

Claims

1. A computer implemented method of providing a payment service for one or more clients for transactions associated with a blockchain, the method implemented by a payment processor and comprising the steps of :

receiving a request from a given client among the one or more clients, the request being to submit to the blockchain a transaction associated with a digital asset, the request associated with a call-back identifier for enabling direct communication between the given client and another entity for the transaction;

submitting the transaction associated with the request to a given miner among a plurality of miners, for including the transaction in the blockchain;

identifying the given miner to the client;

providing the call-back identifier to the miner;

responsive to receiving a response pertaining to a corresponding blockchain transaction for the request from the given miner, the method further includes:

enabling or processing for the client at least one call-back notification pertaining to the corresponding blockchain transaction provided by the miner, the call-back notification being based on the call-back identifier associated with the request.

2. The method as claimed in claim 1 wherein the received response from the miner is associated with a transaction identifier (TxID), the method further including sending a transaction identifier (TxID) for the corresponding blockchain transaction to the client.

3. The method as claimed in any preceding claim wherein the received response is an output script associated with the blockchain transaction, the output script including an Unspent Transaction Output (UTXO) associated with a mempool for the miner, the UTXO including the transaction identifier (TxID) for the blockchain transaction.

4. The method as claimed in any preceding claim wherein the payment processor is implemented as a Representational State Transfer (REST) endpoint for the one or more clients, and wherein the method further comprises the step of providing an application programming interface (API) gateway associated with the payment processor for performing the steps of:

receiving the request from the client using a Hypertext Transfer Protocol Secure (HTTPS) transmission protocol format;

converting the respective request to a Remote procedure Call (RPC) format, and submitting the RPC to the miner;

receiving a response associated with a corresponding blockchain transaction from the miner in an RPC format; and

converting the respective response for sending to the client using the HTTPS transmission protocol.

5. The method as claimed in any preceding claim comprising the step of verifying the identity of the given miner, wherein the verification is based on a digital signature associated with the given miner, or based on an identifier pertaining to the given miner, said identifier being optionally associated with a reputation indicator for the given miner.

6. The method as claimed in any preceding claim wherein the call-back notification relates to a notification of a double-spend of the transaction submitted by the given client, or wherein the call-back notification relates to a proof of inclusion in the blockchain of the transaction submitted by the given client.

7. The method as claimed in any preceding claim, wherein the call-back identifier is a location for a channel associated with the client, or wherein the call-back identifier is a Universal Resource Identifier (URI) for the client.

8. The method as claimed in any preceding claim further comprising the step of providing the given miner access to the channel, wherein the step of providing includes, providing a channel identifier or location for the channel associated with the request, and one or more access tokens associated with the channel to the miner.

9. A computer implemented method for implementing a channel service for one or more clients, the method implemented by a channel processor and comprising the steps of :

receiving a request from a given client among the one or more clients, the request pertaining to creation of a channel;

providing the given client access to one or more functions that enable direct communication between the given client and another entity via the channel, wherein said one or more functions include:

channel functions or procedures pertaining to the channel for transmission of data; and/or

message functions or procedures pertaining to the data being transmitted using the channel;

issuing one or more access tokens for the channel, said one or more access tokens being configured for secure communication with another entity via the channel; and
storing and/or providing one or more notifications associated with the channel for the given client.

10. The method as claimed in claim 9 wherein the one or more functions are application programming interfaces (APIs) issued for or provided to the given client, said APIs including channel API's for the channel, and message APIs for data associated with the channel; and wherein the access tokens are API tokens that are specific to the channel or a given message.

11. The method as claimed in claim 9 or 10 wherein the step of providing access to one or more functions include the provision of a JavaScript Object Notation (JSON) -over-Hyper Text transfer protocol (HTTP) API, to enable creation and /or management of one or more channels.

12. The method as claimed in any one of claims 9 to 11 wherein the one or more notifications associated with the channels are call-back notifications from a miner, the miner being the other entity in direct communication with the given client via the channel.

13. The method as claimed in claim 12 wherein the call-back notification relates to a notification of a double -spend of a transaction submitted by the given client.

