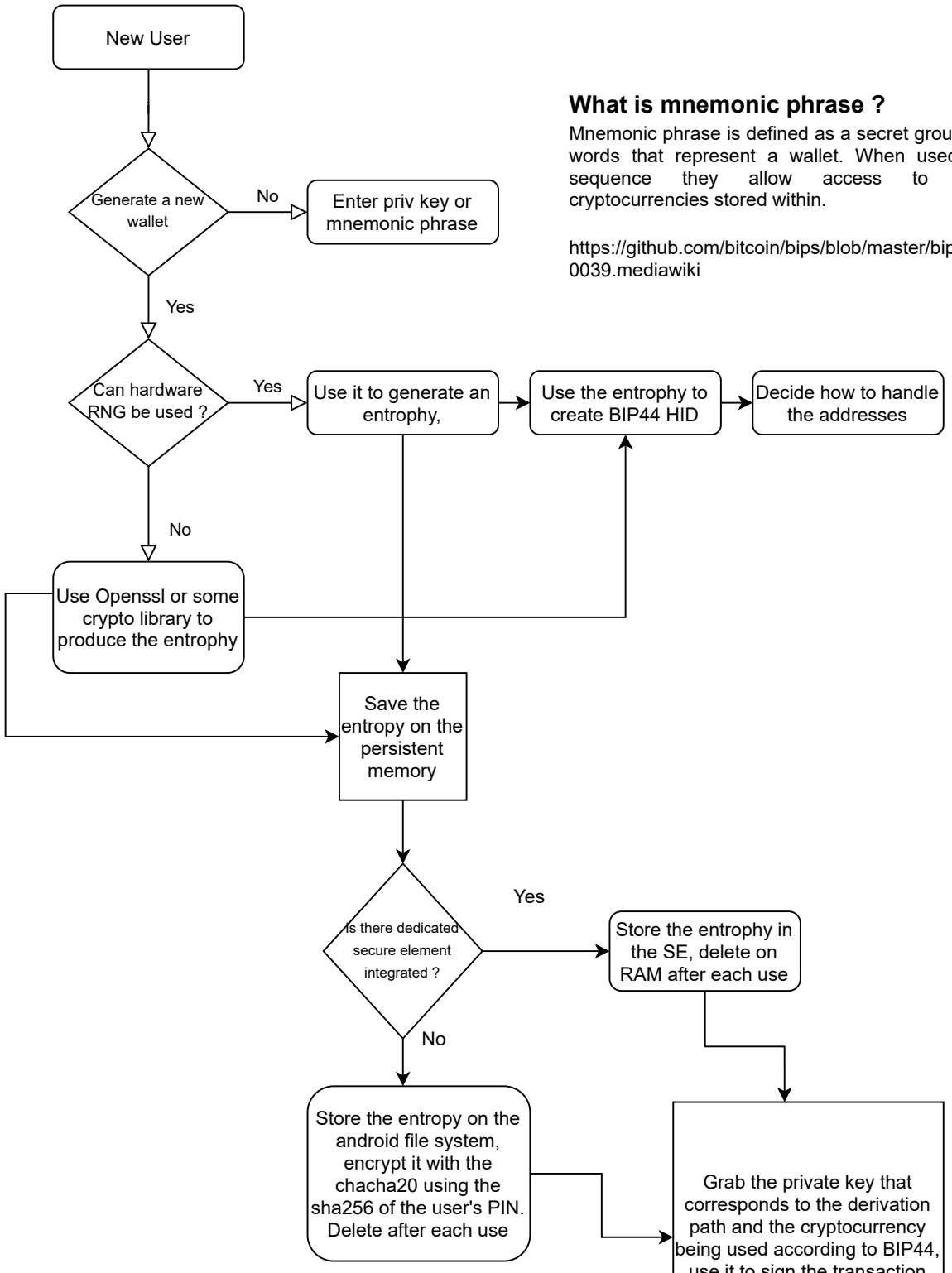

What is mnemonic phrase ?

Mnemonic phrase is defined as a secret group of words that represent a wallet. When used in sequence they allow access to the cryptocurrencies stored within.

https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

How to use the encrypted entrophy

The entropy needs to be read from the filesystem / secure eeprom. Decrypted using the SHA256 of the user's pin. Afterwards according to the derivation path and the cryptocurrency being used, the corresponding private key must be calculated.

https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki