(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第7204231号
(P7204231)
(45)発行日　令和5年1月16日(2023.1.16)　(24)登録日　令和5年1月5日(2023.1.5)

(51)Int.Cl.　　F I
G06Q 20/02 (2012.01)　G06Q 20/02
G06Q 20/10 (2012.01)　G06Q 20/10

請求項の数 40　外国語出願　(全 78 頁)

(21)出願番号　特願2020-209670(P2020-209670)
(22)出願日　令和2年12月17日(2020.12.17)
(62)分割の表示　特願2017-511157(P2017-511157)の分割
原出願日　平成27年5月5日(2015.5.5)
(65)公開番号　特開2021-61021(P2021-61021A)
(43)公開日　令和3年4月15日(2021.4.15)
審査請求日　令和3年1月15日(2021.1.15)
(31)優先権主張番号　61/990,795
(32)優先日　平成26年5月9日(2014.5.9)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　516335038
ミドルトン，レジナルド
アメリカ合衆国，エヌワイ　１１２１８，ブルックリン，１９５　アーガイル　アールディー
(74)代理人　110002952
弁理士法人鷲田国際特許事務所
(72)発明者　ミドルトン，レジナルド
アメリカ合衆国，エヌワイ　１１２１８，ブルックリン，１９５　アーガイル　アールディー
(72)発明者　ボゴシアン，マシュー
アメリカ合衆国，ダブリューエー　９８２２１，アナコルテス，５００７　トータム　ティーアールエル

最終頁に続く

(54)【発明の名称】信頼度が低い、または信頼度が皆無の当事者間での価値転送を円滑化する装置、システム、または方法

(57) [Scope of Claims]

[Claim 1]

A system for facilitating value transfer between a first party using a first client and a second party using a second client via a transfer mechanism, the transfer mechanism comprising: , a facilitator, a facilitator, the first client, and a second client respectively via a computer network, wherein the system comprises: the facilitator, the first client, and the second client; a. The facilitator may: i. A first memory having a transaction record sector and a first key pair sector storing a first asymmetric key pair, said first asymmetric key pair comprising a first private key and a first public key. a first memory having a ii. A first network interface for receiving terms used to determine payment amounts, said terms comprising:A. at least one of a first principal amount and a second principal amount;B. a reference to at least one of a first data source and a second data source, said first data source comprising a first database storing data relating to a first security; B. said reference, wherein the second data source comprises a second database storing data relating to the second security; payment terms;

Ten

20

D. a first network interface including an expiration timestamp; b. Said first client: i. a second memory having a second key pair sector storing a second asymmetric key pair, said second asymmetric key pair having a second private key and a second public key; , ii. a second network interface; iii. A second computer processor coupled to said second memory and said second network interface, comprising: A. B. reading said second private key from said second key pair sector; B. creating and signing a first source transaction record using said second private key; creating an uncompleted commit transaction record, said uncompleted commit transaction record comprising: I. a value from at least one of said first data source and said second data source; II. a committed amount; III. C. a condition requiring approval of at least two of said facilitator, said first client, and said second client; E. creating a complete commit transaction record by signing the incomplete commit transaction record using the second private key; creating an incomplete expiry date transaction record, said incomplete expiry date transaction record comprising: I. A lock time since said expiration timestamp; II. said committed amount; III. F. a first expiration date output comprising a first expiration date amount and a first condition requiring approval of said first client; G. signing said pending expiry transaction record using said second private key; sending said complete committed transaction record and said unfinished expiry transaction record to said second client; c. Said second client: i. a third memory having a third key pair sector storing a third asymmetric key pair, said third asymmetric key pair having a third private key and a third public key; and , ii. a third network interface; iii. A third computer processor coupled to said third memory and said third network interface, comprising: A. B. reading said pending expiry transaction record; B. reading said third private key from said third key pair sector; C. creating a complete expiration date transaction record by signing said incomplete expiration date transaction record using said third private key; A. a first computer processor of said facilitator configured to: transmit said complete expiry date transaction record to said first client; Upon detecting, via an application program interface (API), that said payment terms are met from at least one of said first data source and said second data source, a payment function is applied to: Calculate the above payments; I. at least one of said first principal amount and said second principal amount; II. said value from at least one of said first data source and said second data source;

,

B. B. reading said first private key from said first key pair sector; creating and signing a pending payment transaction record using said first private key, said pending payment transaction comprising: I. the committed amount received from the committed transaction; II. D. the one or more payment amounts; issuing the signed incomplete payment transaction record to the first client and the second client to ensure that at least one of the first client and the second client completes the payment transaction record; and wherein the facilitator, the first client and the second client are configured to create the first network interface, the second network interface and the third network interface. a system coupled to said computer network via respective interfaces. 2. Said payment terms are: i. results from querying at least one of said first data source and said second data source; ii. observing the presence or absence of data at the expected location; iii. Determining if in the expected set of values or matching the expected pattern

,

iv. 3. The system of claim 1, comprising: receiving a signal from a digital device and verifying that the signal value is within an expected range or tolerance. [Claim 3]

wherein said third computer processor validates said second source transaction by creating and signing a second source transaction record and submitting said second source transaction record to said transfer mechanism; 2. The system of claim 1, further configured.
[Claim 4]
The second computer processor is further configured to store the full commit transaction record in the second memory, and the third computer processor stores the full commit transaction record in the third memory. 2. The system of claim 1, further configured to store transaction records and to store said complete expiry date transaction record in said third memory. [Claim 5]

2. The incomplete expiration transaction record of claim 1, further comprising a second expiration output including a second expiration amount and a condition requiring approval of the second client. system. 6. The one or more payment amounts are: i. a first payment amount and a condition requiring approval of said second client; ii. a second payment amount and a condition requiring approval of said first client; iii. 2. The system of claim 1, comprising at least one of: a fee amount; and a condition requiring third party approval.

7. The first
computer processor comprises: a. creating and
signing a pending refund transaction record using said first private key, said pending refund transaction record comprising: i. the committed amount received from the committed transaction; ii. including the refund amount and

b. further configured to issue the pending refund transaction record to at least one of the first client and the second client, wherein the second computer processor or the third computer processor is configured to: creating a complete refund transaction record from the incomplete refund transaction record, wherein said complete refund transaction record protects funds even in the event of a complete failure of said first client or said second client; 11. The system of claim 1, used to create a refund transaction so that it can be collected. [Claim 8]

A method of facilitating value transfer between a first party using a first client and a second party using a second client by a transfer mechanism, the transfer mechanism comprising: comprising a decentralized digital currency accessible via a computer network by a facilitator, said first client, and a second client, respectively, said method comprising: a. Storing by the facilitator a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key; b. Receipt by said facilitator of terms for determining a payment amount, said terms comprising: A. at least one of a first principal amount and a second principal amount;B. a reference to at least one of a first data source and a second data source, said first data source comprising a first database storing data relating to a first security; B. said reference, wherein the second data source comprises a second database storing data relating to the second security; payment terms;D. an expiration timestamp; and c. storing by said first client a second asymmetric key pair, said second asymmetric key pair having a second private key and a second public key; d. reading, by said first client, said second private key from a second key pair sector; e. creating and signing, by said first client, a first source transaction record using said second private key; f. creating, by said first client, an uncompleted commit transaction record comprising; a value from at least one of said first data source and said second data source; II. a committed amount; III. a condition requiring approval of at least two of said facilitator, said first client, and said second client; g. Signing, by the first client, the pending commit transaction record using the second private key; h. creating an incomplete expiry date transaction record including; I. A lock time since said expiration timestamp; II. a committed amount; III. a condition requiring approval of at least two of said facilitator, said first client, and said second client; i. Signing the pending expiry transaction record using the second private key

and j.
sending a complete committed transaction record and the unfinished expiry transaction record to the second client;

k. storing by said second client a third asymmetric key pair, said third asymmetric key pair having a third private key and a third public key; l. reading, by the second client, the pending expiry transaction record;

When ,

m. reading, by said second client, said third private key from a third key pair sector; n. creating a complete expiry date transaction record by said second client by signing said incomplete expiry date transaction record using said third private key; o. sending, by said second client, said complete expiry date transaction record to said first client; p. sending, by said first client, a first source transaction record to said transfer mechanism to validate said first source transaction; q. sending, by said first client, said complete commit transaction record to said transfer mechanism to validate said commit transaction; r. Upon detecting, by the facilitator, via an Application Program Interface (API), from at least one of the first data source and the second data source that the payment terms are met, a payment function is applied to: I. calculating one or more payment amounts; at least one of said first principal amount and said second principal amount; II. said value from at least one of said first data source and said second data source; s. reading, by the facilitator, the first private key from a first key pair sector; t. creating and signing, by said facilitator, using said first private key, a pending payment transaction record containing; the committed amount received from the committed transaction; II. said one or more payment amounts; u. Issuing, by said facilitator, said signed pending payment transaction record to said first client and said second client to ensure that at least one of said first client and said second client completes creating accurate payment transaction records;

Ten

20

30

,

wherein

said facilitator, said first client, and said second client are connected to said computer network via a first network interface, a second network interface, and a third interface, respectively. How it is interfaced.

9. Said payment

terms are: i. results from

40

querying at least one of said first data source and said second data source; ii. observing the presence or absence of data at the expected location; iii. Determining if in the expected set of values or matching the expected pattern

,

iv. 9. The method of claim 8, comprising receiving a signal from a digital device and verifying that signal values are within expected ranges or tolerances. [Claim 10]

creating and signing a second source transaction record by said second client;

50

9. The method of claim 8, further comprising validating the second source transaction by submitting the second source transaction record to the transfer mechanism by the second client. [Claim 11]

storing the full commit transaction in the second memory by the first client; storing the full commit transaction in the third memory by the second client; 9. The method of claim 8, further comprising storing said complete expiry date transaction record in three memories.

[Claim 12]
9. The method of claim 8, wherein the incomplete expiration transaction record further comprises a second expiration output including a second expiration amount and a condition requiring approval of the second client.
.
13. The one or
more payment amounts are: i. a
first payment amount and a condition requiring approval of said second client; ii. a second
payment amount and a condition requiring approval of said first client; and iii. 9. The method
of claim 8, comprising at least one of: a fee amount; and a condition requiring third party
approval. 14. The method comprising: a. creating and signing a pending refund transaction
record using said first private key, said pending refund transaction record: i. the committed
amount received from the committed transaction; ii. the refund amount; and b. issuing said
pending refund transaction record to at least one of said first client and second client; c. creating a
complete refund transaction record from said incomplete refund transaction record, wherein said complete
refund transaction record is sufficient to secure funds even in the event of complete failure of said first
client or said second client; 9. The method of claim 8, comprising: used to create a refund transaction so
that it can be collected. [Claim 15]

A system for facilitating value transfer between a first party using a first client and a second party using a
second client by a transfer mechanism, the transfer mechanism comprising: a distributed digital currency
accessible via a computer network by a facilitator, said first client, and a second client, respectively, said
system comprising said facilitator, said first client, and said second client; including a. The facilitator may:
i. A first memory having a transaction record sector and a first key pair sector storing a first asymmetric
key pair, said first asymmetric key pair comprising a first private key and a first public key. a first memory
having a ii. A first network interface for receiving conditions for determining a payment amount, said
conditions comprising:A. at least one of a first principal amount and a second principal amount;B. a
reference to at least one of a first data source and a second data source, said first data source comprising
a first database storing data relating to a first security, said second data source has a second database
that stores data about the second security,

a first network interface; iii. A first computer processor coupled to said first memory and said first network interface, comprising: A. by applying a payment function to values from at least one of said first principal amount and said second principal amount and from at least one of said first data source and said second data source; , calculating one or more payments;B. B. reading said first private key from said first key pair sector; D. calculating a first cryptographic signature from said first private key; creating a pending payment transaction record, said pending payment transaction record comprising: I. Committed Amount Received from Committed Transactions II. said one or more payment amounts; and III. E. said first cryptographic signature; a first computer processor for issuing said pending payment transaction record to at least one of said first client or said second client; b. Said first client: i. a second memory having a second key pair sector storing a second asymmetric key pair, said second asymmetric key pair having a second private key and a second public key; , ii. a second network interface; iii. A second computer processor coupled to said second memory and said second network interface, comprising: A. B. reading said second private key from said second key pair sector; B. reading said pending payment transaction record; D. calculating a second cryptographic signature from said second private key; creating a completed payment transaction record, said completed payment transaction record comprising: I. said committed amount; II. said one or more payments; III. said first cryptographic signature; and IV. E. said second cryptographic signature; a second computer processor that creates a payment transaction by submitting the completed payment transaction record to the transfer mechanism; c. Said second client: i. a third memory having a third key pair sector storing a third asymmetric key pair, said third asymmetric key pair having a third private key and a third public key; and , ii. a third network interface; iii. a third computer processor coupled to said third memory and said third network interface, said third computer processor reading said third private key from said third key pair sector; said facilitator, said first client, and said second client are connected to said computer network via said first network interface, said second network interface, and said third network interface, respectively; A system that is coupled to

16. The first computer processor comprises: a. creating a third cryptographic signature from the first private key;

b. Create an uncompleted refund transaction record with: i. the committed amount received from the committed transaction; ii. the refund amount; and iii. said third cryptographic signature; c. further configured to issue the pending refund transaction record to at least one of the first client or the second client, wherein the second computer processor or the third computer processor further configured to create a complete refund transaction record from the final refund transaction record, wherein the complete refund transaction record is generated when the first client or the second client encounters a completely unsuccessful event; 16. The system of claim 15, wherein the system is used to create refund transactions so that funds can be recovered even if the

[Claim 17]

A method performed by a system that facilitates value transfer between a first party using a first client and a second party using a second client via a transfer mechanism, comprising: A method, wherein said transfer mechanism comprises a decentralized digital currency accessible via a computer network by a facilitator, said first client, and a second client, respectively, comprising: a. said first client storing a first asymmetric key pair in a first key pair sector of a first memory, said first asymmetric key pair comprising a first public key and a first private key; b. the facilitator storing a second asymmetric key pair in a second key pair sector of a second memory, the second asymmetric key pair having a second public key and a second private key; a step; c. said facilitator storing a third asymmetric key pair in said second key pair sector, said third asymmetric key pair having a third public key and a third private key; . said first client storing a fourth asymmetric key pair in a third key pair sector of a third memory, said fourth asymmetric key pair comprising a fourth public key and a fourth private key; e. said first client sending, via a network interface, terms for determining a payment amount, said terms comprising: i. at least one of a first principal amount and a second principal amount; ii. a reference to at least one of a first data source and a second data source; said first data source comprising a first database storing data relating to securities; having a second database storing data relating to the two securities; f. said facilitator receiving said condition via a second network interface; g. The facilitator uses the payment function to: i. at least one of said first principal amount and said second principal amount; and ii. from at least one of said first data source and said second data source to calculate one or more payment amounts; h. said first client reading said first private key from said first key pair sector; i. said facilitator computing a first cryptographic signature from said first private key; j. the first client creating a first principal transaction record, the first principal transaction record comprising:

i. said first principal amount; and ii. said
first cryptographic signature; k. said first client creating a first
principal transaction by submitting said first principal transaction record to said transfer mechanism; l. said facilitator reading said second private key from said second key pair sector; m. said facilitator computing a second cryptographic signature from said second private key; n. the facilitator creating a commit transaction record, the commit transaction record comprising: i. said first principal amount; ii. a committed amount, and iii. said second cryptographic signature; o. said facilitator creating a commit transaction by submitting said commit transaction record to said transfer mechanism; p. said facilitator retrieving the value of said security from said first data source; q. said facilitator reading said third private key from said second key pair sector; r. said facilitator computing a third cryptographic signature from said second private key; s. the facilitator creating a pending payment transaction record, the pending payment transaction record comprising: i. the committed amount received from the committed transaction; ii. said one or more payment amounts; and iii. said third cryptographic signature; t. said facilitator issuing said pending payment transaction record to at least one of said first client or said second client; u. said first client reading said pending payment transaction record; said first client reading said fourth private key from said third key pair sector; w. said first client computing a fourth cryptographic signature from said fourth private key; x. said first client creating a completed payment transaction record, said completed payment transaction record comprising: i. said committed amount; ii. said one or more payment amounts; iii. said third cryptographic signature, and iv. said fourth cryptographic signature; y. said first client creating a payment transaction by submitting said completed payment transaction record to said transfer mechanism. 18. The method comprising the steps of: a. calculating, by the facilitator, a third cryptographic signature from the first private key; b. creating an uncompleted refund transaction record having i. the committed amount received from the committed transaction; ii. the refund amount; and iii. the third cryptographic signature;

c. issuing said pending refund transaction record to at least one of said first client and said second client; d. Generating a complete refund transaction record from the incomplete refund transaction record, wherein the complete refund transaction record is generated when the first client or the second client fails completely. 18. The method of claim 17, further comprising: used to create a refund transaction so that funds can be recovered even if the transaction has occurred. [Claim 19]

The condition further includes an expiration timestamp, wherein the expiration timestamp is specified by a date and time indicating when the condition expires, or the expiration timestamp indicates that the condition does not expire. 18. The method of claim 17, set to infinity
.

[Claim 20]

An apparatus for facilitating value transfer between a first party using a first client and a second party using a second client by a transfer mechanism, the transfer mechanism comprising: A device comprising a decentralized digital currency accessible via a computer network by said device, said first client, and a second client, respectively, comprising: a. A first memory having a transaction record sector and a first key pair sector storing a first asymmetric key pair, said first asymmetric key pair having a first private key and a first public key. a first memory; b. A first network interface for receiving terms for determining a payment amount, said terms comprising: i. at least one of a first principal amount and a second principal amount; ii. a reference to at least one of a first data source and a second data source; said first data source having a first database storing data relating to a first security; said second data source; a first network interface, the source having a second database storing data relating to the second security; c. a first computer processor coupled to said first memory and said first network interface, comprising: i. A. payment functions; at least one of said first principal amount and said second principal amount; and B. from at least one of said first data source and said second data source to calculate one or more payment amounts, ii. reading said first private key from said first key pair sector; iii. Compute a first cryptographic signature from the first private key; iv. creating a pending payment transaction record, said pending payment transaction record comprising: A. the committed amount received from the committed trade;B. B. said one or more payment amounts; said first cryptographic signature; v. a first computer processor for issuing said pending payment transaction record to at least one of said first client and said second client; said device, said first client, and said A second client is coupled to the computer network via the first network interface, the second network interface, and the third network interface, respectively, the pending payment transaction record comprising: used by at least one of said first client and said second client to create a complete payment transaction by sending a complete payment transaction record to said transfer mechanism;

Said complete payment transaction
record: A. B. the committed
amount; B. said one or more payment
amounts; D. said first cryptographic
signature; a second cryptographic signature calculated from a second private key stored on said first client. 21. The first computer processor comprising: a. Compute a third cryptographic signature from the first private key; b. Create an uncompleted reimbursement transaction record, including i. the committed amount received from the committed transaction; ii. the refund amount; and iii. said third cryptographic signature; iv. lock time; c. and issuing the pending refund transaction record to at least one of the first client or the second client, wherein the pending refund transaction record is sent to the first client and/or 21. The apparatus of claim 20, or wherein the second client is used to create refund transactions so that funds can be recovered even in the event of a completely failed event. [Claim 22]

The condition further includes an expiration timestamp, wherein the expiration timestamp is specified by a date and time indicating when the condition expires, or the expiration timestamp indicates that the condition does not expire. 21. Apparatus according to claim 20, set to infinity
.

