(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2020-99066
(P2020-99066A)
(43)公開日　令和2年6月25日(2020.6.25)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675B	5L055
G09C 1/00	(2006.01)	G09C	1/00	640D	
G06F 21/64	(2013.01)	G06F	21/64		
G06Q 20/38	(2012.01)	G06Q	20/38	310	

審査請求 有　請求項の数 14　ＯＬ　外国語出願　（全 37 頁）

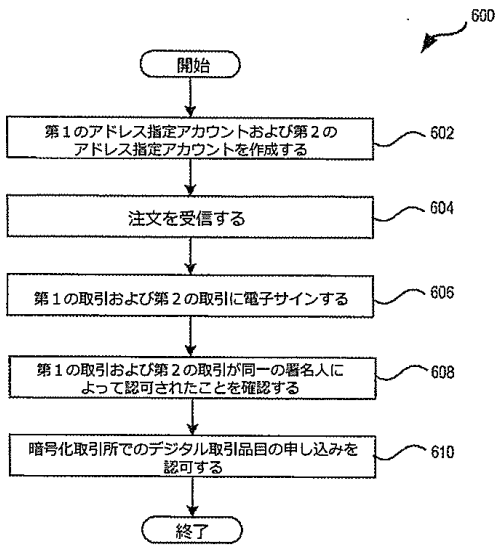
(21)出願番号　特願2020-17696(P2020-17696)
(22)出願日　令和2年2月5日(2020.2.5)
(62)分割の表示　特願2017-559778(P2017-559778)の分割
原出願日　平成28年2月5日(2016.2.5)
(31)優先権主張番号　62/113,931
(32)優先日　平成27年2月9日(2015.2.9)
(33)優先権主張国・地域又は機関
米国(US)

(71)出願人　517276376
ティーゼロ・グループ，インコーポレーテッド
アメリカ合衆国ユタ州８４０４７，ミッドベール，ウエスト・コロシアム・ウェイ７９９
(74)代理人　100118902
弁理士　山本　修
(74)代理人　100106208
弁理士　宮前　徹
(74)代理人　100120112
弁理士　中西　基晴
(74)代理人　100162846
弁理士　大牧　綾子

最終頁に続く

(54)【発明の名称】暗号化統合プラットフォーム

(57)【要約】　（修正有）
【課題】デジタル取引品目を商取引するためのシステム、方法及び構成を提供する。
【解決手段】デジタル取引品目を商取引するプロセスにおいて、各々が共通の識別子を有し、かつ、各々がある１人の顧客に関連付けられる、第１及び第２のアドレス指定アカウントを作成する。システムは、第１のアドレス指定アカウントに関連付けられたデジタル取引品目を売買するための注文を受信する。注文が共通の識別子に関連付けられ、第１のアドレス指定アカウントに関連付けられたプライベートキーを使用して、第１の取引に電子サインする。第１のアドレス指定アカウントから第２のアドレス指定アカウントへデジタル取引品目を転送する。同一のプライベートキーを第２の取引に電子サインするために使用し、第１の取引が、第１の取引と同一のプライベートキーを使用してサインされたことを確認した後に、システムは、暗号化取引所での注文の申し込みを認可する。
【選択図】図６



