(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 816 012**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 29/08 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **11.07.2018 E 18182973 (0)**

(97) Fecha y número de publicación de la concesión europea: **17.06.2020 EP 3595267**

(54) Título: **Procedimiento, dispositivos y sistema para el intercambio de datos entre un sistema distribuido de base de datos y aparatos**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
31.03.2021

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Werner-von-Siemens-Straße 1
80333 München, DE

(72) Inventor/es:

JETZFELLNER, THOMAS

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Procedimiento, dispositivos y sistema para el intercambio de datos entre un sistema distribuido de base de datos y aparatos

La invención se refiere a procedimientos, dispositivos y un sistema para el intercambio de datos entre un sistema distribuido de base de datos y aparatos.

Los aparatos, como aparatos de campo y aparatos de fabricación, están siempre fuertemente entrelazados y por ejemplo pueden ser preparados/operados por diferentes operadores. Frecuentemente a estos aparatos se transmiten series de comandos, que pueden ser ejecutados por el aparato. Al respecto, es una desventaja que frecuentemente los aparatos antiguos no pueden comunicarse sin más con la nueva infraestructura de TI.

A partir del estado de la técnica se conocen los documentos WO 2017/167549 A1, DE 10 2016 215914 A1 y DE 10 2016 118614 A1.

Es un objetivo de la presente invención encontrar una alternativa a las soluciones conocidas del estado de la técnica.

El objetivo es logrado mediante los rasgos indicados en las reivindicaciones independientes. en las reivindicaciones dependientes se presentan mejoras ventajosas de la invención.

La tecnología de las cadenas de bloque (en inglés *Blockchains*) o "registros distribuidos" es actualmente una tecnología intensamente discutida, que en particular puede ser ejecutada como sistema distribuido de base de datos. Aparte de aplicaciones para sistemas descentralizados de pago (por ejemplo *Bitcoin*) en la industria financiera se desarrollan novedosas posibilidades de aplicación. En particular, mediante ellas pueden ejecutarse, con protección frente a la manipulación, transacciones entre compañías, sin intermediarios o centros de intercambio. Esto hace posibles novedosos modelos de negocio, sin un intermediario confiable, reduce los costes de transacción y pueden ofrecerse de manera flexible novedosos servicios digitales, sin por ello tener que establecer una infraestructura con configuración especial y relaciones de confianza. Un registro de datos de transacción (o brevemente transacción) protegido por una cadena de bloque comprende por ejemplo códigos de programa, que pueden ser definidos también como los denominados "contratos inteligentes".

De acuerdo con un primer aspecto, la invención se refiere a un dispositivo receptor, que comprende:

- por ejemplo una primera interfaz de comunicación, en la que

- por ejemplo la primera interfaz de comunicación está configurada para comunicarse con un sistema distribuido de base de datos,

- por ejemplo la primera interfaz de comunicación está configurada para recibir primeros mensajes del sistema distribuido de base de datos;

- por ejemplo un módulo de identificación, en el que

- por ejemplo el módulo de identificación está configurado para calcular, por medio del respectivo contenido de mensajes de los primeros mensajes, una asignación respecto a cuál aparato está designado para un primer mensaje correspondiente;

- por ejemplo un módulo de conversión, en el que

- por ejemplo el módulo de conversión está configurado para convertir el contenido de mensajes del correspondiente primer mensaje, en un formato de datos para el aparato asignado;

- por ejemplo una segunda interfaz de comunicación, en la que

- por ejemplo la segunda interfaz de comunicación está configurada para transmitir el contenido convertido de mensajes y/o el contenido de mensaje del correspondiente primer mensaje (y/o el primer mensaje en sí mismo) al aparato, que está asignado al correspondiente primer mensaje.

En tanto en la siguiente descripción no se indique de otro modo, los conceptos de "ejecutar", "computar", "computarizado", "calcular", "determinar", "generar", "configurar", "reconstruir" y similares se refieren preferiblemente a acciones y/o procesos y/o etapas de procesamiento, que modifican y/o generan datos y/o transforman datos en otros datos, en los que en particular los datos son presentados o pueden estar presentes como magnitudes físicas, por ejemplo como impulsos eléctricos. En particular, la expresión "computador" debería ser interpretada de la manera más amplia posible, para cubrir en particular todos los aparatos electrónicos con propiedades de

procesamiento de datos. Con ello, los computadores pueden ser por ejemplo computadores personales, servidores, controles programables de almacenamiento (SPS), sistemas portátiles de computador, aparatos PC de bolsillo, aparatos móviles de comunicación y otros aparatos de comunicación, que pueden procesar datos computarizados, procesadores y otros aparatos electrónicos para el procesamiento de datos.

En relación con la invención, puede entenderse por "computarizado" por ejemplo una implementación del procedimiento en la cual en particular un procesador ejecuta por lo menos una etapa de procedimiento del método. Por ejemplo se entiende por "computarizado" también "implementado por computador".

En relación con la invención, puede entenderse por un procesador, por ejemplo una máquina o un circuito electrónico. En particular, un procesador puede ser un procesador principal (en inglés *Central Processing Unit*, CPU), un microprocesador o un microcontrolador, por ejemplo un circuito integrado específico para la aplicación o un procesador de señal digital, posiblemente en combinación con una unidad de almacenamiento, para almacenar comandos de programa, etc.. Un procesador puede ser por ejemplo también un IC (circuito integrado, en inglés *Integrated Circuit*), en particular un FPGA (en inglés *Field Programmable Gate Array*) o un ASIC (circuito integrado de aplicación específica, en inglés *Application-Specific Integrated Circuit*), o un DSP (procesador de señal digital, en inglés *Digital Signal Processor*) o un procesador gráfico GPU (*Graphic Processing Unit*). También puede entenderse por un procesador, un procesador virtualizado, una máquina virtual o una CPU blanda. Puede tratarse también por ejemplo de un procesador programable, que está equipado con etapas de configuración para la realización del procedimiento mencionado de acuerdo con la invención o está configurado con etapas de configuración, de modo que el procesador programable ejecuta los rasgos de acuerdo con la invención del procedimiento, los componentes, los módulos u otros aspectos y/o aspectos parciales de la invención.

En relación con la invención, puede entenderse por una "unidad de almacenamiento" o "módulo de almacenamiento" y similares, por ejemplo un almacenamiento volátil en forma de almacenamiento de trabajo (en inglés *Random-Access Memory*, RAM) o un almacenamiento duradero como un disco duro o un medio de datos.

En relación con la invención, puede entenderse por un "módulo", por ejemplo un procesador y/o una unidad de almacenamiento, para el almacenamiento de comandos de programa. Por ejemplo, el procesador está configurado especialmente para ejecutar los comandos de programa, de tal modo que el procesador ejecuta funciones para implementar o ejecutar el procedimiento de acuerdo con la invención o una etapa del procedimiento de acuerdo con la invención. Por ejemplo un módulo puede ser también un nodo del sistema distribuido de base de datos, el cual realiza por ejemplo las funciones/rasgos específicos de un módulo correspondiente. Los respectivos módulos pueden estar formados por ejemplo también como módulos separados o independientes. Para ello, los módulos correspondientes pueden comprender por ejemplo otros elementos. Estos elementos son por ejemplo una o varias interfaces (por ejemplo interfaces de bancos de datos, interfaces de comunicación - por ejemplo interfaz de red, interfaz WLAN) y/o una unidad de evaluación (por ejemplo un procesador) y/o una unidad de almacenamiento. Mediante las interfaces pueden por ejemplo intercambiarse datos (por ejemplo pueden ser recibidos, transmitidos, enviados o preparados). Mediante la unidad de evaluación, los datos pueden por ejemplo ser computarizados y/o comparados de manera automatizada, verificados, procesados, asignados o calculados. Mediante la unidad de almacenamiento, los datos pueden ser almacenados, recuperados o preparados de manera computarizada y/o automatizada.

En relación con la invención puede entenderse por "comprender", en particular en referencia a datos y/o informaciones, por ejemplo un almacenamiento (computarizado) de una información correspondiente o unos datos correspondientes, en una estructura de datos/registro de datos (que a su vez por ejemplo es almacenada en una unidad de almacenamiento).

En relación con la invención, puede entenderse por "asignar", en particular, respecto a datos y/o informaciones, por ejemplo una asignación computarizada de datos y/o informaciones. Por ejemplo, para ello a una primera fecha, mediante una dirección de almacenamiento o un identificador inequívoco (en inglés *unique identifier* (UID)) se asigna una segunda fecha en la cual por ejemplo se almacena en un registro de datos, la primera fecha junto con la dirección de almacenamiento o el identificador inequívoco de la segunda fecha.

En relación con la invención, puede entenderse por "preparación", en particular en referencia a datos y/o informaciones, por ejemplo una preparación computarizada. La preparación ocurre por ejemplo mediante una interfaz (por ejemplo una interfaz de banco de datos, una interfaz de red, una interfaz con una unidad de almacenamiento). Mediante esta interfaz pueden por ejemplo transmitirse y/o enviarse y/o recuperarse y/o recibir datos y/o informaciones correspondientes para la preparación.

En relación con la invención puede entenderse por "preparación" por ejemplo también una carga o un almacenamiento, por ejemplo una transacción con datos correspondientes. Esto puede ocurrir por ejemplo sobre o de un módulo de almacenamiento. Por ejemplo puede entenderse por "preparación" también una transferencia (o un envío o una transmisión) de datos correspondientes de un nodo hasta otro nodo de la cadena de bloque o del

sistema distribuido de base de datos (o su infraestructura).

En relación con la invención, puede entenderse por una "suma de verificación", por ejemplo una suma de verificación de datos de bloque, una suma de verificación de datos, una suma de verificación de nodos, una suma de verificación de transacciones, una suma de verificación de encadenamientos o similares, por ejemplo una suma de verificación criptográfica o resumen o valor de resumen criptográfico, que se forman o se calculan en particular por medio de una función de resumen criptográfico mediante un registro de datos y/o datos y/o una o varias de las transacciones y/o un intervalo parcial de un bloque de datos (por ejemplo el encabezado de bloque de un bloque de una cadena de bloque o encabezado de bloque de datos de un bloque de datos de sistemas distribuidos de base de datos o sólo una parte de las transacciones de un bloque de datos). Una suma de verificación puede ser en particular una(s) suma(s) de verificación o valor(es) de resumen de un árbol de resumen criptográfico (por ejemplo árbol de Merkle, árbol de Patricia). Además, puede entenderse por ellos en particular también una firma digital o un código criptográfico de autenticación de mensajes. Por medio de las sumas de verificación puede efectuarse por ejemplo sobre diferentes planos del sistema de banco de datos, una protección criptográfica/protección de manipulación para las transacciones y los (registros de) datos allí almacenados. Si por ejemplo se requiere una alta seguridad, por ejemplo las sumas de verificación son generadas y comprobadas en los planos de transacción. si se requiere una seguridad menos elevada, por ejemplo las sumas de verificación son generadas y comprobadas en los planos de bloque (por ejemplo sobre la totalidad de bloque de datos o sólo sobre una parte del bloque de datos y/o una parte de las transacciones).

En relación con la invención puede entenderse por una "suma de verificación de bloque de datos", una suma de verificación que es calculada por ejemplo sobre una parte o sobre todas las transacciones de un bloque de datos. Por ejemplo, un nodo puede confirmar/determinar la integridad/autenticidad de la parte correspondiente de un bloque de datos, mediante la suma de verificación de bloque de datos. Adicional o alternativamente, la suma de verificación de bloque de datos puede en particular haber sido formada sobre transacciones de un precedente de bloque de datos/precursor de bloque de datos del bloque de datos. La suma de verificación del bloque de datos puede ser ejecutada al respecto en particular también por medio de un árbol de resumen criptográfico, por ejemplo un árbol de Merkle [1] o un árbol de Patricia, en la que la suma de verificación del bloque de datos es en particular la suma de verificación raíz del árbol de Merkle o de un árbol de Patricia o de un árbol binario de resumen criptográfico. En particular las transacciones son aseguradas mediante otras sumas de verificación del árbol de Merkle o el árbol de Patricia (por ejemplo usando las sumas de verificación de las transacciones), en las que en particular las otras sumas de verificación son hojas en el árbol de Merkle o el árbol de Patricia. La suma de verificación de bloque de datos puede con ello asegurar por ejemplo las transacciones, en lo cual a partir de las otras sumas de verificación se forma la suma de verificación raíz. La suma de verificación de bloques de datos puede ser calculada en particular para transacciones de un bloque de datos determinado, de los bloques de datos. En particular, una tal suma de verificación de bloque de datos puede ser adoptada en un subsiguiente bloque de datos del bloque de datos determinado, para encadenar este subsiguiente bloque de datos por ejemplo con su bloque de datos precedente y en particular con ello hacer comprobable una integridad del sistema distribuido de base de datos. Mediante ello, la suma de verificación de bloque de datos puede por ejemplo asumir la función de la suma de verificación de encadenamiento o adoptar la suma de verificación de encadenamiento. El encabezado de un bloque de datos (por ejemplo de un nuevo bloque de datos o del bloque de datos para el cual se formó la suma de verificación de bloque de datos) puede comprender por ejemplo la suma de verificación de bloque de datos.

En relación con la invención, puede entenderse por "suma de verificación de transacción", una suma de verificación que se forma en particular por una transacción de un bloque de datos. Adicionalmente, por ejemplo puede acelerarse un cálculo de una suma de verificación de bloque de datos para un bloque de datos correspondiente, puesto que para ello por ejemplo pueden usarse sumas de verificación de transacciones ya calculadas, igualmente como hojas por ejemplo de un árbol de Merkle.

En relación con la invención puede entenderse por una "suma de verificación de encadenamiento", una suma de verificación, que en particular indica o referencia un respectivo bloque de datos del sistema distribuido de base de datos, al bloque de datos precedente del sistema distribuido de base de datos (denominado en la literatura especializada en particular frecuentemente como "resumen criptográfico de bloque previo") [1]. Para ello, se forma en particular para el correspondiente bloque de datos precedente, una suma de verificación de encadenamiento correspondiente. Como suma de verificación de encadenamiento puede usarse por ejemplo una suma de verificación de transacciones o la suma de verificación de bloque de datos de un bloque de datos (por consiguiente un bloque de datos existente del sistema distribuido de base de datos), para encadenar un nuevo bloque de datos con un bloque de datos (existente) del sistema distribuido de base de datos. Sin embargo, también es posible por ejemplo que se forme una suma de verificación sobre un encabezado del bloque de datos precedente o sobre la totalidad del bloque de datos precedente, y sea usada como suma de verificación de encadenamiento. Esta puede ser calculada por ejemplo también para varios o todos los bloques de datos precedentes. También es realizable por ejemplo que sobre el encabezado de un bloque de datos y la suma de verificación de bloque de datos, se forme la suma de verificación de encadenamiento. Un respectivo bloque de datos del sistema distribuido de base de datos

comprende sin embargo preferiblemente en cada caso una suma de verificación de encadenamiento, que fue calculada para un bloque de datos precedente, en particular aún más preferido el bloque de datos directamente precedente, del respectivo bloque de datos, o se refiere a este. Por ejemplo también es posible que se forme una correspondiente suma de verificación de encadenamiento, también sólo sobre una parte del correspondiente bloque de datos (por ejemplo bloque de datos precedente). Mediante ello puede realizarse por ejemplo un bloque de datos, que comprende una parte con protección de la integridad y una parte no protegida. Con ello se realiza por ejemplo un bloque de datos, cuya parte que tiene protección de integridad está inmodificada y cuya parte no protegida aun más tarde puede ser modificada. al respecto, en particular se entiende por protección de la integridad, que mediante una suma de verificación puede determinarse una modificación de los datos que tienen protección de integridad.

Los datos que son almacenados por ejemplo en una transacción de un bloque de datos, pueden ser preparados en particular de diferente manera. En lugar de los datos, por ejemplo datos del usuario como datos de medición o datos/situación de propiedad a activos, por ejemplo una transacción de un bloque de datos puede comprender sólo la suma de verificación para estos datos. Al respecto, la correspondiente suma de verificación puede ser ejecutada de diferente forma. Esta puede ser por ejemplo una suma correspondiente de verificación de bloque de datos de un bloque de datos (con los datos correspondientes) de otro banco de datos o del sistema distribuido de base de datos, una suma de verificación de transacciones de un bloque de datos con los correspondientes datos (del sistema distribuido de base de datos u otro banco de datos) o una suma de verificación de datos, que se formó sobre los datos.

Adicionalmente, la correspondiente transacción puede comprender aún una referencia o una información a un sitio de almacenamiento (por ejemplo una dirección de un servidor de archivos e información, sobre donde se encuentran los correspondientes datos en el servidor de archivos; o una dirección de otro banco de datos distribuido, el cual comprende los datos). Los datos correspondientes podrían luego ser preparados por ejemplo también en otra transacción de otro bloque de datos del sistema distribuido de base de datos (por ejemplo cuando los datos correspondientes y las sumas de verificación relacionadas están incluidos en diferentes bloques de datos). Por ejemplo es imaginable también, que estos datos sean preparados mediante otro canal de comunicación (por ejemplo sobre otro banco de datos y/o un canal de comunicación asegurado de modo criptográfico).

