ABSTRACT

A PRIVATE KEY SECURITY MANAGEMENT METHOD OF A COLD WALLET AND A COLD WALLET SERVER THEREOF

A private key security management method of a cold wallet and a cold wallet server thereof, the user provides a mnemonic to generate a private key and a wallet address, and then the system stores the private key fragments in volatile storage devices at different storage addresses, such as RAM. Even if the cold wallet server is hacked and causes data leakage of the RAM, but will not cause the entire private key information leakage, that is, the hacker can only obtain part of the private key fragments, and cannot piece together the complete private key to control the cold wallet assets, which greatly reduces the overall private key leakage risk caused by local security issues. Furthermore, if the cold wallet server detects an illegal intrusion, it will initiate a system restart or power-off protection measure. Once the system restarts or cut off power, the private key fragments stored in the RM will also disappear, further improving the security and reliability of key protection.

Fig. 1