleichen, um sicherzustellen, dass die Software oder Firmware
nicht manipuliert wurden, und/oder
wobei die Anweisungen ferner das Servergerät veranlassen:
als Reaktion auf die Feststellung, dass der Zustand der Software oder Firmware, die in der Prozessanlage ausgeführt werden, nicht mit dem aktuellen Zustand der Software oder Firmware übereinstimmt, die in dem Distributed Ledger gemäß dem kryptographischen Hashwert gespeichert ist, wird verhindert, dass die Software oder Firmware in der Prozessanlage ausgeführt werden, und/oder
wobei die Anweisungen ferner das Servergerät veranlassen:
die Software oder Firmware in einen vorherigen Zustand zurückzuversetzen, und/oder wobei die Anweisungen ferner das Servergerät veranlassen:
als Reaktion auf die Feststellung, dass der Zustand der Software oder Firmware, die in der Prozessanlage ausgeführt werden, mit dem aktuellen Zustand der Software oder Firmware übereinstimmt, der in dem Distributed Ledger gemäß dem kryptographischen Hashwert gespeichert ist, das Netzwerk oder die Prozesssteuerungsvorrichtung veranlasst werden, die Software oder Firmware auszuführen.

7. System nach einem der Ansprüche 5 oder 6, insbesondere nach Anspruch 6 , wobei die Anweisungen ferner das Computergerät veranlassen:
die Transaktion zu einem Transaktionsblock hinzuzufügen;
ein kryptographisches Puzzle auf der Grundlage des Transaktionsblocks zu lösen;
die Lösung des kryptographischen Puzzles zum Transaktionsblock hinzuzufügen; und
den Transaktionsblock an mindestens einen anderen Teilnehmer im Distributed-Ledger-Netzwerk zu übermitteln, und/oder
wobei die Anweisungen ferner das Computergerät veranlassen:
die Identitätsdaten in der Transaktion mit mehreren Sätzen von Identitätsdaten zu vergleichen, die Benutzern entsprechen, die autorisiert sind, den Zustand der Software oder Firmware zu aktualisieren, die in der Prozessanlage ausgeführt werden; und
die Transaktion zum Transaktionsblock hinzuzufügen, wenn die Identitätsdaten in den mehreren Sätzen von Identitätsdaten enthalten sind.

8. System nach einem der Ansprüche 5 bis 7, insbesondere nach Anspruch 5 , wobei der Distributed Ledger eine Permissioned Blockchain ist.

9. Validierungs-Netzwerkknoten in einer Prozessanlage auf einem Distributed-Ledger-Netzwerk, umfassend:
einen Transceiver, der konfiguriert ist, um mit einem Feldgerät oder mehreren Feldgeräten zu kommunizieren, von denen jedes eine physische Funktion zur Steuerung eines industriellen Prozesses in der Prozessanlage ausführt, und um Daten des Distributed Ledgers mit Peer-Netzwerkknoten auszutauschen,

wobei die Daten des Distributed Ledgers Transaktionen umfassen, die Daten enthalten, die den aktuellen Zustand der Software oder Firmware anzeigen, die in der Prozessanlage ausgeführt wird;
ein Speichermedium, das zum Speichern einer Kopie des Distributed Ledgers konfiguriert ist; und
einen Prozessdatenvalidierer, der konfiguriert ist, um einen Satz von Konsensregeln auf die von den Peer-Netzwerkknoten empfangenen Daten des Distributed Ledgers anzuwenden, wobei der Prozessdatenvalidierer ferner konfiguriert ist, um die von den Peer-Netzwerkknoten empfangenen Daten des Distributed Ledgers an die Kopie des Distributed Ledgers anzuhängen wenn die Daten des Distributed Ledgers den Konsensregeln entsprechen.

10. Validierungs-Netzwerkknoten nach Anspruch 9, wobei Daten des Distributed Ledgers, die von Peer-Knoten empfangen wurden, anzuhängen sind, wobei der Transaktionsvalidierer konfiguriert ist, um:
ein kryptographisches Puzzle auf der Grundlage eines Transaktionsblocks zu lösen;
die Lösung des kryptographischen Puzzles zum Transaktionsblock hinzuzufügen;
den Transaktionsblock an die Kopie des Distributed Ledgers anzuhängen; und
den Transaktionsblock an mindestens einen der Peer-Netzwerkknoten im Distributed-Ledger-Netzwerk zu übermitteln.

11. Validierungs-Netzwerkknoten nach Anspruch 9 oder 10, insbesondere nach Anspruch 9, wobei der Satz von Konsensregeln mindestens eines von Folgendem umfasst:
Formatierungsanforderungen für Transaktionen oder Transaktionsblöcke;
einen Mechanismus zum Bestimmen, welcher der Peer-Netzwerkknoten eine nächste Transaktion oder einen nächsten Transaktionsblock zum Distributed Ledger hinzufügt; oder
ein kryptographischer Hashing-Algorithmus zum Hashing von Software- oder Firmware-Zustandsdaten, die in jeder der Transaktionen enthalten sind.

12. Validierungs-Netzwerkknoten nach einem der Ansprüche 9 bis 11, insbesondere nach Anspruch 9, wobei die Daten des Distributed Ledgers, die von den Peer-Knoten empfangen wurden, einen Identitätsnachweis eines Benutzers eines Geräts einschließt, welches eine Transaktion generiert, welche Daten aufweist, die den aktuellen Zustand der Software oder Firmware anzeigen, welche in der Prozessanlage ausgeführt wird.

13. Computerlesbares Speichermedium, welches Instruktionen enthält, um mindestens einen Prozessor zu veranlassen ein Verfahren nach einem der Ansprüche 1 bis 4 zu implementieren.

