



(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:

PCT/EP2018/052990

(22) International Filing Date:

07 February 2018 (07.02.2018)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

17305152.5 10 February 2017 (10.02.2017) EP

(71) Applicant: **NOKIA TECHNOLOGIES OY** [FI/FI];
Karaportti 3, 02610 Espoo (FI).

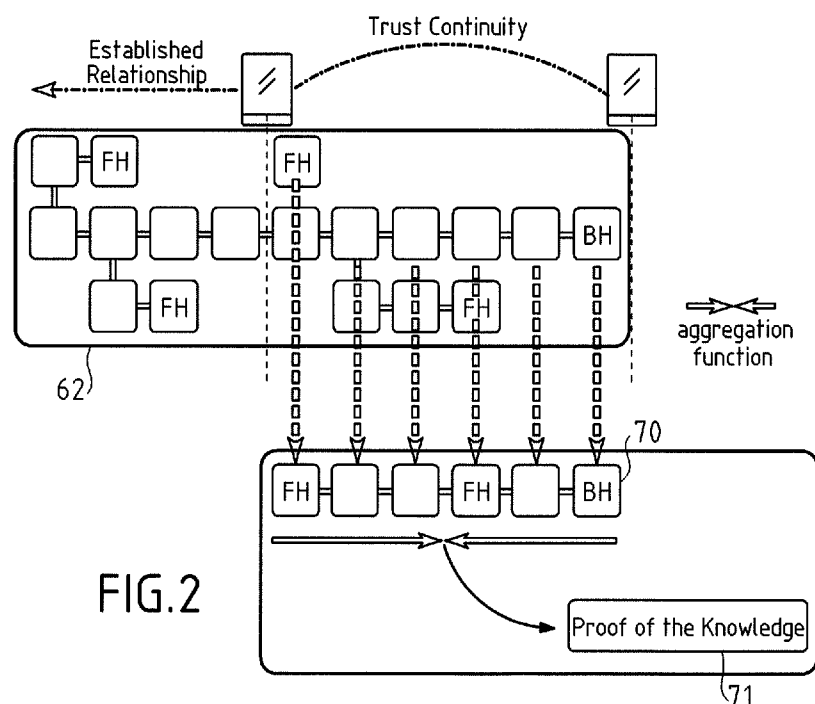
(72) Inventors: **SIGNORINI, Matteo**; Alcatel-Lucent Bell
Labs France, Centre de Villardceaux, Route de Villejust,
91620 Nozay (FR). **DI PIETRO, Roberto**; Alcatel-Lucent
Bell Labs France, Centre de Villardceaux, Route de Ville-

just, 91620 Nozay (FR). **KANOUN, Wael**; Alcatel-Lucent
Bell Labs France, Centre de Villardceaux, Route de Villejust,
91620 Nozay (FR).

(74) Agent: **MOUNEY, Jerome**; Alcatel-Lucent International,
Patent Business, Nokia Paris Saclay site, Route de Villejust,
91620 Nozay (FR).

(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.

(54) Title: BLOCKCHAIN-BASED AUTHENTICATION METHOD AND SYSTEM



(57) Abstract: A method and system of authenticating a device within a network of connected devices that share a ledger of transactions between them under the form of exchanged blockchain messages and comprising: computing a PoK chain (70) based on the enhanced blockchain, receiving an authentication request from an application or a device, the authentication request including one or more PoKs (71), retrieving from the PoK database the PoK chain (70) corresponding to the application or device identified in the authentication request; computing a PoK (71) based on the PoK chain (70) retrieved from the PoK database, comparing it with the PoK (71) included in the authentication request, and if they match, validating the authentication request.

(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))*

Blockchain-based authentication method and system

Field of the invention

The invention relates to the technical field of security within a network of
5 connected devices implementing blockchain technology.

Background

The actual model for device identification and authentication in the Internet is based on atomic protocols where a prover and a verifier exchange
10 information and try to verify them. However, the same information exchanged during the identification protocol can be modified/misused and should not be trusted. This is mainly due to two aspects. First, it is currently cumbersome to physically and permanently tie a device to its identity and, second, the identity itself should not be trusted as it can be easily hacked.

15 To solve the above issues, authentication protocols are usually employed. They can be split to centralized and de-centralized. On the one hand, centralized protocols are based on trusted third parties (such as certification authorities) which are responsible for pairing digital identities to secret data which are given to devices. With this approach, thanks to the trustworthiness in the certification
20 authorities, once an identity is claimed by digitally signing a message, the device sending the message is recognized and authenticated as it is assumed that the secret used to sign the message (e.g. the private key in asymmetric cryptographic solutions, like for RSA based signatures) is kept private and is never accessed by other devices.

25 On the other hand, decentralized authentication protocols try to avoid trusted third parties. The computation and/or the information is then distributed among different devices which must agree on the trustworthiness of a given identity. This approach solves the problem of outsourcing the trust to an external entity by avoiding the exposition of sensitive/private information. However, it is
30 hard to build a trusted network as it is not possible to detect if all the devices are cooperating/working as expected. To address this problem, over the last years,

remote attestation techniques tried to solve the problem of remotely recognizing untrusted devices (such as WO2014141074 or US8966249) via hardware or software approaches. These techniques are based on strong assumptions and, as such, they do not solve the problem but rather make it harder to be accomplished.

5 More recently, blockchain technology was devised and published (originally in the context of Bitcoin) allowing to securely share or process data between multiple parties over a network of non-trusted peers.

Summary

10 The invention provides for blockchain-based authentication methods and systems by building a self-enforced and self-managed network where devices can control the behavior and the trustworthiness of each other without the need of central authorities or software and hardware elements which are assumed secure and trusted by design.

15 The basic idea of the invention consists in providing a decentralized authentication protocol that leverages multiple blockchain distributed ledgers to build a trust continuity factor. To do this, this invention defines a Proof Of Knowledge (PoK) blockchain. This PoK blockchain contains a history of the past blockchain activities and represents a network footprint that can only be recognized/verified by the other peers in the same network. The PoK blockchain is
20 built and updated locally on each device over time, as the blockchain changes. An application or device may be authenticated by sending the PoK.