También, por ejemplo, adicionalmente a la suma de verificación, puede almacenarse un registro adicional de datos (por ejemplo una referencia o una información sobre un lugar de almacenamiento) en las transacciones correspondientes, el cual indica en particular un sitio de almacenamiento, donde los datos pueden ser recuperados. Esto es ventajoso, en particular con el fin de mantener tan bajo como sea posible un tamaño de archivo de la cadena de bloque o del sistema distribuido de base de datos.

En relación con la invención, puede entenderse por "protegido con seguridad", por ejemplo una protección que es ejecutada en particular mediante un procedimiento criptográfico. Por ejemplo esto puede ser ejecutado mediante un aprovechamiento del sistema distribuido de base de datos para la preparación o transferencia o envío de datos/transacciones correspondientes. Se alcanza esto preferiblemente mediante una combinación de las diferentes sumas de verificación (criptográficas), en la cual en particular éstas cooperan de manera sinérgica, para mejorar por ejemplo la seguridad o la seguridad criptográfica para los datos de las transacciones. En otras palabras, en relación con la invención, puede entenderse en particular por "protegido con seguridad" también "protegido de modo criptográfico" y/o "protegido contra la manipulación", en la cual "protegido contra la manipulación" puede ser denominado también como "con integridad protegida".

En relación con la invención, puede entenderse por "encadenar el/los bloque(s) de datos de un sistema distribuido de base de datos" por ejemplo, que los bloques de datos comprenden en cada caso una información (por ejemplo suma de verificación de encadenamiento), que remite a otro bloque de datos o varios otros bloques de datos del sistema distribuido de base de datos, o hacen referencia a estos [1] [4] [5].

En relación con la invención, puede entenderse por "insertar en el sistema distribuido de base de datos" y similares, por ejemplo, que en particular una transacción o las transacciones o un bloque de datos con sus transacciones, son transmitidos a uno o varios nodos de un sistema distribuido de base de datos. Si esas transacciones son por ejemplo validadas de manera exitosa (por ejemplo por el/los nodo(s)), en particular estas transacciones son encadenadas como nuevos bloques de datos con por lo menos un bloque existente de datos del sistema distribuido de base de datos [1][4][5]. para ello, las transacciones correspondientes son almacenadas por ejemplo un nuevo bloque de datos. En particular, esta validación y/o encadenamiento puede ocurrir mediante un nodo confiable (por ejemplo un Nodo de Minería, un Oráculo de Cadena de Bloque o una Plataforma de Cadena de Bloque). En particular, al respecto puede entenderse por una Plataforma de Cadena de Bloque, una cadena de bloque como servicio (en inglés *Blockkette als Service*), como es propuesto en particular por Microsoft o IBM. En particular pueden depositarse un nodo confiable y/o un nodo de en cada caso una suma de verificación de nodo (por ejemplo una firma digital) en un bloque de datos (por ejemplo en el bloque de datos validado y generado por ellos, que luego es encadenado), para hacer posible en particular una facilidad de identificación del creador del bloque de datos y/o

hacer posible una facilidad de identificación del nodo. Al respecto, está suma de verificación de nodos indica cuáles nodos por ejemplo han encadenado el correspondiente bloque de datos con por lo menos otro bloque de datos del sistema distribuido de base de datos.

En relación con la invención puede entenderse por "transacción" o "transacciones" por ejemplo un Contrato Inteligente [4] [5], una estructura de datos o un registro de datos de transacción, el cual comprende en particular en cada caso una de las transacciones o varias transacciones. En relación con la invención, pueden entenderse por "transacción" o "transacciones", por ejemplo también los datos de una transacción de un bloque de datos de una cadena de bloque (en inglés *Blockchain*). Una transacción puede comprender en particular un código de programa, el cual ejecuta por ejemplo un Contrato Inteligente. Por ejemplo, en relación con la invención puede entenderse por transacción, también una transacción de control y/o transacción de confirmación. De modo alternativo, una transacción puede ser por ejemplo una estructura de datos que almacena datos (por ejemplo los comandos de control y/o datos de contrato y/u otros datos como datos de video, datos de usuario, datos de medición, etc.). En relación con la invención, una "transacción" puede ser por ejemplo también un mensaje o un mensaje de comunicación o ser denominado como uno tal. Por ejemplo un mensaje corresponde a una transacción, en el que el mensaje comprende por ejemplo comandos de control para el manejo del aparato y/o comprende también requerimientos (por ejemplo requisitos preestablecidos) para la ejecución de los comandos de control.

En particular se entiende por "almacenamiento de transacciones en bloques de datos", "almacenamiento de transacciones" y similares, un almacenamiento directo o almacenamiento indirecto. Al respecto, puede entenderse por un almacenamiento directo por ejemplo, que el correspondiente bloque de datos (del sistema distribuido de base de datos) o la correspondiente transacción del sistema distribuido de base de datos) comprende los respectivos datos. Al respecto, puede entenderse por un almacenamiento indirecto por ejemplo que el correspondiente bloque de datos o la transacción correspondiente comprende una suma de verificación y opcionalmente un registro adicional de datos (por ejemplo una referencia o una información sobre un sitio de almacenamiento) para los datos correspondientes, y con ello los datos correspondientes no están almacenados directamente en el bloque de datos (o la transacción) (por consiguiente en lugar de ello sólo una suma de verificación para estos datos). En particular, en el almacenamiento de transacciones en bloques de datos, pueden verificarse estas sumas de verificación por ejemplo, del modo como se aclara esto por ejemplo bajo "Inserción en el sistema distribuido de base de datos".

En relación con la invención, puede entenderse por un "código de programa" (por ejemplo un Contrato Inteligente), por ejemplo un comando de programa o varios comandos de programa, que están almacenados en particular en una o varias transacciones. El código de programa es en particular ejecutable y es ejecutado por ejemplo por el sistema distribuido de base de datos. Esto puede ser efectuado por ejemplo mediante un ambiente de ejecución (por ejemplo una máquina virtual), en el que el ambiente de ejecución o el código de programa son de modo preferible completamente Turing. El código del programa es ejecutado preferiblemente por la infraestructura del sistema distribuido de base de datos [4][5]. Al respecto, la infraestructura del sistema distribuido de base de datos realiza por ejemplo una máquina virtual.

En relación con la invención, puede entenderse por un "contrato inteligente", por ejemplo un código de programa ejecutable [4][5] (véase en particular la definición "código de programa"). El Contrato Inteligente es almacenado preferiblemente en una transacción de un sistema distribuido de base de datos (por ejemplo una cadena de bloque), por ejemplo en un bloque de datos del sistema distribuido de base de datos. Por ejemplo, el Contrato Inteligente puede ser ejecutado de la misma manera, en que se aclara en la definición de "código de programa", en particular en relación con la invención.

En relación con la invención, puede entenderse por "Proceso de Contrato Inteligente" o un "Contrato Inteligente", en particular también una ejecución de un código de programa o un Contrato Inteligente en un proceso, por el das sistema distribuido de base de datos o su infraestructura.

En relación con la invención, puede entenderse por "evidencia de prueba de trabajo", por ejemplo una liberación de una tarea intensiva en cálculo, que se resuelve en particular en función del contenido de bloque de datos/contenido de una transacción determinada [1] [4] [5]. Una tarea así de intensiva en cálculo es denominada por ejemplo también como rompecabezas criptográfico.

En relación con la invención, puede entenderse por un "sistema distribuido de base de datos", que puede ser denominado por ejemplo también como banco de datos distribuido, por ejemplo un banco de datos, una cadena de bloque (en inglés *Blockchain*), un registro distribuido, un sistema distribuido de almacenamiento, un sistema a base (DLTS) de tecnología de registro distribuido (DLT), un sistema de banco de datos con seguridad de revisión, una nube, un servicio de nube, una cadena de bloque en una nube o un banco de datos par a par, distribuidos de manera descentralizada. También pueden usarse por ejemplo diferentes implementaciones de una cadena de bloque o un DLTS, como por ejemplo una cadena de bloque o un DLTS, por medio de un gráfico acílico dirigido (DAG), un rompecabezas criptográfico, un gráfico de resumen criptográfico o una combinación de las variantes

mencionadas de implementación [6][7]. También pueden implementarse por ejemplo diferentes procedimientos de consenso (en inglés *consensus algorithms*). Este puede ser por ejemplo un procedimiento de consenso por medio de un rompecabezas criptográfico, Rumor sobre Rumor, votación virtual o una combinación, de los procedimientos mencionados (por ejemplo, se combina Rumor sobre Rumor con rotación virtual) [6][7]. Si por ejemplo se usa una cadena de bloque, entonces ésta puede ser transformada en particular por medio de una realización a base de Bitcoin o una realización a base del Ethereum [1][4][5]. Puede entenderse por un "sistema distribuido de base de datos", por ejemplo también un sistema distribuido de base de datos, del cual al menos una parte de sus nodos y/o aparatos y/o infraestructura, son realizados mediante una nube. Por ejemplo los componentes correspondientes son realizados como nodo/aparato en la nube (por ejemplo como nodos virtuales en una máquina virtual). Esto puede ocurrir por ejemplo mediante equipo VM, Amazon Web Services o Microsoft Azure. Debido a la elevada flexibilidad de las variantes ilustradas de implementación, pueden combinarse mutuamente en particular también aspectos parciales de las mencionadas variantes de implementación, en lo cual como cadena de bloque se usa por ejemplo un gráfico de registro criptográfico, en lo cual la cadena de bloque en sí misma puede por ejemplo no tener bloque.

Si se usa por ejemplo un gráfico acílico directo (DAG) (por ejemplo IOTA o Tangle), en particular las transacciones o bloques o nodos de los gráficos están asociados mutuamente, por bordes dirigidos mutuamente. Esto significa en particular, que los bordes (preferiblemente todos los bordes) tienen la misma dirección (preferiblemente siempre la misma dirección), de modo similar a como es por ejemplo en el tiempo. En otras palabras, en particular no es posible acumular hacia atrás o iniciar (por consiguiente contra la misma dirección conjunta) las transacciones o los bloques o los nodos del gráfico. Al respecto, acíclico significa en particular, que no existen bucles en el transcurso del gráfico.

El sistema distribuido de base de datos puede ser por ejemplo un sistema distribuido público de base de datos (por ejemplo una cadena pública de bloque) o un sistema distribuido cerrado (o privado) de base de datos (por ejemplo una cadena privada de bloque).

Si se trata por ejemplo de un sistema distribuido público de base de datos, esto significa que pueden afiliarse nuevos nodos y/o aparatos sin prueba de autorización o sin autenticación o sin informaciones de inscripción o sin credenciales, al sistema distribuido de base de datos, o pueden ser aceptados por este. En particular, en un caso así puede permanecer anónimo el operador del nodo y/o aparato.

Si el sistema distribuido de base de datos es por ejemplo un sistema distribuido cerrado de base de datos, los nuevos nodos y/o aparatos necesitan por ejemplo una prueba válida de autorización y/o informaciones válidas de autenticación y/o credenciales válidas y/o informaciones válidas de inscripción, para poder afiliarse al sistema distribuido de base de datos o para ser aceptado por éste.

Un sistema distribuido de base de datos puede ser por ejemplo también un sistema de comunicación distribuido para el intercambio de datos. Este puede ser por ejemplo una red o una red par a par. De modo alternativo o adicionalmente, la invención puede ser realizada por ejemplo también mediante una aplicación par a par, en lugar del sistema distribuido de base de datos.

En relación con la invención, puede entenderse por "bloque de datos", que en particular dependiendo del contexto y realización puede denominarse también como "eslabón" o "bloque", por ejemplo un bloque de datos de un sistema distribuido de base de datos (por ejemplo una cadena de bloque o un banco de datos par a par), que es realizado en particular como estructura de datos y preferiblemente comprende en cada caso una de las transacciones o varias de las transacciones. Para una implementación, por ejemplo el banco de datos (o el sistema de banco de datos) puede ser un sistema a base de DLT (DLTS) o una cadena de bloque y un bloque de datos de un bloque de la cadena de bloque o del DLTS. Un bloque de datos puede comprender por ejemplo información sobre el tamaño (tamaño de datos en bites) del bloque de datos, un encabezado de bloque de datos (en inglés *Block-header*), un numerador de transacciones y una o varias transacciones [1]. El encabezado de bloque de datos puede comprender por ejemplo una versión, una suma de verificación de encadenamiento, una suma de verificación de bloque de datos, una marca de fecha, una prueba de evidencia de trabajo y un nonce (valor único, valor aleatorio o numerador, que es usado para la prueba de evidencia de trabajo) [1] [4] [5]. Un bloque de datos puede ser por ejemplo también sólo un intervalo determinado de almacenamiento o de dirección de la totalidad de los datos, que son almacenados en el sistema distribuido de base de datos. con ello se realizan por ejemplo sistema distribuido de base de datos que no tiene bloque (en inglés *blockless*), como por ejemplo la cadena IoT (ITC), IOTA, y *Byteball*. Para ello se combinan mutuamente en particular las funcionalidades de los bloques de una cadena de bloque y las transacciones, de modo que por ejemplo las transacciones en sí mismas aseguran la secuencia o la cadena de transacciones (del sistema distribuido de base de datos) (por consiguiente en particular son almacenados con protección de la seguridad). Para ello, las transacciones pueden encadenarse mutuamente en sí mismas, por ejemplo con una suma de verificación de encadenamiento, en lo cual como suma de verificación de encadenamiento sirve preferiblemente una suma separada de verificación o la suma de verificación de transacciones de una o varias transacciones, que en el almacenamiento de una nueva transacción en el sistema distribuido de base de datos, es almacenada en la nueva transacción correspondiente. En una forma de realización tal, un bloque de datos comprende por ejemplo también

una o varias transacciones, en las que en el caso más simple por ejemplo un bloque de datos corresponde a una transacción.

En relación con la invención, puede entenderse por "nonce", por ejemplo un nonce (abreviatura para: “usado sólo una vez” [2] o "número usado una vez"[3]) criptográfico. En particular define un nonce la combinación individual de números o de letras, que es usada preferiblemente una única vez en el respectivo contexto (por ejemplo transacción, transferencia de datos).

En relación con la invención, puede entenderse por "bloque precedente de datos de un (determinado) bloque de datos del sistema distribuido de base de datos", por ejemplo el bloque de datos del sistema distribuido de base de datos, que en particular precede directamente un (determinado) bloque de datos. De modo alternativo, por "bloque precedente de datos de un (determinado) bloque de datos del sistema distribuido de base de datos" puede entenderse en particular también todos los bloques de datos del sistema distribuido de base de datos, que precede el bloque de datos determinado. Mediante ello puede formarse por ejemplo la suma de verificación de encadenamiento o la suma de verificación de transacciones, en particular sólo sobre el bloque de datos (o sus transacciones) que precede directamente el bloque de datos determinado, o sobre todos los bloques de datos (o sus transacciones) que preceden el primer bloque de datos.

En relación con la invención, puede entenderse por un "nodo de cadena de bloque", "nodo", "nodo de un sistema distribuido de base de datos" y similares, por ejemplo aparatos (por ejemplo aparatos de campo, teléfonos móviles), computadores, teléfonos inteligentes, clientes o participantes, que ejecutan operaciones (con) del sistema distribuido de base de datos (por ejemplo una cadena de bloque) [1] [4] [5]. Tales nodos pueden ejecutar por ejemplo transacciones de un sistema distribuido de base de datos o sus bloques de datos, o introducir o encadenar nuevos bloques de datos con nuevas transacciones en el sistema distribuido de base de datos, por medio de nuevos bloques de datos. En particular esta validación y/o encadenamiento puede ocurrir mediante un nodo confiable (por ejemplo un nodo de minería) o exclusivamente por nodos confiables. Un nodo confiable es por ejemplo un nodo que dispone de medidas adicionales de seguridad (por ejemplo *Firewalls*, limitaciones de acceso a los nodos o similares), para impedir una manipulación del nodo. De modo alternativo o adicionalmente, por ejemplo en el encadenamiento de un nuevo bloque de datos con el sistema distribuido de base de datos, un nodo confiable puede almacenar una suma de verificación de nodos (por ejemplo una firma digital o un certificado) en el nuevo bloque de datos. Con ello puede proveerse en particular una evidencia que indica que se incorporó el correspondiente bloque de datos de un nodo determinado, o indica su origen. Los aparatos (por ejemplo el correspondiente aparato) son por ejemplo aparatos de un sistema técnico y/o instalación industrial y/o una red de automatización y/o una instalación de fabricación, que son en particular también un nodo del sistema distribuido de base de datos. al respecto, los aparatos pueden ser por ejemplo aparatos de campo o los aparatos pueden ser asuntos en Internet, que en particular también son un nodo del sistema distribuido de base de datos. Los nodos pueden comprender por ejemplo también al menos un procesador, para ejecutar por ejemplo su funcionalidad implementada por computador.