14. The method as claimed in claim 13 wherein the call-back notification is associated with a return payload in the channel, said return payload provided by the miner, the return payload including the following data:

- the transaction identifier (TxID) of the blockchain transaction that is a double - spend; and optionally
- a service endpoint for the payment processor that submitted the blockchain transaction

15. The method as claimed in claim 12 wherein the call-back notification relates to a proof of inclusion of a transaction submitted by the given client in the blockchain.

16. The method as claimed in claim 15 wherein the call-back notification is associated with a return Merkle proof in the channel, said return Merkle proof provided by the miner, the return Merkle proof including the following data:

- a transaction identifier (TxID) of a blockchain transaction that the Merkle proof relates to ;
- a block header of the block in which the blockchain transaction is included; and
- an array of sibling hashes for the transaction identifier (TxID).

17. The method as claimed in any one of claims 9 to 16, when the client is offline or not communicatively connected to the channel processor, the one or more call back notifications are push notifications for data that is stored or queued for the given client in the channel.

18. The method as claimed in any one of claims 9 to 17 , when the client is online or communicatively connected to the channel processor, the data associated with the one or more call back notifications is provided or pulled from the channel.

19. The method as claimed in any one of claims 9 to 18 wherein the channel processor is or includes a payment processor, and wherein the method includes the method implemented by the payment processor according to any one of claims 1 to 8.

20. A computer implemented method for processing transactions associated with a blockchain, the method implemented by one or more processors associated with a client and comprising the steps of:

- sending a channel request pertaining to a channel service, the channel service implemented by a channel processor, the request relating to creation of a channel for communication with another entity;

- obtaining from the channel service access to one or more functions that enable direct communication between the given client and the other entity, said one or more functions including :

- channel functions or procedures pertaining to a channel for transmission of data; and/or

- message functions or procedures pertaining to the data being transmitted using a channel;

- obtaining from the channel service one or more access tokens, said access tokens enabling secure communication with the other entity;

- sending to a payment processor implementing a payment service, a request to submit to the blockchain a transaction associated with a digital asset;

obtaining from the payment processor a transaction identifier (TxID) for a blockchain transaction corresponding to the submitted transaction;

identifying a miner associated with the corresponding blockchain transaction based on a response from the payment processor;

using one or more channel functions received from the channel processor, creating a given channel for communication with the identified miner;

sending the one or more access tokens associated with the given channel to the miner;

receiving at least one call-back notification associated with the given channel, the notification pertaining to data in the given channel associated with blockchain transaction, said data provided by the miner.

21. The method as claimed in claim 20 wherein, when the client is offline or not communicatively connected to the channel processor, the call back notifications are obtained as push notifications for data or messages that are queued in the given channel.

22. The method as claimed in claims 20 or 21 wherein, when the client is online or communicatively connected to the channel processor, the data associated with the call back notifications are pulled from the given channel.

23. The method as claimed in any one of claims 20 to 22 wherein the one or more functions are application programming interfaces (APIs) for the given client, said APIs including channel API's for enabling creation and /or management of one or more channels; and message APIs to enable the given client and one or more other entities to exchange messages, and/or read data from, and/or write data to the given channel; and wherein the access tokens are API tokens that are specific to a given channel or a given message.

24. The method as claimed in any one of claims 20 to 23, wherein the channel request is a Hypertext Transfer Protocol Secure (HTTPS) transmission GET request to the channel processor, and wherein the request to the payment processor is a Hypertext Transfer Protocol Secure (HTTPS) transmission POST request to the payment processor.

25. The method as claimed in any one of claims 20 to 24 further comprising the steps of:
providing a client endpoint;
providing at least one client addressing key associated with the client;
obtaining a miner endpoint;
obtaining at least one miner addressing key associated with the miner;

exchanging one or more handshake messages using the given channel based on the client and miner addressing keys;

based on a handshake result or pattern, obtaining a shared secret key;
wherein any communication using the given channel is encrypted based on the shared secret key.

26. The method as claimed claim 25 wherein the client endpoint is a Hyper Text Transfer Protocol (HTTP) Application programming Interface (API) endpoint, and wherein said client endpoint is delivered using a HTTP Secure (HTTPS).

