

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
05. April 2018 (05.04.2018)



(10) Internationale Veröffentlichungsnummer
WO 2018/059855 A1

(51) Internationale Patentklassifikation:

G06F 21/64 (2013.01) H04L 9/32 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2017/071543

(22) Internationales Anmeldedatum:
28. August 2017 (28.08.2017)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2016 118 614.7
30. September 2016 (30.09.2016) DE

(71) Anmelder: ENDRESS+HAUSER GMBH+CO. KG
[DE/DE]; Hauptstr. 1, 79689 Maulburg (DE).

(72) Erfinder: KILIAN, Markus; Großmattenweg 2 a, 79249
Merzhausen (DE).

(74) Anwalt: ANDRES, Angelika; Colmarer Str. 6, End-
ress+Hauser (Deutschland) AG+Co. KG, 79576 Weil am
Rhein (DE).

(81) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare nationale Schutzrechtsart): AE, AG, AL,
AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,
BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN,
KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD,
ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO,
NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW,
SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(54) Title: METHOD FOR TAMPER-PROOF STORAGE OF DATA OF A FIELD DEVICE

(54) Bezeichnung: VERFAHREN ZUM MANIPULATIONSSICHEREN SPEICHERN VON DATEN EINES FELDDERÄTS

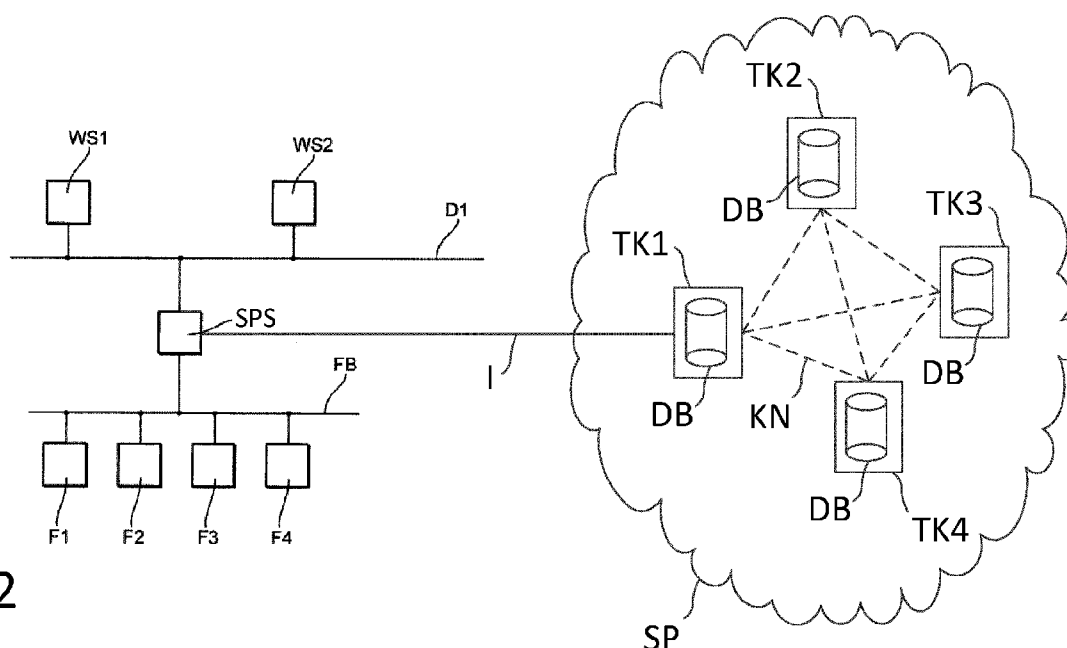


Fig. 2

(57) Abstract: The invention relates to a method for tamper-proof storage of data of a field device (F1, F2, F3, F4) operated by means of automation technology, where the field device (F1, F2, F3, F4) comprises a sensor and/or actuator and an electronic unit, the field device (F1, F2, F3, F4) generating data, including particularly measuring data, control data, history data, parametering data, diagnosis and/or status data, said method comprising: creation of at least one transaction (TA), where the transaction (TA) contains generated data of the field device (F1, F2, F3, F4); storage of the transaction (TA) in a data block (BL1, BL2), the data block (BL1, BL2) being designed in accordance with a data block of Blockchain technology and therefore comprising a data field (DF) containing stored transactions (TA), and a hash value (#1, #2, #3); linking of the data block to previously created data blocks (BL1, BL2), by calculating the hash value (#1, #2, #3) of the data block (BL1, BL2) from the data contained in the transaction (TA) and the hash value (#1, #2, #3) of a previous data block (BL1, BL2); storage of the data block (BL1, BL2) in a service platform (SP), the previously created data blocks (BL1, BL2) being



(84) Bestimmungsstaaten (soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— mit internationalem Recherchenbericht (Artikel 21 Absatz 3)

stored in the service platform (SP); creation and storage of a security data block (SB) in the service platform (SP), where transactions (TA) of the hash value (#1, #2, #3) of the previous data block (BL1, BL2) to be stored are additionally or alternatively contained in the data field (DF) of the security data block (SB), the hash value (#1, #2, #3) of the previous data block (BL1, BL2) being signed with a first private key.

(57) Zusammenfassung: Verfahren zum manipulationssicheren Speichern von Daten eines Feldgeräts (F1, F2, F3, F4) der Automatisierungstechnik, wobei das Feldgerät (F1, F2, F3, F4) einen Sensor und/oder Aktor und eine Elektronikeinheit aufweist, wobei das Feldgerät (F1, F2, F3, F4) Daten generiert, bei denen es sich insbesondere um Messdaten, Steuerdaten, Historiendaten, Parametrierdaten, Diagnose- und/oder Statusdaten handelt, umfassend: - Erstellen zumindest einer Transaktion (TA), wobei die Transaktion (TA) generierte Daten des Feldgeräts (F1, F2, F3, F4) enthält; - Speichern der Transaktion (TA) in einem Datenblock (BL1, BL2), wobei der Datenblock (BL1, BL2) entsprechend einem Datenblock der Blockchain-Technologie ausgestaltet ist und somit ein Datenfeld (DF), enthaltend gespeicherte Transaktionen (TA), und einen Hashwert (#1, #2, #3) aufweist; - Verknüpfen des Datenblocks mit zu früheren Zeitpunkten erstellten Datenblöcken (BL1, BL2), indem der Hashwert (#1, #2, #3) des Datenblocks (BL1, BL2) aus den in der Transaktion (TA) enthaltenen Daten sowie dem Hashwert (#1, #2, #3) eines vorherigen Datenblocks (BL1, BL2) berechnet wird; - Speichern des Datenblocks (BL1, BL2) in einer Service-Plattform (SP), wobei in der Service-Plattform (SP) die zu früheren Zeitpunkten erstellten Datenblöcke (BL1, BL2) gespeichert sind; - Erstellen und Speichern eines Sicherheits-Datenblocks (SB) in der Service-Plattform (SP), wobei im Datenfeld (DF) des Sicherheits-Datenblocks (SB) zusätzlich oder alternativ zu gespeicherten Transaktionen (TA) der Hashwert (#1, #2, #3) des vorherigen Datenblocks (BL1, BL2) enthalten ist, wobei der Hashwert (#1, #2, #3) des vorherigen Datenblocks (BL1, BL2) mit einem ersten privaten Schlüssel signiert ist.