En relación con la invención, puede entenderse por un "oráculo de cadena de bloque" y similares, por ejemplo nodos, aparatos o computadores que disponen por ejemplo de un módulo de seguridad, que por ejemplo dispone de mecanismos de protección de software (por ejemplo procedimientos criptográficos), aparatos de protección mecánica (por ejemplo una carcasa que puede ser bloqueada) o aparatos eléctricos de protección, (por ejemplo comprende protección contra la alteración o un sistema protector, que borra los datos del módulo de seguridad para un uso/manipulación indebidos del oráculo de cadena de bloque). Al respecto, el módulo de seguridad puede comprender por ejemplo claves criptográficas, que son necesarias para el cálculo de las sumas de verificación (por ejemplo suma de verificación de transacciones o sumas de verificación de nodos).

En relación con la invención, puede entenderse por un "computador" o un "aparato", por ejemplo un (sistema de) computador, un cliente, un teléfono inteligente, un aparato o un servidor, que está dispuesto en cada caso por fuera de la cadena de bloque y no son una parte de la infraestructura del sistema distribuido de base de datos o forman una infraestructura separada aparte. Un aparato es por ejemplo un aparato de fabricación y/o un aparato electromecánico y/o un aparato electrónico y/o un aparato de una red de automatización (por ejemplo para instalaciones técnicas industriales, instalaciones de fabricación, instalaciones de distribución de energía o recursos), en particular estos aparatos no están en capacidad de comunicarse directamente con el sistema distribuido de base de datos.

Por ejemplo, un aparato así por fuera del sistema distribuido de base de datos no puede acceder a los datos del sistema distribuido de base de datos, puesto que el aparato por ejemplo es muy antiguo y no dispone de las capacidades criptográficas y/o de seguridad de TI necesarias, ni es compatible con el formato de datos del sistema distribuido de base de datos.

Con la invención es posible en particular acoplar una infraestructura (a base de cadena de bloque) periférica con aparatos antiguos o legados. Con la invención puede ocurrir en particular un acoplamiento de tales aparatos

antiguos, a una nueva infraestructura a base de cadena de bloque. Esto es ventajoso por ejemplo para redes de suministro de energía, cuyo control es traspasado a una infraestructura de cadena de bloque, en la que sin embargo no está intercambiado cada uno de los aparato individuales de la red existente de suministro de energía. La invención permite por ejemplo, que por ejemplo por medio de una cadena de bloque se envíen mensajes (por ejemplo en transacciones) con comandos de control al aparato individual, en el que el dispositivo E receptor está dispuesto en comunicación entre los aparatos y el sistema distribuido de base de datos y ejecuta la asignación y/o transmisión de los respectivos mensajes en un aparato (correspondiente). En particular los contenidos correspondientes de los mensajes son convertidos también a un formato de datos, que es compatible con un aparato. También puede verificarse de modo por ejemplo criptográfico un contenido de un mensaje y/o puede eliminarse una protección criptográfica (por ejemplo mediante una descodificación del contenido del mensaje).

Para una primera forma de realización del dispositivo receptor, el dispositivo receptor recupera un estado de aparato (por ejemplo estado de error, estado de operación) del aparato asignado, de un correspondiente primer mensaje (por ejemplo por medio del módulo de identificación o de la segunda interfaz de comunicación), en el que ocurre una transferencia al aparato asignado, dependiente del estado recuperado el aparato.

El dispositivo E receptor es para ese efecto ventajoso, para verificar en el aparato, en particular antes de la transmisión del contenido del mensaje, si por ejemplo el aparato correspondiente está conectado o está operacional. Con ello puede impedirse en particular el envío de mensajes al aparato que se encuentra en un estado de error. Si por ejemplo no se envía un mensaje a un aparato asignado correspondiente (por ejemplo porque esto no es posible de modo correspondiente al estado del aparato), un mensaje o transacción correspondiente que comprende este estado de aparato (por ejemplo el estado de error), puede ser transmitido al sistema distribuido de base de datos o ser almacenado en el sistema distribuido de base de datos.

Para otras formas de realización del dispositivo receptor, el estado del aparato comprende un registro de datos sobre los recursos disponibles del aparato y/o propiedades actuales del aparato.

Para otras formas de realización del dispositivo receptor, ocurre una transferencia al correspondiente aparato, cuando el aparato asignado satisface requerimientos preestablecidos del primer mensaje correspondiente, en lo cual por ejemplo se verifica la satisfacción de los requerimientos preestablecidos, mediante el estado del aparato.

El dispositivo E receptor es para ese efecto ventajoso, en particular para verificar si un mensaje correspondiente puede ser procesado de cualquier modo en un aparato. Si un mensaje correspondiente comprende por ejemplo comandos de control para iniciar o controlar un generador o una planta generadora de reserva, por ejemplo en los requerimientos puede pretenderse que debiera generarse por lo menos una cantidad determinada de energía. De modo alternativo (por consiguiente en otro escenario de aplicación) mediante los requerimientos establecidos puede fijarse una determinada precisión de fabricación o duración de fabricación, que debiera ser cumplida. estos requerimientos pueden ser verificados por ejemplo por el dispositivo receptor, en lo cual se verifican los correspondientes recursos disponibles del aparato y/o que el estado del aparato y/o las propiedades actuales del aparato (por ejemplo si el aparato está instalado en el lugar correcto, por ejemplo para no dañar instrucciones de protección de datos; está el aparato o los datos procesados por el aparato protegidos contra el acceso de una persona no autorizada - por ejemplo criptográficamente -, para proteger en particular compañías/conocimiento de fabricación). Esta verificación de los requisitos fijados, que son almacenados por ejemplo en un registro de datos correspondiente, puede ser ejecutada por ejemplo del módulo de identificación, el módulo de conversión, la segunda interfaz de comunicación (por ejemplo una interfaz de red) o un módulo de evaluación del dispositivo receptor, que está dispuesto antes de la interfaz de comunicación (por ejemplo interfaz de red) de un bus de comunicación del dispositivo receptor.

Los requerimientos especificados pueden ser por ejemplo también comandos de control necesarios o comprender unos que especifican comandos de control requeridos por ejemplo, que estos debieran ser ya ejecutados por uno de los aparatos o del aparato, antes de que el mensaje o contenido del mensaje correspondientes (por ejemplo el contenido convertido en mensaje) sea transmitido al aparato. De modo alternativo o adicionalmente, los comandos de control requeridos pueden referirse también a otro aparato, en los que los otros aparatos son por ejemplo aparatos de otra red de automatización. Por ejemplo para verificar si los comandos de control requeridos ya son ejecutados, por ejemplo pueden leerse o verificarse correspondientes mensajes o transacciones en el sistema distribuido de base de datos, que confirman por ejemplo una ejecución de los comandos de control requeridos. Estos correspondientes mensajes o transacciones pueden ser denominados por ejemplo como transacciones de confirmación y pueden ser almacenados en los aparatos correspondientes por ejemplo después de una ejecución de los comandos de control requerido, por ejemplo por medio del dispositivo de envío, en el sistema distribuido de base de datos.

Para otras formas de realización del dispositivo receptor, el dispositivo receptor comprende un módulo de criptografía, en el que el módulo de criptografía comprende datos criptográficos asignados al aparato.

En otras formas de realización, el dispositivo receptor verifica y/o descodificar el módulo de criptografía por medio de los datos criptográficos de al menos una parte del contenido del mensaje del correspondiente primer mensaje para un aparato asignado, en la que por ejemplo para la verificación y/o la descodificación, se cargan los correspondientes datos criptográficos por medio del aparato asignado.

El dispositivo E receptor es ventajoso para el efecto, para verificar en particular los mensajes que deberían ser transmitidos a un aparato correspondiente. Para ello, el creador del mensaje puede por ejemplo haber obtenido una primera clave criptográfica, con la cual se forma por ejemplo una suma de verificación (por ejemplo una suma de verificación de transacciones u otra de las sumas de verificación mencionadas) sobre el mensaje o el contenido del mensaje. De modo alternativo, con esta primera clave criptográfica puede por ejemplo haberse codificado también el contenido del mensaje. Por ejemplo con la primera clave criptográfica (en el caso de un procedimiento criptográfico simétrico) o una segunda clave criptográfica, que está asignada a la primera clave criptográfica (por ejemplo para un procedimiento criptográfico asimétrico en el cual por ejemplo la primera clave es una clave privada y la segunda clave es una clave pública), puede ocurrir la descodificación o verificación del correspondiente contenido del mensaje.

Los datos criptográficos (por ejemplo la clave criptográfica) pueden haber sido generados por ejemplo mediante datos específicos del aparato de manera específica para un aparato (por ejemplo un UID del aparato, un número aleatorio que fue generado por el aparato correspondiente, o fue calculado con ayuda de datos sensores característicos para el aparato - por ejemplo una característica calculada para una señal con ruido, que fue determinada por un sensor del aparatos). De modo alternativo o adicionalmente, los datos criptográficos son una combinación de datos específicos del aparato y datos específicos del dispositivo receptor (por ejemplo un UID del dispositivo receptor, un número aleatorio que fue generado por el dispositivo receptor, o fue calculado por datos sensores para el dispositivo receptor - por ejemplo una característica calculada para una señal con ruido, que fue determinada por un sensor del dispositivo receptor). Por ejemplo también es posible que, por medio de datos específicos para el aparato y/o datos específicos para el dispositivo receptor se determinen de manera reproducible los datos criptográficos para el aparato correspondiente, o que por medio de estos datos se suspenda una protección criptográfica (por ejemplo una codificación), con la cual se protegen los datos criptográficos correspondientes de un aparatos, (por ejemplo sea descodificada) y/o sea verificada (por ejemplo se verifique una firma digital). Los datos específicos del aparato pueden ser recuperados por ejemplo en la recuperación del estado del aparato, para un aparato. Los datos específicos de aparato y/o datos específicos de dispositivo receptor son preferiblemente datos que pueden ser falseados sólo difícilmente, por ejemplo una característica de una señal de ruido (que es capturada por ejemplo por un sensor o un módulo de protección contra la manipulación), que es modificada en una manipulación del aparato, de modo que la característica cambia de forma que los datos criptográficos son inválidos o ya no puede tenerse acceso a estos. Los datos específicos del aparato pueden ser determinados o intercambiados también mediante un procedimiento de desafío-respuesta, en el cual por ejemplo el procedimiento está configurado en el lado del aparato y en el lado del dispositivo receptor, con valores iniciales correspondientes (por ejemplo en lo cual en un almacenamiento protegido del aparato o del dispositivo receptor, se configuran previamente valores iniciales correspondientes o se calculan y/o suministran estos valores iniciales por la memoria protegida) y los correspondientes datos específicos del aparato (por ejemplo una clave criptográfica o una parte de una clave criptográfica) puede ser recuperada del dispositivo receptor.

De acuerdo con otro aspecto, la invención se refiere a un dispositivo de envío, que exhibe

- por ejemplo una primera interfaz de comunicación, en la que

- por ejemplo la primera interfaz de comunicación está configurada para comunicarse con aparatos,

- por ejemplo la interfaz de comunicación está configurada para recibir primeros mensajes de los aparatos;

- por ejemplo un módulo de identificación, en el que

- por ejemplo el módulo de identificación está configurado para calcular, mediante el respectivo contenido del mensaje del primer mensaje, una asignación respecto a cuál aparato ha enviado un correspondiente primer mensaje;

- por ejemplo un módulo de conversión, en el que

- por ejemplo el módulo de conversión está configurado para convertir el contenido del mensaje del correspondiente primer mensaje, en un formato de datos para el sistema distribuido de base de datos;

- por ejemplo una segunda interfaz de comunicación, en la que

- por ejemplo la segunda interfaz de comunicación está configurada para comunicarse con un sistema distribuido de

base de datos,

- por ejemplo la interfaz de comunicación está configurada para transmitir el contenido convertido del mensaje y/o el contenido del mensaje del primer mensaje correspondiente (y/o el primer mensaje en sí mismo) al sistema distribuido de base de datos.

Con la invención es posible en particular acoplar una infraestructura periférica con aparatos antiguos o legados. Con la invención puede realizarse en particular un acoplamiento de tales aparatos antiguos a una nueva infraestructura a base de cadenas de bloque. Esto es ventajoso por ejemplo para redes de suministro de energía, cuyo control es adaptado a una infraestructura de cadenas de bloque, en la cual sin embargo no se han cambiado todos los aparatos individuales de la red existente de suministro de energía. La invención permite por ejemplo, que por ejemplo un aparato envíe mensajes (por ejemplo con comandos de control o reportes de estado para la ejecución de comandos de control) al sistema distribuido de base de datos, en lo cual el dispositivo de envío está dispuesto en comunicación entre los aparatos y el sistema distribuido de base de datos, y se realiza la asignación y/o transmisión de los respectivos mensajes al sistema distribuido de base de datos. En particular los correspondientes contenidos de mensajes son convertidos también en un formato de datos que es compatible con el sistema distribuido de base de datos. En particular, los aparatos no tienen que estar ajustados a la nueva infraestructura.

En otras formas de realización del dispositivo de envío, el dispositivo de envío comprende un módulo de criptografía, en el que el módulo de criptografía comprende datos criptográficos asignados al aparato.

En otras formas de realización, el dispositivo de envío carga datos criptográficos correspondientes al módulo de criptografía, mediante el aparato asignado, en lo cual mediante los correspondientes datos criptográficos (que preferiblemente son específicos del aparato) al menos una parte del contenido del mensaje del correspondiente primer mensaje, es protegida de modo criptográfico específico para el aparato, para el aparato asignado, y en el que por ejemplo la protección criptográfica ocurre antes del envío del contenido del mensaje.

El dispositivo de envío es ventajoso para el efecto de proteger de modo criptográfico en particular los mensajes que son enviados al sistema distribuido de base de datos (y/o son almacenados por éste). Esto puede ocurrir por ejemplo mediante la protección y/o codificación del correspondiente contenido del mensaje por medio de una suma de verificación (criptográfica) (por ejemplo una suma de verificación de transacciones). Para ello, el dispositivo de envío puede comprender por ejemplo una primera clave criptográfica (ésta es por ejemplo específica para el aparato), con la cual se forma por ejemplo una suma de verificación sobre los mensajes o el contenido de los mensajes. De modo alternativo, con esta primera clave criptográfica puede codificarse también por ejemplo el contenido de los mensajes. Un receptor del mensaje puede por ejemplo con la primera clave criptográfica (en el caso de un procedimiento criptográfico simétrico) o una segunda clave criptográfica, que es asignada a la primera clave criptográfica (por ejemplo para un procedimiento criptográfico asimétrico en el cual por ejemplo la primera clave es una clave privada y la segunda clave es una clave pública), ejecutar la descodificación o verificación del correspondiente contenido del mensaje. En este caso, el correspondiente material clave del receptor puede haber sido transmitido por ejemplo por un canal seguro.

Los datos criptográficos (por ejemplo la llave criptográfica) pueden haber sido generados por ejemplo mediante datos específicos para el aparato (por ejemplo un UID del aparato, un número aleatorio que fue generado por el correspondiente aparato, o fue calculado mediante datos de sensor característicos para el aparato - por ejemplo una característica calculada para una señal de ruido que fue determinada mediante un sensor del aparato). De modo alternativo o adicional, los datos criptográficos son una combinación de datos específicos del aparato y datos específicos del dispositivo de envío (por ejemplo un UID del dispositivo de envío, un número aleatorio que fue generado por el dispositivo de envío, o fue calculado mediante datos de sensor para el dispositivo de envío - por ejemplo una característica calculada para una señal de ruido, que fue determinada mediante un sensor del dispositivo de envío). Por ejemplo, también es posible que por medio de los datos específicos para el aparato y/o datos específicos para el dispositivo de envío, se determinen de manera reproducible los datos criptográficos para el correspondiente aparato. Por ejemplo mediante datos específicos del aparato y/o datos específicos del dispositivo de envío puede suspenderse (por ejemplo descodificarla) una protección criptográfica (por ejemplo una codificación), con la cual se protegen los correspondientes datos criptográficos de un aparato, y/o verificarse (por ejemplo se verifica una firma digital o se verifica una suma de verificación (criptográfica) para los datos criptográficos), cuando por ejemplo de los datos específicos del aparato y/o datos específicos del dispositivo de envío, para ello se deriva o calcula una llave criptográfica separada. Los datos específicos para el aparato pueden ser almacenados por ejemplo en el mensaje del aparato correspondiente. Los datos específicos del aparato y/o datos específicos del dispositivo de envío son preferiblemente datos que pueden ser falseados sólo difícilmente, por ejemplo una característica de una señal de ruido (es capturada por ejemplo por un sensor o un módulo protector contra la manipulación), que por una manipulación del aparato es modificada de modo que la característica cambia de manera que los datos criptográficos se tornan inválidos o ya no puede tenerse acceso a estos. Los datos específicos del aparato pueden también ser determinados o intercambiados por medio de un procedimiento de desafío-respuesta, en el cual por

ejemplo el procedimiento es configurado en el lado del aparato y el lado del dispositivo de envío, con valores iniciales correspondientes (por ejemplo en lo cual en un almacenamiento protegido del aparato o del dispositivo de envío, se configuran previamente valores iniciales correspondientes o se calculan y/o suministran estos valores iniciales por la memoria protegida) y los correspondientes datos específicos del aparato (por ejemplo una clave criptográfica o una parte de una clave criptográfica) puede ser recuperada del dispositivo de envío.

