THIS IS NOT A PROSPECTUS OF ANY SORT

This document does not constitute a prospectus of any kind. It is not a solicitation for investment and does not in any way pertain to an offering of securities in either Canada or the United States. Canadian and United States residents are excluded from purchasing Adbank tokens. This document constitutes a description of the Adbank platform and the functionality of Adbank tokens.
TITLE
Detection System for Identifying Abuse and Fraud Using Artificial Intelligence Across a Peer-to-Peer Distributed Content or Payment Networks

INVENTOR
Chiron Bramberger, Adbank inc.

ABSTRACT
Method of detecting forms of abuse and fraud using artificial intelligence on peer-to-peer network system is disclosed. A system is described where content or payment information is shared or executed across a network or series of networks. The networks are used to host, server, store, share, sync, and swarm content to and from various nodes on the network. Where some portions of these transactions represent legitimate transactions and behavior, others are fraudulent or abusive of the system itself and the contracts upon which the transactions are based or implied behavior is distorted, misrepresented, or manipulated. Artificial intelligence is used as a means to analyze the content itself, as well as metadata external to the content itself and content passed between nodes on the network, such that patterns of potentially abusive or fraudulent behavior can be deduced, learned, or otherwise identified by the software. These identifications can then be forwarded to other systems, software, or people who can then analyze the potential abuse or fraud and make a final determination of the activity and content matches the expectations of legitimate behavior. More specifically, a cryptocurrency network is described, where a peer-to-peer database, or more specifically, a block-chain, is analyzed for transactions and is compared to other sources of metadata about the network and transactions and artificial intelligence is used to determine if the transaction fit patterns of known fraudulent behavior. More specifically, an advertising system built upon blockchain technologies is described, whereby ads are hosted on the blockchain network, as well as payment information is transacted upon the blockchain as cryptocurrency between typical agents in the system, such as advertisers, ad networks, and publishers and these transactions are analyzed by artificial intelligence techniques to identify where potential fraud is occurring between the various agents.
Fig. 3
Fig. 4
Fig. 5
Fig. 7
Fig. 11
Fig. 12
Fig. 13
Fig. 14
Fig. 15
CLAIMS

1. A device, devices, or virtual machine devices, acting as a server or multiple of servers comprise: at least a storage medium for storing content and payment data and metadata relating to advertising content, advertising transactions, and payment transactions therefrom; at least a processor in communication with at least one storage medium for retrieving peer-to-peer instruction data thereof and for executing the instruction data to execute a distributed peer-to-peer advertising network system, which facilitates an advertising network which executes payment data and metadata relating to advertising transactions, advertising content, and payment transactions therein; a transceiver for establishing a connection between the servers and other servers, or a service provider, the connection for being controlled by at least a processor in execution of the peer-to-peer advertising network data, wherein some of the data is for execution of instructions for receiving further data from a plurality of nodes on the peer-to-peer network and for storing instruction data within at least a storage medium, as well as storing instruction data on other nodes within the distributed peer-to-peer advertising network for execution by said nodes, and relating to the further advertising data, the stored instruction data for being executed by the processor, or virtual machine processor built upon the peer-to-peer network for execution on each of the nodes of the network, to result in execution of advertising delivery, advertising transactions, advertising asset content storage, and data and metadata functions, and, wherein the peer-to-peer distributed advertising network, and for advertising data therefrom for executing peer-to-peer distributed advertising network functions on the advertising network server; at least a distributed peer-to-peer advertising network service whereby a traditional currency or non-traditional currency, points, reward points, cryptocurrency, tokens, bitcoin, ethereum ether, and custom-created smart-contract based ethereum tokens, is traded and exchanged for the purpose of facilitating advertising ad content exchange on the network, whereby said currency can be exchanged for other forms of currency; at least a distributed peer-to-peer advertising network which is built upon software, which creates a common data store that synchronizes across the nodes of the network, whereby this system may employ a blockchain system, virtual machine, and ability to run software or smart-contract that automatically executes across the nodes of the network, and an ability to run code remotely on all nodes to reconcile
data store, blockchain, or ledger automatically, ensuring trust and integrity of the data, metadata, transactions, and content across the distributed peer-to-peer advertising network; at least a data store of multiple data stores where transaction data and metadata is available as an input to an artificial intelligence based module or modules, such that a plurality of different types of fraud and abuse can be detected and flagged for follow-up by other modules or software, as well as people who can manually review the detected findings of the artificial intelligence fraud detection system.

2. A distributed peer-to-peer advertising network as defined in claim 1, whereby a method of detecting forms of abuse and fraud using artificial intelligence on peer-to-peer network system is used; at least a system whereby where content or payment information is shared or executed across a network or series of networks, which are used to host, server, store, share, sync, and swarm content to and from various nodes on the network whereby some portion of these transactions represent legitimate transactions and behavior and others are fraudulent or abusive of the system itself and the contracts upon which the transactions are based or implied behavior is distorted, misrepresented, or manipulated; at least one module built upon artificial intelligence is used as a means to analyze the content itself, as well as metadata external to the content itself and content passed between nodes on the network, such that patterns of potentially abusive or fraudulent behavior can be deduced, learned, or otherwise identified by the software and these identifications can then be forwarded to other systems, software, or people who can then analyze the potential abuse or fraud and make a final determination of the activity and content matches the expectations of legitimate behavior.

3. A distributed peer-to-peer advertising network as defined in claim 2, whereby a cryptocurrency network and peer-to-peer database or, more specifically a blockchain, is analyzed for transactions and is compared to other sources of metadata about the network and transactions and artificial intelligence is used to determine if the transaction fit patterns of known in the industry and to those skilled in the art as fraudulent behavior.
4. A distributed peer-to-peer advertising network as defined in claim 3, whereby an advertising system built on blockchain technologies is described, whereby ads are hosted upon the blockchain network, as well as payment information is transacted upon the blockchain as cryptocurrency between typical agents in the system, such as advertisers, ad networks and publishers, and these transactions are analyzed by artificial intelligence techniques to identify where potential fraud is occurring between the various agents.

5. A distributed peer-to-peer advertising network as defined in claim 4, whereby the artificial intelligence used is a module or series of modules based on neural networks, fuzzy logic, genetic algorithm, sentiment analysis, Markov chains, expert systems, deep learning, natural language processing rule-based system, machine learning, deep learning, supervised learning, unsupervised learning, reinforcement learning, symbolic AI, activity recognition, and big data analysis, wherein the at least one or a plurality of the inputs to the artificial intelligence software include token transaction information, blockchain transaction information, and publisher site information and access records, as well as records on what percentage of ad content was loaded, identifying information regarding publishers and end-user consumer visitors, such as, but not limited to, time of day, date, Internet Protocol (IP) address, geo-location information, browser and operating system information, and other world news and world markets information, such that the system is able to predict and identify past, current, and future changes in the information and nature of activity on the network such that potential fraudulent and abusive behavior can be identified and flagged for follow-up by other software or persons engaged in fraud and abuse verification, and the associated agents involved, such as advertisers, ad networks, publishers, and end user as also flagged for analysis by software or persons engaged in fraud and abuse verification on the distributed peer-to-peer advertising network.

