

What is claimed is:

1. A method for presenting an advertisement in conjunction with media content, the method comprising:

transmitting, with a transceiver of a first computing device, a first message to a second computing device, the first message requesting media content from the second computing device, the media content having a defined location at which an advertisement can be presented in conjunction with the media content;

receiving, with the transceiver, a second message from the second computing device, the second message including the media content;

wherein the second message comprises at least one of (i) a first content mapping key from a set of content mapping keys associated with the second computing device, (ii) associations between each content mapping key in the set of content mapping keys, and (iii) at least one media content classifier being stored on the at least one blockchain;

selecting, with a processor of the first computing device, a first advertisement from a set of advertisements based on a first targeting model for the first advertisement, the first targeting model being stored on at least one blockchain and defining a target audience for the first advertisement; and

presenting, with an output device of the first computing device, the first advertisement in conjunction with the media content at the defined location.

2. The method according to claim 1, ~~wherein the second message includes a first content mapping key from a set of content mapping keys associated with the second computing device, associations between each content mapping key in the set of content mapping keys~~

~~and at least one media content classifier being stored on the at least one blockchain, the method~~ further comprising:

exchanging, with the transceiver, at least one message with the second computing device to obtain a first proof of interest from the second computing device, the first proof of interest being a signature signed under the first content mapping key and of first data at least including (i) the first content mapping key and (ii) a first public key of the first computing device; and

storing, in a memory of the first computing device, the first proof of interest with a first plurality of proofs of interest, each proof of interest in the first plurality of proofs of interest being a signature signed under a respective content mapping key and of data at least including (i) the respective content mapping key and (ii) the first public key of the first computing device, associations between the respective content mapping key under which each proof of interest in the first plurality of proofs of interest is signed and at least one respective media content classifier being stored on the at least one blockchain.

3. The method according to claim 2, the exchanging the at least one message with the second computing device to obtain the first proof of interest further comprising:

generating, with the processor, a random private key and a corresponding random public key;

calculating, with the processor, a blinded message as the random public key multiplied with a hash of the first data;

transmitting, with the transceiver, the blinded message to the second computing device;

receiving, with the transceiver, a signature of the blinded message from the second computing device, the signature of the blinded message being signed under the first content mapping key; and

determining, with the processor, the first proof of interest based on the signature of the blinded message and using the random private key.

4. The method according to claim 2 further comprising:

periodically replacing the first public key with a new public key by:

generating, with the processor, the new public key and a corresponding private key;

transmitting, with the transceiver, the new public key to a third computing device; and

receiving, with the transceiver, a certificate for the new public key from the third computing device, the certificate being stored on the at least one blockchain by the third computing device.

5. The method according to claim 2 further comprising, prior to transmitting the first message to the second computing device:

receiving, with the transceiver, a respective targeting model for each respective advertisement in the set of advertisements, each respective targeting model being stored on the at least one blockchain and defining a respective target audience for the respective advertisement;

evaluating, with the processor, the respective targeting model for each respective advertisement in the set of advertisements based on the first plurality of proofs of interest, to determine whether a user associated with the first computing device fits within the respective target audience for each respective advertisement in the set of advertisements; and

generating, with the processor, a list of advertisements from the set of advertisements for which the user fits within the respective target audience,

wherein the selecting the first advertisement further comprises selecting the first advertisement from the list of advertisements.

6. The method according to claim 5, the evaluating the respective targeting model for each respective advertisement in the set of advertisements further comprising:

evaluating the respective targeting model based on the at least one respective media content classifier associated with the content mapping key under which each proof of interest in the first plurality of proofs of interest was signed.

7. The method according to claim 5, the evaluating the respective targeting model for each respective advertisement in the set of advertisements further comprising:

in response to the first plurality of proofs of interest stored in the memory having less than a predetermined number of proofs of interest, evaluating the respective targeting model for each respective advertisement in the set of advertisements based on a second plurality of proofs of interest, to determine whether the user associated with the first

computing device fits within the respective target audience for each respective advertisement in the set of advertisements,

wherein the memory of the first computing device stores the second plurality of proofs of interest, each proof of interest in the second plurality of proofs of interest being a signature signed under a respective content mapping key and of data at least including (i) the respective content mapping key and (ii) a second public key of the first computing device.

8. The method according to claim 21, wherein the second message includes a first set of constraints defining allowable advertisements that can be presented in conjunction with the media content at the defined location, the method further comprising:

receiving, with the transceiver, a respective second set of constraints for each of a plurality of advertisements from the set of advertisements, each respective second set of constraints being stored on the at least one blockchain and defining allowable media content that the respective advertisement can be presented in conjunction with; and

selecting, with the processor, the first advertisement from the set of advertisements based on the first targeting model for the first advertisement, the first set of constraints, and the respective second set of constraints for the first advertisement.