En otras formas de realización del dispositivo de envío y/o del dispositivo receptor, el sistema distribuido de base de datos es una cadena de bloque, en la que por ejemplo los mensajes que son enviados y/o recibidos por el sistema distribuido de base de datos, son transacciones.

En otras formas de realización del dispositivo de envío y/o del dispositivo receptor, al menos una parte del aparato, es aparato de una red de automatización.

De acuerdo con otro aspecto, la invención se refiere a un sistema que comprende:

- por ejemplo un dispositivo receptor o un dispositivo receptor de acuerdo con la invención, de acuerdo con una de las formas de realización mencionadas;

- por ejemplo un dispositivo de envío de acuerdo con la invención o un dispositivo de envío de acuerdo con una de las formas de realización mencionadas.

De acuerdo con otro aspecto, la invención se refiere a un procedimiento para la recepción computarizada de mensajes, con las siguientes etapas de procedimiento:

- por ejemplo una etapa de procedimiento para la recepción de primeros mensajes de un sistema distribuido de base de datos, por medio de una primera interfaz de comunicación;

- por ejemplo una etapa de procedimiento para el cálculo de una asignación para los primeros mensajes, en la que en el cálculo se determina para cual aparato está determinado un primer mensaje correspondiente;

- por ejemplo una etapa de procedimiento para la conversión del contenido del mensaje del correspondiente primer mensaje, a un formato de datos para el aparato asignado;

- por ejemplo una etapa de procedimiento para la transmisión del contenido convertido del mensaje, al aparato que está asignado al correspondiente primer mensaje.

En otra forma de realización del procedimiento, el procedimiento comprende otras etapas de procedimiento para realizar los rasgos funcionales u otros rasgos del dispositivo receptor o sus formas de realización.

De acuerdo con otro aspecto, la invención se refiere a un procedimiento para el envío computarizado de mensajes, con las siguientes etapas de procedimiento:

- por ejemplo una etapa de procedimiento para la recepción de (otros) primeros mensajes de aparatos, por medio de una interfaz de comunicación;

- por ejemplo una etapa de procedimiento para el cálculo de una asignación, mediante el respectivo contenido de mensajes de los (otros) primeros mensajes, en el que se calcula cuál aparato ha enviado un correspondiente primer otro mensaje;

- por ejemplo una etapa de procedimiento para la conversión del contenido de mensajes del correspondiente primer (otro) mensaje, a un formato de datos para el sistema distribuido de base de datos;

- por ejemplo una etapa de procedimiento para la transmisión del contenido convertido del mensaje, al sistema distribuido de base de datos.

En otras formas de realización del procedimiento, el procedimiento comprende otras etapas de procedimiento, para realizar los rasgos funcionales u otros rasgos del dispositivo de envío o sus formas de realización.

Además, se reivindica un producto de programa de computador con comandos de programa, para la ejecución de las mencionadas etapas de acuerdo con la invención, en la que por medio del producto de programa de computador en cada caso es ejecutable uno de los procedimientos de acuerdo con la invención, todos los procedimientos de acuerdo con la invención o una combinación de los procedimientos de acuerdo con la invención.

Adicionalmente, se reivindica una variante del producto de programa de computador con comandos de programa, para la configuración de un aparato de creación, por ejemplo una impresora en tres dimensiones, un sistema de computador o una máquina de producción adecuada para la creación de procesadores y/o aparatos, en los que el

aparato de creación está configurado con los comandos de programa, de modo que se crean los mencionados dispositivo de envío y/o dispositivo receptor de acuerdo con la invención.

Además, se reivindica un dispositivo de preparación para el almacenamiento y/o preparación del producto de programa de computador. El dispositivo de preparación es por ejemplo un vehículo de datos que alimenta y/o prepara el producto de programa de computador. De modo alternativo y/o adicional, el dispositivo de preparación es por ejemplo un servicio de red, un sistema de computador, un sistema de servidor, en particular un sistema distribuido de computador, un sistema de cálculo basado en la nube y/o sistema virtual de cálculo, que alimenta y/o prepara el producto de programa de computador, preferiblemente en forma de una corriente de datos.

La preparación ocurre por ejemplo como descarga en forma de un bloque de datos de programa y/o bloque de datos de comando, preferiblemente como datos, en particular como datos de descarga o como corriente de datos, en particular como corriente de datos de descarga, del producto completo de programa de computador. Esta preparación puede ocurrir por ejemplo sin embargo como descarga parcial, que consiste en varias partes y en particular es descargada mediante una red par a par o es preparada como corriente de datos. Un producto de programa de computador así es leído en un sistema, por ejemplo, usando un dispositivo de suministro en forma del vehículo de datos y ejecuta los comandos de programa, de modo que el procedimiento de acuerdo con la invención es puesto en ejecución en un computador, o el aparato de creación es configurado de modo que crea el dispositivo de envío y/o el dispositivo receptor de acuerdo con la invención.

Las propiedades, rasgos y ventajas de esta invención descritos anteriormente, así como el modo y forma en que son alcanzados, son más claros y más evidentes en relación con la siguiente descripción de los ejemplos de realización, que se ilustran en más detalle en relación con las figuras. al respecto, muestran en representación esquemática:

Fig. 1 un primer ejemplo de realización de la invención;

Fig. 2 otro ejemplo de realización de la invención;

Fig. 3 otro ejemplo de realización de la invención;

Fig. 4 otro ejemplo de realización de la invención; y

Fig. 5 otro ejemplo de realización de la invención.

En tanto no se indique de otro modo, en las figuras se da a elementos con la misma función, los mismos signos de referencia.

Los siguientes ejemplos de realización exhiben, en tanto no se indique de otro modo o ya se haya indicado, al menos un procesador y/o una unidad de almacenamiento, para implementar o ejecutar el procedimiento.

También en particular un experto (relevante) en el conocimiento de la/las reivindicación del procedimiento/reivindicaciones del procedimiento, conoce evidentemente todas las posibilidades factibles en el estado de la técnica para la realización de productos o posibilidades para la implementación, de modo que no es necesaria en particular una divulgación independiente en la descripción. En particular pueden realizarse estas variantes de ejecución convencionales y conocidas por los expertos, exclusivamente por (componentes de) hardware o exclusivamente por (componentes de) software. De modo alternativo y/o adicional el experto puede, en el marco de su habilidad profesional, elegir de la manera más amplia cualesquier combinaciones de acuerdo con la invención, de (componentes de) hardware y (componentes de) software, para implementar variantes de ejecución de acuerdo con la invención.

Una combinación de acuerdo con la invención de (componentes de) hardware y (componentes de) software puede ocurrir entonces en particular cuando una parte de los efectos de acuerdo con la invención es causada preferiblemente exclusivamente por hardware especial (por ejemplo un procesador en forma de un ASIC o FPGA) y/u y otra parte por el software (procesador y/o memoria protegidos).

En particular, considerando el elevado número de diferentes posibilidades de realización, es imposible y también para el entendimiento de la invención no es productivo o necesario, nombrar todas estas posibilidades de realización. En tanto en particular todos los siguientes ejemplos de realización debieran mostrar algunas rutas solamente a modo de ejemplo, como en particular tales realizaciones podrían parecer la enseñanza de acuerdo con la invención.

En consecuencia, en particular los rasgos de los ejemplos individuales de realización no se limitan al respectivo ejemplo de realización, sino que se refieren en particular a la invención en general. De modo correspondiente, preferiblemente rasgos de un ejemplo de realización pueden servir también como rasgos de otro ejemplo de realización, en particular sin que esto tenga que ser mencionado de manera explícita en el respectivo ejemplo de

realización.

La Fig. 1 muestra un primer ejemplo de realización de la invención. La Fig. 1 muestra al respecto un sistema SYS que comprende un dispositivo S de envío y un dispositivo E receptor. Adicionalmente, la Fig. 1 muestra una red AN de automatización con un primer aparato D1, un segundo aparato D2 y un tercer aparato D3. Los aparatos (D1, D2, D3) de la red de automatización (que puede ser denominada también como red de automatización) están unidos en comunicación mutua mediante una segunda red NW2 (por ejemplo una red de comunicación como el internet o una red Ethernet).

Además, la Fig. 1 muestra bloques B, por ejemplo un primer bloque B1, un segundo bloque B2 y un tercer bloque B3, una cadena de BC, en la que en este caso en particular se muestra como ejemplar un corte de la cadena BC de bloque.

Los bloques B comprenden en cada caso varias transacciones T. Las transacciones T pueden al respecto comprender transacciones de control y/o transacciones de confirmación.

El primer bloque B1 comprende por ejemplo una primera transacción T1a, una segunda transacción T1b, una tercera transacción T1c y una cuarta transacción T1d.

El segundo bloque B2 comprende por ejemplo una quinta transacción T2a, una sexta transacción T2b, una séptima transacción T2c y una octava transacción T2d.

El tercer bloque B3 comprende por ejemplo una novena transacción T3a, una décima transacción T3b, una decimoprimera transacción T3c y una decimosegunda T3d.

Los bloques B comprenden en cada caso adicionalmente aun una de las sumas CRC de verificación de encadenamiento, que se forman en función del bloque precedente directo. Con ello, el primer bloque B1 comprende una primera suma CRC1 de verificación de encadenamiento de su bloque precedente, el segundo bloque B2 una segunda suma CRC2 de verificación de encadenamiento del primer bloque B1, y el tercer bloque B3 una tercera suma CRC3 de verificación de encadenamiento del segundo bloque B2.

La respectiva suma CRC1, CRC2, CRC3 de verificación de encadenamiento se forma preferiblemente sobre el encabezado de bloque del correspondiente bloque precedente. Las sumas CRC de verificación de encadenamiento pueden formarse preferiblemente usando una función de resumen criptográfico como por ejemplo SHA-256, KECCAK-256 o SHA-3. Por ejemplo, la suma de verificación de encadenamiento puede ser calculada adicionalmente sobre la suma de verificación de bloque de datos o el encabezado comprende la suma de verificación de bloque de datos (la suma de verificación de bloque de datos es aclarada a continuación).

Adicionalmente, cada uno de los bloques puede comprender una suma de verificación de bloque de datos. Esta puede ser realizada por ejemplo por medio de un árbol de resumen criptográfico.

Para formar el árbol de resumen criptográfico, para cada transacción de un (bloque de) datos se calcula una suma de verificación de transacciones (por ejemplo así mismo un valor de resumen criptográfico). De modo alternativo o adicional, puede usarse nuevamente una suma de verificación de transacciones, que fue creada por el generador de la transacción, preferiblemente en la generación de la transacción.

Usualmente se usa un árbol de resumen criptográfico, por ejemplo un árbol de Merkle o árbol de Patricia, cuya suma de verificación de raíz-valor de resumen criptográfico/raíz es depositada preferiblemente como la correspondiente suma de verificación de bloque de datos en los respectivos bloques.

En una variante, la suma de verificación de bloque de datos es usada como suma de verificación de encadenamiento.

Un bloque puede exhibir además una marca de fecha, una firma digital, una detección de prueba de trabajo, así como se aclara en las formas de realización de la invención.

La cadena BC de bloque en sí misma es realizada mediante una infraestructura de cadenas de bloque con varios nodos BCN de cadena de bloque. Los nodos pueden ser por ejemplo cuchilla de cadena de bloque o nodos confiables o un sistema SYS. Los nodos están unidos en comunicación mutua mediante una primera red NW1 (por ejemplo una red de comunicación como el Internet o una red de Ethernet). Por medio de la infraestructura de cadena de bloques se replican por ejemplo al menos una parte de los bloques B de datos o todos los bloques B de datos de la cadena BC de bloque, para una parte o todos los nodos de la cadena de bloque.

Mediante el sistema SYS se une la red AN de automatización con el sistema distribuido de base de datos. Para ello, el sistema SYS comprende, aparte del dispositivo S de envío y el dispositivo E receptor, una primera interfaz NI1 de

comunicación, que está unida con la primera red NW1 y con ello se realiza una unión de comunicación con el sistema distribuido de base de datos. Además, el sistema SYS comprende una segunda interfaz NI2 de comunicación, que está unida con la segunda red NW2 y con ello realiza una unión de comunicación con la red AN de automatización.

El dispositivo E receptor está unido en comunicación mediante un primer bus BE1 con la primer interfaz NI1 de comunicación y unido en comunicación mediante un segundo bus BE2 con la segunda interfaz NI2 de comunicación.

El dispositivo S de envío está unido en comunicación mediante un tercer bus BS1 con la segunda interfaz NI2 de comunicación y unido en comunicación mediante un cuarto bus BS2 con la primera interfaz NI1 de comunicación.

Preferiblemente el sistema SYS o el dispositivo S de envío y/o el dispositivo E receptor previene una comunicación directa entre la red AN de automatización y el sistema distribuido de base de datos (realizada por ejemplo como cadena BC de bloque). Esto es ventajoso puesto que la red AN de automatización con los aparatos (D1, D2, D3) pueden ser un sistema antiguo, cuya operación puede ser por ejemplo perturbada, cuando se transmiten los mensajes del sistema distribuido de base de datos directamente a la red de automatización. Por ello pueden ocurrir problemas por ejemplo respecto al ancho de banda, de modo que se limita o perturba la comunicación entre los aparatos (D1-D3) debido por ejemplo a una elevada carga de la red (que puede ser generada por los mensajes del sistema distribuido de base de datos) de la segunda red NW2. Adicionalmente, puede perturbarse la operación del aparato por ejemplo, dado que el aparato recibe mensajes que están presentes en un formato de datos que no son procesables para él o no van a ser procesados.

La Fig. 2 y la Fig. 3 aclara de manera detallada el modo de función del dispositivo S de envío (Fig. 3) y del dispositivo E receptor (Fig. 2).

Dependiendo de la variante de implementación, el sistema SYS puede comprender también el dispositivo S de envío o el dispositivo E receptor. Si el sistema SYS debiera comprender el dispositivo S de envío (por consiguiente sin el dispositivo E receptor, al respecto entonces el dispositivo S de envío corresponde al sistema SYS), un sistema tal es ventajoso para el efecto de permitir por ejemplo (sólo) un envío de los mensajes del aparato. Este puede ser el caso cuando el aparato envía por ejemplo informaciones de estado o envía comandos de control, pero no debería/tiene que procesar informaciones del sistema distribuido de base de datos. Si el sistema SYS debiera comprender por ejemplo un dispositivo E receptor (sin el dispositivo S de envío, al respecto el dispositivo E receptor corresponde al sistema SYS), entonces esto puede ser ventajoso cuando el aparato (D1-D3) por ejemplo debiera recibir solamente datos y trabajar estos sin retornar/transmitir de vuelta al respecto mensajes al sistema distribuido de base de datos. Por ejemplo, en un sistema tal podrían transmitirse mediante otro canal de comunicación informaciones sobre el estado del procesamiento de mensajes por el aparato (por ejemplo mediante sensores que están unidos mediante una tercera red de comunicación o mediante la primera red de comunicación, con el sistema distribuido de base de datos).

El dispositivo E receptor comprende una primera interfaz 210 de comunicación (por ejemplo una interfaz de red con una red Ethernet), un módulo 220 de identificación, un módulo 230 de conversión y una segunda interfaz 240 de comunicación (por ejemplo una interfaz de red con una red Ethernet), que están unidos en comunicación mutua mediante un bus 201.

El dispositivo E receptor está unido en comunicación mediante un primer bus BE1 con la primera interfaz NI1 de comunicación y está unido en comunicación mediante un segundo bus BE2 con la segunda interfaz NI2 de comunicación.

La primera interfaz 210 de comunicación está configurada para comunicarse con un sistema distribuido de base de datos y está unida con el primer bus BE1. Con ello, la primera interfaz 210 de comunicación está unida en comunicación mediante el primer bus BE1 con la primera interfaz NI1 de comunicación del sistema SYS. Además, la primera interfaz de comunicación está configurada para recibir primeros mensajes (por ejemplo la primera transacción T1a y/u otras transacciones del primer bloque B1) del sistema distribuido de base de datos. Los primeros mensajes son almacenados por ejemplo en un formato de datos (por ejemplo un formato XML de datos) del sistema distribuido de base de datos.

El módulo de identificación está configurado para calcular, mediante el respectivo contenido del mensaje del primer mensaje, una asignación respecto a cuál aparato está designado a un correspondiente primer mensaje TE. Por ejemplo un correspondiente contenido de mensaje puede comprender una firma digital, un certificado digital, una dirección del aparato (por ejemplo una dirección de red), una determinada tarea técnica, un identificador inequívoco (por ejemplo un UID) o una combinación de ellos, mediante los cuales puede ser designado el aparato o los aparatos. Por ejemplo el mensaje o el contenido del mensaje puede comprender una información relacionada con que el aparato debería satisfacer una tarea tecnológica determinada. el módulo 220 de identificación identifica luego cuál aparato es adecuado para satisfacer esa tarea. Por ejemplo, el objetivo puede ser que una planta generadora

de reserva, dentro de un tiempo preestablecido (por ejemplo 4 horas) por un periodo preestablecido (por ejemplo 24 horas) debiera generar una potencia preestablecida (por ejemplo 500 MW). el módulo 220 de identificación designa luego el aparato que es necesario para la ejecución de una tarea tal. Por ejemplo el primer aparato D1 puede ser una turbina a gas con 200 MW de potencia, el segundo aparato puede ser una turbina a gas con 200 MW de potencia y el tercer aparato puede ser una turbina a gas con 200 MW de potencia. si la red de automatización o el aparato están en capacidad de ejecutar la tarea, se envía al sistema distribuido de base de datos un correspondiente mensaje de confirmación. si la red de automatización o el aparato no están en capacidad de realizar la tarea, se envía al sistema distribuido de base de datos un correspondiente mensaje de rechazo para la tarea.