Verfahren zum manipulationssicheren Speichern von Daten eines Feldgeräts

Die Erfindung betrifft ein Verfahren zum manipulationssicheren Speichern von Daten eines Feldgeräts der Automatisierungstechnik.

5

Aus dem Stand der Technik sind bereits Feldgeräte bekannt geworden, die in industriellen Anlagen zum Einsatz kommen. In der Prozessautomatisierungstechnik ebenso wie in der Fertigungsautomatisierungstechnik werden vielfach Feldgeräte eingesetzt. Als Feldgeräte werden im Prinzip alle Geräte bezeichnet, die prozessnah eingesetzt werden und die prozessrelevante Informationen liefern oder verarbeiten. So werden Feldgeräte zur Erfassung und/oder Beeinflussung von Prozessgrößen verwendet. Zur Erfassung von Prozessgrößen dienen Messgeräte, bzw. Sensoren. Diese werden beispielsweise zur Druck- und Temperaturmessung, Leitfähigkeitsmessung, Durchflussmessung, pH-Messung, Füllstandmessung, etc. verwendet und erfassen die entsprechenden Prozessvariablen Druck, Temperatur, Leitfähigkeit, pH-Wert, Füllstand, Durchfluss etc. Zur Beeinflussung von Prozessgrößen werden Aktoren verwendet. Diese sind beispielsweise Pumpen oder Ventile, die den Durchfluss einer Flüssigkeit in einem Rohr oder den Füllstand in einem Behälter beeinflussen können. Neben den zuvor genannten Messgeräten und Aktoren werden unter Feldgeräten auch Remote I/Os, Funkadapter bzw. allgemein Geräte verstanden, die auf der Feldebene angeordnet sind.

20

Eine Vielzahl solcher Feldgeräte wird von der Endress+Hauser-Gruppe produziert und vertrieben.

In modernen Industrieanlagen sind Feldgeräte in der Regel über Kommunikationsnetzwerke wie beispielsweise Feldbusse (Profibus®, Foundation® Fieldbus, HART®, etc.) mit übergeordneten Einheiten verbunden. Normalerweise handelt es sich bei den übergeordneten Einheiten um Steuereinheiten, wie beispielsweise eine SPS (speicherprogrammierbare Steuerung) oder einen PLC (Programmable Logic Controller). Die übergeordneten Einheiten dienen unter anderem zur Prozesssteuerung, sowie zur Inbetriebnahme der Feldgeräte. Die von den Feldgeräten, insbesondere von Sensoren, erfassten Messwerte werden über das jeweilige Bussystem an eine (oder gegebenenfalls mehrere) übergeordnete Einheit(en) übermittelt, die die Messwerte gegebenenfalls weiterverarbeiten und an den Leitstand der Anlage weiterleiten. Der Leitstand dient zur Prozessvisualisierung, Prozessüberwachung und Prozesssteuerung über die übergeordneten Einheiten. Daneben ist auch eine Datenübertragung von der übergeordneten Einheit über das Bussystem an die Feldgeräte erforderlich, insbesondere zur Konfiguration und Parametrierung von Feldgeräten sowie zur Ansteuerung von Aktoren.

35

Feldgeräte erstellen und/oder verarbeiten eine Vielzahl unterschiedlicher Daten. Bei diesen Daten

handelt es sich neben bereits oben genannten Messdaten von Sensoren, durch welche ein Anlagenbetreiber Informationen über die aktuellen Prozesswerte der Messstellen seiner Anlage erhält, beispielsweise um Steuerdaten, bspw. zur Stellregelung eines Aktors. Des Weiteren handelt es sich bei den Daten um Diagnose-, Historien-, und/oder Statusdaten, durch die der

5 Anlagenbetreiber über Probleme der Feldgeräte, bzw. dem aktuellen Status der einzelnen Feldgeräte informiert wird, oder um Kalibrier-/Parametrierdaten.

Heutzutage ist es üblich, diese Daten an einer zentralen Stelle in der Anlage zu speichern, beispielsweise in einer Datenbank in einem Workstation-PC in der Leitebene der Anlage. Dies ist

10 jedoch mit Nachteilen verbunden: Fällt die Datenbank aus, bzw. wird die Datenbank zerstört, bzw. unlesbar, so sind die auf dieser Datenbank gespeicherten Daten verloren.

Des Weiteren sind die Daten manipulierbar, da sie häufig unverschlüsselt über das Kommunikationsnetzwerk gesendet werden, bzw. unverschlüsselt auf der Datenbank abgelegt

15 werden. Werden Daten im Nachhinein manipuliert, so kann dies nur sehr schwer nachverfolgt werden, bzw. aufgrund der Vielzahl an gespeicherten Daten mitunter erst sehr spät bemerkt werden.

Ausgehend von dieser Problematik liegt der Erfindung die Aufgabe zugrunde, ein Verfahren vorzustellen, welches es erlaubt, Daten einer Vielzahl von Feldgeräten in einer Anlage der

20 Prozessautomatisierung auf (manipulations)sichere Art und Weise zu speichern.

Die Aufgabe wird durch ein Verfahren zum manipulationssicheren Speichern von Daten eines Feldgeräts der Automatisierungstechnik gelöst, wobei das Feldgerät einen Sensor und/oder Aktor und eine Elektroneinheit aufweist, wobei das Feldgerät Daten generiert, bei denen es sich

25 insbesondere um Messdaten, Steuerdaten, Historiendaten, Parametrierdaten, Diagnose- und/oder Statusdaten handelt, umfassend:

- Erstellen zumindest einer Transaktion, wobei die Transaktion generierte Daten des Feldgeräts enthält;
- Speichern der Transaktion in einem Datenblock, wobei der Datenblock entsprechend

30 einem Datenblock der Blockchain-Technologie ausgestaltet ist und somit ein Datenfeld, enthaltend gespeicherte Transaktionen, und einen Hashwert aufweist;- Verknüpfen des Datenblocks mit zu früheren Zeitpunkten erstellten Datenblöcken, indem der Hashwert des Datenblocks aus den in der Transaktion enthaltenen Daten sowie dem Hashwert eines vorherigen Datenblocks berechnet wird;
- Speichern des Datenblocks in einer Service-Plattform, wobei in der Service-Plattform die

35 zu früheren Zeitpunkten erstellten Datenblöcke gespeichert sind;

- Erstellen und Speichern eines Sicherheits-Datenblocks in der Service-Plattform, wobei im Datenfeld des Sicherheits-Datenblocks zusätzlich zu oder alternativ gespeicherten Transaktionen der Hashwert des vorherigen Datenblocks enthalten ist, wobei der Hashwert des vorherigen Datenblocks mit einem ersten privaten Schlüssel signiert ist.