9. The method according to claim 2, further comprising:

identifying a subset of proofs of interest from the first plurality of proofs of interest, based on the first targeting model, the set of proofs of interest being signed under content mapping keys associated with media content classifiers that indicate that a user

associated with the first computing device fits within the target audience defined first targeting model;

determining, with the processor, an aggregated signature as an aggregation of the subset of proofs of interest; and

transmitting, with the transceiver, a third message to a third computing device indicating that the first advertisement was presented in conjunction with the media content, the third message including the aggregated signature.

10. The method according to claim 9, the determining the aggregated signature further comprising:

determining the aggregated signature as a product of all of the proofs of interest in the subset of proofs of interest.

11. The method according to claim 9, wherein the second message includes a first set of constraints defining allowable advertisements that can be presented in conjunction with the media content at the defined location and includes a signature of the first set of constraints under a public key of the second computing device, the method further comprising:

transmitting, with the transceiver, the third message to the third computing device, the third message including the aggregated signature, the first set of constraints, and the signature of the first set of constraints.

~~12.— A method for providing an advertisement impression in which an advertisement is presented in conjunction with media content, the method comprising:~~

~~receiving, with a transceiver of the second computing device, a first message from a first computing device, the first message requesting media content from the second computing device, the media content having a defined location at which an advertisement can be presented in conjunction with the media content;~~

~~transmitting, with the transceiver, a second message to the first computing device, the second message including the media content;~~

~~receiving, with the transceiver, a third message from a third computing device indicating that an advertisement is presented in conjunction with media content to form a valid advertisement impression, the third message including a signature under a public key of the third computing device; and~~

~~transmitting, with the transceiver, a fourth message to at least one of a fourth computing device and at least one first smart contract stored on at least one blockchain, the fourth message including the signature under the public key of the third computing device, the fourth message causing an entity associated with the second computing device to receive credit or payment for valid advertisement impression.~~

~~13.— The method according to claim 12, wherein the second message includes a first content mapping key from a set of content mapping keys associated with the second computing device, associations between each content mapping key in the set of content mapping keys and at least one media content classifier being stored on the at least one blockchain, the method further comprising:~~

~~exchanging, with the transceiver, at least one message with the first computing device to provide a first proof of interest to the first computing device, the first proof of interest being a signature signed under the first content mapping key and of first data at least including (i) the first content mapping key and (ii) a first public key of the first computing device.~~

~~14. The method according to claim 13, the exchanging the at least one message with the first computing device to provide the first proof of interest further comprising:~~

~~receiving, with the transceiver, a blinded message from the first computing device, the blinded message being a random public key multiplied with a hash of the first data;~~

~~determining, with the processor, a signature of the blinded message by signing the blinded message under the first content mapping key;~~

~~transmitting, with the transceiver, the signature of the blinded message to the first computing device, the first proof of interest being determined by the first computing device based on the signature of the blinded message.~~

~~15. The method according to claim 13 further comprising:~~

~~generating, with the processor, set of content mapping keys and a corresponding set of private keys; and~~

~~transmitting, with the transceiver, a fourth message to at least one second smart contract stored on the at least one blockchain, the fourth message including the set of~~

~~content mapping keys and indicating the associations between each content mapping key in the set of content mapping keys and the at least one media content classifier;~~

~~wherein the fourth message causes publication, on the at least one blockchain, of the set of content mapping keys and the associations between each content mapping key in the set of content mapping keys and the at least one media content classifier.~~

~~16. The method according to claim 15 further comprising:~~

~~periodically replacing the set of content mapping keys with a new set of content mapping keys by:~~

~~generating, with the processor, the new set of content mapping keys and a corresponding new set of private keys; and~~

~~transmitting, with the transceiver, a fifth message including the new set of content mapping keys to the at least one second smart contract stored on the at least one blockchain,~~

~~wherein receipt of the fifth message by the at least one second smart contract causes publication of the new set of content mapping keys on the at least one blockchain.~~

~~17. The method according to claim 16, wherein:~~

~~the at least one blockchain stores multiple sets of content mapping keys associated with the second computing device;~~

~~receipt of the fifth message by the at least one second smart contract causes publication of the new set of content mapping keys on the at least one blockchain as one of the multiple sets of content mapping keys associated with the second computing device; and~~

~~receipt of the fifth message by the at least one second smart contract causes revocation of an oldest of the multiple sets of content mapping keys associated with the second computing device on the at least one blockchain.~~

~~18. The method according to claim 12, wherein the second message includes a first set of constraints defining allowable advertisements that can be presented in conjunction with the media content at the defined location.~~

~~19. The method according to claim 18, wherein the second message includes a signature of the first set of constraints under a public key of the second computing device.~~

~~20. The method according to claim 12, wherein the signature under the public key of the third computing device is an aggregated signature, the aggregated signature being an aggregation of a plurality of signatures, each under a respective public key of a respective computing device in a plurality of computing devices that includes the third computing device.~~