El módulo 230 de conversión está configurado para convertir el contenido del mensaje del correspondiente primer mensaje TE en un formato de datos para el aparato asignado (por ejemplo el primer aparato D1). En particular los aparatos antiguos (denominados aparatos de legado) no están en capacidad de procesar los datos de comunicación de un sistema distribuido de base de datos o una cadena de bloque. De modo correspondiente, mediante el aparato asignado se verifica cuales datos del contenido del mensaje en cualquier caso pueden ser procesados por el aparato y se confirma mediante el aparato asignado, cómo pueden convertirse estos datos para un aparato correspondiente. Por ejemplo, en el caso de la tarea técnica mencionada anteriormente (control de la planta generadora de reserva), que está almacenada en el mensaje, puede convertirse en comandos concretos de control para los aparatos o generadores. Los comandos de control son determinados de manera correspondiente por los requerimientos de la tarea. Por ejemplo, los primeros dos aparatos o turbinas a gas pueden ser usados u operados con potencia completa y la tercera turbina a gas sólo con la mitad de la potencia, para generar los 500 MW de potencia requerida. Al respecto, el formato de datos es por ejemplo un formato de datos de propietario del aparato.

La segunda interfaz 240 de comunicación está configurada para transferir el contenido convertido de mensajes al aparato, que está asignado al correspondiente primer mensaje. De modo correspondiente, la segunda interfaz 240 de comunicación está unida con el segundo bus BE2 y está mediante éste en unión con comunicación con la segunda interfaz NI2 de comunicación del sistema SYS. El correspondiente contenido de mensaje que es transferido al correspondiente aparato o los correspondientes aparatos, puede ser transferido a los aparatos/al aparato por ejemplo en forma de un segundo mensaje NE.

En una variante, el módulo 230 de conversión es en particular un módulo opcional. Este es el caso por ejemplo, cuando el contenido del mensaje del correspondiente primer mensaje no tiene que ser convertido o el contenido del mensaje o el correspondiente primer mensaje exhibe un formato de datos que puede ser procesado por los aparatos. En un caso así, en la transferencia al aparato o los aparatos, el contenido convertido de mensajes corresponde al contenido (no convertido) de mensajes del correspondiente primer mensaje. En consecuencia, por ejemplo se envía el correspondiente primer mensaje como segundo mensaje al aparato o los correspondientes aparatos. En consecuencia, en particular para otras formas de realización dado el caso del dispositivo receptor, el contenido del mensaje del correspondiente primer mensaje corresponde al contenido convertido de mensajes.

En esta variante, el dispositivo receptor puede comprender los siguientes rasgos:

- por ejemplo una primera interfaz de comunicación, en la que

- por ejemplo la primera interfaz de red está configurada para comunicar con un sistema distribuido de base de datos,

- por ejemplo la primera interfaz de comunicación está configurada para recibir primeros mensajes del sistema distribuido de base de datos;

- por ejemplo un módulo de identificación, en el que

- por ejemplo el módulo de identificación está configurado para calcular, mediante el uso del respectivo contenido del mensaje del primer mensaje, una asignación respecto a cuál aparato está designado para un correspondiente primer mensaje;

- por ejemplo una segunda interfaz de comunicación, en la que

- por ejemplo la segunda interfaz de comunicación está configurada para transferir el contenido convertido de mensajes y/o el contenido del mensaje del correspondiente primer mensaje (y/o el primer mensaje en sí mismo) al aparato, que está asignado al correspondiente primer mensaje.

En una variante, el dispositivo E receptor recupera un estado de aparato del aparato (por ejemplo aparato D1) asignado a un correspondiente primer mensaje TE. Al respecto, una transferencia al aparato asignado depende del estado recuperado del aparato.

También, por ejemplo con el estado del aparato puede recuperarse un registro de datos mediante los recursos

disponibles del aparato y/o propiedades actuales del aparato.

En particular para aparatos antiguos, es razonable verificar si los aparatos, en cualquier caso están en capacidad de procesar los mensajes correspondientes.

Si por ejemplo la segunda turbina (segundo aparato) tiene, debido a desgaste o un defecto técnico, actualmente una potencia reducida, esto puede ser considerado por ejemplo en la designación del aparato y también ser considerado en la conversión o creación de comandos de control para el arranque o conducción de las turbinas a gas. De modo correspondiente por ejemplo el primer y tercer aparatos pueden ser usados o iniciados a potencia total y el segundo aparato puede ser usado de manera correspondiente con la mitad de la potencia.

En otras palabras, la transferencia al correspondiente aparato o aparatos ocurre cuando el aparato asignado satisface requerimientos preestablecidos del correspondiente primer mensaje TE, en lo cual por ejemplo mediante el estado del aparato se verifica la satisfacción de los requisitos establecidos. Al respecto, la tarea técnica puede ser establecida por ejemplo por los requerimientos establecidos previamente. Al respecto, los requerimientos establecidos previamente pueden ser almacenados en un correspondiente registro de datos del correspondiente primer mensaje TE. Los requerimientos preestablecidos pueden comprender por ejemplo un requerimiento para el suministro de 500 MW por 24 h en una fecha preestablecida (por ejemplo 9 de julio de 2018 a las 14:43 horas) en un sitio o región preestablecidos (por ejemplo Múnich o Baviera o Alemania). Los requerimientos preestablecidos pueden comprender por ejemplo instrucciones de fabricación u objetivos de fabricación, para manufacturar por ejemplo un engranaje o parte de un engranaje en una fecha preestablecida (por ejemplo 9 de julio de 2018 a las 14:43 horas), en un sitio o región preestablecidos (por ejemplo Múnich o Baviera o Alemania), dentro de un intervalo de tiempo preestablecido (iniciando en la fecha preestablecida), con una precisión preestablecida (por ejemplo desviación de los datos de CAD de máximo). De modo correspondiente, los requerimientos preestablecidos pueden comprender los ejemplos mencionados o una combinación de los ejemplos mencionados.

Los requerimientos establecidos previamente pueden ser por ejemplo comandos de control requeridos, o comprenderlos. Los requerimientos preestablecidos especifican al respecto por ejemplo que los comandos de control requeridos por ejemplo por un aparato o el aparato correspondiente ya deberían haberse implementado, antes de la transmisión de los correspondientes mensajes o contenido del mensaje (por ejemplo el contenido convertido de mensajes), al aparato. de modo alternativo o adicional, los comandos de control requeridos pueden referirse también a otros aparatos, en el que los otros aparatos son por ejemplo aparatos de otra red de automatización. Por ejemplo se necesita que de la otra red de automatización (por ejemplo una red de distribución para combustible), se suministre al menos una cantidad preestablecida de combustible para los generadores, antes de que se transfieran a los aparatos (por ejemplo turbinas, turbinas a gas) los correspondientes mensajes con comandos de control. Para verificar por ejemplo si los comandos de control requeridos ya fueron implementados, pueden leerse o verificarse por ejemplo mensajes o transacciones correspondientes en el sistema distribuido de base de datos, que confirman por ejemplo una ejecución de los comandos de control requeridos. Estos mensajes o transacciones correspondientes pueden ser denominados por ejemplo como transacciones de confirmación y son almacenados por los aparatos correspondientes por ejemplo después de una ejecución de los comandos de control requeridos, por ejemplo por medio del dispositivo S de envío, en el sistema distribuido de base de datos. Estas transacciones de confirmación pueden comprender por ejemplo informaciones sobre la realización de los comandos de control requeridos (por ejemplo lugar, momento y duración de la realización de los comandos de control requeridos), propiedades de los aparatos (por ejemplo cuales aparatos han implementado los comandos de control requeridos), estado de los aparatos (por ejemplo estaba el aparato en un estado regular de operación, estaba en un estado de espera).

Los comandos de control adelantados son ventajosos al efecto también cuando la red AN de automatización y los aparatos son una instalación de fabricación (por ejemplo los aparatos son máquinas de fabricación). Por ejemplo con los comandos de control requeridos puede asegurarse también que una pieza de trabajo que va a ser manufacturada se encuentra en un estado (de fabricación), con ello los comandos de control del contenido (convertido) de mensajes que van ser transferidos pueden ser correctamente implementados para otro procesamiento de la pieza de trabajo. Por ejemplo en los comandos de control requeridos se especifica que una pieza de trabajo sea procesada primero en un torno (por ejemplo el primer aparato D1) y para el otro procesamiento sea colocada en una posición preestablecida. El contenido (actual, convertido) de mensajes con comandos de control, el cual debería ser transmitido, está determinado por ejemplo para una máquina pulidora (por ejemplo que segundo aparato D2) (por consiguiente debería transmitirse a éste), que la pieza de trabajo correspondiente sea ubicada en la posición preestablecida, y pulida.

Los comandos de control adelantados son ventajosos para el efecto cuando la red AN de automatización y los aparatos por ejemplo dispensadores de efectivo o cajeros automáticos de banco entrelazados. Por ejemplo con los comandos de control requeridos puede asegurarse también que ocurre un desembolso de dinero por un dispensador de efectivo (por ejemplo por el aparato D1) cuando previamente se ejecutó de manera exitosa una autenticación del

cliente del banco y se almacenó una confirmación para ello en correspondientes transacciones de confirmación del sistema distribuido de base de datos.

Por ejemplo en los comandos de control requeridos (por consiguiente los requisitos preestablecidos) se especifica que por ejemplo tiene que ocurrir de manera exitosa una autenticación del usuario o autenticación del usuario, por medio de un procedimiento preestablecido de autenticación (por ejemplo autenticación de dos factores, ingreso de Pin), antes de permitir o ejecutar por ejemplo el desembolso del dinero. El dispositivo E receptor (por ejemplo por medio de la segunda interfaz 240 de comunicación) transmite justo entonces el correspondiente contenido (convertido) de mensajes (del primer mensaje correspondiente con comandos de control al aparato (por ejemplo al cajero automático), cuando por ejemplo en el sistema distribuido de base de datos existe una transacción de confirmación, que confirma por ejemplo una autenticación exitosa del usuario. Con los comandos de control se configura luego por ejemplo el dispensador de dinero, que suministra la cantidad de dinero requerida por el usuario o cliente del banco y a continuación abre la aleta para el retiro del dinero.

En particular en estas variantes, también el dispositivo S de envío está formado para el efecto de transmitir al sistema distribuido de base de datos los mensajes o transacciones de confirmación correspondientes, dado el caso para los comandos de control requeridos, o almacenar en el sistema distribuido de base de datos, cuando los aparatos han ejecutado exitosamente el comando o los comandos de control requerido(s) correspondiente(s). Si la ejecución por ejemplo no fue exitosa, entonces estos pueden ser almacenados en el sistema distribuido de base de datos, también en transacciones de confirmación o correspondientes mensajes.

El dispositivo S de envío comprende una primera interfaz 310 de comunicación (por ejemplo una interfaz de red con una red Ethernet), un módulo 320 de identificación, un módulo 330 de conversión y una segunda interfaz 340 de comunicación (por ejemplo una interfaz de red con una red Ethernet), que están unidos en comunicación mutua mediante un bus 301.

La primera interfaz 310 de comunicación está configurada para comunicarse con los aparatos. La primera interfaz 310 de comunicación está unida con el tercer bus BS1 y está con ello unida con comunicación con la segunda interfaz NI2 de comunicación del sistema SYS. Además, la primera interfaz de comunicación está configurada para recibir primeros mensajes de los aparatos. Al respecto, los primeros mensajes son almacenados por ejemplo en un formato de datos de propietario de los aparatos.

El módulo 320 de identificación está configurado para calcular, mediante el respectivo contenido del mensaje de los primeros mensajes, una asignación respecto a cuál aparato ha enviado un correspondiente primer mensaje NS.

Por ejemplo, un correspondiente contenido del mensaje puede comprender una firma digital, un certificado digital, una dirección de aparatos (por ejemplo una dirección de red), un estado de aparatos (por ejemplo un estado de aparato) o un identificador inequívoco (por ejemplo un UID), mediante los cuales pueden designarse los correspondientes aparato o aparatos. Por ejemplo, el mensaje o el contenido del mensaje puede comprender un estado de aparato, respecto al grado en que se satisfizo la tarea técnica, por los aparatos o la red de automatización.

Volviendo al ejemplo mencionado anteriormente con las turbinas a gas: podría ser por ejemplo que en suma los aparatos no generen la potencia necesaria. Por ejemplo, la potencia generada puede ser en suma de sólo 300 MW. También pueden haberse enviado en cada caso mensajes individuales a través de los aparatos, por ejemplo respecto al grado o a la extensión en que en cada caso ellos han satisfecho la tarea técnica (por ejemplo primer aparato 50 MW, segundo aparato 100 MW, tercer aparato 150 MW de potencia generada). El dispositivo S de envío u otro aparato (por ejemplo que ha enviado el mensaje al dispositivo S de envío) de la red AN de automatización calculan entonces la extensión en que se satisface la tarea técnica. La parte faltante de la potencia puede ser enviada por ejemplo nuevamente como mensaje sobre el sistema distribuido de base de datos, a otra red de automatización de una planta generadora a carbón o una instalación generadora eólica como segundo mensaje TS. Estas pueden generar entonces por ejemplo el déficit de potencia en la generación de energía. El segundo mensaje TS es almacenado entonces por ejemplo en transacciones (por ejemplo la decimosegunda transacción T3d) del sistema distribuido de base de datos, o el segundo mensaje (por ejemplo la decimosegunda transacción T3d) es ya una transacción almacenada en el sistema distribuido de base de datos, una vez aquella fue enviada o transmitida exitosamente.

El módulo 330 de conversión está configurado para convertir el contenido del mensaje del correspondiente primer mensaje NS en un formato de datos para el sistema distribuido de base de datos. Por ejemplo el contenido del mensaje del correspondiente primer mensaje puede ser convertido en un formato universal de datos (por ejemplo XML o correspondiente a un esquema XML), que es compatible con el sistema distribuido de base de datos o es un formato de datos, que puede procesar el sistema distribuido de base de datos.

En una variante, el módulo 330 de conversión es en particular un módulo opcional. Este es el caso por ejemplo

cuando el contenido de mensaje del correspondiente primer mensaje no tiene que ser convertido o el contenido del mensaje o el correspondiente primer mensaje exhibe un formato de datos que puede ser procesado por el sistema distribuido de base de datos. En un caso así, el contenido convertido del mensaje en la transferencia al sistema distribuido de base de datos corresponde al contenido (no convertido) del mensaje del respectivo primer mensaje. En consecuencia por ejemplo el respectivo primer mensaje es enviado como segundo mensaje al sistema distribuido de base de datos. En consecuencia, en particular para respectivas formas de realización del dispositivo de envío, dado el caso el contenido del mensaje del correspondiente primer mensaje corresponde al contenido convertido del mensaje.

En esta variante, el dispositivo de envío puede comprender los siguientes rasgos:

- por ejemplo una primera interfaz de comunicación, en la que

- por ejemplo la primera interfaz de comunicación está configurada para comunicarse con aparatos,

- por ejemplo la interfaz de comunicación está configurada para recibir primeros mensajes de los aparatos;

- por ejemplo un módulo de identificación, en el que

- por ejemplo el módulo de identificación está configurado para calcular, mediante el respectivo contenido de mensaje del primer mensaje, una asignación respecto a cuál aparato ha enviado un correspondiente primer mensaje;

- por ejemplo una segunda interfaz de comunicación, en la que

- por ejemplo la segunda interfaz de comunicación está configurada para comunicarse con un sistema distribuido de base de datos,

- por ejemplo la interfaz de comunicación está configurada para transmitir el contenido convertido del mensaje y/o el contenido de mensaje del correspondiente primer mensaje (y/o el primer mensaje en sí mismo) al sistema distribuido de base de datos.

La segunda interfaz 340 de comunicación está configurada para transmitir el contenido convertido del mensaje al sistema distribuido de base de datos. De modo correspondiente, la segunda interfaz 340 de comunicación está unida con el cuarto bus BS2 y está unida en comunicación mediante éste con la segunda interfaz NI2 de comunicación del sistema SYS. El contenido correspondiente del mensaje, que es transmitido al sistema distribuido de base de datos, puede ser transmitido por ejemplo forma de un segundo mensaje TE a los aparatos/el aparato. El segundo mensaje TE puede ser al respecto por ejemplo una transacción del sistema distribuido de base de datos, en el que el segundo mensaje comprende/almacena el contenido convertido del mensaje.

