

CLAIMS

1. Computer-implemented method of controlling by a control authority (2) digital asset emission or digital asset destruction, comprising the steps of:

5 sending, by a first user (16) using an electronic device of the first user, a request for registering a transfer of digital asset towards a digital account of the first user (16), or a request for registering a transfer of digital asset between the digital account of the first user (16) and a digital account of a second user (26), to an operator (12), preferably a commercial bank or an Automated Teller Machine (ATM),
10 accredited to the control authority (2), the operator (12) sending the request received from the first user to a ledger (8), preferably a blockchain, accredited to the control authority (2), via a gateway (14) accredited to the control authority (2), the control authority (2) having a control authority identification number and having access to the ledger (8) for transmitting and storing data in the ledger;

15 receiving from the operator (12) and through an interface (6), by the ledger (8) being configured to store digital assets and comprising a processing unit and a database, the request for registering the transfer of digital asset towards the digital account of the first user (16) corresponding to a first user identification number indicated in the request, or the request for registering the transfer of digital asset
20 between the digital account of the first user (16) and the digital account of the second user (26) corresponding to a second user identification number further indicated in the request;

 accessing and reading data stored in the ledger (8), wherein

 the first user digital account indicates a first user digital account balance,
25 the first user digital account balance associated with the first user identification number being registered in the ledger (8);

 the second user digital account indicates a second user digital account balance, the second user digital account balance associated with the second user identification number being registered in the ledger (8);

30 processing a received request by the ledger (8), stamping time and storing the received request and any update of a user digital account balance; and

i) registering, by the ledger (8), the transfer of digital asset towards the first user digital account according to the received request by updating the first user digital account balance accordingly, wherein the request for registering the transfer of

35

digital asset towards the first user digital account is sent to the ledger (8) via a gateway (14) accredited to the control authority and having a gateway identification number, wherein each one of the control authority, the first user and the gateway indicates its identification number in each data transfer; the gateway has a set of gateway parameters and a set of gateway rules validated by the control authority (2) and applicable to the request sent via the gateway (14) to the ledger (8), the gateway parameters indicating at least a maximal amount, or a maximal amount during a time period, of digital asset that can be requested via the gateway (14), and the set of gateway rules indicating rules applicable to digital asset emission and digital asset destruction resulting from any request transmitted via the gateway; the gateway identification number, the set of gateway parameters and the set of gateway rules being part of a gateway application program stored by the control authority (2) into the ledger (8); and the ledger (8) further executes the gateway application program corresponding to the gateway identification number of the accredited gateway according to the request received from said gateway and to the corresponding set of gateway parameters and set of gateway rules for registering the transfer of digital asset to the first user digital account and updating the first user digital account balance accordingly only in case the request is in further accordance with said set of gateway parameters, said set of gateway rules, and a gateway current state indicating the amount, or the amount during the time period, of digital asset already requested; and

ii) registering, by the ledger (8), the transfer of digital asset between the first user digital account and the second user digital account according to the received request by updating accordingly the first user digital account balance and the second user digital account balance only in case an updated digital account balance of the user account to be debited corresponds to a positive balance.

2. Method according to claim 1, wherein the control authority accredits a further gateway (24) by the steps of:

- 5 a) assigning to the further gateway a further gateway identification number and a corresponding further gateway application program containing a set of further gateway parameters and a set of further gateway rules, the further gateway parameters indicating at least a maximal amount, or a maximal amount during a time period, of digital asset that can be requested via the further gateway (24), and
- 10 the set of further gateway rules indicating rules applicable to digital asset emission

and digital asset destruction resulting from any request transmitted via the further gateway (24); and

b) sending to the ledger (8), and storing in the ledger (8), the assigned further gateway identification number and the corresponding further gateway application program,
5 thereby accrediting the further gateway (24).

3. Method according to any one of claims 1 and 2, wherein each user identification number is a user public key that is obtained by means of a digital signature
10 algorithm from a corresponding user private key owned by the user.

4. Method according to claim 3, wherein each user generates a corresponding user digital signature by means of an application running on a user electronic device and using the digital signature algorithm, by entering its user private key into the user
15 electronic device and obtaining said user digital signature, the user signing any request sent to the ledger (8) with the obtained user digital signature, the ledger checking that a user digital signature on a received request has been validly generated from the corresponding received user public key by means of a user private key, thereby authenticating the received request; and, in case the user digital
20 signature is not valid, the ledger (8) prevents registering the transfer of digital asset specified in the request.

