

Claims

1. A computer implemented method of implementing a payment service for one or more clients for transactions associated with a distributed ledger, the method
5 comprising:
creating a machine readable resource associated with the payment service,
wherein the machine readable resource comprises:
at least one endpoint identifier associated with a host computing resource
responsible for implementing the payment service for each client, each client being
10 associated with an alias, the alias including or related to a network identifier;
an entry associated with at least one capability among a plurality of
capabilities supported by the payment service, and
instructions and/or a specification for accessing or obtaining a public
address associated with the alias, the public address used for facilitating
15 transactions associated with the alias; and
providing the machine readable resource at a predictable or known location
associated with the payment service.
2. The method as claimed in claim 1 wherein each client of the one or more
20 clients is associated with a digital wallet.
3. The method as claimed in claim 1 or 2 wherein the plurality of
capabilities include one or more of:
payer entity or payee entity validation,
25 multiple digital signatures for transactions,
payee entity approval for transactions,
email-protocol related payment transactions,
simplified payment protocol or flow for payment transactions,
and/or
30 call-back requests or responses.
4. The method as claimed in any one of claims 1 to 3 further including the
step of determining a location for the host computing resource by a computer
implemented method of implementing a payment service for one or more clients for
35 transactions associated with a distributed ledger comprising the steps of:

providing an alias for a given client among the one or more clients, the alias being specific to the given client, the alias including or related to a network identifier;

associating the alias with the network identifier in a directory, the step of associating including:

- 5 creating a service record based on the network identifier in the directory;
- updating the service record to indicate that the payment service is provided by a network or domain associated with the network identifier; and
- updating the service record to indicate a location for a host computing resource responsible for the payment service, wherein the host computing
- 10 resource is configured to facilitate identification of the digital wallet associated with the alias, responsive to a request pertaining to a transaction related to the alias;
- wherein the endpoint identifier in the machine readable resource is based on the determined location.

- 15 5. The method as claimed in any one of claims 1 to 4 wherein, responsive to a request from a requesting entity pertaining to a transaction associated with an alias, the method further comprises steps of:

 based on the network identifier associated with the alias in the request, identifying the payment service associated with the alias;

- 20 based on the identified payment service, accessing the machine readable resource from the predictable or known location;

 responsive to identifying if one or more capabilities required for the transaction are present in the machine readable resource, returning an endpoint identifier of the host computing resource for the payment service from the machine readable resource; and

- 25 obtaining a public address associated with the alias based on one or more of the instructions and/or specification in the machine readable resource.

- 6. A method associated with a transaction for a distributed ledger, wherein an alias is provided for a given client among one or more clients, the alias being specific to
- 30 the given client, the alias including or related to a network identifier, the method comprising the steps of:

 sending from a requesting entity a request pertaining to a transaction, the request associated with the alias;

accessing the machine readable resource from a location associated with the payment service, wherein the payment service is identified based on the network identifier in the alias, and wherein the machine readable resource is created according to claim 1;

5 based on identifying if one or more capabilities required for the transaction are present in the machine readable resource, receiving an endpoint identifier of the host computing resource for the payment service associated with the alias; and

obtaining a public address associated with the alias using one or more of the instructions and/or specification in the machine readable resource.

10 7. The method as claimed in any one of claims 5 or 6, wherein each client is associated with a digital wallet pertaining to a user or entity registered for the payment service in the network, wherein each digital wallet is a cryptocurrency wallet associated with a public key and a private key of an asymmetric cryptography key pair for transactions on the distributed ledger, and wherein the step of obtaining the public
15 address includes obtaining the public key of the digital wallet associated with the alias.

8. The method as claimed in claim 7, wherein the public address associated with the alias is based on a cryptographic hash of the public key of the digital wallet associated with the alias.

20

9. The method as claimed in any one of claims 7 or 8, wherein the public key of the digital wallet is an elliptic curve digital signature algorithm (ECDSA) public key, wherein the public key is not part of any transaction previously stored on or posted to the distributed ledger.

25

10. The method as claimed in any one of claims 5 to 9, wherein the one or more instructions and/or specification in the machine readable resource comprises:

obtaining a public key infrastructure (PKI) request template from the machine readable resource for a PKI endpoint identifier;

30 including the alias and the network identifier in the template to generate a complete PKI request; and

sending a HTTP GET request based on the complete PKI request to obtain a public key associated the alias.

11. The method as claimed in any of claims 1 to 10 wherein the known or predictable location of the machine readable resource is based on at least one of the endpoint identifier, an Internet protocol communication port used by the payment service and/or a configuration specification of the payment service included in a publicly
5 accessible well-known domain repository.

12. The method as claimed in any one of claims 1 to 11 wherein the machine readable resource is generated using a Java Script Object Notation (JSON) format.

10 13. A computer implemented method of implementing a payment service for one or more clients for transactions associated with a distributed ledger, the method comprising:

updating a machine-readable resource associated with the payment service, the machine-readable resource being provided at or accessible from a predictable or known
15 location associated with the payment service, the machine-readable resource created according to claim 1, the step of updating comprising:

adding at least one further capability that is supported by the payment service, wherein the at least one further capability includes implementing a simplified protocol for processing a digital asset for a given client among the one or more clients.

20

14. The method as claimed in claim 4 comprising the step of receiving an acknowledgement of the cryptocurrency payment from the payment service associated with the payee entity.

25 15. The method as claimed in any preceding claim wherein the alias is a payment handle associated with a client.

16. A method for configuring a prefix for making a request pertaining to a transaction from a requesting entity to an alias associated with a client, the method
30 comprising, responsive to receipt of a request from the requesting entity that includes the prefix and the alias, triggering the steps of any one of the preceding claims based on the alias.

17. A computing device or a computer system, comprising:
35 a processor; and

memory including executable instructions that, as a result of execution by the processor, causes the system to perform the computer-implemented method of any preceding claims.

- 5 18. A non-transitory computer-readable storage medium having stored thereon executable instructions that, as a result of being executed by a processor of a computer system, cause the computer system to perform the computer-implemented method of any one of claims 1 to 16.