5

Der große Vorteil des erfindungsgemäßen Verfahrens besteht darin, dass Daten manipulationssicher in Form von Datenblöcken gespeichert werden. Das Datenfeld eines Datenblocks enthält sämtliche Transaktionen, welche nach dem Zeitpunkt des Erstellens des letzten Datenblocks generiert wurden. Diese Transaktionen werden über einen Algorithmus zu einem Zwischenwert verrechnet, beispielsweise wird die „Merkle Root“ aller im Datenfeld des Datenblocks enthaltenen Transaktionen errechnet. Der Hashwert des Datenblocks wird aus diesem Zwischenwert und dem Hashwert des vorangehenden Datenblocks erzeugt. Eine Aneinanderreihung mehrerer Datenblöcke wird als Blockchain bezeichnet. Dadurch, dass die in einem Datenblock gespeicherten Daten zu einem Hashwert berechnet werden, können diese Daten nicht verändert/manipuliert werden, ohne den Hashwert des Datenblocks und somit die jeweiligen Hashwerte aller nachfolgenden Datenblöcke zu verändern.

10

15

20

25

30

Selbst wenn es einem Angreifer gelingen sollte, Daten eines Datenblocks zu manipulieren, sowie die Hashwerte der nachfolgenden Datenblöcke konform zu dem manipulierten Datenblock zu verändern, kann eine Manipulation auf einfache Art und Weise detektiert werden. Der Sicherheitsdatenblock enthält in seinem Datenfeld nämlich den Hashwert des vorherigen Datenblocks, welcher mittels eines ersten privaten Schlüssels signiert ist. Der erste private Schlüssel ist lediglich dem Besitzer des Feldgeräts und/oder dem Betreiber der Serviceplattform bekannt. Ein Angreifer kann diesen gespeicherten Hashwert daher ohne Kenntnis des ersten privaten Schlüssels nicht manipulieren. In dem Falle, dass, wie oben beschrieben, Hashwerte der Datenblöcke bearbeitet werden, um die Konformität der Blockchain zu erhalten, wird der im Datenfeld des Sicherheits-Datenblocks gespeicherte, signierte Hashwert des dem Sicherheits-Datenblock vorangehenden Datenblocks nicht verändert. Durch Abgleich des Hashwerts des vorangehenden Datenblocks mit dem signierten Hashwert kann eine Manipulation detektiert werden, da sich der Hashwert des vorangehenden Datenblocks im Falle einer Manipulation von dem im Datenfeld des Sicherheits-Datenblocks gespeicherten Hashwert unterscheidet.

35

Das Feldgerät ist vorzugsweise direkt oder indirekt – beispielsweise mittels eines Feldbusses der Automatisierungstechnik, der mit einem Internetfähigen Gerät, vorzugsweise einem Gateway oder einem Edge Device in Kommunikationsverbindung steht - mit dem Internet verbunden. Über das Internet kontaktiert das Feldgerät die Service-Plattform und sendet dieser seine generierten Daten. Die Service-Plattform selbst erstellt die Transaktionen, sowie die die Transaktionen enthaltenden

Datenblöcke, und speichert diese.

Feldgeräte, welche im Zusammenhang mit dem erfindungsgemäßen Verfahren genannt werden, sind bereits im einleitenden Teil der Beschreibung beispielhaft beschrieben.

5

Eine bevorzugte Ausgestaltung des erfindungsgemäßen Verfahrens sieht vor, dass die Service-Plattform zumindest eine Datenbank umfasst, in der die Datenblöcke, bzw. die Sicherheits-Datenblöcke, zentral über eine Client-Server-Architektur gespeichert werden. Wie bereits oben genannt dient das Feldgerät lediglich als Ersteller der Daten und sendet diese Daten an die Service-Plattform, in der die Transaktionen und die Datenblöcke, bzw. die Sicherheits-Datenblöcke, erstellt werden. Das Feldgerät muss daher zur Ausführung des erfindungsgemäßen Verfahrens nicht aufgerüstet werden, wodurch keine zusätzlicher Zeit- und Kostenaufwand entsteht.

10

Gemäß einer vorteilhaften Weiterbildung des erfindungsgemäßen Systems ist vorgesehen, dass die Service-Plattform dezentral mit Hilfe einer Blockchain Technologie betrieben wird und aus einer Vielzahl von Teilnehmerknoten besteht, wobei die Teilnehmerknoten Datenblöcke, bzw. Sicherheits-Datenblöcke, erstellen, wobei in jedem Teilnehmerknoten jeweils zumindest eine Datenbank integriert wird, und wobei die Datenblöcke, bzw. die Sicherheits-Datenblöcke, dezentral in den Datenbanken gespeichert werden. Ein Teilnehmerknoten wird von einer Recheneinheit gebildet. Die verschiedenen Teilnehmerknoten sind miteinander über ein Netzwerk, beispielsweise über das Internet, miteinander verbunden. Das Feldgerät kontaktiert einen der Teilnehmerknoten der Service-Plattform und übermittelt diesem die zu speichernden Daten. Der Teilnehmerknoten übermittelt diese Daten ggf. zur Validierung an alle übrigen Teilnehmerknoten und erstellt daraufhin einen neuen Datenblock, bzw. einen Sicherheits-Datenblock, der die Transaktion und ggf. weitere Transaktionen enthält.

15

20

25

Es ist dabei vorgesehen, dass auf allen Datenbanken zu allen Zeitpunkten dieselben Datenblöcke, bzw. Sicherheits-Datenblöcke, daraus folgend also die identischen Daten gespeichert und verfügbar sind. Fallen eine oder mehrere Datenbanken aus, bzw. werden durch einen Angreifer manipuliert, so können die Informationen aus den restlichen Datenbanken ausgelesen werden, wodurch ein vollständiger Datenverlust so gut wie unmöglich ist. Ein Beispiel für eine solche Service-Plattform ist beispielsweise Ethereum.

30

Gemäß einer vorteilhaften Ausgestaltung des erfindungsgemäßen Verfahrens ist vorgesehen, dass ein erstellter Datenblock, bzw. Sicherheits-Datenblock, von allen Teilnehmerknoten verifiziert wird und nur dann in der Service-Plattform gespeichert wird, wenn zumindest eine vorgegebene Anzahl aller Teilnehmerknoten den Hashwert des Datenblocks erfolgreich verifiziert. Die Validierung des

35

Datenblocks, bzw. des Sicherheits-Datenblocks, erfolgt derart, dass dessen Hashwert überprüft wird. Nur wenn der gültige Hashwert des vorherigen Datenblocks verwendet wird, kann der Datenblock, bzw. der Sicherheits-Datenblock erfolgreich validiert werden. Dies führt dazu, dass Daten in einem erfolgreich validierten Datenblock nicht geändert werden können, ohne die nachfolgenden Datenblöcke dementsprechend zu verändern. Eine Änderung von Daten erzeugt einen geänderten Zwischenwert, wodurch auch der Hashwert des jeweiligen Datenblocks verändert wird. Der darauffolgende Datenblock passt somit nicht mehr zu seinem vorherigen Datenblock. Daten eines einmal erfolgreich validierten Datenblocks sind dadurch für einen Angreifer nicht mehr veränderbar.