Es folgen 18 Seiten Zeichnungen

Anhängende Zeichnungen

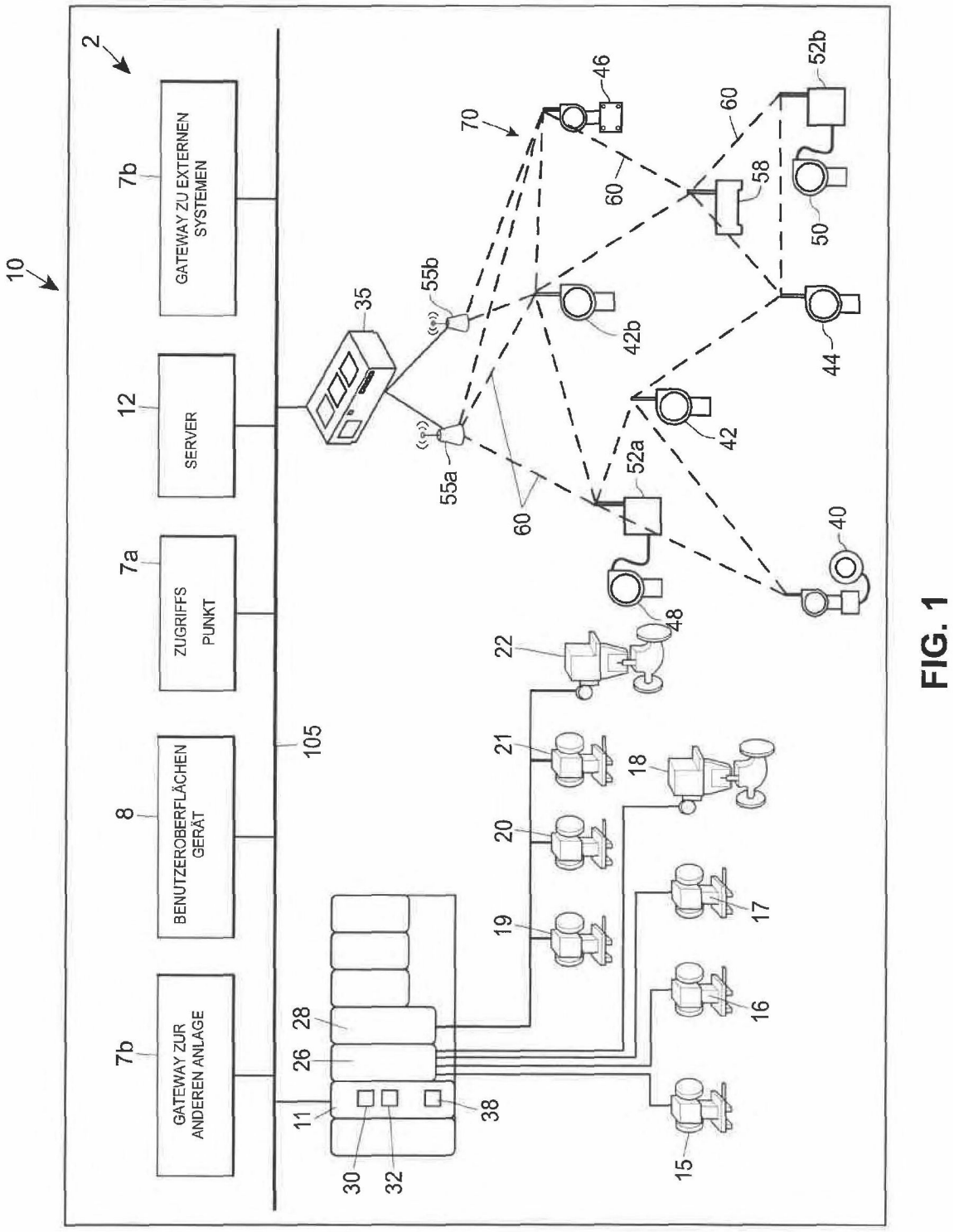


FIG. 1

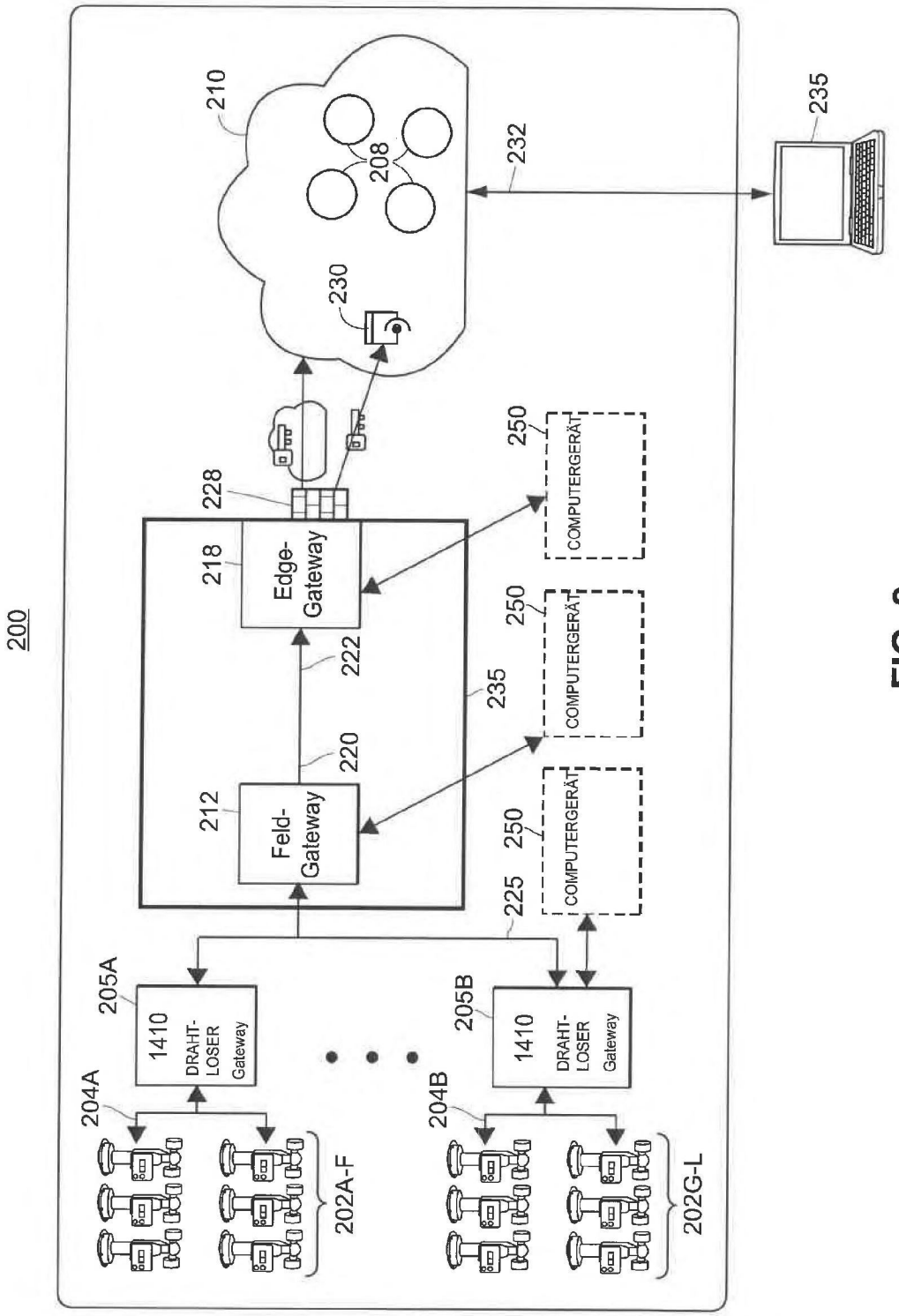

200
210
208
232
235
230
228
218
Edge-Gateway
222
250
COMPUTERGERÄT
235
220
212
Feld-Gateway
225
205A
1410
DRAHT-LOSER Gateway
205B
204A
204B
202A-F
202G-L

FIG. 2

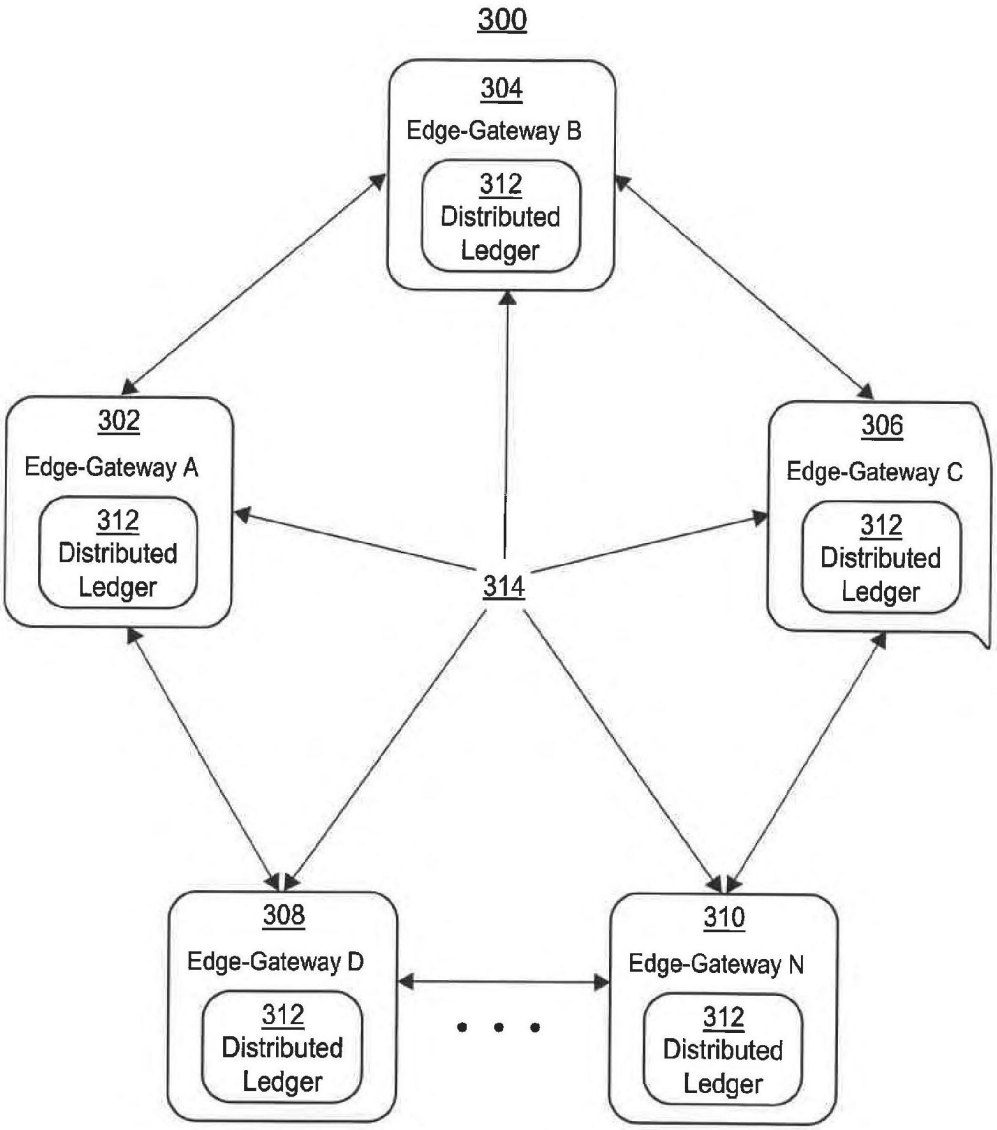

300
304
Edge-Gateway B
312
Distributed
Ledger
302
Edge-Gateway A
312
Distributed
Ledger
306
Edge-Gateway C
312
Distributed
Ledger
314
308
Edge-Gateway D
312
Distributed
Ledger
310
Edge-Gateway N
312
Distributed
Ledger

FIG. 3

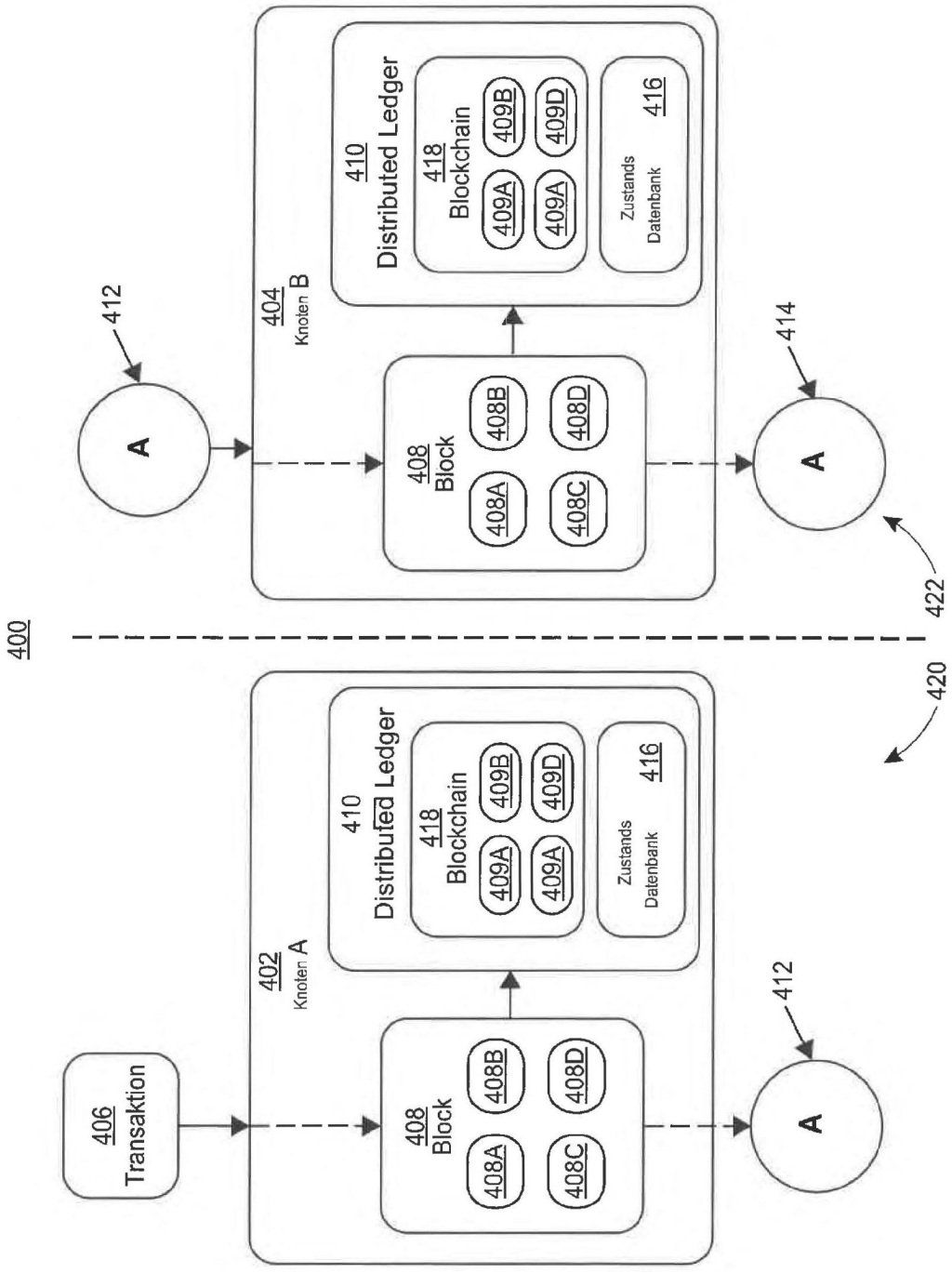

400
406
Transaktion
402
Knoten A
408
Block
408A
408B
408C
408D
410
Distributed Ledger
418
Blockchain
409A
409B
409A
409D
Zustands
Datenbank
416
412
A
404
Knoten B
414
422
420