The invention provides a device to be connected to a network where connected devices share a ledger of transactions between them under the form of a main blockchain composed of blocks, each block containing a timestamp and a link
25 to a previous block, such device comprising:

a chain manager being configured to add forked chains extracted at the device to a main blockchain in order to build an enhanced blockchain and to store the enhanced blockchain in a chain database;

the device further comprising:

30 a Proof-of-Knowledge – i.e. PoK - manager comprising:

- a PoK builder being configured to compute at least one PoK chain based at least on the enhanced blockchain, a PoK chain being composed of PoK blocks, each PoK block containing a timestamp and a link to a previous PoK block,
- a PoK database storing the PoK chain;
- 5 an authentication manager configured to
- receive an authentication request from an application or a device, the authentication request including at least one PoK,
- retrieve, from the PoK database, at least one PoK chain corresponding to the application or device identified in the authentication request;
- 10 send the at least one PoK included in the authentication request and the at least one PoK chain retrieved from the PoK database to an authentication validator, the authentication validator being configured to compute at least one PoK based on the at least one PoK chain retrieved from the PoK database, compare it with the at least one PoK included in the authentication request, and if they match, validate the
- 15 authentication request.

- In embodiments, the device further comprises a miner and a fork broadcast, the miner being configured to analyze received blockchains messages, build a new block according to the received blockchains messages, and send the new block to the fork broadcast and to all the other devices within the network,
- 20 the fork broadcast being configured to receive blocks from the miner and from other devices within the network and to extract forked chains from received blocks.

- In embodiments, the PoK builder is configured to aggregate, using an aggregation function, each forked chain head of the enhanced block chain with the block of the main chain they are attached to so as to form a single PoK block, the
- 25 PoK blocks forming the PoK chain.

In embodiments, the aggregation function is a Hash function.

In embodiments, the aggregation function is a bitwise XOR.

In embodiments, the device further comprises an authentication database storing for each device or application a time of last authentication, and

wherein, the authentication manager is configured to retrieve from the authentication database the time of last authentication of the application or device, and forward it to the authentication validator,

and wherein, the authentication validator computes the PoK by aggregating the
5 blocks of the PoK chain retrieved from the PoK database having a timestamp comprised between the time of last authentication of the application or device and the current time.

In embodiments, the request for authentication includes a PoK policy including a list of PoK chains required to compute the PoK and to validate the
10 authentication request,

the device further comprising a cooperation manager configured to interact with other devices within the network in order to retrieve additional PoK chains,
and wherein, the authentication manager is further configured, if the PoK database of the device does not include all the PoK chains required in the PoK policy, to send
15 a request for additional PoK chains to the cooperation manager.

In embodiments, the request for additional PoK chains comprises all PoK chains stored in the PoK database of the device, the PoK chains included in said request being intended to be used by the device receiving said request for authenticating the sender of said request.

20 The invention also provides a method of authenticating a device within a network of connected devices that share a ledger of transactions between them under the form of a blockchain composed of blocks, each block contains a timestamp and a link to a previous block, the method comprising:

extracting forked chains from received blocks;
25 adding all forked chains to a main blockchain in order to build an enhanced blockchain;
storing the enhanced blockchain in a chain database;
computing at least one PoK chain based at least on the enhanced blockchain, a PoK chain being composed of PoK blocks, each PoK block containing a timestamp and a
30 link to a previous PoK block,

receiving an authentication request from an application or a device, the authentication request including at least one PoK,

retrieving from the PoK database at least one PoK chain corresponding to the application or device identified in the authentication request;

- 5 computing at least one PoK based on the at least one PoK chain retrieved from the PoK database, comparing it with the at least one PoK included in the authentication request, and if they match, validating the authentication request.

10 In embodiments, the method further comprises analyzing received blockchains messages, building a new block according to the received blockchains messages, and sending the new block to all the other devices within the network.

In embodiments, the request for authentication includes a PoK policy including a list of PoK chains required to compute the PoK and to validate the authentication request,

the method further comprising:

- 15 if the PoK database does not include all the PoK chains required in the PoK policy, retrieving additional PoK chains from other devices within the network,

The method further comprises a computer program comprising executable code that causes a computer to perform all the steps of a method as described above when executed.

- 20 This invention enables the creation of trust relationships kept alive by continuously exchanging information about the network activity over time. This allows the establishment of self-enforced and self-managed networks without the need of any trusted third party such as certification authorities. Another feature is that this trust relationship can be verified in a totally distributed and decentralized
25 manner. The trust relationship between two devices is defined in an initial setup process (that can be done by the device owner or an administrator) and it is then seamlessly kept alive by them (without any security assumption) for as long as they remain in the same network or context. Once one of the two devices leaves the network, it gets de-authenticated and if it comes back it will be required again to
30 pass the initial setup process.

To avoid central point of trust, such as certification authorities, all the other solutions leverage distributed approaches where each device cooperates in controlling the network. However, in order to prove its trustworthiness, each device has to authenticate itself and to prove the integrity of the data being provided. To do so, they need strong security assumptions on hardware or software elements that are exploited to store cryptographic keys used to sign and/or encrypt all the communications.

This invention builds trusted communications without any security assumption on the involved devices. Indeed, it is impossible for a device to alter the blockchain or to forge fake forks. This also avoids any need of encryption or signature primitives.

Brief description of the drawings

These and other aspects of the invention will be apparent from and elucidated with reference to the embodiments described hereinafter, by way of example, with reference to the drawings.

Figure 1 is a representation of a network with connected devices implementing the blockchain technology.

Figure 2 illustrates the proof of knowledge (PoK) construction according to the invention.

Figure 3 is a functional representation of a connected device that implements the blockchain-based authentication method according to the invention.

