Claims:

1. A method for establishing cryptographic communications between an attention application terminal and a guardian terminal with a black box accumulator (BBA) in an attention rewards architecture comprising:

receiving an advertising (ad) catalog with N ads at the attention application terminal, wherein N corresponds to a quantity of ads in the ad catalog;

receiving an ad policy vector of length N, wherein each index in the ad policy vector corresponds to an ad in the ad catalog and represents a reward value for interactions with the ad at the attention application terminal;

transmitting to the guardian terminal, an initialization request for a signed BBA tuple using a source of randomness supplied by the attention application terminal with counters initialized at zero, the initialization request including a request for a first signature over the BBA tuple;

receiving, from the guardian terminal, the first signature;

storing, at the attention application terminal, the first signature, the BBA tuple, and the source of randomness, used in the initialization request;

matching ads from the ad catalog with a user of the attention application terminal;

displaying matched ads to the user at the attention application terminal;

detecting user interactions with the matched ads at the attention application terminal;

repeatedly and automatically incrementing an ad interaction counter based on the detected user interactions to yield a notice requesting an update to an ad interaction vector;

randomizing the BBA tuple to generate a randomized BBA tuple;

transmitting the randomized BBA tuple to the guardian terminal with the notice requesting the update to the ad interaction vector;

receiving, from the guardian terminal, a second signature over a new BBA tuple;

upon receipt of the second signature over the new BBA tuple, storing, at the attention application terminal, updated randomization; and

verifying the new BBA tuple is a correct reflection of ad interaction state requested in the notice requesting an update to the ad interaction vector.

2. The method of claim 1, further comprising:

de-randomizing, at the attention application terminal, the new BBA tuple to yield a proof of correctness of the reward owed;

generating a request for rewards based on the proof of rewards owed by:

disclosing an identifier of the BBA;

computing an inner product between the ad interaction vector and the ad policy vector;

proving an addition of all counters does not exceed a limit set by the guardian terminal; and

generating a zero knowledge proof of correctness and transmitting the proof of correctness to the guardian terminal.

3. The method of claim 2, further comprising:

receiving, at the attention application terminal, a reward based on the proof of correctness of reward owed; and

zeroing out the ad interaction counter.

4. The method of claim 1, wherein transmitting the initialization request comprises:

transmitting the initialization request through an anonymous channel.

5. The method of claim 1, wherein transmitting the randomized BBA tuple comprises:

transmitting the randomized BBA tuple from the attention application terminal through a broadcast encryption terminal.

6. The method of claim 1, further comprising:

committing, by the attention application terminal, the BBA tuple and the request for rewards based on proof of rewards owed to a public blockchain.

7. The method of claim 6, wherein the public blockchain includes a smart contract equipped to verify computation of proof of rewards owned committed thereon and records a verification to the public blockchain if the proof of rewards owed is correct.

8. A decentralized system for establishing cryptographic communications with a black box accumulator (BBA) in an attention rewards architecture comprising:

an attention application computing system including a computer network communications interface, a memory storing instructions, and a processor that, when executing the instructions causes the processor to:

request an initialized BBA from a guardian computing system;

receive an initialized and signed BBA from the guardian computing system;

record ad interactions with a user of the attention application computing system with ads displayed from an ad catalog to yield an ad interaction counter;

randomize the BBA to yield a randomized BBA;

transmit the randomized BBA and a notice requesting update of the randomized BBA according to the ad interaction counter;

receive a signed and updated BBA according to the notice requesting update of the randomized BBA;

generate a reward proof based on the signed and updated BBA and an ad policy vector; and

commit the reward proof based on the signed and updated BBA to a public blockchain.

9. The system of claim 8, wherein to commit the reward proof, the instructions are executable by the processor to transmit the reward proof to the guardian computing system to cause the reward proof to be committed to the public blockchain.

10. The system of claim 8, wherein communications between the attention application computing system and the guardian computing system are according to an anonymous channel.

11. The system of claim 8, wherein the public blockchain includes a smart contract equipped to verify computation of proof of rewards owned committed thereon and records a verification to the public blockchain if the proof of rewards owed is correct.

12. The system of claim 8, wherein communications between the attention application computing system and the guardian computing system are according to a broadcast encryption channel wherein only qualified advertisers may read the communications under a distributed keying arrangement.

13. A decentralized system for establishing cryptographic communications with a black box accumulator (BBA) in an attention rewards architecture comprising:

a guardian computing system including a computer network communications interface, a memory storing instructions, and a processor that, when executing the instructions causes the processor to:

receive a request for an initialized BBA from an attention application computing system;

initialize and sign a BBA with a null ad interaction vector with a secret key;

transmit the BBA to the attention application computing system;

receive a randomized BBA and a notice requesting update of the randomized BBA according to an ad interaction counter on the attention application computing system;

apply a state update to the randomized BBA and sign the randomized BBA with the secret key to yield an updated and signed randomized BBA;

transmit the updated and signed randomized BBA to the attention application computing system;

search a copy of a public blockchain for a request for reward payment and a proof of correctness of rewards for the updated and signed randomized BBA;

determine whether the proof of correctness of rewards for the updated and signed randomized BBA is valid; and

if the updated and signed randomized BBA is valid, then broadcast a blockchain transaction transmitting rewards to the attention application computing system.

14. The system of claim 13, wherein to receive the request for the initialized BBA, the instructions are executable by the processor to:

receive the request for initialized BBA through an anonymous channel.

15. The system of claim 13, wherein communications with the attention application computing system are according to a broadcast encryption channel.

16. The system of claim 13, wherein the public blockchain includes a smart contract equipped to verify computation of proof of rewards owned committed thereon and records a verification to the public blockchain if the proof of rewards owed is correct.