6. A distributed peer-to-peer advertising network as defined in claim 5, whereby the artificial intelligence system is trained using at least a dataset of known access and mouse click or finger press patterns upon an interactive computer, phone, watch, or tablet screen of real end-user consumers naturally accessing and acting on what interests them and is compared and
trained against a known dataset of fraudulent behavior, where it is known that either automatic systems are generating the false end-user behavior or real people are being incentivized to engage the content in such a manner as to optimize the returns of the fraudulent publisher who is deliberating gaming the system for fraudulent gain; at least a plurality of other data sources are also compared against the real and fraudulent user behavior datasets, such as date, time of day, and range of time within a given day, and to compare and use as weighting to further support the system as flagging a given collection of information as representative of fraudulent behavior, whereby a software or person follows-up on the flagged events to make a final determination as to the fraudulent status of the event and agents involved.

7. A distributed peer-to-peer advertising network as defined in claim 5, whereby the artificial intelligence system is trained using the output from at least an image analysis system, whereby a publisher’s content is recorded as an image, and then the record of ad transaction that generated the image are compared to image patterns within the image using image recognition known to someone skilled in the art, such that ads that were intended to be loaded and visible on the content can be verified and at least each ad that was recorded as being delivered was in fact delivered and is visible, whereby it becomes obvious that in fact images must be deduced as being obfuscated or stacked as a fraudulent method of loading multiple ads on a given page without actually having them being displayed and possibly allow overloading the content with more ads than would ever be reasonable to someone attempting to consume the content is a reasonable way; at least one or more of a plurality of methods would be combined in this approach to support the determination of fraudulent behaviors as defined in claim 5 and claim 6.

8. A distributed peer-to-peer advertising network as defined in claim 7, whereby the artificial intelligence system uses image recognition and source code analysis of the content to determine if ads that shouldn’t be present in the content are due to ad injection and flags multiple content for follow-up by software or a person, as known in the industry and to those skill-in-the-art.
9. A distributed peer-to-peer advertising network as defined in claim 5, whereby the artificial intelligence system is trained using the output a plurality of web crawling activities such that the cookies sent with each session are evaluated against known well-behaved cookie activity and potentially fraudulent cookie behavior is flagged multiple contents for follow-up by software or a person.

10. A distributed peer-to-peer advertising network as defined in claim 7, whereby the artificial intelligence system is trained using publisher requests where the publisher requesting ads for a given domain are checked against the actual publisher site requesting the ad delivery; wherein images rendered of the content from the request are compared against the content rendered from the known publisher site and if the domain or content are mismatched following patterns of known fraudulent behavior, whereby at least the domains from the publisher site and ad request are compared, as well as additional image analysis, and potentially fraudulent cookie behavior is flagged as multiple contents for follow-up by software or a person.

11. A distributed peer-to-peer advertising network as defined in claim 7, whereby the artificial intelligence system is trained using image analysis of content from publishers, where the publisher web page has the most profitable keywords, such as keyword which fetch the highest cost per click, whereby the web pages are automatically and dynamically built such that the pages are filled with an abnormal amount of the high profit keywords to generate search ads as known in the industry and to those skilled-in-the-art, and analysis for actual content and patterns of content that are creating false high value pages, such that images of sites with actual content can be detected, along with a plurality of as defined in claim 5 and claim 6, where the collection of input to the artificial intelligence results in auto-generated and manipulative false content pages are flagged as fraudulent content for follow-up by software or a person.

12. A distributed peer-to-peer advertising network as defined in claim 5, where at least website form validation software ties into the artificial intelligence system, where the form software may be implemented but is not limited to JavaScript code that makes available user input behavior not
currently typically captured buy web forms, and whereby the artificial intelligence system is trained to analyze input-form end-user consumer activity and compared against known data-sets of natural end-user behavior and compared against known data-sets of known fraudulent form filling activity, such that the system is able to determine that the apparent form engagement and false determine as this user being a real person who represents a hot-lead with high probable conversion to new business for the advertiser and is instead determined to be automatic fraudulent software behavior whereby the collection of input to the artificial intelligence results in auto-generated and manipulative false content pages are flagged multiple contents for follow-up by software or a person.

13. A distributed peer-to-peer advertising network as defined in claim 5, whereby the artificial intelligence system is trained monitor publisher sites on the network over time and build profiles of change and rates of change and new content creation such that rapid and usual forms of change and content which are indicative of a content hacking fraud, whereby the website of a legitimate non-fraudulent publisher is now loading ads that are usual for the publisher as also are requested from another publisher identification that doesn't match the usual publisher requests or identification, and is instead determined to be fraudulent behavior as a result of hacking the publisher site and whereby the collection of input to the artificial intelligence results in the manipulative false content pages are flagged for follow-up by software or a person.

14. A distributed peer-to-peer advertising network as defined in claim 5, whereby the artificial intelligence system is trained to detect traffic fraud or audience extension fraud, whereby the original advertising order placed within the system is compared against the actual ad requests, and if there is a mid-campaign departure from the expected interactions, which is a sign of the publisher buying traffic from a third party due to a shortfall of impression supply, whereby the collection of input to the artificial intelligence results in the inconsistent interaction patterns are flagged for fraud analysis review by software or a person.
15. A distributed peer-to-peer advertising network as defined in claim 7, whereby the artificial intelligence system is trained to detect occurrences of images not being loaded and present in the final content rendering, such that code that indicates that images are being loaded within the dimensions of one pixel by one pixel, and are thus difficult to see even though they are being loaded, and are, therefore, flagged for fraud analysis review by software or a person.

16. A distributed peer-to-peer advertising network as defined in claim 5, whereby the artificial intelligence system is trained to monitor an ad request from the App Software Development Kits which may have been compromised through device hijacking, whereby the normal patterns of request from a given user identification are compared against known previous patterns of request and other personally identifying data and metadata, such as location, IP address, date, time, and types of applications that request ads, such that a rapid shift in these ad requested are detected as straying from normal usage patterns for that user and users in general, such that the device and potential fraudulent publisher are flagged for fraud analysis review by software or a person.

17. A distributed peer-to-peer advertising network as defined in claim 5, whereby the artificial intelligence system is trained to monitor pop-up and pop-under ads and windows from a given publisher site, through the analysis of activity on the same device as the artificial intelligence server, or in a separate device or virtual machine, whereby variables such as frequency, duration, and quantity of pop-ups and pop-unders that are detected as being fraudulent and abusive pop-up and pop-under behaviors is fraud analysis review for the genuine publisher and flagged for follow-up by software or a person.

18. A distributed peer-to-peer advertising network as defined in claim 5, whereby the artificial intelligence system is trained to monitor the network transaction on the distributed peer-to-peer advertising network to look for patterns of transactions and potential redemption of tokens, such that normal publisher behavior is compared against fraudulent publisher behavior, and publishers can be flagged for fraud analysis review by software
or a person such that the publisher content is reviewed for other signs of potential fraud.

