



- (51) **International Patent Classification:**
G06Q 30/02 (2012.01)
- (21) **International Application Number:**
PCT/GB2021/050238
- (22) **International Filing Date:**
03 February 2021 (03.02.2021)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
2001719.0 07 February 2020 (07.02.2020) GB
- (71) **Applicant: BEACONSOFT LIMITED** [GB/GB]; 71-75
Shelton Street, Covent Garden, London WC2H 9JQ (GB).
- (72) **Inventors: BOUTCHER, Stewart Lawrence;** c/o Beacon-
soft Limited, 71-75 Shelton Street, Covent Garden, Lon-

don WC2H 9JQ (GB). **TOWNEND, Michael Anthony**; c/o Beaconsoft Limited, 71-75 Shelton Street, Covent Garden, London WC2H 9JQ (GB). **BRIDGES, Nigel Paul**; c/o Beaconsoft Limited, 71-75 Shelton Street, Covent Garden, London WC2H 9JQ (GB).

- (74) **Agent: MURGITROYD & COMPANY;** Murgitroyd House, 165-169 Scotland Street, Glasgow G5 8PL (GB).

- (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, IT, 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,

- (54) Title:** JOURNEY VALIDATION TOOL

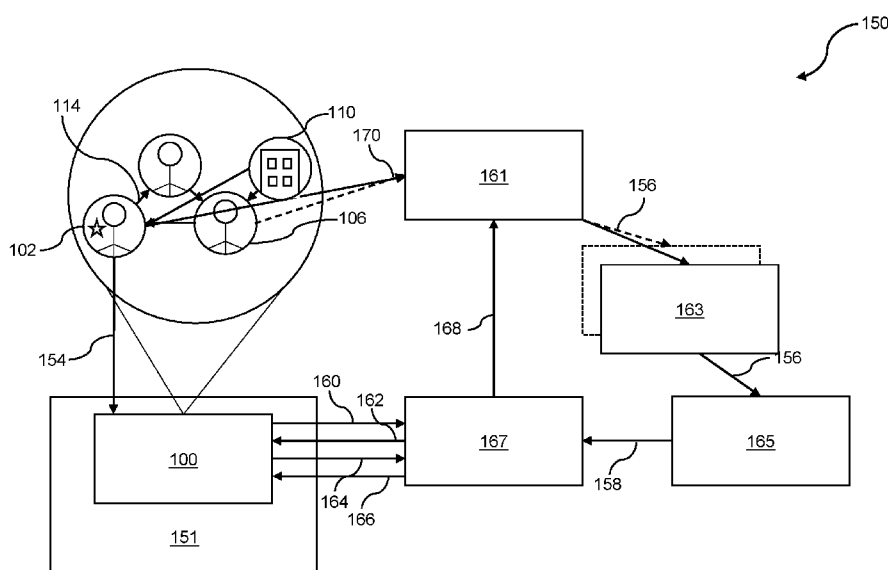


FIG. 1B

- (S7) Abstract:** The present invention relates to a user digital journey validation method comprising the steps of: connecting, by a fully distributed blockchain computer system, a trust network comprising: a plurality of user nodes; a plurality of trusted party nodes; a visitor node corresponding to a visitor to a digital service; and a plurality of links, the user nodes corresponding to users, the trusted party nodes corresponding to trusted parties, the visitor node being the most recent node in the trust network, the links being the connections between nodes; rating, by the trust network, the visitor node, the rating being a visitor trust score; recording, via a digital journey mapping system, a digital journey of the visitor; analysing, by the AI system, the digital journey of the visitor; detecting, by the AI system, bot-like behaviour associated with the visitor node or the user nodes; assigning, by the AI system, a warning flag to the visitor node or the user if the visitor node or user node has associated bot-like behaviour; removing, by the AI system, any fraudulent nodes

SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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))*

in the trust network, the fraudulent nodes being user nodes or visitor nodes having associated warning flags; updating, by the trust network, the visitor trust score based on the analysis results of the digital journey and the removal of any links connected to or from fraudulent nodes; and providing, by the AI system, a signal or value indicative of a degree of trustworthiness, to the digital service. The present invention aims to provide a means of validating whether a visitor of a digital service is a human.

JOURNEY VALIDATION TOOL

Field of the Invention

5 The present invention relates to user digital journey validation in digital marketing campaigns which involve digital advertisements. Particularly the present invention relates to an AD-fraud detection system wherein the journey validation tool provides a digital service with information useful for deciding whether a visitor is a human or software performing an automated task over the Internet (i.e. a bot).

Background to the invention

Over the past three decades, marketing has had to keep up and contend with leaps in technology and our relation to it ever since. The advent of the commercially available
15 personal computer and portable internet connected devices, along with the internet, has arguably had the largest impact on marketing than any previous innovations. Where previously a sales team would utilise the telephone or the television, it has now become more commonplace to place advertisements on the internet.

20 It is difficult for organisations to reap the full benefits of digital marketing due to the presence of “Ad-fraud”, when digital traffic for an advertisement is falsely recorded. Digital marketing campaigns are subject to average losses due to fraud and missing clicks of 30% (and, in extreme cases, some enterprises have reported 50% or more of clicks as bot clicks). As a result, advertisers wasted up to \$19 billion of their
25 digital advertising budget in 2019 alone.

Ad-fraud is difficult to stop as nefarious computer programs (also called “bots”) mimic the actions of real users, meaning that the number of impressions and clicks by real people registered by digital advert clicks are inflated. Ad-fraud can ruin a business as
30 an ad could be seen (measured as “impressions”) or clicked by a bot that never ends up purchasing a product, thereby wasting the advertiser’s money.

Current Ad-fraud solutions analyse server-side logs or network traffic. These solutions are effective in identifying fraudulent activity to a certain degree, but such single point

solutions may not be effective at countering ever more sophisticated bot technology and in many cases is relatively easily bypassed.

It is therefore desirable to provide a means of validating a visitor to a digital service as a 'real human' proactively instead of reactively such that an advertiser can be assured that their investment is providing the desired benefit.