5. Method according to claim 1 and any one of claims 3 and 4, wherein the gateway identification number is a gateway public key that is obtained by means of a digital
25 signature algorithm from a corresponding gateway private key owned by the gateway (14, 24).

6. Method according to claim 5, wherein the gateway (14, 24) generates a corresponding gateway digital signature by means of a gateway application and
30 using the digital signature algorithm, by running the gateway application with the gateway private key and obtaining said gateway digital signature, the gateway signing any request sent to the ledger (8) with the obtained gateway signature, the ledger (8) checking that a gateway digital signature on a received request has been validly generated from the corresponding received gateway public key by means of

a gateway private key, thereby authenticating the received request; and, in case the gateway digital signature is not valid, the ledger (8) prevents registering the transfer of digital asset specified in the request and updating the corresponding user digital asset balance.

5

7. Method according to any one of claims 1 to 6, wherein

a control unit (4) accredited to the control authority (2) and having a control unit identification number, the control unit (4) accessing to the ledger (8) and reading any stored request sent by a gateway (14) and the corresponding stored gateway application program, the control unit (4) indicating its identification number in each data transfer to the ledger (8), the control unit detecting in a request from a gateway (14,24) stored in the ledger (8) whether a security rule regarding transmission of request has been infringed by said gateway (14,24) and, in case of infringement, storing into the ledger (8) a security alert message containing the gateway identification number of the infringing gateway;

15

the ledger (8), upon reception of a request from a gateway (14,24), checking whether a stored security alert message indicates that a gateway identification number corresponding to said gateway (14,24) is an infringing gateway, and preventing any registering operation relating to a request sent by an infringing gateway.

20

8. System for controlling by a control authority digital asset emission or digital asset destruction, the system comprising one or more processors and memory storing instructions, wherein the one or more processors are configured to execute the instructions such that the processor and memory are configured to,

25

after sending, by a first user (16) using an electronic device of the first user, a request for registering a transfer of digital asset towards a digital account of the first user (16), or a request for registering a transfer of digital asset between the digital account of the first user (16) and a digital account of a second user (26), to an operator (12), preferably a commercial bank or an Automated Teller Machine (ATM), accredited to the control authority (2), the operator (12) sending the request received from the first user to a ledger (8), preferably a blockchain, accredited to the control authority (2), via a gateway (14) accredited to the control authority (2), the control authority (2) having a control authority identification number and having

30

access to the ledger (8) via the communication network for transmitting and storing data in the ledger,

5 receive from the operator (12) and through an interface (6), by the ledger (8) being configured to store digital assets and comprising a processing unit and a database, the request for registering the transfer of digital asset towards the digital
10 account of a first user (16) corresponding to a first user identification number indicated in the request, or the request for registering the transfer of digital asset between the digital account of the first user (16) and the digital account of the second user (26) corresponding to a second user identification number further
15 indicated in the request;
access and read data stored in the ledger (8), wherein

the first user digital account indicates a first user digital account balance, the first user digital account balance associated with the first user identification number being registered in the ledger (8);

the second user digital account indicates a second user digital account balance, the second user digital account balance associated with the second user identification number being registered in the ledger (8);

process a received request by the ledger (8), stamp time and store the received request and any update of a user digital account balance; and

i) register, by the ledger (8), the transfer of digital asset towards the first user digital account according to the received request by updating the first user digital account balance accordingly, wherein the request for registering the transfer of digital asset towards the first user digital account is sent to the ledger (8) via a gateway (14) accredited to the control authority and having a gateway identification number, wherein each one of the control authority, the first user and the gateway indicates its identification number in each data transfer; the gateway has a set of gateway parameters and a set of gateway rules validated by the control authority (2) and applicable to the request sent via the gateway (14) to the ledger (8), the gateway parameters indicating at least a maximal amount, or a maximal amount during a time period, of digital asset that can be requested via the gateway (14), and the set of gateway rules indicating rules applicable to digital asset emission and digital asset destruction resulting from any request transmitted via the gateway; the gateway identification number, the set of gateway parameters and the set of gateway rules being part of a gateway application program stored by the control authority (2) into the ledger (8); and the ledger (8) is further operable to execute the gateway application program corresponding to the gateway identification number of the accredited gateway according to the request received from said gateway and to the corresponding set of gateway parameters and set of gateway rules for registering the transfer of digital asset to the first user digital account and update the first user digital account balance accordingly only in case the request is in further accordance with said set of gateway parameters, said set of gateway rules, and a gateway current state indicating the amount, or the amount during the time period, of digital asset already requested; and