19. A distributed peer-to-peer advertising network as defined in claim 5, whereby the artificial intelligence system is trained to monitor the network transaction on the distributed peer-to-peer advertising network to look for patterns of transactions between advertisers, ad network, and publishers, such that rebates and other advertisers' unfriendly activities between the ad network and publisher are analyzed and flagged for potential pricing fraud and the genuine publisher is flagged for fraud analysis review by software or a person.

20. A distributed peer-to-peer advertising network as defined in claim 5, whereby the artificial intelligence system is able to request content from publisher sites without triggering actual ad billing, so avoid the fraud detection system from effectively engaging in the very non-person behavior the system is trying to avoid and results in false billings from the advertiser to the publisher of the site being examined.

21. A distributed peer-to-peer advertising network as defined in claim 1 through claim 20, whereby the artificial intelligence system uses unguided machine learning to monitor and learn from a plurality of sources to find non-obvious connections between variables that are linked to fraudulent behavior.

22. A distributed peer-to-peer advertising network as defined in claim 5, whereby the artificial intelligence system works with software running on the end-user consumer's device, which may but is not limited to taking the form of a web browser plugin or extension, a stand-alone purpose-built web browser, or software or service executing and operating in the background of the operating system, and communicates with the artificial intelligence system, such that user activity and behavior data and metadata is communicated back to the artificial intelligence system to aid in further analyzing the interactions between advertisers, ad networks, and publishers, wherein the artificial intelligence system can detect fraud as defined in claim
5 and can provide deeper insights and ability to detect fraud through leveraging the additional source of data.

23. A distributed peer-to-peer advertising network as defined in claim 22, whereby the artificial intelligence system uses additional data and interaction with end-user consumer software, wherein such software monitors the various other software running on the device, such as, but not limited to, other applications or apps running or installed the device, wherein monitoring of the system takes place and, upon installation of new software, interactions between the installed app and communication with devices outside the device, more specifically wherein the communication is with an advertiser, publisher, ad network, or other advertising system, wherein the device is reporting the successful installation, first time execution, or any other software event, upon which when reported back to the advertising system, results in a payment from one advertising entity to another entity, where at least the artificial intelligence fraud detection system is able to infer that the resulting communication may have been the result of a form of fraud commonly known in the industry and to those skilled-in-the-art as "click injection," whereby a fraudulent report regarding an application is reported to an advertising entity that results in a payment taking place outside the expectations of the purchase of the advertising, wherein the result of the interaction isn't a reflection of the behavior of the end user is reported as being incorrectly attributed to the actions of advertising and, therefore, encouraging the end user to initiate the call-to-action of advertising resulting in the desired behavior on the part of the user to the benefit of the original advertiser; whereby a distributed peer-to-peer advertising network with an artificial intelligence system and custom application running on a mobile device such that where fraudulent predatory software or malware-based application is sending out fake install notifications back to ad networks to get a third and entitled party to receive payments where ads would normally be intended to drive natural traffic to the installation and first time running of applications, are detected, known to those skilled-in-the-art as click injection, the artificial intelligence system works with a custom app installed on the mobile device which uses the similar methods of scanning for system app installs and first execution, to identify a fraudulent emission of an installation and first running to the system such that information involved in the click injection is flagged and a
report is generated and passed along to an artificial intelligence system to analyze for fraud, and finally generates a report that is sent to a person to review and confirm the fraud, and marking the entity in the system as an agent propagating fraud.

24. A distributed peer-to-peer advertising network as defined in claim 22, whereby end-user consumer software works in conjunction with the artificial intelligence system uses additional data and interaction with end-user consumer software, wherein such software allows users to create accounts for themselves on the system and the end-user consumer software, which facilitates a greater deep of tracking online activity, such that when a user engaging in research about a product, service, or topic of interest that leads directly to a purchasing decision, product engagement, or other activity deemed desirable to a advertising entity, such that the system is able to, upon completion of the desirable action, to track back through the user's history and is able to reward both the user as well as all the other advertising entities that have encouraged the user to engage in the desirable activity, through the transfer of tokens, such that an additional bonus is awarded to the other advertising entities that played a direct or indirect role is leading to the desirable user behavior or outcome; wherein fraudulent behavior known in the advertising industry and to those skilled-in-the-art as "retargeting fraud" and involves the automatic software controlled activity of accessing material on devices that mimics the behavior of genuine end-user research into products, services, or ideas which may lead to behavior desirable to advertising entities, such that said entities would normally pay higher rates for delivering ads to high value "hot prospects" or other seemly realistic online behavior that appears to be close to executing the desirable behavior, but is in reality software designed to fool these systems into paying higher rates for higher paying ads through retargeting the delivery of lower paying ads into higher paying ads and defrauding the advertiser who pays these higher rates, wherein the combination of end-user software and artificial intelligence tracking of online behavior creates higher incentive to pay higher rates after the desirable behavior takes place, having the unforeseen advantage of creating an advertising environment in which higher rates are shifted away from scenarios conducive to retargeting fraud and towards situations whereby the higher rates are paid for the reliable delivery of desired behavior, thereby starving the market forces leading to higher pay
for the easier to exploit retargeting fraud and thus greatly reducing the occurrences of fraud of this nature.

25. A distributed peer-to-peer advertising network as defined in claim 22, whereby the artificial intelligence system interacts with the end-user consumer software, for example, but not limited to, a browser plugin, whereby this plugin monitors the click or touch-enabled behavior upon an ad, or the automatic execution of an ad, such that the user's browser is redirected to another Internet location, or triggers an action or other unexpected behavior, such as redirecting the user screen or device to access an online location, such as an app store or shopping application or website, wherein an advertising entity is earning payment for desirable behavior which is not actually the result of the intended user behavior, but is instead the result of software or presentation misdirection, tricks, obfuscation, or other insincere and predatory execution, such that a fraudulent advertising entity benefits and receives payment or other reward which falls outside the intended spirit of the advertising arrangement; wherein at least an end-user consumer's device is tagged or uniquely identified such that activity is falsely attributed as conversion as if an end-user consumer eventually downloads an app or engages in other desirable behavior, known in the advertising industry and by those skilled in the art as "automatic redirection"; whereby the artificial intelligence software, working in conjunction with end-user consumer's browser plugin, is able to identify that a user has not actually clicked or normally interacted with the ad, such that the user is automatically redirected to another location or application, and the advertising entities involved, such as, but not limited to, advertiser, ad network, or publisher, wherein the artificial intelligence software marks the potential advertising entities as possibly engaged in "automatic redirection" fraud, and generates the flagging for fraud analysis review by software or a person such that the entity is reviewed for other signs of potential fraud.