10

In einer besonders vorteilhaften Ausgestaltung des erfindungsgemäßen Verfahrens ist vorgesehen, dass die erstellte Transaktion vor dem Speichern in den Datenblock, bzw. in den Sicherheits-Datenblock, an alle Teilnehmerknoten übermittelt wird und von den Teilnehmerknoten validiert wird und wobei die erstellte Transaktion nur dann in dem Datenblock, bzw. in dem Sicherheits-Datenblock, gespeichert wird, wenn diese von zumindest einem der Teilnehmerknoten erfolgreich validiert wird. Hierdurch wird eine zusätzliche Sicherheitsstufe erzielt. Es wird insbesondere geprüft, ob der Ersteller der Transaktion ein gültiger Teilnehmerknoten ist, bzw. dass die in der Transaktion enthaltenen Daten beispielsweise in einem gültigen Wertebereich liegen.

15

20

In einer bevorzugten Weiterbildung des erfindungsgemäßen Verfahrens ist vorgesehen, dass das Feldgerät selbst einen Teilnehmerknoten der Service-Plattform bildet und Transaktionen und/oder Datenblöcke, bzw. Sicherheits-Datenblöcke, erstellt. Hierfür muss das Feldgerät jedoch gegebenenfalls über eine ausreichende Leistung und Energie, ggf. zugeführt mittels einer zusätzlichen Energieversorgung, verfügen, da zur Erstellung eines Datenblocks komplexe Algorithmen ausgeführt werden. Im Gegensatz zur Erstellung eines Datenblocks benötigt die Erstellung einer Transaktion erheblich weniger Leistung, so dass das Feldgerät keine zusätzliche Stromversorgung besitzen muss und auch über das Kommunikationsnetzwerk mit Energie versorgt werden kann.

25

30

Es kann dabei vorgesehen sein dass die zur Erstellung der Transaktionen und/oder der Datenblöcke, bzw. der Sicherheits-Datenblöcke, benötigten Algorithmen in der Elektronikeinheit des Feldgeräts integriert sind oder dass das Feldgerät eine modulare Zusatzelektronikeinheit, insbesondere ein Steckmodul, aufweist, in welchem diese Algorithmen implementiert sind. Die hierfür benötigten Algorithmen/Softwarebefehle können hierfür beispielsweise in Form eines Firmwareupdates auf einen beschreibbaren Speicher in der Elektronikeinheit, bzw. der Zusatzelektronikeinheit geladen werden.

35

Eine besonders vorteilhafte Ausgestaltung des erfindungsgemäßen Verfahrens sieht vor, dass das Feldgerät vor Erstellen der Transaktion den Hashwert des vorherigen Datenblocks erhält und die generierten Daten und/oder den Hashwert des vorherigen Datenblocks mit dem ersten privaten Schlüssel, oder mit einem vom ersten privaten Schlüssel abweichenden zweiten Schlüssel signiert und/oder verschlüsselt. Dies ist ein zusätzlicher Sicherheitsmechanismus, da nun auch die einzelnen Daten der Transaktionen und daraus folgend auch der Datenfelder der Datenblöcke signiert, bzw. verschlüsselt werden. Ohne Kenntnis des ersten, bzw. des zweiten Schlüssels kann ein Angreifer die Daten eines Datenblocks nicht verändern. Bei dem zweiten Schlüssel kann es sich um einen privaten Schlüssel oder um einen öffentlichen Schlüssel handeln, welcher auch asymmetrisch sein kann.

Gemäß einer bevorzugten Weiterbildung des erfindungsgemäßen Verfahrens ist vorgesehen, dass der Sicherheits-Datenblock nach definierten Zeitabständen erstellt wird. Vorteilhaft ist es, die Zeitabstände abhängig von der Menge und der Rate an neu erstellten Datenblöcken zu wählen. Insbesondere, wenn neue Datenblöcke vergleichsweise häufig erstellt werden ist es vorteilhaft, kurze Zeitabstände zu wählen.

Gemäß einer besonders bevorzugten Ausgestaltung des erfindungsgemäßen Verfahrens ist vorgesehen, dass der signierte Hashwert mittels eines zu dem ersten privaten Schlüssel korrespondierenden öffentlichen Schlüssels verifiziert wird. Mittels des öffentlichen Schlüssels kann die Signatur des Hashwerts im Prinzip von jedem verifiziert werden. Eine Manipulation dieses Hashwertes ist jedoch ohne Kenntnis des ersten privaten Schlüssels nicht möglich.

Die Erfindung wird anhand der nachfolgenden Figuren näher erläutert. Es zeigen

Fig. 1: eine Erläuterung von Datenblöcken, welche im erfindungsgemäßen Verfahren zum Einsatz kommen; und

Fig. 2: ein Ausführungsbeispiel des erfindungsgemäßen Verfahrens.

Fig. 1 zeigt eine Erläuterung von Datenblöcken BL1, BL2, SB, welche entsprechend der Blockchain-Technologie ausgestaltet sind und im erfindungsgemäßen Verfahren zum Einsatz kommen. Die Blockchain-Technologie wurde als Basis der Internet-Währung „Bitcoin“ bekannt. Eine Blockchain, also eine Kette verknüpfter Datenblöcke BL1, BL2, SB erlaubt eine hohe Datenintegrität. Im Folgenden sei die Funktionsweise einer Blockchain, ausgestaltet für das erfindungsgemäße Verfahren, kurz erläutert.

Ein besagter Datenblock BL1, BL2, SB besteht in der Regel aus zumindest zwei Komponenten: Zum

einem ist das ein Datenfeld DF. In diesem Datenfeld DF sind Daten in Form von Transaktionen TA gespeichert. Als Transaktion TA wird eine Übermittlung der Daten von einem ersten Teilnehmerknoten TK zu einem zweiten Teilnehmerknoten TK in einem Kommunikationsnetzwerk KN bezeichnet. Eine Transaktion TA enthält einen übermittelten Wert, in diesem Fall also Daten, sowie den Sender und den Empfänger der Transaktion TA. Als Teilnehmerknoten TK werden alle Geräte bezeichnet, welche die Blockchain-Technologie in dem Kommunikationsnetzwerk KN nutzen.

Ein Datenfeld DF eines Datenblocks BL1, BL2, SB enthält zumindest eine Transaktion TA, häufiger mehrere Transaktionen TA.