Figure 3b is a functional representation of an enhanced blockchain manager according to an embodiment of the invention

Figure 4 illustrates the PoK chain computation according to the invention.

Figure 5 illustrates the validation step according to the invention.

Figure 6 illustrates the proof of knowledge database.

Detailed description of the embodiments

Figure 1 is a representation of a network 10 with connected devices 11 implementing the blockchain technology. Network 10 may be Wifi, 3G, LTE, Bluetooth, RFID/NFC, wired connections, or any type of network that supports protocols for exchanges of messages between connected devices over connections

5 13. The messages being exchanged can belong to one or multiple blockchain-based applications on different levels such as HTTP/FTP based applications (to keep track of network traffic), SSH/Telnet/RDP/VNC/VPN based applications (to keep track of remote accesses), RFID/NFC based applications (to keep track of physical interactions), Wi-Fi application, Bluetooth application, etc. Each application or

10 protocol to monitor is associated with at least a blockchain. Different blockchains may be associated with the same application or protocol.

Each connected device 11 maintains all the ledgers (i.e. the blockchains) which are shared between connected devices and to which it has access.

Each connected device 11 can contain a miner 20 depending on its

15 resources and computational power. Messages received at the miner 20 contain standard blockchain transactions which are collected to build the next block within the mainstream chain. Each block contains a timestamp and a link to a previous block. Once a new block has been built by the miner 20, it is sent in broadcast to all the other devices. Each new block built by the miner 20 of the device or received by

20 another miner is added to the blockchain and written in a blockchain database 21. Once a device receives one or multiple blocks which have been built by other devices, it compares the new blocks with the one locally stored. If they do not match, and the received chain is longer than the local one, the local chain is labeled as a fork. Once a fork is detected, the miner discards it and overwrites a portion/all

25 of the blockchain with the new received one. Forks are discarded as they create concurrent mining with parallel branches from the main chain 60. These parallel branches, may lead to conflicting transactions which, in blockchain-based contexts, is particularly problematic.

Due to delays in the network, devices belonging to a same group

30 (associated to a same context) see blockchain changes in the same way (receive

blockchain updates in the same order), while devices from other groups (belonging to other contexts) see blockchain changes differently (receive blockchain updates in different orders).

A novel authentication method based on the blockchain technology and exploiting the above mentioned observation is provided.

A connected device 11 according to the invention is illustrated on Figure 3. The device contains the miner 20 and the blockchain database 21. In addition, it contains an enhanced blockchain manager 4 and a proof of knowledge (PoK) manager 5.

In reference to figure 3b, the enhanced blockchain manager 4 contains:

- a transaction filter 40 that intercepts blockchain messages (M11) and forwards them to both the miner (with M12 messages), and a chain manager 42 with M13 messages. This parallel processing allows the un-interrupted (i.e. not modified or slowed down) handling of standard blockchain protocol by the miner and the blockchain database, through M14 message. The transaction filter collects M11 metadata such as the message sender, the recipient, the timestamp, and discards duplicated messages.
- a fork broadcast 41, added to the miner, extracts any forked chain (M15) before it is discarded and overwritten by the miner.
- a chain manager 42 receives M13 messages from the transaction filter, and M15 messages from the fork broadcast. The chain manager computes from M13 and M15 an enhanced blockchain composed by the standard blockchain, and the forked chains. As M13 and M15 do not describe the whole chain but rather updates on top of it, the chain manager retrieves through M16 the main blockchain 60 from the chain database 43. Then it merges to the main blockchain 60 all the information obtained with M13 and/or M15. Once the enhanced blockchain has been computed, it is sent back through M16 to be stored in the chain database 43. M13 and M15 do not necessarily reach the chain manager at the same time. Hence, the chain manager can receive either M13 messages (each time a standard blockchain message has

been received) or M15 messages (each time M12 forces the miner to discard previous forks).

The PoK manager 5 comprises:

5 a PoK builder 54 being configured to load the up to date version of the enhanced blockchain from the chain database 21, and compute a PoK chain 70 based on the forked chained heads (the latest block in each forked chain) and on the main blockchain, and to send the PoK chain 70 to an authentication manager 59 in response to a request of authentication;

10 a PoK database 55 storing all the PoK chains, one for each application or/and protocol being monitored by the blockchains;

the authentication manager 59 being configured to receive an authentication request including a proof of knowledge value (PoK) 71, and load PoK chains from the PoK database 55;

15 an authentication validator 58 configured to compare the information obtained from the authentication manager 59 to control if the PoK received is the same as the one internally stored within the PoK database 55 and if they match, validating the authentication request.

As illustrated by figure 2, the PoK builder 54 loads (M1) one enhanced blockchain for each application or protocol to monitor. The PoK builder 54 first
20 reduces the complexity/size of the enhanced blockchains by aggregating and consolidating the forked chains with an aggregation function (e.g. a Hash function, a bitwise XOR, etc.). All the devices use the same aggregating function. Then it again aggregates the remaining forked chain heads (FHs) to obtain the PoK chain 70 which is the original blockchain merged with FH information.

25 Figure 4 illustrates the PoK chain 70 built by the PoK builder 54. Starting from the enhanced blockchain, the forked chain heads FH are collected and exploited to build, together with the main blockchain blocks, a proof of knowledge (PoK). The enhanced blockchain 62 stored in chain database 21 is composed of the main blockchain 60 headed by a block head BH, and other forked chains 61, each
30 one headed by its own fork head block FH. Each forked chain 61 of the enhanced

block chain 62 is aggregated using the aggregation function into a single forked block 73. Then, all the forked blocks are aggregated with their origin block in the main chain 60 so as to form a single PoK block, the PoK blocks forming the PoK chain 70.

5 All the PoK chains 70, one for each application or protocol being monitored by the blockchains, are then stored (M2) within the PoK database 55 as shown in Figure 6.

The authentication manager 59 receives authentication requests from internal/external applications and verifies them. Upon receiving an authentication
10 request the authentication manager 59 first loads (M4) the PoK chains from the PoK database 55 and then sends them (M6) to the authentication validator 58.