FIG. 4

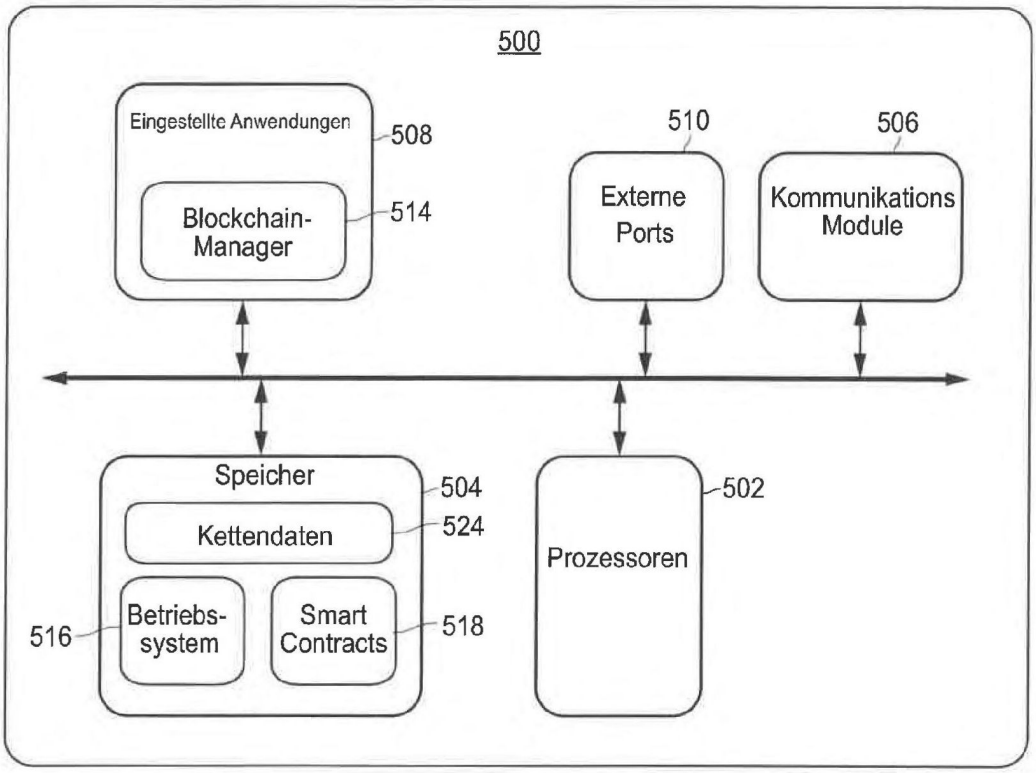

500
Eingestellte Anwendungen
508
Blockchain-Manager
514
510
Externe Ports
506
Kommunikations Module
Speicher
504
Kettendaten
524
Betriebs-system
516
Smart Contracts
518
Prozessoren
502

FIG. 5

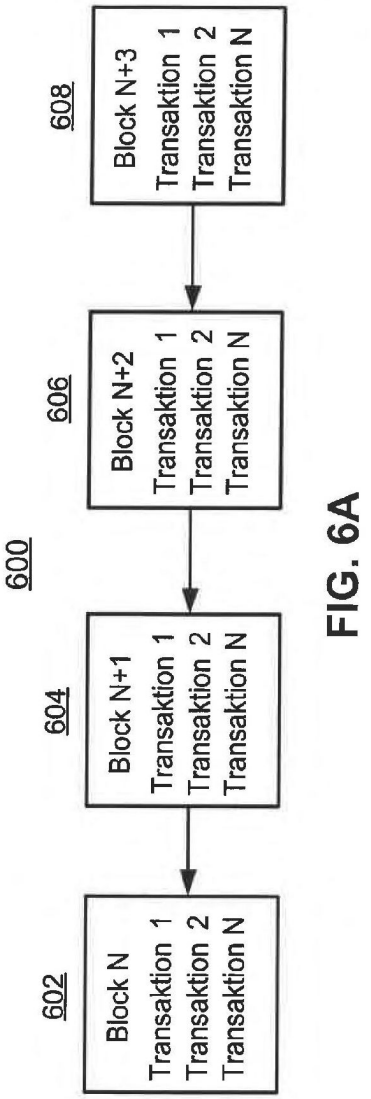

600
602
Block N
Transaktion 1
Transaktion 2
Transaktion N
604
Block N+1
Transaktion 1
Transaktion 2
Transaktion N
606
Block N+2
Transaktion 1
Transaktion 2
Transaktion N
608
Block N+3
Transaktion 1
Transaktion 2
Transaktion N

FIG. 6A

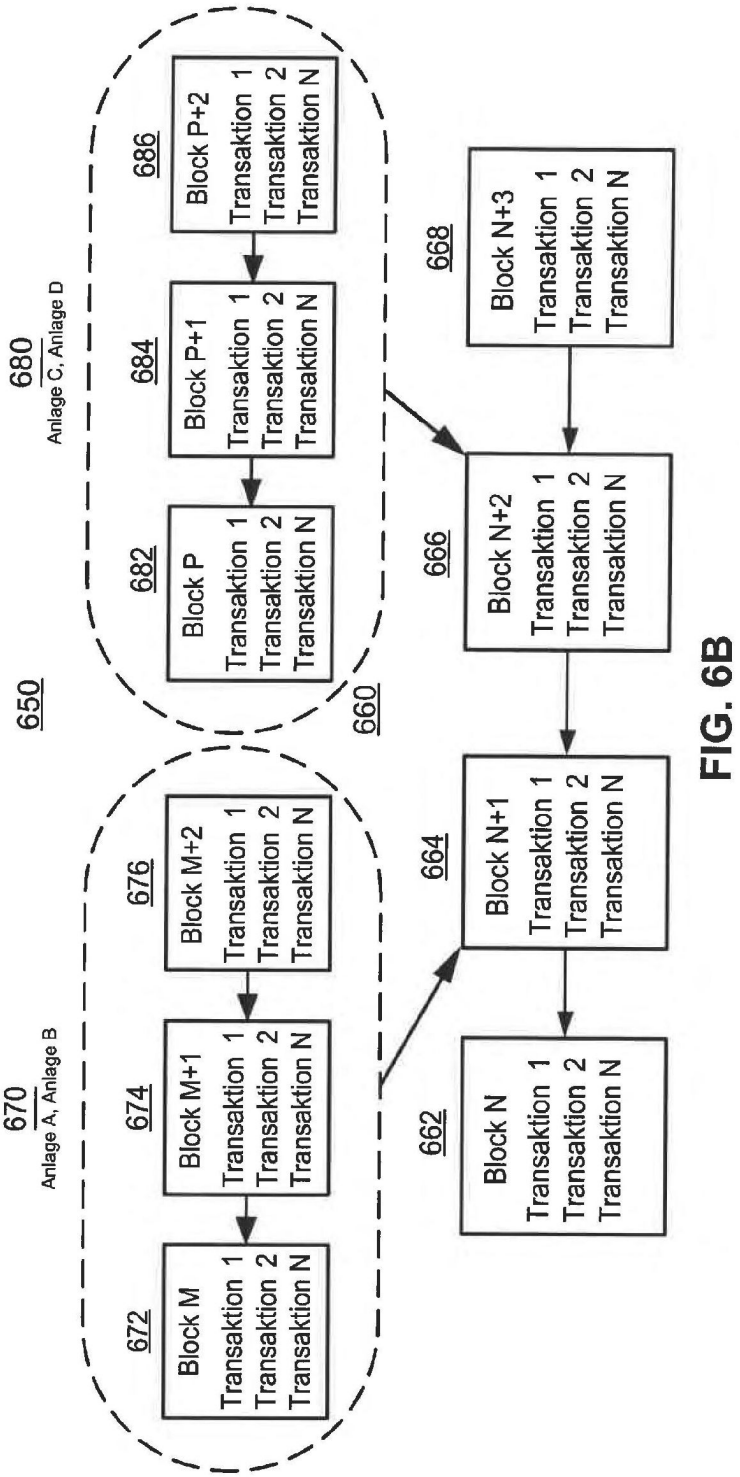

650
660
670
Anlage A, Anlage B
672
Block M
Transaktion 1
Transaktion 2
Transaktion N
674
Block M+1
Transaktion 1
Transaktion 2
Transaktion N
676
Block M+2
Transaktion 1
Transaktion 2
Transaktion N
680
Anlage C, Anlage D
682
Block P
Transaktion 1
Transaktion 2
Transaktion N
684
Block P+1
Transaktion 1
Transaktion 2
Transaktion N
686
Block P+2
Transaktion 1
Transaktion 2
Transaktion N
662
Block N
Transaktion 1
Transaktion 2
Transaktion N
664
Block N+1
Transaktion 1
Transaktion 2
Transaktion N
666
Block N+2
Transaktion 1
Transaktion 2
Transaktion N
668
Block N+3
Transaktion 1
Transaktion 2
Transaktion N

