(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
07 March 2019 (07.03.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/042754 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04L 9/30* (2006.01)

(21) International Application Number:
PCT/EP2018/071879

(22) International Filing Date:
13 August 2018 (13.08.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
17189163.3 04 September 2017 (04.09.2017) EP

(71) Applicant: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Werner-von-Siemens-Straße 1, 80333 München (DE).

(72) Inventor: **FALK, Rainer**; Primelweg 9, 85586 Poing (DE).

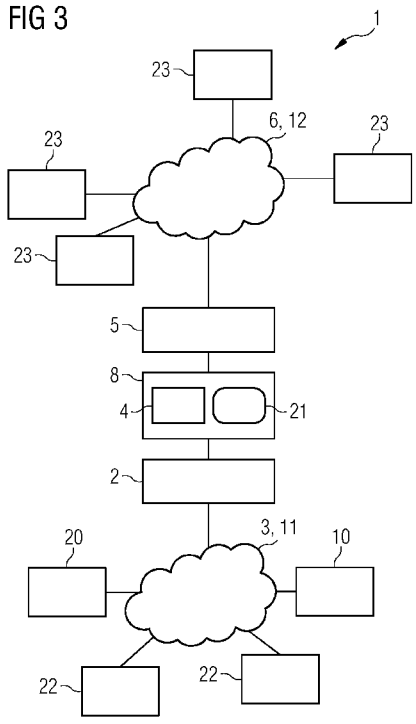
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS,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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report (Art. 21(3))*

(54) **Title:** FILTER UNIT BASED DATA COMMUNICATION SYSTEM INCLUDING A BLOCKCHAIN PLATFORM

FIG 3



(57) **Abstract:** An object of the present application is to provide a system and a respective method for performing data communication in between a first network and a second, blockchain-based network, wherein the communication is adapted to prevent invalid and/or unwanted data traffic. According to this, a system adapted for performing data communication is provided. The system comprises a first interface adapted to communicate with a first network, a filter unit and a second interface. The second interface is adapted to communicate with a second network connected to the first network via the filter unit, and the second network is adapted to operate as a blockchain platform. The filter unit is adapted to selectively permit data received from the first network via the first interface to be transmitted to the second network via the second interface.

WO 2019/042754 A1

Description

Filter unit based data communication system including a blockchain platform

BACKGROUND

In the present time of a rising demand for cross-company IT solutions, information between companies are to be transmitted in the form of transactions. In several cases, such as in the case of the Bitcoin technology or Smart Contracts, these transactions may be based on the blockchain technology, offering an open or public platform for sharing, executing, and reviewing the respective transactions.

In the case of such open transaction platforms, there is a risk that inadvertently sensitive company information or not released transactions or not duly approved transactions may be transmitted into an open transaction database, e.g. the blockchain database. This can e.g. occur by the fact that employees use a blockchain software, the right of which is not conferred to use, or by using a company-used blockchain platform, which is used in an inadmissible manner.

SUMMARY

Therefore, there is a need to prevent invalid and/or unwanted data traffic from a first network to a second, blockchain-based network.

It is an object of the present application to provide a system and a respective method for performing data communication in between a first network and a second, blockchain-based network, which is adapted to prevent invalid and/or unwanted data traffic.

A system and a method according to the independent claims are provided. Further embodiments are defined in the dependent claims.

According to an embodiment, a system adapted for performing data communication is disclosed. The system comprises a first interface adapted to communicate with a first network. The system further comprises a filter unit. The system further comprises a second interface adapted to communicate with a second network connected to the first network via the filter unit, wherein the second network is adapted to operate as a blockchain platform. According to this, the filter unit is adapted to selectively permit data received from the first network via the first interface to be transmitted to the second network via the second interface.

Such an approach may be based on the finding that the arrangement of a filter unit in between a first network and a blockchain-based second network may provide a technical implementation enabling an additional restriction of the data traffic originating from the first network and reaching the second network. Since such a blockchain based second network may operate by processing data in an irreversible manner, such technical means may help to prevent publishing data which otherwise could not be deleted, or to prevent processing of transactions comprised within the data for which the effect of processing could not be reversed anymore. The filtering realizing the additional restriction can be defined independently of the blockchain logic for verifying the validity of transactions. This allows to flexibly define which transactions can be submitted by a firm to the blockchain based second network, e.g. to an open or public blockchain platform for processing. Company-specific authorizations, approvals, can be flexibly checked, without the blockchain platform being required to process company-internal permission information. Company-internal authorization services and authorization information can be easily integrated, without exposing the company-internal authorization information to an

open or public blockchain platform. Changes within the organization of the firm can be reflected by modified filter rules, i.e. without requiring changes to the blockchain platform or to the data processed by the blockchain infrastructure.

The filtering of data before being submitted to the blockchain based second network, e.g., a blockchain platform or a blockchain infrastructure, for processing is required when using open or public blockchain platforms by a firm or in enterprise environments. In contrast to a conventional firewall, the purpose is not to prevent network attacks on the company network by limiting network communication, but to enforce rules on outgoing transactions that cannot be deleted or reversed once accepted and processed by the blockchain infrastructure. So, the invention enables the safe, controlled use of an open or public blockchain infrastructure. Incoming transactions can be filtered as well before importing the transactions in company-internal IT systems.