The number of PoK chains required to compute the PoK is embedded within the PoK policy which is loaded within the authentication request as shown in Figure 4 (labeled as M3).

15 The device further comprises an authentication database 56 storing a list of PoK for each device or application . During the authentication validation, the authentication manager 59 retrieves (M7) from the authentication database 56 the list of PoK to provide for authentication of the application. In particular, the authentication database 56 stores for each device or application a time of last
20 authentication. During the authentication validation, the authentication manager 59 retrieves from the authentication database 56 the time of last authentication of the application or device, and forward it to the authentication validator 58.

As illustrated by figure 5, the authentication validator 58 compares the PoK received in the authentication request with the PoK computed from the PoK chain
25 stored within the PoK database 55. If they match, the authentication request is validated. To that end, the authentication validator 58 computes, for the PoK chain for the PoK chain 70 retrieved from the PoK database 55, an expected PoK 71 by aggregating the blocks of the PoK chain 70 having a timestamp comprised between the time of last authentication and the current time. The authentication validator
30 58 then compares the PoK 71 included in the authentication request and the PoK 71

computed with the PoK chain 70 retrieved from the PoK database 55. If they are identical, the authentication validator 58 validates the authentication request.

If some of the PoK chain 70 requested for authentication are not stored within the verifier's PoK database 55, the authentication manager 59 sends a request (message M5) to a cooperation manager 53.

The cooperation manager 53 interacts (M8) with other devices within the network in order to retrieve additional PoK information. The request for additional PoK information has to be authenticated. Thus, the authentication manager 59 writes within M5 all the information stored in the PoK database 55. The cooperation manager 53 then use the information sent in the M5 message to build an authentication request sent to other devices. Once all the external PoK information are retrieved by the cooperation manager 53, they are sent back to the authentication manager 59. Each time a new block is created it is sent to all the devices. However, due to delays in the network, devices belonging to a same group (associated to a same context) will receive the new blocks in the same order, thus being able to keep building the same enhanced blockchain 62, which will make them able to identify as a group, while devices from other groups will receive the new blocks in different orders and will build a different enhanced blockchain 62 which will make them able to identify as another group.

For example, in a peer to peer network messages are not collected in the same order due to the network latency. As such, devices can receive messages in different orders. Hence, this information can be used to distinguish between devices which are, as an example, connected to the same local network from devices which are remotely connected.

As another example, two devices will eventually agree on the blockchain but on the short term they can disagree leading to a fork. Forks can also be exploited by malicious users. Indeed, such users may try to force victim devices in accepting and using fake information. During the attack, the victim devices (which are now disconnected from the network due to the attack) will collect and share some info that will make their enhanced blockchain different from the enhanced

blockchain of another group. Hence, this info may be used to distinguish between a device belonging to said group and other devices.

All devices belonging to a same group (associated to a specific context) share the same enhanced blockchain and as a consequence the same PoK. Hence,
5 devices can prove to other devices that they belong to the same group by comparing their PoKs. A device is able to check whether another device belongs to his own group by comparing the received PoK with the PoK that he computes based on the PoK chain retrieved from his PoK database.

Elements such as the miner, the transaction filter, the fork broadcast, the
10 chain manager, the PoK manager, the PoK builder, the authentication manager, the authentication validator, or the cooperation manager, could each be e.g. hardware means like e.g. an ASIC, or a combination of hardware and software means, e.g. an ASIC and an FPGA, or at least one microprocessor and at least one memory with software modules located therein.

15 The invention is not limited to the described embodiments. The appended claims are to be construed as embodying all modifications and alternative constructions that may occur to one skilled in the art, and which fairly fall within the basic teaching as set forth herein.

The use of the verb “to comprise”, “to include” or “to contain” and their
20 conjugations does not exclude the presence of elements or steps other than those stated in a claim. Furthermore, the use of the article “a” or “an” preceding an element or step does not exclude the presence of a plurality of such elements or steps.

In the claims, any reference signs placed between parentheses shall not be
25 construed as limiting the scope of the claims.

CLAIMS

1. A device (11) to be connected to a network (10) where connected devices share a ledger of transactions between them under the form of a main blockchain (60) composed of blocks, each block containing a timestamp and a link to a previous block, such device comprising:
- 5 a chain manager (42) being configured to add forked chains (61) extracted at the device to a main blockchain (60) in order to build an enhanced blockchain (62) and to store the enhanced blockchain in a chain database (43);
- the device further comprising:
- 10 a Proof-of-Knowledge – i.e. PoK - manager (5) comprising:
- a PoK builder (54) being configured to compute at least one PoK chain (70) based at least on the enhanced blockchain (62), a PoK chain (70) being composed of PoK blocks, each PoK block containing a timestamp and a link to a previous PoK block,
- a PoK database (55) storing the PoK chain (70);
- 15 an authentication manager (59) configured to
- receive an authentication request from an application or a device, the authentication request including at least one PoK (71),
- retrieve, from the PoK database (55), at least one PoK chain (70) corresponding to the application or device identified in the authentication request;
- 20 send the at least one PoK (71) included in the authentication request and the at least one PoK chain (70) retrieved from the PoK database (55) to an authentication validator (58),
- the authentication validator (58) being configured to compute at least one PoK (71) based on the at least one PoK chain (70) retrieved from the PoK database (55),
- 25 compare it with the at least one PoK (71) included in the authentication request, and if they match, validate the authentication request.
2. The device of claim 1, further comprising a miner (20) and a fork broadcast (41),

the miner (20) being configured to analyze received blockchains messages (13), build a new block according to the received blockchains messages (13), and send the new block to the fork broadcast (41) and to all the other devices within the network,

- 5 the fork broadcast (41) being configured to receive blocks from the miner (20) and from other devices within the network and to extract forked chains (61) from received blocks.