FIG. 6B

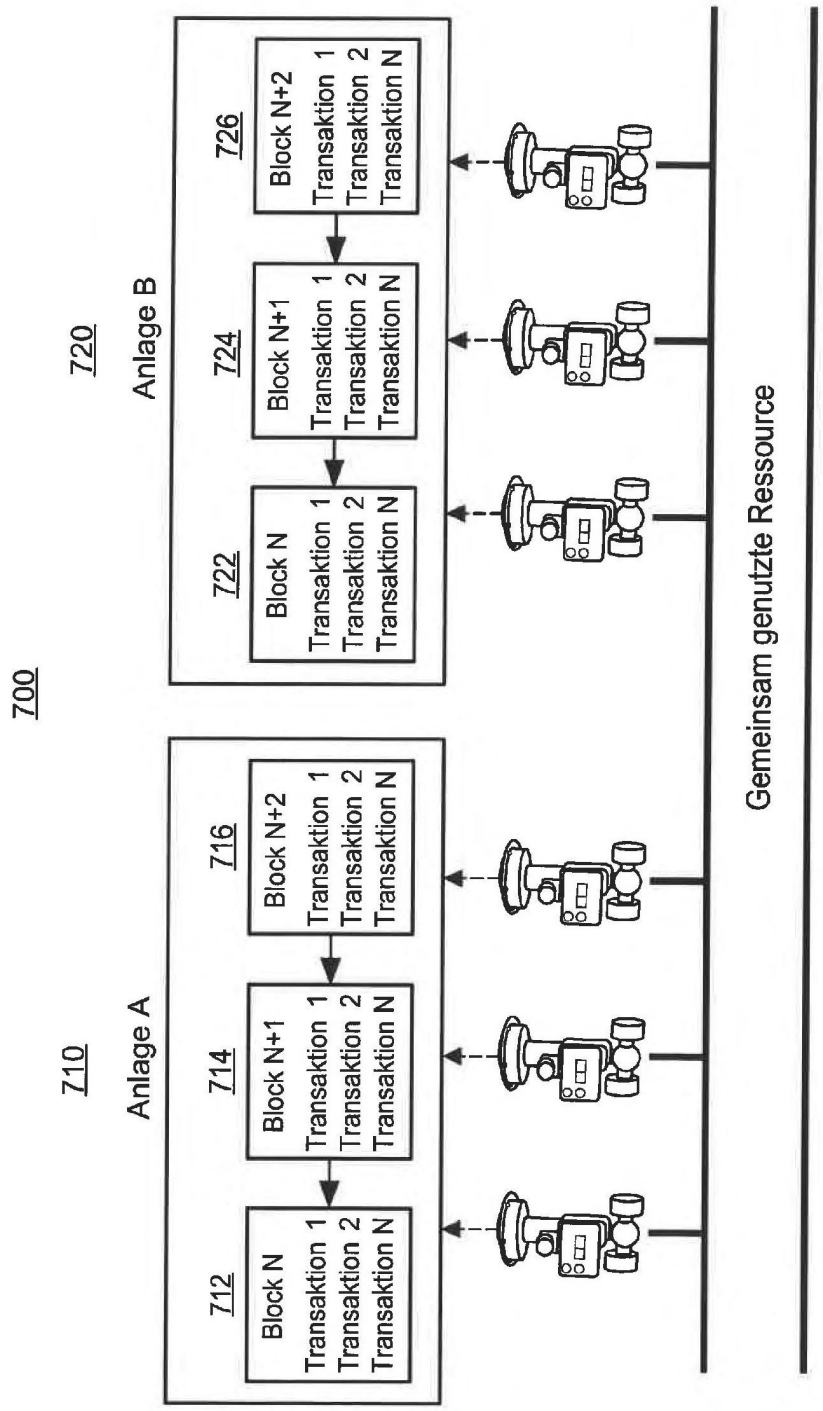

700
710
Anlage A
712
Block N
Transaktion 1
Transaktion 2
Transaktion N
714
Block N+1
Transaktion 1
Transaktion 2
Transaktion N
716
Block N+2
Transaktion 1
Transaktion 2
Transaktion N
720
Anlage B
722
Block N
Transaktion 1
Transaktion 2
Transaktion N
724
Block N+1
Transaktion 1
Transaktion 2
Transaktion N
726
Block N+2
Transaktion 1
Transaktion 2
Transaktion N
Gemeinsam genutzte Ressource

FIG. 7A

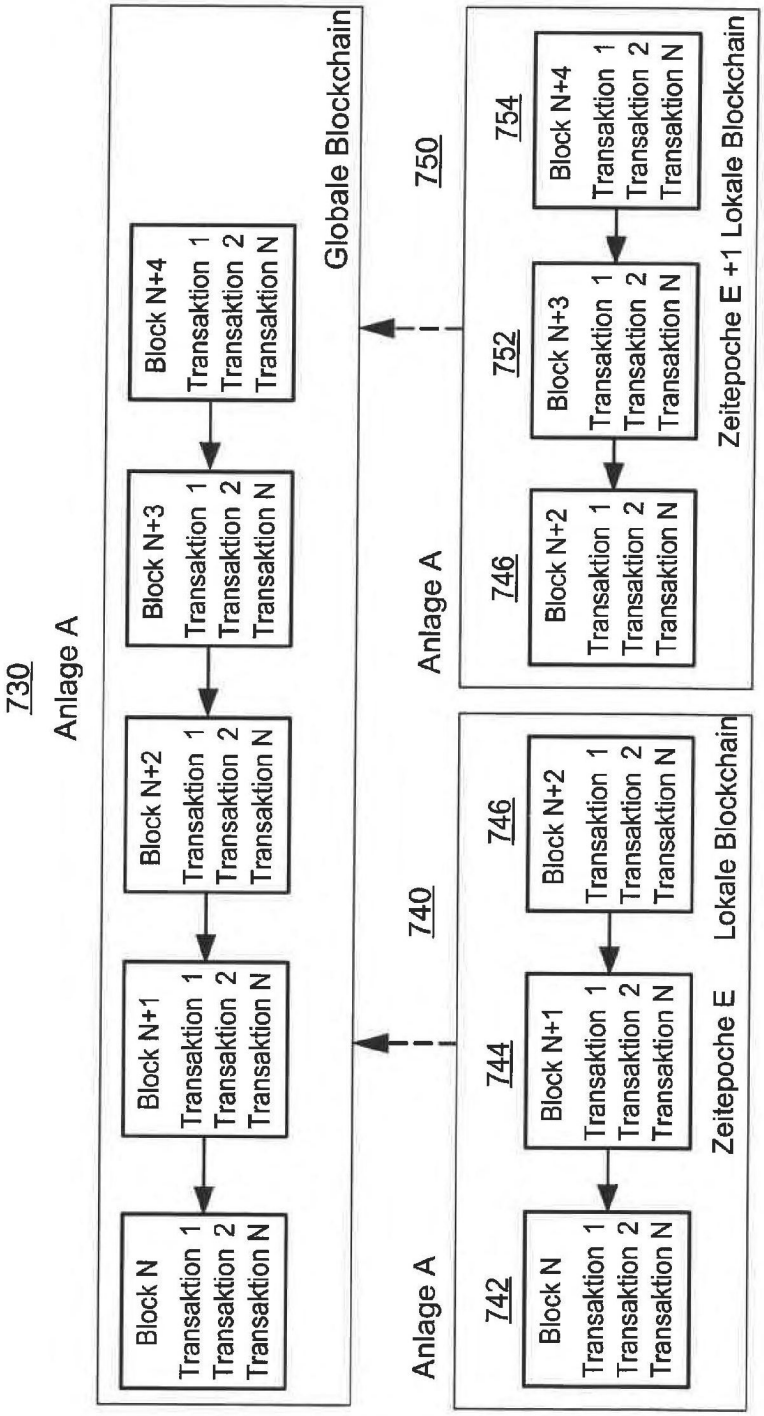

730
Anlage A
Globale Blockchain
Block N
Transaktion 1
Transaktion 2
Transaktion N
Block N+1
Transaktion 1
Transaktion 2
Transaktion N
Block N+2
Transaktion 1
Transaktion 2
Transaktion N
Block N+3
Transaktion 1
Transaktion 2
Transaktion N
Block N+4
Transaktion 1
Transaktion 2
Transaktion N
740
Anlage A
Lokale Blockchain
Zeitepoche E
742
744
746
750
Anlage A
Zeitepoche E +1 Lokale Blockchain
746
752
754

FIG. 7B

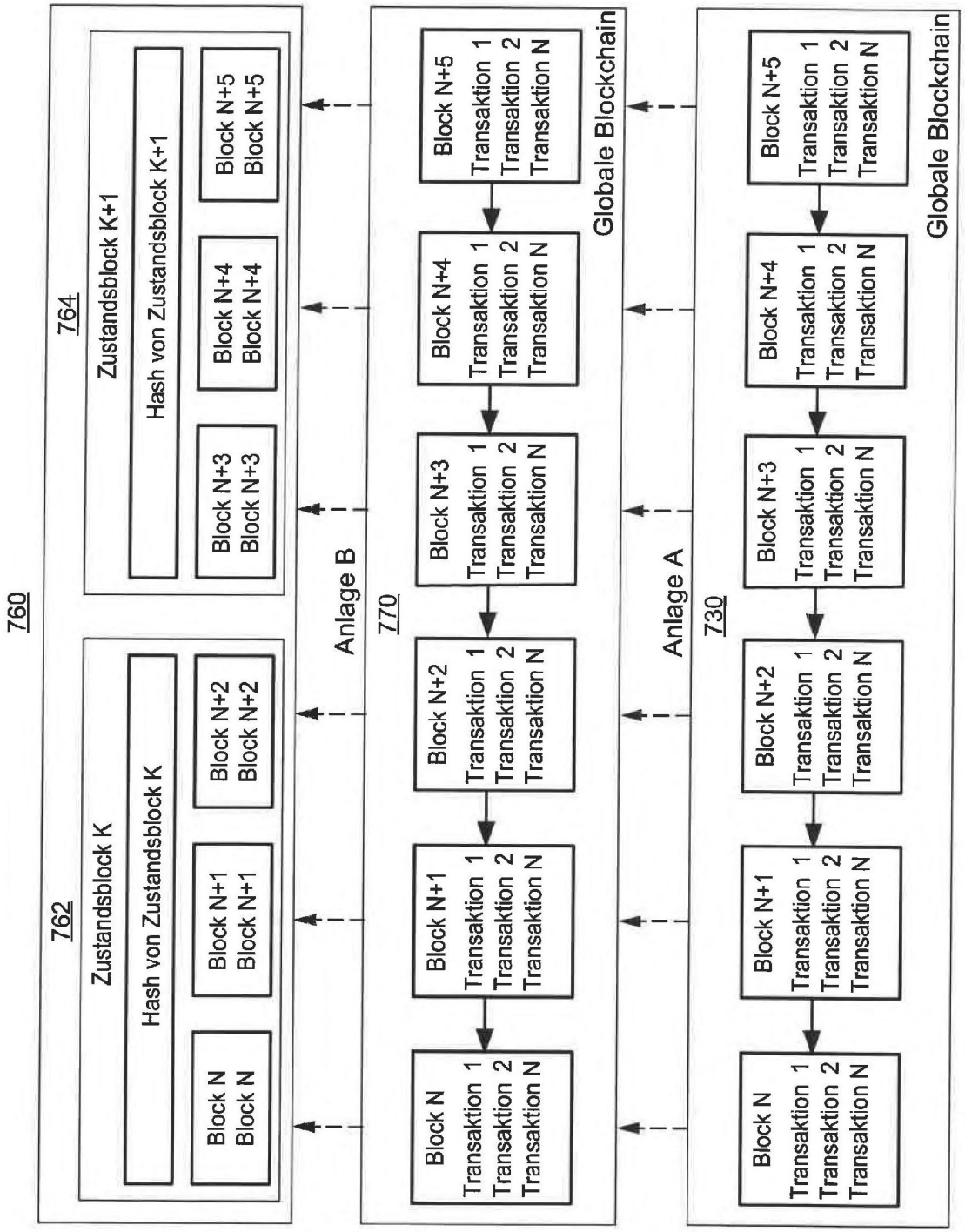

760
762
Zustandsblock K
Hash von Zustandsblock K
Block N
Block N
Block N+1
Block N+1
Block N+2
Block N+2
764
Zustandsblock K+1
Hash von Zustandsblock K+1
Block N+3
Block N+3
Block N+4
Block N+4
Block N+5
Block N+5
Anlage B
770
Globale Blockchain
Block N
Transaktion 1
Transaktion 2
Transaktion N
Block N+1
Transaktion 1
Transaktion 2
Transaktion N
Block N+2
Transaktion 1
Transaktion 2
Transaktion N
Block N+3
Transaktion 1
Transaktion 2
Transaktion N
Block N+4
Transaktion 1
Transaktion 2
Transaktion N
Block N+5
Transaktion 1
Transaktion 2
Transaktion N
Anlage A
730
Globale Blockchain
Block N
Transaktion 1
Transaktion 2
Transaktion N
Block N+1
Transaktion 1
Transaktion 2
Transaktion N
Block N+2
Transaktion 1
Transaktion 2
Transaktion N
Block N+3
Transaktion 1
Transaktion 2
Transaktion N
Block N+4
Transaktion 1
Transaktion 2
Transaktion N
Block N+5
Transaktion 1
Transaktion 2
Transaktion N

FIG. 7C

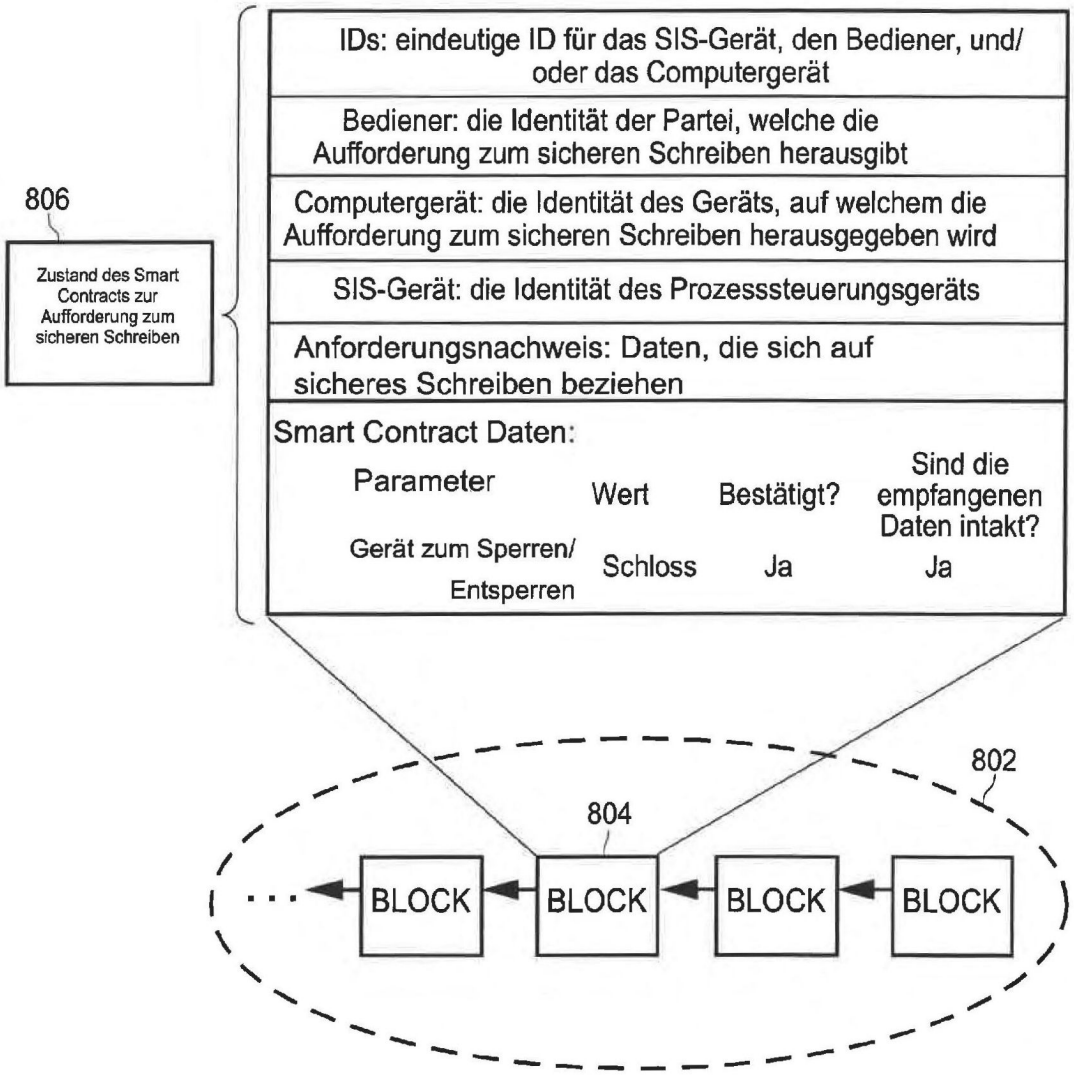

806
Zustand des Smart Contracts zur Aufforderung zum sicheren Schreiben
IDs: eindeutige ID für das SIS-Gerät, den Bediener, und/ oder das Computergerät
Bediener: die Identität der Partei, welche die Aufforderung zum sicheren Schreiben herausgibt
Computergerät: die Identität des Geräts, auf welchem die Aufforderung zum sicheren Schreiben herausgegeben wird
SIS-Gerät: die Identität des Prozesssteuerungsgeräts
Anforderungsnachweis: Daten, die sich auf sicheres Schreiben beziehen
Smart Contract Daten:
Parameter
Wert
Bestätigt?
Sind die empfangenen Daten intakt?
Gerät zum Sperren/ Entsperren
Schloss
Ja
Ja
802
804
BLOCK
BLOCK
BLOCK
BLOCK

FIG. 8

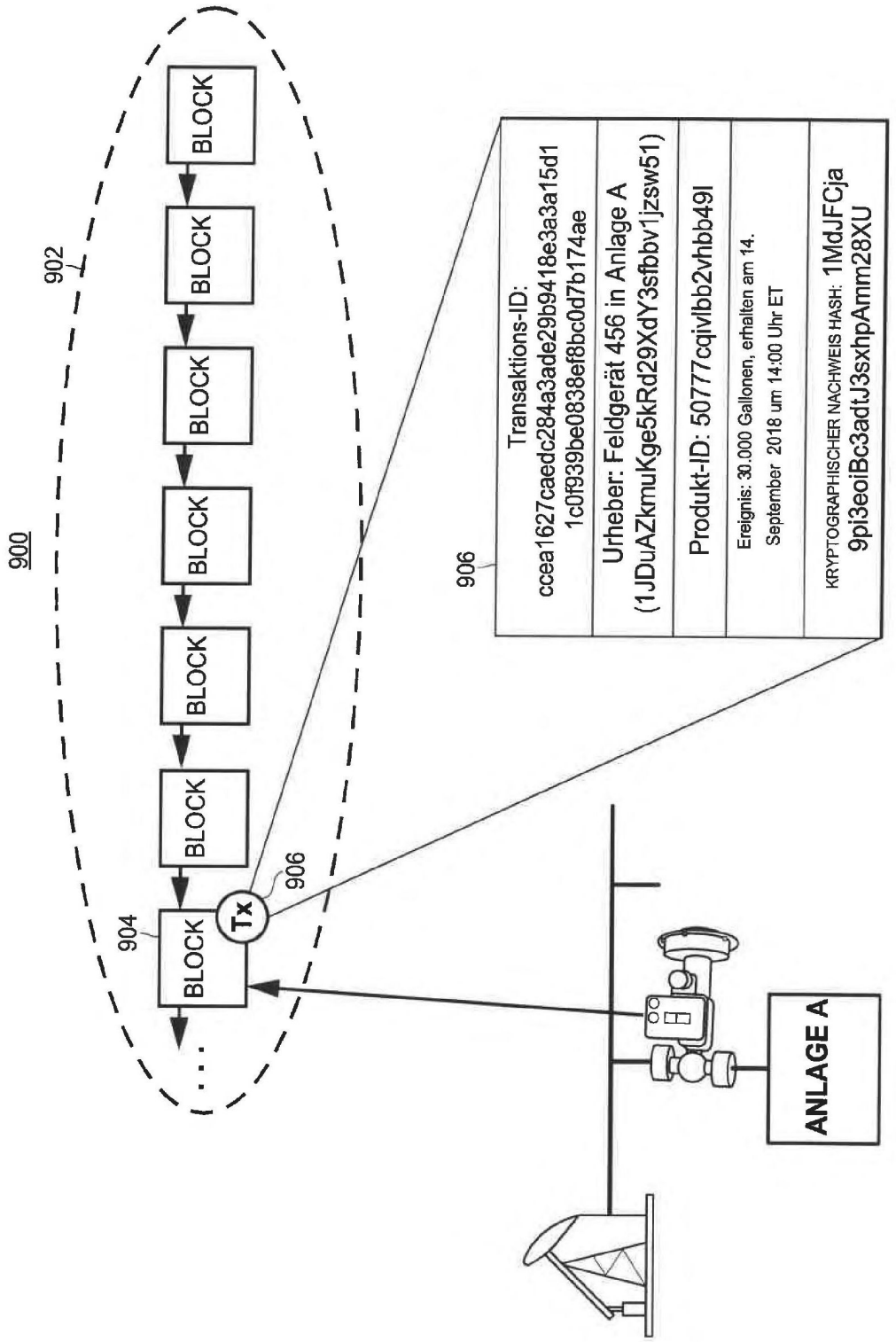

900
902
BLOCK
BLOCK
BLOCK
BLOCK
BLOCK
BLOCK
BLOCK
904
Tx
906
906
Transaktions-ID:
ccea1627caedc284a3ade29b9418e3a3a15d1
1c0f939be0838ef8bc0d7b174ae
Urheber: Feldgerät 456 in Anlage A
(1JDuAZkmuKge5kRd29XdY3sfbbv1jzsw51)
Produkt-ID: 50777cqivlbb2vhbb49l
Ereignis: 30.000 Gallonen, erhalten am 14.
September 2018 um 14:00 Uhr ET
KRYPTOGRAPHISCHER NACHWEIS HASH: 1MdJFCja
9pi3eoiBc3adtJ3sxhpAmm28XU
ANLAGE A

FIG. 9

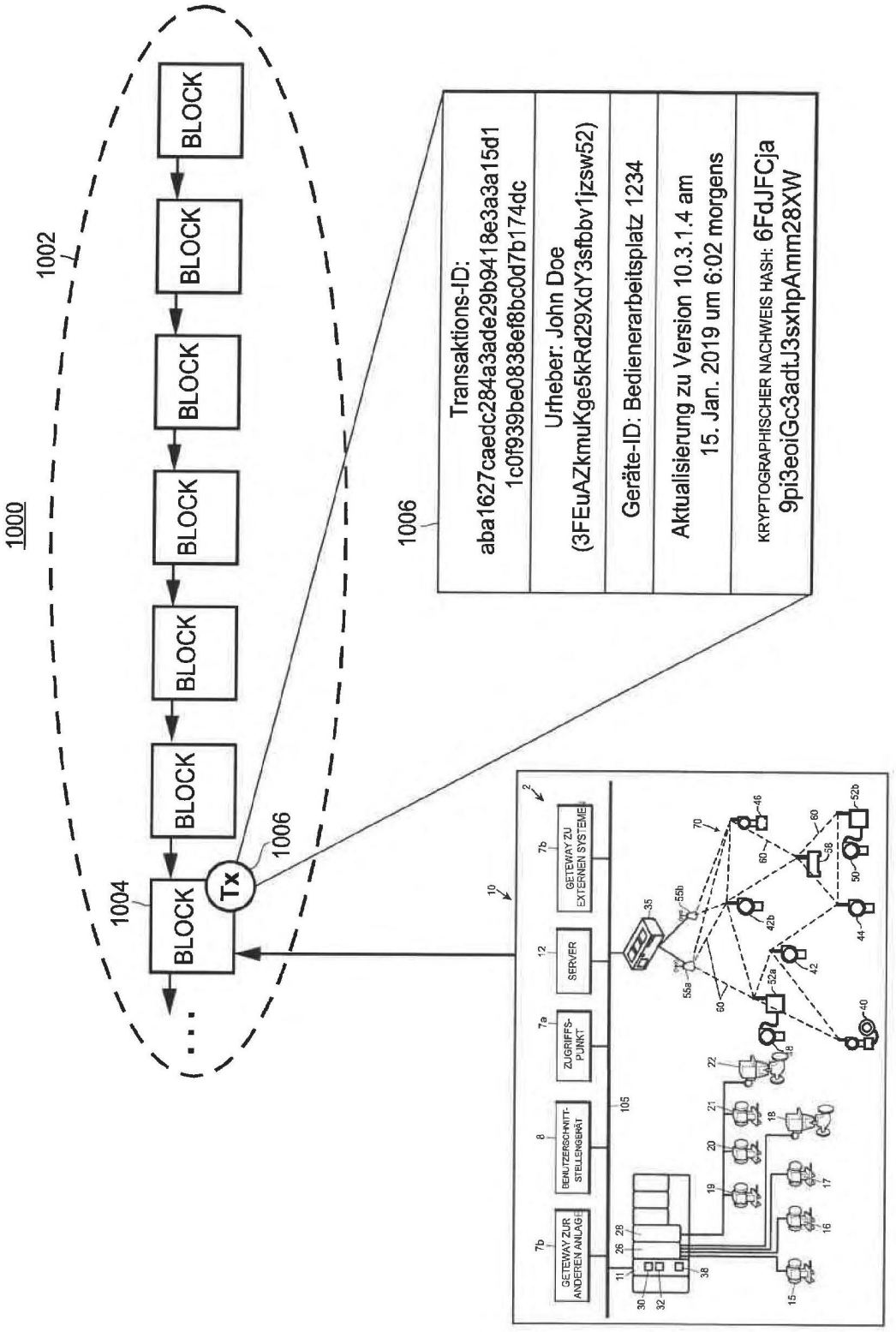

1000
1002
BLOCK
BLOCK
BLOCK
BLOCK
BLOCK
BLOCK
BLOCK
1004
Tx
1006
1006
Transaktions-ID:
aba1627caedc284a3ade29b9418e3a3a15d1
1c0f939be0838ef8bc0d7b174dc
Urheber: John Doe
(3FEuAZkmuKge5kRd29XdY3sfbbv1jzsw52)
Geräte-ID: Bedienerarbeitsplatz 1234
Aktualisierung zu Version 10.3.1.4 am
15. Jan. 2019 um 6:02 morgens
KRYPTOGRAPHISCHER NACHWEIS HASH: 6FdJFCja
9pi3eoiGc3adtJ3sxhpAmm28XW
10
105
GETEWAY ZUR ANDEREN ANLAGE
BENUTZERSCHNITT-STELLENGERÄT
ZUGRIFFS-PUNKT
SERVER
GETEWAY ZU EXTERNEN SYSTEME

FIG. 10

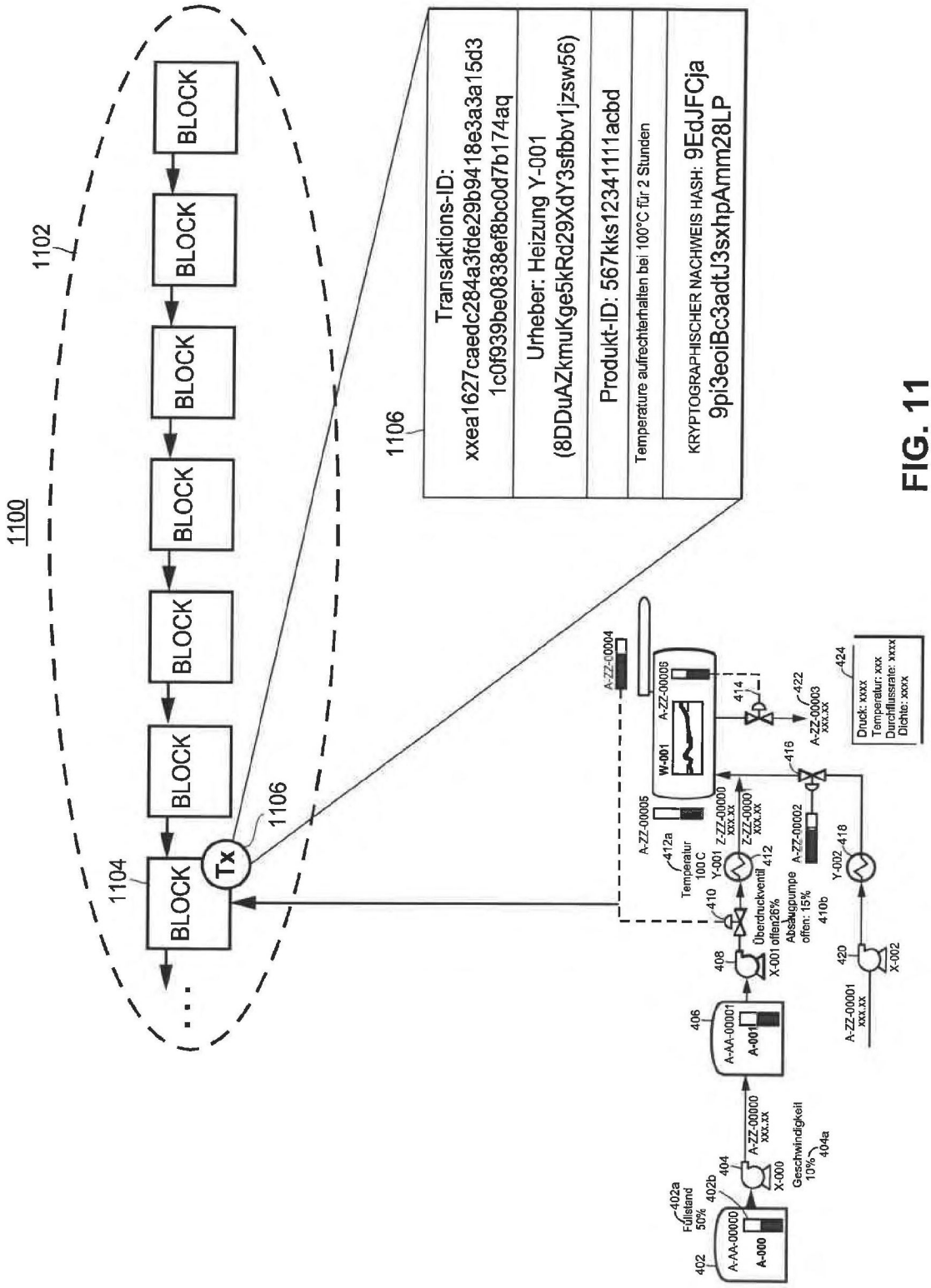

1100
1102
BLOCK
BLOCK
BLOCK
BLOCK
BLOCK
BLOCK
BLOCK
1104
Tx
1106
1106
Transaktions-ID:
xxea1627caedc284a3fde29b9418e3a3a15d3
1c0f939be0838ef8bc0d7b174aq
Urheber: Heizung Y-001
(8DDuAZkmuKge5kRd29XdY3sfbbv1jzsw56)
Produkt-ID: 567kks12341111acbd
Temperature aufrechterhalten bei 100°C für 2 Stunden
KRYPTOGRAPHISCHER NACHWEIS HASH: 9EdJFCja
9pi3eoiBc3adtJ3sxhpAmm28LP
A-ZZ-00004
A-ZZ-00006
W-001
A-ZZ-00005
412a
Temperatur 100 C
Y-001
Z-ZZ-00000 xxx.xx
Z-ZZ-0000 xxx.xx
412
414
422
A-ZZ-00003 xxx.xx
416
A-ZZ-00002
424
Druck: xxxx
Temperatur: xxx
Durchflussrate: xxxx
Dichte: xxxx
410
Überdruckventil offen:26%
408
X-001
Absaugpumpe offen: 15%
410b
Y-002
418
420
X-002
A-ZZ-00001 xxx.xx
406
A-AA-00001
A-001
A-ZZ-00000 xxx.xx
404
X-000
Geschwindigkeit 10%
404a
402a
Füllstand 50%
402b
A-AA-00000
A-000
402

FIG. 11

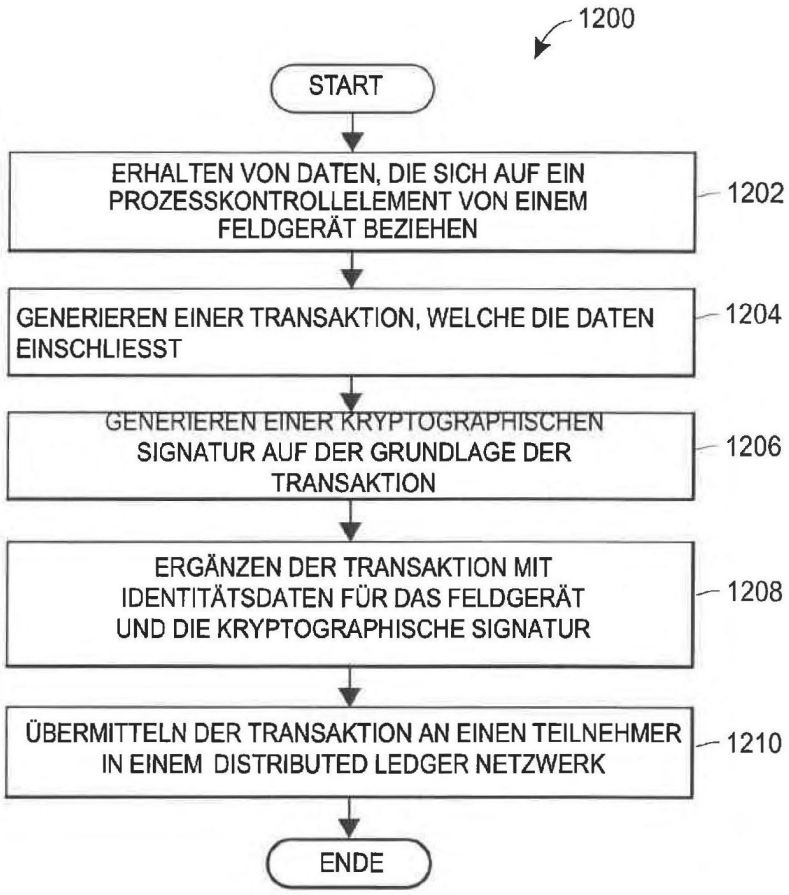

1200
START
ERHALTEN VON DATEN, DIE SICH AUF EIN PROZESSKONTROLLELEMENT VON EINEM FELDGERÄT BEZIEHEN
1202
GENERIEREN EINER TRANSAKTION, WELCHE DIE DATEN EINSCHLIESST
1204
GENERIEREN EINER KRYPTOGRAPHISCHEN SIGNATUR AUF DER GRUNDLAGE DER TRANSAKTION
1206
ERGÄNZEN DER TRANSAKTION MIT IDENTITÄTSDATEN FÜR DAS FELDGERÄT UND DIE KRYPTOGRAPHISCHE SIGNATUR
1208
ÜBERMITTELN DER TRANSAKTION AN EINEN TEILNEHMER IN EINEM DISTRIBUTED LEDGER NETZWERK
1210
ENDE

FIG. 12

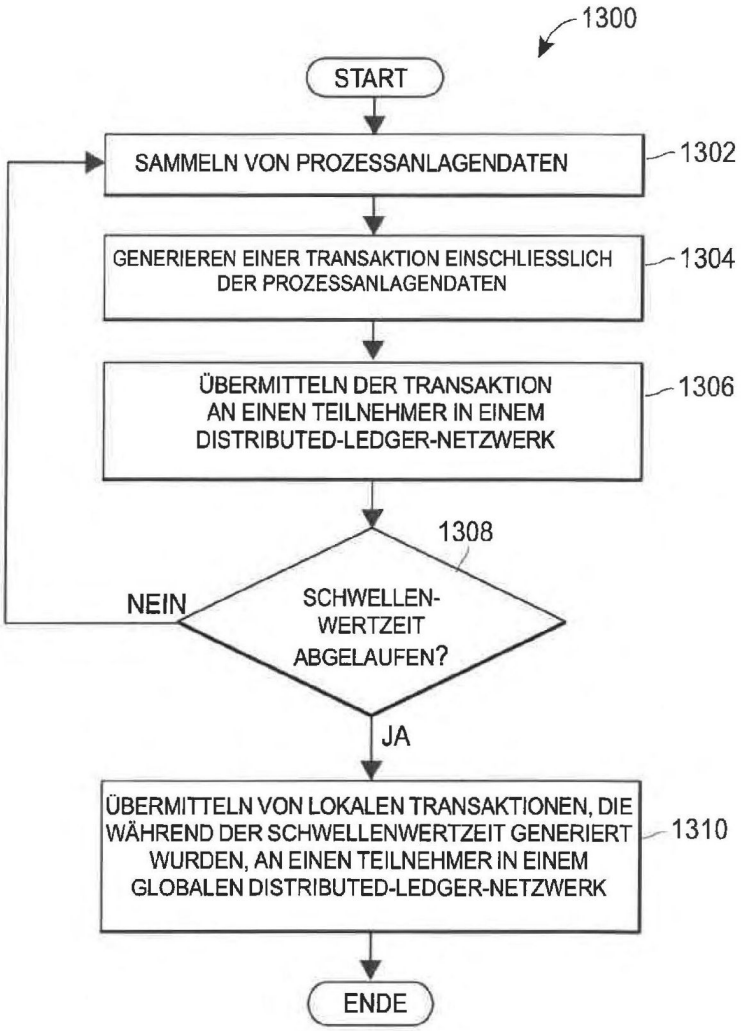

1300
START
SAMMELN VON PROZESSANLAGENDATEN
1302
GENERIEREN EINER TRANSAKTION EINSCHLIESSLICH DER PROZESSANLAGENDATEN
1304
ÜBERMITTELN DER TRANSAKTION AN EINEN TEILNEHMER IN EINEM DISTRIBUTED-LEDGER-NETZWERK
1306
1308
SCHWELLEN-WERTZEIT ABGELAUFEN?
NEIN
JA
ÜBERMITTELN VON LOKALEN TRANSAKTIONEN, DIE WÄHREND DER SCHWELLENWERTZEIT GENERIERT WURDEN, AN EINEN TEILNEHMER IN EINEM GLOBALEN DISTRIBUTED-LEDGER-NETZWERK
1310
ENDE