Summary of the Invention

In accordance with a first aspect of the present invention, there is provided a digital user validation method comprising the steps of: connecting, by a fully distributed blockchain computer system including a central processor, a plurality of user nodes, a plurality of trusted party nodes, a visitor node corresponding to a visitor to a digital service, and a plurality of links, the user nodes corresponding to users, the trusted party nodes corresponding to trusted parties, the visitor node being the most recent node in the trust network, the links being connections between nodes; rating, by the trust network, the visitor node, the rating being a visitor trust score; recording, via a digital journey mapping system, a digital journey of the visitor; analysing, by the AI system, the digital journey of the visitor; detecting, by the AI system, bot-like behaviour associated with the visitor node or the user nodes; assigning, by the AI system, a warning flag to the visitor node or the user node if the if the visitor node or user node has associated bot-like behaviour; removing, by the AI system, any fraudulent nodes in the trust network, the fraudulent nodes being user nodes or visitor nodes having associated warning flags; updating, by the AI system, the visitor trust score based on the analysis results of the digital journey and the removal of any links connected to or from fraudulent nodes; and providing, by the AI system, a signal or value, indicative of a degree of trustworthiness, to the digital service.

The term "blockchain computing system" in the context of the present invention will be understood by the skilled addressee to include "distributed ledger technology".

Preferably, the visitor trust score is based on: the number of user nodes; user trust weightings each corresponding to a respective user node; the number of trusted party nodes; and trusted party trust weightings each corresponding to a respective trusted

party node. In this way, the visitor trust score may dynamically change depending on the trust values of nodes present in the trust network.

5 Preferably, the digital journey of the visitor comprising a series of visitor interactions between the visitor and the said digital service, the said digital service being digital content. In this way, the digital journey of the visitor can be anonymously recorded. This may also be used to record visitor engagement.

10 Preferably, the present invention includes a computer program product including a program for a processing device, comprising software code portions for performing the steps of the user journey validation method, when the program is run on the processing device.

15 Preferably, the present invention includes the computer program product comprises a computer-readable medium on which the software code portions are stored, wherein the program is directly loadable into an internal memory of the processing device.

20 In accordance with a second aspect of the present invention, there is provided a user journey validation system for detecting and eliminating fraudulent activity, the fraudulent activity detection system comprising: a trust network; a fully distributed blockchain computer system; a digital journey mapping system; and an AI system; wherein the trust network comprises: a trust network comprising a plurality of nodes and a plurality of edges connecting the nodes, each of the edges between the nodes representing a single degree of separation between the nodes, the nodes comprising:
25 a visitor node corresponding to a visitor; one or more user nodes, each corresponding to a user; and one or more trusted party nodes, each corresponding to a trusted party; and a visitor trust score; wherein the fully distributed blockchain computer system is configured to: continuously update the trust network in response to an interaction between a digital service and a visitor; implement the trust network using a blockchain
30 ledger; and store the trust network in the blockchain ledger; wherein the digital journey mapping system is configured to anonymously record a digital journey of the visitor, the digital journey comprising a series of visitor interactions between the visitor and the digital service, the digital service being digital content; and wherein the AI system is configured to: analyse the digital journey and provide analysis results to the trust

network such that the trust network is arranged to change the visitor trust score according to the analysis results.

Preferably, the visitor node is arranged to be the most recent node on the trust network. In this way, the visitor node preferably be configured to receive its trust score based on the nodes that precede the visitor node in the trust network.

Preferably, the user nodes each comprise an associated user trust weighting and an associated user trust score and the trusted party nodes each comprise an associated trusted party trust weighting and an associated trusted party trust score. In this way, the user nodes that have a high trust score (i.e. are more trustworthy) may be associated with a higher degree of trust. The same may be true for trusted party nodes (e.g. banks and government bodies) which may inherently be more trustworthy than an independent unverified node. Advantageously, all ad-related parties (nodes) may be connected through the hack-proof blockchain ledger and peer-to-peer validation may be possible to prove that the visitor is an actual human without exposing the visitor's personal data.

In preferable embodiments, the visitor trust score is calculated based on: the number of user nodes in the trust network; the number of trusted party nodes in the trust network; the user trust weighting associated with each of the user nodes in the trust network; the trusted party trust weighting associated with each of the trusted party nodes in the trust network; and the analysis results. In this way, the visitor trust score may be increased if the trust network comprises a higher number of user nodes that have a high trust rating (i.e. are more trustworthy) or a higher number of trusted party nodes. For example, if a visitor has visited a series of trusted party nodes associated with government bodies, the visitor trust score will be high. Advantageously, higher scored individuals and "verified" accounts (like banks) have more weight when authenticating someone else.

Preferably, the visitor node comprises an associated visitor trust score. In this way the visitor node may have a higher visitor trust score if the trust network comprises more trustworthy nodes (as a result of there being a higher number of trusted user nodes and trusted party nodes).

Preferably, the digital service comprises a trust threshold.

Preferably, the visitor can gain access to the digital service if the corresponding visitor trust score satisfies the trust threshold. In this way, if a visitor has a high trust score (indicating a high level of trustworthiness), they may be able to access the digital service. Therefore, if the visitor had previously been verified by, for example, government bodies, they may have a higher trust score and be more likely to gain access to the digital service.

Preferably, the visitor is presented with a verification step if the visitor trust score does not satisfy the trust threshold as defined solely by the digital service. In this way, even if the visitor has a lower trust score than is required to satisfy the trust threshold, they may still be able to gain access to the digital service if they pass the verification step which may be (but is not limited to) a 2 step verification or “call a number”. A further potential consequence is that it may still be possible for the visitor to build on their visitor trust score by completing verification steps presented to them when they do not satisfy trust thresholds.

Preferably, either one of: the user does not gain access to the digital service or a warning flag is associated with the visitor if the visitor fails the verification step. In this way, the visitor may be flagged up to the AI system as potentially being a bot by the AI system.

Preferably, the digital journey mapping system is further configured to store a visitor engagement indicator, the visitor engagement indicator indicating visitor engagement with content items. In this way, the visitor’s journey may be anonymously recorded – including all their activity. Thus, information can be associated with the user concerning the visitor’s engagement. This information may be useful in further steps for Ad-fraud detection.