3. The device of claim 1 or 2, wherein the PoK builder (54) is configured to
10 aggregate, using an aggregation function, each forked chain head of the enhanced block chain (62) with the block of the main chain they are attached to so as to form a single PoK block, the PoK blocks forming the PoK chain (70).

4. The device of claim 3, wherein the aggregation function is a Hash function.
15

5. The device of claim 3, wherein the aggregation function is a bitwise XOR.

6. The device of any one of claims 1 to 5, further comprising an authentication database (56) storing for each device or application a time of last authentication,
20 and

- wherein, the authentication manager (59) is configured to retrieve from the authentication database (56) the time of last authentication of the application or device, and forward it to the authentication validator (58),
and wherein, the authentication validator (58) computes the PoK (71) by
25 aggregating the blocks of the PoK chain (70) retrieved from the PoK database (55) having a timestamp comprised between the time of last authentication of the application or device and the current time.

7. The device of any one of claims 1 to 6, wherein, the request for authentication includes a PoK policy including a list of PoK chains required to compute the PoK (71) and to validate the authentication request, the device further comprising a cooperation manager (53) configured to interact with other devices within the network in order to retrieve additional PoK chains (70), and wherein, the authentication manager (59) is further configured, if the PoK database (55) of the device does not include all the PoK chains (70) required in the PoK policy, to send a request for additional PoK chains to the cooperation manager (53).

8. The device of any one of claims 1 to 7, wherein, the request for additional PoK chains comprises all PoK chains (70) stored in the PoK database (55) of the device, the PoK chains (70) included in said request being intended to be used by the device receiving said request for authenticating the sender of said request.

9. A method of authenticating a device within a network (10) of connected devices (11) that share a ledger of transactions between them under the form of a blockchain (60) composed of blocks, each block contains a timestamp and a link to a previous block, the method comprising:

extracting forked chains (61) from received blocks;
adding all forked chains (61) to a main blockchain (60) in order to build an enhanced blockchain (62);
storing the enhanced blockchain in a chain database;
25 computing at least one PoK chain (70) based at least on the enhanced blockchain (62), a PoK chain (70) being composed of PoK blocks, each PoK block containing a timestamp and a link to a previous PoK block,
receiving an authentication request from an application or a device, the authentication request including at least one PoK (71),
30 retrieving from the PoK database (55) at least one PoK chain (70) corresponding to the application or device identified in the authentication request;

computing at least one PoK (71) based on the at least one PoK chain (70) retrieved from the PoK database (55), comparing it with the at least one PoK (71) included in the authentication request, and if they match, validating the authentication request.

5

10. The method of claim 9 further comprising analyzing received blockchains messages (13), building a new block according to the received blockchains messages (13), and sending the new block to all the other devices within the network.

10 11. The method of claim 9 or 10, wherein the request for authentication includes a PoK policy including a list of PoK chains required to compute the PoK (71) and to validate the authentication request,
the method further comprising:

15 if the PoK database (55) does not include all the PoK chains (70) required in the PoK policy, retrieving additional PoK chains (70) from other devices within the network,

12. A computer program comprising executable code that causes a computer to perform all the steps of a method in accordance with any one of claims 9 to 11
20 when executed.

