

What Is Claimed Is:

1. A computer-implemented method for privacy-preserving verification of profit-sharing between users, wherein the method is performed by one or more nodes in a blockchain system and comprises:

receiving instructions to setup a verification program for automatically determining whether a plurality of users are sharing a profit according to one or more defined rules;

receiving protected transaction information, the protected transaction information comprising a protected value P_i representing a shared profit p_i in a protected format, the shared profit p_i being an amount to be distributed to a user i of the plurality of users, wherein the shared profit p_i is not received by the blockchain system;

processing the protected transaction information using the verification program to automatically determine whether the amount to be distributed to the user i is in accordance with the one or more defined rules;

in response to a determination that the amount to be distributed to the user i is in accordance with the one or more defined rules, accepting the protected value P_i as valid, wherein accepting the protected value P_i as valid comprises recording the protected value P_i on a blockchain; and

in response to a determination that the amount to be distributed to the user i is not in accordance with the one or more defined rules, refusing to accept a recordation of the protected value P_i .

2. The method of claim 1, wherein the verification program comprises a smart contract deployed in the blockchain system.
3. The method of any preceding claim, wherein the protected value P_i is a commitment value of the shared profit p_i .
4. The method of claim 3, wherein the protected value P_i is calculated based on an additively homomorphic commitment scheme.
5. The method of any preceding claim, wherein the protected transaction information further comprises a protected revenue R representing a revenue r in the protected format and a protected cost C representing a cost c in the protected format.
6. The method of claim 5, wherein the verification program further defines a sharing factor α_i for the user i .
7. The method of claim 6, wherein the processing the protected value P_i using the verification program further comprises:

determining that the amount to be distributed to the user i is in accordance with the one or more defined rules when $P_i = (R/C)^{\alpha_i}$.
8. A device for privacy-preserving verification of profit-sharing between users, comprising:

one or more processors; and

one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any of claims 1 and 4-9.

9. An apparatus for privacy-preserving verification of profit-sharing, the apparatus comprising a plurality of modules for performing the method of any of claims 1 and 4-9.

10. A non-transitory computer-readable medium having stored therein instructions that, when executed by a processor of a device, cause the device to perform the method of any of claims 1 and 4-9.