

METHOD AND SYSTEM FOR BLOCKCHAIN VARIANT USING DIGITAL SIGNATURES

ABSTRACT OF THE DISCLOSURE

5

A method for using digital signatures for signing blockchain transactions includes:
generating a domain key pair comprising a domain private key and a domain public
key, wherein the domain public key is signed after generation; receiving a plurality of
member public keys, wherein each member public key is received from an associated
10 member of a blockchain network and is a public key in a key pair comprising the
member public key and a member private key corresponding to the associated
member; signing each member public key using the domain private key; receiving a
transaction block from a specific member of the blockchain network, wherein the
transaction block includes a plurality of blockchain transaction values and a hash
15 signed using the member private key corresponding to the specific member; signing
the received transaction block using the domain private key; and transmitting the
signed transaction block.

[Fig. 6]