Preferably, the AI system is arranged to scan multiple digital services and multiple digital journeys simultaneously. In this way, many visitors may be recorded individually and at the same time.

Preferably, the AI system is further configured to detect suspicious behaviour of the users associated with the user nodes and create a warning flag in response to the suspicious behaviour. In this way, the digital service may be able to respond to block user nodes with warning flags associated with them. A further potential consequence is that if one of the users in the trust network was a bot, the AI system may recognise this and respond accordingly.

Preferably, the suspicious behaviour comprises: bot-like behaviour; or identity fraud.

Preferably, the warning flag is associated with the visitor node or the one or more user nodes that exhibited the suspicious behaviour.

Preferably, the AI system is configured to remove any user nodes or visitor nodes each associated with one or more warning flags in the trust network and update the network trust score and the user trust scores of the trust network. In this way, the AI system may shut down any fraudulent nodes in the trust network and update scores across the board such that the trust network remains constantly updated and retains its reliability.

Preferably, the AI system removes any user nodes or visitor nodes each associated with one or more warning flags in real time.

Preferably, the AI system comprises a machine learning AI-engine.

The AI system is preferably configured to analyse data in a database containing all ad-fraud detection information and is preferably arranged to learn from said data to improve the specific analytics responsible for Ad-fraud anticipation. The more data the AI system collects, the better and more refined the analytics are. The AI system is preferably arranged to continuously learn from false positives and improve the predictive power over time, both globally and on a per click basis.

Detailed Description

FIG. 1A shows a schematic view of a trust network in accordance with the present invention;

FIG. 1B shows a schematic view of a user journey validating system 150 according to a second aspect of the present invention;

5 FIG. 2 shows a schematic view of a user journey validating method according to a first aspect of the present invention; and

Figure 3 shows a schematic view of a user journey validating method in an alternative embodiment.

10

Referring to FIG. 1A, there is shown a schematic view of the trust network 100 in accordance with the present invention.

15

The trust network 100 comprises a visitor node 102 associated with a visitor 104, any number of user nodes 106 associated with any number of users 108 and any number of trusted party nodes 110 associated with any number of trusted parties 112. The trusted parties 112 may be, for example, banks or government bodies. The trust network further comprises any number of edges 114 representing connections 114 between different nodes within the trust network 100. The connections 114 are formed when the visitor 104, users 108 and trusted parties 112 authenticate each other's humanity/validity via one of a range of potential signings/validation technologies. The user nodes 106 each have an associated user trust score 107 and the trusted party nodes each have an associated trusted party trust score 111. Finally, the trust network 100 comprises a visitor trust score 116 corresponding to the trust network score 116.

25

In use, the visitor trust score 116 is created by the trust network 100. The trust network 100 creates the visitor trust score 116 based on the trust scores (107, 111) associated with each of the nodes within the trust network. Trusted party nodes 110 user nodes 106 with a high user trust score 107 have more weight when authenticating the visitor/other users 108 than user nodes 106 with a low user trust score 107.

30

Turning now to FIG. 1B, there is shown a schematic view of the user journey validating system 150 according to the second aspect of the present invention, configured to carry out the user journey validating method 200. FIG. 1B shows system features as apparatus and connections as arrows.

35

The user journey validating system 150 comprises the trust network 100, a fully distributed blockchain computer system 151, a digital journey mapping system 163 and a user journey 165.

5

The fully distributed blockchain computer system 151 is arranged to connect 114 the different nodes within the trust network 100. In addition, the fully distributed blockchain computer system 151 is arranged to continuously update the trust network 100 by either removing or rearranging the nodes and edges 102 within the trust network 100.

10

The user journey validating system 150 further comprises a digital journey mapping system 163 configured to anonymously record 156 the digital journey 165 of the visitor 104 associated with the visitor node 102. The digital journey mapping system 163 records 156 the digital journey 165 following the visitor 104 interacting 170 with a digital service 161. The digital journey 165 comprises a series of interactions between the visitor 104 and the digital service 161, the digital service 161 being, for example, a website. It should be noted that the digital journey mapping system 163 may record 156 user journeys associated with the user nodes 106 such that multiple digital journeys 165 are recorded 156.

15

20

The user journey validating system 150 further comprises an AI system 167. The AI system 167 is configured to analyse 158 the user journey 165 and detect 160 both suspicious and human indicative behaviour associated with the visitor node 102. The suspicious behaviour may be bot-like behaviour. It should be noted that the AI system 167 may analyse 158 and detect 160 suspicious behaviour associated with the digital journeys 165 of the user nodes 106 simultaneously such that multiple digital journeys 165 are recorded 156 by the digital journey mapping system 163 and analysed 158 by the AI system 167. The AI system 167 is further configured to assign 162 a warning flag to the visitor node 102 or user nodes 106 if suspicious behaviour is detected from the user journeys 165 of said nodes. The AI system 167 is also configured to remove 164 any fraudulent nodes within the trust network. Finally, the AI system is configured to provide 168, to the digital service 161, a signal or value indicative of suspicious behaviour being associated with the visitor node 102. The digital service 161 may respond accordingly by blocking the visitor 104 associated with the visitor node 102.

25

30

35

Referring to FIG. 2, there is shown a schematic view of the user journey validating method 200 according to the first aspect of the present invention. The user journey validating method 200 is configured to carry out the sequential steps of:

5 Connecting 114, by the fully distributed blockchain computer system 151, the trust network 100 comprising: a plurality of user nodes 106; a plurality of trusted party nodes 110; and a visitor node 102. The visitor node 102 corresponds to the visitor 104 of the digital service 112, the user nodes 106 correspond to users 108, the trusted party nodes 110 correspond to trusted parties 112. The visitor node 102 is the most recent
10 node in the trust network 100.

Rating 154, by the trust network 100, the visitor node 102, the rating being a visitor trust score 116.