According to another embodiment, a method for performing data communication is disclosed. The method comprises selectively permitting data received from a first network to be transmitted to a second network. According to this method, the second network is operated as a blockchain platform based on the permitted data.

Such an approach may be based on selectively filtering data before reaching the blockchain based second network. Data, which are not determined as suitable for processing by the blockchain technology, may therefore be prevented reaching the second network, which may operate in an irreversible manner.

A network within the meaning of the present disclosure may refer to any set of nodes which enables a plurality of participants to perform data communication with each other. The network may be a public network or a private network. The

network may or may not be based on a blockchain platform. The network may be connected to at least one further network. The network may irreversibly process the data based on blockchain techniques.

A filter unit within the meaning of the present disclosure may refer to any unit, which is adapted to separate first set of data from a second set of data. The data may comprise at least one transaction to be processed by a blockchain platform. Separation may take place in that the first set of data is permitted to pass the filter unit and the second set of data is not permitted to pass the filter unit. Here, separation may be controlled by a user input.

A blockchain platform within the meaning of the present disclosure may refer to any database implemented in a network, which is at least partly based on the blockchain technique. The blockchain may comprise a plurality of blocks comprising data related to transactions and/or Smart Contracts. Chaining of different blocks may be implemented by cryptographic hash values stored in each block, wherein each hash value may refer to data of a previous block.

In an embodiment of the system, the filter unit is adapted to selectively permit the data based on a data content and/or a data origin.

The provision of a unit adapted for filtering data based on its data content may thereby enable to control a distribution of information based on the level of confidentiality of these information. The provision of a unit adapted for filtering data based on its data origin may thereby enable to distribute data based on given regulations, such as a firm policy. For example, a policy may be compared with the data content and/or the data origin to decide whether to permit the data or not.

In another embodiment, the filter unit is adapted to selectively permit the data based on a user input.

Thereby, selection criteria of a filter unit may be adapted according to the present circumstances and the user's needs.

In another embodiment, the filter unit is part of a) a network firewall located at a transition in between the first network and the second network or b) a cloud-based service.

With respect to the network firewall, the filter unit may be implemented by preferably simple technical means. Pertaining to the cloud-based service, filtering data traffic may be outsourced from a present network connection, thereby saving resources of the present networks.

In another embodiment, the data comprises a transaction, which may be processed by the blockchain platform.

Thereby, the second network comprising the blockchain platform may be used as an openly accessible database, enabling any participants sharing and reviewing the transactions to be performed. The second network may be a permissioned blockchain platform that is accessible by a multitude of firms.

In another embodiment, the filter unit is adapted to perform the selective permission of the data comprising the transaction independent from or of other transactions, which have been received by the filter device previously.

Thereby, a reliable permission of transactions to be processed by the blockchain platform independent from or of a transaction protocol may be provided.

In another embodiment, the filter unit is adapted to perform the selective permission of the data comprising the transac-

tion based on other transactions, which have been received by the filter unit previously.

Thereby, e.g. the amount of transactions processed by the blockchain platform previously may be taken into account for providing further transactions to the blockchain platform. As a matter of consequence, the number of transactions performed in a predefined time interval may be limited. Also, other properties of the earlier transactions may be taken into account, e.g., data content and/or data origin, etc. Heuristic rule sets for permitting the data may be developed.

In another embodiment, the data comprises a classification of the transaction and the selective permission of the filter unit is adapted to be based on the classification of the transaction.

Thereby, based on any transaction characteristic, different transactions can be handled in a different manner. The classification may parameterize certain details of the transaction such that different transactions can be easily compared.

In another embodiment, the classification of the transaction comprises a security label of the transaction.

Thereby, the level of confidentiality referring to a transaction may be taken into account for an evaluation, whether a transaction is provided for processing to the blockchain platform of the second network.

In another embodiment, the filter unit is adapted for receiving, from a transaction approval unit of the first network, instructions for blocking the transaction, e.g. if the transaction approval unit does not receive a predetermined number of approval messages from respective participants.

Thereby, the filter unit is adapted to be controlled - at least partly - by regulations implemented in the first net-

work, which correspond to approvals of participants sharing the first network. These approvals to be given for transmitting a transaction to a blockchain platform may represent the authority of the respective participants in a community, e.g. a firm. As a matter of consequence, such an adaption may e.g. implement a given firm policy. The firm policy may also reflect regulations that allow the firm to comply with company rules or regulatory limitations.

In another embodiment, the system further comprises a labelling unit, which is adapted to label the data comprising the transaction permitted by the filter unit using a checksum, wherein the label is indicative of the respective filter unit of a plurality of filter units. The labelling unit may also label the transaction using another unique key, alternatively or additionally to the checksum. The checksum may be a cryptographic checksum, e.g. a message authentication code or a digital signature.

Thereby, any data received by the first network may be assigned to a specific filter unit, which is adapted to control permission of the data for reaching the second network. Therefore, these means may facilitate the inspection of filtering processes.

In another embodiment, the system further comprises a modification unit, which is adapted to modify the transaction permitted by the filter unit, wherein the modified transaction is transmitted to the second network via the second interface and the non-modified transaction is not transmitted to the second network via the second interface.