[Claim 23]
An apparatus for facilitating value transfer between a first party using a first client and a second party using a second client by a transfer mechanism, the transfer mechanism comprising: A device comprising a decentralized digital currency accessible via a computer network by said device, said first client, and a second client, respectively, comprising: a. A first memory having a transaction record sector and a first key pair sector storing a first asymmetric key pair, said first asymmetric key pair comprising a first private key and a first public key. a first memory; b. A first network interface for receiving terms for determining a payment amount, said terms comprising: i. at least one of a first principal amount and a second principal amount; ii. a reference to at least one of a first data source and a second data source; said first data source having a first database storing data relating to a first security; and said second data source has a second database storing data relating to a second security; iii. a first network interface including an expiration timestamp and

When ,
c. a first computer processor coupled to said first memory and said first network interface, comprising: i. A. payment functions; at least one of said first principal amount and said second principal amount; and B. from at least one of said first data source and said second data source to calculate one or more payment amounts, ii. reading said first private key from said first key pair sector;

iii. Compute a first cryptographic signature from the first private key; iv. creating a pending payment transaction record, said pending payment transaction record comprising: A. B. Commitments received from Commitment Transactions; B. said one or more payment amounts; said first cryptographic signature; v. a first computer processor for issuing said pending payment transaction record to at least one of said first client and said second client, wherein said first client: a. a second memory having a second key pair sector storing a second asymmetric key pair, said second asymmetric key pair having a second private key and a second public key; a memory; b. a second network interface; c. a second computer processor coupled to said second memory and said second network interface, comprising: i. reading said second private key from said second key pair sector; ii. reading the pending payment transaction record; iii. Compute a second cryptographic signature from the second private key; iv. creating a completed payment transaction record, said completed payment transaction record comprising: A. said contracted amount;B. B. the one or more payments; D. said first cryptographic signature; said second cryptographic signature; v. a second computer processor that creates a payment transaction by submitting the completed payment transaction record to the transfer mechanism, wherein the second client: a. a third memory having a third key pair sector storing a third asymmetric key pair, said third asymmetric key pair having a third private key and a third public key; a memory; b. a third network interface; c. a third computer processor coupled to said third memory and said third network interface, said third computer processor reading said third private key from said third key pair sector. and said device, said first client, and said second client connect to said computer network via said first network interface, said second network interface, and said third network interface, respectively. coupled with the first computer processor further comprising: a. Compute a third cryptographic signature from the first private key; b. creating an uncompleted refund transaction record, said uncompleted refund transaction record comprising: i. said committed amount received from said committed transaction; ii. the refund amount; iii. said third cryptographic signature, and iv. including lock time; c. issuing said pending refund transaction record to at least one of said first client or said second client; a. said first key pair sector further stores a fourth asymmetric key pair, said fourth asymmetric key pair having a fourth private key and a fourth public key; b. The first computer processor may further: i. reading the fourth private key from the first key pair sector;

ii. Compute a fourth cryptographic signature from the fourth private key; iii. creating a contract transaction record, said contract transaction record comprising: A. B. said first principal amount; B. said contracted amount; said fourth cryptographic signature; iv. creating the executed transaction by submitting the executed transaction record to the transfer mechanism, wherein the first asymmetric key pair is the same as the fourth asymmetric key pair, and the first private key is the same as the fourth asymmetric key pair; is identical to four private keys, said first public key being identical to said fourth public key; a. said reference to said first data source or said second data source includes at least one of a reference to a base security or a reference to a quote security; b. The first computer processor further calculates the payment amount after the expiration timestamp. [Claim 24]

Ten

An apparatus for facilitating value transfer between a first party using a first client and a second party using a second client by a transfer mechanism, the transfer mechanism comprising: A device comprising a decentralized digital currency accessible via a computer network by said device, said first client, and a second client, respectively, comprising: a. A first memory having a transaction record sector and a first key pair sector storing a first asymmetric key pair, said first asymmetric key pair comprising a first private key and a first public key. a first memory; b. A first network interface for receiving terms for determining a payment amount, said terms comprising: i. at least one of a first principal amount and a second principal amount; ii. a reference to at least one of a first data source and a second data source; said first data source having a first database storing data relating to a first security; and said second data source has a second database storing data relating to a second security; iii. a first network interface including an expiration timestamp and

20

30

When ,

c. a first computer processor coupled to said first memory and said first network interface, comprising: i. A. payment functions; at least one of said first principal amount and said second principal amount; and B. from at least one of said first data source and said second data source to calculate one or more payment amounts, ii. reading said first private key from said first key pair sector; iii. Compute a first cryptographic signature from the first private key; iv. creating a pending payment transaction record, said pending payment transaction record comprising: A. B. Commitments received from Commitment Transactions; B. said one or more payment amounts; said first cryptographic signature; v. a first computer processor for issuing said pending payment transaction record to at least one of said first client or said second client, wherein said first client: a. a second memory having a second key pair sector storing a second asymmetric key pair;

40

50

a second memory, wherein said second asymmetric key pair comprises a second private key and a second public key; b. a second network interface; c. a second computer processor coupled to said second memory and said second network interface, comprising: i. reading said second private key from said second key pair sector; ii. reading the pending payment transaction record; iii. Compute a second cryptographic signature from the second private key; iv. creating a completed payment transaction record, said completed payment transaction record comprising: A. said contracted amount;B. B. the one or more payments; D. said first cryptographic signature; said second cryptographic signature; v. a second computer processor that creates a payment transaction by submitting the completed payment transaction record to the transfer mechanism, wherein the second client: a. a third memory having a third key pair sector storing a third asymmetric key pair, said third asymmetric key pair having a third private key and a third public key; a memory; b. a third network interface; c. a third computer processor coupled to said third memory and said third network interface, said third computer processor reading said third private key from said third key pair sector. and said device, said first client, and said second client connect to said computer network via said first network interface, said second network interface, and said third network interface, respectively. coupled, wherein said first computer processor performs said payment function by: i. said first principal amount; and ii. calculating said one or more payments by applying to said value of said first security; a. said first key pair sector further stores a fourth asymmetric key pair, said fourth asymmetric key pair having a fourth private key and a fourth public key; b. The first computer processor may further: i. reading said fourth private key from said first key pair sector; ii. Compute a third cryptographic signature from the fourth private key; iii. creating a contract transaction record, said contract transaction record comprising: A. B. said first principal amount; B. said contracted amount; said third cryptographic signature; iv. creating the executed transaction by submitting the executed transaction record to the transfer mechanism, wherein the first asymmetric key pair is the same as the fourth asymmetric key pair, and the first private key is the same as the fourth asymmetric key pair; is identical to four private keys, said first public key being identical to said fourth public key; a. said reference to said first data source or said second data source includes at least one of a reference to a base security or a reference to a quote security; b. The first computer processor further calculates the payment amount after the expiration timestamp.

[Claim 25]

An apparatus for facilitating the transfer of value between a first party using a first client and a second party using a second client via a transfer mechanism, the transfer mechanism comprising: , a decentralized digital currency accessible by each of said device, said first client, and a second client via a computer network, comprising: a. A first memory having a transaction record sector and a first key pair sector storing a first asymmetric key pair, said first asymmetric key pair comprising a first private key and a first public key. a first memory; b. A first network interface for receiving terms for determining a payment amount, said terms comprising: i. at least one of a first principal amount and a second principal amount; ii. a reference to at least one of a first data source and a second data source; said first data source having a first database storing data relating to a first security; and said second data source has a second database storing data relating to a second security; iii. a first network interface including an expiration timestamp; and c. a first computer processor coupled to said first memory and said first network interface, comprising: i. A. payment functions; at least one of said first principal amount and said second principal amount; and B. from at least one of said first data source and said second data source to calculate one or more payment amounts, ii. reading said first private key from said first key pair sector; iii. Compute a first cryptographic signature from the first private key; iv. creating a pending payment transaction record, said pending payment transaction record comprising: A.,B. Commitments received from Commitment Transactions; B. said one or more payment amounts; said first cryptographic signature; v. a first computer processor for issuing said pending payment transaction record to at least one of said first client or said second client, wherein said first client: a. a second memory having a second key pair sector storing a second asymmetric key pair, said second asymmetric key pair having a second private key and a second public key; a memory; b. a second network interface; c. a second computer processor coupled to said second memory and said second network interface, comprising: i. reading said second private key from said second key pair sector; ii. reading the pending payment transaction record; iii. Compute a second cryptographic signature from the second private key; iv. creating a completed payment transaction record, said completed payment transaction record comprising: A. said contracted amount;B. B. the one or more payments; D. said first cryptographic signature; said second cryptographic signature; v. a second computer processor that creates a payment transaction by submitting the completed payment transaction record to the transfer mechanism;

Said second client a. a third
memory having a third key pair sector storing a third asymmetric key pair, said third asymmetric key pair having a third private key and a third public key; a memory; b. a third network interface; c. a third computer processor coupled to said third memory and said third network interface, said third computer processor reading said third private key from said third key pair sector. and said device, said first client, and said second client connect to said computer network via said first network interface, said second network interface, and said third network interface, respectively. coupled, wherein said first computer processor performs said payment function by: i. said first principal amount; and ii. calculating said one or more payment amounts by applying to said value of said first security; said first computer processor further comprising: a. Compute a third cryptographic signature from the first private key; b. creating an uncompleted refund transaction record, said uncompleted refund transaction record comprising: i. said committed amount received from said committed transaction; ii. the refund amount; iii. said third cryptographic signature, and iv. including lock time; c. An apparatus for issuing said pending refund transaction record to at least one of said first client or said second client. [Claim 26]

a. said first key pair sector further stores a fourth asymmetric key pair, said fourth asymmetric key pair having a fourth private key and a fourth public key; b. The first computer processor may further: i. reading said fourth private key from said first key pair sector; ii. Compute a fourth cryptographic signature from the fourth private key; iii. creating a contract transaction record, said contract transaction record comprising: A. B. said first principal amount; B. said contracted amount; said fourth cryptographic signature; iv. 26. The apparatus of claim 25, wherein said execution transaction is created by submitting said execution transaction record to said transfer mechanism. [Claim 27]

The first asymmetric key pair is identical to the fourth asymmetric key pair, the first private key is identical to the fourth private key, and the first public key is identical to the fourth 27. Apparatus according to claim 26, identical to four public keys. [Claim 28]

a. said reference to said first data source or said second data source includes at least one of a reference to a base security and a reference to a quote security; b. 27. The apparatus of Claim 26, wherein said first computer processor further calculates said payment amount after said expiration timestamp.

[Claim 29]

a. said first key pair sector further stores a fourth asymmetric key pair, said fourth asymmetric key pair having a fourth private key and a fourth public key; b. The first computer processor may further: i. reading said fourth private key from said first key pair sector; ii. Compute a fourth cryptographic signature from the fourth private key; iii. creating a contract transaction record, said contract transaction record comprising: A. B. said first principal amount; B. said contracted amount; said fourth cryptographic signature; iv. creating the executed transaction by submitting the executed transaction record to the transfer mechanism, wherein the first asymmetric key pair is the same as the fourth asymmetric key pair, and the first private key is the same as the fourth asymmetric key pair; is identical to four private keys, said first public key being identical to said fourth public key; a. said reference to said first data source or said second data source includes at least one of a reference to a base security and a reference to a quote security; b. 26. The apparatus of claim 25, wherein said first computer processor further calculates said payment amount after said expiration timestamp. [Claim 30]

A system for facilitating value transfer between a first party using a first client and a second party using a second client via a transfer mechanism, the transfer mechanism comprising: , a facilitator, a facilitator, the first client, and a second client respectively via a computer network, wherein the system comprises: the facilitator, the first client, and the second client; a. The facilitator may: i. A first memory having a transaction record sector and a first key pair sector storing a first asymmetric key pair, said first asymmetric key pair comprising a first private key and a first public key. a first memory having a ii. A first network interface for receiving conditions for determining a payment amount, said conditions comprising:A. at least one of a first principal amount and a second principal amount;B. a reference to at least one of a first data source and a second data source; said first data source having a first database storing data relating to a first security; and said second data source has a second database storing data relating to the second security;B. a first network interface including an expiration timestamp; and

,

iii. A first computer processor coupled to said first memory and said first network interface, comprising: A. applying a payment function to at least one of said first principal amount and said second principal amount and to values from at least one of said first data source and said second data source; Calculate one or more payments;B. B. reading said first private key from said first key pair sector; D. calculating a first cryptographic signature from said first private key; creating an unfinished payment transaction record, said unfinished payment transaction record comprising:

I. Commitments Received from Execution
Transactions II. said one or more payment amounts;
and III. E. said first cryptographic signature; a first
computer processor for issuing said pending payment transaction record to at least one of said first client or said second client; b. Said first client: i. a second memory having a second key pair sector storing a second asymmetric key pair, said second asymmetric key pair having a second private key and a second public key; , ii. a second network interface; iii. A second computer processor coupled to said second memory and said second network interface, comprising: A. B. reading said second private key from said second key pair sector; B. reading said pending payment transaction record; D. calculating a second cryptographic signature from said second private key; creating a completed payment transaction record, said completed payment transaction record comprising: I. said contracted amount; II. said one or more payments; III. said first cryptographic signature; and IV. E. said second cryptographic signature; a second computer processor for creating a payment transaction by submitting the completed payment transaction record to the transfer mechanism; c. Said second client: i. a third memory having a third key pair sector storing a third asymmetric key pair, said third asymmetric key pair having a third private key and a third public key; and , ii. a third network interface; iii. a third computer processor coupled to said third memory and said third network interface, said third computer processor reading said third private key from said third key pair sector; wherein said facilitator, said first client and said second client are connected to said computer network via said first network interface, said second network interface and said third network interface respectively; coupled to a work, the first computer processor further comprising: a. Compute a third cryptographic signature from the first private key; b. creating an uncompleted refund transaction record, said uncompleted refund transaction record comprising: i. said committed amount received from said committed transaction; ii. the refund amount, and iii. said third cryptographic signature; c. issuing said pending refund transaction record to at least one of said first client or said second client; a. said first key pair sector further stores a fourth asymmetric key pair, said fourth asymmetric key pair having a fourth private key and a fourth public key; b. The first computer processor may further: i. a. B. said first principal amount; said value of said first security;

calculating said one or more payments by applying to; ii. reading
said fourth private key from said first key pair sector; iii. Compute a fourth cryptographic signature from the fourth private key; iv. creating a contract transaction record, said contract transaction record comprising: A. B. said first principal amount; B. said contracted amount; v. said fourth cryptographic signature; creating said execution transaction by submitting said execution transaction record to said transfer mechanism, said second computer processor: a. Compute a fifth cryptographic signature from the second private key; b. creating a first principal transaction record, said first principal transaction record comprising: i. said first principal amount; and ii. said fifth cryptographic signature; c. creating a first principal transaction by submitting said first principal transaction record to said transfer mechanism.

[Claim 31]
a. said reference to said first data source or said second data source includes at least one of a reference to a base security and a reference to a quote security; b. 31. The system of claim 30, wherein said first computer processor further calculates said payment amount after said expiration timestamp. [Claim 32]

The third computer processor may further: i. compute a
sixth cryptographic signature from the third private key; ii. creating a second principal transaction record, said second principal transaction record comprising: A. said second principal amount; and B. said sixth cryptographic signature; iii. 31. The system of claim 30, wherein submitting the second principal transaction record to the transfer mechanism creates a second principal transaction. [Claim 33]

a. said reference to said first data source or said second data source includes at least one of a reference to a base security and a reference to a quote security; b. said first computer processor further calculates said payment amount after said expiration timestamp; c. The third computer processor may further: i. compute a sixth cryptographic signature from the third private key; ii. creating a second principal transaction record, said second principal transaction record comprising: A. said second principal amount; and B. said sixth cryptographic signature; iii. 31. The system of claim 30, wherein submitting the second principal transaction record to the transfer mechanism creates a second principal transaction. [Claim 34]

A system for facilitating value transfer between a first party using a first client and a second party using a second client via a transfer mechanism, the transfer mechanism comprising: , the facilitator, the first client, and the second client, each accessible via a computer network.

said system comprising said facilitator, said first client, and said second client; a. The facilitator may: i. A first memory having a transaction record sector and a first key pair sector storing a first asymmetric key pair, said first asymmetric key pair comprising a first private key and a first public key. a first memory having a ii. A first network interface for receiving conditions for determining a payment amount, said conditions comprising:A. at least one of a first principal amount and a second principal amount;B. a reference to at least one of a first data source and a second data source; said first data source having a first database storing data relating to a first security; and said second data source has a second database storing data relating to the second security;B. a first network interface including an expiration timestamp; and

,

iii. A first computer processor coupled to said first memory and said first network interface, comprising: A. applying a payment function to at least one of said first principal amount and said second principal amount and to values from at least one of said first data source and said second data source; Calculate one or more payments;B. B. reading said first private key from said first key pair sector; D. calculating a first cryptographic signature from said first private key; creating a pending payment transaction record, said pending payment transaction record comprising: I. Commitments Received from Execution Transactions II. said one or more payment amounts; and III. E. said first cryptographic signature; a first computer processor for issuing said pending payment transaction record to at least one of said first client or said second client; b. Said first client: i. a second memory having a second key pair sector storing a second asymmetric key pair, said second asymmetric key pair having a second private key and a second public key; , ii. a second network interface; iii. A second computer processor coupled to said second memory and said second network interface, comprising: A. B. reading said second private key from said second key pair sector; B. reading said pending payment transaction record; D. calculating a second cryptographic signature from said second private key; creating a completed payment transaction record, said completed payment transaction record comprising: I. said contracted amount; II. said one or more payments; III. said first cryptographic signature; and IV. E. said second cryptographic signature; a second computer processor for creating a payment transaction by submitting the completed payment transaction record to the transfer mechanism; c. The second client is

i. a third memory having a third key pair sector storing a third asymmetric key pair, said third asymmetric key pair having a third private key and a third public key; and , ii. a third network interface; iii. a third computer processor coupled to said third memory and said third network interface, said third computer processor reading said third private key from said third key pair sector; wherein said facilitator, said first client and said second client are connected to said computer network via said first network interface, said second network interface and said third network interface respectively; the facilitator and the first client are the same device; the first computer processor and the second computer processor are the same processor; and the first memory and the second memory are the same memory, the first network interface and the second network interface are the same network interface, and the first computer processor further: a. Compute a third cryptographic signature from the first private key; b. creating an uncompleted refund transaction record, said uncompleted refund transaction record comprising: i. said committed amount received from said committed transaction; ii. the refund amount, and iii. said third cryptographic signature; c. a system for issuing said uncompleted refund transaction record to at least one of said first client and said second client;