15 Recording 156, via a digital journey mapping system 163, a digital journey 165 of the visitor 104.

Analysing 158, by the AI system 167, the digital journey 165 of the visitor 104.

20 Detecting 160, by the AI system 167, bot-like behaviour associated with the visitor node 102 or the user nodes 106.

Assigning 162, by the AI system 167, a warning flag to the visitor node 102 or the user node 106 if the visitor node 102 or user node 106 has associated bot-like behaviour
25

Removing 164, by the AI system 167, any fraudulent nodes in the trust network 100, the fraudulent nodes being user nodes 106 or visitor node 102 having associated warning flags.

30 Updating 166, by the trust network 100, the trust network score 116 based on the analysis results of the digital journey 165 and the removal of any fraudulent nodes.

Providing 168, by the AI system 167, a signal or value arranged as to be indicative of blocking the visitor 104 from accessing the digital service 112, if the visitor node 102
35 has a warning flag assigned.

In use, a visitor 104 attempts to access a digital service 161 (the digital service 161 being a third party) by, for example, clicking on an advertisement. The digital service 161 receives a visitor trust score 116 associated with the visitor node 102. If the visitor trust score 116 satisfies a trust threshold (for example by having a visitor trust score 116 that is greater than a minimum value required to satisfy the trust threshold) then the digital service 161 allows the visitor 104 to gain access to the digital service 161.

The visitor trust score 116 is created by a trust network 100. The trust network 100 comprises a visitor node 102, user nodes 106 (other individuals) and trusted nodes 110 (trusted organisations such as bank or government bodies). There may only be one visitor node 102 per trust network 100. Each of the nodes within the trust network 100 has an associated trust score. Some of the nodes within the trust network 100 contribute to the visitor trust score 116. It will be appreciated by the skilled addressee that each respective user node 106 in the trust network 100 is considered to be a visitor node 102 of a corresponding trust network 100

The trust network 100 is built as the visitor 104 interacts with different ad parties or trusted parties. For example, if the visitor 104 interacts 170 with the digital service 112 of a bank then that bank digital service 112 will be incorporated into the trust network 100. The trust score of each node within the trust network 100 influences the visitor trust score 116. A higher trust score (107, 111) associated with a node leads to a higher visitor trust score 116. As a result, if a visitor 104 interacts with a greater number of ad parties that each have a high trust score (107, 111) than if the visitor 104 had interacted with fewer high trust score (107, 111) ad parties, then the visitor trust score 116 would be greater. Additionally, if a visitor 104 interacts with ad parties that have a higher trust score (107, 111) than ad parties with a lower trust score (107, 111), then the visitor trust score 116 will be greater.

Following the visitor 104 gaining access to the digital service 161 by satisfying the trust threshold, the digital journey 163 associated with the visitor 104 is recorded 156 by the centralised AI system 167. The AI system 167 may also be used for recording user engagement for marketing/message validation. The AI system 167 analyses 158 the visitor 104's digital journey 165 and data acquired relating to the digital journey 165 is fed back into a trust network 100. The trust network 100 uses this data to refine and

update 166 scores (107, 111, 116) associated with nodes (102, 106, 110) throughout the entire trust network 100. The AI system 167 scans multiple digital services 112 and user journeys 165 simultaneously. The AI system 167 determines whether the visitor 104 displays bot-indicative behaviour (examples include, but are not limited to: no touch point on a mobile device; no mouse movements on a laptop device; or mouse movement which is too accurate to be generated by a human measured on a pixel basis). The AI system 167 also detects when duplicate individual accounts associated with the visitor 104 are present in multiple web address locations at the same time – indicating identity fraud. If bot-like behaviour is detected, then the digital service 161 will be able to respond to block the visitor 104 with the associated bot-like behaviour from accessing the digital service 161. The AI system 167 and trust network 100 will then remove the visitor node 102 with corresponding blocked visitor 104 from the trust chain and the trust score is updated 166 to reflect the removal of the node. If duplicate individual accounts are detected 160, then the AI system 167 will create a warning flag. The digital service 112 may then respond by blocking if the digital services' 112 own trust threshold isn't met.

In use in an alternative embodiment, with reference to Figure 3, a visitor 104 attempts to access 302 a digital service 161 (the digital service 161 being a third party) by, for example, interacting with a digital advertisement associated with the digital service 161.

In response to the interaction, the AI system 167 evaluates 304 the visitor 104 based on a number of metrics. The metrics include, but are not limited to, an IP, a network, a browser signature, a JavaScript capability, and the visitor's 104 actions within the digital service. The AI system 167 evaluates 304 the visitor 104 by comparing the metrics to a predetermined list of known active bots stored in the blockchain computer system 151, each known active bot having a corresponding set of metrics. The AI system 167 determines that the visitor 104 meets a predetermined threshold similarity score to a known bot of the list of known active bots. The threshold similarity score is set at an appropriate level for the AI system 167 to be sure that the visitor 104 is similar enough to the known bot.

The AI system 167 then automatically notifies the digital service 161 that the visitor 104 has a metric profile that matches or is similar to the profile of the known bot. The visitor 104 is subsequently blocked 306 from accessing the digital service 161.

5 The AI system 167 also updates 308 the blockchain system 151 by assigning a warning flag to a visitor node 102 stored in the blockchain system 151. The visitor node 102 is associated with the visitor 104 and the warning flag is indicative of a metric profile matching a known bot. Future attempts to access a digital service 161, by the visitor 104 having the associated warning flag, can therefore be thwarted. The AI
10 system 167 also updates 308 the block chain 151 by reducing a visitor trust score 116 of the visitor node 102, thereby reducing the chances of the visitor 102 accessing digital services 161, as discussed above in the method of Figure 2.

If the AI system 167 determines in step 304 that the visitor 104 does not meet the
15 threshold similarity score (i.e. the visitor 104 does not display similar enough metrics to a known active bot), they are “presumed human”. Before access is granted, the AI system 167 or the digital service 161 provides 310 additional validation measurements. These validation measurements are selected by the AI system 167 or the digital service 161 and include, but are not limited to, CAPTCHA, smart device
20 validation, mobile text validation, or browser JavaScript testing.