Thereby, the modified transaction, which is permitted to reach the blockchain platform, and the non-modified transaction, which is not permitted to reach the blockchain platform, may carry different information. As an example, information, which is to be available to participants of the first network, but which is not to be available to participants of

the second network, may merely be included in the non-modified, but not in the modified, transaction. Consequently, these means may enable a desired distribution of information. Anonymisation is possible. Privacy-sensitive information may be filtered.

In another embodiment, the filter unit is further adapted to selectively permit data received from the second network to be transmitted to the first network.

Thereby, malware resided in the second network may be blocked from also reaching the first network. Furthermore, only transactions that comply with filter rules may be imported and may be processed in company-internal IT systems. In particular, only transactions complying with filter rules may be imported automatically. Other transactions may be rejected, or may require an explicit approval before importing them in a company-internal IT system.

In another embodiment, the first network is a private network and/or the second network is a public network.

Thereby, the filter unit may be implemented in filtering data traffic originating from a first network to a second network, wherein the first network comprises a smaller number of participants than the second network. Thus, these means are adapted to control the data traffic to different circles of participants.

In an embodiment of the method, the method is performed by a system according to any of the embodiments above.

Thereby, the method may be performed based on a preferably simple technical implementation.

A network firewall within the meaning of the present disclosure may refer to a security system in between different networks that controls the incoming and/or outgoing data traffic

based on predetermined security rules. The data traffic may comprise transactions to be processed by a blockchain platform. The security rules may be controlled by a user input.

A cloud-based service within the meaning of the present disclosure may refer to any technical concepts implemented in a cloud-computing infrastructure. Hereby, it may be enabled to computing capabilities storing and processing data in either a privately owned cloud, or on a third-party server located in a data center in order to make data accessing mechanisms more efficient and reliable.

A security level within the meaning of the present disclosure may refer to a characteristic of a transaction, which refers to a requirement of controlling a transaction when transmitting from a first network to a second network. The security level of the transaction may be assigned by a participant of the first network. The security level may refer to a level of confidentiality of the transaction. For example, restricted information may be discriminated from top secret information, etc..

A private network within the meaning of the present disclosure may refer to a network accessible to a smaller or restricted number of participants than a public network. A private network may refer to a company-internal network. The private network may be adapted to be used for transmitting data to which a higher confidentiality is attributed.

A public network within the meaning of the present disclosure may refer to a network accessible to a larger number of participants than a private network. For example, unrestricted access may be provided to the public network. A public network may refer to an open network, but may also refer to a company-internal network. The public network may be adapted not to be used for transmitting data to which a higher confidentiality is attributed.

According to an embodiment, a computer program product comprises program code. The program code may be executed by at least one processor. Executing the program code causes the at least one processor to perform a method for performing data communication. The method comprises selectively permitting data received from a first network to be transmitted to a second network. The second network is operated as a blockchain platform based on the permitted data.

According to an embodiment, a computer program comprises program code. The program code may be executed by at least one processor. Executing the program code causes the at least one processor to perform a method for performing data communication. The method comprises selectively permitting data received from a first network to be transmitted to a second network. The second network is operated as a blockchain platform based on the permitted data.

The above summary is merely intended to give a short overview over some features of some embodiments and implementations and is not to be construed as limiting. Other embodiments may comprise other features than the ones explained above.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other elements, features, steps and characteristics of the present disclosure will be more apparent from the following detailed description of embodiments with reference to the following figures:

Figure 1 schematically illustrates a blockchain section, which may be assembled based on a system and a method according to the present disclosure.

Figure 2 schematically illustrates another blockchain section, which may be assembled based on a system and a method according to the present disclosure.

Figure 3 schematically illustrates a filter unit based data communication system according to various examples.

Figure 4 represents a flowchart of a method performed by the data communication system according to various examples.

DETAILED DESCRIPTION OF EMBODIMENTS

In the following, embodiments of the invention will be described in detail with reference to the accompanying drawings. It is to be understood that the following description of embodiments is not to be taken in a limiting sense. The scope of the invention is not intended to be limited by the embodiments described hereinafter or by the drawings, which are taken to be illustrative only.

The drawings are to be regarded as being schematic representations and elements illustrated in the drawings, which are not necessarily shown to scale. Rather, the various elements are represented such that their function and general purpose become apparent to a person skilled in the art. Any connection or coupling between functional blocks, devices, components, or other physical or functional units shown in the drawings or described herein may also be implemented by an indirect connection or coupling. A coupling between components may also be established over a wireless connection. Functional blocks may be implemented in hardware, firmware, software, or a combination thereof.

Figure 1 schematically illustrates a blockchain section, which may be assembled based on a system 1 and a method 100 according to the present disclosure.

According to this, such a blockchain 13 may comprise a plurality of blocks 14a-14c connected to each other. In such an assembling, each block 14a, 14b, 14c may be coupled with two neighboring blocks 14a-14c, wherein coupling is - according

to Figure 1 - depicted as chain 16. A new block 14a-14c to be included in the blockchain 13 may be assembled at an open end of the chain 16 of the block chain 13. Each block 14a-14c may comprise a plurality of transactions 9 to be processed. The creation of the chain 16 coupling the blocks 14a-14c to assemble the blockchain 13 may be supported by hash values 15a-15c, each implemented in their respective block 14a-14c. Hereby, each hash value for 15a to 15c depends on the predecessor block 14a to 14c. Specifically, the respective hash value 15a-15c is evaluated based on the data of the respective predecessor block 14a-14c.