FIG. 13

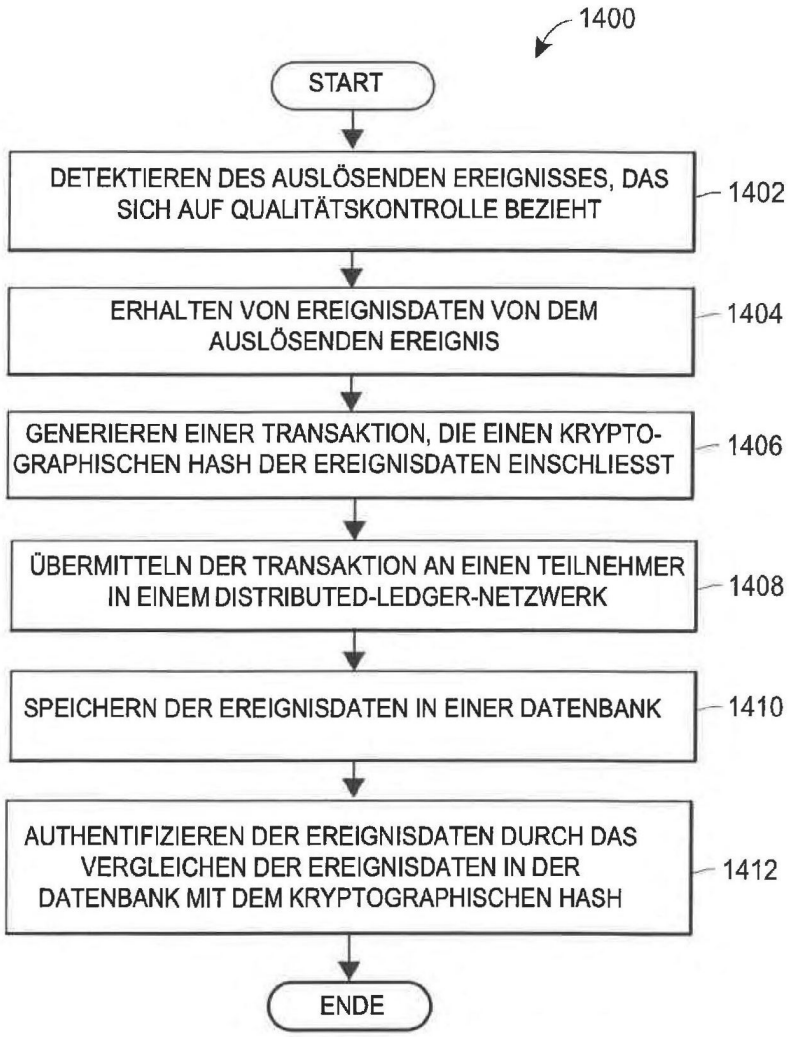

1400
START
DETEKTIEREN DES AUSLÖSENDEN EREIGNISSES, DAS SICH AUF QUALITÄTSKONTROLLE BEZIEHT
1402
ERHALTEN VON EREIGNISDATEN VON DEM AUSLÖSENDEN EREIGNIS
1404
GENERIEREN EINER TRANSAKTION, DIE EINEN KRYPTO-GRAPHISCHEN HASH DER EREIGNISDATEN EINSCHLIESST
1406
ÜBERMITTELN DER TRANSAKTION AN EINEN TEILNEHMER IN EINEM DISTRIBUTED-LEDGER-NETZWERK
1408
SPEICHERN DER EREIGNISDATEN IN EINER DATENBANK
1410
AUTHENTIFIZIEREN DER EREIGNISDATEN DURCH DAS VERGLEICHEN DER EREIGNISDATEN IN DER DATENBANK MIT DEM KRYPTOGRAPHISCHEN HASH
1412
ENDE

FIG. 14

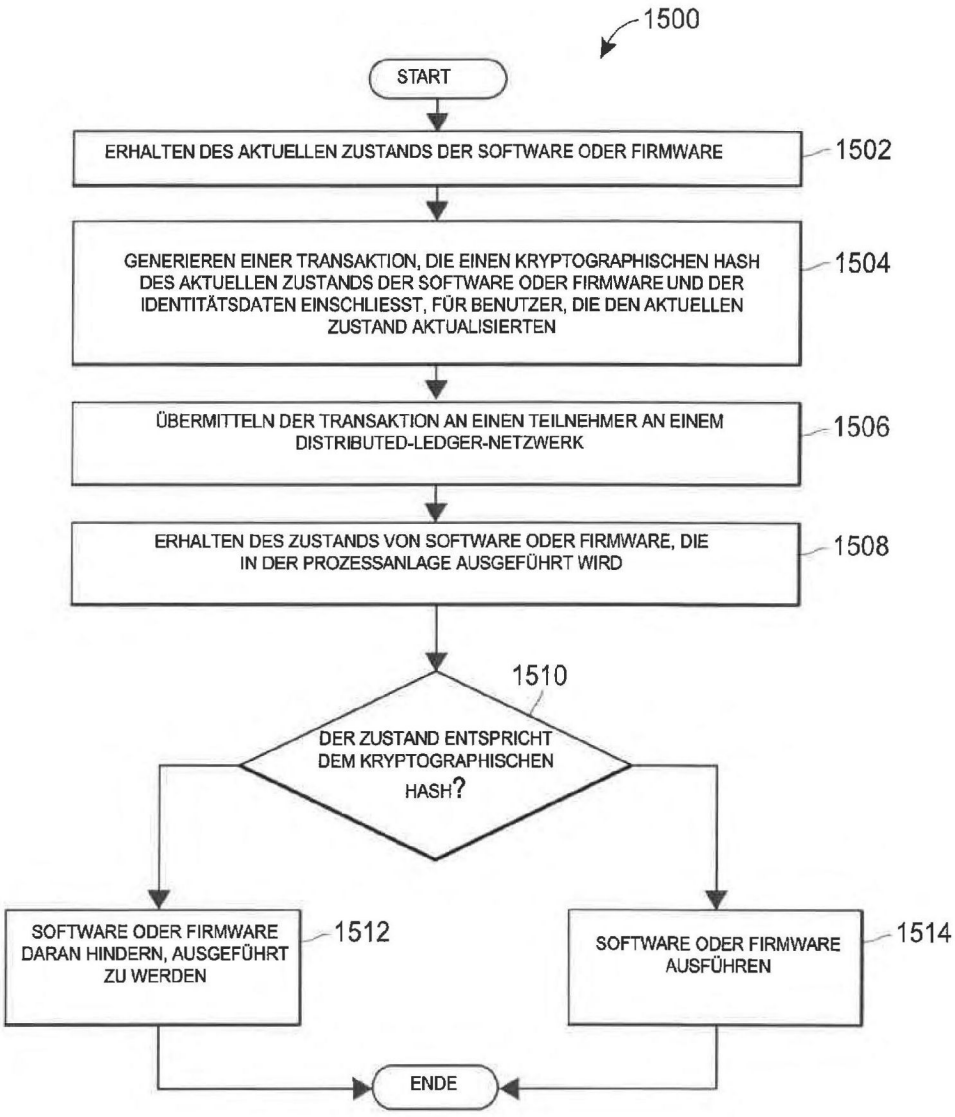

1500
START
ERHALTEN DES AKTUELLEN ZUSTANDS DER SOFTWARE ODER FIRMWARE
1502
GENERIEREN EINER TRANSAKTION, DIE EINEN KRYPTOGRAPHISCHEN HASH DES AKTUELLEN ZUSTANDS DER SOFTWARE ODER FIRMWARE UND DER IDENTITÄTSDATEN EINSCHLIESST, FÜR BENUTZER, DIE DEN AKTUELLEN ZUSTAND AKTUALISIERTEN
1504
ÜBERMITTELN DER TRANSAKTION AN EINEN TEILNEHMER AN EINEM DISTRIBUTED-LEDGER-NETZWERK
1506
ERHALTEN DES ZUSTANDS VON SOFTWARE ODER FIRMWARE, DIE IN DER PROZESSANLAGE AUSGEFÜHRT WIRD
1508
1510
DER ZUSTAND ENTSPRICHT DEM KRYPTOGRAPHISCHEN HASH?
SOFTWARE ODER FIRMWARE DARAN HINDERN, AUSGEFÜHRT ZU WERDEN
1512
SOFTWARE ODER FIRMWARE AUSFÜHREN
1514
ENDE

FIG. 15

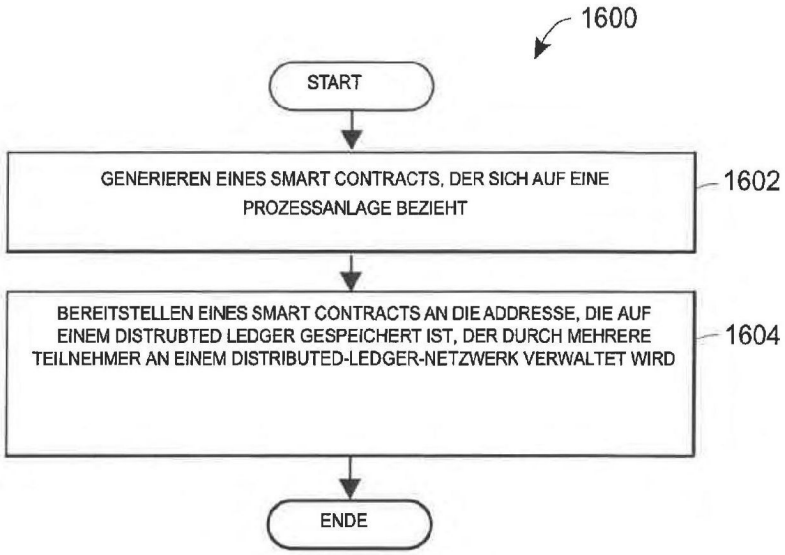


FIG. 16

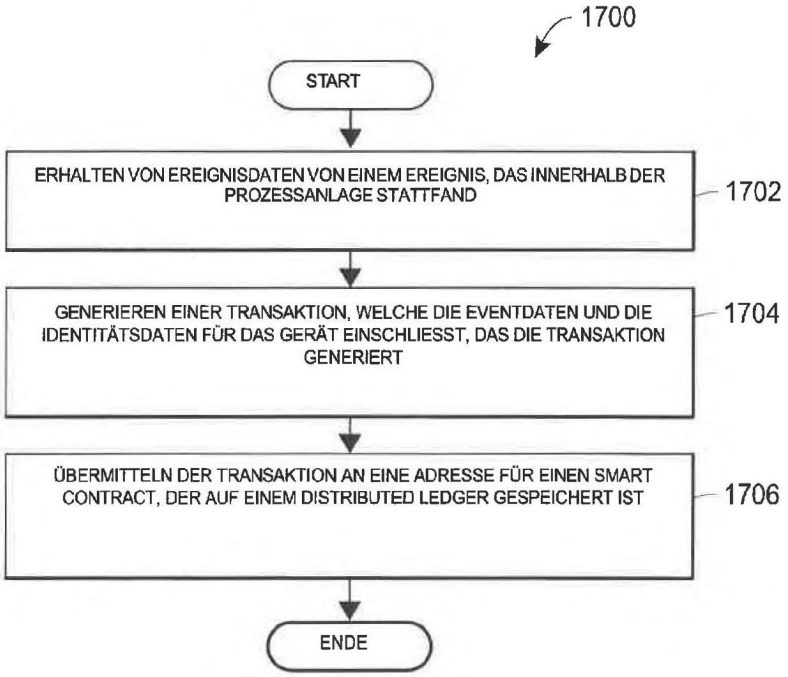


FIG. 17