The AI system 167 or the digital service 161 determine 312 that the visitor 104 is valid based on the validation measurements. The visitor 104 is therefore able to access the digital service 161. If the AI system 167 or digital service 161 determine 314 that the
25 visitor 104 is invalid based on the validation measurements, the visitor 104 is not granted access to the digital service 161. The visitor 104 is subsequently blocked 306 from accessing the digital service 161. The AI system 167 also updates 308 the blockchain system 151 by assigning a warning flag to the visitor node 102 stored in the blockchain system 151 and updating the visitor trust score 116.

30 Following the visitor 104 accessing and being active on the digital service 161, the digital journey mapping system 163 records and stores 314 all interactions that the visitor 104 has with the digital service 161. That is, the digital journey mapping system 167 records and stores a digital journey 165 of the visitor 104. These interactions of

the digital journey 165 include, but are not limited to, clicks, mouse movement, form fills, and time periods between any of the aforementioned interactions.

5 The AI system 167 subsequently and/or simultaneously analyses 316 the interactions of the digital journey 165. In particular, the AI system 167 determines whether the visitor displays bot-indicative behaviour (examples include, but are not limited to: no touch point on a mobile device; no mouse movements on a laptop device; or mouse movement which is too accurate to be generated by a human measured on a pixel basis). It should be noted that the AI system 167 analyses and detects bot-indicative
10 behaviour associated with the digital journeys 165 of the visitor 104 across multiple different digital services 161 simultaneously. In this case, multiple digital journeys 165 are recorded by the digital journey mapping system 163 and analysed by the AI system 167.

15 Once the AI system 167 has determined that the visitor 104 has displayed bot-indicative behaviour on at least one of the associated digital journeys 165 across the one or more digital services 161, the visitor 104 is blocked 306 from accessing the digital service 161. The AI system 167 also updates 308 the blockchain system 151 by assigning a warning flag to the visitor node 102 stored on the blockchain system
20 151. The visitor node 102 is associated with the visitor 104 and the warning flag is indicative of bot-like behaviour of the visitor 104. The above process is in real-time such that if bot-indicative behaviour is detected for one of the digital journeys 165, the one or more digital services 161 are notified that the visitor 104 is a potential bot. The digital services 161 can then take immediate action by blocking any further access to
25 the visitor 104 associated with the visitor node 102 stored on the blockchain system 151, including preventing the visitor 104 from seeing advertisements for the digital service 161 on any third party platforms such as Google or Facebook. The metrics associated with the visitor 104 having bot-like behaviour are also stored as an entry in the list of known active bots such that the AI system 167 can determine that a future
30 visitor 104 accessing a digital service 161 is one of the known active bots. After a threshold time period has passed, and a particular known bot has not been detected, the bot will be removed from the list of known active bots such that the list is active and timely.

It will be appreciated that the above described embodiments are given by way of example only and that various modifications may be made to the described embodiments without departing from the scope of the invention as defined in the appended claims. For example, the digital service may be any digital service such as
5 an advertisement, the trust network may comprise any number of nodes, the trust threshold may be any value decided by the digital service and the sequence of steps in the method may be of any order.

There may be user nodes and trusted nodes within the trust network that are not
10 connected to the visitor node.

The steps of the method may be arranged in an alternative order.

Although the distributed blockchain computer system, the trust network, the digital
15 journey mapping system and the AI system have been described in the context of being stand-alone/individual systems, they may be incorporated into any combination of each.

In the described embodiment the digital journey mapping system has been described
20 as being separate to the AI system. However, embodiments exist wherein the digital journey mapping system is incorporated into the AI system.

CLAIMS

1. A user digital journey validation method comprising the steps of:

- a) connecting, by a fully distributed blockchain computer system, a trust network comprising: a plurality of user nodes; a plurality of trusted party nodes; a visitor node corresponding to a visitor to a digital service; and a plurality of links, the user nodes corresponding to users, the trusted party nodes corresponding to trusted parties, the visitor node being the most recent node in the trust network, the links being the connections between nodes;
- b) rating, by the trust network, the visitor node, the rating being a visitor trust score;
- c) recording, via a digital journey mapping system, a digital journey of the visitor;
- d) analysing, by the AI system, the digital journey of the visitor;
- e) detecting, by the AI system, bot-like behaviour associated with the visitor node or the user nodes;
- f) assigning, by the AI system, a warning flag to the visitor node or the user if the visitor node or user node has associated bot-like behaviour;
- g) removing, by the AI system, any fraudulent nodes in the trust network, the fraudulent nodes being user nodes or visitor nodes having associated warning flags;
- h) updating, by the trust network, the visitor trust score based on the analysis results of the digital journey and the removal of any links connected to or from fraudulent nodes; and
- i) providing, by the AI system, a signal or value indicative of a degree of trustworthiness, to the digital service.

2. The method according to claim 1, wherein the visitor trust score is based on:

- the number of user nodes;
- user trust weightings each corresponding to a respective user node;
- the number of trusted party nodes; and

trusted party trust weightings each corresponding to a respective trusted party node.

5 3. The method according to claim 1 or claim 2, wherein the digital journey of the visitor comprising a series of visitor interactions between the visitor and the said digital service, the said digital service being digital content.

10 4. A computer program product including a program for a processing device, comprising software code portions for performing the steps of claim 1, when the program is run on the processing device.

15 5. A computer program product according to any of the preceding claims, wherein the computer program product comprises a computer-readable medium on which the software code portions are stored, wherein the program is directly loadable into an internal memory of the processing device.