With respect to the transactions 9 implemented in each block 14a-14c, the program code may be implemented as a smart contract. The program code may carry information with respect to whether a transaction 9 is admissible. According to this, different business processes may be flexibly realized by a common blockchain infrastructure. Usually, a hash tree, e.g. a Merkle tree or a Patricia tree, may be used for storing the respective hash values in each of the blocks 14a-14c.

Figure 2 schematically illustrates another blockchain section, which may be assembled based on a system and a method according to the present disclosure.

According to this, the blockchain 13 comprises blocks 14a-14c, which are connected by chain 16. The creation of the blockchain 13 by assembling blocks 14a-14c by chain 16 is hereby supported by hash values 15a-15c, each of them is implemented in the respective block 14a-14c.

Specifically, each of the blocks 14a to 14c comprises specific configurations of the transactions 9. As an example, the transactions 9 may be configured as payment transaction 17, ownership transfer transaction 18 and register smart contract 19. Hereby, the transaction 9 may comprise further attributes, which may e.g. be adapted to indicate a receiver of a payment, an object and its new owner or a program code of a

smart contract. Blockchain transactions may be used also to control an energy automation network. A transaction may cause an energy generator to feed a certain amount of electric energy into the energy grid, to cause an energy consumer to limit the energy consumption, or to perform a switching operation in the energy grid. The attributes of a blockchain transaction may indicate an electric device and the action to be performed by the device.

Figure 3 schematically illustrates a filter unit based data communication system 1 according to various examples.

According to this, the system 1 comprises at least one first interface 2 adapted to communicate with a first network 3. The first network 3 may be a private network 11, such as a firm network. Access to the private network 11 may be restricted. Any arbitrary number of first network nodes 22 may be provided by the first network 3.

In addition, the system 1 also comprises at least one second interface 5 adapted to communicate with a second network 6. The second network 6 may be a public network 12, such as the internet or any further network available to different firms and/or communities. Hereby, the second network 6 may be adapted to operate as a blockchain platform 7. Any arbitrary number of second network nodes 23 may be provided by the second network 6.

The first network 3 and the second network 6 may be connected to each other via a filter unit 4. The filter unit 4 may be adapted to selectively permit data received from the first network 3 via the first interface 2 to be transmitted to the second network 6 via the second interface 5. These data may comprise at least one transaction 9, which may be processed by the blockchain platform 7.

The filter unit 4 may be implemented in a network firewall 8, as depicted in Figure 3. Such a network firewall 8 may addi-

tionally comprise a memory 21 for storing rules. In addition, the filter unit 4 may also be implemented in a cloud-based service. Further, for filtering data, a cross-domain security solution may also be used.

The filter unit 4 may be adapted to selectively permit the data based on a data content. Such a data content may e.g. refer to the content of the transaction 9. The filter unit 4 may also be adapted to selectively permit the data based on a data origin. Such a data origin may refer to an origin of a transaction 9, e.g. a computer from which the transaction 9 is transmitted or a user logged in the respective computer. These transaction data may refer to attributes and/or smart contracts.

Further, the filter unit 4 may also be adapted to selectively permit the data based on a user input, which may change the filter criteria based on modified circumstances, such as a modified firm policy or modified public regulations.

The filter unit 4 may further be adapted to perform the selective permission of the data comprising the transaction 9 independent of other transactions 9, which have been received by the filter unit 4 previously. In addition, the filter unit 4 may also be adapted to perform the selective permission of the data comprising the transaction 9 based on other transactions 9, which have been received by the filter unit 4 previously. In the latter case, these means can be implemented in payment actions, which may only be admissible in the case that a total amount of money spent during a time interval remains below an admissible, predetermined threshold value.

Further, the filter unit 4 may be adapted to selectively permit data received from the second network 6 to be transmitted to the first network 3. In such a case, the respective filtering mechanism may operate bidirectional. Such a mechanism may e.g. be used for blocking data traffic originating from the public network 12 and flowing towards the private network

11. Such a blocked data traffic may e.g. be constructive with respect to malware adapted to damage the private network 11, such as a firm network. In addition, the filter unit 4 may also be adapted for receiving, from a transaction approval unit 10 of the first network 3, instructions for blocking the transaction 9, if the transaction approval unit 10 does not receive a predetermined number of approval messages from respective participants.

As can be deduced from Figure 3, the first network 3 configured as a private network 11 may additionally provide for a transaction classification unit 20. Based on this unit, the data may comprise a classification of the transaction 9, and the selective permission of the filter unit 4 may be adapted to be based on the classification of the transaction. Such a classification may e.g. comprise a security label of the transaction 9 and may be used to attribute a level of confidentiality to the respective transactions 9. In addition, the first network 3 configured as a private network 11 may additionally provide for a transaction approval unit 10 adapted to receive a plurality of approvals from different participants of the private network 11 before a transaction 9 is permitted reaching the blockchain platform 7.