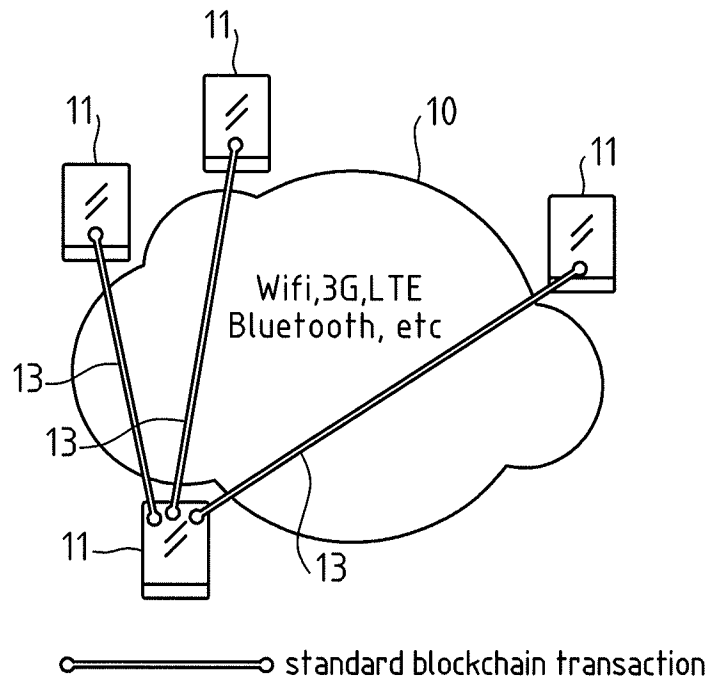


FIG. 1

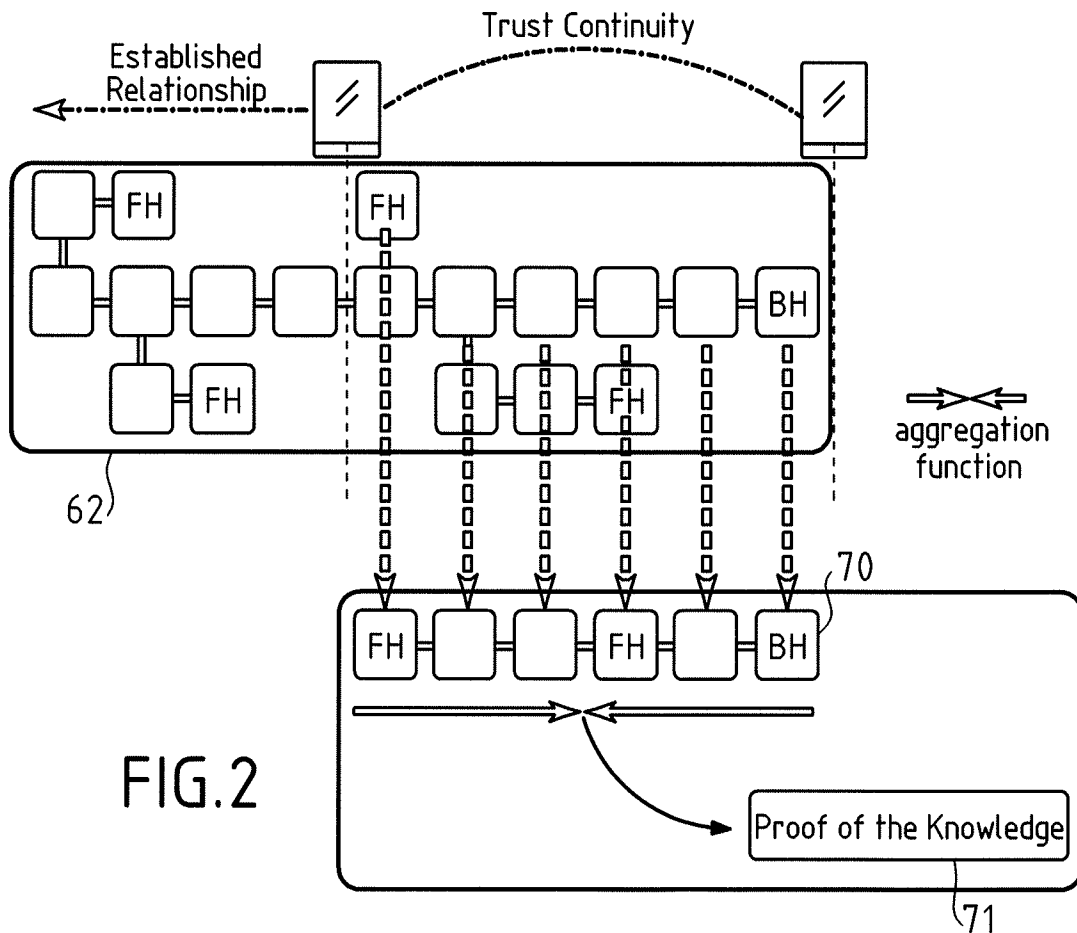


FIG. 2

2/4

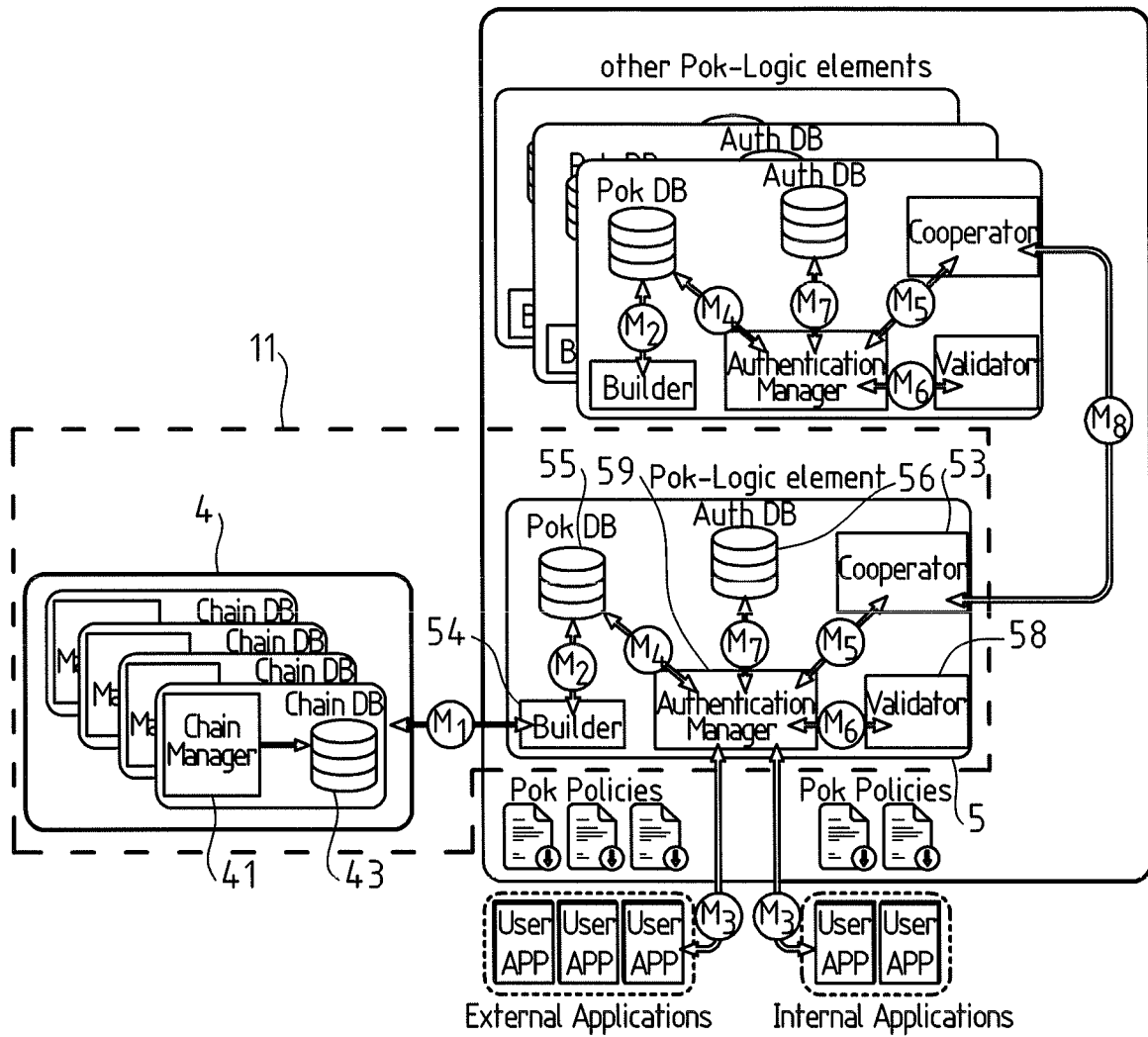


FIG. 3a

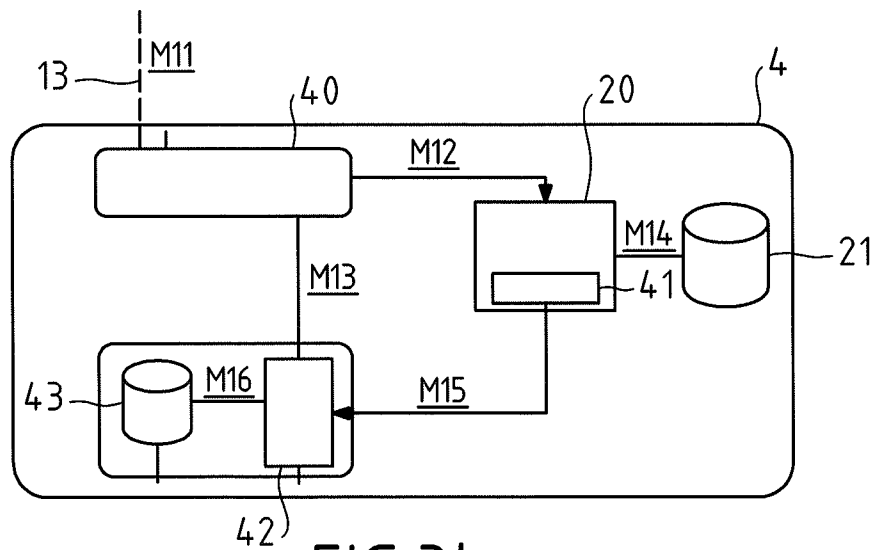


FIG. 3b

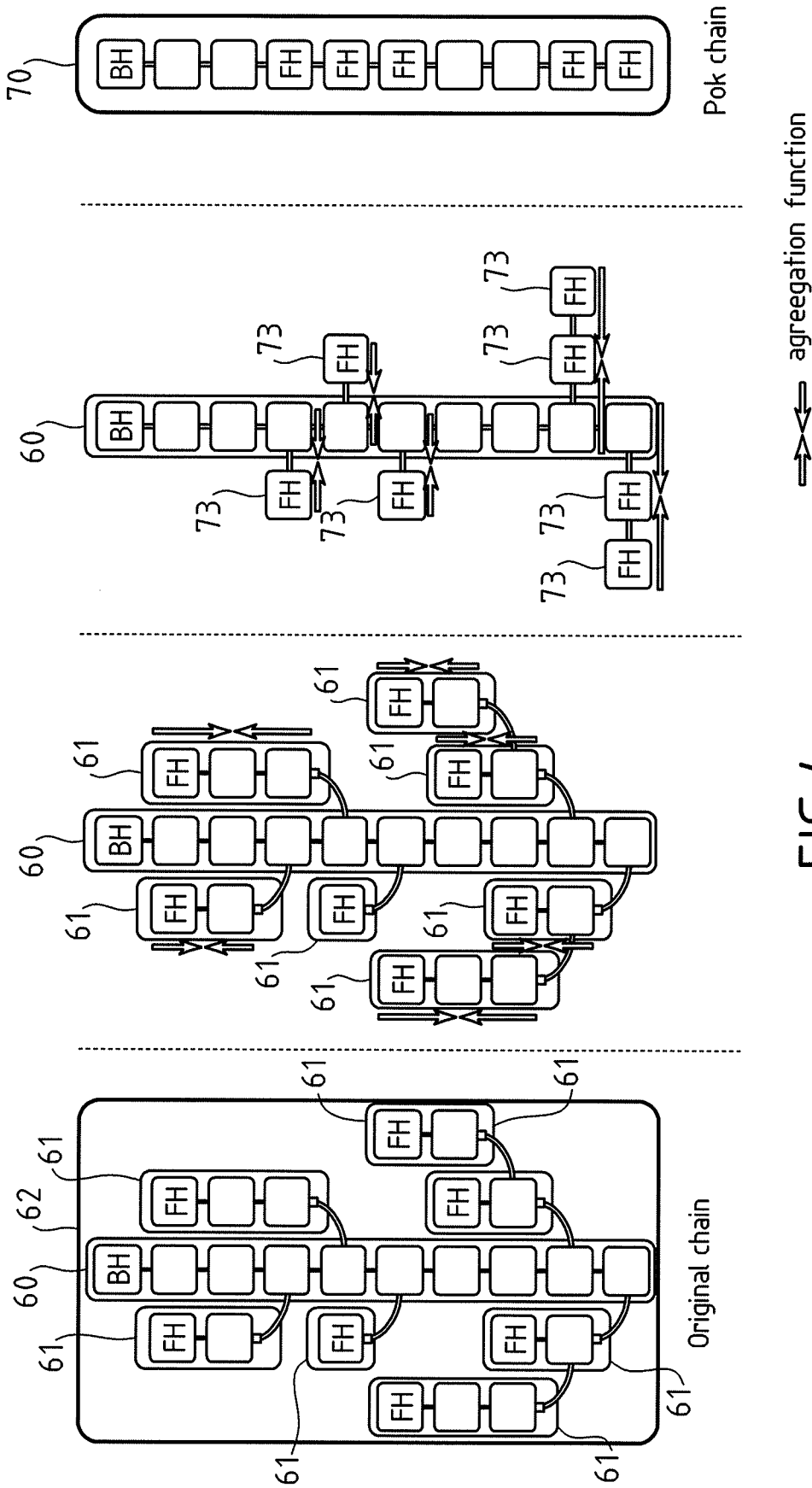


FIG.4

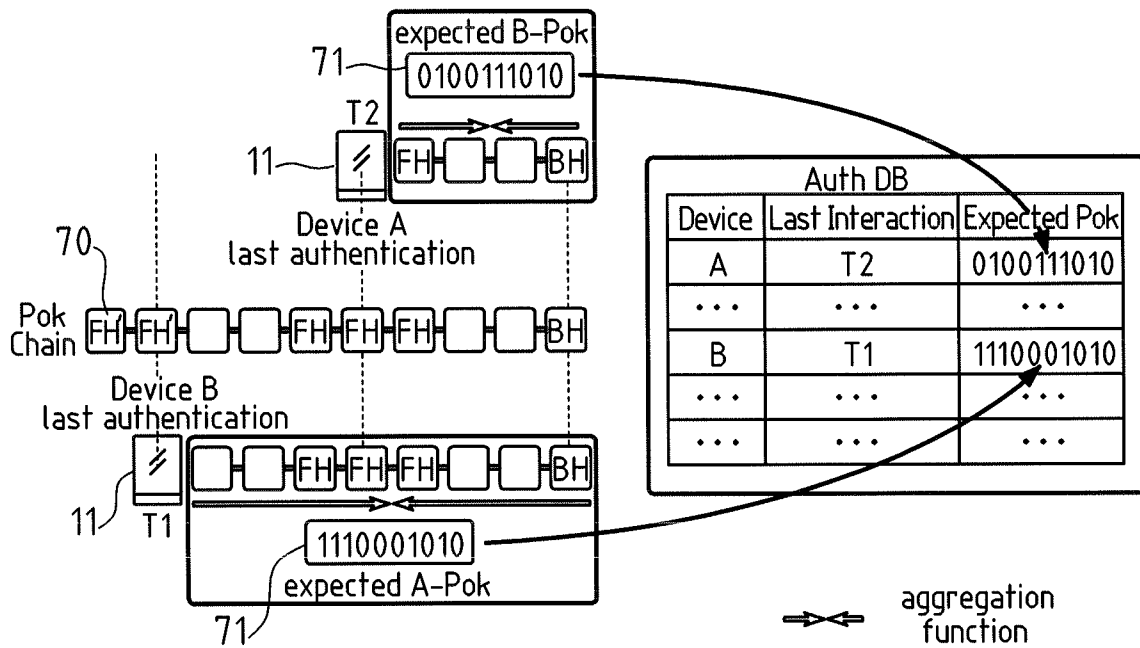


FIG. 5

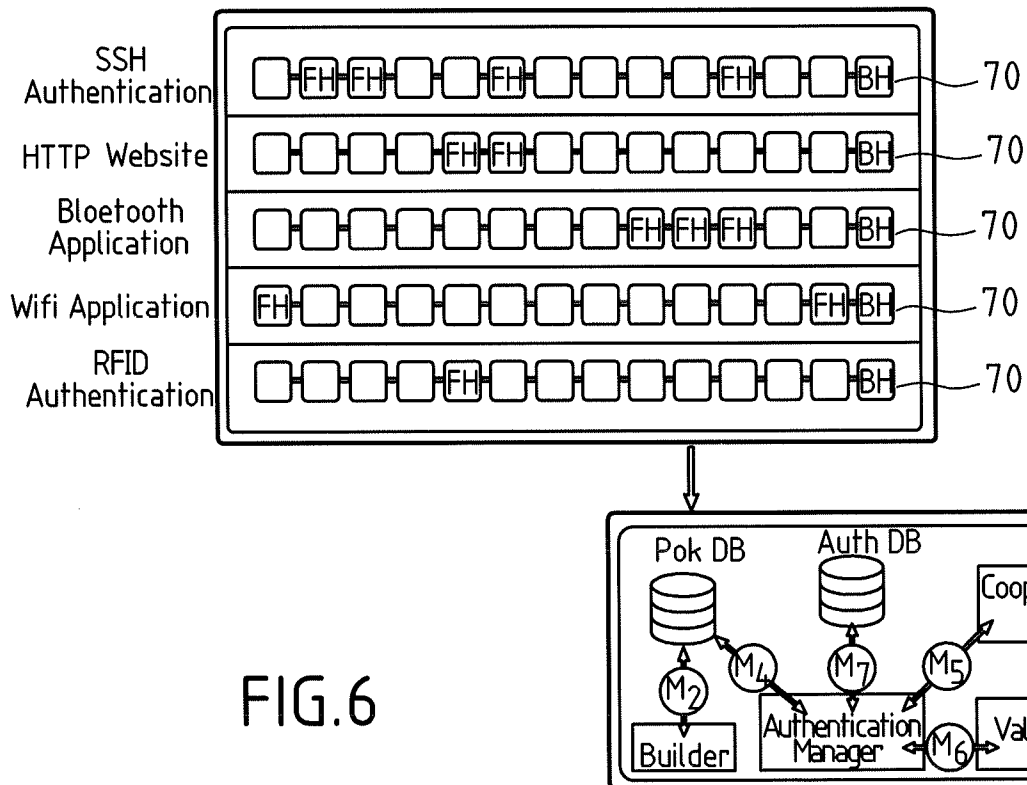


FIG. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2018/052990

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/32
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
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 2016/162897 A1 (FEENEY PATRICK JOSEPH [US]) 9 June 2016 (2016-06-09) abstract paragraph [0004] paragraph [0031] - paragraph [0087]; figures 1A,1B,3	1-12
A	Melanie Swan: "Blockchain: Blueprint for a New Economy" In: "Blockchain: Blueprint for a New Economy", 8 February 2015 (2015-02-08), O'Reilly, XP055279098, ISBN: 978-1-4919-2049-7 page 27, line 1 - page 67, line 2 ----- -/-	1-12



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

20 April 2018

Date of mailing of the international search report

04/05/2018

Name and mailing address of the ISA/

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

Authorized officer

Spranger, Stephanie

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2018/052990

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	AHMED KOSBA ET AL: "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20150721:040253, 21 July 2015 (2015-07-21), pages 1-32, XP061018923, page 4, right-hand column, line 46 - page 10, right-hand column, line 37 -----	1-12

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2018/052990

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2016162897	A1	09-06-2016	NONE