20 6. A user journey validation system for detecting and eliminating fraudulent activity, the user journey validation system comprising:
a trust network;
a fully distributed blockchain computer system;
a digital journey mapping system; and
an AI system;

25 wherein the trust network comprises:
a trust network comprising a plurality of nodes and a plurality of edges connecting the nodes, each of the edges between the nodes representing a single degree of separation between the nodes, the nodes comprising: a visitor node corresponding to a visitor; one or more user nodes, each corresponding to a user; and one or more trusted
30 party nodes, each corresponding to a trusted party; and
a trust network score;

 wherein the fully distributed blockchain computer system is configured to:
continuously update the trust network in response to an
interaction between a digital service and a visitor;
35 implement the trust network using a blockchain ledger; and

store the trust network in the blockchain ledger;
wherein the digital journey mapping system is configured to anonymously
record a digital journey of the visitor, the digital journey comprising a
series of visitor interactions between the visitor and the digital service,
the digital service being digital content; and
wherein the AI system is configured to:

analyse the digital journey and provide analysis results to the
trust network such that the trust network is arranged to change the trust
network score according to the analysis results.

7. The system of claim 6, wherein the visitor node is arranged to be the most
recent node on the trust network.

8. The system of claim 6 or 7, wherein the user nodes each comprise: an
associated user trust weighting and an associated user trust score and
wherein the trusted party nodes each comprise: an associated trusted party
trust weighting and an associated trusted party trust score

9. The system of claim 8, wherein the trust network score is calculated based
on:

the number of user nodes in the trust network;
the number of trusted party nodes in the trust network;
the user trust weighting associated with each of the user nodes in the
trust network;

the trusted party trust weighting associated with each of the trusted
party nodes in the trust network; and
the analysis results.

10. The system of any one of claims 6 to 9, wherein the visitor node comprises
an associated visitor trust score, the visitor trust score corresponding to the
trust network score.

11. The system of any one of claims 6 to 10, wherein the digital service
comprises a trust threshold.

12. The system of claim 11, wherein the visitor can gain access to the digital service if the corresponding visitor trust score satisfies the trust threshold.

13. The system of either one of claim 11 or claim 12 wherein the visitor is presented with a verification step if the visitor trust score does not satisfy the trust threshold as defined solely by the digital service.

14. The system of claim 13, wherein either one of: the user does not gain access to the digital service or a warning flag is associated with the user if the visitor fails the verification step.

15. The system of any one of claims 6 to 14, wherein the digital journey mapping system is further configured to store a visitor engagement indicator, the visitor engagement indicator indicating visitor engagement with content items.

16. The system of any one of claims 6 to 15, wherein the AI system is arranged to scan multiple digital services and multiple digital journeys simultaneously.

17. T The system of any one of claim 6 to 16, wherein the AI system is further configured to detect suspicious behaviour of the users associated with the user nodes and create a warning flag in response to the suspicious behaviour.

18. The system of claim 17, wherein the suspicious behaviour comprises:
bot-like behaviour; or
identity fraud.

19. The system of either one of claim 17 or claim 18, wherein the warning flag is associated with the visitor node or the one or more user nodes that exhibited the suspicious behaviour.

20. The system of either one of claim 18 or claim 19, wherein the AI system is configured to remove any user nodes or visitor nodes each associated with

one or more warning flags in the trust network and update the network trust score and the user trust scores of the trust network.

21. The system of any one of claims 18 to 20, wherein the AI system removes any user nodes or visitor nodes each associated with one or more warning flags in real time.

