BLOCKCHAIN ORACLE METHODS AND SYSTEMS BASED ON ZERO-KNOWLEDGE PROOF

Embodiments of the present disclosure are directed to systems and methods for a zero-knowledge (zk) oracle (zkOracle) system that executes customized computation code for blockchain applications and secure the execution result by providing one or more zero-knowledge proofs (zkp). The disclosure provides a zkMiddleware structure (or blockchain middleware) and how zero-knowledge proofs can be applied for verifying blockchain states. This in turn enables data collection, verification, and process capabilities for blockchain-based applications by establishing credibility and trust based solely on verifiable blockchain technologies, computuations, and underlying mathematics.

FIG. 1