CLAIMS

1. A system for providing non-repudiation and data integrity of communications in ad sales online, the system comprising one or more servers communicably connected to a communications network, the one or more servers including at least one processor configured for:

receiving, from a first party, an ad request for an ad impression available for sale, wherein the ad request includes a plurality of attributes associated with the ad impression and a first cryptographic proof that provides non-repudiation and data integrity of the ad request;

authenticating non-repudiation and data integrity of the ad request by querying a blockchain; wherein the blockchain comprises a public key infrastructure;

accessing a database of second parties seeking to purchase ads online, wherein the database stores attributes associated with each second party;

matching the ad request with a selected second party in the database based on the attributes associated with each second party in the database and the attributes associated with the ad impression of the ad request;

and,

transmitting, to the first party, a message comprising an ad for the selected second party and a second cryptographic proof that provides non-repudiation and data integrity of the message, so as to fill the ad impression with the ad for the selected second party;

wherein the public key infrastructure comprises a public key associated with the first party;

wherein the public key infrastructure authenticates the first cryptographic proof against the public key associated with the first party;

wherein the first cryptographic proof comprises a third cryptographic proof of the first party; and

wherein the public key infrastructure authenticates the third cryptographic proof against the public key associated with the first party.

2. The system of claim 1, wherein the second cryptographic proof of the message comprises a fourth cryptographic proof of the system, and wherein the blockchain comprises ~~a~~ the public key infrastructure that authenticates the fourth cryptographic

proof of the system against a public key associated with the system.

3. The system of claim 2, wherein the second cryptographic proof of the message comprises a signature of the system, and wherein the blockchain authenticates the signature of the system against the public key associated with the system.

4. The system of claim 1, wherein the at least one processor is further configured for recording of at least a fifth cryptographic proof of the message in the blockchain.

5. The system of claim 1, wherein the step of receiving, from a first party, an ad request, further comprises:

receiving, from ~~a~~ the first party, ~~an~~ the ad request for ~~an~~ the ad impression available for sale, wherein the ad request includes ~~a~~ the plurality of attributes associated with the ad impression, consumer behavior data associated with the ad impression and the first cryptographic proof that provides non-repudiation and data integrity of the ad request.

6. The system of claim 1, wherein the step of matching the ad request, further comprises:

matching the ad request with ~~a~~ the selected second party in the database based on the attributes associated with each second party in the database, the attributes associated with the ad impression of the ad request, and consumer behavior data associated with the ad impression of the ad request.

7. The system of claim 1, wherein the at least one processor is further configured for broadcasting to the second parties a message including a sixth cryptographic proof that includes consumer behavior data, wherein the sixth cryptographic proof allows only a subset of the second parties to open and view the consumer behavior data.

8. A system for providing non-repudiation and data integrity of communications in ad sales online, the system comprising one or more servers communicably connected to a communications network, the one or more servers including at least one processor configured for:

providing a blockchain comprising a public key infrastructure including public keys of parties against which a plurality of cryptographic proofs of said parties may be authenticated;

wherein the public keys of parties comprise a public key associated with ~~the~~ a first party;

receiving, from ~~a~~ the first party, an ad request for an ad impression available for sale, wherein the ad request includes a plurality of attributes associated with the ad impression and a first cryptographic proof that provides non-repudiation and data integrity of the ad request; authenticating non-repudiation and data integrity of the ad request by querying the blockchain;

wherein the authenticating comprises authenticating the first cryptographic proof against the public key associated with the first party;

wherein the first cryptographic proof comprises a third cryptographic proof of the first party; and

wherein the public key infrastructure authenticates the third cryptographic proof against the public key associated with the first party;

accessing a database of second parties seeking to purchase ads online, wherein the database stores attributes associated with each second party;

matching the ad request with a selected second party in the database based on the attributes associated with each second party in the database and the attributes associated with the ad impression of the ad request;

and,

transmitting, to the first party, a message comprising an ad for the selected second party and a second cryptographic ~~second~~ proof that provides non-repudiation and data integrity of the message, so as to fill the ad impression with the ad for the selected second party.