26. A method for providing an interactive distributed peer-to-peer advertising network, the method comprising the steps of: providing a distributed peer-to-peer advertising network comprising a storage medium for storing a distributed peer-to-peer advertising network server for establishing a connection between the distributed peer-to-peer advertising network and another node on the distributed peer-to-peer advertising
network and for controlling events taking place on the distributed peer-to-peer advertising network; coupling the distributed peer-to-peer advertising network to another distributed peer-to-peer advertising network node through a broadband access network; and establishing a configuration of the distributed peer-to-peer advertising network according to messages received from another node on the distributed peer-to-peer advertising network, the configuration including events taking place on the distributed peer-to-peer advertising network.

27. A distributed peer-to-peer advertising network as defined in claim 1, wherein at least a storage medium includes non-volatile random access memory.

28. A method for providing a distributed peer-to-peer advertising network service as defined in claim 5, wherein the storage medium is non-volatile random access memory.

29. A method for providing a distributed peer-to-peer advertising network service as defined in claim 5, wherein the storage medium is random access memory.

30. A method for providing a distributed peer-to-peer advertising network service as defined in claim 5, wherein the storage medium is read-only memory.

31. A method for providing a distributed peer-to-peer advertising network service as defined in claim 5, wherein the storage medium is a compact disc or DVD.

32. A method for providing a distributed peer-to-peer advertising network service as defined in claim 5, wherein the storage medium is a USB storage device.
33. A method for providing a distributed peer-to-peer advertising network service as defined in claim 28, wherein the distributed peer-to-peer advertising network is stored in the non-volatile random access memory.

34. A distributed peer-to-peer advertising network as defined in claim 1 through claim 33, whereby the person who engages the system to review flagged potential fraud events, is the end user and consumer of the system, and earns tokens for working within the system to supply a person’s review and analyze of the artificial intelligence output, supplying the end user with an incentive to work to improve the integrity of the system; at least a means for the user to redeem earned tokens for advertising, either online or off-line such as but not limited to a website product or service purchase or an in-store purchase whereby a brick-and-mortar store has a system and means of sending customer information to the distributed peer-to-peer advertising network as defined in claim 1 through claim 33 such that the user purchase information is made available to the distributed peer-to-peer advertising network as defined in claim 1 through claim 33, as well as other benefits such as, but not limited to, paying for the removal of ads to the publisher to suppress the display of ads for sites the end-user consumer choices to support, purchasing of special offers, rewards, coupons, and promotions by advertisers, removal of end-user data from advertiser databases that support opt-out through token payments, and other incentives offered typically in the industry and known by people skilled in the art.

35. A distributed peer-to-peer advertising network as defined in claims 1 through claims 33, whereby the artificial intelligence system accesses publisher websites through anonymous services, such as, but limited to, VPN, whereby the publisher sites are unaware of the artificial intelligence system scanning their systems and avoid them delivering content designed to fool the system into thinking that the site is not engaging in fraud.

36. A distributed peer-to-peer advertising network as defined in claims 1 through claims 34, whereby the artificial intelligence system accesses publisher websites in order of priority, such that situations that result in high-value ad payouts are prioritized as the first systems to scan, since they
are the most likely high-value targets of the sites engaging in fraudulent behavior.

37. A distributed peer-to-peer advertising network as defined in claims 1 through claims 35, such that artificial intelligence software, distributed peer-to-peer advertising network, end-user consumer software, and all other claimed software instances, modules, plugins, and other applications and software services, executes on a micro-controller-based system, embedded system, router, switch, network appliance, server, database, file server, distributed cloud service, virtual machine, workstation computer, desktop computer, laptop, portable computer, tablet, phone, watch, or other microprocessor-based system.

38. A distributed peer-to-peer advertising network as defined in claims 1 through claims 37, whereby the artificial intelligence system is trained to detect advertising purchasing and placement which seeks to have the effect of, or otherwise disrupts normal marketplace activity, such that a particular advertiser or other agent on the advertising network is “priced out of the market” or is otherwise usable to purchase ads without paying prices that are far too high to make the activity profitable; whereby the artificial intelligence system examines the ad purchases, ad purchasing parameters, other ad purchasing data or meta-data, transaction on the block-chain, ad prices within a certain market vertical, and finally analyses the purchasing behavior of potential competitors, such that such price manipulation, price fixing, or other forms of anticompetitive practices are identified and the manipulative behavior is identified by the artificial intelligence system, and a report is generated and flagged for follow-up by software or a person.

FIELD OF THE INVENTION
The present invention generally relates to peer-to-peer networks and advertising and, more specifically, to blockchain-based cryptocurrencies and tokens and the use of artificial intelligence to address major forms of fraud and abuse in traditional advertising.
BACKGROUND OF THE INVENTION
A common trend is emerging in modern designs of distributed peer-to-peer networks, as well as various advertising networks built upon this and other technologies, such that the creation of cryptocurrency- and token-based networks are being created to address many issues surrounding traditional networks and platforms.

In this context, exciting new developments are occurring in the areas of blockchain-based technologies, with a popular example being ethereum and it’s Smart Contracts, such that ease of new token-based economies are being created at a pace as of yet unseen. However, fraud in the advertising industry is rampant and represents a major loss of resources for advertisers and existing solutions are fragmented and struggle to make a significant impact in reducing fraud in advertising.

OBJECT OF THE INVENTION
It is, therefore, an object of the present invention to provide a system and method for creating a distributed peer-to-peer advertising network and a system built upon aforementioned network such that the system software acts as an artificial intelligence agent to monitor and flag potential fraud, leading to an advertising platform that is conducive to predictable use by advertisers, ad networks, publishers, and end users.

SUMMARY OF THE INVENTION
In accordance with an aspect of the instant invention, a system is proposed that creates a distributed peer-to-peer advertising network, built upon technologies such as the cryptocurrency- and token-based blockchain-based systems, which execute software that uses advanced artificial intelligence techniques to analyze a large collection of potential fraudulent behavior and flagged potential bad agents within the advertiser ecosystem, so that software or people can follow up and help ensure the authenticity and integrate of the system.
BRIEF DESCRIPTION OF THE DRAWINGS

An exemplary embodiment of the present invention will be described in conjunction with the following drawing, in which similar reference numbers designate similar items:

**Figure 1** displays a diagram of the distributed peer-to-peer advertising network with a general artificial intelligence system analyzing the advertising database against a publisher's website, along with examining the ethereum blockchain; and finally passing a report to a person to evaluate potential fraud and marking a potential entity, such as a publisher, as a bad actor in the system.

**Figure 2** displays a diagram of the distributed peer-to-peer advertising network and an artificial intelligence system that is specifically purposed with analyzing a publisher's website rendered as an image and using image detection to verify that each ad that is supposed to be displayed on the publisher website is actually visible. This avoids forms of ad obfuscation whereby publishers create sites that do not actually visually display ads even though they are being loaded and are fraudulently generating income of the publisher.