22. The system of any one of the preceding claims, wherein the AI system comprises a machine learning AI-engine.

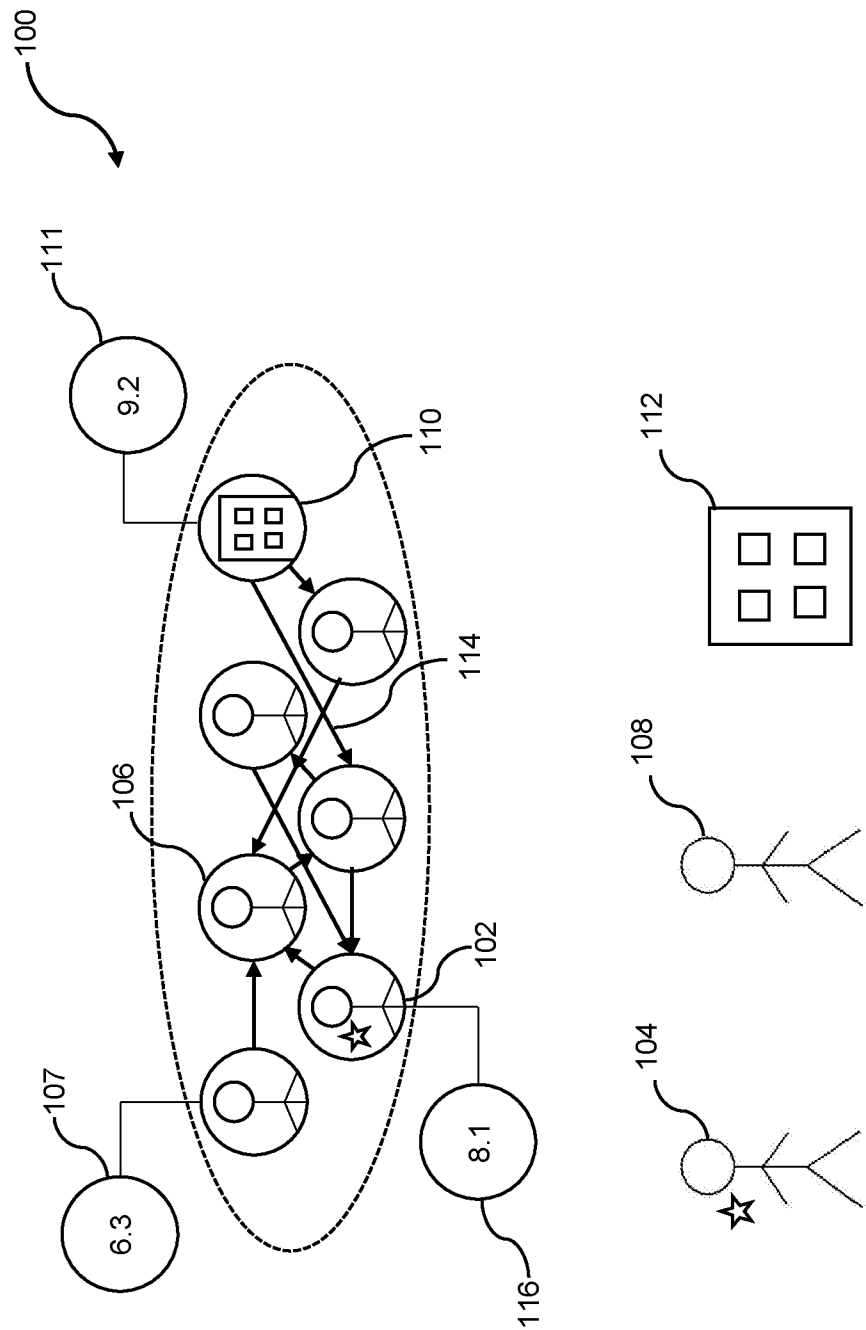


FIG. 1A

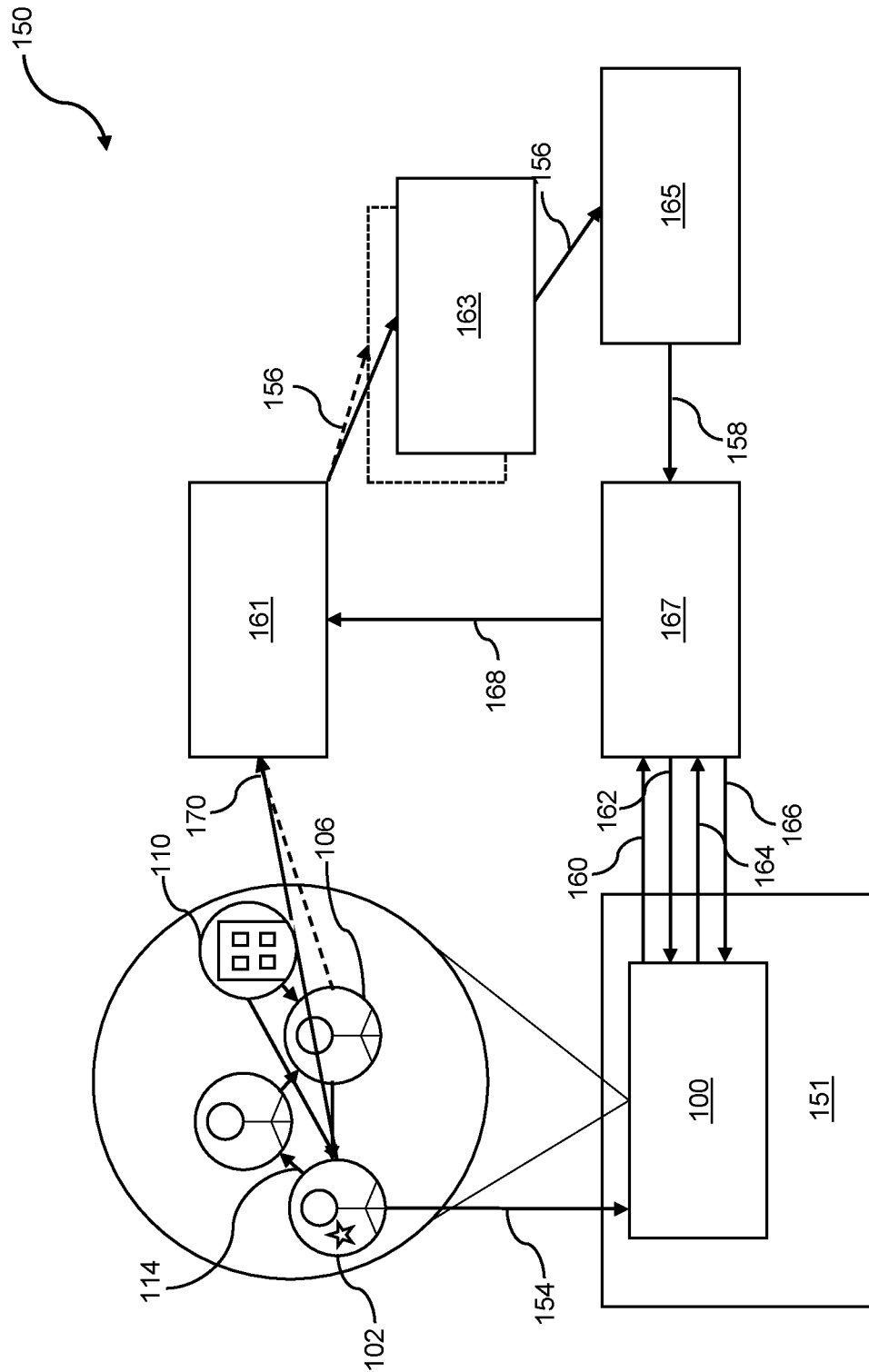


FIG. 1B

200

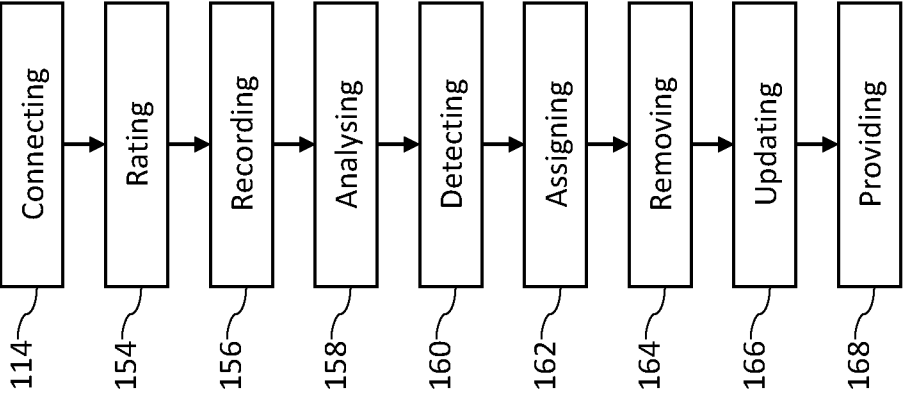


FIG. 2

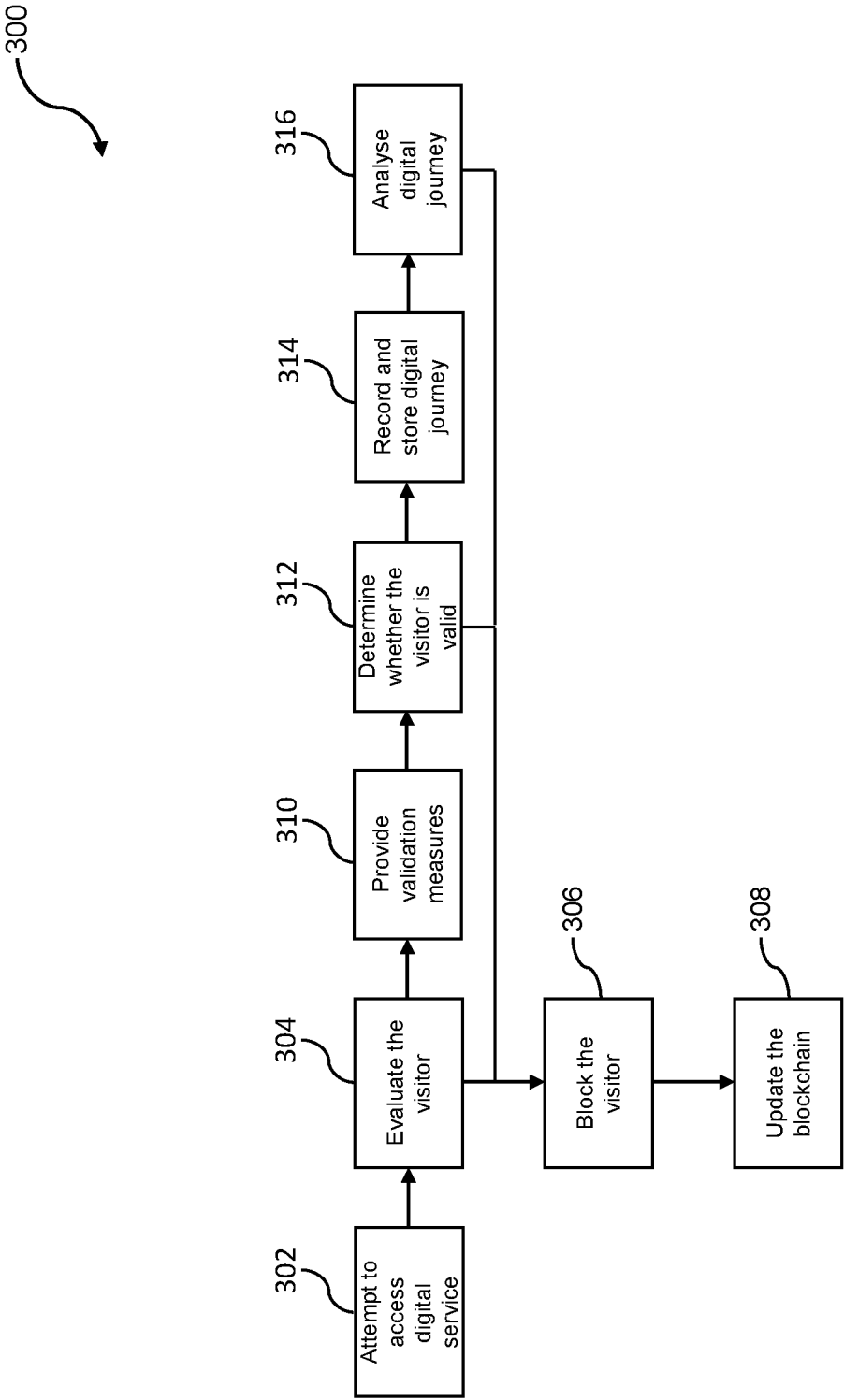


FIG. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2021/050238

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q30/02
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)
G06Q H04L G06F

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 2019/122258 A1 (BRAMBERGER CHIRON RICHARD [CA] ET AL) 25 April 2019 (2019-04-25) paragraph [0006] - paragraph [0051] paragraph [0079] - paragraph [0226] figure 1	1-22
A	----- ZI CHU ET AL: "Blog or block: Detecting blog bots through behavioral biometrics", COMPUTER NETWORKS, vol. 57, no. 3, 1 February 2013 (2013-02-01), pages 634-646, XP055129268, ISSN: 1389-1286, DOI: 10.1016/j.comnet.2012.10.005 abstract page 634 - page 643 ----- -/-	1-22



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

27 April 2021

Date of mailing of the international search report

07/05/2021

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

Bohner, Michael

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2021/050238

