

CLAIMS

1. A computer-implemented method for implementing identity endorsement on a blockchain, comprising:

~~step S101: submitting~~receiving, at a third-party certification authority, byfrom a user as an applicant, certification information ~~to a third-party certification authority,~~
reviewing by the third-party certification authority, the certification information and
generating, by the third-party certification authority a certification statement according to the certification information, generating, by the third-party certification authority, corresponding deposit information of the certification statement according to the certification statement, storing the deposit information on a blockchain, attaching the deposit information into the certification statement, and returning a complete certification statement comprising the deposit information to the user, the user being an individual user or an enterprise; ~~and~~

~~step S102: requesting, by an information requester, for the certification statement from the user, informing of, by the user, one of own accounts, decrypting the certification statement and then sending it to the information requester in a secure manner, checking, by the information requester, in the blockchain, to verify validity of the certification statement and qualification of the third-party certification authority, and completing user identity certification after confirmation.~~

receiving, from the applicant, a signed certification statement, wherein the signed certification statement is the certification statement signed by the applicant with a private key;

wherein the generating, by the third-party certification authority, corresponding deposit information includes generating the corresponding deposit information according to the certification statement signed by the applicant; and

storing, by the third-party certification authority, the complete certification statement comprising the deposit information on the blockchain.

- ~~2. The computer-implemented method for implementing identity endorsement on a blockchain according to claim 1, wherein step S101 comprises:~~

~~step S1011: registering, by a user, an account on the blockchain;~~

~~step S1012: submitting, by the user as an applicant, certification information to a third-party certification authority;~~

~~step S1013: reviewing, by the third-party certification authority, the certification information, generating a certification statement according to materials submitted by the user, and signing, by the third-party certification authority, the certification statement with a private key to create a signed certification statement;~~

~~step S1014: returning, by the third-party certification authority, the signed certification statement to the applicant, signing, by the applicant, the certification statement with a private key corresponding to an account of the applicant after confirming that information in the certification statement is correct, and returning the certification statement signed with the private key corresponding to the account to the third-party certification authority;~~

~~step S1015: generating, by the third-party certification authority, corresponding deposit information of the certification statement according to the certification statement signed by the applicant, storing the deposit information on the blockchain, attaching the deposit information into the certification statement, returning a complete certification statement comprising the deposit information to the applicant, and storing, also by the third-party certification authority, a complete certification statement comprising the deposit information; and~~

~~step S1016: storing, by the applicant, a complete certification statement comprising the deposit information.~~

32. The computer-implemented method for implementing identity endorsement on a blockchain according to Claim 1, the user identity being supplementarily registered after ~~step S102~~ in a supplementary registration, wherein supplementarily registering the user identity comprises:

~~step S1021: issuing~~receiving, at a blockchain smart contract, ~~by~~from a user, a supplementary certification application ~~and sending the application to a blockchain smart contract~~, the supplementary certification application containing signature information of an account of the user that has been certificated, and signature information corresponding to one or more to-be-supplementarily-registered accounts;

step S1022: verifying, by the blockchain smart contract, whether the account that has been certificated is valid, if yes, proceeding to step S1023, otherwise, ending the supplementary registration;

step S1023: certificating, by the blockchain smart contract, whether the user is an actual holder of the to-be-supplementarily-registered account, if yes, proceeding to step S1024, and if no, ending the supplementary registration; and

step S1024: binding, by the blockchain smart contract, a plurality of supplementarily registered accounts submitted by the user to the deposit information of the certification statement that has been certificated.

43. The computer-implemented method for implementing identity endorsement on a blockchain according to Claim 32, wherein verifying, by the blockchain smart contract, whether the account that has been certificated is valid comprises:

S1: checking whether account information submitted by the user exists in the blockchain, if yes, proceeding to S2, otherwise, the verification failing;

S2: determining whether the account information has been certificated, ~~that is, wherein the~~ determining whether the account information has been certificated includes determining whether the account has been bound to the deposit information of the certification statement , if the account submitted by the user is in response to the account information submitted by the user being a main account, determining whether the main account has been bound to the deposit information of the certification statement , ~~if the user submits in response to the account information submitted by the user being~~ a sub-account, checking whether the sub-account has a main account associated therewith and determining whether the main account has been bound to the deposit information of the certification statement , if the account information has been certificated, proceeding to S3, and if the account information has not been certificated, the verification failing; and

S3: determining whether the bound deposit information of the certification statement has been canceled, if yes, the verification failing, and if no, passing the verification.

54. The computer-implemented method for implementing identity endorsement on a blockchain according to Claim 1, wherein the user identity may be canceled after step S102, wherein the cancellation of the user identity comprises two cancellation modes: a user-based active cancellation mode and a third-party certification authority-based cancellation mode;

the user-based active cancellation mode comprises:

S1: ~~sending, by~~ receiving, at the blockchain, from the user, cancellation information corresponding to an account to the blockchain directly by himself/herself or through an agency;

S2: after the blockchain verifies the user identity through the account, canceling the deposit information of the certification statement of the user; and

S3: monitoring, by the third-party certification authority, the generated certification statement, and if the deposit information of the certification statement that is actively canceled by the user is found, executing, by the third-party certification authority, an internal cancellation process to cancel the certification statement of the user stored in the third-party certification authority;

the third-party certification authority-based cancellation mode comprises:

- 1): sending, by the third-party certification authority, cancellation information to the blockchain;
- 2): after the blockchain verifies the ~~authority~~ identity of the third-party certification authority through the account of the third-party certification authority, canceling specified deposit information of the certification statement ; and
- 3): after confirming that the cancellation is successful, informing, by the third-party authority, the user of that the user identity has been canceled.