Figure 4 represents a flowchart of a method 100 performed by the data communication system 1 according to various examples, wherein - according to this example - the communicated data correspond to a transaction 9. Herein, 110, 150, 160, 165 and 170 refer to the common handling of transactions 9 to be performed in a blockchain environment.

At 110, a transaction 9 is released by a participant of the first network 3, e.g., a private network 11.

Subsequently at 120, the released transaction 9 is received by a filter unit 4 connected to the first network 3 via the first interface 2.

Subsequently at 130, the filter unit 130 examines whether the received transaction 9 is to be permitted to reach the blockchain platform 7. According to this, transactions 9 received from a first network 3 via a first interface 2 is selectively permitted by the filter unit 4.

In case that, based on 130, the transaction 9 is not permitted reaching the blockchain platform 7, the blockchain transaction is blocked at 145 – e.g., discarded or rejected. Otherwise and with respect to 140, the transaction 9 is forwarded to the blockchain platform 7 via a second interface 5.

At the blockchain platform 7, common transaction 9 handling is performed. The blockchain platform 7 checks the validity of the transaction 7 before including the transaction 9 in a block of the blockchain, confirming the transaction to be valid. At 150, the blockchain platform 7 examines whether the transaction 9 are valid. For this purpose, hash values 15a-15c may be taken into account, and smart contracts may be processed according to the common proceedings.

In case that, based on 150, the transaction 9 may not be validated, the non-valid transaction 9 is refused at 165. Otherwise, a block comprising the validated transaction 9 is attached to the blockchain 13 at 160 and the transaction 9 is performed.

Subsequently at 170, the method 100 is stopped.

Claims

1. System (1) adapted for performing data communication, comprising

a first interface (2) adapted to communicate with a first network (3);

a filter unit (4); and

a second interface (5) adapted to communicate with a second network (6) connected to the first network (3) via the filter unit (4), the second network (6) being adapted to operate as a blockchain platform (7),

wherein the filter unit (4) is adapted to selectively permit data received from the first network (3) via the first interface (2) to be transmitted to the second network (6) via the second interface (5).

2. System (1) according to claim 1, wherein the filter unit (4) is adapted to selectively permit the data based on a data content and/or a data origin.

3. System (1) according to any of claims 1 and 2, wherein the filter unit (4) is adapted to selectively permit the data based on a user input.

4. System (1) according to any of the preceding claims, wherein the filter unit (4) is part of a) a network firewall (8) located at a transition in between the first network (3) and the second network (6) or b) a cloud-based service.

5. System (1) according to any of the preceding claims, wherein the data comprises a transaction (9), which may be processed by the blockchain platform (7).

6. System (1) according to claim 5, wherein the filter unit (4) is adapted to perform the selective permission of the data comprising the transaction (9) independent from other transactions (9), which have been received by the filter unit (4) previously.

7. System (1) according to any of claims 5, wherein the filter unit (4) is adapted to perform the selective permission of the data comprising the transaction (9) based on other transactions (9), which have been received by the filter unit (4) previously.

8. System (1) according to any of claims 5 to 7, wherein the data comprises a classification of the transaction (9), and wherein the selective permission of the filter unit (4) is adapted to be based on the classification of the transaction (9).

9. System (1) according to claim 8, wherein the classification of the transaction (9) comprises a security label of the transaction (9).

10. System (1) according to any of claims 5 to 9, wherein the filter unit (4) is adapted for receiving, from a transaction approval unit (10) of the first network (3), instructions for blocking the transaction (9), if the transaction approval unit (10) does not receive a predetermined number of approval messages from respective participants.

11. System (1) according to any of claims 5 to 10, further comprising a labelling unit, which is adapted to label the data comprising the transaction (9) permitted by the filter unit (4) using a checksum, wherein the label is indicative of

the respective filter unit (4) of a plurality of filter units (4).

12. System (1) according to any of claims 5 to 11, further comprising a modification unit, which is adapted to modify the transaction (9) permitted by the filter unit (4), wherein the modified transaction is transmitted to the second network (6) via the second interface (5) and the non-modified transaction is not transmitted to the second network (6) via the second interface (5).

13. System (1) according to any of the preceding claims, wherein the filter unit (4) is further adapted to selectively permit data received from the second network (6) to be transmitted to the first network (3).

14. System (1) according to any of the preceding claims, wherein the first network (3) is a private network (11) and/or the second network (6) is a public network (12).

15. Method (100) for performing data communication, comprising:

selectively permitting (130) data received from a first network (3) to be transmitted to a second network (6) , the second network (6) being operated as a blockchain platform (7) based on the permitted data.