[Claim 35]

a. said reference to said first data source or said second data source includes at least one of a reference to a base security and a reference to a quote security; b. said first computer processor further calculates said payment amount after said expiration timestamp; c. The second computer processor further comprises: i. compute a fourth cryptographic signature from the second private key; ii. creating a first principal transaction record, said first principal transaction record comprising: A. B. said first principal amount; said fourth cryptographic signature; iii. creating a first principal transaction by submitting said first principal transaction record to said transfer mechanism; d. The third computer processor may further: i. compute a fifth cryptographic signature from the third private key; ii. creating a second principal transaction record, said second principal transaction record comprising: A. said second principal amount; and B. said fifth cryptographic signature; iii. 35. The system of claim 34, wherein submitting the second principal transaction record to the transfer mechanism creates a second principal transaction. [Claim 36]

A system for facilitating value transfer between a first party using a first client and a second party using a second client via a transfer mechanism, the transfer mechanism comprising: , the facilitator, the first client, and the second client

a decentralized digital currency accessible via a computer network, said system comprising said facilitator, said first client, and said second client; a. The facilitator may: i. A first memory having a transaction record sector and a first key pair sector storing a first asymmetric key pair, said first asymmetric key pair comprising a first private key and a first public key. a first memory having a ii. A first network interface for receiving conditions for determining a payment amount, said conditions comprising:A. at least one of a first principal amount and a second principal amount;B. a reference to at least one of a first data source and a second data source; said first data source having a first database storing data relating to a first security; and said second data source has a second database storing data relating to the second security;B. a first network interface including an expiration timestamp; and

,

iii. A first computer processor coupled to said first memory and said first network interface, comprising: A. applying a payment function to at least one of said first principal amount and said second principal amount and to values from at least one of said first data source and said second data source; Calculate one or more payments;B. B. reading said first private key from said first key pair sector; D. calculating a first cryptographic signature from said first private key; creating a pending payment transaction record, said pending payment transaction record comprising: I. Commitments Received from Execution Transactions II. said one or more payment amounts; and III. E. said first cryptographic signature; a first computer processor for issuing said pending payment transaction record to at least one of said first client or said second client; b. Said first client: i. a second memory having a second key pair sector storing a second asymmetric key pair, said second asymmetric key pair having a second private key and a second public key; , ii. a second network interface; iii. A second computer processor coupled to said second memory and said second network interface, comprising: A. B. reading said second private key from said second key pair sector; B. reading said pending payment transaction record; D. calculating a second cryptographic signature from said second private key; creating a completed payment transaction record, said completed payment transaction record comprising: I. said contracted amount; II. said one or more payments; III. said first cryptographic signature; and IV. E. said second cryptographic signature; a second computer processor that creates a payment transaction by submitting the completed payment transaction record to the transfer mechanism;

c. Said second client: i. a third memory
having a third key pair sector storing a third asymmetric key pair, said third asymmetric key pair having a third private key and a third public key; and , ii. a third network interface; iii. a third computer processor coupled to said third memory and said third network interface, said third computer processor reading said third private key from said third key pair sector; wherein said facilitator, said first client and said second client are connected to said computer network via said first network interface, said second network interface and said third network interface respectively; the facilitator and the first client are the same device; the first computer processor and the second computer processor are the same processor; and the first memory and said second memory are the same memory, and said first network interface and said second network interface are the same network interface, a. said first key pair sector further stores a fourth asymmetric key pair, said fourth asymmetric key pair having a fourth private key and a fourth public key; b. The first computer processor may further: i. a. B. said first principal amount; calculating said one or more payments by applying to said value of said first security; ii. reading said fourth private key from said first key pair sector; iii. Compute a third cryptographic signature from the fourth private key; iv. creating a contract transaction record, said contract transaction record comprising: A. B. said first principal amount; B. said contracted amount; v. said third cryptographic signature; creating said execution transaction by submitting said execution transaction record to said transfer mechanism, said second computer processor: a. Compute a fourth cryptographic signature from the second private key; b. creating a first principal transaction record, said first principal transaction record comprising: i. said first principal amount; and ii. said fourth cryptographic signature; c. creating a first principal transaction by submitting said first principal transaction record to said transfer mechanism; a. said reference to said first data source or said second data source includes at least one of a reference to a base security and a reference to a quote security; b. The first computer processor further calculates the payment amount after the expiration timestamp; a. The third computer processor may further: i. compute a fifth cryptographic signature from the third private key; ii. creating a second principal transaction record, said second principal transaction record comprising: A. said second principal amount; and B. said fifth cryptographic signature; iii. a second principal transaction record by submitting said second principal transaction record to said transfer mechanism;

A system that creates a
principal transaction.

[Claim 37]

A method performed by a system that facilitates value transfer between a first party using a first client and a second party using a second client via a transfer mechanism, comprising: wherein the transfer mechanism includes a decentralized digital currency accessible via a computer network by a facilitator, the first client, and a second client, respectively, wherein the first client is a first storing an asymmetric key pair in a first key pair sector of a first memory, said first asymmetric key pair having a first public key and a first private key; storing a second asymmetric key pair in a second key pair sector of a second memory, said second asymmetric key pair having a second public key and a second private key; and said facilitator storing a third asymmetric key pair in said second key pair sector, said third asymmetric key pair having a third public key and a third private key; , said first client storing a fourth asymmetric key pair in a third key pair sector of a third memory, said fourth asymmetric key pair comprising a fourth public key and a fourth private key; a key; and said first client sending, via a network interface, conditions for determining a payment amount, said conditions: i. at least one of a first principal amount and a second principal amount; ii. a reference to at least one of a first data source and a second data source; said first data source having a first database storing data relating to securities; having a second database storing data relating to two securities; iii. an expiration timestamp; said facilitator receiving said terms and conditions via a second network interface; and said facilitator activating a payment function to: i. at least one of said first principal amount and said second principal amount; and ii. from the first data source and/or the second data source; reading said first private key from a sector; said facilitator calculating a first cryptographic signature from said first private key; and said first client performing a first principal transaction. creating a record, said first principal transaction record comprising: i. said first principal amount; and ii. said first client creating a first principal transaction by submitting said first principal transaction record to said transfer mechanism; a facilitator reading said second private key from said second key pair sector; said facilitator computing a second cryptographic signature from said second private key; creating a record, wherein the execution transaction record is

,

i. said first principal amount; ii. a
commitment amount, and iii. said second
cryptographic signature; said facilitator creating a filled transaction by submitting
said filled transaction record to said transfer mechanism; deriving the value of a security; said facilitator reading said third private key from said second key pair sector; and said facilitator computing a third cryptographic signature from said second private key. and said facilitator creating a pending payment transaction record, said pending payment transaction record comprising: i. said committed amount received from said committed transaction; ii. said one or more payment amounts; and iii. said third cryptographic signature; said facilitator issuing said pending payment transaction record to at least one of said first client and said second client; the first client reading the pending payment transaction record; the first client reading the fourth private key from the third key pair sector; the first client reading the third calculating a fourth cryptographic signature from four private keys; and creating a completed payment transaction record by said first client, said completed payment transaction record comprising: i. said contracted amount; ii. said one or more payment amounts; iii. said third cryptographic signature, and iv. the fourth cryptographic signature; the first client creating a payment transaction by submitting the completed payment transaction record to the transfer mechanism; computing a fifth cryptographic signature from three private keys; and said facilitator creating a pending refund transaction record, said pending refund transaction record comprising: i. said committed amount received from said committed transaction; ii. the refund amount; iii. said fifth cryptographic signature, and iv. lock time; said facilitator issuing said pending refund transaction record; a. the second asymmetric key pair and the third asymmetric key pair are the same key pair, the second private key and the third private key are the same key, and the second public key and said third public key is the same key; b. the first asymmetric key pair and the fourth asymmetric key pair are the same key pair, the first private key and the fourth private key are the same key, and the first public key and the fourth public key is the same key; c. wherein the first memory and the third memory are the same memory, and the first key pair sector and the third key pair sector are the same sector. [Claim 38]

said second client storing a fifth asymmetric key pair in a fourth key pair sector of a fourth memory, said fifth asymmetric key pair comprising a fifth private key and a fifth public said second client reading said fifth private key from said fourth key pair sector; said second client reading said fifth private key from said fifth private key; computing a cryptographic signature; and said second client creating a second principal transaction record, said second principal transaction record comprising: i. said second principal amount; and ii. said second client creating a second principal transaction by submitting said second principal transaction record to said transfer mechanism; said The facilitator activates the payment function by: i. said value of said security; andA. said first principal amount; or B. 38. The method of claim 37, further comprising calculating one or more payment amounts by applying to at least one of said second principal amount. [Claim 39]

A method performed by a system that facilitates value transfer between a first party using a first client and a second party using a second client via a transfer mechanism, comprising: wherein the transfer mechanism includes a decentralized digital currency accessible via a computer network by a facilitator, the first client, and a second client, respectively, wherein the first client is a first storing an asymmetric key pair in a first key pair sector of a first memory, said first asymmetric key pair having a first public key and a first private key; storing a second asymmetric key pair in a second key pair sector of a second memory, said second asymmetric key pair having a second public key and a second private key; and said facilitator storing a third asymmetric key pair in said second key pair sector, said third asymmetric key pair having a third public key and a third private key; , said first client storing a fourth asymmetric key pair in a third key pair sector of a third memory, said fourth asymmetric key pair comprising a fourth public key and a fourth private key; a key; and said first client sending, via a network interface, conditions for determining a payment amount, said conditions: i. at least one of a first principal amount and a second principal amount; ii. a reference to at least one of a first data source and a second data source; said first data source having a first database storing data relating to securities; having a second database storing data relating to two securities; iii. an expiration timestamp; said facilitator receiving said terms and conditions via a second network interface; and said facilitator activating a payment function to: i. at least one of said first principal amount and said second principal amount; and

ii. from the first data source and/or the second data source; reading said first private key from a sector; said facilitator calculating a first cryptographic signature from said first private key; and said first client performing a first principal transaction. creating a record, said first principal transaction record comprising: i. said first principal amount; and ii. said first client creating a first principal transaction by submitting said first principal transaction record to said transfer mechanism; a facilitator reading said second private key from said second key pair sector; said facilitator computing a second cryptographic signature from said second private key; creating a record, said execution transaction record comprising: i. said first principal amount; ii. a commitment amount, and iii. said second cryptographic signature; said facilitator creating a filled transaction by submitting said filled transaction record to said transfer mechanism; deriving the value of a security; said facilitator reading said third private key from said second key pair sector; and said facilitator computing a third cryptographic signature from said second private key. and said facilitator creating a pending payment transaction record, said pending payment transaction record comprising: i. said committed amount received from said committed transaction; ii. said one or more payment amounts; and iii. said third cryptographic signature; said facilitator issuing said pending payment transaction record to at least one of said first client and said second client; the first client reading the pending payment transaction record; the first client reading the fourth private key from the third key pair sector; the first client reading the third calculating a fourth cryptographic signature from four private keys; and creating a completed payment transaction record by said first client, said completed payment transaction record comprising: i. said contracted amount; ii. said one or more payment amounts; iii. said third cryptographic signature, and iv. the fourth cryptographic signature; the first client creating a payment transaction by submitting the completed payment transaction record to the transfer mechanism; and the second client: , store the fifth asymmetric key pair in the fourth memory

,

wherein said fifth asymmetric key pair has a fifth private key and a fifth public key; and said second client is able to access said reading a fifth private key; said second client computing a fifth cryptographic signature from said fifth private key; and said second client performing a second principal transaction creating a record, said second principal transaction record comprising: i. said second principal amount; and ii. said second client creating a second principal transaction by submitting said second principal transaction record to said transfer mechanism; said The facilitator activates the payment function by: i. said value of said security; andA. said first principal amount; or B. calculating one or more payment amounts by applying to at least one of said second principal amount; and said facilitator calculating a sixth cryptographic signature from said third private key. and said facilitator creating an uncompleted refund transaction record, said uncompleted refund transaction record comprising: i. said committed amount received from said committed transaction; ii. one or more refund amounts; iii. said sixth cryptographic signature, and iv. lock time; and said facilitator issuing said pending refund transaction record; a. said second asymmetric key pair and said third asymmetric key pair are the same asymmetric key pair, said second private key and said third private key are the same private key, and said second public key and said third public key are the same public key; b. the first asymmetric key pair and the fourth asymmetric key pair are the same key pair, the first private key and the fourth private key are the same private key, and the first public key and said fourth public key are the same public key, c. said fifth asymmetric key pair and said fourth asymmetric key pair are the same asymmetric key pair, said fifth private key and said fourth private key are the same private key, and said fifth public key and said fourth public key are the same public key; d. said first memory and said third memory are the same memory, and said first key pair sector and said third key pair sector are the same key pair sector; e. wherein the fourth memory and the third memory are the same memory, and the fourth key pair sector and the third key pair sector are the same key pair sector. [Claim 40]

A method performed by a system that facilitates value transfer between a first party using a first client and a second party using a second client via a transfer mechanism, comprising: the transport mechanism is accessed by a facilitator, the first client, and a second client, respectively, over a computer network;

capable of decentralized digital currency, wherein said first client stores a
first asymmetric key pair in a first key pair sector of a first memory, said first asymmetric a key pair having a first public key and a first private key; and said facilitator storing a second asymmetric key pair in a second key pair sector of a second memory; two asymmetric key pairs having a second public key and a second private key; and said facilitator storing a third asymmetric key pair in said second key pair sector, said a third asymmetric key pair having a third public key and a third private key; and said first client storing a fourth asymmetric key pair in a third key pair sector of a third memory. said fourth asymmetric key pair having a fourth public key and a fourth private key; and said first client determining a payment amount via a network interface. sending a condition, said condition comprising: i. at least one of a first principal amount and a second principal amount; ii. a reference to at least one of a first data source and a second data source; said first data source having a first database storing data relating to securities; having a second database storing data relating to two securities; iii. an expiration timestamp; said facilitator receiving said terms and conditions via a second network interface; and said facilitator activating a payment function to: i. at least one of said first principal amount and said second principal amount; and ii. from the first data source and/or the second data source; reading said first private key from a sector; said facilitator calculating a first cryptographic signature from said first private key; and said first client performing a first principal transaction. creating a record, said first principal transaction record comprising: i. said first principal amount; and ii. said first cryptographic signature; k. said first client creating a first principal transaction by submitting said first principal transaction record to said transfer mechanism; the facilitator calculating a second cryptographic signature from the second private key; and the facilitator creating a trade record, wherein the trade record is i. said first principal amount; ii. a commitment amount, and iii. said second cryptographic signature; said facilitator creating a filled transaction by submitting said filled transaction record to said transfer mechanism; The step of extracting the value of a security

,

When ,

the facilitator reading the third private key from the second key pair sector; the facilitator computing a third cryptographic signature from the second private key; creating a completed payment transaction record, said incomplete payment transaction record comprising: i. said committed amount received from said committed transaction; ii. said one or more payment amounts; and iii. said third cryptographic signature; said facilitator issuing said pending payment transaction record to at least one of said first client and said second client; the first client reading the pending payment transaction record; the first client reading the fourth private key from the third key pair sector; the first client reading the third calculating a fourth cryptographic signature from four private keys; and creating a completed payment transaction record by said first client, said completed payment transaction record comprising: i. said contracted amount; ii. said one or more payment amounts; iii. said third cryptographic signature, and iv. the fourth cryptographic signature; the first client creating a payment transaction by submitting the completed payment transaction record to the transfer mechanism; computing a fifth cryptographic signature from three private keys; and said facilitator creating a pending refund transaction record, said pending refund transaction record comprising: i. said committed amount received from said committed transaction; ii. the refund amount; iii. said fifth cryptographic signature, and iv. said facilitator issuing said pending refund transaction record; and said second client placing a fifth asymmetric key pair in a fourth key pair sector of a fourth memory. said fifth asymmetric key pair having a fifth private key and a fifth public key; said second client calculating a sixth cryptographic signature from said fifth private key; and said second client reading a second principal transaction record creating, said second principal transaction record comprising: i. said second principal amount; and ii. said second client creating a second principal transaction by submitting said second principal transaction record to said transfer mechanism; said The facilitator activates the payment function by: i. said value of said security; andA. said first principal amount; or B. at least one of said second principal amount;

calculating one or more payment amounts by applying a. said second asymmetric key pair and said third asymmetric key pair are the same asymmetric key pair, said second private key and said third private key are the same private key, and said second public key and said third public key are the same public key; b. the first asymmetric key pair and the fourth asymmetric key pair are the same key pair, the first private key and the fourth private key are the same private key, and the first public key and said fourth public key are the same public key, c. said fifth asymmetric key pair and said fourth asymmetric key pair are the same asymmetric key pair, said fifth private key and said fourth private key are the same private key, and said fifth public key and said fourth public key are the same public key,

d. said first memory and said third memory are the same memory, and said first key pair sector and said third key pair sector are the same key pair sector; e. The method, wherein the fourth memory and the third memory are the same memory, and the fourth key pair sector and the third key pair sector are the same key pair sector.
Description: TECHNICAL FIELD [0001]

Relevant fields are telecommunications, digital communications and computer technology.
[0002]
PRIORITY
CLAIM This application claims priority to US Provisional Application No. 61/990,795, filed May 9, 2014. This application is hereby incorporated by reference for the disclosure of all applications referred to in this paragraph as if fully set forth herein.
COPYRIGHT
STATEMENT
BACKGROUND
ART [0004]
Market efficiency tends to increase, thereby reducing transaction costs in proportion to the mutual trust of the parties. However, interest rates tend to exceed market interest rates in proportion to the expansion of the market size, and therefore reliability tends to decline. Efficient and productive participation in a larger market [1] will need to mitigate this reliability issue, but it also comes at a cost. This cost is often reduced by economies of scale, but even today buffering against risks from counterparties, intermediaries, post-delivery payment failures, guarantor failures, escrows, etc. is quite costly. . [0005]

Since the mid-1990s, there has been an explosion of commercial activity, with transactions agreed, sometimes across national borders, using the Internet as the primary medium of communication between parties who, until then, did not know each other. Establishing and maintaining trust between parties played an important role, and various solutions were tried through traditional and inefficient methods. [0006]

Some of the markets that these individuals interact with include financial instruments (stocks, bonds, options, futures,

swaps, uncovered transit balances, etc.). The advent of financial engineering has enabled individuals and businesses to take advantage of computations in financial transactions, such as automating entry into and exit from transactions through programmed conditions and algorithms. But even as the use of technology in this area explodes, such technology is overwhelmingly stacked within traditional centralized markets. Almost all charge relatively high costs to trade. Some of the larger exchanges tout their “high value” (i.e. high paying) customers as being prioritized over less sophisticated or less skilled investors. . Some question the fairness of such practices. [0007]

Moreover, the cost of enforcing contracts in international trade can be prohibitive, and success can be very difficult to predict. Moreover, the seller may wish to receive one currency, while the buyer may wish to send another. The value of currencies denominated in other currencies may be volatile. Until now, third-party intervention has often been a way for parties to mitigate risk in remote transactions. One such mechanism is a letter of credit (L/C). Letters of credit are useful when the seller does not necessarily trust the buyer with the large order, but the bank with which the buyer has placed the line of credit can be trusted. The buyer and bank agree to release funds from the credit facility when the seller meets certain conditions. The bank issues a promise (letter of credit) to the seller (often contingent on sending proof of shipment to the bank before a certain date and time), and the seller and buyer agree to the rest of the terms. However, payments are often made on a later date than agreed and exchange rates may fluctuate between the date agreed and payment. Only the largest institutions have the resources to adequately manage such exchange rate volatility. In addition, the amounts charged by banks for letters of credit and exchanges are substantial. Conversely, intermediaries are required to have a high degree of credibility to effectively act as self-interest document examiners who can independently verify the veracity of such documents before releasing funds; This can leave sellers with a lot of risk of error, counterfeiting or fraud. Letters of credit are therefore not well suited for transactions or consumer transactions where relative currency values can fluctuate significantly. [0008]

It promises a tightly controlled production of assets, requires little third-party intervention when strictly defined criteria are met, and has very low transfer costs compared to previous mechanisms. Decentralized digital currencies (so-called cryptocurrencies) with the ability to transfer control or ownership of assets are relatively new creatures. Bitcoin and its derivatives (Ethereum, Litecoin, etc.) are one such technology that has seen a recent surge in popularity (and reputation). [0009]

For the purpose of illustrating it as a non-limiting example, these particular decentralized digital currencies generally contain a “ledger” of all transactions that are “verified” by the participants of the network (referred to as a “blockchain”). It functions by maintaining a history of some or all of Transactions work roughly as follows [2], with a few exceptions that are beyond the scope of this invention. A transaction consists of at least one input, an output, and an input consists of an input "script" that can be performed by systematically well-defined executable operations. The output is also constructed by a second output script containing such operations. New (child) transactions are made by combining output and input scripts from existing (parent) transactions in a predictable way. A new transaction is considered valid and produces the expected result if the majority of network participants agree that the combination is acceptable given the given rules. A trade output is considered “spent” when it is associated with a valid child transaction by the majority of network participants, and is considered not associated with a valid child transaction by the majority of network participants. are considered "unused". The notion of “ownership” or “right” of the output of a transaction depends on which entity controls said output, or more specifically, who creates new transactions or has access to the majority of network participants.

It is defined by having the output "used" in a way that is recognized as effective.
[0010]
More specifically, an entity seeking to submit a new transaction to the ledger broadcasts (or "broadcasts") a transaction record containing details of the desired transaction to a number of network participants (called "peers") with whom it knows. I do. Each of these peers attempts to verify the transaction record, and if successful, further forwards the transaction record to their peers, and so on. Ultimately, the transaction record contains the transaction so that it reaches the participant configured to execute the transaction. [0011]

A transaction occurs when an entity produces a child transaction that is accepted as valid by the majority and whose inputs are associated with unused outputs from the parent transaction. In most cases, this is a simple transfer of control to a second entity and the new transaction's output script creates a corresponding input script for a single entity possessing a particular asymmetric grid key pair. is a small set of operations that are computationally trivial for one entity and computationally impractical for all others. In other words, it is addressed to an entity that has access to a particular private key. Existing software abstracts these addresses and simple transactions for ordinary people who are not programmers or protocol experts. [0012]

However, the scripts described as the conditions under which a transaction will be accepted as valid are taken into account by the set of available operations. Since the common way of describing these operations is usually binary or programming code [3], it is not possible for ordinary people to create or understand arbitrary transactions. For example, as of April 21, 2014, the Bitcoin Contracts Wild page consists of several theoretical brief explanations (Non-Patent Document 4). Regardless of their role in the trade, it is difficult for the common man to even comprehend these instructions. There is a lack of basic steps and combinations of such trades to conduct similar trades with confidence. Despite its great potential, this kind of unabstracted complexity prevents the Bitcoin protocol and its derivatives from becoming as pervasive as previous “easy” payment methods.

Decentralized
digital currency or “virtual currency”
[0014]
The design and functionality of the Bitcoin protocol and its derivatives can be explained as follows (Non-Patent Document 5). Although this section refers to Bitcoin by name, this description holds true for nearly all decentralized digital currencies currently known in the art. [0015]

Blockchain: A “blockchain” is a public ledger that records Bitcoin transactions. The new solution allows block maintenance to be achieved without central authority intervention. Chaining is performed by a communication network via communication nodes running Bitcoin software. Transactions of the type “payer X sends bitcoins to payee Z” are broadcast to this network using readily available software applications. Network nodes can validate transactions, add them to their copy of the ledger, and broadcast these ledger additions to other nodes. Each network node stores its own copy of the blockchain to independently verify ownership of any bitcoin amount. Approximately 6 times per hour, a new group (block) of accepted transactions is created and published to all nodes immediately after being added to the blockchain. This allows Bitcoin software to determine when a particular Bitcoin was spent. This is necessary to prevent double spending in environments without a central authority. Traditional ledgers record the transfer of promissory notes that exist separately from the actual invoice or

Blockchain, on the other hand, is the only place Bitcoin can be said to exist in the form of unspent transaction output. [0016]

Unit: Bitcoin's unit of account is bitcoin (). Small multiples of Bitcoin that are used as alternative units are MilliBitcoin (mBTC), MicroBitcoin (ÿBT) and Satoshi. Named after Bitcoin's creator, "Satoshi" is the smallest multiple of Bitcoin, representing 0.00000001, or one hundred millionth of Bitcoin. A millibitcoin represents 0.001 bitcoin, or one thousandth of a bitcoin, and a microbitcoin represents 0.000001 bitcoin, or one millionth of a bitcoin. Micro Bitcoins are also called “bits”.

[0017]

Ownership: See Figure 24 Bitcoin ownership means that a user can use Bitcoin in association with a specific address. This requires the payer to digitally sign the transaction using a personal key. Without knowledge of the private key, transactions cannot be signed and Bitcoin cannot be used. The network uses the public key to verify the signature. If you lose your personal key, the Bitcoin network will not recognize any other proof of ownership. The coin is therefore unusable and is effectively lost. In 2013, one user said he lost 7,500 bitcoins (valued at $7.5 million) when he threw away the hard drive that held his personal keys. [0018]

Transactions: Transactions typically require one or more inputs. ("Coinbase" is a special transaction to create bitcoins with 0 inputs. See "Mining" and "Supply" below). must be an "unused" output of And all inputs require a digital signature. Multiple entries imply the use of multiple coins in a cash transaction. Transactions can also have multiple outputs and can batch multiple payments at once. The output of a trade can be specified as any multiple of "Satoshi". As with cash transactions, the input total (coins for payment) can be greater than or equal to the total payment amount. In such cases, the additional output returns change to the payer. Any satoshi input that is not included in the transaction output becomes the transaction fee.

[0019]

All transaction records are accompanied by a "lock time". This prevents the transaction from being accepted as valid, making it pending or redeemable until some agreed future point. In Bitcoin and similar protocols it can be specified as a block index or timestamp. Transaction records will not be accepted into the blockchain until the lock time is reached. Other more flexible mechanisms have also been proposed [6].

[0020]

Mining: “Mining” is a record keeping service. Miners keep the blockchain constant, complete, and immutable by repeatedly validating the blockchain, collecting newly announced transactions into new transaction groups called “blocks”. A new block contains information that "connects" to the previous block. The information (hence the name) is a cryptographic hash of the previous block using the SHA-256 hash tag algorithm.

.

The new block must contain a so-called "proof of work". The Proof of Work contains numbers called "Difficulty Targets" and the technical term "nonce", numbers used only once. Miners must find a “nonce” that generates a hash of a new block smaller than indicated in the difficulty goal. Network nodes can easily verify proofs when new blocks are created and distributed to the network. On the other hand, finding proofs is a considerable task, since there is only one way to find the "nonce" needed for a secure cryptographic hash. That

The method is to try 1, 2, 3, different integers one by one until the desired output is obtained. The fact that the hash of a new block is less than the difficulty target is why proving that this heavy lifting is actually being done is called "proof of work." [0022]

Block chaining and proof-of-work systems make it extremely difficult to change a blockchain, as an attacker would have to modify all subsequent blocks for one block to be accepted. New blocks are being mined all the time, so the number of subsequent blocks (also called confirmation of a given block) increases over time, and the difficulty of changing blocks increases.

[0023]
Supply: Miners who successfully find new blocks are rewarded with newly created bitcoins and transaction fees. As of November 28, 2012, the reward was 25 newly minted Bitcoins for each block added to the blockchain. A special transaction called “Coinbase” is included in the processed payment to get rewarded. Every bitcoin in circulation can be traced back to its coinbase transaction. The Bitcoin protocol specifies that the reward for adding blocks halves approximately every four years. Ultimately, the discretionary limit, when 21 million Bitcoins are in circulation around 2140, the reward itself will be abolished, and recordkeeping will be rewarded only with transaction fees.
.

[0024] [Non-
Patent Document
1] Electronic
Trading, Rose, David C.; Moral Foundations in Economic Behavior, New York Oxford UP, 2011 Print, 'online' escrow and dispute resolution using expensive third parties, various reputation systems, third party guarantors, etc. [Non-Patent Document 2] This is an oversimplified description of the Bitcoin protocol. detailed

Information is available on the Bitcoin Wiki <https://en. bitcoin. See it/>. More information about the Ethereum protocol can be found on the Ethereum Wiki <https://github. com/etliereum/wiki/wiki>. Ledger records (i.e. valid “blocks” see detailed description below)

[Non-Patent Document 3] "Method for Creating Bitcoin Multi-Signature 2-of-3 Transactions" See StackExchange March 23, 2014 Web April 2014. https://bitcoin. stackexchangexom/questions/ 37i2/how-can-i-create-a-multi-signature-2-of-3-transaction) [Non-Patent Document 4] Hahn, Mike “Contract” Bitcoin Bitcoin Community April 2014 Mon 9th Web April 2014 <https://bitcoin. stack exchange exom/questions/37i2/how-can-i-create-a-multi-signature-2-of-3-transaction>.

[Non-Patent Document 5] <https://en. wikipedia. org/wiki/Bitcoin> and <https://en. bitcoin. Quote from it/wiki/Contracts>.) [Non-Patent Document 6] Example "BIP-65: Revisiting i LockTime" Qntra. net, November 13, 2014. Web May 4, 2015 <http: //qntra. net/2014/11/bip-65-revisiti11g-n

iocktime/>.

[Outline of the invention]

[0025]
The present invention relates to negotiating and enforcing agreements, at any distance, subject to the input of third parties, without special technical knowledge of the underlying transport mechanisms. intervene, represent transferors and transferees, replace periods, modify, improve, etc. Such transfers can be ensured without the expensive third-party intermediaries previously required and without the counterparty risk previously associated with them. [0026]

In this application, we consider two forms of value transfer: arbitrary swaps and letters of credit. Any swap or letter of credit is useful as an illustration because the two are quite different. However, the present invention has remarkably similar expressions and force. Parties will understand that this invention can be applied to many other value transfers.
[0027]
In one example, A believes that if Bitcoin were valued in New Zealand dollars, it would appreciate significantly in the coming weeks. And B thinks the opposite, that if Bitcoin is valued in New Zealand dollars, it will fall in value in the coming weeks. Neither of them know each other, but they want to make a small bet in line with their beliefs. One embodiment of the present invention allows both parties to find each other, negotiate to determine specific terms, and enforce this agreement without the expensive methods of the past.
.
[0028]
In another example, A is a merchant who wants to be able to pay for services in Bitcoin, but also wants to be paid in US dollars rather than the volatile bitcoin. She doesn't care if bitcoin goes up or down against the US dollar. On a regular basis (either once a day or on each transaction) you can sell your exposure in USD valued Bitcoin in proportion to the Bitcoin you receive from your customers. In other words, it converts Bitcoin exposure into US dollars. B wants bitcoin but has more US dollars and wants more exposure to bitcoin valued in US dollars. One embodiment of the present invention allows B to discover A, exchange or swap exposure with A, and even if the value of Bitcoin falls against the US dollar, the value of Bitcoin will change to the US dollar. On the other hand, it is also possible for A to receive payment for goods and services in bitcoins, provided that B will receive the amount of the increase when the price rises. Other embodiments automatically seek out these swaps whenever A is sensed to have received additional bitcoins. [0029]

Combinations are possible. For example, A accepts the Australian dollar (AUD) but prefers the US dollar and wants to hedge against the volatility of the Australian dollar against the US dollar. In one embodiment of the present invention, if A exchanges its US dollar exposure with B in bitcoin and exchanges its bitcoin exposure with C in Australian dollars over a similar period, then the Australian dollar risk hedge is in US dollars. Can be synthesized. B and C need not be different entities, and A (which could be the same person) need not make two different transactions. Further, various embodiments of the present invention allow parties to conduct such transactions without maintaining foreign currency deposits or purchasing or exchanging currency.
[0030]
In yet another example, if A wishes to purchase goods from B who are not familiar with each other, B wants assurance of the availability of funds from A, but A expects B to show proof of shipment (and other prescribed may not want to release those funds to B (or the transferor) until the
[0031]
In one embodiment involving a swap, the first device and the second client, called "clients," are either the first client, the first client, or the intermediary.

Any two parties may collude to combine the assets of the first party (e.g., unutilized trading output) with the assets of the It may also participate in a series of transactions in which the assets of the two parties remain committed until they are released.

[0032]
In other embodiments related to letters of credit, the first and second clients are the first client and the intermediary the first client based on observations of external conditions, such as verifying the shipper or delivery to an address. It may also participate in a series of transactions that remain committed until the asset is released. [0033]

In a further embodiment, the asset may be refunded with an expiration timestamp if no such observations are made. [0034]

In another embodiment, the commitment of assets may be deferred until a favorable settlement is reached by an arbitrator. BRIEF DESCRIPTION OF THE FIGURES [0035] FIG. 1 illustrates a system in which different participants, such as clients (120, 160, 170), transport mechanisms (110, 150), facilitators (100), and data sources (130) An exemplary embodiment of the present invention that uses and includes a transfer mechanism such as a distributed digital currency (150) linked by a computer network (140).

FIG. 2 illustrates aspects of one embodiment relating to swaps that include one or more source and commit trades; FIG. 3 illustrates aspects of one embodiment relating to swaps, including commit transactions, refund transactions;
are doing.
4-5 relate to a relatively simple swap involving principal and collateral; FIG.
showing the side of FIG. 5
Same as above. [Figure
6] Figures 6 and 7 show that if one of the parties wants to withdraw before the termination but has not been able to guarantee the other party's agreement, it still finds a third party willing to take the place of the party that wants to withdraw.
Figure 10 shows a transaction chain from multiple example swap embodiments for multiple digits;
FIG. 7 Same as
above. FIG. 8 illustrates aspects of one embodiment relating to a letter of credit including a source transaction, a commit transaction;
are doing.
FIG. 9 illustrates aspects of one embodiment relating to letters of credit including commit transactions, expiry transactions;
showing.
10 and 11 illustrate an implementation involving a relatively simple letter of credit containing principal and collateral;
It shows the aspect of form.
FIG. 11 Same as above.
FIGS. 12-14 illustrate multiple embodiments relating to letters of credit involving replacement of parties;
Fig. 3 shows a trading chain from an example;
FIG. 13 Same as above. FIG. 14 Same as
above. Figures 15 and 16 illustrate aspects
of an embodiment where parties to a value transfer have set up an intermediary for disputes. FIG. 16 Same as above. Figures 17-22 illustrate the major stages of value transfer within one embodiment. FIG. 18 Same as above. FIG. 19 Same as above. FIG. 20 Same as above.

FIG. 21 Same as
above. FIG. 22
Same as above. FIG. 23 shows an example including a client (120) or facilitator (100)
Fig. 3 shows the components of a typical embodiment;
Figure 24 (prior art) shows a simplified chain of ownership in a decentralized digital currency; MODES FOR CARRYING OUT THE INVENTION

The present invention is not limited to the following embodiments. The following description is by way of illustration and not by way of limitation. Other systems, methods, features and advantages will become apparent to one with skill in the art upon examination of the drawings and detailed description. It is intended that all such additional systems, methods, features, and advantages be within the scope of the present inventive subject matter, be included within this description, and be protected by the accompanying claims. [0037]

For example, the Bitcoin protocol is often used in this application by way of example, but the invention is not specifically limited to the Bitcoin protocol. Techniques that make it difficult enough to recharacterize ownership of assets (virtual or otherwise) can be substituted, unless certain strictly defined criteria are met. The invention is not limited to distributed or centralized transport mechanisms. For example, in one embodiment, it can be recognized (i.e., facilitated) by authority (centralized), while in another embodiment, election
(decentralized) can be verified by, etc. [0038]

Additionally, while technologies similar to the Bitcoin protocol explicitly distinguish between "inputs" and "outputs" in transactions, the present invention is not limited to such transfer mechanisms. Various embodiments of the present invention can be implemented in any context in which asset ownership can be reclassified, provided that the transfer mechanism exposes the necessary functionality. This application uses the terms "input" and "output" literally (such as for Bitcoin and its derivative technologies) and figuratively (such as other technologies such as double-entry bookkeeping, chain of title, etc.). In a more traditional model, for example, "input" meant some or all of the available "balance" of an account under the control of an entity. (such as traditional banks) and 'output' includes, for example, references to accounts of other entities (account numbers, etc.), and in such models reclassification of assets satisfies certain conditions. Gradually, the first entity's account is debited and the second entity's account balance is increased (as little as possible) in the second entity's account. This is but one example of an alternate transfer mechanism with which the present invention may be implemented.
[0039]
Further, this application may use terms such as "display," "user input," "display device," "user input device," etc. to disclose or imply subject matter of the present invention. However, the present invention is not limited to being practiced by persons having general sensory abilities, and a "display (device)" clearly presents information to humans through either the senses or a combination of senses. It is intended to include any device capable of communicating. For example, blind people can use devices with 'audio displays', including text-to-speech synthesizers, and Braille terminals. Similarly, user input (device) is intended to include any device capable of receiving information from a human being. Popular user input devices, called ModernSy, include not only keyboards, mice, touch screens, etc., but also speech synthesizers, breath-operated devices, click-and-type devices, movement or gesture recognizers. These are just a few examples. A variety of such displays and user input devices are known in the art and can of course be used in practicing the present invention.

.
[0040]
In the embodiment shown in FIG. 1, the present invention is implemented by the illustrated participants on a computer network.

Including part or all. The participants are typically a first client (A) acting on behalf of a first party (not shown) connected to the computer network, a second party permanently or intermittently connected to the computer network. (not shown), includes a transport mechanism accessible via a computer network, a facilitator accessible to the computer network, and optionally one or more data sources accessible by the facilitator. In typical embodiments, computer networks include the Internet and related technologies, but this is not a requirement. Other configurations are also possible. For example, a computer network can include multiple independent computer networks, such as private networks, VPNs, secure tunnels, frame relay, etc., for connecting any subset of participants. Non-limiting examples of modern equipment include hardwire, firmware, software, and together with Ethernet, Wireless EthernetTM (Wi-Fi), mobile radios (e.g. CDMA, FDMA, SOMA, TDMA, GSMTM). GRPS), UMTS, EDGE, LTE, etc.), Bluetooth®, Firewire, USB, IP, TCP, UDP, SSL, etc., may also be used.

[0041]

In exemplary embodiments, the first client, the second client and the facilitator each comprise a computer processor configured to perform certain steps within the scope of the present invention. In some embodiments, such as those using the Ethereum protocol as a transport mechanism, the facilitator includes instructions for computations by which network participants are evaluated by the Proof of Work protocol, in which case the network The network participant comprises a computer processor configured to evaluate the instructions for computation. In many embodiments, the client will have a display device and input device for interacting with a human, but this is not strictly necessary. In other embodiments, the client can be automated to completion without requiring human intervention. In one such embodiment, the first client's computer processor is configured to monitor the status of the transport mechanism, facilitator, data source, second client, etc. or some other input. , and are configured to automatically interact with various participants based on state changes. [0042]

For example, the transfer mechanism in one embodiment includes the Bitcoin protocol, with each client and facilitator having a key pair and a fixed data store to back up the first transaction. Observing that the first client has acquired new ownership of Bitcoin, the first client exchanges, via the facilitator, one financial instrument or security (e.g., USD) for exposure in exchange for another financial instrument or security (e.g., Bitcoin).) to initiate an offer to trade the exposure of [0043]

FIG. 1 shows an exemplary embodiment of the invention, in which the client, transport mechanism, facilitator, and data source are separate participants, particularly for use with distributed transport mechanisms. However, the illustrated configuration is not the only configuration contemplated by the present invention. In another embodiment, the facilitator indicates some or all aspects of the transfer mechanism. In another embodiment, the facilitator includes some or all aspects of the client. For example, some or all of the client's data store, the ability to initiate or accept offers, etc., can be "embedded" in the facilitator, thereby allowing the facilitator to represent the client. In yet another embodiment (eg, instead of being controlled by the facilitator's owner or a third party that has delegated control to the facilitator), the facilitator comprises a data source. Many configurations contemplated by the present invention are possible and will become apparent to those skilled in the art.

.

[0044]

FIG. 2 illustrates aspects of one embodiment for a swap that includes one or more source and commit trades. As shown, a commit transaction has a first input to accept a first quantity from a first source transaction (i.e., a first party) and a second input from a second source transaction (i.e., a second (from the parties), and one or more outputs for directing portions of these quantities to one or more other transactions (not shown), often the first and second The amount of is equal but not necessarily the sum of expected amounts including the principal amount (P) and (optional) collateral amount (C) in some cases as shown in several charts. is.

[0045]

In an exemplary embodiment, a commit transaction makes some or all of the amount available via its output(s) to at least one of the first and second parties, the facilitator, and any third party. It can be used only after confirmation from two parties. In other embodiments, a commit transaction is one of the facilitator or any trusted third party and one of the first and second parties, in part or all of the amount available via its output. It is configured so that it can be used only after confirmation. Another embodiment of the commit trade is that some or all of the amount available through its output is trusted by the first party or the second party, the third party, and optionally It is structured so that it can be verified and forwarded by any of the third parties. These are non-limiting examples, and in addition to the examples presented here, commit transactions may be set up to establish ownership regardless of the number of outputs. These transactions are somewhat analogous to checking accounts which must be signed by an authorized party.

.

[0046]

Although a first source transaction and a second source transaction are shown in FIG. 2, this should not be construed as limiting the invention. Amounts may be entered into committed transactions from any number of different sources. Overage will be refunded to the original or different party upon completion. The only limitation is that commit transactions must, at least in some embodiments, be adjusted to compensate for fees (not shown) charged for sending amounts from their respective sources to said inputs. . For example, transfer mechanisms may impose transfer fees, withdrawal fees, wire charges, etc. The Bitcoin protocol, for example, may require a “mining fee” to ensure timely transactions on the blockchain. [0047]

FIG. 3 illustrates aspects of one embodiment for a swap that includes a commit. Includes transactions and refund transactions. A committed trade includes a first input to receive a first principal amount (P A), a second input to receive a second principal amount (P B), and a committed output. A refund transaction includes an input to receive the amount from the commit output, a first refund output to the first party, and a second refund output to the second party. In typical embodiments, refund transaction records are generated after a period of time after a commit transaction, or are generated such that they are valid only after a period of time in the future if the commit output has not yet been used. This allows the commit output to be used in preference to another transaction and, if no such other transaction has been created, send the refund transaction record to the transfer mechanism to put the parties back on their feet. You can return it.

[0048]

4-5 illustrate aspects of swap embodiments involving relatively simple payment transactions in a swap situation involving principal and collateral. As shown in Figures 2-4, a commit transaction includes a first principal and collateral input from a first party and a second principal and collateral input from a second party. As shown in Figure 5, a commit transaction consists of a first principal (P A) from the first party, a first collateral (C A) from the first party, and a second principal input from the second party. (P B), and a second collateral from a second party (C B). These are just two of many possible configurations that will be apparent to those skilled in the art. For example, a commit transaction may include principal entry from a first party, collateral entry from a second party (e.g., first party guarantor not shown), and principal and collateral entry from a third party. can be done.

[0049]

In the embodiment shown in Figures 4 and 5, each payment transaction includes an input for receiving the amount from the commit output. Figure 4 shows the adjusted principal and collateral payment output to the first party, the adjusted principal and collateral payment output to the second party, and the fee (ÿ) output to any third party. include. In Figure 5, a payment transaction consists of a collateral payment output to the first party, a modified principal payment output to the first party, a modified collateral payment output to the second party, and an optional collateral payment output to the third party. Includes commission output. These are just two of many possible configurations that will be apparent to those skilled in the art. For example, a payment transaction, similar to the above, may consist of a modified principal payment output to the first party, a potentially modified collateral payment output to a third party (e.g., the first party's guarantor) (in the event of principal depletion) or a potentially modified collateral payment output to the second party (in the event of principal depletion).

[0050]

In the embodiment shown in Figures 4 and 5, the commission is apportioned from the adjusted principal and distributed evenly among the parties to the transaction, but this is not required. Fees can be allocated in any tier or in multiple tiers. It is also possible for one of the parties to bear all or a greater proportion, and in each of the embodiments shown in FIGS. Include the difference (ÿ) that is negative for the parties. For example, in the payment transaction shown in Figure 5, an allocation of the amount from the collateral is required once the second principal is exhausted before the expiration of the swap. In other words:

$$\delta > P_B - \frac{1}{2}\varphi \qquad \text{[eq. 1]}$$

[0051]

Some of the various components described above can be used to facilitate the basic swap agreement. To illustrate the method, in a Bitcoin or similar protocol transfer mechanism where the parties do not trust each other and the facilitator is not trusted by either party to complete, the following steps are performed: Assume it occurs within one embodiment. 1. A first client sends an offer with the following conditions. Conditions include: (a) a reference to a data source containing at least one of an underlying security and a quoted security; (b) a principal amount; (c) an expiration timestamp; (d) optionally a reference to a nominal asset. (e) optionally collateral amount; (f) optionally payment function. For example, it can be expressed as follows.

[Table 1]

Example terms:

Base: USD

Quote: AUD

Denominating: BTC

Principal: 0.5 (BTC)

Collateral: 2 × principal

$res_{base}(b_o, q_o, b_f, q_f)$: $principal \times \frac{b_f - b_o}{q_f - q_o}$

Expiration: 2014-06-01T12:34:56Z

2. Optionally, the facilitator verifies aspects of the offer (eg, the facilitator can interpret the terms, the expiration date is within acceptable limits, etc.). If verification is not granted, the facilitator can reject the offer and optionally send an error message to the first client. 3. A second client retrieves the offer from the facilitator. 4. A first client creates a first source transaction record that includes a transaction ID to the transfer mechanism. 5. A second client creates a second source transaction record containing a transaction ID to the transfer mechanism. 6. The second client sends the transaction ID of the second source transaction record, optionally via the facilitator, to the first client (eg, via offer ID, offer hash, etc. in the same message). In another embodiment, the first client sends the transaction ID of the first source transaction record to the second client, and subsequent steps reflect the following of this embodiment. 7. One of the second client and the facilitator sends the second public key to the first client in a manner associated with the offer. 8. The first client signs (ie, computes and associates a cryptographic signature with) the first principal entry of the uncompleted commit trade record to create a completed commit trade record. An uncompleted commit transaction record includes: (a) a first principal input to receive a first principal amount from a first source transaction; (b) a second principal amount to receive a second principal amount from a second source transaction. (c) Subject to the signature of two private keys of (i) the first public key, (ii) the second public key, and (iii) the facilitator's public key. Commit output including. Example of an uncompleted commit transaction record:

[Table 2]

```
Input:

        Previous tx: 85e5...e61f

        Index: 1

        scriptSig: efd6...ea1601 a6a6...2c2b

Input:

        Previous tx: 705d...9ce2

        Index: 0

        scriptSig: [sig. placeholder]

...

Output:

        Value: 300000000

        scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
        OP_CHECKMULTISIG

...
```

9. The first client, possibly through the facilitator, sends the pending commit transaction record to the second client. The Facilitator optionally verifies aspects of the Initial Commitment Transaction Record (e.g., that the Initial Commitment Transaction Record is signed by the first party, that the first and second principal amounts are each met, etc.). . If verification is not granted, the facilitator can reject the first commit transaction and possibly display an error message to the first client. The facilitator optionally sends the offer and initial commit transaction record to the second client. 10. The second client optionally verifies that the pending commit transaction record was signed by the first party, and so on. 11. The second client creates a completed commit transaction record by signing the uncompleted commit transaction record and optionally stores it in permanent memory. Completed commit transaction records include: (a) a first principal input to receive a first principal amount from a first original transaction; (b) a second principal input to receive a second principal amount from said second source transaction; This input, (c) the committed amount and (i) the first public key (ii) the second public key. (iii) a commit output contingent on requiring signatures of two private keys of the facilitator's public keys; Example of completed commit transaction record:

[Table 3]

```
ID: 6b24...b607

Input:

      Previous tx: 85e5...e61f

      Index: 1

      scriptSig: efd6...ea1601 a6a6...2c2b

Input:

      Previous tx: 705d...9ce2

      Index: 0

      scriptSig: 78eb...fc4501 531f...00dd

...

Output:

      Value: 300000000

      scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
      OP_CHECKMULTISIG

...
```

12. The second client signs a pending refund transaction record containing: (a) lock time after expiration timestamp, (b) input to receive committed amount from committed transaction record, (c) first refund amount and first condition requiring first party approval. a first refund output containing

(d) A second refund output containing the second refund amount and the terms requiring second party approval. Examples of incomplete refund transactions

[Table 4]

```
Input:

      Previous tx: 6b24...b607

      Index: 0

      scriptSig: OP_0 [sig. placeholder] c255...d80301

Output:

      Value: 149995000

      scriptPubKey: OP_DUP OP_HASH160 53a5...8974 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 149995000

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
      OP_CHECKSIG

...

nLockTime: 2014-06-03T12:34:56Z
```

13. The second client sends the completed committed transaction record and the pending refund transaction record to the first client, possibly through the facilitator. The Facilitator optionally verifies completed committed transaction records and uncompleted refund transaction records. (e.g. a completed refund transaction record signed by a first party and a second party, an unfinished check refund transaction record signed by a second party, or an unfinished refund transaction record and a completed commit). The description of the transaction record amount is equivalent, or the uncompleted withdrawal amount is equal to or less than the first principal amount, the second withdrawal amount of the small withdrawal transaction record is equal to or less than the second principal amount, and the lock time is The facilitator can reject the refund transaction record or the completed commit transaction record, optionally reporting an error to the second client, if the validation fails (e.g., after the expiration timestamp). You can also send messages. The facilitator optionally sends the completed committed transaction record and the uncompleted refund transaction record to the first client. 14. The first client optionally verifies that the completed committed transaction record is as expected and signed by the first party and the second party, and that the initial refund transaction record is as expected and signed by the second party. Confirm that 15. The first client optionally saves a copy of the completed committed transaction record in permanent memory. 16. The first client optionally creates a completed refund transaction record and saves a copy of it in permanent memory. The completed refund transaction record contains (a) the lock time after the expiration timestamp, (b) an input to receive the committed amount from the completed committed transaction, and (c) the first refund amount and the first party's approval. a first refund output containing a first condition requiring a second refund amount and a second refund output containing a condition requiring second party approval;

It is included. Example

of completed refund transaction record

[Table 5]

```
ID: d5f8...8ab5

Input:

      Previous tx: 6b24...b607

      Index: 0

      scriptSig: OP_0 b859...452c01 c255...d80301

Output:

      Value: 149995000

      scriptPubKey: OP_DUP OP_HASH160 53a5...8974 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 149995000

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
      OP_CHECKSIG

...

nLockTime: 2014-06-03T12:34:56Z
```

17. The first client, possibly through the facilitator, sends the completed refund transaction record to the second client. The Facilitator optionally verifies aspects of the Completed Refund Transaction Record (e.g., signed by both parties, that the Completed Refund Transaction Record has not been otherwise modified, the terms and conditions of the Completed Commit Transaction Record). similar, etc.). If verification fails, the facilitator can refuse to record the completed refund transaction or optionally send an error message to the first client. The facilitator optionally sends the completed refund transaction record to the second client. 18. The second client optionally verifies that the completed refund transaction record is as expected and signed by the first party and the second party. 19. 20. After creating or receiving both the completed commit transaction and the completed refund transaction, the first client sends a first source transaction record for executing the source transaction to the transfer mechanism; After creating or receiving both the completed commit transaction and the completed refund transaction, the second client submits the second source transaction record to the transfer mechanism to execute the second source transaction. 21. After confirming that both the first source transaction and the second source transaction have been submitted to the transfer mechanism, one or both of the first client and the second client complete to execute the commit transaction. Submit a commit transaction record. 22. At or after the expiry timestamp, or at a point defined by the terms and conditions and prior to the lock time of the completed refund transaction record, the facilitator optionally accesses one or more data sources (e.g., publicly traded financial instruments). (e.g., the most recent price of the

Calculate the conditions for In one embodiment, data sources include external data feeds, internal databases, other data sources, and the like. In an exemplary embodiment, given a time t, the data source can be a reference asset at time t , a quote commodity, a nominal asset bt as a reference asset, an asset qt , or a quote for a base measure (e.g., (if the base or pro forma instrument is a nominal asset). Continuing the example above, the underlying commodity would be USD, the quote would be AUD, and the asset would be Bitcoin. 0 is the USD value of Bitcoin at the time the trade is initiated and bf is the USD value of Bitcoin at the time the trade is completed. q0 is the AUD value of Bitcoin at the time the trade begins and qf is the AUD value of Bitcoin at the time the trade is completed. The calculation used by the facilitator to calculate the first and second payment amounts is that the loss of res base (b) is proportional to the other party's profit, implying that: means:

Ten

0 , q 0 , , q f). In an exemplary embodiment, the parties b f

$$res_{quote}(b_0, q_0, b_f, q_f) = -res_{base}(b_0, q_0, b_f, q_f) \quad \text{[eq. 2]}$$

23. The facilitator has (a) an input to receive the committed amount from the committed transaction, (b) a first payment output containing the first payment amount and a first condition requiring approval by the first party, (c) a second payment amount output including the second payment amount and terms requiring second party approval; and (d) any fees and terms including third party approval. Sign the check transaction record containing the third payment output. Typically, the sum of the first payment amount, the second payment amount and any fee amount is less than or equal to the committed amount of the completed committed transaction. Examples of payment transaction records:

20

[Table 6]

```
Input:

      Previous tx: 6b24...b607

      Index: 0

      scriptSig: OP_0 [sig. placeholder] ddbb...b00601

Output:

      Value: 142500736

      scriptPubKey: OP_DUP OP_HASH160 53a5...8974 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 157479264

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 10000

      scriptPubKey: OP_DUP OP_HASH160 d377...5c8c OP_EQUALVERIFY
      OP_CHECKSIG

...
```

24. The facilitator sends the pending transaction record to both the first client and the second client. Either party may independently verify, sign and submit the payment transaction record to the transfer mechanism before the other party submits the completed refund transaction record.

[0052]

The above is but one embodiment of value transfer according to the present invention, and equivalent or alternative procedures may be utilized in other embodiments. The following describes embodiments that include atypical but exemplary mechanisms. 1. A first client sends an offer to a second client. 2. A first client sends an offer to a facilitator. 3. The facilitator sends an uncompleted committed transaction record to the first client to create a completed committed transaction record. The uncompleted committed trade record includes (a) a first principal entry to receive a first principal amount from a first source trade; (b) (i) a first party; Parties, (iii) a first input containing a first committed amount for terms requiring approval by two of the three parties of the facilitator. 4. The facilitator sends a second pending commit transaction record to the second client to create a completed committed transaction record, the second pending commit transaction record being: (a) the second source transaction from the second source transaction; and (b) the three parties of (i) the first party, (ii) the second party, and (iii) the facilitator

A first input is included that includes a second committed amount for which two of the terms require approval. 5. The first client signs the first source transaction record. 6. The first client signs the pending commit transaction record (eg, with SIGHASH_SINGLE | SIGHASH_ANYONECANPAY). Example of first uncompleted commit transaction record

[Table 7]

```
Input:

      Previous tx: 85e5...e61f

      Index: 1

      scriptSig: 5e7c...a11a83 ecad...d0ba

...

Output:

      Value: 150000000

      scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
      OP_CHECKMULTISIG

...
```

7. The first client sends the first pending committed transaction record to the facilitator. 8. A second client signs a second source transaction record. 9. The second client completes and signs the second pending commit transaction record (eg, with SIGHASH_SINGLE | SIGHASH_ANYONECANPAY). Example of a second uncompleted commit transaction record:

[Table 8]

```
...

Input:

      Previous tx: 705d...9ce2

      Index: 0

      scriptSig: ade1...9dcb83 f058...878a

...

Output:

      Value: 150000000

      scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
      OP_CHECKMULTISIG

...
```

10. A second client sends a second unfinished committed transaction record to the facilitator
.

11. The facilitator creates a completed committed trade record from the first pending committed trade record and the second pending committed trade record, wherein the completed committed trade record: (a) receives a first principal amount from the first source transaction; and (b) the first committed amount; and (i) the first party; (ii) the second party; (c) a second principal input to receive a second principal amount from a second source transaction; and (d) a second committed amount and (i) a first It consists of a second commit output of terms requiring approval by two of the parties (ii) the second party (iii) the facilitator. Completed commit transaction record example

[Table 9]

```
ID: 11f0...8ea8

Input:

      Previous tx: 85e5...e61f

      Index: 1

      scriptSig: 5e7c...a11a83 ecad...d0ba

Input:

      Previous tx: 705d...9ce2

      Index: 0

       scriptSig: ade1...9dcb83 f058...878a

  ...

  Output:

       Value: 150000000

       scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
       OP_CHECKMULTISIG

  Output:

       Value: 150000000

       scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
       OP_CHECKMULTISIG

  ...
```

In another embodiment, the first client sends the transaction ID of the first source transaction record to the facilitator before the facilitator sends the first pending committed transaction record and the second pending committed transaction record. and the second client provides the transaction ID of the second source transaction record to the facilitator. The facilitator creates a first uncompleted committed trade record identical to the second uncompleted committed trade record, each with a first principal amount having a placeholder signature.

An input and a second principal input with a placeholder signature. Once each pending commit trade record has been sent to each client, the client must complete each principal entry (e.g., SIGHASH_ALL | SIGHASH_ANYONECANPAY). The Facilitator collects the signed pending commit transaction records and integrates the signed entries into the completed commit transaction records. In such embodiments, the first commit output and the second commit output can be combined, and the corresponding payment transaction record and refund transaction record can omit their respective second inputs. 12. The facilitator sends the completed commit transaction record to the first client, which optionally stores it in permanent memory. 13. The facilitator sends the completed commit transaction record to the second client, which optionally saves it in permanent memory. 14. The first client signs an uncompleted refund transaction record (eg, with SIGHASH_ALL | SIGHASH_ANYONECANPAY or SIGHASH_SINGLE | SIGHASH_ANYONECANPAY) that includes: (a) lock time after expiration timestamp; (b) first input to receive committed amount from first committed transaction; (c) second input to receive committed amount from second committed transaction; (d) a first refund output containing a first refund amount and a first condition requiring first party approval; (e) a second refund amount and requiring second party approval. Second refund output with conditions. Example of an open refund transaction record

[Table 10]

```
Input:

      Previous tx: 11f0...8ea8

      Index: 0

      scriptSig: OP_0 78a2...203181 [sig. placeholder]

Input:

      Previous tx: 11f0...8ea8

      Index: 1

      scriptSig: OP_0 fdbe...893f81 [sig. placeholder]

...

Output:

      Value: 149995000

      scriptPubKey: OP_DUP OP_HASH160 53a5...8974 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 149995000

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
      OP_CHECKSIG

...

nLockTime: 2014-06-03T12:34:56Z
```

15. The first client sends the pending refund transaction record and the completed refund transaction record to the second client. 16. The second client creates a completed refund transaction record from the pending refund transaction record (eg, signed with SIGHASH_ALL | SIGHASH_ANYONECANPAY or SIGHASH_SINGLE | SIGHASH_ANYONECANPAY) and stores it in permanent memory. Example of completed refund transaction record

[Table 11]

```
ID: eb09...3d15

Input:

      Previous tx: 11f0...8ea8

      Index: 0

      scriptSig: OP_0 78a2...203181 b765...fc4383

Input:

      Previous tx: 11f0...8ea8

      Index: 1

      scriptSig: OP_0 fdbe...893f81 91e4...4dd583

...

Output:

      Value: 149995000

      scriptPubKey: OP_DUP OP_HASH160 53a5...8974 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 149995000

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
      OP_CHECKSIG

...

nLockTime: 2014-06-03T12:34:56Z
```

17. The second client sends the completed refund transaction record to the first client. 18. After creating or receiving both the completed commit transaction record and the completed refund transaction record, the first client submits the first source transaction record to the transfer mechanism. 19. After creating or receiving both the completed commit transaction record and the completed refund transaction record, the second client submits the second source transaction record to the transfer mechanism. 20. After confirming that both the first source transaction record and the second source transaction record have been submitted, one or both of the first client and the second client submit a completed committed transaction record. 21. On or after the expiration of the time stamp, or prior to the Lock Time of the Completed Refund Transaction Record at a predetermined time determined by the Terms, the Facilitator will calculate according to the Terms to determine the amounts of the first and second payments. and optionally request information from one or more data sources to use in calculations. 22. The facilitator signs the pending payment transaction record. (for example, SIGHAS

H_ALL | SIGHASH_ANYONECANPAY or SIGHASH_SINGLE | SIGHASH_ANYONECANPAY)
Examples of pending payment transaction records: Table 12

```
Input:
      Previous tx: 11f0...8ea8
      Index: 0
      scriptSig: OP_0 [sig. placeholder] 8cd3...d86481
Input:
      Previous tx: 11f0...8ea8
      Index: 1
      scriptSig: OP_0 [sig. placeholder] 12bc...825281
...
Output:
      Value: 142500736
      scriptPubKey: OP_DUP OP_HASH160 53a5...8974 OP_EQUALVERIFY
      OP_CHECKSIG
  Output:
       Value: 157479264
       scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
       OP_CHECKSIG
  Output:
       Value: 10000
       scriptPubKey: OP_DUP OP_HASH160 d377...5c8c OP_EQUALVERIFY
       OP_CHECKSIG
  ...
```

23. The facilitator sends the pending payment transaction record to both the first client and the second client, either of which can submit it as in the previous exemplary embodiment. [0053]

Various verification steps have been omitted for the sake of brevity.
[0054]
It will be apparent to those skilled in the art that aspects of each of the above embodiments can be mixed. For example, a first client can send an offer to a facilitator and a second

Clients can find and recruit facilitators. As noted above, the facilitator is required to act on behalf of one or both of the parties, so aspects of one or both of the first and second clients may be consistent with the facilitator. Yes, the facilitator can omit most of the above steps that were deemed superfluous. The facilitator can include aspects of one client, but not the other. In that case, the client may optionally independently verify the transaction record received from the facilitator prior to signing. In such embodiments, the facilitator typically includes a method of controlling aspects of the client through an interface such as a web-based user interface (UI), application programmer interface (API), or the like.

[0055]

In such embodiments, the party delegating authority to the facilitator must trust the facilitator to act in a safe and fair manner, which many parties already do to traditional third-party intermediaries. Similar to having expectations. The first party has independent access to the same key pair for the facilitator to act on behalf of the first party, and similarly the second party has independent access to the same key pair for the facilitator to act on behalf of the second party. So if the facilitator is destroyed, in the worst case, the first party and the second party will be able to complete the refund after the lock time if they keep a copy of the completed refund transaction record in permanent memory. They can get their assets back by submitting transaction records.

.

In one embodiment, when a client detects a new consumable output (e.g., by monitoring blockchain changes or updates when using Bitcoin or a protocol with a similar transfer mechanism), it automatically creates a new Accept as many remote offers as consumable power. In yet another embodiment, if the client detects a second available output, it will attempt to disable it. If successful, send out a new offer with some or all of the new consumable output. Other variations are also possible. For example, a client could scan for available offers and configure them to match consumable outputs. Algorithms are known in the art and vary in complexity. For example, a client implementation of the Bitcoin protocol provides an algorithm that matches simple transaction inputs to consumable outputs. Such algorithms are adaptable by those of ordinary skill in the art and embodiments of similar inventions. [0057]

In some embodiments, these conditions optionally include the ratio at which the first security and the second security are assigned to assets, and the amount each participant must allocate. For example, in one embodiment, these terms may provide for “selling” 2 Bitcoins/USD from each party with a required allocation of 3 Bitcoins, in other words, 2 Bitcoins/USD. 2 Bitcoins and 1 Bitcoin for the duration of the swap (i.e., until it expires or until one party's principal and collateral is exhausted). should be allocated to collateral. [0058]

Each party's allocation need not be equal. In some embodiments, if the market expects a particular commodity pair to decline over the duration of the swap, the party accepting the exposure to that commodity pair is required to be allocated more collateral than the other party. In some cases. In the example above, the risks between the parties are asymmetric. The maximum amount an offerer can lose is 2 Bitcoins (if Bitcoin becomes worthless in USD). However, the receiver's loss is unlimited (if the US dollar becomes worthless against Bitcoin), so

[Number 3]

$$res_{base}(b_o, q_o, b_f, q_f) = principal \times \frac{b_f - b_o}{q_f - q_o} \quad [\text{eq. } 3]$$

An alternative is:

$$res_{base}(b_o, q_o, b_f, q_f) = principal \times \left(\frac{b_f}{q_f} - \frac{b_o}{q_o} \right) \quad [\text{eq. } 4]$$

[0060]

Other embodiments may employ a symmetrical model.

[Equation 5]

$$res_{base}(b_o, q_o, b_f, q_f) = \begin{cases} \frac{b_t}{q_f} \leq \frac{b_o}{q_o} & : principal \times \left(\frac{b_f q_o}{b_o q_f} - 1 \right) \\ \frac{b_t}{q_f} > \frac{b_o}{q_o} & : principal \times \left(1 - \frac{b_o q_f}{b_f q_o} \right) \end{cases} \quad [\text{eq. } 5]$$

[0061]

where res base (ÿ) is the initial value of the base security at that time b 0 , the initial value of the quoted security q 0 , the value of the base security at time f b f , the value of the quoted security at time f q f is the profit or loss of the party taking the exposure of the conditional base security. The resulting gain or loss of the party taking the exposure of the pro forma security is reversed.

[Formula 6]

$$res_{quote}(b_o, q_o, b_f, q_f) = -res_{base}(b_o, q_o, b_f, q_f)$$

$$= \begin{cases} \frac{b_f}{q_f} \leq \frac{b_o}{q_o} & : principal \times \left(1 - \frac{b_f q_o}{b_o q_f} \right) \\ \frac{b_f}{q_f} > \frac{b_o}{q_o} & : principal \times \left(\frac{b_o q_f}{b_f q_o} - 1 \right) \end{cases} \quad [\text{eq. } 6]$$

[0062]

In this example, the party risk formula is symmetrical. Even if the Base Security becomes nil, only the principal is lost by the party with the Base Security exposure. Similarly, if the quoted security falls to zero, the party with the quoted security exposure will only lose principal. Note that no collateral is required. As an alternative, the following can be considered.

[Formula 7]

$$res_{base}(b_o, q_o, b_f, q_f) = -res_{quote}(b_o, q_o, b_f, q_f)$$

$$= \begin{cases} \frac{b_f}{q_f} \leq \frac{b_o}{q_o} & : -principal \times \frac{b_o q_f}{b_f q_o} \\ \frac{b_f}{q_f} > \frac{b_o}{q_o} & : principal \times \frac{b_f q_o}{b_o q_f} \end{cases} \quad [\text{eq. } 7]$$

[0063]

The party risk formula is also symmetrical in this embodiment. But if the underlying asset becomes zero, the loss of the party that took the underlying asset approaches infinity and all others are equal. Similarly, if the Estimated Equity becomes zero, the loss suffered by the party that took the Estimated Equity approaches infinity, all else being equal. Please note that collateral is required if losses exceed the principal amount.

More volatile product pairs may require more collateral to minimize the risk of premature termination. These are basic examples. The conditions affecting the calculations for determining the allocation payment can be arbitrarily complex and are limited only by the imagination of the participants. All such variations are contemplated by the present invention.

[0064]

There are situations in which one of the parties wishes to terminate the transfer of value (eg swap) before it expires. Both parties may agree to terminate prematurely. In one embodiment, the facilitator facilitates this by creating a pending payment transaction record as if the swap had expired when the parties agreed to terminate. The party requesting termination signs and transmits the pending payment transaction record to the agreeing party, who submits it to the transfer mechanism. If the facilitator involves outputting a fee to a third party, the agreeing party may require that the fee be borne in greater or full extent by the requesting party. [0065]

If one of the parties wishes to terminate the transfer of value before the time expires but is unable to obtain the other party's agreement, another option is for the party wishing to terminate to seek third party representation. . Figures 6 and 7 show various examples of swap embodiments in which such surrogates are involved.

Figure 6 shows the case where the withdrawing party (A) persuades the entrant (C) to transfer value to the remaining party (B) on behalf of A. In addition, the entrant pays the withdrawal side the negotiated amount (ÿ). This is facilitated in this embodiment by proxy transactions, second commit transactions, and second refund transactions. [0067]

For clarity, the output of the committed trade and the corresponding input of the proxy trade are: first principal (P A) first collateral (CA) second principal (P B) second collateral (CB) are shown separately. This is not a limitation of the invention. As in the previous embodiment, the output of the commit transaction and the corresponding input of the proxy transaction may be of any structure deemed valid by the transfer mechanism. The output of the proxy trade and the input of the second commit trade are similarly drawn for clarity. Also, all structures of inputs and outputs between transactions are contemplated by the present invention.

[0068]

The difference (ÿ) is the difference for calculating the first payment and the second payment, assuming that the transaction has expired at the time the transaction is proxied. As with the embodiment shown in FIG. 6, this favors the remaining side. The proxy transaction record is structured so that the exiting side accepts the loss of the difference and the entrant side supplies assets to fill the vacant position. [0069]

Also, in the embodiment shown in FIG. 6, the proxy refund is asymmetric. The entrant will be refunded the amount that party committed (minus the amount negotiated), and the remaining side will be refunded what it received assuming the swap had expired at the time of proxy. Other variations are also possible. For example, in one embodiment, the negotiated amount may be split and transferred in other stages of value transfer or in other value transfers altogether. [0070]

In the embodiment shown in Figure 7, the surrogate favors the withdrawal side. In that embodiment the proxy refund is symmetrical. The Remaining Party receives the refunded portion of the original transaction.

[0071]

In one embodiment, delegation is facilitated as follows. 1.

The facilitator performs a computation along the terms to determine the withdrawal amount, optionally requesting information from one or more data sources for that computation. 2. The facilitator should

(a) a first input to receive an amount from a commit transaction;

(b) an entry input to receive the entry amount from the source transaction; (c) a withdrawal output containing the withdrawal amount and any conditions that require the approval of the first party; (d) a surrogate amount and (i) the second party (ii)) third party (iii) of the facilitator

Create an incomplete proxy transaction record containing proxy output, including a second condition that requires approval from two of the parties. Example of incomplete agency transaction record: [Table 13]

```
Input:
      Previous tx: 6b24...b607
      Index: 0
        scriptSig: OP_0 [sig. placeholder] [sig. placeholder]
  Input:
      Previous tx: dd66...ae8e
      Index: 3
      scriptSig: [sig. placeholder]
  Output:
      Value: 300000000
      scriptPubKey: 2 bf9a...f9e3 952b...0542 cffd...1373 3
      OP_CHECKMULTISIG
  Output:
      Value: 121871000
      scriptPubKey: OP_DUP OP_HASH160 6250...6cfc OP_EQUALVERIFY
      OP_CHECKSIG
  ...
```

3. The facilitator sends the pending agent transaction record to the first party and the third party. 4. The first party creates a signed incomplete agency transaction record by signing the first incomplete agency transaction record (e.g., signing with SIGHASH_ALL | SIGHASH_ANY ONECANPAY) and sends the first incomplete agency transaction record to the facilitator. Submit proxy transaction records. 5. The third party creates a second pending agency transaction record by signing the pending agency transaction record (e.g., by signing with SIGHA SH_ALL | SIGHASH_ANYONECANPAY) and the second signed agency transaction record. to the facilitator. 6. The facilitator creates a completed agent transaction record (eg ID: 9c8b...4794) using the first and second open agent transaction records.

7. The facilitator must provide
(a) a lock time after the expiration timestamp, (b) an input to
receive the surrogate amount from the surrogate transaction, (c)
the first refund amount and the terms that require the second party's approval. a first refund output to be received and
(d) Signing the pending surrogate refund transaction record, including a second refund output that includes the second refund amount and terms requiring third party approval. Example of an incomplete proxy refund transaction record: [Table 14]

```
Input:

      Previous tx: 9c8b...4794

      Index: 0

      scriptSig: OP_0 [sig. placeholder] b2ac...8a4601

Output:

      Value: 178124000

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 121866000

      scriptPubKey: OP_DUP OP_HASH160 94e2...4fb6 OP_EQUALVERIFY
      OP_CHECKSIG

...

nLockTime: 2014-06-03T12:34:56Z
```

8. The facilitator signs the open proxy refund transaction record to create a signed proxy refund transaction record and sends the signed proxy refund transaction record to the second party and the third party. 9. The Facilitator submits a complete substitute refund transaction record to the Transfer Mechanism. [0072]

Details of various verifications and procedures involved in the foregoing embodiments have been omitted for the sake of brevity. In other embodiments, various transaction records are created or signed by the first party or the second party rather than by the facilitator. For example, a first party or a second party may agree on an amount on a proxy transaction record, which can be signed without the need for a facilitator. All such variations are envisioned. [0073]

A letter of credit (L/C) is well known in the art, but it is fundamentally a third party's agreement to a first party prior to a given time provided pre-agreed terms are met. is an agreement to transfer value to a second party on behalf of It typically involves manual and esoteric reviews of shipping documents by expensive intermediaries before releasing the buyer's funds. Such an expensive approach, however, is not expected, as the facilitator may store the payment transaction record in a known tracking number or other implementations, such as the shipper's public API, letter of credit (L/C) valuation survey results, etc.

observing the presence or absence of data at a location, checking whether the values of a variable or response from an API are within a set of expected values or matching an expected pattern, receiving a signal from a digital device (temperature sensor, GPS, etc.) and conditions the origination or creation of a payment transaction based on the results of a query such as verifying that the signal value is within an expected range or tolerance. can be avoided by For example, US patent application Ser. No. 13/970,755 ('755) describes a system and method for efficiently computing geospatial proximity. Others are known in the art. Calculations in one embodiment include states where an object was "at" or "near" (ie, within a certain distance) a particular location. (e.g., automatic identification and data capture (AIDC) devices such as self-reporting GPS, barcodes, quick response (QR) codes, radio frequency identification (RFID) tags, etc. in the vicinity of reporting detectors or sensors at known locations.). Many possible structures are envisioned by the present invention and will be apparent to those skilled in the art. [0074]

FIG. 8 illustrates aspects of one embodiment relating to a letter of credit (L/C) with source and commit transactions. As shown, a commit transaction is a first input to accept a first amount from a first source transaction (e.g., first party) or to inject a first amount into one or more transactions. Contains outputs (not shown). A commit transaction in another embodiment (shown in other figures) includes a second input for accepting a second amount from a second source transaction. Here the sum of the first amount and the second amount includes in some cases a principal amount (P) and (optionally) a collateral amount (C) as shown in various figures. Only the first source transaction is shown in FIG. It should not be construed as a limitation of the invention.
[0075]
FIG. 9 illustrates aspects of one embodiment relating to a commit transaction, an expiry date transaction synonymous with the refund transaction shown in the previous embodiment, and a letter of credit. However, refund transactions have exclusive implications for the collection of funds in the event of an exception (such as when a facilitator is unable to create or sign a payment record) and expiry transactions in addition to collection of funds. The use of is assumed by the offer (e.g. the facilitator was on board but the set conditions were not met within the deadline timestamp). The difference is mostly conceptual. Within the scope of the present invention, the two are essentially the same function. A commit trade includes a first input for receiving a first principal amount (P A) and a commit output. The expiry date transaction includes an input for receiving a committed output amount that is a first output to the first party, and includes a second input for receiving a second amount. Contains a second output for two parties.
[0076]
10-11 illustrate aspects of embodiments involving relatively simple payment transactions involving letters of credit in situations involving principal and collateral. FIG. 10 contains the principal and collateral ((P+C) A) inputs from the first party . In other embodiments, the inputs need not be coupled just as described above. The commit transaction of FIG. 11 includes an initial applied principal and collateral input from the first party and a second collateral (C B) input from the second party. These are two of the many possible configurations contemplated by the present invention. For example, a commit transaction may include primary input from a first party, collateral input from a third party (e.g., a guarantee from the first party, not shown) and collateral input from a second party. It may also be composed of [0077]

The embodiments shown in FIGS. 10-11 include inputs for receiving the amount of output for each commit of the payment transaction. FIG. 10 shows that a payment transaction has a first collateral payment output to the first party, a first principal output to the second party, and any fees deducted from the collateral. FIG. 11, a payment transaction, has the output of the collateral payment to the first party, the participating principal and the collateral loan disbursement, output to the second party. Commit transactions also have the option premium output to third parties equally borne by the parties in the payment transaction. These are the multi-layers of the present invention.

are just two examples of many possible configurations. For example, any fee output can be assigned at any stage, and at any number of stages. It can also be borne disproportionately by one of the parties. [0078]

To exemplify how the various components above can be used to facilitate letter of credit agreements, the following procedure using Bitcoin or a similar protocol as the transfer mechanism is one. This is what happens in the embodiment. In this embodiment, the parties do not trust each other, nor is the facilitator fully trusted by either party:1. A first client provides: (a) payment terms including one or more references to data sources, payment functions including one or more references to data sources, and one or more references to data sources; Payment Terms

Ten

,

(b) a principal amount;
(c) an expiration timestamp; (d) an
optional first collateral amount; (e) an
optional second collateral amount.
Condition example: [Table 15]

```
Payer principal: 0.5 (BTC)

Payer collateral: 1 × principal

Payee collateral: 0.05 × principal

  Disbursement condition:

  FedEx("987654321").deliveredToCarrier() == true

  Expiration: 2014-06-01T12:34:56Z

  ...
```

2. A first client signs a first source transaction record. 3. (a) a first input to receive a first amount from a first source transaction; (b) optionally a second input to receive a second amount from a second source transaction; c) the committed amount and (i) the first party (ii) the second party (iii) the third party

Create a first uncompleted commit transaction record containing a commit output, including conditions that require approval from two of them. 4. The first client

40

optionally sends the offer to the facilitator and the facilitator validates the offer. If the validation fails (such as that the expiration timestamp is within the acceptable range, or that the terms can be interpreted), the Facilitator can optionally reject the offer, optionally with an error message. can be sent to the client. 5. A first client sends an offer to a second client. 6. A second client creates a source transaction record. The second client sends the uncompleted commit transaction record to the first client. 7. The first client signs the pending commit transaction record (e.g., SIGHAS

Create a commit transaction record completed by H_ALL |

.

```
ID: c215...fc9b

Input:

      Previous tx: 85f7...e06c

      Index: 4

      scriptSig: 186b...ed3d81 9a9c...0fc5

Input:

      Previous tx: 6b03...e16e

      Index: 7

      scriptSig: c48e...353c81 4afe...2c8d

...

Output:

      Value: 150000000

      scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
      OP_CHECKMULTISIG

...
```

8. The first client signs a pending expiration transaction record containing: (a) the lock time since the expiry timestamp, (b) an input to receive the committed amount from the commit transaction, (c) from the first expiry amount and a condition requiring first party approval. (d) optionally, a second expiration date output consisting of a second expiration amount and a condition requiring approval of the second party. Example of a complete expiry transaction record:

[Table 17]

```
Input:

      Previous tx: c215...fc9b

      Index: 0

      scriptSig: OP_0 7d17...0b5101 [sig. placeholder]

...

Output:

      Value: 99995000

      scriptPubKey: OP_DUP OP_HASH160 53a5...8974 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 4995000

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
      OP_CHECKSIG

...

nLockTime: 2014-06-01T12:34:56Z
```

9. The first client sends the completed committed transaction and the uncompleted expiry transaction record to the second client, which optionally stores it in permanent memory. 10. The second client creates a completed expiration transaction record by signing the incomplete expiration transaction record and optionally stores the completed expiration transaction record in permanent memory. 11. The second client sends the completed expiry transaction record to the first client
.

12. After creating or receiving the completion expiry date transaction record and the completion committed transaction record, the first client submits the first source transaction record to the transfer mechanism to conduct the first source transaction. 13. After the second client creates or receives the completion expiry date transaction record and the completion committed transaction record, it submits the second source transaction record to the transfer mechanism for conducting the second source transaction. 14. After confirming that both the first source transaction record and the second source transaction record have been submitted, one or both of the first or second client sends the complete committed transaction record to the transfer mechanism, Execute commit trades. 15. Expiration trade record at a time defined by terms or upon inquiry from first and second clients (optionally providing one or more of full commit trade record, reference to committed trade, and terms) Before the full lock time of the facilitator, the facilitator performs the calculation of the first payment amount and optionally the second payment amount, optionally requesting information from the data source to use in the calculation. (e.g. whether a scheduled shipment has been sent to the shipper). This can be done via external APIs, internal database queries, etc.

.

In a typical embodiment, payment amounts are such that remaining collateral is returned to the respective provider and principal is transferred from the provider (payer) to the counterparty (payee).

16. The facilitator provides: (a) an input to receive a committed amount from the committed transaction;

(c) a second payment amount output including a second payment amount and a condition requiring first party approval; and (d) a second payment amount output including a condition requiring third party approval. and a third payment output, typically including a sum of the first payment amount, the second payment amount, and any fee amount that does not exceed the committed amount from the committed amount. sign a transaction or transaction record

.

Example of pending payment transaction record: Table 18

```
Input:

      Previous tx: c215...fc9b

      Index: 0

      scriptSig: OP_0 [sig. placeholder] 8205...424901

Output:

      Value: 49990000

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 54990000

      scriptPubKey: OP_DUP OP_HASH160 6250...6cfc OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 10000

      scriptPubKey: OP_DUP OP_HASH160 d377...5c8c OP_EQUALVERIFY
      OP_CHECKSIG

...
```

17. As in the previous embodiment, the facilitator signs the transfer mechanism to send the pending payment transaction record to both the first client and the second client, which can both be submitted.

[0079]

In another embodiment, the state of the commit output requires approval of either the first party and the second party or the second party and one or more service providers (eg, shipper, insurance company, prosecutor, etc.). A pending payment transaction record consists of a second party placeholder and a service provider. If all service providers sign each, a second party can sign and submit the payment transaction record to the transfer mechanism. In still other embodiments, the service providers are paid from their respective payment transactions when the second party commits assets in the commit transaction to pay the service provider in the commit transaction. [0080]

Figures 12-14 illustrate example embodiments of various series of letters of credit that include party replacements. FIG. 12 illustrates aspects of an embodiment in which a payer (A) convinced an assigner (C) to assign a transaction with a payee (B). The payer also transfers the negotiated amount (ÿ) to the assigner. For example, if the payer party has promised to purchase the goods from the payee, it has decided, at a loss, to sell the right to receive the goods to the assignee due to unforeseen market conditions. This is facilitated by proxy transactions and secondary expiry transactions in the illustrated embodiment. In a related embodiment, the payer sells the right to receive a share of the profits, and the negotiated amount may be passed from the assignor to the payer. In the embodiment shown in FIG. A voluntary fee (ÿ) is paid to a third party, which is borne by the recipient. [0081]

FIG. 13 illustrates aspects of an embodiment in which a payee (B) has convinced an assigner (C) to assign a transaction with a payer (A). The assignor also transfers the negotiated amount (ÿ) to the payer. For example, a third party may be interested in having the right to receive payment in future payment transactions, perhaps on the reduced relative value of the assignee's other assets. This is facilitated by agency transactions in the illustrated embodiment, and in related embodiments where the payee has sold the right to receive the payment, the negotiated amount may also be paid to the assignor. As in FIG. 12, in FIG. 13 an optional fee (ÿ) is paid to a third party, which is borne by the assignor. [0082]

Figure 14 shows that the payer (A) partially completes the transaction with the payee (B) (as shown covering the collateral originally paid by the payer). A mode in which is substituted for is shown. In addition, the assigner transfers the negotiated amount (ÿ) to the payer. This is facilitated in the illustrated embodiment by a proxy transaction and a second expiry date transaction, and in some embodiments the proxy output of the proxy transaction is three out of three, three out of four, including conditions requiring approval of three parties, two of four, etc. (e.g., where the assignee is delegated power of attorney and authorized to approve or sign on behalf of the payer). Many possible configurations are contemplated by the present invention. In such embodiments, the facilitator acts as a referee in creating agency transactions to the satisfaction of all parties, including maintaining the ability to contest transactions with selected intermediaries as described below. can act.
[0083]

For clarity of explanation in the figures, FIGS. 12 to 14 show that the output of the committed trade and the corresponding input of the proxy trade are the principal and collateral ((P+C) A) and the second collateral (CB). are shown separately as This is not a limitation of the invention. The output of the commit transaction and the input of the corresponding agency transaction may be any configuration deemed valid by the transfer mechanism. The output of the proxy transaction and the input to the second commit transaction are shown for illustrative purposes. All valid configurations of inputs and outputs are contemplated by this invention. In yet another embodiment, any fee may be paid in part or in whole by any party (even a fourth party).
[0084]

In a decentralized digital currency used as a transfer mechanism (e.g., Bitcoin protocol, Ethereum protocol, etc.), another embodiment of the present invention is that any swap, letter of credit, etc., where the terms indicated by the facilitator are expressed or Any offer that is understood can include its terms or a reference to its terms (such as a URL or hash of terms).

, etc.), if combinations etc. are encoded in the transaction record itself rather than outside the transaction mechanism (referred to as “off-blockchain” in decentralized digital transit) or in a central authority or shared decentralized data store (such as torrents or altcoins). , by submitting a special transaction record. [0085]

In one embodiment, this can be encoded as transaction record metadata and unused data for input or output (e.g., single output via <data> OP_DROP <script>, OP_RETURN <data> techniques, etc.). . For illustrative purposes, the steps below describe a few examples of such a variety of embodiments:1. In one embodiment, a first client (provider) creates an offer transaction record containing relevant data and an offer containing an offer amount and terms, optionally requiring approval by one of the first party and the facilitator. Create output. Associated data includes one or both of the conditions and references to the conditions. Optionally, the associated data includes a reference to the facilitator (eg, domain name, payment address, D&B number, URI, etc.). Optionally, the first client may review the terms, relevant data, and offer transaction record for verification (e.g., the facilitator may interpret the terms and the facilitator may properly to the facilitator to ensure they are identified). In another embodiment, at the request of the first client, the facilitator creates a first incomplete offer transaction record (e.g., does not include a signed entry) to create a completed offer transaction record, and the first Client optionally verifies availability of Facilitator-provided references (if applicable), etc., Facilitator accurately created open offer transaction records, etc. Example of an uncompleted offer transaction record: Table 19

```
% # Post the terms to the facilitator
% curl -X POST -d
'{"base":"USD","quote":"AUD","denom":"BTC","pcpl":0.5,"cltl":1.0,"res":
"symunbound","offerexp":"2014-06-01T00:00:00Z","swapexp":"2014-07-
01T00:00:00Z","facuri":"https://facilitator.dom/api/v1"}' ...
https://facilitator.dom/api/v1/swap
{"ok":true,"offersha256":"3a72...f9a4","offerref":"facswap:3a72...f9a4"
,"offeruri":"https://facilitator.dom/api/v1/swap/3a72...f9a4"}

      ID: 9fcd...429c

      ...

      Output:

            Value: 150000000

            scriptPubKey: 666163737761703a3a72...f9a4 OP_DROP 1
            67c1...4a70 cffd...1373 2 OP_CHECKMULTISIG

      ...
```

In this exemplary embodiment, the facilitator prefixes the condition hash with "666163 737761703a", which is the hexadecimal number of the 8-byte ASCII string "facswap:". This is not necessary, but if a transaction is of a certain "type"

It is a convenient means of recognition and aids in monitoring by network participants.
Example of an offer transaction record for another embodiment:

```
% # Post the terms to the facilitator
% curl -X POST -d '{"pubkey":"67c1...4a70","terms":
{"base":"USD",...,"facuri":"https://facilitator.dom/api/v1"}}' ...
https://facilitator.dom/api/v1/swap
{"ok":true,"offersha256":"3a72...f9a4","offerref":"facswap:3a72...f9a4"
,"offeruri":"https://facilitator.dom/api/v1/swap/3a72...f9a4","offertxn
":"04000000...0280d1f008000000008901014b67c1...4a704bcffd...13730102ae.
..0000000000000002a6a2866163737761703a3a72...f9a400000000"}
% # Validate "offertxn", add change outputs, etc.
```

"offertxn" is annotated as follows:

```
04000000 [version: 4] ... 02 [output count: 1] 80d1f00800000000
[amount: 1.5 BTC] 89 [script len: 137] 01 [push next 1 byte] 01 [1] 4b
[push next 75 bytes] 67c1...4a70 [pub. key] 4b [push next 75 bytes]
cffd...1373 [fac. pub. key] 01 [push next 1 byte] 02 [2] ae
[OP_CHECKMULTISIG] ... 0000000000000000 [amount: 0.0 BTC] 2a [script
len: 42] 6a [OP_RETURN] 28 [push next 40 bytes]
66616373776l703a3a72...f9a4 [offerref: "facswap:3a72...f9a4"] 00000000
[lock time: none]
```

Note that in some parts (such as inputs and placeholders) the ellipsis has been omitted to aid readability. In another embodiment, Pay-to-Script Hash (P2SH) is used to hide the output script that would normally be present in the parent transaction. In such embodiments, the actual output script is sent to the required participants via some other means. 2. In one embodiment, the first client creates an uncompleted committed transaction record and in another embodiment the facilitator creates a completed committed transaction record, and the first commit input is an offer transaction from an offer transaction. It is like the previous embodiment except that it is for receiving an amount and for receiving an amount from a source transaction for which a second input has not yet been found. 3. The first client creates a completed offer transaction record by signing the uncompleted offer transaction record and submits it to the transfer mechanism for executing the offer transaction.

.

4. A facilitator receives an offer deal from a transfer mechanism. 5. The second client sends the public key to the facilitator. 6. The facilitator adds the public key to the uncompleted committed transaction record and sends the first committed transaction record to the second client. 7. A second client signs the source transaction record with the transaction ID. 8. The second client adds the transaction ID to the pending commit transaction record and signs it. An example of an unfinished commit record transaction record:

[Table 21]

```
Input:

      Previous tx: 9fcd...429c

      Index: 0

      scriptSig: [sig. placeholder]

Input:

      Previous tx: b5e8...6f57

      Index: 6

      scriptSig: 9b6b...8f3701 ac2f...b01b

...

Output:

      Value: 149990000

      scriptPubKey: 2 67c1...4a70 dbe4...4cbe cffd...1373 3
      OP_CHECKMULTISIG

...
```

9. The second client sends the signed pending commit transaction record to the facilitator. 10. The first client and optionally (if permitted) the facilitator create and optionally secure a completed commit transaction record (ID: 6996...ec3d, etc.) by signing the incomplete commit transaction record. Store completed transaction records in memory. 11. The facilitator creates a pending refund or expiry transaction record and sends the pending refund or expiry transaction record to the second client. 12. The second client signs the pending refund or expiration transaction record and sends the signed pending refund or expiration transaction record to the facilitator. 13. The First Client and optionally (if permitted) the Facilitator create a completed refund or expiry transaction record by signing the refund transaction record and store the completed refund transaction or expiry transaction record in fixed memory. Store. 14. The facilitator sends a completed committed transaction record and a completed refund or completed expiry transaction record to the second client. 15. A second client submits the source transaction record to the transfer mechanism to execute the source transaction. 16. After confirming that the source transaction has been submitted, one, some, or all of the first client, the second client, and the facilitator submit a completed committed transaction record to the transfer mechanism for subsequent The process is similar to the previous embodiment.

[0086]

In another embodiment, the offer comprises a "hard offer", where the terms of offer output require approval by both the first party and the facilitator, the facilitator receiving a lock time set at a point in time and said offer amount. Requires input and first party approval

Sign and send to the First Party an Offer Expiration Transaction Record containing an Expiration Date output containing the expiration date and conditions to be applied. [0087]

In another embodiment of the invention, the parties to the transaction agree to have a third party act as a dispute mediator. For example, if a facilitator becomes unavailable, rather than opting to invoke a refund, one party creates a dispute in which the arbitrator stands in for the unavailable facilitator. The terms of the commit output of a commit transaction require approval from two of the first party, the second party, the facilitator, and the mediator. At the Expiry Timestamp or at a time defined by the Terms and before the Lock Time of the Completed Refund Transaction Record, the disputing party and the intermediary shall each sign, one party signing the first party, the second party , and submit a Dispute Transaction Record containing terms and dispute outputs requiring approval by two of the mediators. Once a dispute is resolved, the signatures of the parties, or the intermediary and one of the parties, will sign a payment transaction record similar to the payment transaction record described above, reflecting the mediated settlement. [0088]

Figures 15-16 show aspects of two such embodiments. The disputed transaction in Figure 15 has a first fee output containing the amount of the facilitator's fee (ÿ X) and a second fee output containing the amount of the mediator's fee (ÿ ÿ), a fee output shared between the parties, and the dispute initiated. Consists of the Settlement Transaction including mediator fees paid by Party (B). As shown in Figure 16, a dispute transaction includes a facilitator fee shared between the parties, and a settlement transaction includes a mediator fee paid by the party initiating the dispute (B). In another embodiment, any mediator fees are determined as settlement terms and included in the settlement transaction. [0089]

Optionally (and preferably) the parties sign and send a dispute reimbursement transaction record similar to that described above, instead taking input from the dispute transaction and establishing a sufficient locktime to reach settlement. . In this way, if the mediator becomes unavailable, the parties can resubmit the Dispute Reimbursement Transaction Record. In another embodiment, dispute resolution is “brokerable” and can allow chaining of disputes, e.g. naming a second broker if the broker becomes unavailable, and refunds are not possible. If the transaction record lock time is approaching, the arbitrator can extend the lock time. [0090]

In other embodiments, arbitration can be automated. For example, in embodiments involving swaps or similar transactions, the facilitator may periodically send an unsigned payment transaction record to the trader as if the transaction had been stopped at the time the unsigned payment transaction record was created. Send to An unsigned payment transaction contains a verifiable time at which it was created, or a reference to such time (e.g., if the transfer mechanism is Bitcoin or a similar protocol and embedded in one of the scripts). (e.g., a separate key owned by an unused signature data facilitator and not used to sign input). If the facilitator becomes unavailable prior to sending it to the parties, submitting a signed payment transaction record, or becoming unavailable past the expiration date, a dispute will be initiated between the parties and the terms and conditions and from the facilitator. There is a period of time to exchange some or all of the unsigned payment transaction records received by the mediator. (Preferably signed by each party, but not required if parties agree, i.e. send the same terms to the mediator). The Mediator will review unsigned or signed terms received from both parties and all verifiable unsigned payment transaction records. In another embodiment, the mediator simply selects the most recent verifiable unsigned payment transaction record. In another embodiment, the intermediary "plays" the unsigned payment transaction records in sequence and verifies whether the unsigned payment records would have caused the early termination of the transaction (e.g. , if one party's principal and collateral are exhausted). In yet another embodiment, the mediator requests information from one or more data sources and independently evaluates the conditions.

on behalf of the facilitator. It is created by the facilitator so that the mediator can decide to create a new young transaction that is as close as possible to the payment transaction record. [0091]

It should be noted that the illustrated embodiment is more basic of the invention. Source trades, commit trades, payout trades, refund trades, expiry trades, inputs, outputs, and various combinations of principal, collateral or fees are limited solely by the agreement between the participants and are enabled by the present invention. . Furthermore, certain steps of the embodiments disclosed throughout this application are described as being performed by certain entities. In other embodiments, similar or equivalent steps may be performed, in whole or in part, by different parties instead of or in addition to those described herein. All such embodiments are considered within the scope of the present invention.

[0092]
As a very simple example, in embodiments using decentralized digital currencies, transactions use P2SH instead of multi-signaling transactions. Other steps may be omitted in certain embodiments. For example, in embodiments using decentralized digital currencies, the creation of a signed completed refund or revoked transaction record is strongly recommended as a remedy to avoid loss in the event that the facilitator or counterparty disappears or becomes uncooperative. Recommended, but not strictly necessary. Dispute resolution records that are not signed in embodiments of the invention that include a mediator are created by the facilitator and sent to the parties for use with the mediator, for example when a refund transaction or expiry date transaction record is created and sent. be done.
[0093]
Figures 17-22 illustrate the major stages of value transfer in the form of swaps within one embodiment using a transfer mechanism that includes a decentralized digital currency, including blockchain. Figures 17 and 18 show the first stage, the client confirms the first order with the facilitator, including the first order (base security, quote security, principal, collateral, payment features, expiry timestamp, etc.). do. The client submits (broadcasts) a first principal transaction record that meets its terms to the Transfer Mechanism to create a first principal transaction. The facilitator monitors the blockchain for updates and activates the first order when the first principal transaction is confirmed. FIG. 19 illustrates the first and second principal trades by the facilitator matching the first order to the second order, creating a commit trade record and submitting (broadcasting) it to the transfer mechanism to generate a commit. shows the second stage of committing the output from . Optionally, the facilitator expends the output from the commit transaction to create and provide to each client a refund or "rollback" transaction record that cannot be used until after the expiration timestamp. In the event of a catastrophic failure of the facilitator, both clients may also sign and submit a refund transaction record, returning both clients to their original respective positions. FIG. 20 illustrates the third stage, in which the facilitator receives one or more values from a data source, applies payment functions to the value, principal, and collateral to monitor valuations and communicates to one party. Principal and collateral are exhausted. Optionally, each client receives status updates from the facilitator and independently receives status updates of the facilitator one or more values from the data source. Figures 21-22 also show that after the expiry timestamp (or if either party's principal and collateral are exhausted, whichever comes first), the facilitator spends the output of the committed trade on one or more Create a pending payment transaction record with one or more payment outputs, including the amount of the payment. Either client receives the completed payment transaction record, completes (signs) it, and creates a completed payment transaction record. To create a payment transaction, the client submits (broadcasts) a completed payment transaction record to the transfer transaction, releasing both client funds simultaneously. [0094]

FIG. 23 illustrates a typical implementation including a client (120) or facilitator (100).

Fig. 3 shows the components of the embodiment; It comprises a computer processor (160) coupled to a memory (170) and a network interface (190). The computer processor (160) is not limited to a single processing unit as shown, but may include multiple cores, multiple computer processors, clusters of networked computing devices, as known in the art. , a memory (170), and the like. Memory is also not limited to hard disks, but has fixed memory technology that allows data for files to be stored in separate logical sectors (180) (e.g., may contain more than one logical file). One or more logical records in a system, such as one or more logical records in a file or database), and the data can persist when the power supply to the computer processor is interrupted. Solid state storage, flash drives, RAID, JBOD, NA8, remote storage services like Amazon's S3, Google's cloud storage, memory cluster devices, etc. are examples of such combinations as are known in the art. not only For the client (120), the memory (170) comprises one or more logical sectors containing one or more key pair sectors for storing the asymmetric key pair (200). In the case of the facilitator (100), the memory (170) includes one or more key pair sectors (200) as well as one or more transaction record sectors for storing one or more transaction records. Contains one or more logical sectors. Network interface (190) is not limited to a single network interface as shown. Network interfaces include, but are not limited to, load balancers known in the art, two or more multiplexed network interfaces, or any combination thereof. be able to.

[0095]

Figure 24 (Prior Art) shows a simplified chain of ownership in a decentralized digital currency, but in reality a transaction can have multiple inputs and multiple outputs.

[Industrial Applicability]

This invention relates to agreements between separate parties considering the transfer of ownership, as well as to any industry in which this invention may be of value or importance.

[0097]

Explanation of Terms These are brief explanations of terms provided for convenience. It is not intended to be a limiting definition but supplement any feature, property, behavior, embodiment understood in the art or described elsewhere in this specification. be. [0098]

"Client" (120): A device for storing an asymmetric key pair comprising a computer processor (160) and a memory (170) having a sector (200) of the pair key, a network interface (190), and its book. It is configured to interact with at least one other client (120, 170) or facilitator (100) to facilitate value transfer via the inventive transfer mechanism (110).

For virtual currency, see "decentralized digital currency." [0100]

"Decentralized Digital Currencies" (150): Transfer Mechanisms (110) Including a Distributed Ledger of Transactions (such as the Bitcoin protocol and its offspring; often referred to as "blockchains") typically includes one or more network participants, including one or more miners. Also called "virtual currency".

[0101]

"Facilitator" (100): Transfer between a first party using a first client (120,160) and a second party using a second client (120,170).

A device (110) for facilitating value transfer via a transfer mechanism (110), the device storing, in accordance with the present invention, a computer processor (160), a transaction record sector, and an asymmetric key pair. and a memory (170) containing a network interface (190). [0102]

“Securities”: Any kind of thing of value that can be traded. It can be either cash, evidence of an ownership interest in an entity, or a contractual right to receive or provide cash or other financial instruments. Also called a "financial instrument". According to International Financial Reporting Standards, it is a “contract giving rise to the financial assets of one entity and the financial liabilities or equity securities of another entity”.
[0103]
"Lock Time": A timestamp containing a date and time, optionally including a time zone, that prevents a transaction from being accepted as valid by the transfer mechanism until the timestamp has passed.
[0104]

"Party": a legal entity that may exercise ownership rights. For example, an individual or a legal entity.
[0105]
“Publish transaction records to [device]”: Making transaction records available for reading and copying by devices, e.g. Transmit records or write transaction records so that they can be read or copied to devices as needed, optionally implementing authentication schemes that allow transaction records to be read and copied but not created, updated or destroyed. etc. Non-limiting examples include shared file systems (e.g., NFS, SSHFS, etc.), database APIs (e.g., SQL, REST, etc.), proprietary APIs, third-party shared storage (e.g., Google Docs, Dropbox, etc.).)and so on.

[0106]
"Submit Transaction Record to [Transfer Mechanism (110)]": refers to the process by which a valid transaction record is accepted by the Transfer Mechanism (110) to execute a transaction. In the context of decentralized digital currencies (150), typically a transaction record accepted by one or more miners containing transaction records in a valid block recognized as valid by a majority of network participants. including broadcasting transaction records to one or more network participants who have In the context of decentralized digital currencies (150), acceptance of transactions validated by multiple network participants is permanent and irreversible (e.g., attempts to spend already spent outputs etc. later found out by most of the network participants, thus invalidating the transaction record, etc.)

"Transaction": A unit of value transfer in a transfer mechanism (110) that recharacterizes the ownership or management of an asset (sometimes based on specific terms). In the context of decentralized digital currencies (150), this is sometimes referred to as a “confirmed transaction,” meaning a transaction record that has been approved by the majority ledger or blockchain of network participants. [0108]

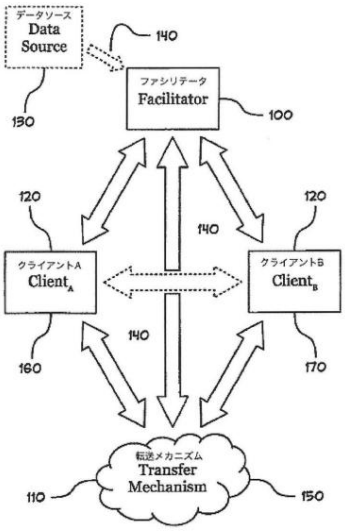
“Transaction Record”: A data structure that describes a transaction and is submitted to a transfer mechanism to execute the transaction. As a non-limiting example, in the context of decentralized digital currencies, transaction records typically have one or more inputs (zero inputs are possible in special cases), one or more outputs, and optionally Contains a cryptographic signature. In the context of decentralized digital currencies (150) this is also (sometimes incorrectly) called a “transaction”. For the avoidance of ambiguity, this specification uses “transaction record” to refer to the data structures that can be sent and received between network participants, and to the part of the ledger or block within the blockchain that contains transaction records. A book or block is accepted as valid by a majority of network participants (i.e., a "confirmed transaction"), using a "transaction" to do so.
[0109]

"Transfer Mechanism" (110): The means by which transactions (e.g. submission of successful transaction records) are created and enforced (e.g. decentralized digital currency).

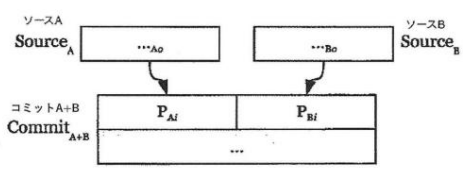
[0110]

"Value Transfer": The process of transferring rights (such as ownership, control, etc.) in things of economic value (money, goods, services, obligations to perform, etc.) between parties.

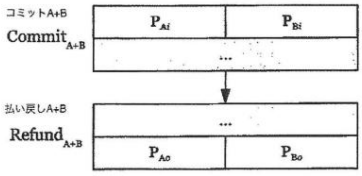
[Fig. 1]



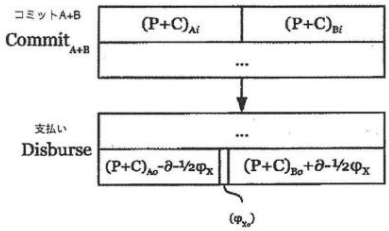
[Figure 2]



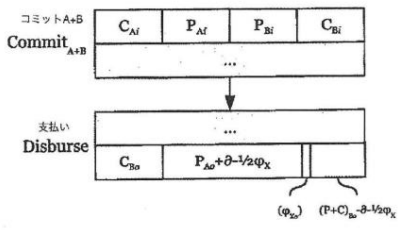
[Figure 3]



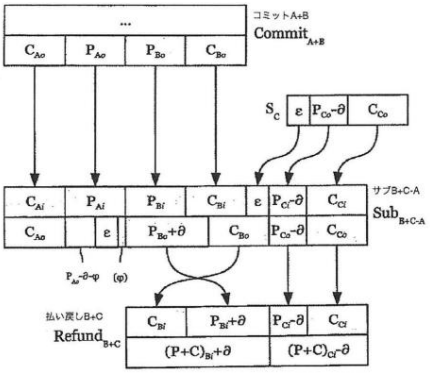
[Figure 4]



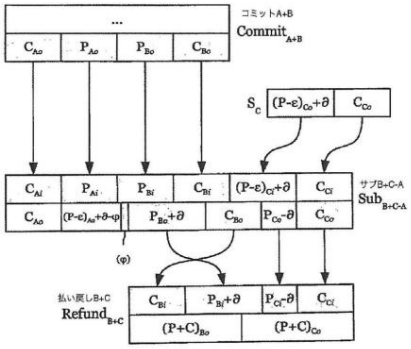
[Figure 5]



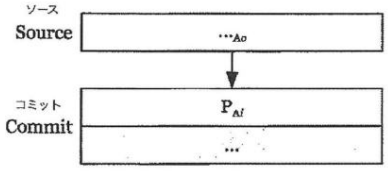
[Fig. 6]



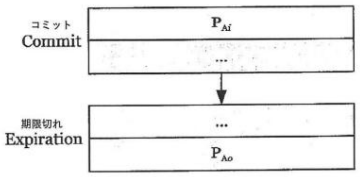
[Fig. 7]



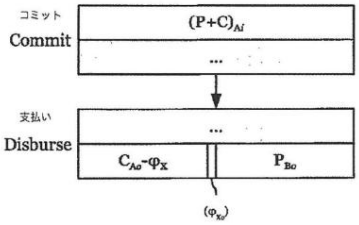
[Fig. 8]



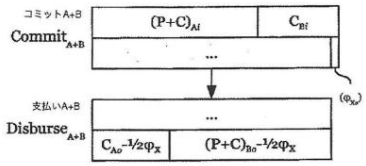
[Fig. 9]



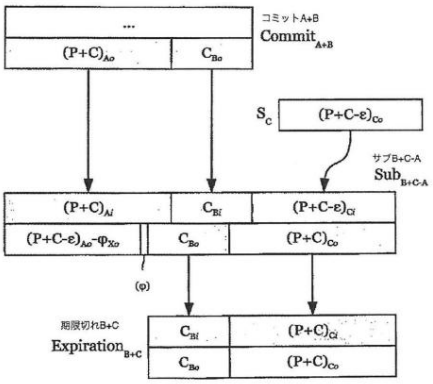
[Fig. 10]



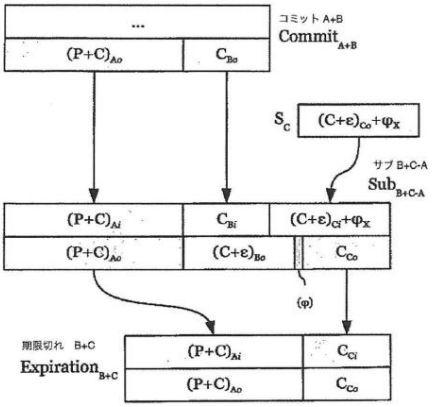
[Fig. 11]



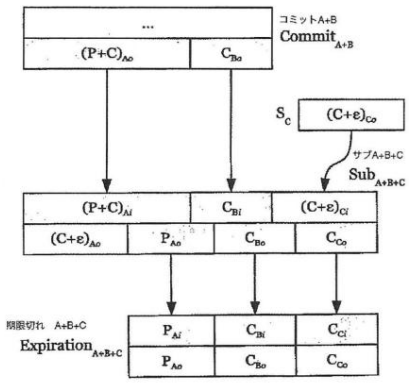
[Fig. 12]



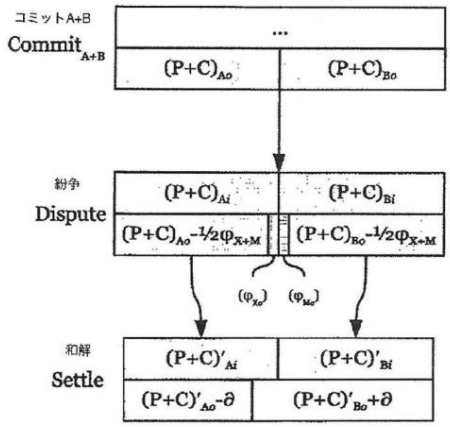
[Fig. 13]



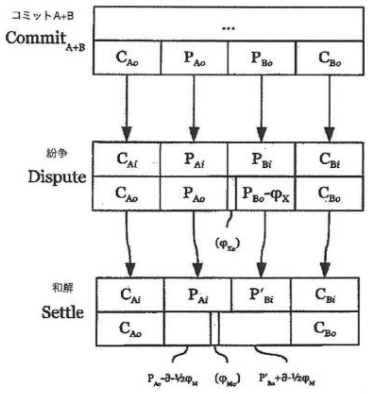
[Fig. 14]



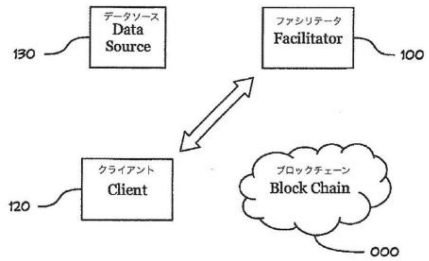
[Fig. 15]



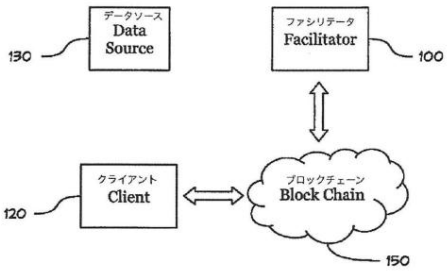
[Fig. 16]



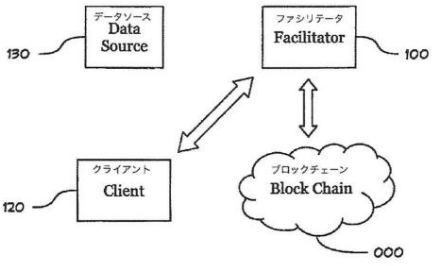
[Fig. 17]



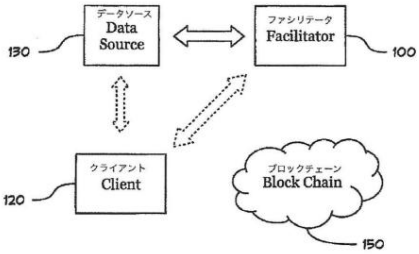
[Fig. 18]



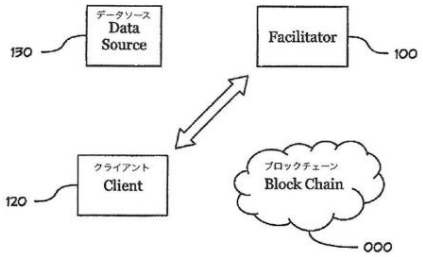
[Fig. 19]



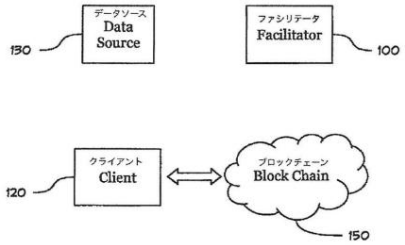
[Fig. 20]



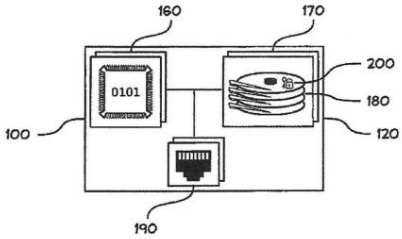
[Fig. 21]



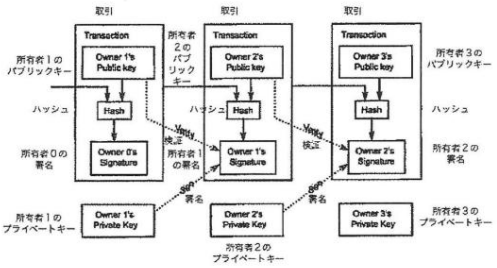
[Fig. 22]



[Fig.23]



[Fig.24]



continuation of the front page

Examiner Hirofumi Seki

(56) References JP 2002-230448 (JP, A) JP 06-162059 (JP, A)
US Patent No. 07546275 (US, B1) International Publication No.
2013/127713 (WO, A1)

(58) Investigated field (Int.Cl., DB
name) G06Q 10/00-99/00