9. The system of claim 8, wherein the second cryptographic proof of the message comprises a fourth cryptographic proof of the system, and wherein the blockchain allows the fourth cryptographic proof of the system to be authenticated against a public key associated with the system.

10. The system of claim 9, wherein the second cryptographic proof of the message comprises a signature of the system, and wherein the blockchain authenticates the

signature of the system against the public key associated with the system.

11. The system of claim 10, wherein the at least one processor is further configured for recording of at least a fifth cryptographic proof of the message in the blockchain.

12. The system of claim 11, wherein the step of receiving, from a first party, an ad request, further comprises:

receiving, from ~~a~~ the first party, ~~an~~ the ad request for ~~an~~ the ad impression available for sale, wherein the ad request includes ~~a~~ the plurality of attributes associated with the ad impression, consumer behavior data associated with the ad impression and the first cryptographic proof that provides non-repudiation and data integrity of the ad request.

13. The system of claim 12, wherein the step of matching the ad request, further comprises:

matching the ad request with ~~a~~ the selected second party in the database based on the attributes associated with each second party in the database, the attributes associated with the ad impression of the ad request, and the consumer behavior data associated with the ad impression of the ad request.

14. The system of claim 13, wherein the at least one processor is further configured for broadcasting to the second parties a message including a sixth cryptographic proof that includes the consumer behavior data, wherein the sixth cryptographic proof allows only a subset of the second parties to open and view the consumer behavior data.

15. A system for providing non-repudiation and data integrity of communications in ad sales online, the system comprising one or more servers communicably connected to a communications network, the one or more servers including at least one processor configured for:

providing a blockchain comprising a public key infrastructure including public keys of parties against which a plurality of cryptographic proofs of said parties may be authenticated;

wherein the public keys of parties comprise a public key associated with ~~the~~ a first party;

distributing a separate cryptographic key to each of a plurality of parties and creating a separate space on the blockchain corresponding to each of the plurality of parties, such that each of the plurality of parties may edit its corresponding space on the blockchain using a cryptographic key received from the system;

receiving, from ~~a~~ the first party, an ad request for an ad impression available for sale, wherein the ad request includes a plurality of attributes associated with the ad impression and a first cryptographic proof that provides non-repudiation and data integrity of the ad request;

authenticating non-repudiation and data integrity of the ad request by querying the blockchain;

wherein the authenticating comprises authenticating the first cryptographic proof against the public key associated with the first party;

wherein the first cryptographic proof comprises a third cryptographic proof of the first party; and

wherein the public key infrastructure authenticates the third cryptographic proof against the public key associated with the first party;

accessing a database of second parties seeking to purchase ads online, wherein the database stores attributes associated with each second party;

matching the ad request with a selected second party in the database based on the attributes associated with each second party in the database and the attributes associated with the ad impression of the ad request;

and,

transmitting, to the first party, a message comprising an ad for the selected second party and a second cryptographic proof that provides non-repudiation and data integrity of the message, so as to fill the ad impression with the ad for the selected second party.

16. The system of claim 15, wherein the at least one processor is further configured for broadcasting to the second parties a second message including a fourth cryptographic proof that includes consumer behavior data, wherein the fourth cryptographic proof allows only a subset of the second parties to open and view the consumer behavior data.

17. The system of claim 16, wherein a fifth cryptographic proof of a second party message comprises a sixth cryptographic proof of the second party, and wherein the blockchain authenticates the sixth cryptographic proof of the second party against a public key associated with the second party; wherein the first cryptographic proof of the message comprises a seventh cryptographic proof of the system; and
wherein the blockchain authenticates the seventh cryptographic proof of the system against a public key associated with the system.

18. The system of claim 17, wherein the first cryptographic proof of the message comprises a signature of the system, and wherein the blockchain allows the signature of the system to be authenticated against the public key associated with the system.