16. Method according to claim 15, which is performed by a system (1) according to any of claims 1 to 14.

FIG 1

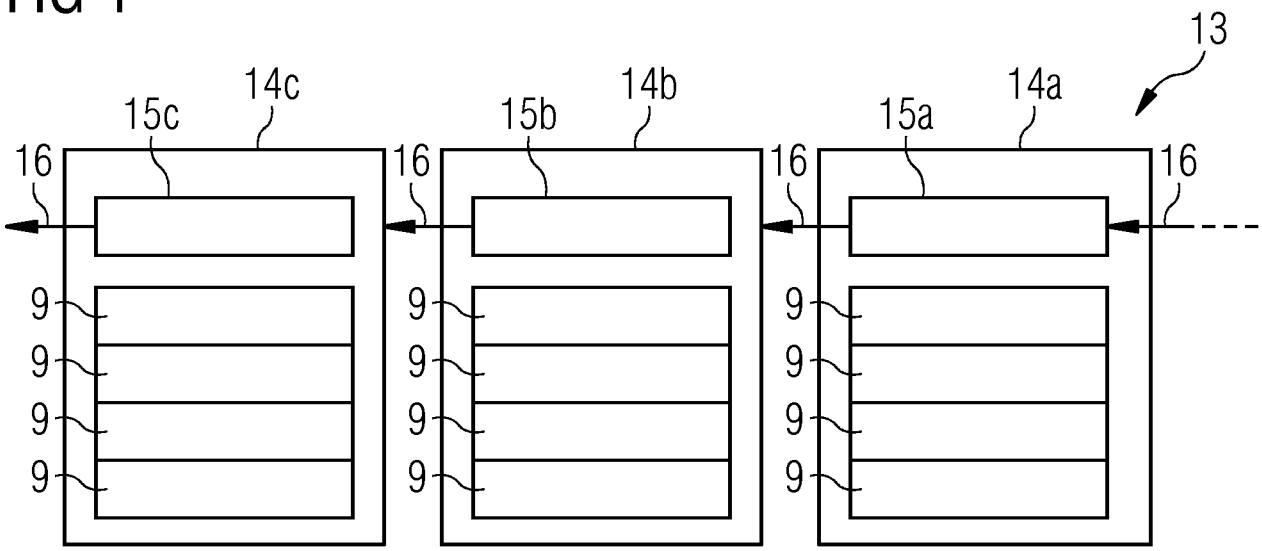

13
14c
15c
14b
15b
14a
15a
16
16
16
16
9
9
9
9
9
9
9
9
9
9
9
9

FIG 2

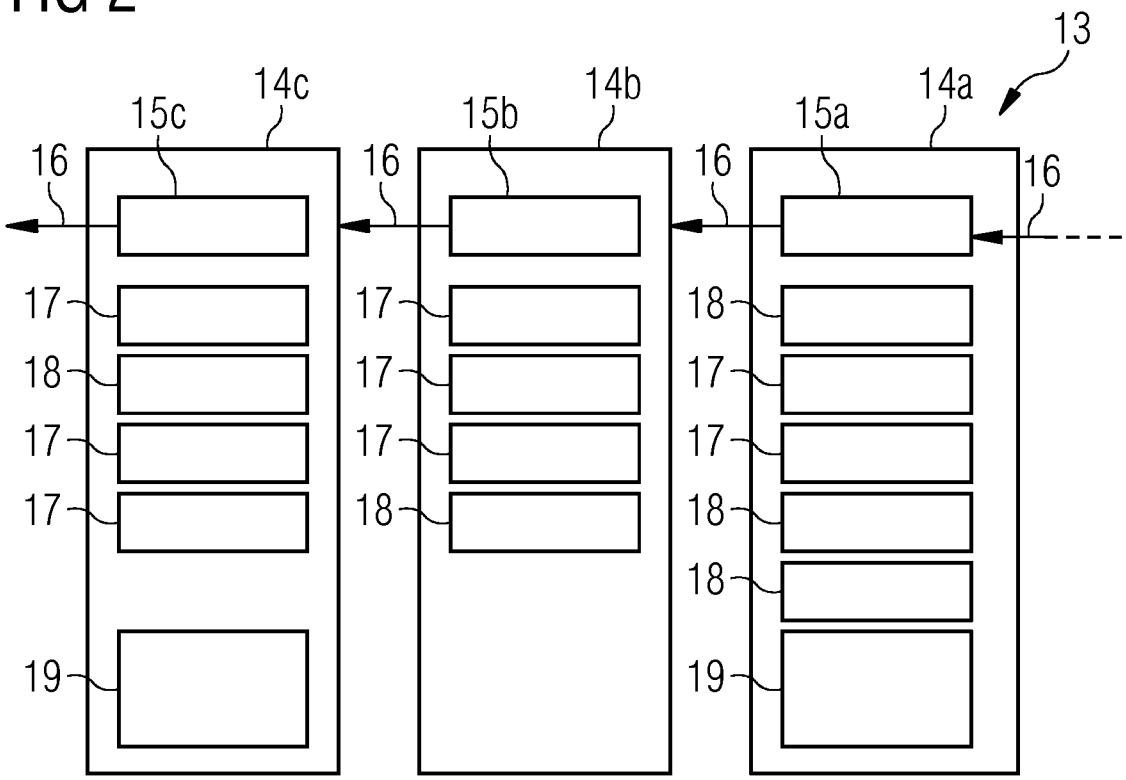

13
14c
15c
14b
15b
14a
15a
16
16
16
16
17
18
17
17
17
17
17
18
18
17
17
17
18
18
18
19
19