65. A device for implementing identity endorsement on a blockchain, comprising:

an identity registration module, configured to submit, by a user as an applicant, certification information to a third-party certification authority, review by the third-party certification authority the certification information, and generate a certification statement according to the certification information, generate, by the third-party certification authority, corresponding deposit information of the certification statement according to the certification statement, store the deposit information on a blockchain, attach the deposit information into the certification statement, and return a complete certification statement comprising the deposit information to the user, the user being an individual user or an enterprise; and

an identity certification module, configured to request, by an information requester, for the certification statement from the user, ~~inform of, by the user, one of own accounts,~~ receive a decrypted version of the requested ~~the certification statement~~ from the user ~~and then send it to the information requester in a secure manner~~, check, by the information requester, in the blockchain, to verify validity of the certification statement and qualification of the third-party certification authority, and complete user identity certification after confirmation.

76. The device for implementing identity endorsement on a blockchain according to Claim 65, wherein the identity registration module comprises:

a registration sub-module, configured to register, by a user, an account on the blockchain;

a certification information submitting sub-module, configured to submit, by the user as an applicant, certification information to a third-party certification authority;

a reviewing sub-module, configured to review, by the third-party certification authority, the certification information, generate a certification statement according to materials submitted by the user, and sign, by the third-party certification authority, the certification statement with a private key to create a signed certification statement;

a confirmation sub-module, configured to return, by the third-party certification authority, the signed certification statement to the applicant, sign, by the applicant, the certification statement with a private key corresponding to an account of the applicant after confirming that information in the certification statement is correct, and return the certification statement signed with the private key corresponding to the account to the third-party certification authority;

a first storage sub-module, configured to generate, by the third-party certification authority, corresponding deposit information of the certification statement according to the certification statement signed by the applicant, store the deposit information on the blockchain, attach the deposit information into the certification statement, return a complete certification statement comprising the deposit information to the applicant, and store, also by the third-party certification authority, a complete certification statement comprising the deposit information; and

a second storage sub-module, configured to store, by the applicant, a complete certification statement comprising the deposit information.

87. The device for implementing identity endorsement on a blockchain according to Claim 65, further comprising: a supplementary registration module, configured to supplementarily register the user identity, wherein the supplementary registration module comprises:

a supplementary certification application sub-module, configured to issue, by a user, a supplementary certification application and send the application to a blockchain smart contract, the supplementary certification application containing signature information of an account of the user that has been certificated, and signature information corresponding to one or more to-be-supplementarily-registered accounts;

a first determination sub-module, configured to verify, by the blockchain smart contract, whether the account that has been certificated is valid;

a second determination sub-module, configured to certificate, by the blockchain smart contract, whether the user is an actual holder of the to-be-supplementarily-registered account; and

an information binding sub-module, configured to bind, by the blockchain smart contract, a plurality of supplementarily registered accounts submitted by the user to the deposit information of the certification statement that has been certificated.

98. The device for implementing identity endorsement on a blockchain according to Claim 87, wherein the first determination sub-module comprises:

a check sub-module, configured to check whether account information submitted by the user exists in the blockchain;

a determination sub-module, configured to determine whether the account information has been certificated, that is, whether the account has been bound to the deposit information of the certification statement , if the account submitted by the user is a main account, determine whether the main account has been bound to the deposit information of the certification statement , if the user submits a sub-account, check whether the sub-account has a main account associated therewith, and determine whether the main account has been bound to the deposit information of the certification statement ; and

a cancellation determination sub-module, configured to determine whether the bound deposit information of the certification statement has been canceled.

109. The device for implementing identity endorsement on a blockchain according to Claim 65, further comprising: an identity cancellation sub-module, configured to cancel the user identity, wherein the cancellation of the user identity comprises two cancellation modes: a user-based active cancellation mode and a third-party certification authority-based cancellation mode.

110. A system for implementing identity endorsement on a blockchain, comprising:

a processor, configured to execute a plurality of instructions; and

a memory, configured to store the plurality of instructions,

wherein the plurality of instructions are configured to be stored by the memory and loaded by the processor to perform the computer-implemented method for

implementing identity endorsement on a blockchain according to any one of Claims 1 or ~~2-54~~.

~~1211~~. A computer-readable storage medium, storing a plurality of instructions therein that are configured to be loaded by a processor and perform the computer-implemented method for implementing identity endorsement on a blockchain according to any one of Claims 1 ~~or 2-54~~.

12. The computer-implemented method for implementing identity endorsement on a blockchain according to Claim 1, further comprising:
requesting, by an information requester, for the certification statement from the user,
decrypting, by the user, the requested certification statement and then sending, by the
user, the decrypted certification statement to the information requester in a secure
manner, checking, by the information requester, in the blockchain, to verify the validity
of the certification statement and qualification of the third-party certification authority,
and completing user identity certification after confirmation according to the result of
the verify step.

13. The computer-implemented method for implementing identity endorsement on a
blockchain according to Claim 1, wherein the complete certification statement
including the deposit information includes the certification statement signed by the
third-party certification authority and then signed by the account corresponding to the
applicant, and the deposit information, wherein the deposit information includes a main
account and a plurality of sub-accounts of the user, a Hash of information contained in
the certification statement, and signature information of the third-party certification
authority.