27. The method as claimed in claim 25 wherein the client endpoint is a Universal Resource Location (URL) included in a message from the given client sent using the given channel.

28. The method as claimed in any one of claims 25 to 27 wherein the client endpoint is an alias associated with the client, the alias being specific to the client and provided by an alias-based addressing service, the addressing service having a machine readable resource that is accessible from a defined or well-known location, the machine readable resource including one or more capabilities pertaining to the client, and wherein the alias is associated with an asymmetric cryptographic key pair for authentication.

29. A computer implemented method for processing transactions associated with a blockchain, the method implemented by one or more processors associated with a miner among a plurality of miners, the plurality of miners being communicatively coupled to at least one payment processor implementing a payment service for a given client, the method comprising the steps of:

receiving a request for submission of a transaction to the blockchain from the payment processor;

generating a blockchain transaction corresponding the request;

sending an output script(UTXO) associated with the blockchain transaction to the payment processor, wherein the output script includes a transaction identifier (TxID) associated with the corresponding blockchain transaction;

receiving access to a channel, the channel enabling direct communication with the given client;

based on an access token associated with the channel, obtaining a message function or a message API for providing or writing data associated with a call-back notification in the channel, the data pertaining to the corresponding blockchain transaction.

30. The method as claimed in claim 29 wherein, based on a determination of that the corresponding blockchain transaction is a double spend of a previous transaction submitted by the client; the method further includes the step of providing a return payload, the return payload including the following data:

- a transaction identifier (TxID) of the given blockchain transaction that is a double - spend; and optionally
- a service endpoint for the payment processor that submitted the given blockchain transaction

31. The method as claimed in claim 29 wherein, responsive to mining the corresponding blockchain transaction in a block, method further includes the step of providing a return Merkle proof confirming inclusion of the transaction in a block, the return Merkle proof including the following data:

- a transaction identifier (TxID) of a blockchain transaction that the Merkle proof relates to ;
- the block header of the block; and
- an array of sibling hashes for the transaction identifier.

32. The method as claimed in any one of claims 29 to 31 further comprising the steps of :
obtaining a client endpoint;
obtaining at least one client addressing key associated with the client;
providing a miner endpoint;
providing at least one s miner addressing key associated with payment processor;
exchanging one or more handshake messages using the channel based on the client and miner addressing keys;
based on a handshake result or pattern, obtaining a shared secret key;
wherein any communication using the channel is encrypted based on the shared secret key.

33. A computing device comprising a processor and memory, the memory including executable instructions that, as a result of execution by the processor, causes the device to perform the computer-implemented method as claimed in any one of claims 1 to 8, the computing device pertaining to a payment processor.

34. A computing device comprising a processor and memory, the memory including executable instructions that, as a result of execution by the processor, causes the device to perform the computer-implemented method as claimed in any one of claims 9 to 19, the computing device pertaining to a channel processor.

35. A computing device comprising a processor and memory, the memory including executable instructions that, as a result of execution by the processor, causes the device to perform the computer-implemented method as claimed in any one of claims 20 to 28, the computing device pertaining to a client.

36. A computing device comprising a processor and memory, the memory including executable instructions that, as a result of execution by the processor, causes the device to perform the computer-implemented method as claimed in any one of claims 29 to 32, the computing device pertaining to a miner.

37. A computer system comprising:
a payment processor communicatively coupled to at least one client and at least one miner via a wireless communication network, wherein the payment processor is implemented in accordance with the computing device as claimed in claim 33;
a client communicatively coupled to the payment processor via the wireless communication network, and being capable of communication with at least one customer; the client being implemented in accordance with the computing device as claimed in claim 35;
the client communicatively coupled to a channel processor via the wireless communication network, wherein the channel processor is implemented in accordance with the computing device as claimed in claim 34; and
a plurality of miners communicatively coupled to the payment processor via the wireless communication network, each miner being implemented in accordance with the computing device as claimed in claim 38.

38. A computer-readable storage medium having stored thereon executable instructions that, as a result of being executed by a processor of a computer, cause the computer to perform the method of any one of claims 1 to 32.