

ABSTRACT

Provided is an electronic cash-based offline transaction method and system. The method includes: receiving, by a back-end server from a smart card, an anti-replay factor generated by the smart card; determining, by the back-end server in accordance with a predetermined
5 algorithm, whether an abnormal transaction occurs on the smart card, generating, by the back-end server when no abnormal transaction occurs, a security information signature by signing security information with a private key of the back-end server, and transmitting, by the back-end server, the security information and the security information signature to the smart card (S2); and receiving, by the smart card, the security information and the security information
10 signature from the back-end server, performing a signature verification, by the smart card, on the security information signature by using a public key of the back-end server, determining, by the smart card after the signature verification succeeds, whether the anti-replay factor in the security information is consistent with the anti-replay factor generated by the smart card, and storing, by the smart card, the active field information, when the anti-replay factor in the
15 security information is consistent with the anti-replay factor generated by the smart card (S3).
(Fig.1)