Zum anderen enthält ein Datenblock BL1, BL2, SB eine Prüfsumme #1, #2, #3. Eine solche Prüfsumme #1, #2, #3 ist ein Hashwert und wird durch mitunter aufwendige Berechnungen erstellt. Hierfür werden alle Transaktionen TA des Datenfelds eines Blocks BL1, BL2, SB zu einem Zwischenwert berechnet. Hierfür wird beispielsweise die Merkle-Root der Gesamtzahl der Transaktionen TA berechnet. Auf das genaue Funktionsprinzip wird an dieser Stelle nicht eingegangen. Es sei hierfür beispielsweise auf https://en.wikipedia.org/wiki/Merkle_tree verwiesen.

Dieser errechnete Zwischenwert wird anschließend mit der Prüfsumme #1, #2, #3 des vorherigen Datenblocks BL1, BL2, SB zur Prüfsumme #1, #2, #3 des aktuellen Datenblocks BL1, BL2, SB verrechnet. Beispielsweise enthält der in Fig. 1 gezeigte Datenblock BL2 eine Prüfsumme #2. Diese Prüfsumme #2 wurde also aus den in dem Datenfeld DF des Datenblocks BL2 gespeicherten Transaktionen TA und der Prüfsumme #1 des vorangehenden Datenblocks BL1 berechnet. Analog dazu enthält der in Fig. 1 gezeigte Datenblock SB, ein Sicherheitsdatenblock (dazu später mehr) eine Prüfsumme #3. Diese Prüfsumme #3 wurde also aus den in dem Datenfeld DF des Datenblocks SB gespeicherten Transaktionen TA und der Prüfsumme #2 des vorangehenden Datenblocks BL2 berechnet.

Die Integrität der Daten, also die Sicherung der Daten gegen nachträgliche Manipulationen, ist somit durch die Speicherung der Prüfsumme #1, #2 des vorangehenden Datenblocks BL1, BL2 im jeweils nachfolgenden Datenblock BL2, SB gesichert. Eine Blockchain besteht also aus einer Reihe von Datenblöcken BL1, BL2, SB, in denen jeweils eine oder mehrere Transaktionen TA zusammengefasst und mit der Prüfsumme #1, #2, #3 versehen sind. Eine Änderung von Daten erzeugt einen geänderten Zwischenwert, wodurch auch die Prüfsumme #1, #2, #3 des jeweiligen Datenblocks BL1, BL2, SB verändert wird. Der darauffolgende Datenblock BL1, BL2, SB passt somit nicht mehr zu dem vorangehenden Datenblock BL1, BL2, SB. Daten eines einmal erfolgreich validierten Datenblocks BL1, BL2, SB sind dadurch für einen Angreifer nicht mehr veränderbar. Neue Datenblöcke BL1, BL2, SB werden in regelmäßigen Zeitabständen erstellt. In das Datenfeld

des neuen Datenblocks BL1, BL2, SB werden alle Transaktionen TA gespeichert, welche nach dem Zeitpunkt der erstellen des letzten Datenblocks BL1, BL2, SB erstellt wurden.

- Die Komplexität der Blockerstellung kann dadurch erhöht werden, dass die erstellte Prüfsumme #1, #2, #3 ein vorgegebenes Format aufweisen muss. Beispielsweise wird festgelegt, dass die Prüfsumme 24 Stellen lang sein muss, wobei die ersten vier Stellen den Zahlenwert 0 aufweisen müssen. Hierfür wird neben dem Zwischenwert der Transaktionen TA und der Prüfsumme des vorherigen Datenblocks eine zu ermittelnde Zahlenfolge, als „Nonce“ bezeichnet, mit einer festgelegten Länge zur Berechnung der Prüfsumme #1, #2, #3 des aktuellen Datenblocks BL1, BL2, SB verwendet. Die Berechnung der neuen Prüfsumme #1, #2, #3 dauert entsprechend länger, da nur wenige Noncen vorhanden sind, welche zur Berechnung einer Prüfsumme #1, #2, #3 mit den vorgegebenen Kriterien führen. Das Auffinden einer solchen geeigneten Nonce verursacht hierbei den beschriebenen zusätzlichen Zeitaufwand.
- 15 Nachdem die Prüfsumme #1, #2, #3 eines neuen Datenblocks BL1, BL2, SB erstellt wurde, wird der Datenblock an alle Teilnehmerknoten TK übermittelt. Die Teilnehmerknoten TK überprüfen nun die Prüfsumme #1, #2, #3 des neuen Datenblocks BL1, BL2, SB. Erst nach erfolgreicher Validierung wird der Datenblock BL1, BL2, SB in allen Teilnehmerknoten TK gespeichert. Insbesondere wird hierzu eine erfolgreiche Validierung von mehr als der Hälfte aller Teilnehmerknoten TK benötigt. Ein
- 20 Angreifer müsste daher zum Einschleusen/Erstellen eines fremden, schädlichen Datenblocks BL1, BL2, SB eine große Anzahl an Teilnehmerknoten TK manipulieren, bzw. kontrollieren, um den eingeschleusten Datenblock BL1, BL2, SB erfolgreich zu validieren. Bei steigender Anzahl an Teilnehmerknoten TK ist dies als so gut wie unmöglich anzusehen.
- 25 Für die Validierung eines Datenblocks BL1, BL2, SB ist ein wesentlich geringerer Aufwand als zur Erstellung des Datenblocks BL1, BL2, SB nötig. Die Prüfsumme #1, #2, #3 wird rückgerechnet, der Zwischenwert der Transaktionen TA, bzw. die Prüfsumme #1, #2, #3 des vorherigen Datenblocks BL1, BL2, SB zurückgewonnen und mit dem tatsächlichen Zwischenwert, bzw. mit der tatsächlichen Prüfsumme #1, #2, #3 des vorherigen Datenblock BL1, BL2, SB verglichen. Stimmen diese Werte
- 30 überein, so ist der Datenblock BL1, BL2, SB erfolgreich validiert.

- Im erfindungsgemäßen Verfahren ist eine weitere Sicherheitsstufe implementiert: Im in Fig. 1 gezeigten Ausführungsbeispiel sind zwei normale Datenblöcke BL1, BL2 und ein sogenannter Sicherheits-Datenblock SB gezeigt. Zusätzlich zu den Transaktionen TA ist im Datenfeld DF dieses
- 35 Sicherheits-Datenblocks SB der Hashwert *#2* des vorangehenden Datenblocks BL2 gespeichert und mit einem privaten Schlüssel signiert. Selbst wenn es einem Angreifer gelingen sollte, Daten eines der dem Sicherheits-Datenblock SB vorangehenden Datenblöcke BL1, BL2 zu manipulieren,

