

METHODS AND DEVICES FOR PROTECTING AND VERIFYING STATE INFORMATION OF RECORD

ABSTRACT

Disclosed herein are methods, devices, and apparatuses, including computer programs stored on computer-readable media, for verifying state transition of a record. One of the methods includes: receiving a transaction submitted by a user, the transaction including an identification of the record, a protected state value representing a state of the record after performing an operation on the record, and a proof; determining whether the proof is acceptable by determining whether the proof indicates that the user is in possession of information generated at least partially based on a plaintext value of the state of the record after performing the operation; in response to a determination that the proof is unacceptable, refusing to process the transaction submitted by the user; and in response to a determination that the proof is acceptable, setting a recorded state of the record to the protected state value.

Fig. 5