FIG 3

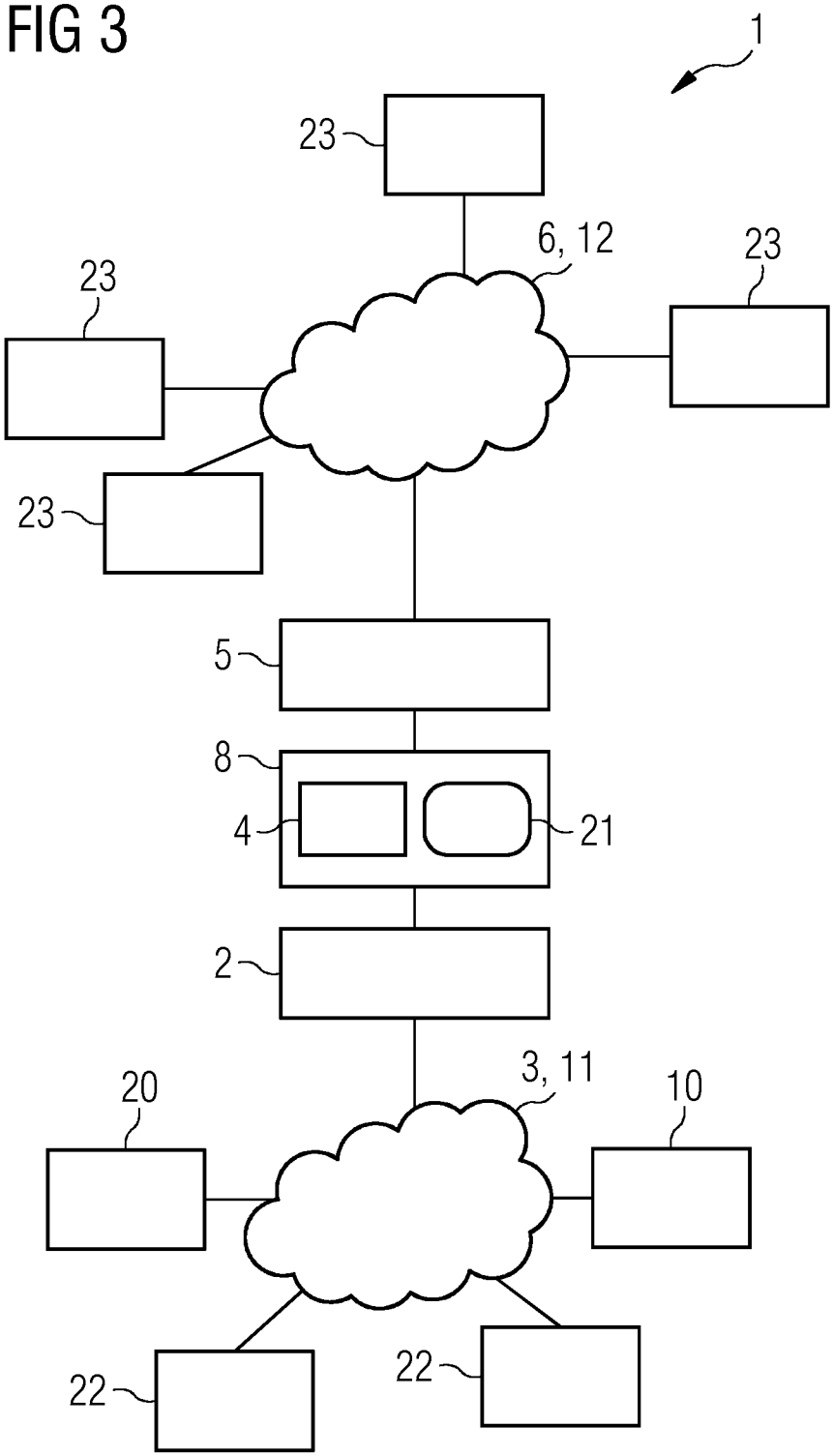
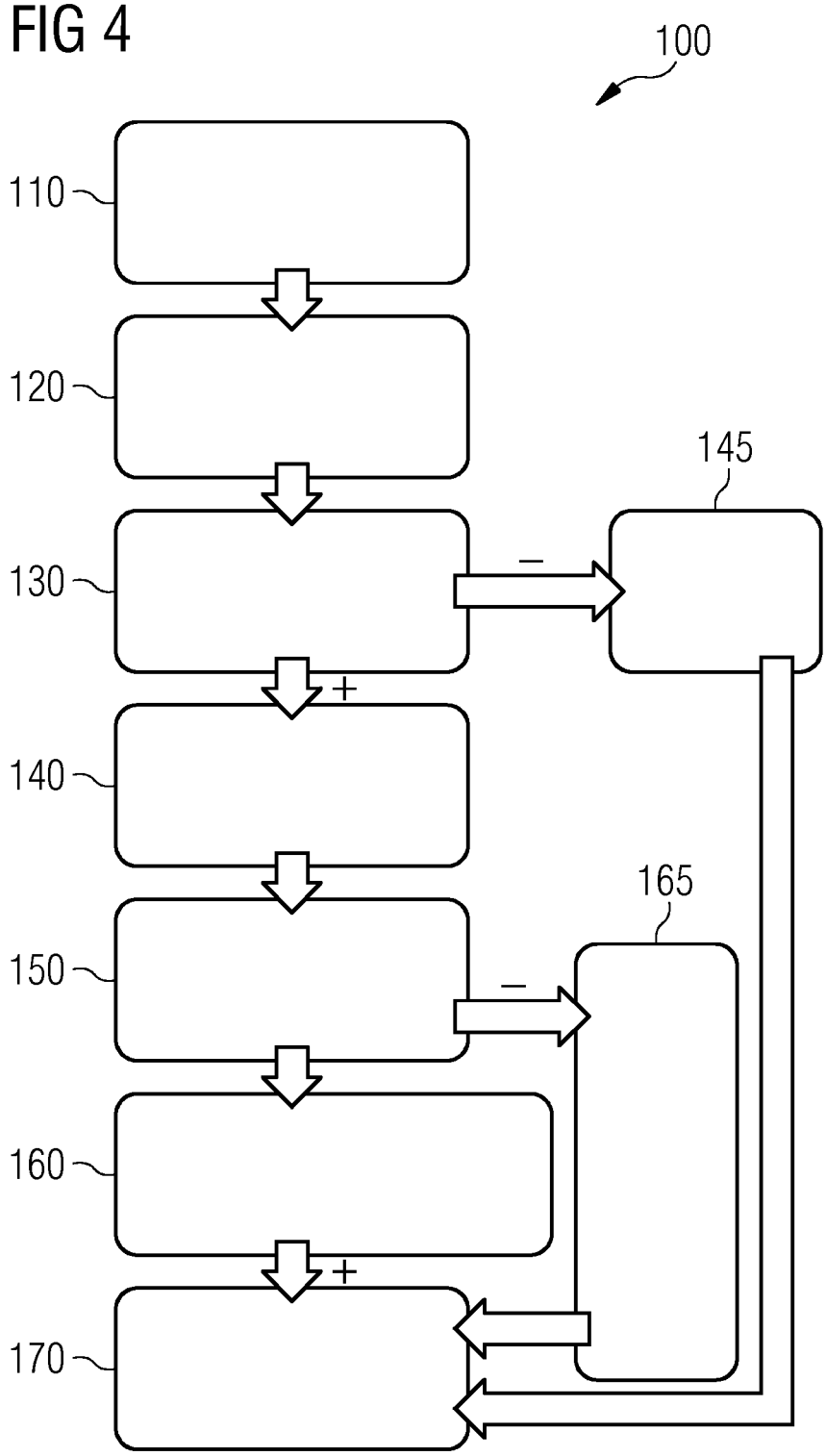


