

CRYPTOLOGIC COORDINATED SYMMETRIC CONDITIONAL KEY RELEASE

Technical Field

5 [001] This disclosure relates to key release operations that are conditional and coordinated.

Background

[002] Rapid advances in electronics and communication technologies, driven by immense customer demand, have resulted in newly emerging secure network transactions. Improvements in the hardware and software implementations of the
10 underlying processing and privacy features for the transactions will increase the security, reliability, and speed of the implementations.

Summary

15 [003] According to a first aspect, there is provided a system including: network interface circuitry configured to: obtain a peer challenge: the peer challenge established, at least in part, in a pre-exchange proposal between a reciprocal exchange party and a leading exchange party; the peer challenge configured to designate an exchange execution platform for a cryptologically-locked asset transaction, the
20 exchange execution platform selected and identified during the pre-exchange proposal, the cryptologically-locked asset transaction configured to, when released, transfer an asset to the leading exchange party; the peer challenge configured to release the cryptologically-locked asset transaction, after: an exchange key is provided on behalf of the leading exchange party, and the cryptologically-locked asset transaction is signed
25 by the exchange execution platform; and obtain the exchange key to facilitate release of the cryptologically-locked asset transaction, the exchange key originating from the leading exchange party; and exchange circuitry in data communication with the network interface circuitry and operating on behalf of the exchange execution platform, the exchange circuitry configured to: execute the release of the cryptologically-locked
30 transaction asset by: determining an address of the leading exchange party based on the cryptologically-locked asset transaction; generating a request for the exchange key from the leading exchange party; providing the request to the leading party at the address; verifying the exchange key

against the peer challenge; and after verification of the exchange key, finalizing by: facilitating release of the cryptologically-locked asset transaction by signing the cryptologically-locked asset transaction; and at a time of authorizing release of the cryptologically-locked asset transaction, releasing the exchange key to the reciprocal exchange party.

[004] According to a second aspect, there is provided a method including: at network interface circuitry: obtaining a peer challenge: the peer challenge established, at least in part, in a pre-exchange proposal between a reciprocal exchange party and a leading exchange party; the peer challenge configured to designate an exchange execution platform for a cryptologically-locked asset transaction, the exchange execution platform selected and identified during the pre-exchange proposal, the cryptologically-locked asset transaction configured to, when released, transfer an asset to the leading exchange party; the peer challenge configured to release the cryptologically-locked asset transaction, after: an exchange key is provided by leading exchange party, and the cryptologically-locked asset transaction is signed by the exchange execution platform; and obtaining the exchange key to facilitate release of the cryptologically-locked asset transaction, the exchange key originating from the leading exchange party; and at exchange circuitry in data communication with the network interface circuitry and operating on behalf of the exchange execution platform: executing the release of the cryptologically-locked transaction asset by: determining an address of the leading exchange party based on the cryptologically-locked asset transaction; generating a request for the exchange key from the exchange party; providing the request to the leading party at the address; verifying the exchange key against the peer challenge; and after verification of the exchange key, finalizing by: facilitating release of the cryptologically-locked asset transaction by signing the cryptologically-locked asset transaction; and at a time of authorizing release of the cryptologically-locked asset transaction, releasing the exchange key to the reciprocal exchange party.

[005] According to a third aspect, there is provided a product including: machine-readable media other than a transitory signal; and instructions stored on the machine-readable media, the instructions configured to, when executed, cause a machine to: at network interface circuitry: obtain a peer challenge: the peer challenge established, at least in part, in a pre-exchange proposal between a reciprocal exchange party and a leading exchange party; the peer challenge configured to designate an exchange execution platform for a cryptologically-locked

asset transaction, the exchange execution platform selected and identified during the pre-exchange proposal, the cryptologically-locked asset transaction configured to, when released, transfer an asset to the leading exchange party; the peer challenge configured to release the cryptologically-locked asset transaction, after: an exchange key is provided by leading exchange party, and the cryptologically-locked asset transaction is signed by the exchange execution platform; and obtain the exchange key to facilitate release of the cryptologically-locked asset transaction, the exchange key originating from the leading exchange party; and at exchange circuitry in data communication with the network interface circuitry and operating on behalf of the exchange execution platform: execute the release of the cryptologically-locked transaction asset by: determining an address of the leading exchange party based on the cryptologically-locked asset transaction; generating a request for the exchange key from the exchange party; providing the request to the leading party at the address; verifying the exchange key against the peer challenge; and after verification of the exchange key, finalizing by: facilitating release of the cryptologically-locked asset transaction by signing the cryptologically-locked asset transaction; and at a time of authorizing release of the cryptologically-locked asset transaction, releasing the exchange key to the reciprocal exchange party.