**Figure 3** displays a diagram of the distributed peer-to-peer advertising network and an artificial intelligence system that is specifically purposed with analyzing a publisher's website rendered as an image and using image detection to verify that each ad that is supposed to be displayed on the publisher website is actually visible. This avoids forms of ad obfuscation, whereby publishers create sites that stack display ads even though they are being loaded and are frugally generating income of the publisher.

**Figure 4** displays a diagram of the distributed peer-to-peer advertising network with an artificial intelligence system analyzing the ethereum blockchain transactions seeking to identify transactions that are indicative of potential fraud. When the system detects a potential fraud scenario, a report is generated and passed along to a person to review and confirm the fraud, and marking the entity in the system as an agent propagating fraud.
**Figure 5** displays a diagram of the distributed peer-to-peer advertising network with an artificial intelligence system that examines patterns of mouse movement or finger presses on a touchscreen and analyses the events over time such that automated software designed to simulate a person naturally browsing the publisher website is revealed as fraudulent. A report is generated and passed along to a person to review and confirm the fraud and marking the entity in the system as an agent propagating fraud.

**Figure 6** displays a diagram of the distributed peer-to-peer advertising network with an artificial intelligence system that analyses a publisher’s website source code and advertising ad database to determine if there are patterns of source code, ads, and website rendering, such that potential source code based fraud efforts are revealed and a report is generated and passed along to a person to review and confirm the fraud, and marking the entity in the system as an agent propagating fraud.

**Figure 7** displays a diagram of the distributed peer-to-peer advertising network and artificial intelligence system that analyses that patterns over time of publisher website with form elements as they are filled in and identifies scenarios where the form filling activity is clearly not a natural process of human data entry, but is, instead, highly likely to be software designed to automate the process of filling in forms. A report is generated and passed along to a person to review and confirm the fraud and marking the entity in the system as an agent propagating fraud.

**Figure 8** displays a diagram of the distributed peer-to-peer advertising network with an artificial intelligence system that examines a rendering of a publisher website over time and identifies unusual sudden changes in content, as well as identifies the change as a potential change as a sign of fraud or publisher site hacking. A report is generated and passed along to a person to review and confirm the fraud and marking the entity in the system as an agent propagating fraud.
**Figure 9** displays a diagram of the distributed peer-to-peer advertising network with an artificial intelligence system that analyses sources of web traffic to a publisher website over time, such that it detects when unexpected changes in the location and timing of web visits from users appear less like natural organic traffic and is instead indicative of paid or other fraudulent forms of web traffic. A report is generated and passed along to a person to review and confirm the fraud and marking the entity in the system as an agent propagating fraud.

**Figure 10** displays a diagram of the distributed peer-to-peer advertising network and artificial intelligence system that uses a computer or virtual machine to analyze the behavior of publisher websites such that excessive use of pop-ups and pop-unders are detected and flagged as potentially fraudulent behavior. A report is generated and passed along to a person to review and confirm the fraud and marking the entity in the system as an agent propagating fraud.

**Figure 11** displays a diagram of the distributed peer-to-peer advertising network with an artificial intelligence system that attempts to identify single pixel hidden ads that fraudulently display enough to trigger a payment to the website publisher while failing to display enough of the ad to make any impression upon the website visitor. A report is generated and passed along to a person to review and confirm the fraud and marking the entity in the system as an agent propagating fraud.

**Figure 12** displays a diagram of the distributed peer-to-peer advertising network with an artificial intelligence system that analyses the blockchain to identify unusual patterns of transactions that indicate there are significant flows of rebate flowing from publishers back to other agents in the system. A report is generated and passed along to a person to review and confirm the fraud and marking the entity in the system as an agent propagating fraud.

**Figure 13** displays a diagram of the distributed peer-to-peer advertising network with an artificial intelligence system and custom application...
running on a mobile device such that where fraudulent and predatory software- or malware-based application is sending out fake install notifications back to ad networks to get a third and entitled party to receive payments where ads would normally be intended to drive natural traffic to the installation and first time running of applications, are detected. Known to those skilled in the art as click injection, the artificial intelligence system works with a custom app installed on the mobile device which uses the same methods of scanning for system app installs and first execution, to identify a fraudulent emission of a installation and first running to the system such that information involved in the click injection is flagged and a report is generated and passed along to a person to review and confirm the fraud and marking the entity in the system as an agent propagating fraud.

**Figure 14** displays a diagram of the distributed peer-to-peer advertising network with an artificial intelligence system interfacing with a computer or virtual machine that loads publisher websites and analyses behavior looking for excessive and fraudulent signs of redirection that the user did not initiate or intend. A report is generated and passed along to a person to review and confirm the fraud and marking the entity in the system as an agent propagating fraud.

**Figure 15** displays a diagram of the distributed peer-to-peer advertising network with an artificial intelligence system analyzing a log of events that have lead to a direct purchase or sale of product or service. The post-sale analysis allows publishers who have contributed to the purchase or call-to-action behavior to be rewarded for their role in driving the sale. This helps dis-incentivize large payouts for behavior that appears to lead to a sale but in reality doesn't lead to the purchase outcome. A form of fraud exists whereby a large payout for ads when a user appears to be researching and working towards a purchase but, in reality, is a software system designed to simulate a motivated potential user, thus garnering higher paying ads. The embodiment proposed in Figure 15 is designed to create a better system that is resistant to this form of fraud and will lead to lower payouts before a purchasing decision. A report is generated for a person to review the analysis of the sale and the links identified by the artificial intelligence system.
DETAILED DESCRIPTION OF THE INVENTION

The present invention is now described with respect to a specific embodiment thereof, wherein a distributed peer-to-peer advertising network built upon a cryptocurrency or tokens is used to with a software module or modules that perform analysis of a plurality of factors, wherein the said software attempts to detect a plurality of occurrences of various types of fraud.

Of course, the invention described herein is not restricted to a particular example, which will be described in what follows, but equally applies to other architectures possibly used to establish and provide a system and method for fraud detection using artificial intelligence built upon a blockchain-based advertising network.

In one embodiment, an artificial intelligence system is created upon and with access to an advertising network built upon a cryptocurrency- and blockchain-based system. The artificial intelligence system would be trained, programmed, evolved, or otherwise brought into a state whereby the system is able to detect patterns of fraud known to those skilled in the art. The training data is based on both known examples of organic, natural web visitors accessing websites, as well as datasets of known fraudulent behavior. The methods for this training are known to those skilled in the art.

Referring to Figure 1, a general diagram of the token-based distributed peer-to-peer advertising network platform is presented. The system in this embodiment is built upon the ethereum network blockchain 101, which is made up of the data and content layers, smart contracts and tokens data store. The system also contains an artificial intelligence system 100, advertising database 102, a system for providing delivery of online reporting to a person to review potential fraudulent occurrences represented which is represented in 104, and finally a database of agents within the network which are flagged as engaging in fraudulent behavior. The artificial intelligence system 100 engages scan 107 of a publisher website 103 and ads
represented in 115 and compares this information through system call 106 to search, images, logs, or other information in the platform ad database 102, and in this particular embodiment an example ad element entry 114 in database 102 which is compared to website ad 115 and may be found to match or not match what the expected outcome is in a general embodiment. The artificial intelligence system 100 also engages scan 108 of the ethereum network 101 and its blockchain, to leverage additional information that may lead to connections found in the artificial intelligence system such that non-obvious connections can be learned and made by the artificial intelligence system. Once potential fraud activity is identified, the artificial intelligence system generates a report and sends this report to a person 112 through a system call 109 and displayed to person 112 for review as illustrated in 104. Once the report is evaluated as being either fraud or not fraud then update 111 is triggered in the list of fraudulent agents shown in database 105 through system call 110.

