

**LEADING-PARTY-INITIATED CRYPTOLOGIC
COORDINATED SYMMETRIC CONDITIONAL KEY RELEASE**

Technical Field

[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 underlying processing and privacy features for the transactions will increase the security, reliability, and speed of the implementations.

Summary

[003] According to a first aspect of the invention, 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 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 a request to release the cryptologically-locked asset transaction, the request originating from the leading exchange party, the request being addressed to the exchange execution platform; 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: based on the request,

obtaining the exchange key; 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 symmetrically, along with authorizing release of the cryptologically-locked asset transaction, releasing the exchange key to the reciprocal exchange party.

[004] According to a second aspect of the invention, 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 on behalf of the leading exchange party, and the cryptologically-locked asset transaction is signed by the exchange execution platform; and obtaining a request to release the cryptologically-locked asset transaction, the request originating from the leading exchange party, the request being addressed to the exchange execution platform; 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: based on the request, obtaining the exchange key; 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 symmetrically, along with authorizing release of the cryptologically-locked asset transaction, releasing the exchange key to the reciprocal exchange party.

[005] According to a third aspect of the invention, 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 on behalf of the leading exchange party, and the cryptologically-locked asset transaction is signed by the exchange execution platform; and obtain a request to release the cryptologically-locked asset transaction, the request originating from the leading exchange party, the request being addressed to the exchange execution platform; 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: based on the request, obtaining the exchange key; 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 symmetrically, along with 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

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 a request to release the cryptologically-locked asset transaction, the request originating from the leading exchange party, the request being addressed to the exchange execution platform; 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:

based on the request, obtaining the exchange key;

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

symmetrically, along with 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 request includes the exchange key; and
the exchange circuitry is configured to obtain the exchange key by extracting the exchange key from the request.
3. The system of claim 1, where the network interface circuitry is configured to obtain the request by:
accessing the request on a distributed ledger;
decrypting the request using a private key associated with an identity controlled by the exchange execution platform;
receiving the request from a peer node within a peer network; or
any combination of the foregoing.
4. The system of claim 1, where the request is signed using a private key associated with an identity controlled by the leading exchange party.
5. The system of claim 1, where the network interface circuitry is configured to obtain the request after a leading node associated with the leading exchange party performs an inspection of the cryptologically-locked asset transaction.
6. The system of claim 5, where the inspection includes a determination that the asset includes an asset defined in the pre-exchange proposal.

7. The system of claim 1, where the request does not include the exchange key.
8. The system of claim 7, where the exchange circuitry is configured to obtain the exchange key by:
 - sending a communication to the leading exchange party in response to request;
 - accessing the exchange key based on a reference within the request;
 - receiving a message including the exchange key, the message sent on behalf of the leading exchange party, the message separate from the request; or
 - any combination of the foregoing.
9. 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 on behalf of the leading exchange party, and
 - the cryptologically-locked asset transaction is signed by the exchange execution platform; and
 - obtaining a request to release the cryptologically-locked asset transaction, the request originating from the leading exchange party, the request being addressed to the exchange execution platform; 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:

based on the request, obtaining the exchange key;
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
symmetrically, along with authorizing release of the cryptologically-
locked asset transaction, releasing the exchange key to the
reciprocal exchange party.

10. The method of claim 9, where:

the request includes the exchange key; and

where obtaining the exchange key includes extracting the exchange key from the
request.

11. The method of claim 9, where obtaining the request includes:

accessing the request on a distributed ledger;

decrypting the request using a private key associated with an identity controlled
by the exchange execution platform;

receiving the request from a peer node within a peer network; or

any combination of the foregoing.

12. The method of claim 9, where the request is signed using a private key
associated with an identity controlled by the leading exchange party.

13. The method of claim 9, where the network interface circuitry is configured to
obtain the request after a leading node associated with the leading exchange party
performs an inspection of the cryptologically-locked asset transaction.

14. The method of claim 13, where the inspection includes a determination that the asset includes an asset defined in the pre-exchange proposal.

15. 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 on behalf of the leading exchange party, and

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

obtain a request to release the cryptologically-locked asset transaction, the request originating from the leading exchange party, the request being addressed to the exchange execution platform; 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:

based on the request, obtaining the exchange key;

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

symmetrically, along with authorizing release of the cryptologically-locked asset transaction, releasing the exchange key to the reciprocal exchange party.

16. The product of claim 15, 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.