Brief Description of the Drawings

- [006] Figure 1 shows an example exchange environment.
- [007] Figure 2 shows example exchange logic.
- [008] Figure 3 shows an example exchange execution platform.
- [009] Figure 4 shows an example illustrative execution scenario for example implementation exchange logic.
- [010] Figure 5 shows example exchange logic.

Detailed Description

- [011] Exchange parties may determine to perform an asset exchange. The asset exchange may be facilitated through pre-selected exchange platform. For example, the exchange parties may lack commonality in asset types among their respective holdings or commonality in asset geography. Additionally or alternatively, the exchange parties may lack commonality in transaction networking, transaction relationships, and/or transaction infrastructure. Thus, a third party may provide a platform on which the exchange parties may provide assets in types and

Claims

What is claimed is:

1. A system including:

network interface circuitry configured to:

obtain a peer challenge:

the peer challenge established, at least in part, in a pre-exchange proposal between a reciprocal exchange party and a leading exchange party;

the peer challenge configured to designate an exchange execution platform for a cryptologically-locked asset transaction, the exchange execution platform selected and identified during the pre-exchange proposal, the cryptologically-locked asset transaction configured to, when released, transfer an asset to the leading exchange party;

the peer challenge configured to release the cryptologically-locked asset transaction, after:

an exchange key is provided on behalf of the leading exchange party, and

the cryptologically-locked asset transaction is signed by the exchange execution platform; and

obtain the exchange key to facilitate release of the cryptologically-locked asset transaction, the exchange key originating from the leading exchange party; and

exchange circuitry in data communication with the network interface circuitry and operating on behalf of the exchange execution platform, the exchange circuitry configured to:

execute the release of the cryptologically-locked transaction asset by:

determining an address of the leading exchange party based on the cryptologically-locked asset transaction;

generating a request for the exchange key from the leading exchange party;

providing the request to the leading party at the address;

verifying the exchange key against the peer challenge; and

after verification of the exchange key, finalizing by:

facilitating release of the cryptologically-locked asset transaction
by signing the cryptologically-locked asset transaction; and
at a time of authorizing release of the cryptologically-locked
asset transaction, releasing the exchange key to the reciprocal
exchange party.

2. The system of claim 1, where:

the cryptologically-locked asset transaction configured to, upon expiry without
release, return an asset to the reciprocal exchange party instead of transferring the
asset to the leading exchange party;

the cryptologically-locked asset transaction is configured to establish a timeout
window; and

after expiry of the timeout window, the cryptologically-locked asset transaction is
configured to expire without release.

3. The system of claim 1, where the pre-exchange proposal includes:

transfer of a cryptologic puzzle from the leading exchange party to the
reciprocal exchange party while withholding the exchange key,
the exchange key corresponding to a solution of the cryptologic puzzle.

4. The system of claim 3, where a reciprocal node, on behalf of the reciprocal
exchange party, is configured to generate the peer challenge based on the
cryptologic puzzle.

5. The system of claim 1, where the exchange circuitry is configured to release
the exchange key to the reciprocal exchange party by:

publishing the exchange key on a distributed ledger;

storing the exchange key in a decrypted form;

distributing the exchange key over a peer network;

encrypting the exchange key using a public key associated with the reciprocal
exchange party;

addressing the exchange key to the reciprocal exchange party;

sending, via the network interface circuitry, the exchange key to a reciprocal node over a communication link, the reciprocal node associated with the reciprocal exchange party; or
any combination of the foregoing.

6. The system of claim 1, where the network interface circuitry is configured to obtain the peer challenge by:

receiving the peer challenge over a communication link from a reciprocal node associated with the reciprocal exchange party;
accessing the peer challenge on a distributed ledger;
receiving the peer challenge from a peer node within a peer network; or
any combination of the foregoing.

7. The system of claim 1, where the cryptologically-locked asset transaction is digitally signed using a reciprocal private key associated with the reciprocal exchange party.

8. The system of claim 1, where exchange circuitry is configured to verify the exchange key against the peer challenge by:

sending the cryptologically-locked asset transaction to the leading exchange party; and
after sending the cryptologically-locked asset transaction, obtaining the cryptologically-locked asset transaction digitally signed using a leading private key associated with the leading exchange party.

9. The system of claim 1, where the peer challenge includes a hash.

10. The system of claim 1, where the request for the exchange key includes:

a reference to the peer challenge;
a reference to the cryptologically-locked asset transaction;
the peer challenge;
the cryptologically-locked asset transaction; or
any combination of the foregoing.

