ABSTRACT

DEVICE AND METHOD FOR SELF-SOVEREIGN IDENTITY AUTHENTICATION

The present invention relates to a blockchain-based identity authentication technique, and more specifically, to a self-sovereign identity authentication device and a method thereof, which can update identity information using a registration blockchain and a revocation blockchain when self-sovereign identity authentication is performed based on a blockchain, and securely manage self-sovereign identity information by cryptographically splitting and storing the information. According to an embodiment of the present invention, as the technical characteristics of the blockchain can be maintained as they are when an identity is authenticated, forgery and falsification of information are impossible. In addition, it is easy to defend against social engineering attacks such as a human error through secure split, restoration, and backup management of a private key, and the private key may be restored although the user platform in which the private key is stored is lost or damaged.

[No. Fig]