【特許請求の範囲】
【請求項１】
コンピュータによって、各々が共通の識別子を有し、かつ各々がある１人の第１の顧客に関連付けられる、第１のアドレス指定アカウントおよび第２のアドレス指定アカウントを作成するステップと、
リモートのコンピュータデバイスから、前記第１のアドレス指定アカウントに関連付けられた１つまたは複数のデジタル取引品目を売買するための注文を受信するステップであって、前記注文が前記共通の識別子に関連付けられている、ステップと、
前記第１のアドレス指定アカウントに関連付けられたプライベートキーを使用して、第１の取引に電子サインし、前記第１のアドレス指定アカウントから前記第２のアドレス指定アカウントへ前記１つまたは複数のデジタル取引品目を転送するステップと、
前記第１のアドレス指定アカウントに関連付けられた前記プライベートキーを使用して、第２の取引に電子サインするステップと、
前記第１の取引が、前記第２の取引と同一のプライベートキーを使用してサインされたことを確認するステップと、
暗号化取引所での前記注文の申し込みを、前記第１の取引が、前記第２の取引と同一のプライベートキーを使用してサインされたことの確認に基づいて、認可するステップとを含む、コンピュータ化された方法。
【請求項２】
前記第２のアドレス指定アカウントが、第２の公開キーおよび第２のプライベートキーを含む第２のキーペアに関連付けられる、請求項１に記載のコンピュータ化された方法。
【請求項３】
分散化された台帳から、前記注文に関連付けられた前記１つまたは複数のデジタル取引品目が、前記第１の公開キーを使用することによって前記第１のアドレス指定アカウントに関連付けられることの確認を受信するステップと、
前記注文に関連付けられた前記１つまたは複数のデジタル取引品目が、前記第１のアドレス指定アカウントに関連付けられることの確認の受信に基づいて、前記第１の取引および前記第２の取引を作成するステップとをさらに含む、請求項１に記載のコンピュータ化された方法。
【請求項４】
分散化された台帳に、前記第１のアドレス指定アカウントおよび前記第２のアドレス指定アカウントとの残高を通知するステップをさらに含む、請求項１に記載のコンピュータ化された方法。
【請求項５】
前記注文が、デジタル資産またはデジタル負債を取得するための注文である、請求項１に記載のコンピュータ化された方法であって、
前記リモートのコンピュータデバイスから、資本金で前記デジタル資産または前記デジタル負債を取得できることを示す情報を受信するステップであって、前記１つまたは複数のデジタル取引品目が、前記資本金のデジタル表現である、ステップと、
前記資本金の前記デジタル表現を、前記１つまたは複数のデジタル取引品目として、前記第１のアドレス指定アカウントに関連付けるステップとをさらに含む、コンピュータ化された方法。
【請求項６】
前記注文が、前記１つまたは複数のデジタル取引品目を売却するための注文であって、前記１つまたは複数のデジタル取引品目が、１つまたは複数のデジタル資産または１つまたは複数のデジタル負債である、請求項１に記載のコンピュータ化された方法であって、
前記リモートのコンピュータデバイスから、前記１つまたは複数のデジタル資産に対応した資産、または前記１つまたは複数のデジタル負債に対応した負債が、売却できることを示す情報を受信するステップをさらに含む、コンピュータ化された方法。
【請求項７】

第３のアドレス指定アカウントを作成するステップをさらに含む、請求項１に記載のコンピュータ化された方法であって、前記第３のデジタルアドレス指定アカウントが、前記第１のアドレス指定アカウントに関連付けられた第１のキーペアと、前記第２のアドレス指定アカウントに関連付けられた第２のキーペアとを含む、コンピュータ化された方法。

【請求項８】

前記第１の取引を作成するステップであって、前記第１の取引が、前記１つまたは複数のデジタル取引品目、前記識別子、および前記第２のアドレス指定アカウントの公開キーのうちの少なくとも１つを含む、ステップと、

前記第１の取引のハッシュを作成するステップと、

前記第２の取引を作成するステップであって、前記第２の取引が、前記注文のタイプ、前記識別子、前記第２のアドレス指定アカウントの公開キー、および前記第１の取引の前記ハッシュのうちの少なくとも１つを含む、ステップとをさらに含む、請求項１に記載のコンピュータ化された方法。

【請求項９】

前記暗号化取引所へ前記第１の取引を送信するステップと、

代替の商取引システムへ前記第２の取引を送信するステップとをさらに含む、請求項１に記載のコンピュータ化された方法。

【請求項１０】

前記注文が前記暗号化取引所での第２の注文にマッチしたことの通知を受信するステップと、

実行報告を作成するステップとをさらに含む、請求項９に記載のコンピュータ化された方法。

【請求項１１】

前記第１のアドレス指定アカウントが、顧客ポートフォリオアカウントであり、前記第２のアドレス指定アカウントが、顧客委託アカウントである、請求項１に記載のコンピュータ化された方法。