Referring to Figure 2, a diagram of the token-based distributed peer-to-peer advertising network platform is presented. In this embodiment of an anti-fraud module, the artificial intelligence system 200 access images from the ad database 201 via a request 207 and compares that image with a rendering of the publisher website 202 and scans via a request for the render 208 the image for occurrences of images that match what is in the web-page 202. This image matching is done to ensure that every ad that was supposed to be delivered to the publisher website 202 is present, and thus avoiding ad fraud whereby images are loaded but not presented to the web visitor, which earns the publisher a payout for displaying the ad when, in fact, no ad was ever actually shown to the user. Once this scenario is detected as a potential fraud by the artificial intelligence system 200 and a report 206 is generated via system request 209 such that a person can review the potential fraud as illustrated in 203. Once the report is evaluated as being either fraud or not fraud then update 211 is triggered in the list of fraudulent agents shown in database 204 through system call 210. This module runs in conjunction with the other modules as described in claims 1 through 37, such that results of the module described in Figure 2 can be compared to activity on the blockchain and used to support evaluations of fraud.
Referring to Figure 3, a diagram of the token-based distributed peer-to-peer advertising network platform is presented. In this embodiment of an anti-fraud module, the artificial intelligence system 300 scans the publisher website 302 seeking to match images on the website through system call 306 that retrieves information from the publisher website 302 against ads contained in the database 301 through a system call 305. Images can be matched against this database and additionally image location can be requested from the HTML document object module DOM through system call 306 such that the artificial intelligence system can determine the positional information of the images and make a determination that a form of fraud is occurring whereby image stacking is taking place which is known in the industry and to those skilled in the art. Once this scenario is detected as a potential fraud by the artificial intelligence system 300 and a report 312 is generated via system request 307 such that a person 310 can review the potential fraud as illustrated in 303. Once the report is evaluated as being either fraud or not fraud then update 308 is triggered in the list of fraudulent agents shown in database 304 through system call 309. This module runs in conjunction with the other modules as described in claims 1 through 37, such that results of all the modules can be compared and the module described in Figure 3 can additionally be compared to activity on the blockchain and used to support evaluations of fraud.

Referring to Figure 4, a diagram of the token-based distributed peer-to-peer advertising network platform is presented. In this embodiment of an anti-fraud module, the artificial intelligence system scans for activity on the ethereum blockchain 401 such that transactions over time can be evaluated and patterns of fraudulent behavior can be detected when compared to known examples of typical behavior which is not associated with fraud through system call 409 to examine the ethereum blockchain and through system call 410 which examines transactions of tokens as exposed by specifically programmed elements of an ethereum contract that exposes token transaction information. Once this scenario is detected as a potential fraud by the artificial intelligence system 400 and a report 405 is generated via system request 408 such that a person 404 can review the potential fraud as illustrated in 402. Once the report is evaluated as being either fraud or not fraud, then update 406 is triggered in the list of fraudulent agents shown in database 403 through system call 407. This module runs in conjunction with
the other modules as described in claims 1 through 37, such that results of all the modules can be compared and the module described in Figure 4 can additionally be compared to activity on the blockchain and used to support evaluations of fraud.

Referring to Figure 5, a diagram of the token-based distributed peer-to-peer advertising network platform is presented. In this embodiment of an anti-fraud module, the artificial intelligence system 500 accesses database 502 through a system call 513 which contains the information gathered by mouse click and touch events collected through system call 515 from user interaction with publisher websites illustrated in 500. The artificial intelligence system 500 then analyses the user interaction events from database 502 and makes a determination if the events are of a typical person interacting with the website or if the interaction events aren't typical and indicate the presence of an automated software used to interaction with the websites acting to mimic the behavior of people. This behavior and fraud is known in the industry and by those skilled in the art as typically executed by "bot farms" where many computers are running software that pretend to be people in order to generate fake website traffic for a publisher site. This causes the publisher to get paid by advertisers when, in fact, the ads shown are never seen by people and thus fail to deliver the intended value to the advertiser. Once this scenario is detected as a potential fraud by the artificial intelligence system 500 and a report 505 is generated via system request 511 such that a person 504 can review the potential fraud as illustrated in 503. Once the report is evaluated as being either fraud or not fraud, then update 507 is triggered in the list of fraudulent agents shown in database 506 through system call 508. This module runs in conjunction with the other modules as described in claims 1 through 37, such that results of all the modules can be compared and the module described in Figure 5 can additionally be compared to activity on the blockchain and used to support evaluations of fraud.

Referring to Figure 6, a diagram of the token-based distributed peer-to-peer advertising network platform is presented. In this embodiment of an anti-fraud module, the artificial intelligence system 600 scans the source code of a website 602 through system call 611 where the code is analyzed both generally for hidden relationships to fraud, as well as with a specific focus on
code that is related to the delivery of ads, as example 612 illustrates. This information is compared to ads in the database 603 such as example ad 613 through system call 614 and finally compared to the rendered image of website 604 through system call 616, such that example ad 615 is matched against both ad 613 in database 603 and the image source code 612. When these comparisons do not match known properly formed websites and rendering, then a potential fraud exists. The nature of the fraud may indicate more complex types of fraud depending on the nature of the discrepancy and requires a person to evaluate the presence and nature of the fraud. Once this scenario is detected as a potential fraud by the artificial intelligence system 600 and a report 606 is generated via system request 610 such that a person 607 can review the potential fraud as illustrated in 601. Once the report is evaluated as being either fraud or not fraud then update 608 is triggered in the list of fraudulent agents shown in database 605 through system call 609. This module runs in conjunction with the other modules as described in claims 1 through 37, such that results of all the modules can be compared and the module described in Figure 6 can additionally be compared to activity on the blockchain and used to support evaluations of fraud.