ii) register, by the ledger (8), the transfer of digital asset between the first user digital account and the second user digital account according to the received request by updating accordingly the first user digital account balance and the second user

digital account balance only in case an updated digital account balance of the user account to be debited corresponds to a positive balance.

9. System according to claim 8, wherein the gateway (14,24) is operable to run on an Automated Teller Machine (ATM) (14b, 24b) or a smartphone or a tablet or a Web interface.

5 10. System according to any one of claims 8 and 9, wherein the control authority (2) is operable to accredit a further gateway (24) by:

- a) assigning to the further gateway a further gateway identification number and a corresponding further gateway application program containing a set of further gateway parameters and a set of further gateway rules, the further gateway
10 parameters indicating at least a maximal amount, or a maximal amount during a time period, of digital asset that can be requested via the further gateway, and the set of further gateway rules indicating rules applicable to digital asset emission and digital asset destruction resulting from any request transmitted via the further gateway; and
- 15 b) sending to the ledger via the communication network, and storing in the ledger, the assigned further gateway identification number and the corresponding further gateway application program,
thereby accrediting the further gateway.

11. System according to any one of claims 8 to 10, wherein each user identification number is a user public key obtained from a corresponding user private key owned by the user by means of a corresponding user identifying device having processing capabilities and having installed a programmed digital signature algorithm operable to provide said user public key upon entering in the user identifying device, and processing, said user private key.

12. System according to claim 11, wherein each user can generate a corresponding user digital signature by means of an application running on a user electronic device and using the digital signature algorithm, by entering its user private key into the user electronic device and obtaining said user digital signature, the user signing any request sent to the ledger with the obtained user digital signature, the ledger being operable to check that a user digital signature on a received request has been validly generated from the corresponding received user public key by means of a user private key, thereby authenticating the received request.

13. System according to claim 8 and any one of claims 11 and 12, wherein the gateway identification number is a gateway public key that is obtained by means of a digital signature algorithm from a corresponding gateway private key owned by the gateway.

14. System according to claim 13, wherein the gateway is operable to generate a corresponding gateway digital signature by means of a gateway application and using the digital signature algorithm, by running the gateway application with the gateway private key and obtaining said gateway digital signature, the gateway being operable to sign any request sent to the ledger with the obtained gateway digital signature, the ledger being operable to check that a gateway digital signature on a received request has been validly generated from the corresponding received gateway public key by means of a gateway private key, thereby authenticating the received request; and, in case the gateway digital signature is not valid, the ledger is operable to prevent registering the transfer of digital asset specified in the request and updating the corresponding user digital asset balance.

15. System according to any one of claims 8 to 14, wherein

a control unit accredited to the control authority and having a control unit identification number, the control unit being operable to access to the ledger via a control communication link and read any stored request sent by a gateway and the corresponding stored gateway application program, the control unit indicating its
5 identification number in each data transfer to the ledger, the control unit being operable to detect in a request from a gateway stored in the ledger whether a security rule regarding transmission of request has been infringed by said gateway and, in case of infringement, store into the ledger a security alert message containing the gateway identification number of the infringing gateway; and
10 the ledger, upon reception of a request from a gateway, being operable to check whether a stored security alert message indicates that a gateway identification number corresponding to said gateway is an infringing gateway, and being operable to prevent any registering operation and updating of the corresponding user digital account balance relating to a request sent by an infringing
15 gateway.

16. System according to any one of claims 8 to 15, wherein
each user has a corresponding user digital wallet, corresponding to the user identification number, operable to be connected to the ledger by sending to the
20 ledger a connection message containing the user identification number, and read the corresponding user digital account balance stored in the ledger and update a digital asset amount in the wallet based on the read digital account balance.