

BLOCK CONTENT EDITING METHODS AND APPARATUSES

ABSTRACT

One or more embodiments of the present specification provide a block content editing method, and apparatus of using the same. The method can include the following: a blockchain node Bi receives a block editing transaction, which is used to edit original block content m of a block Qi to target block content m' , wherein a parent hash corresponding to block Qi is recorded in a block header of block $Qi+1$ and is generated through calculation using original block content m , public key H , and original random number r ; blockchain node Bi executes a smart contract that generates a random number when determining that a consensus on the block editing transaction succeeds, wherein the smart contract is used to generate private key X through secure multi-party computing; and determine corresponding target random number r' based on original block content m , target block content m' , original random number r , and private key X , wherein a hash value generated through calculation by using target block content m' , public key H , and target random number r' is the same as the parent hash; and blockchain node Bi updates (m, r) to (m', r') .

FIG. 1