Referring to Figure 7, a diagram of the token-based distributed peer-to-peer advertising network platform is presented. In this embodiment of an anti-fraud module, the artificial intelligence system 700 accesses database 702 through system call 711, which contains a log of user interface interactions as illustrated in 701. The information in database 702 contains events such as mouse clicks 710 as illustrated in 701, as well as timing information such that the artificial intelligence system 700 can compare this information to natural people visiting the website and accessing and fulfilling in the form elements such as 713 in web-page 701 to unnatural form filling activity know in the industry and those skilled-in-the-art whereby bots or automated software behaves like a real person filling in web forms. This activity is usually a level of user engagement that is highly valued by advertisers as a call-to-action and thus pays publishers well. The fraudulent form of this behavior earns publishers much higher payments than some other forms of advertising and, therefore, is a highly attractive form of fraud, as the software costs very little and can emulate the behavior of people quickly enough to create very high earnings for the publisher while the advertiser loses the intended outcome.
of the interaction which could be behavior such as completing a form for signing up as a new user, signing up for communications and additional information, or more simply providing survey information. Once this scenario is detected as a potential fraud by the artificial intelligence system 700 and a report 707 is generated via system request 706 such that a person 705 can review the potential fraud as illustrated in 703. Once the report is evaluated as being either fraud or not fraud then update 708 is triggered in the list of fraudulent agents shown in database 704 through system call 709. This module runs in conjunction with the other modules as described in claims 1 through 37, such that results of all the modules can be compared and the module described in this Figure can additionally be compared to activity on the blockchain and used to support evaluations of fraud.

Referring to Figure 8, a diagram of the token-based distributed peer-to-peer advertising network platform is presented. In this embodiment of an anti-fraud module, the artificial intelligence system 800 scans renderings of a given publisher website over time. In rendering of the website 803 at some point in the past, the artificial intelligence system makes a system call 812 to request a website rendering and compares this with a later example, website rendering 804 from system call 813, and finally with the most recent website rendering 805 made through system call 814. If a given website has a recent and radical departure of the amount and layout of ads in the past, such as illustrated in 805 whereby additional ads are present as shown in 805 by ads 815, this may indicate either the publisher engaging in fraud or the publisher may be hacked by a third-party group that has embedded their own advertising spots which siphon potential advertising profits from the legitimate publisher while also compromising the integrity of the publisher site as known in the industry and those skilled-in-the-art. Once this scenario is detected as a potential fraud or abuse by the artificial intelligence system 800 and a report 807 is generated via system request 811 such that a person 806 can review the potential fraud as illustrated in 801. Once the report is evaluated as being either fraud or not fraud then update 808 is triggered in the list of fraudulent agents shown in database 810 through system call 809. This module runs in conjunction with the other modules as described in claims 1 through 37, such that results of all the modules can be compared and the module described in this Figure can additionally be compared to activity on the blockchain and used to support evaluations of fraud.
Referring to Figure 9, a diagram of the token-based distributed peer-to-peer advertising network platform is presented. In this embodiment of an anti-fraud module, the artificial intelligence system 900 submits a request 910 to a database 911, which is populated by information about website visitors to specific publisher sites from all over the world as illustrated in 901 and contains information such as, but not limited to, geographic traffic. There exists a known in the industry and those skilled-in-the-art form of fraud whereby publishers who are running short of traffic sold within the context of a specific advertising deal and campaign will purchase traffic in order to bring their overall traffic within the level according to the advertising agreement. This traffic would represent a major shift in where and when the new traffic starts coming from partway through the campaign. The artificial intelligence system 900 uses the information from the database 911 to determine if an unusually and unnatural change is traffic has taken place, which indicates that fraudulent traffic may have been purchased. Once this scenario is detected as a potential fraud by the artificial intelligence system 900 and a report 906 is generated via system request 909 such that a person 905 can review the potential fraud as illustrated in 903. Once the report is evaluated as being either fraud or not fraud then update 907 is triggered in the list of fraudulent agents shown in database 904 through system call 908. This module runs in conjunction with the other modules as described in claims 1 through 37, such that results of all the modules can be compared and the module described in this Figure can additionally be compared to activity on the blockchain and used to support evaluations of fraud.

Referring to Figure 10, a diagram of the token-based distributed peer-to-peer advertising network platform is presented. In this embodiment of an anti-fraud module, the artificial intelligence system 1000 accesses a computer, server, mobile device, or virtual machine, as illustrated in 1003, through a system call 1009, whereby a website is loaded in a specially modified web browser that is able to monitor and report on the loading of pop-ups and pop-unders. There is a form of fraud known in the industry and those skilled-in-the-art whereby ads are loaded into pop-ups and pop-unders such that the ads generate revenue for the publisher but the ads themselves are never seen by the visit to the website since they can potentially be loaded in behind a given website as illustrated in 1003 by a
pop-up 1007 and pop-under 1010. Once this scenario is detected as a potential fraud by the artificial intelligence system 1000 and a report is generated via system request 1004 such that a person can review the potential fraud as illustrated in 1001. Once the report is evaluated as being either fraud or not fraud then update 1005 is triggered in the list of fraudulent agents shown in database 1002 through system call 1006. This module runs in conjunction with the other modules as described in claims 1 through 37, such that results of all the modules can be compared and the module described in this Figure can additionally be compared to activity on the blockchain and used to support evaluations of fraud.

Referring to Figure 11, a diagram of the token-based distributed peer-to-peer advertising network platform is presented. In this embodiment of an anti-fraud module, the artificial intelligence system 1100 access a rendering of the website 1102 via system call 1113, and is compared to ads in the ad database 1101 through system call 1112, whereby the system compares the size of the image and determines if the size actually displays is too small to be seen by the average web user and isn't a good comparison to the original image dimensions as listed in database 1101. There is a form of fraud known in the industry and those skilled-in-the-art whereby ads are loaded into a size or container such that they are 1 by 1 pixel in size and couldn't possibly deliver the intended results to an advertiser. This gives the publisher revenue from loading ads without having to impact the end-user experience on the publisher website. Once this scenario is detected as a potential fraud by the artificial intelligence system 1100 and a report 1105 is generated via system request 1111 such that a person 1104 can review the potential fraud as illustrated in 1103. Once the report is evaluated as being either fraud or not fraud then update 1109 is triggered in the list of fraudulent agents shown in database 1110 through system call 1108. This module runs in conjunction with the other modules as described in claims 1 through 37, such that results of all the modules can be compared and the module described in this Figure can additionally be compared to activity on the blockchain and used to support evaluations of fraud.

Referring to Figure 12, a diagram of the token-based distributed peer-to-peer advertising network platform is presented. In this embodiment of an anti-fraud module, the artificial intelligence system 1200 makes a request for
historical transaction information to 1201 via system call 1209 to return information from the ethereum transactions, as well as system call 1210 to the token transaction history as exposed by Smart Contracts built to return basic transaction information. A form of fraud known in the industry and those skilled-in-the-art whereby ad networks give payments to other ad agencies and networks as rewards for engaging them in specific ways desirable to the ad network such as increased sales, or engaging specific types of media or technologies. These payments are often kept secret from advertisers even though it is ultimately the advertisers that pay for the advertising and thus fund the payments or "kick-backs" as they are known. These kick-backs can be found by the artificial intelligence system whereby the transaction history on the block-chain 1201 can be used to make connections between transactions over time that show payments happening in association with particular agents on the network such that kick-backs can be inferred by the artificial intelligence system 1200 when compared against normal flows of payments between agents on the network over time. Once this scenario is detected as a potential fraud by the artificial intelligence system 1200 and a report 1205 is generated via system request 1208 such that a person 1204 can review the potential fraud as illustrated in 1202. Once the report is evaluated as being either fraud or not fraud then update 1206 is triggered in the list of fraudulent agents shown in database 1203 through system call 1207. This module runs in conjunction with the other modules as described in claims 1 through 37, such that results of all the modules can be compared and the module described in this Figure can additionally be compared to activity on the blockchain and used to support evaluations of fraud.

Referring to Figure 13, a diagram of the token-based distributed peer-to-peer advertising network platform is presented. In this embodiment of an anti-fraud module, a form of complex fraud known in the industry and those skilled-in-the-art as click injection, whereby a malware application 1305 installed on a device 1319 such as a computer, server, phone, tablet, watch, or other mobile device, accesses a locally installed app 1315 through system call 1307 when it is first executed by a mouse or touch event 1317 and intercepts the app emitting a normal notification of installation to its creators and advertisers, which would normally result in ads that drive a user to download and install an app, are instead copied and re-emitted through a system call
1313 as fraudulent installation notifications 1309 which misidentifies the referring ad and instead submits a publisher identification through system call 1310 that generates a payment to another publisher 1311 whom was never actually involved in displaying ads that delivered users to the app store to download and install the app. To combat and identify this form for fraud, the token-based distributed peer-to-peer advertising network platform provides software app 1306 which also accesses locally installed app 1315 through system call 1308, as well as accessing the base device operating system such that it detects the fake install event as illustrated by 1304 and extracts the malware 1305 emitting fraudulent notification 1309 through system call 1313 and emits the details of this fake notification 1309 to the artificial intelligence system 1300 through system call 1316 such that when the artificial intelligence system accessing this event through system call 1304 it can compare the information to known legitimate and fraudulent information in database 1303. Once this scenario is detected as a potential fraud by the artificial intelligence system 1300 and a report is generated via system request 1320 such that a person can review the potential fraud as illustrated in 1301. Once the report is evaluated as being either fraud or not fraud then an update is triggered in the list of fraudulent agents shown in database 1302 through system call 1321. This module runs in conjunction with the other modules as described in claims 1 through 37, such that results of all the modules can be compared and the module described in this Figure can additionally be compared to activity on the blockchain and used to support evaluations of fraud.

Referring to Figure 14, a diagram of the token-based distributed peer-to-peer advertising network platform is presented. In this embodiment of an anti-fraud module, the artificial intelligence system 1400 monitors and interacts with a device such as a computer, tablet, phone, watch, mobile device, or other system or virtual machine, such that a special browser 1405 is accessed through system call 1408 as illustrated in 1403 such that the browser 1405 is monitored for a form of fraud known in the industry and to those skilled-in-the-art as "automatic redirection". This is where an ad is not actually clicked or tapped by a user action or event but is instead trigger through website software code, which automatically triggers visiting the website as shown by 1406 which takes the browser to the website 1407 which is intended to be visited by the advertisement. Normally, this would
be a high value ad event which triggers a high payment to the publisher. In the case of fraud, the user never actually naturally clicked or touched the link and thus the publisher is receiving high payment for an event which was artificially created and violates the intention and spirit of the advertising agreement. This is shown in illustration 1404, whereby the browser 1407 displays automatically another website which is detected by a system call interaction 1409 upon which the artificial intelligence system 1400 receives information about the redirection event 1406, as well as the supporting metadata about the event. Once this scenario is detected as a potential fraud by the artificial intelligence system 1400 and a report is generated via system request 1410, such that a person can review the potential fraud as illustrated in 1401. Once the report is evaluated as being either fraud or not fraud then an update is triggered in the list of fraudulent agents shown in database 1402 through system call 1411. This module runs in conjunction with the other modules as described in claims 1 through 37, such that results of all the modules can be compared and the module described in this Figure can additionally be compared to activity on the blockchain and used to support evaluations of fraud.

Referring to Figure 15, a diagram of the token-based distributed peer-to-peer advertising network platform is presented. In this embodiment of an anti-fraud module, the artificial intelligence system 1500 makes a system call request 1516 to database 1505, which is a store of information about individual users purchasing and website activity, as well as any brick-and-mortar in-store interactions or purchases, as recorded by system calls 1511, 1512, 1513, 1514, and 1515. In this embodiment, a user accesses a website 1506 and accesses information on specific topic or other information related to a purchasing decision. This leads the user to click on an ad which triggers 1516 visiting another related website 1507. On this site, the user again investigates topics around a potential purchasing decision and this leads the user to click on an ad which triggers 1517 visiting another related website 1508. On this site, the user again investigates topics around a potential purchasing decision and this leads the user to click on an ad which triggers 1518 visiting another related website 1509 and because the user now has a history making it clear they are a potential high value user for ads targeting a purchase, this is the step whereby a form of fraud known in the industry and those skilled-in-the-art takes place. Since this user is now on the threshold of making a
purchasing decision, the ads that are shown have a very high payout to the website publishers. This situation has lead to automated website visiting bot farms as known in the industry and those skilled in the art, which recreate the conditions of a high value customer, which is, in actuality, a fake person simulated by the bot farm software. In order to deter and starve the conditions, which create this fraud potential, the token-based distributed peer-to-peer advertising network platform looks at actual purchasing data 1515 supplied by an actual purchase as shown in the purchasing event 1519, which leads to the final sale recorded in database 1515 by 1510 which may be a website but, in another embodiment, could be a terminal or device in a brick-and-mortar in-store system.

Once this scenario is detected as a sale by the artificial intelligence system 1500, a scan of the database 1505 is taken via system request 1516, such that the system is able to determine connections in events 1511, 1512, 1513, 1514, and 1515, and in time data surrounding those events, such that each of the websites 1506, 1507, 1508, and 1509, leading up to the purchase can be paid post-purchase as an additional publisher payment for a confirmed purchasing on 1510. This system is an improvement over rewarding the publisher at 1509 since the fraud cannot be executed in this system without actually making the final purchase at 1510 which makes the fraud no longer financially tenable.

In this embodiment, an optional step takes place whereby the artificial intelligence system 1500 creates a report for a person to review and ensure that, in fact, a proper chain of events has taken place which warrants a post-purchase payment to publishers. A report is generated via system request 1501, such that a person can review the potential post-purchase report as illustrated in 1502. Once the report is evaluated as being worthy of a post-purchase payment, then an update is triggered marking publishers to receive a post-purchase payment shown in database 1504 through system call 1503. This module runs in conjunction with the other modules as described in claims 1 through 37, such that results of all the modules can be compared and the module described in this Figure can additionally be compared to activity on the blockchain and used to support evaluations of post-purchase worthy transactions.
Although the instant invention has been described with respect to a specific embodiment thereof, various changes and modifications are optionally carried out by those skilled-in-the-art without departing from the scope of the invention. Therefore, it is intended that the instant invention encompass such changes and modifications as fall within the scope of the appended claims.