【請求項１２】

前記第１の取引が、前記第１の取引の額に対応した総額内の資本金または前記第１の取引の前記額に対応した前記総額内の前記資本金の表示、および前記第１のアドレス指定アカウントの公開キーのうちの少なくとも１つを含み、前記第２の取引が、前記第２のアドレス指定アカウントの公開キー、前記注文のタイプ、前記識別子、前記第２のアドレス指定アカウントの公開キー、および前記第１の取引のハッシュのうちの少なくとも１つを含む、請求項１に記載のコンピュータ化された方法。

【請求項１３】

ブローカディーラから、買入取引と売却取引をマッチさせる要求を受信するステップであって、

前記買入取引が、前記１つまたは複数のデジタル取引品目の額に対応した総額で前記１つまたは複数のデジタル取引品目を取得するための買入注文を含み、前記売却取引が、前記総額で前記１つまたは複数のデジタル取引品目を売却するための売却注文を含み、

前記買入取引が、前記買入注文を識別する第１のアドレス指定アカウントに対応した関連付けられた第１のサインを有し、前記売却取引が、前記売却注文を識別する第２のアドレス指定アカウントに対応した関連付けられた第２のサインを有し、前記第１のアドレス指定アカウントが、第１の顧客に関連付けられ、前記第２のアドレス指定アカウントが、第２の顧客に関連付けられ、

前記総額が、前記第１の顧客に関連付けられた第３のアドレス指定アカウントに関連付けられ、前記１つまたは複数のデジタル取引品目が、前記第２の顧客に関連付けられた第４のアドレス指定アカウントに関連付けられる、ステップと、

コンピュータによって、前記買入取引を前記第３のアドレス指定アカウントへ、前記売却取引を前記第４のアドレス指定アカウントへマッピングするステップと、

暗号化取引所へ、前記買入取引を委託するために前記第１のサインおよび前記第２のサ

インを含むマッチ要求回答を送信するステップと、
前記買入取引および前記売却取引を確定し、清算するために、前記第１のアドレス指定アカウントへ前記１つまたは複数のデジタル取引品目を転送し、前記第２のアドレス指定アカウントへ前記総額を転送するステップとを含む、コンピュータ化された方法。
【請求項１４】
分散化された台帳から、前記マッチ要求回答を送信する前に、前記総額が、前記第３のアドレス指定アカウントに関連付けられ、前記１つまたは複数のデジタル取引品目が、前記第４のアドレス指定アカウントに関連付けられている確認を受信するステップをさらに含む、請求項１３に記載の方法。
【請求項１５】
前記１つまたは複数のデジタル取引品目が、１つまたは複数のデジタル資産またはデジタル負債を含み、前記総額が、前記１つまたは複数のデジタル取引品目の額に対応した通貨、暗号化通貨、または前記通貨もしくは前記暗号化通貨の表示の総額を含む、請求項１３に記載のコンピュータ化された方法。
【請求項１６】
リモートのコンピュータデバイスへ、前記買入取引および前記売却取引を確定、清算した結果を公表するステップをさらに含む、請求項１３に記載のコンピュータ化された方法。
【請求項１７】
前記第１のサインが、前記第１のアドレス指定アカウントに関連付けられたプライベートキーであり、前記第２のサインが、前記第２のアドレス指定アカウントに関連付けられたプライベートキーである、請求項１３に記載のコンピュータ化された方法。
【請求項１８】
前記第１のアドレス指定アカウントが、前記第１の顧客に関連付けられた顧客ポートフォリオアカウントであり、
前記第２のアドレス指定アカウントが、前記第２の顧客に関連付けられた顧客ポートフォリオアカウントであり、
前記第３のアドレス指定アカウントが、前記第１の顧客に関連付けられた顧客委託アカウントであり、
前記第４のアドレス指定アカウントが、前記第２の顧客に関連付けられた顧客委託アカウントである、請求項１３に記載のコンピュータ化された方法。
【請求項１９】
少なくとも１つのプロセッサと、
少なくとも１つのコンピュータ可読記憶媒体であって、命令が、そこに格納され、前記少なくとも１つのプロセッサによって実行されるとき、前記暗号化統合システムに、
第１のアドレス指定アカウントに関連付けられた１つまたは複数のデジタル取引品目のための商取引を実行する注文を受信するステップであって、前記注文、前記第１のアドレス指定アカウント、および第２のアドレス指定アカウントは、ある１つの識別子に関連付けられた、ステップと、
前記第１のアドレス指定アカウントから前記第２のアドレス指定アカウントへ前記１つまたは複数のデジタル取引品目を転送する第１の取引を発生させるステップと、
前記注文を含む第２の取引を発生させるステップと、
前記第１の取引が、前記第２の取引と同一の署名人によって認可されたことを確認するステップと、
前記第１の取引が、前記第２の取引と同一の署名人によって認可されたことを確認した後に、暗号化取引所での前記注文の申し込みを認可するステップとを実行させる、少なくとも１つのコンピュータ可読記憶媒体とを備える、暗号化統合システム。
【請求項２０】
前記第１の取引および前記第２の取引が、同一のキーによってサインされたとき、前記第１の取引が、前記第２の取引と同一の署名人によって認可される、請求項１９に記載の