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	AL-OUFI SAMAH ET AL: "A group trust metric for identifying people of trust in online social networks", EXPERT SYSTEMS WITH APPLICATIONS, vol. 39, no. 18, 15 December 2012 (2012-12-15), pages 13173-13181, XP028935471, ISSN: 0957-4174, DOI: 10.1016/J.ESWA.2012.05.084 abstract page 13173 - page 13180 -----	1-22
A	XUE YU ET AL: "A Enhanced Trust Model Based on Social Network and Online Behavior Analysis for Recommendation", COMPUTATIONAL INTELLIGENCE AND SOFTWARE ENGINEERING (CISE), 2010 INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 10 December 2010 (2010-12-10), pages 1-4, XP031841233, ISBN: 978-1-4244-5391-7 abstract page 1 - page 4 -----	1-22
A	Anonymous: "reCAPTCHA - Wikipedia", 11 January 2020 (2020-01-11), pages 1-8, XP055798995, Retrieved from the Internet: URL:https://en.wikipedia.org/w/index.php?title=ReCAPTCHA&oldid=935326099#cite_note-25 [retrieved on 2021-04-26] the whole document -----	1-22
A	US 2019/147451 A1 (DEUTSCHMANN INGO [DE] ET AL) 16 May 2019 (2019-05-16) paragraph [0007] - paragraph [0020] paragraph [0025] - paragraph [0040] -----	1-22

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/GB2021/050238

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2019122258	A1	25-04-2019	NONE

US 2019147451	A1	16-05-2019	NONE