El dispositivo S de envío y el dispositivo E receptor pueden comprender en diferentes variantes en cada caso un módulo de criptografía independiente. Esto es ventajoso para elevar la seguridad, puesto que si por ejemplo se obtuviera un acceso no autorizado a los datos criptográficos de uno de los módulos de criptografía, este atacante recibe acceso no automático a los otros datos criptográficos de los otros módulos de criptografía. De modo alternativo, el dispositivo S de envío y el dispositivo E receptor pueden usar un módulo conjunto de criptografía. Esto es ventajoso para mantener bajos los costes de producción de los módulos individuales. En el caso de un módulo conjunto de criptografía, los correspondientes datos criptográficos del dispositivo S de envío y/o el dispositivo E receptor pueden ser usados conjuntamente. El módulo de criptografía es protegido de un acceso de atacantes preferiblemente mediante un módulo de protección de manipulación (por ejemplo mecanismos contra la adulteración/mecanismos de protección contra la manipulación). Por ejemplo el módulo de criptografía puede comprender un dispositivo de protección mecánico y/o uno eléctrico y/o electrónico y/o electromecánico. Esto puede ser realizado por ejemplo mediante almacenamiento en el módulo de criptografía de los datos criptográficos para los aparatos, en un módulo de almacenamiento o memoria protegidos (por ejemplo una memoria con clave), sobre cuyos datos (sólo) puede acceder el módulo de criptografía. de modo correspondiente, esta memoria y/o el módulo de criptografía están protegidos por una carcasa de acero (dispositivo mecánico de protección), que por ejemplo previene el acceso de un atacante. de modo alternativo o adicional, el módulo de criptografía o la memoria pueden ser protegidos mediante una lámina con protección contra la perforación. Una vez alguien intenta acceder a la memoria de manera no autorizada o mediante una interfaz no permitida, por ejemplo se eliminan los datos criptográficos.

El módulo de criptografía comprende por ejemplo datos criptográficos específicos para los aparatos (datos criptográficos específicos para los aparatos).

Los datos criptográficos pueden ser por ejemplo una o varias llaves criptográficas, que son calculadas de manera específica para un aparato respectivo. Las llaves criptográficas pueden ser por ejemplo llaves criptográficas

simétricas o ser llaves criptográficas asimétricas (por ejemplo un par de llaves pública/privada).

Estos datos criptográficos pueden ser almacenados, por ejemplo, de manera duradera en el o a través del módulo de criptografía.

De manera alternativa, los datos criptográficos pueden ser borrados del módulo de criptografía después de un tiempo preestablecido (por ejemplo cuando un aparato correspondiente no ha comunicado datos/mensajes por algunas horas). Si el aparato correspondiente se comunica nuevamente más tarde, puede calcularse nuevamente la llave criptográfica necesaria. De modo correspondiente, los datos criptográficos pueden ser calculados de manera reproducible para un aparato respectivo o ser calculados nuevamente. Para ello pueden usarse por ejemplo datos inequívocos específicos de aparato del correspondiente aparato. Son datos inequívocos específicos de aparato por ejemplo un UID del aparato, un identificador inequívoco que fue calculado mediante datos sensores característicos para el aparato - por ejemplo una característica calculada para una señal de ruido, que fue determinada mediante un sensor del aparato. Estos datos inequívocos específicos de aparato pueden ser usados por ejemplo en combinación con un valor secreto de inicio (por ejemplo una semilla), que es almacenado o manejado de manera segura por ejemplo mediante el módulo de criptografía, para calcular nuevamente los datos criptográficos correspondientes. Por ejemplo puede usarse un primer valor secreto de inicio, para calcular los datos criptográficos para el dispositivo de envío y puede usarse un segundo valor secreto de inicio para calcular los datos criptográficos para el dispositivo receptor. Los cálculos mencionados ocurren preferiblemente mediante el módulo de criptografía, de modo que por ejemplo también se protegen los algoritmos usados y datos calculados de manera temporal, ante el acceso de un atacante.

El módulo de criptografía puede luego cargar, calcular o acceder a, los correspondientes datos criptográficos, por ejemplo mediante el aparato asignado.

La carga de los datos criptográficos puede ocurrir por ejemplo también mediante formación, por medio de datos específicos para el aparato y/o con datos específicos para el dispositivo (por ejemplo datos específicos para el dispositivo de envío y/o datos específicos para el dispositivo receptor), primero de otra llave criptográfica, para poder acceder por ejemplo a los datos criptográficos específicos para el aparato de un aparato correspondiente. Los datos criptográficos (específicos de aparato) son al respecto - como ya se mencionó - almacenados preferiblemente por el o en el módulo de criptografía. Por ejemplo se combina un UID de un aparato correspondiente con un valor secreto de inicio del dispositivo S de envío y/o del dispositivo E receptor y/o del sistema SYS, para formar otra llave criptográfica, por ejemplo para descodificar los datos criptográficos. Para formar la otra llave criptográfica pueden ensamblarse por ejemplo los datos hasta una cadena de signos combinada (UID + valor secreto de inicio). De modo alternativo o adicional, la cadena combinada de signos o una parte de la cadena combinada de signos sirve como parámetro de entrada para una función derivada de la llave, en la que puede derivarse de manera reproducible una llave correspondiente, en tanto como parámetro de entrada se use por ejemplo la cadena de signos sustancialmente igual/idéntica.

En el caso del dispositivo S de envío, por ejemplo por medio de los correspondientes datos criptográficos puede protegerse criptográficamente al menos una parte del contenido del mensaje del primer mensaje correspondiente, de modo específico al aparato para el aparato asignado (por consiguiente se genera por ejemplo un protector criptográfico específico para el aparato). Esta protección criptográfica ocurre por ejemplo antes del envío del contenido del mensaje. En el caso de un dispositivo E receptor, mediante los datos criptográficos se verifica y/o se descodifica al menos una parte del contenido de mensaje del correspondiente primer mensaje, para un aparato asignado. Al respecto, por ejemplo, se entiende por una protección criptográfica específica del aparato, que por ejemplo los mensajes (o su contenido de mensaje), que provienen de un aparato correspondiente, son protegidos por medio de los datos criptográficos específicos para el aparato, para hacer verificable preferiblemente una autenticidad de los correspondientes mensajes o el contenido del mensaje.

En el dispositivo S de envío es ventajoso para el efecto, para proteger criptográficamente en particular los mensajes que son enviados al sistema distribuido de base de datos (y/o que son almacenados por este) (o mensajes que fueron enviados por el aparato), verificar criptográficamente por ejemplo de manera análoga al dispositivo receptor. Esto puede ocurrir por ejemplo mediante protección y/o codificación del correspondiente contenido de mensaje, por medio de una suma (criptográfica) de verificación. Para ello, el dispositivo S de envío puede comprender por ejemplo una primera llave criptográfica (por ejemplo esta es específica para el aparato), con la cual se forma por ejemplo una suma de verificación sobre los mensajes o el contenido de los mensajes. De modo alternativo, con esta primera llave criptográfica puede codificarse por ejemplo también el contenido del mensaje. Un receptor del mensaje puede por ejemplo con la primera llave criptográfica (en el caso de un procedimiento criptográfico simétrico) o una segunda llave criptográfica, que está asignada a la primera llave criptográfica (por ejemplo para un procedimiento criptográfico asimétrico en el cual por ejemplo la primera llave es una llave privada y la segunda llave es una llave pública), ejecutar la descodificación o verificación del correspondiente contenido del mensaje. Para ello el correspondiente material de llave del receptor puede por ejemplo haber sido transmitido por un canal seguro.

Los datos criptográficos (por ejemplo las llaves criptográficas), por ejemplo para el dispositivo S de envío, pueden haber sido generados por ejemplo por medio de datos específicos de aparato o datos inequívocamente específicos de aparato, de un aparato correspondiente (por ejemplo un UID del aparato, un número aleatorio que fue generado por el correspondiente aparato, o que fue calculado por medio de datos sensores característicos para el aparato - por ejemplo una característica calculada para una señal de ruido, que fue determinada mediante un sensor del aparato). De modo alternativo o adicional, los datos criptográficos son una combinación de datos específicos (inequívocos) del aparato y datos específicos de dispositivo (por ejemplo un UID del dispositivo de envío, un número aleatorio que fue generado por el dispositivo de envío, o que fue calculado por medio de datos de sensor para el dispositivo S de envío - por ejemplo una característica calculada para una señal de ruido, que fue determinada mediante un sensor del dispositivo de envío).

Al respecto, los datos de sensor pueden ser captados por ejemplo por un sensor, que capta por ejemplo el ruido térmico de un circuito del aparato o puede usarse el ruido del sensor en sí mismo. Puede usarse por ejemplo también el ruido de una interfaz de datos no usada o también de una interfaz de datos usada. Esta puede ser por ejemplo (por ejemplo para el aparato o para el sistema SYS) una interfaz de red de anillo de ficha de un aparato o una interfaz RS232. También puede usarse por ejemplo el ruido de un hardware de adquisición de datos.

Por ejemplo, para el dispositivo S de envío también es posible que por medio de los datos específicos de aparato y/o datos específicos de dispositivo de envío (por ejemplo el valor secreto de inicio) se determinen de manera reproducible los datos criptográficos para el aparato correspondiente o por medio de estos datos se suspenda (por ejemplo se descodifique) una protección criptográfica (por ejemplo una codificación), con la cual se protegen los correspondientes datos criptográficos de un aparato, y/o se verifique (por ejemplo se verifique una firma digital). Los datos específicos de aparato pueden ser almacenados por ejemplo en el mensaje del aparato correspondiente. Los datos específicos de aparato y/o datos específicos de dispositivo de envío son preferiblemente datos que pueden ser falseados sólo difícilmente, por ejemplo una característica de una señal de ruido (por ejemplo se incluye de un sensor o un módulo de protección contra la manipulación). En una manipulación del aparato o del dispositivo (por ejemplo dispositivo de envío o dispositivo receptor) se cambiarían estos datos específicos de aparato y/o datos específicos de dispositivo (de envío), de modo que se modifica por ejemplo la característica de manera que los datos criptográficos se tornan no válidos o ya no puede accederse a éstos.

Por ejemplo por medio de un procedimiento de desafío-respuesta pueden intercambiarse también datos criptográficos o material de clave o datos específicos de aparato o datos inequívocamente específicos de aparato de un aparato correspondiente. Esto puede ocurrir por ejemplo mediante configuración del procedimiento en el lado del aparato y el lado del dispositivo de envío, con valores iniciales correspondientes (por ejemplo configurando previamente valores iniciales correspondientes en una memoria protegida del aparato o del dispositivo de envío o mediante cálculo y/o suministro de estos valores iniciales por la memoria protegida) y/o pueden recuperarse datos específicos de aparato correspondientes (por ejemplo una llave criptográfica o una parte de una llave criptográfica) del dispositivo de envío.

El dispositivo E receptor es ventajoso al efecto con un módulo de criptografía, para verificar criptográficamente en particular los mensajes que deberían ser transmitidos a un aparato correspondiente (o por ejemplo proteger también de manera criptográfica, de forma análoga al dispositivo de envío). Para ello, el creador del mensaje puede haber obtenido por ejemplo una primera llave criptográfica, con la cual se formó por ejemplo una suma de verificación sobre los mensajes o el contenido del mensaje, que fueron recibidos por el dispositivo E receptor. de modo alternativo, con esta primera llave criptográfica puede por ejemplo haberse codificado también el contenido del mensaje. Por ejemplo con la primera llave criptográfica (en el caso de un procedimiento criptográfico simétrico) o una segunda llave criptográfica, que está asignada a la primera llave criptográfica (por ejemplo para un procedimiento criptográfico asimétrico en el cual por ejemplo la primera llave es una llave privada y la segunda llave es una llave pública), puede ocurrir la descodificación o verificación del correspondiente contenido del mensaje.

Los datos criptográficos (por ejemplo la llave criptográfica) del dispositivo E receptor pueden haber sido generados por ejemplo por medio de datos específicos de los aparatos o datos inequívocos específicos de los aparatos, de un aparato correspondiente (por ejemplo un UID del aparato, un número aleatorio que fue generado mediante el aparato correspondiente, o fue calculado mediante el uso de datos de sensor característicos para el aparato - por ejemplo una característica calculada para una señal de ruido, que fue determinada mediante un sensor del aparato).

Los datos de sensor pueden ser captados para el dispositivo E receptor y/o el sistema SYS por ejemplo por un sensor, el cual capta por ejemplo el ruido térmico de un circuito del aparato o se usa el ruido del sensor en sí mismo. Puede usarse también el ruido de una interfaz de datos no usada o también una interfaz de datos usada. Esta puede ser por ejemplo una interfaz de red de anillo de ficha de un aparato o una interfaz RS232. También puede usarse por ejemplo el ruido de un hardware de adquisición de datos.

De modo alternativo o adicional, los datos criptográficos para un dispositivo E receptor son una combinación de

datos específicos de aparato y datos específicos de dispositivo receptor (por ejemplo un UID del dispositivo receptor, un número aleatorio que fue generado por el dispositivo E receptor, o fue calculado mediante el uso de datos de sensor para el dispositivo receptor - por ejemplo una característica calculada para una señal de ruido, que fue determinada por un sensor del dispositivo E receptor). Por ejemplo, también es posible que por medio de los datos específicos de aparato y/o datos específicos de dispositivo receptor para el correspondiente aparato, se determinen de manera reproducible los datos criptográficos. Por ejemplo, mediante estos datos específicos de aparato y/o datos específicos de dispositivo receptor puede suprimirse (por ejemplo descodificarse) una protección criptográfica (por ejemplo una codificación), con la cual se protegen los correspondientes datos criptográficos de un aparato, y/o verificarse (por ejemplo se verifica una firma digital). Para ello puede calcularse, dado el caso mediante estos datos, una llave criptográfica para ejecutar las operaciones criptográficas necesarias para ello.

Los datos específicos de aparato del aparato para el dispositivo E receptor pueden ser recuperados por ejemplo en la recuperación del estado del aparato para un aparato. Los datos específicos de aparato y/o datos específicos de dispositivo receptor son preferiblemente datos que pueden ser falseados sólo difícilmente, por ejemplo un valor secreto de inicio o una característica de una señal de ruido (por ejemplo está incluida de un sensor o un módulo de protección contra la manipulación), que en una manipulación del aparato es modificada de modo que por ejemplo la característica cambia, tal que a su vez los datos criptográficos se tornan no válidos o ya no puede accederse a ellos.

Si por ejemplo se intercambia un aparato por otro aparato manipulado por un atacante, por ejemplo es muy difícil que el aparato manipulado duplique o falsifique la característica de una señal de ruido del aparato original. Se usa ahora por ejemplo la característica de la señal de ruido (del aparato manipulado), para generar una llave criptográfica. Por medio de la llave criptográfica se intenta ahora por ejemplo descodificar los datos criptográficos. Puesto que mediante la característica de la señal de ruido modificada no podría formarse la llave correcta para la descodificación, en consecuencia por ejemplo no es exitosa la descodificación de los datos criptográficos.

Por ejemplo también por medio de un procedimiento de desafío-respuesta pueden determinarse o intercambiarse datos específicos de aparato o datos inequívocos específicos de aparato (por ejemplo en la recuperación de un estado de aparato), en lo cual por ejemplo el procedimiento es configurado en el lado del aparato y en el lado del dispositivo receptor, con valores de inicio correspondientes (por ejemplo en lo cual en una memoria protegida del aparato o el correspondiente dispositivo E receptor, se configuran previamente valores iniciales o estos valores iniciales son calculados y/o suministrados por la memoria protegida) y pueden recuperarse correspondientes datos específicos de aparato (por ejemplo una llave criptográfica o una parte de una llave criptográfica) del dispositivo receptor.

También el dispositivo S de envío y/o el dispositivo E receptor pueden comprender en cada caso un módulo de inicio o usar un módulo conjunto de inicio. Este módulo de inicio está configurado para que por ejemplo en un aparato nuevo, se calculen los datos criptográficos correspondientes, cuando para este aparato debiera recibirse datos por primera vez o enviarse datos por primera vez. Esto puede ser generado por ejemplo mediante el procedimiento mencionado (datos inequívocos específicos de aparato + semilla).

En una variante, el dispositivo S de envío y/o el dispositivo E receptor forman también aparatos virtuales, que exhiben los correspondientes interfaces y rasgos técnicos, para comunicarse con el sistema distribuido de base de datos. Por ejemplo los aparatos virtuales correspondientes pueden ser representados con una configuración preestablecida, en los que la configuración es determinada o calculada sobre el aparato físico, en función de correspondientes informaciones de los aparatos. Al respecto, se entiende por configuración por ejemplo cuáles interfaces y funciones debería suministrar un aparato virtual correspondiente.

Esto puede ocurrir por ejemplo por medio de un ambiente de virtualización como por ejemplo equipamiento VM. Si se comunica sólo un nodo del sistema distribuido de base de datos con un aparato virtual, entonces el dispositivo S de envío y/o el dispositivo E receptor reenvían las informaciones correspondientes al aparato antiguo o aparato legado, en lo cual antes del reenvío ocurren los correspondientes conversión y procesamiento, como se describió anteriormente. esto es en particular ventajoso para máquinas de fabricación, cuando concretamente éstas por ejemplo no están en capacidad de formar cadenas de bloque, pero son controladas por un sistema de control a base de cadenas de bloque. Por ejemplo, el módulo de identificación puede usar para ello los correspondientes aparatos virtuales, o el módulo de identificación es un componente/elemento que es realizado por uno o varios aparatos virtuales. Preferiblemente, los aparatos virtuales se comportan como un nodo del sistema distribuido de base de datos e imitan o completan funciones para el aparato físico, que no tienen estos para una comunicación o un trabajo conjunto con los nodos del sistema distribuido de base de datos.

