BLOCKCHAIN ORACLE METHODS AND SYSTEMS BASED ON ZERO-KNOWLEDGE PROOF

CROSS REFERENCE TO RELATED APPLICATIONS

This application claims priority to and the benefit of U.S. Provisional Application Ser. No. 63/447,615 entitled "Blockchain Middleware Methods and Systems Based on Zero-Knowledge Proof," filed on 22 February 2023, U.S. Provisional Application Ser. No. 63/449,812 entitled "Blockchain Middleware Methods and Systems Based on Zero-Knowledge Proof," filed on 3 March 2023, U.S. Provisional Application Ser. No. 63/614,662 entitled "Blockchain Middleware Methods and Systems Based on Zero-Knowledge Proof," filed on 25 December 2023, and U.S. Provisional Application Ser. No. 64/023,351 entitled "Blockchain Middleware Methods and Systems Based on Zero-Knowledge Proof," filed on 19 January 2024, the disclosures of which are incorporated herein by reference in their entireties.

This application relates to a concurrently filed, co-pending application U.S. patent application Ser. No. 18,443,217, entitled "Blockchain Middleware Methods and Systems Based on Zero-Knowledge Proof With Recursive Prover" by Jiatian Wang and Xiaohang Yu, owned by the applicants of this application and incorporated herein by reference.

BACKGROUND

Technical Field

[0001] The present disclosure generally relates to blockchain technologies and, more particularly blockchain middleware systems with zero-knowledge proof.

Background Art

[0002] Current solutions in conducting credible verification of the correctness, validity, and availability of the source, processing, and delivery of blockchain data generally are divided in two types. The first type is generally known as "trust endorsement" in the context of a centralized scenario. Social credit such as business reputation is used to guarantee data credibility through trust endorsement and other methods. The second type is referred to as "reward and punishment incentives" in the contest of a decentralized scenario. A certain degree of credibility is maintained through a reward and punishment mechanism linked to economic incentives, i.e., rewarding honest participants and punishing evil or inaction participants. Although "trust endorsement" and "reward and punishment incentives" are widely used in the blockchain industry, both of these two