FIG 4



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2018/071879

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD. H04L9/30

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

B. FIELDS SEARCHED

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

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2017/063789 A1 (MARCINKOWSKI JAMES M [US] ET AL) 2 March 2017 (2017-03-02) abstract; claims 1,8,14; figure 1B paragraphs [0007], [0008], [0014], [0015], [0026], [0027], [0029] - [0031]	1-16
X	US 2015/312188 A1 (WHITE STEVEN [US] ET AL) 29 October 2015 (2015-10-29) abstract; claims 1,8; figures 1-3 paragraphs [0022] - [0025], [0029] - [0042]	1-16

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 October 2018	12/10/2018

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Wolters, Robert

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2018/071879

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WENTING LI ET AL: "Towards Scalable and Private Industrial Blockchains", PROCEEDINGS OF THE ACM WORKSHOP ON BLOCKCHAIN, CRYPTOCURRENCIES AND CONTRACTS, 2 April 2017 (2017-04-02), pages 9-14, XP055397747, DOI: 10.1145/3055518.3055531 ISBN: 978-1-4503-4974-1 abstract Section 3. -----	1-16
A	US 2017/046638 A1 (CHAN PAUL MON-WAH [CA] ET AL) 16 February 2017 (2017-02-16) abstract; figures 1,4 paragraphs [0073] - [0075], [0080], [0096], [0105], [0106] -----	1-16

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2018/071879

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2017063789 A1	02-03-2017	US 2017063789 A1	02-03-2017
		WO 2016019293 A1	04-02-2016
US 2015312188 A1	29-10-2015	NONE	
US 2017046638 A1	16-02-2017	CA 2938519 A1	13-02-2017
		CA 2938530 A1	13-02-2017
		CA 2938754 A1	13-02-2017
		CA 2938756 A1	13-02-2017
		CA 2938757 A1	13-02-2017
		CA 2938758 A1	13-02-2017
		CA 2938759 A1	13-02-2017
		CA 2948106 A1	09-05-2017
		CA 2948116 A1	09-05-2017
		CA 2948239 A1	10-05-2017
		CA 2948241 A1	10-05-2017
		US 2017046526 A1	16-02-2017
		US 2017046638 A1	16-02-2017
		US 2017046651 A1	16-02-2017
		US 2017046652 A1	16-02-2017
		US 2017046664 A1	16-02-2017
		US 2017046693 A1	16-02-2017
		US 2017046694 A1	16-02-2017
		US 2017046698 A1	16-02-2017
		US 2017046709 A1	16-02-2017
		US 2017046792 A1	16-02-2017
		US 2017046799 A1	16-02-2017
		US 2017046806 A1	16-02-2017
		US 2017048216 A1	16-02-2017