Un módulo de identificación correspondiente (con aparatos virtuales) para un dispositivo E receptor puede ser realizado por ejemplo como sigue. Al respecto, el módulo de identificación está configurado para calcular, mediante el respectivo contenido de mensaje de los primeros mensajes, a cuál aparato virtual está asignado un primer mensaje correspondiente. Los aparatos virtuales comprenden al respecto por ejemplo el módulo de conversión y/o la

segunda interfaz de comunicación o comprenden en cada caso una variante virtual propia de ésta o acceden al módulo de conversión y/o la segunda interfaz de comunicación, para transferir el mensaje o el contenido del mensaje al aparato físico asignado al correspondiente aparato virtual.

Un dispositivo receptor con aparatos virtuales correspondiente puede exhibir por ejemplo los siguientes rasgos:

- por ejemplo una primera interfaz de comunicación, en la que

- por ejemplo la primera interfaz de red está configurada para comunicarse con un sistema distribuido de base de datos,

- por ejemplo la primera interfaz de comunicación está configurada para recibir primeros mensajes del sistema distribuido de base de datos;

- por ejemplo aparatos virtuales, en los que

- por ejemplo los aparatos virtuales están asignados en cada caso a un correspondiente aparato (físico) (por ejemplo la red AN de automatización),

por ejemplo mediante el respectivo contenido del mensaje (por ejemplo dirección objetivo del correspondiente mensaje) de los primeros mensajes, se calcula una asignación respecto a cuál de los aparatos virtuales está asignado a un primer mensaje correspondiente;

por ejemplo un módulo de conversión, en el que

por ejemplo el módulo de conversión está configurado para convertir el contenido del mensaje del correspondiente primer mensaje, en un formato de datos para el aparato asignado;

por ejemplo una segunda interfaz de comunicación, en la que

por ejemplo la segunda interfaz de comunicación está configurada para transferir el contenido convertido del mensaje y/o el contenido de mensaje del primer mensaje correspondiente (y/o el primer mensaje en sí mismo) al aparato que está asignado por el primer mensaje correspondiente.

Un módulo de identificación correspondiente para un dispositivo S de envío puede ser realizado por ejemplo como sigue. Al respecto, el módulo de identificación está configurado para calcular, mediante el respectivo contenido de mensaje de los primeros mensajes, una asignación, respecto a cuál aparato físico recibiría un mensaje. Mediante esta asignación se determina ahora cuál aparato virtual debería procesar y/o enviar un mensaje correspondiente. Los aparatos virtuales comprenden al respecto el módulo de conversión y/o la segunda interfaz de comunicación o comprenden en cada caso una variante virtual propia de estos, o acceden al módulo de conversión y/o la segunda interfaz de comunicación, para transmitir los mensajes o el contenido de mensaje por medio del correspondiente aparato virtual, al sistema distribuido de base de datos.

Un dispositivo S de envío con los correspondientes aparatos virtuales puede exhibir por ejemplo los siguientes rasgos:

- por ejemplo una primera interfaz de comunicación, en la que

- por ejemplo la primera interfaz de comunicación está configurada para comunicarse con aparatos,

- por ejemplo la interfaz de comunicación está configurada para recibir los primeros mensajes de los aparatos;

- por ejemplo aparatos virtuales, en los que

- por ejemplo al aparato virtual está asignado en cada caso un correspondiente aparato (físico) (por ejemplo una red de automatización),

- por ejemplo mediante el respectivo contenido de mensaje (por ejemplo dirección de red del emisor) de los primeros mensajes, calcular una asignación respecto a cuál aparato ha enviado un primer mensaje correspondiente;

- por ejemplo un módulo de conversión, en el que

por ejemplo el módulo de conversión está configurado para convertir el contenido de mensaje del primer mensaje correspondiente, en un formato de datos para el sistema distribuido de base de datos;

por ejemplo una segunda interfaz de comunicación, en la que

- por ejemplo la segunda interfaz de comunicación está configurada para comunicarse con un sistema distribuido de base de datos,

- por ejemplo la interfaz de comunicación está configurada para transmitir el contenido convertido del mensaje y/o el contenido de mensaje del correspondiente primer mensaje (y/o el primer mensaje en sí mismo), al sistema distribuido de base de datos.

Las variantes mencionadas con los aparatos virtuales pueden evitar por ejemplo también el módulo de conversión, cuando por ejemplo no es necesaria una conversión de datos.

También, las variantes con los aparatos virtuales pueden comprender en cada caso un módulo de criptografía correspondiente, que comprende los datos criptográficos correspondientes para un aparato (físico o virtual) y/o para varios aparatos (físicos y/o virtuales). Para ello, por ejemplo un aparato virtual puede comprender en cada caso un módulo de criptografía correspondiente, o los aparatos virtuales acceden a un módulo de criptografía conjunto.

El dispositivo E receptor puede ser implementado por ejemplo de modo pasivo o activo.

En una implementación activa se envían los primeros mensajes por ejemplo directamente por el sistema distribuido de base de datos, al dispositivo E receptor o al sistema SYS (o los recibe el dispositivo E receptor o el sistema SYS). Al respecto, los mensajes correspondientes pueden comprender por ejemplo una información respecto a cuál aparato de la red AN de automatización está designado al mensaje correspondiente.

En una implementación pasiva los primeros mensajes son recibidos por ejemplo indirectamente por el dispositivo E receptor o el sistema SYS. Para ello, el dispositivo E receptor o el sistema SYS captan o reciben los mensajes de la primera red NW1 por ejemplo con un filtro de paquete o una herramienta de análisis de red (por ejemplo Wireshark) o una herramienta para recuperar paquetes de datos de la red (por ejemplo WinPCap, libpcap). Al respecto, los mensajes correspondientes no están enfocados por ejemplo al dispositivo E receptor (o al sistema SYS) o sus direcciones de red, sino que están enfocados a los aparatos de la red AN de automatización (en lo cual por ejemplo se designa en el mensaje o su contenido un determinado tipo de aparato).

Para establecer si por ejemplo un primer mensaje correspondiente está determinado para un aparato de la red AN de automatización, el dispositivo receptor (o el sistema SYS) comprende por ejemplo un banco de datos de aparatos, que comprende un directorio de los aparatos de la red AN de automatización. Adicionalmente, en este directorio pueden por ejemplo almacenarse también informaciones de aparato sobre los respectivos aparatos. Las informaciones de aparatos pueden comprender por ejemplo informaciones generales respecto a un aparato. Estas pueden comprender por ejemplo rasgos técnicos como potencia, velocidad de fabricación, consumo de energía, precisión de fabricación, ubicación del aparato o una combinación de ellos. De modo alternativo o adicional, las correspondientes informaciones de aparatos pueden comprender también los estados de aparatos recibidos o recuperados recientemente. Si por ejemplo, dentro de un periodo preestablecido de tiempo ya se recibió un estado de aparato, entonces puede evitarse por ejemplo una nueva recuperación de un estado actual el aparato. Si el intervalo preestablecido de tiempo es de 5 minutos y, por ejemplo, antes de 1 minuto se recibió un estado de aparato para el aparato, no es necesario, hasta transcurrido el periodo preestablecido de tiempo, recibir nuevamente un mensaje de estado.

El dispositivo S de envío puede ser implementado por ejemplo de modo pasivo o activo.

Para una implementación activa, se envían los primeros mensajes por ejemplo directamente por el aparato de la red de automatización, al dispositivo S de envío o al sistema SYS. Al respecto, los correspondientes mensajes pueden comprender por ejemplo una información respecto a cuál sistema distribuido de base de datos (en caso de que existan varios de estos sistemas) o red (por ejemplo la primera red de comunicación) está determinada al mensaje correspondiente.

En una implementación pasiva, los primeros mensajes son recibidos por ejemplo indirectamente por el dispositivo S de envío o el sistema SYS. Para ello, el dispositivo S de envío o el sistema SYS captan o reciben los mensajes de la segunda red NW2 por ejemplo con un filtro de paquete o una herramienta de análisis de red (por ejemplo Wireshark) o una herramienta para recuperar paquetes de datos de la red (por ejemplo WinPCap, libpcap). Al respecto, los mensajes correspondientes no están por ejemplo orientados al dispositivo S de envío (o al sistema SYS) o sus direcciones de red, sino que es tan orientados por ejemplo a otra dirección u otro aparato. Por ejemplo una parte de una infraestructura de comunicación originalmente presente puede haber sido reemplazado por el sistema distribuido de base de datos, y los correspondientes aparatos o direcciones de red, a los cuales deberían haberse enviado los correspondientes primeros mensajes, ya no existen. Puesto que los aparatos correspondientes tampoco pueden ya ser reconfigurados sin más, sin el dispositivo S de envío los correspondientes mensajes no estarían disponibles para la nueva infraestructura de comunicación o no podían ser transmitidos a ésta.

También el dispositivo S de envío puede comprender un banco de datos de aparatos (por ejemplo de manera análoga al dispositivo receptor), para establecer por ejemplo cuál aparato ha enviado un mensaje correspondiente. Si por ejemplo los mensajes son recibidos de manera pasiva, puede determinarse una información tal por ejemplo mediante el uso de la dirección de envío del mensaje. Para ello, las informaciones de los aparatos son recuperadas por ejemplo por medio de las direcciones de envío.

La invención es ventajosa para el efecto de permitir la comunicación por ejemplo de aparatos legados, de cuya configuración no se permitirían cambios, con una nueva infraestructura de cadenas de bloque. La conversión de los datos toma el control del dispositivo o el sistema.

También, los dispositivos (por ejemplo el dispositivo de envío o el dispositivo receptor) o el sistema, pueden ejecutar en cada caso contratos inteligentes para los sistemas legados o aparatos. Con ello puede darse a los aparatos en particular la capacidad de formar cadenas de bloque, sin cambiar de ninguna forma estos aparatos.

En particular, estos dispositivos o el sistema comprenden los componentes necesarios para comunicarse con una cadena de bloque. Estos son por ejemplo memorias con clave con claves criptográficas, para firmar transacciones/mensajes para la cadena de bloque o para verificar las sumas de verificación correspondientes.

En una variante de implementación puede implementarse un módulo, pueden implementarse varios módulos o pueden implementarse todos los módulos como componente de software o componente de hardware, o como una combinación de componentes de hardware y de software.

El sistema y/o el módulo y/o el dispositivo de envío y/o el dispositivo receptor y/o el sistema distribuido de base de datos y/o los nodos del sistema distribuido de base de datos (por ejemplo nodos de cadenas de bloque) y/o, aparatos pueden por ejemplo en cada caso adicionalmente exhibir aun uno u otros más componente(s), como por ejemplo un procesador, una unidad de memoria, otras interfaces de comunicación (por ejemplo Ethernet, WLAN), un aparato de ingreso, en particular un teclado de computador o un ratón de computador, y un aparato de despliegue (por ejemplo una pantalla). El procesador puede comprender por ejemplo varios otros procesadores, que en particular pueden ser usados para la realización de otros ejemplos de ejecución.

El procesador puede ser por ejemplo un ASIC, que fue realizado de manera específica para la aplicación, para las funciones de un respectivo módulo o todos los módulos del ejemplo de ejecución (y/u otros ejemplos de ejecución), en los que los componentes de programa y/o los comandos de programa en particular son realizados como circuitos integrados. El procesador puede ser por ejemplo también un FPGA, el cual en particular está configurado mediante los comandos de programa de modo que el FPGA ejecuta las funciones de un respectivo módulo o todos los módulos del ejemplo de ejecución (y/u otros ejemplos de ejecución).

En los ejemplos mencionados de realización, las interfaces de red pueden estar formadas también como interfaces integrales de red. Por ejemplo, la primera interfaz NI1 de comunicación del sistema SYS y la primera interfaz 210 de comunicación del dispositivo E receptor y/o la segunda interfaz 340 de comunicación del dispositivo S de envío, pueden estar formadas como una primera interfaz integral de comunicación. Por ejemplo la segunda interfaz NI2 de comunicación del sistema SYS y la segunda interfaz 240 de comunicación del dispositivo E receptor y/o la primera interfaz 310 de comunicación del dispositivo S de envío, pueden estar formadas como una segunda interfaz integral de comunicación. Pueden formarse por ejemplo la primera interfaz integral de comunicación y la segunda interfaz integral de comunicación como interfaces integrales conjuntas de comunicación.

En otras variantes, el dispositivo S de envío y/o el dispositivo E receptor y/o el sistema SYS pueden estar formados por ejemplo como un componente integral de uno de los aparatos, en lo cual la interfaz correspondiente de comunicación para comunicarse con los aparatos correspondientes, por ejemplo en un caso tal, es una interfaz de comunicación para un bus de datos (por ejemplo una interfaz PCI, una interfaz USB). Por ejemplo, en una de tales variantes los aparatos de legado o aparatos pueden estar unidos directamente al sistema distribuido de base de datos, en lo cual por ejemplo el dispositivo S de envío y/o die dispositivo E receptor y/o el sistema SYS están integrados en una interfaz de comunicación de aparatos de legados o de aparatos (por ejemplo como ASIC o FPGA). En la interfaz de comunicación el aparato puede ser por ejemplo una carta intercambiable de red, en la cual por ejemplo una antigua carta de red fue reemplazada por una correspondiente interfaz de acuerdo con la invención de comunicación. En otras palabras, en una variante así, una interfaz de comunicación puede comprender el dispositivo S de envío y/o el dispositivo E receptor y/o el sistema SYS, o la interfaz de comunicación está formado como el dispositivo S de envío y/o el dispositivo E receptor y/o el sistema SYS.

La Fig. 4 muestra un cuarto ejemplo de realización de la invención, como diagrama de flujo del procedimiento de acuerdo con la invención.

El procedimiento es realizado preferiblemente de manera computarizada.

En detalle, en este ejemplo de realización se ejecuta un procedimiento para el recibo computarizado de mensajes.

El procedimiento comprende una primera etapa 410 de procedimiento para la recepción de primeros mensajes de un sistema distribuido de base de datos, por medio de una primera interfaz de comunicación. Los primeros mensajes son almacenados por ejemplo en un formato de datos (por ejemplo un formato de datos XML) del sistema distribuido de base de datos.

El procedimiento comprende una segunda etapa 420 de procedimiento para el cálculo de una asignación para los primeros mensajes, en el que en el cálculo se establece para cuales aparatos está determinado un primer mensaje.

El procedimiento comprende una tercera etapa 430 de procedimiento para la conversión del contenido de mensaje del correspondiente primer mensaje, en un formato de datos para el aparato asignado. El formato de datos es en particular un formato de datos de propietario del aparato.

La tercera etapa de procedimiento es en particular una etapa opcional de procedimiento. Este es el caso por ejemplo cuando el contenido de mensaje del correspondiente primer mensaje no tiene que ser convertido o el contenido de mensaje o el correspondiente primer mensaje exhibe un formato de datos, que puede ser procesado por el aparato. En un caso así, el contenido convertido de mensajes de la cuarta etapa de procedimiento corresponde al contenido de mensaje (no convertido) del correspondiente primer mensaje, o el correspondiente primer mensaje es enviado como segundo mensaje al o los aparato(s) correspondiente(s).

El procedimiento comprende una cuarta etapa 440 de procedimiento para la transmisión del contenido convertido del mensaje, al aparato que está asignado al correspondiente primer mensaje.

La Fig. 5 muestra un quinto ejemplo de realización de la invención, como diagrama de flujo del procedimiento de acuerdo con la invención.

El procedimiento es realizado preferiblemente de manera computarizada.

En detalle, en este ejemplo de ejecución se realiza un procedimiento para el envío computarizado de mensajes.

El procedimiento comprende una primera etapa 510 de procedimiento para recibir primeros (otros) mensajes de aparatos, por medio de una interfaz de comunicación. Estos mensajes son almacenados por ejemplo en un formato de datos de propietario del aparato.

El procedimiento comprende una segunda etapa 520 de procedimiento para el cálculo de una asignación mediante el contenido respectivo del mensaje de los primeros (otros) mensajes, en el que se calcula cuál aparato ha enviado un correspondiente primer otro mensaje.

El procedimiento comprende una tercera etapa 530 de procedimiento para la conversión del contenido de mensaje de los correspondientes primeros (otros) mensajes, a un formato de datos para el sistema distribuido de base de datos, en el que el formato de datos puede ser procesado por ejemplo por el sistema distribuido de base de datos. El formato de datos puede ser por ejemplo un formato de datos XML, para el cual está disponible un esquema que se ajustan a XML. Los nodos del sistema distribuido de base de datos pueden así evaluar por ejemplo un estado de aparato de uno de los aparatos de la red de automatización, para enviar un mensaje por ejemplo a la correspondiente red de automatización o al correspondiente aparato, en función del estado del aparato.