- sowie die Hashwerte #1, #2, #3 der nachfolgenden Datenblöcke BL1, BL2, SB konform zu dem manipulierten Datenblock BL1, BL2 zu verändern, kann eine Manipulation auf einfache Art und Weise detektiert werden. Der erste private Schlüssel ist lediglich dem Ausführenden des Signaturprozesses bekannt. Ein Angreifer kann diesen im Sicherheits-Datenblock SB gespeicherten Hashwert *#2* daher ohne Kenntnis des ersten privaten Schlüssels nicht manipulieren. In dem Falle, dass Hashwerte #1, #2, #3 der Datenblöcke BL1, BL2 SB bearbeitet werden, um die Konformität der Blockchain zu erhalten, wird der im Datenfeld DF des Sicherheits-Datenblocks SB gespeicherte, signierte Hashwert *#2* des dem Sicherheits-Datenblock SB vorangehenden Datenblocks BL2 nicht verändert. Durch Abgleich des Hashwerts #2 des vorangehenden Datenblocks BL2 mit dem signierten Hashwert *#2* kann eine Manipulation detektiert werden, da sich der Hashwert #2 des vorangehenden Datenblocks BL2 im Falle einer Manipulation von dem im Datenfeld DF des Sicherheits-Datenblocks SB gespeicherten Hashwert *#2* unterscheidet, bzw. die Signatur ungültig ist.
- Der Zeitpunkt, an dem ein solcher Sicherheits-Datenblock erstellt wird, kann definiert werden und sollte an die Menge und die Rate neu erstellter Datenblöcke BL1, BL2 angepasst werden.

Fig. 2 zeigt eine Ausgestaltung des erfindungsgemäßen Verfahrens. Hierbei ist eine Anlage der Automatisierungstechnik dargestellt. An einem Datenbus D1, bei dem es sich beispielsweise um einen Feldbus der Leitebene, beispielsweise Ethernet handelt, sind mehrere Rechneinheiten WS1, WS2 in Form von Workstation-PCs in der Leitebene der Anlage angeschlossen. Diese Rechneinheiten dienen als übergeordnete Einheiten (Leitsystem bzw. Steuereinheit), unter anderem zur Prozessvisualisierung, Prozessüberwachung und zum Engineering wie zum Bedienen und Überwachen von Feldgeräten F1, F2, F3, F4. Über eine Steuereinheit SPS, die beispielsweise als speicherprogrammierbare Steuerung ausgestaltet ist und im Grunde genommen auch als übergeordnete Einheit bezeichnet wird, ist die Leitebene der Anlage mit mehreren Feldgeräten F1, F2, F3, F4 verbunden. Bei den Feldgeräten F1, F2, F3, F4 kann es sich sowohl um Sensoren oder um Aktoren handeln. Der Feldbus FB arbeitet entsprechend nach einem der bekannten Feldbusstandards, z.B. Profibus®, Foundation Fieldbus® oder HART®. Anstatt des Feldbusses FB kann es sich auch um ein Local-Area-, oder um ein Wide-Area-Network, zum Beispiel das Internet, handeln.

Die Steuerungseinheit SPS besitzt eine Schnittstelle, über die die Steuerungseinheit SPS an ein weiteres Netzwerk I, in diesem Ausführungsbeispiel das Internet, angeschlossen wird. Über das Internet I ist die Steuerungseinheit SPS mit einer Service-Plattform SP verbunden. Die Service-Plattform SP weist mehrere Teilnehmerknoten TK1, TK2, TK3, TK4 auf. Die Teilnehmerknoten TK1, TK2, TK3, TK4 sind mittels eines Kommunikationsnetzwerks KN miteinander verbunden, sind dazu

ausgestaltet, eine Blockchain mit den in Fig. 1 beschriebenen Eigenschaften und Funktionen auszuführen und weisen jeweils eine Datenbank DB auf.

5 Über die Steuerungseinheit SPS senden die Feldgeräte F1, F2, F3, F4 ihre generierten Daten über das Internet an die Serviceplattform SP. Eine Definition von Feldgeräten F1, F2, F3, F4 und den möglichen generierten Daten ist bereits im einleitenden Teil der Beschreibung beschrieben. Alternativ können die Daten der Feldgeräte F1, F2, F3, F4 auch über ein anderes, am Feldbus FB angeschlossenes, mit dem Internet I verbundenes Gerät, beispielsweise ein Gateway oder ein Edge-Device, an die Service-Plattform SP übermittelt werden. Es kann auch vorgesehen sein, dass 10 die Feldgeräte F1, F2, F3, F4 jeweils eine eigene Schnittstelle aufweisen, über die die Feldgeräte F1, F2, F3, F4 mit dem Internet I verbunden werden können.

Nach Erhalt der Daten der Feldgeräte F1, F2, F3, F4 erstellt ein Teilnehmerknoten TK1, TK2, TK3, TK4 der Service-Plattform eine oder mehrere Transaktionen TA, die die Daten enthalten. Nach 15 Validierung der Transaktionen TA durch alle Teilnehmerknoten TK1, TK2, TK3, TK4 erfolgt, wie in Fig. 1 beschrieben, eine Blockerstellung, bzw. eine Erstellung eines Sicherheits-Datenblocks SP und ggf. eine Durchführung der weiteren, in Fig. 1 beschriebenen Schritte.

Zum Abschluss sind einige Vorteile des erfindungsgemäßen Verfahrens noch einmal aufgeführt:

20 - Dezentrale Speicherung der Daten der Anlage in mehreren Datenbanken DB statt in einer zentralen Datenbank DB, wodurch die Verletzlichkeit der Daten gesenkt wird;

- Integrität der Daten durch Verknüpfung der Datenblöcke BL1, BL2, BL3;

- Durchlaufen mehrerer Validierungsvorgänge, wodurch nur den Anforderungen genügende Transaktionen TA, bzw. gültige Datenblöcke BL1, BL2, BL3 gespeichert werden;

25 - Zusätzlicher Schutz vor Angriffen durch Erstellen eines Sicherheits-Datenblocks SB in vorgegebenen Zeitpunkten, welcher den signierten Hashwert *#2* des vorangehenden Datenblocks BL2 enthält.

Es versteht sich von selbst, dass die gezeigten Ausführungsbeispiele ausschließlich beispielhafter 30 Natur sind und das erfindungsgemäße Verfahren mit jeglicher Art und Anordnung von Feldgeräten in einer Anlage der Prozessautomatisierung ausführbar ist.