11. A method including:

at network interface circuitry:

obtaining a peer challenge:

the peer challenge established, at least in part, in a pre-exchange proposal between a reciprocal exchange party and a leading exchange party;

the peer challenge configured to designate an exchange execution platform for a cryptologically-locked asset transaction, the exchange execution platform selected and identified during the pre-exchange proposal, the cryptologically-locked asset transaction configured to, when released, transfer an asset to the leading exchange party;

the peer challenge configured to release the cryptologically-locked asset transaction, after:

an exchange key is provided by leading exchange party, and

the cryptologically-locked asset transaction is signed by the exchange execution platform; and

obtaining the exchange key to facilitate release of the cryptologically-locked asset transaction, the exchange key originating from the leading exchange party; and

at exchange circuitry in data communication with the network interface circuitry and operating on behalf of the exchange execution platform:

executing the release of the cryptologically-locked transaction asset by:

determining an address of the leading exchange party based on the cryptologically-locked asset transaction;

generating a request for the exchange key from the exchange party;

providing the request to the leading party at the address;

verifying the exchange key against the peer challenge; and

after verification of the exchange key, finalizing by:

facilitating release of the cryptologically-locked asset transaction by signing the cryptologically-locked asset transaction; and

at a time of authorizing release of the cryptologically-locked asset transaction, releasing the exchange key to the reciprocal exchange party.

12. The method of claim 11, where releasing the exchange key to the reciprocal exchange party includes:

- publishing the exchange key on a distributed ledger;
- storing the exchange key in a decrypted form;
- distributing the exchange key over a peer network;
- encrypting the exchange key using a public key associated with the reciprocal exchange party;
- addressing the exchange key to the reciprocal exchange party;
- sending, via the network interface circuitry, the exchange key to a reciprocal node over a communication link, the reciprocal node associated with the reciprocal exchange party; or
- any combination of the foregoing.

13. The method of claim 11, where obtaining the peer challenge includes:

- receiving the peer challenge over a communication link from a reciprocal node associated with the reciprocal exchange party;
- accessing the peer challenge on a distributed ledger;
- receiving the peer challenge from a peer node within a peer network; or
- any combination of the foregoing.

14. The method of claim 11, where the cryptologically-locked asset transaction is digitally signed using a reciprocal private key associated with the reciprocal exchange party.

15. The method of claim 11, where verifying the exchange key against the peer challenge includes:

- sending the cryptologically-locked asset transaction to the leading exchange party; and

after sending the cryptologically-locked asset transaction, obtaining the cryptologically-locked asset transaction digitally signed using a leading private key associated with the leading exchange party.

16. The method of claim 11, where the peer challenge includes a hash
17. The method of claim 11, where the request for the exchange key includes:
 - a reference to the peer challenge;
 - a reference to the cryptologically-locked asset transaction;
 - the peer challenge;
 - the cryptologically-locked asset transaction; or
 - any combination of the foregoing.
18. A product including:
 - machine-readable media other than a transitory signal; and
 - instructions stored on the machine-readable media, the instructions configured to, when executed, cause a machine to:
 - at network interface circuitry:
 - obtain a peer challenge:
 - the peer challenge established, at least in part, in a pre-exchange proposal between a reciprocal exchange party and a leading exchange party;
 - the peer challenge configured to designate an exchange execution platform for a cryptologically-locked asset transaction, the exchange execution platform selected and identified during the pre-exchange proposal, the cryptologically-locked asset transaction configured to, when released, transfer an asset to the leading exchange party;
 - the peer challenge configured to release the cryptologically-locked asset transaction, after:
 - an exchange key is provided by leading exchange party,
 - and

the cryptologically-locked asset transaction is signed by the exchange execution platform; and
obtain the exchange key to facilitate release of the cryptologically-locked asset transaction, the exchange key originating from the leading exchange party; and
at exchange circuitry in data communication with the network interface circuitry and operating on behalf of the exchange execution platform:
execute the release of the cryptologically-locked transaction asset by:
determining an address of the leading exchange party based on the cryptologically-locked asset transaction;
generating a request for the exchange key from the exchange party;
providing the request to the leading party at the address;
verifying the exchange key against the peer challenge; and
after verification of the exchange key, finalizing by:
facilitating release of the cryptologically-locked asset transaction by signing the cryptologically-locked asset transaction; and
at a time of authorizing release of the cryptologically-locked asset transaction, releasing the exchange key to the reciprocal exchange party.

19. The product of claim 18, where the pre-exchange proposal includes:
transfer of a cryptologic puzzle from the leading exchange party to the reciprocal exchange party while withholding the exchange key,
the exchange key corresponding to a solution of the cryptologic puzzle.
20. The product of claim 19, where a reciprocal node, on behalf of the reciprocal exchange party, is configured to generate the peer challenge based on the cryptologic puzzle.