La tercera etapa del procedimiento es en particular una etapa opcional. Este es el caso por ejemplo cuando el contenido de mensaje del correspondiente primer mensaje no tiene que ser convertido o el contenido de mensaje o el correspondiente primer mensaje exhibe un formato de datos, que puede ser procesado por el sistema distribuido de base de datos. En un caso así, el contenido convertido de mensajes de la cuarta etapa de procedimiento corresponde al contenido de mensaje (no convertido) del correspondiente primer mensaje, o el correspondiente primer mensaje es enviado como segundo mensaje al sistema distribuido de base de datos.

El procedimiento comprende una cuarta etapa 540 del procedimiento para la transmisión del contenido convertido del mensaje al sistema distribuido de base de datos.

La invención se refiere por ejemplo a una puerta de entrada o un adaptador de red, con el cual los aparatos antiguos o aparatos legados pueden estar unidos a un sistema distribuido de base de datos como una cadena de bloque, sin tener que cambiar una configuración de los aparatos antiguos.

De modo correspondiente, por ejemplo los mensajes que son enviados por el sistema distribuido de base de datos o son recibidos de este, son transacciones. De modo correspondiente, por ejemplo los mensajes que son enviados al sistema distribuido de base de datos son transacciones.

Si por ejemplo la segunda red NW2 con sus aparatos (Fig. 1 - 3) por ejemplo es también un sistema distribuido de base de datos, entonces por ejemplo pueden comunicarse mutuamente por medio de la invención (dispositivos, sistema, procedimientos) también dos sistemas diferentes distribuidos de base de datos.

Aunque la invención fue ilustrada y descrita en detalle mediante los ejemplos de realización, la invención no está limitada por los ejemplos divulgados, y el experto puede derivar otras variaciones, sin abandonar el alcance de protección de la invención.

[1] Andreas M. Antonopoulos "Mastering Bitcoin: Unlocking Digital Cryptocurrencies", O'Reilly Media, diciembre de 2014

[2] Roger M. Needham, Michael D. Schroeder "Using encryption for authentication in large networks of computers" ACM: Communications of the ACM. volumen 21, Nr. 12 de diciembre de 1978,

[3] Ross Anderson "Security Engineering. A Guide to Building Dependable Distributed Systems" Wiley, 2001

[4] Henning Diedrich"Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations", CreateSpace Independent Publishing Platform, 2016

[5] "The Ethereum Book Project/Mastering Ethereum" https://github.com/ethereumbook/ethereumbook, Stand 5.10.2017

[6] Leemon Baird "The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance", Swirlds Tech Report SWIRLDS-TR-2016-01, 31.5.2016

[7] Leemon Baird "Overview of Swirlds Hashgraph", 31.5.2016

[8] Blockchain Oracles https://blockchainhub.net/blockchain-oracles/ Stand 14.03.2018

REIVINDICACIONES

1. Dispositivo (E) receptor, que comprende:

- una primera interfaz (210) de comunicación, en la que

- la primera interfaz de comunicación está configurada para recibir primeros mensajes de un sistema distribuido de base de datos;

- un módulo (220) de identificación, en el que

- el módulo de identificación está configurado para calcular, mediante el respectivo contenido del mensaje del primer mensaje, una asignación a los primeros mensajes, respecto a qué aparato está designado para un primer mensaje correspondiente;

- un módulo (230) de conversión, en el que

- el módulo de conversión está configurado para convertir el contenido de un mensaje del correspondiente primer mensaje, en un formato de datos para el aparato asignado,

- un módulo de criptografía, en el que el módulo de criptografía comprende los datos criptográficos asociados a los aparatos,

los datos criptográficos son determinados mediante una combinación de datos inequívocamente específicos del aparato y datos específicos del receptor de aparato y para el correspondiente aparato se determinan de manera reproducible datos criptográficos;

- para un aparato asignado, el módulo de criptografía comprueba y/o descifra mediante el uso datos criptográficos, al menos una parte del contenido del mensaje del correspondiente primer mensaje,

- para la comprobación y/o la descodificación se cargan los correspondientes datos criptográficos en virtud del aparato asignado;

- una segunda interfaz de comunicación (240), en la que

- la interfaz de comunicación está configurada para transferir al aparato el contenido convertido del mensaje, el cual está asignado al correspondiente primer mensaje.

2. Dispositivo (E) receptor de acuerdo con la reivindicación 1, en el que

- el dispositivo receptor recupera un estado de aparato del aparato asignado al primer mensaje correspondiente,

- ocurre una transmisión al aparato asignado, que es función del estado recuperado del aparato.

3. Dispositivo (E) receptor de acuerdo con la reivindicación 2, en el que

- el estado de aparato comprende un registro de datos sobre los recursos disponibles de aparato y/o propiedades actuales del aparato.

4. Dispositivo (E) receptor de acuerdo con una de las reivindicaciones precedentes, en el que

- ocurre una transmisión al correspondiente aparato, cuando el aparato asignado satisface los requerimientos preestablecidos del correspondiente primer mensaje,

- por ejemplo se comprueba el cumplimiento de los requisitos establecidos previamente mediante el uso del estado del aparato.

5. Dispositivo (S) de envío, que exhibe

- una primera interfaz de comunicación (310), en la que

- la primera interfaz de comunicación está configurada para comunicarse con aparatos,

- la interfaz de comunicación está configurada para recibir los primeros mensajes de los aparatos;

- un módulo de identificación (320), en el que

- el módulo de identificación está configurado para calcular una asignación mediante el uso del respectivo contenido

de mensaje de los primeros mensajes, respecto a cuál aparato ha enviado un correspondiente primer mensaje;

- un módulo (330) de conversión, en el que

- el módulo de conversión está configurado para convertir el contenido de mensaje del correspondiente primer mensaje en un formato de datos para el sistema distribuido de base de datos;

- un módulo de criptografía, en el que

- el módulo de criptografía comprende datos de criptografía asignados a los aparatos,

los datos criptográficos son determinados mediante una combinación de datos inequívocamente específicos al aparato y datos específicos del dispositivo de envío, y para el aparato correspondiente los datos criptográficos son determinados de manera reproducible;

- usando los aparatos asignados, el módulo de criptografía carga los correspondientes datos criptográficos,

- mediante los correspondientes datos criptográficos protege criptográficamente al menos una parte del contenido del mensaje del correspondiente primer mensaje de modo específico para el aparato, para el Aparato asignado;

- una segunda interfaz (340) de comunicación, en la que

-la segunda interfaz de comunicación está configurada para comunicarse con un sistema distribuido de base de datos,

- la interfaz de comunicación está configurada para transmitir el contenido convertido del mensaje, al sistema distribuido de base de datos.

6. Dispositivo (S) de envío y/o dispositivo (E) receptor de acuerdo con una de las reivindicaciones precedentes, en el que

- el sistema distribuido de base de datos es una cadena de bloque,

- por ejemplo los mensajes que son enviados y/o recibidos por el sistema distribuido de base de datos, son transacciones.

7. Dispositivo (S) de envío y/o dispositivo (E) receptor de acuerdo con una de las reivindicaciones precedentes, en el que

- al menos una parte de los aparatos, son aparatos de una red de automatización.

8. Sistema (SYS), que exhibe:

- un dispositivo (E) receptor de acuerdo con una de las reivindicaciones 1-4 o 6 - 7;

- un dispositivo (S) de envío de acuerdo con una de las reivindicaciones 5-7.

9. Procedimiento para la recepción computarizada de mensajes, con las siguientes etapas del procedimiento:

- recepción de primeros mensajes de un sistema distribuido de base de datos, mediante una primera interfaz de comunicación;

- cálculo de una asignación para los primeros mensajes, en el que en el cálculo se determina a cuál aparato se determina un primer mensaje correspondiente;

- conversión del contenido de mensaje del correspondiente primer mensaje, a un formato de datos para el aparato asignado;

- carga de datos criptográficos mediante el uso del aparato asignado, en la que los datos criptográficos son asignados al aparato asignado y se determinan los datos criptográficos mediante una combinación de datos inequívocamente específicos al aparato y datos específicos del receptor del aparato, y para el aparato correspondiente se determinan de manera reproducible los datos criptográficos;

- mediante datos criptográficos, comprobación y/o descodificación de al menos una parte del contenido del mensaje del correspondiente primer mensaje, para el aparato asignado;

- transmisión del contenido convertido del mensaje al aparato, que está asignado al correspondiente primer mensaje.

10. Procedimiento para el envío computarizado de mensajes, con las siguientes etapas de procedimiento:

- recepción de primeros mensajes de aparatos, mediante una interfaz de comunicación;

- cálculo de una asignación mediante el respectivo contenido de mensajes de los primeros mensajes, en el cual se calcula cuál aparato ha enviado un primer otro mensaje correspondiente;

- conversión del contenido de mensajes del correspondiente primer mensaje, a un formato de datos para el sistema distribuido de base de datos;

- carga de datos criptográficos usando el aparato asignado, en la que los datos criptográficos son asignados al aparato asignado, y los datos criptográficos son determinados mediante una combinación de datos inequívocamente específicos al aparato y datos específicos al dispositivo de envío, (página 51 de la descripción, filas 28-32) y los datos criptográficos son determinados de manera reproducible para el correspondiente aparato; en el que mediante los correspondientes datos criptográficos, al menos una parte del contenido del mensaje del correspondiente primer mensaje, es protegida criptográficamente de modo específico al aparato para el aparato asignado;

- transmisión del contenido convertido de los mensajes, al sistema distribuido de base de datos.

11. Producto de programa de computador con comandos de programa, que en la ejecución del programa mediante un procesador ordenan a éste, realizar las etapas del procedimiento de acuerdo con las reivindicaciones 9 o 10.

12. Aparato de suministro para el producto de programa de computador de acuerdo con la reivindicación 11, en el que el aparato de suministro almacena y/o suministra el producto de programa de computador.

FIG 1

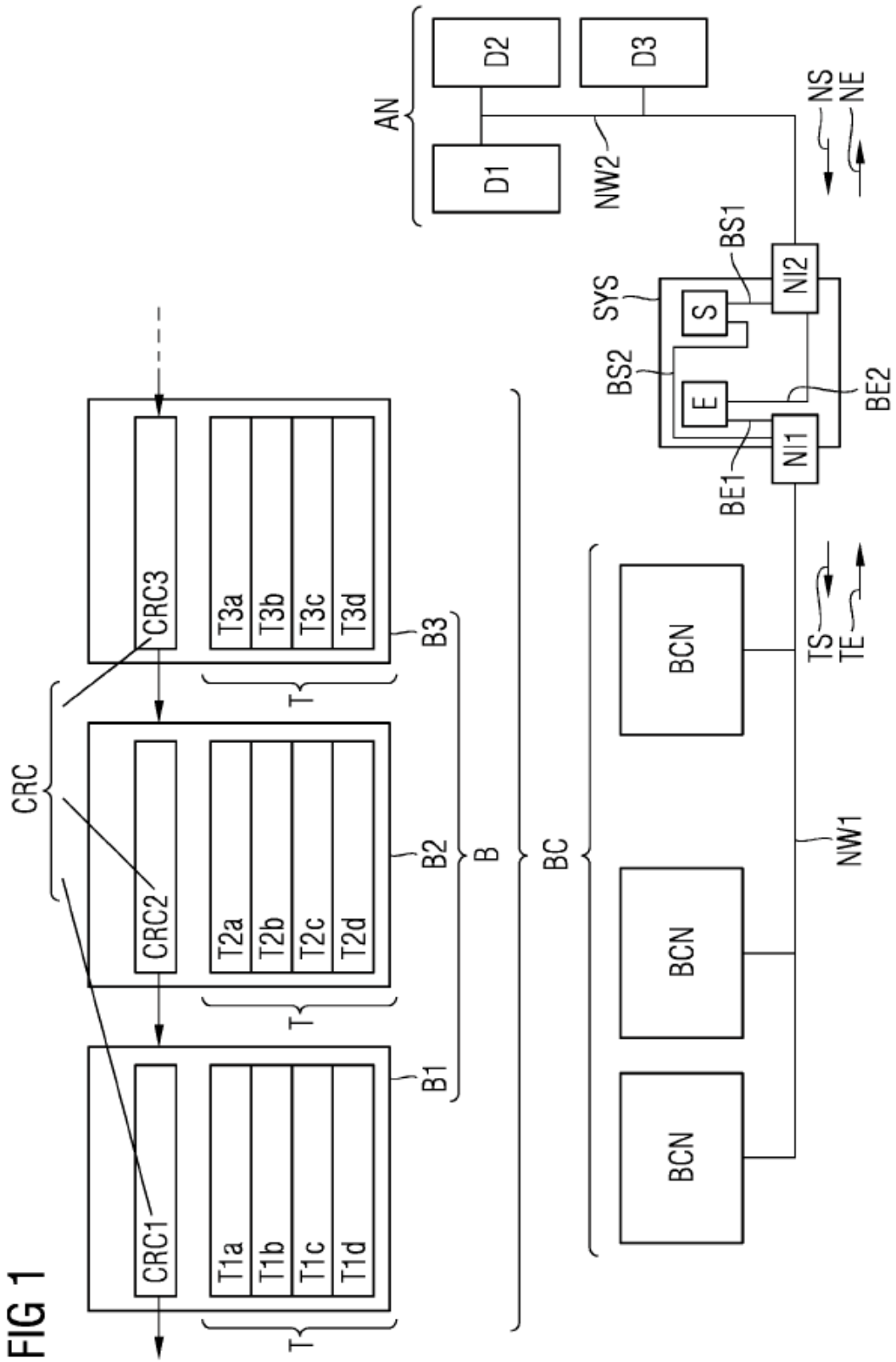
AN
D2
D3
D1
NW2
NS
NE
BS1
SYS
S
NI2
BS2
E
BE2
NI1
BE1
BCN
BCN
BCN
TS
TE
NW1
BC
B
B3
B2
B1
T
T
T
CRC
CRC3
CRC2
CRC1
T3a
T3b
T3c
T3d
T2a
T2b
T2c
T2d
T1a
T1b
T1c
T1d

FIG 2

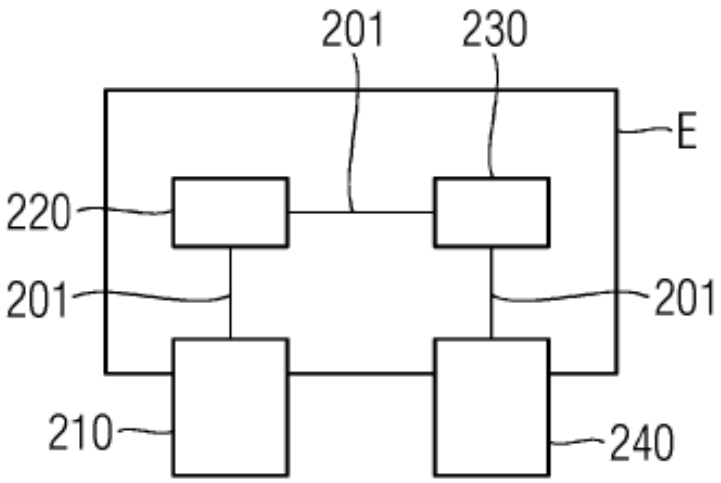

FIG 3

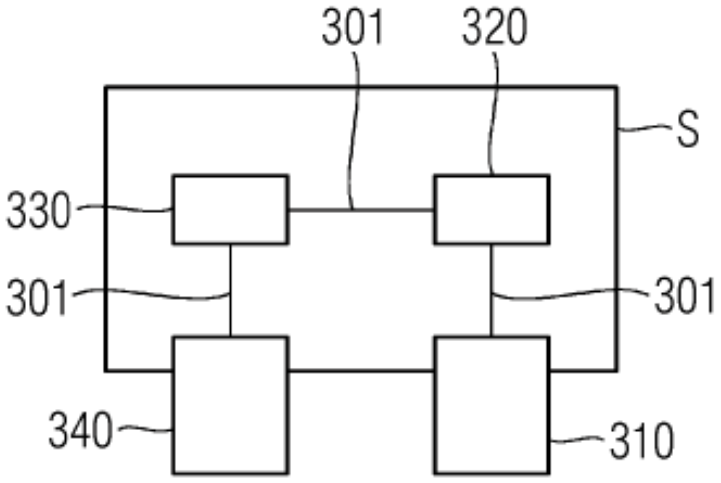

FIG 4

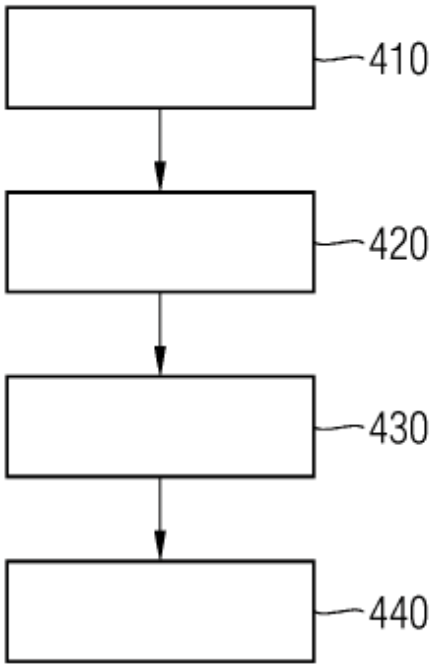

FIG 5