Bezugszeichenliste

	BL1, BL2	Datenblock
	D1	Datenbus
5	DB	Datenbank
	DF	Datenfeld
	F1, F2, F3, F4	Feldgerät
	FB	Feldbus
	KN	Kommunikationsnetzwerk
10	SB	Sicherheits-Datenblock
	SPS	Steuereinheit
	SP	Service-Plattform
	TA	Transaktion
	TK1, TK2, TK3, TK4	Teilnehmerknoten
15	WS1, WS2	Workstation-PC
	#1, #2, #3	Hashwerte der Datenblöcke
	#2	signierter Hashwert

Patentansprüche

1. Verfahren zum manipulationssicheren Speichern von Daten eines Feldgeräts (F1, F2, F3, F4) der Automatisierungstechnik, wobei das Feldgerät (F1, F2, F3, F4) einen Sensor und/oder Aktor und eine Elektroneinheit aufweist, wobei das Feldgerät (F1, F2, F3, F4) Daten generiert, bei denen es sich insbesondere um Messdaten, Steuerdaten, Historiendaten, Parametrierdaten, Diagnose- und/oder Statusdaten handelt, umfassend:
- Erstellen zumindest einer Transaktion (TA), wobei die Transaktion (TA) generierte Daten des Feldgeräts (F1, F2, F3, F4) enthält;
 - Speichern der Transaktion (TA) in einem Datenblock (BL1, BL2), wobei der Datenblock (BL1, BL2) entsprechend einem Datenblock der Blockchain-Technologie ausgestaltet ist und somit ein Datenfeld (DF), enthaltend gespeicherte Transaktionen (TA), und einen Hashwert (#1, #2, #3) aufweist;
 - Verknüpfen des Datenblocks mit zu früheren Zeitpunkten erstellten Datenblöcken (BL1, BL2), indem der Hashwert (#1, #2, #3) des Datenblocks (BL1, BL2) aus den in der Transaktion (TA) enthaltenen Daten sowie dem Hashwert (#1, #2, #3) eines vorherigen Datenblocks (BL1, BL2) berechnet wird;
 - Speichern des Datenblocks (BL1, BL2) in einer Service-Plattform (SP), wobei in der Service-Plattform (SP) die zu früheren Zeitpunkten erstellten Datenblöcke (BL1, BL2) gespeichert sind;
 - Erstellen und Speichern eines Sicherheits-Datenblocks (SB) in der Service-Plattform (SP), wobei im Datenfeld (DF) des Sicherheits-Datenblocks (SB) zusätzlich oder alternativ zu gespeicherten Transaktionen (TA) der Hashwert (#1, #2, #3) des vorherigen Datenblocks (BL1, BL2) enthalten ist, wobei der Hashwert (#1, #2, #3) des vorherigen Datenblocks (BL1, BL2) mit einem ersten privaten Schlüssel signiert ist.
2. Verfahren nach Anspruch 1, wobei die Service-Plattform (SP) zumindest eine Datenbank (DB) umfasst, in der die Datenblöcke (BL1, BL2), bzw. die Sicherheits-Datenblöcke (SB), zentral über eine Client-Server-Architektur gespeichert werden.
3. Verfahren nach Anspruch 1, wobei die Service-Plattform (SP) dezentral mit Hilfe einer Blockchain Technologie betrieben wird und aus einer Vielzahl von Teilnehmerknoten (TK1, TK2, TK3, TK4) besteht, wobei die Teilnehmerknoten (TK1, TK2, TK3, TK4) Datenblöcke (BL1, BL2) bzw. Sicherheits-Datenblöcke (SB), erstellen, wobei in jedem Teilnehmerknoten (TK1, TK2, TK3, TK4) jeweils zumindest eine Datenbank (DB) integriert wird, und wobei die Datenblöcke (BL1, BL2) bzw. die Sicherheits-Datenblöcke (SB), dezentral in den Datenbanken (DB) gespeichert werden

4. Verfahren nach Anspruch 3, wobei ein erstellter Datenblock (BL1, BL2), bzw. Sicherheits-Datenblock (SB), von allen Teilnehmerknoten (TK1, TK2, TK3, TK4) verifiziert wird und nur dann in der Service-Plattform (SP) gespeichert wird, wenn zumindest eine vorgegebene Anzahl aller Teilnehmerknoten (TK1, TK2, TK3, TK4) den Hashwert (#1, #2, #3) des Datenblocks (BL1, BL2),
5 bzw. des Sicherheits-Datenblocks (SB), erfolgreich verifiziert.
5. Verfahren nach zumindest einem der Ansprüche 3 oder 4, wobei die erstellte Transaktion (TA) vor dem Speichern in den Datenblock (BL1, BL2), bzw. in dem Sicherheits-Datenblock (SB) an alle Teilnehmerknoten (TK1, TK2, TK3, TK4) übermittelt wird und von den Teilnehmerknoten
10 (TK1, TK2, TK3, TK4) validiert wird und wobei die erstellte Transaktion (TA) nur dann in dem Datenblock (BL1, BL2), bzw. in dem Sicherheits-Datenblock (SB), gespeichert wird, wenn diese von zumindest einem der Teilnehmerknoten (TK1, TK2, TK3, TK4) erfolgreich validiert wird.
6. Verfahren nach zumindest einem der Ansprüche 3 bis 5, wobei das Feldgerät (F1, F2, F3, F4)
15 selbst einen Teilnehmerknoten (TK1, TK2, TK3, TK4) der Service-Plattform (SP) bildet und Transaktionen (TA) und/oder Datenblöcke (BL1, BL2), bzw. Sicherheits-Datenblöcke (SB), erstellt.
7. Verfahren nach zumindest einem der vorherigen Ansprüche, wobei das Feldgerät (F1, F2, F3, F4) vor Erstellen der Transaktion (TA) den Hashwert (#1, #2, #3) des vorherigen Datenblocks (BL1, BL2) erhält und die generierten Daten und/oder den Hashwert (#1, #2, #3) des vorherigen Datenblocks (BL1, BL2) mit dem ersten privaten Schlüssel, oder mit einem vom ersten privaten Schlüssel abweichenden zweiten Schlüssel signiert und/oder verschlüsselt.
20
8. Verfahren nach einem der vorherigen Ansprüche, wobei der Sicherheits-Datenblock (SB) nach definierten Zeitabständen erstellt wird.
25
9. Verfahren nach zumindest einem der vorherigen Ansprüche, wobei der signierte Hashwert (#1, #2, #3) mittels eines zu dem ersten privaten Schlüssel korrespondierenden öffentlichen
30 Schlüssels verifiziert wird.

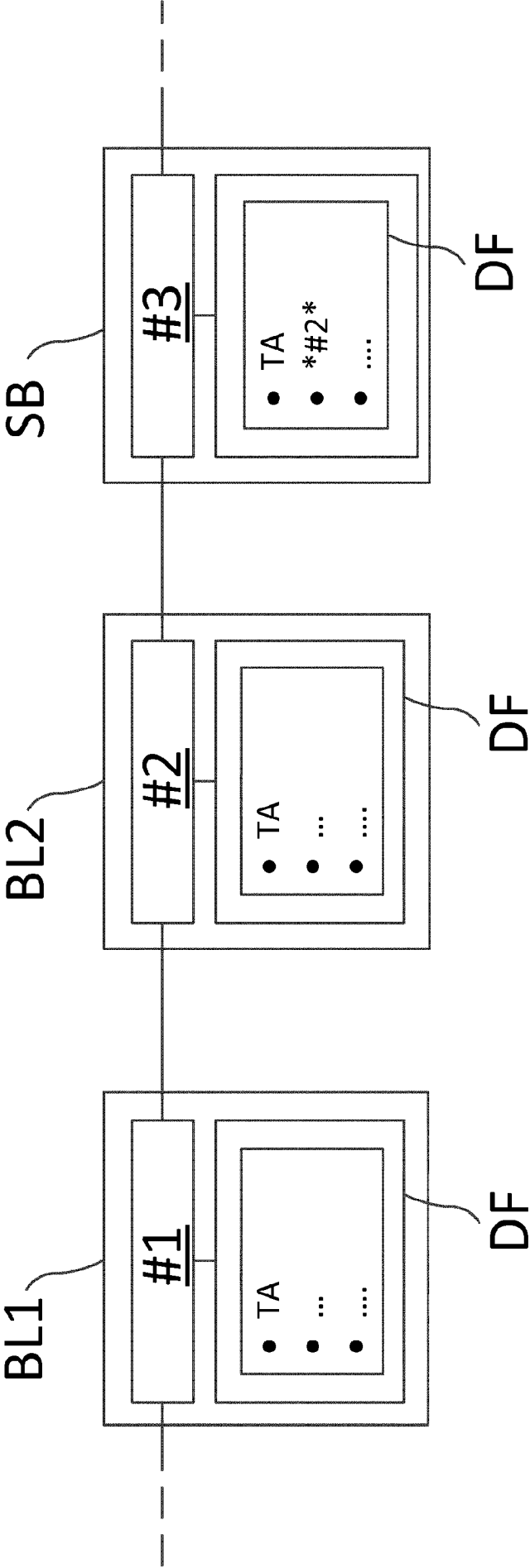


Fig. 1

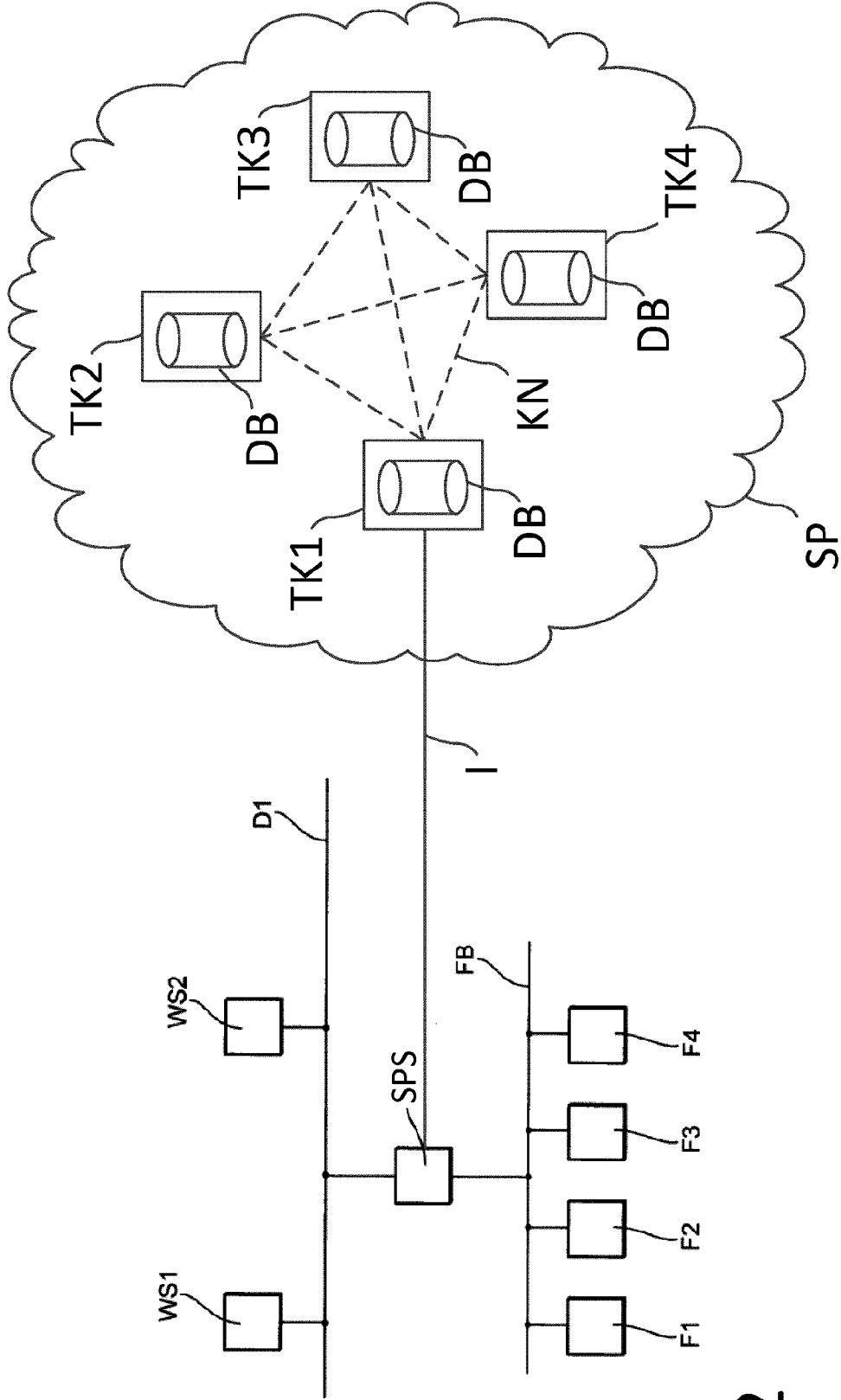


Fig. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/071543A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/64 H04L9/32
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F H04L H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CHALLAL Y ET AL: "A taxonomy of multicast data origin authentication: Issues and solutions", IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, US, vol. 2, no. 3, 1 July 2004 (2004-07-01), pages 34-57, XP011285495, ISSN: 1553-877X the whole document ----- -/--	1-9



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

9 November 2017

Date of mailing of the international search report

17/11/2017

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Mariggis, Athanasios

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2017/071543

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	YUN ZHOU ET AL: "Multimedia Broadcast Authentication Based on Batch Signature [Advances in Mobile Multimedia]", IEEE COMMUNICATIONS MAGAZINE, IEEE SERVICE CENTER, PISCATAWAY, US, vol. 45, no. 8, 1 August 2007 (2007-08-01), pages 72-77, XP011190292, ISSN: 0163-6804 the whole document -----	1-9

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06F21/64 H04L9/32
ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G06F H04L H04W

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	CHALLAL Y ET AL: "A taxonomy of multicast data origin authentication: Issues and solutions", IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, US, Bd. 2, Nr. 3, 1. Juli 2004 (2004-07-01), Seiten 34-57, XP011285495, ISSN: 1553-877X das ganze Dokument ----- -/--	1-9



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

9. November 2017

Absendedatum des internationalen Recherchenberichts

17/11/2017

Name und Postanschrift der Internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Mariggis, Athanasios

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	YUN ZHOU ET AL: "Multimedia Broadcast Authentication Based on Batch Signature [Advances in Mobile Multimedia]", IEEE COMMUNICATIONS MAGAZINE, IEEE SERVICE CENTER, PISCATAWAY, US, Bd. 45, Nr. 8, 1. August 2007 (2007-08-01), Seiten 72-77, XP011190292, ISSN: 0163-6804 das ganze Dokument -----	1-9