

CLAIMS:

1. A system for executing a sequence of verified Blockchain transactions that operate as an offer and acceptance by verifying certain identity information of a transferee, characterized in that the system is operable to:

form by one or more servers, a blockchain, the blockchain having one or more nodes each node comprising a blockchain address, wherein a first node of the one or more nodes has a first blockchain address with an unspent transaction (UTXO),

create, by the one or more servers, a first private key identifying a root certification authority's identity,

generate, by the one or more servers, a root-of-trust on the blockchain using the first private key identifying the root certification authority's identity, at the request of a first entity/transferee to a verified blockchain transaction on the blockchain including generating a root certification certificate associated with the first entity/transferee, wherein the root certification certificate specifies a public key include as a field of the certificate, wherein the public key correspond to the first block chain address associated with the unspent transaction (UTXO) on the blockchain

issue, from the one or more servers, the root certification certificate to the first entity/transferee, in response to the request

generate, by a first computing device of the first entity/transferee, a first blockchain address using the first private key,

generate, by the one or more servers, a second private key identifying the issuing authority's identity,

generate, by the one or more servers, a second blockchain address using the second private key, the second blockchain address comprising the address of an identity token of the first entity/transferee,

generate, by the one or more servers, a certificate signing request (CSR) for the first entity to the verified blockchain transaction,

issue, by the one or more servers, a leaf certificate to the first entity/transferee to the verified blockchain transaction from the first entity's certificate signing request (CSR),

generate, by the one or more servers, an issuing transaction, using the first private key of the certification authority's root address, wherein the issuing transaction includes at least two outputs, a first output that is the identity token spendable by the public key corresponding to certification certificate issued from the certification/issuing server from its root certificate to the first entity/transferee, and a new root output that replace the current root output,

create, by a second computing device associated with the a second entity/transferor, an offer transaction having a transfer output spendable by the public key of the identity token output of the first entity/offeree,

create, by the first computing device associated with the first entity/transferee to the transaction, an acceptance transaction including as an input, the transfer output created during the offer transaction.

2. The system of claim 1, wherein the act of creating an offer transaction by the second computing device comprises:

generating a third private key,
establishing an identity corresponding to a user of the third private key, and
creating a transfer output using the third private key to create a blockchain transaction with an output spendable by the Blockchain address of the first user's identity token.

3. The system of claim 1, wherein the act of creating an offer transaction by the second computing device comprises:
 - adding an input to the first user's identity token output, wherein the added input requires a signature on the transaction from the first user.
4. The system of claim 1, wherein the act of creating an offer transaction by the second computing device comprises:
 - including an output in the offer transaction which when spent operates as a specified offeree's acceptance, wherein said output requires a signature by a private key of a corresponding identity token output.
5. The system of claim 1, wherein the act of creating an acceptance transaction by the first computing device comprises signing the transfer output with a private key corresponding to the identity token of the first entity/transferee.
6. A method for executing a sequence of verified Blockchain transactions that operate as an offer and acceptance by verifying certain identity information of a transferee, comprising:
 - forming, by a first computing device, a blockchain having one or more nodes, each node having a blockchain address, wherein a first node of the one or more nodes have a first blockchain address associated with an unspent transaction (UTXO) on the blockchain,
 - creating, by a certification/issuing server, a first private key identifying a root certification authority's identity,
 - generating, by a certification/issuing server, at the request of a first entity/transferee to a transaction on the blockchain, and using a first private key, a root of trust on the blockchain including generating a certification certificate associated with the first entity/transferee, the certificate specifying a public key included as a field of the certificate, the public key corresponding to the first block chain associated with the unspent transaction (UTXO) on the blockchain,

issuing, by the certification/issuing server, the root certification certificate to the first entity/transferee to the transaction in response to the request, generating, by the first entity/transferee to the transaction, a first blockchain address using the first private key,

generating, by the certification/issuing server, a second private key identifying the issuing authority's identity,

generating, by the certification/issuing server. A second blockchain address using the second private key, the second blockchain address comprising the address of the first entity/transferee's identity token,

generating, by the first server, a certificate signing request (CSR) for the first entity/transferee to the transaction,

issuing, by the first server, a leaf certificate to the first entity to the verified blockchain transaction from the first entity's CSR,

generating, by the certification/issuing server, an issuing transaction using the first private key of the certification authority's root address including as input, the certification authority's root output, and further including an output that spends the unspent transaction output (UTXO) on the blockchain, wherein the output is only spendable by the public key of the certification authority's root certificate,

creating, by a first computing device associated with second entity/offeree, an offer transaction having, a transfer output spendable by the public key of the identity token of the first entity,

creating, by a second computing device associated with a first entity/transferee to the transaction, an acceptance transaction including the transfer output created during the offer transaction as input.

7. The method of claim 6 wherein the issuing transaction has at least two outputs comprising:

an identity token output spendable by the public key corresponding to certification certificate issued from the second server from its root certificate to the first entity/transferee, and a new root output that replaces the current root output.

8. The method of claim 6 wherein the act of creating an acceptance transaction, by said first computing device comprises signing the transfer output with the private key corresponding to the identity token associated with the issuing transaction.

9. The method of claim 6, wherein generating, by the first entity/transferee to the transaction, a first blockchain address using the first private key comprises, creating a wallet import format (WIF) string using the first private key, and importing the first private key into a blockchain transaction system using the WIF string, wherein the first blockchain address is identical to the certification authority's root blockchain address.