暗号化統合システム。
【請求項２１】
前記キーが、前記第１のアドレス指定アカウントのプライベートキーであり、前記第２の取引が、前記第１の取引のハッシュを含む、請求項２０に記載の暗号化統合システム。
【請求項２２】
前記命令が、前記少なくとも１つのプロセッサによって実行されるとき、前記暗号化統合システムに、
前記暗号化取引所から、前記注文と第２の注文をマッチさせる要求を受信するするステップであって、前記第２の注文が、第２の識別子に関連付けられている、ステップと、
前記注文を確定し、清算するために、前記１つまたは複数のデジタル取引品目を前記第２の識別子に関連付けられたアドレス指定アカウントへ転送し、１つまたは複数の他のデジタル取引品目を前記第１のアドレス指定アカウント内に転送するステップとをさらに実行させる、請求項１９に記載の暗号化統合システム。
【請求項２３】
前記暗号化取引所へ前記第１の取引を送信するステップと、
代替の商取引システムへ前記第２の取引を送信するステップとに適合する、暗号化アダプタ構成要素をさらに備える、請求項１９に記載の暗号化統合システム。
【請求項２４】
１つまたは複数のプロセッサによって実行されるとき、装置に、
各々が共通の識別子を有し、かつ各々がある１人の第１の顧客に関連付けられる、第１のアドレス指定アカウントおよび第２のアドレス指定アカウントを作成するステップと、
前記第１のアドレス指定アカウントに関連付けられた１つまたは複数のデジタル取引品目を売買するための注文を受信するステップであって、前記注文が前記共通の識別子に関連付けられている、ステップと、
前記第１のアドレス指定アカウントに関連付けられたプライベートキーを使用して、第１の取引に電子サインし、前記第１のアドレス指定アカウントから前記第２のアドレス指定アカウントへ前記１つまたは複数のデジタル取引品目を転送するステップと、
前記第１のアドレス指定アカウントに関連付けられた前記プライベートキー、第２の取引に電子サインするステップと、
前記第１の取引が、前記第２の取引と同一のプライベートキーを使用してサインされたことを確認するステップと、
暗号化取引所での前記注文の申し込みを、前記第１の取引が、前記第２の取引と同一のプライベートキーを使用してサインされたことの確認に基づいて、認可するステップとを実行させる、命令のセットを含む非一時的コンピュータ可読記憶媒体。
【請求項２５】
１つまたは複数のプロセッサによって実行されるとき、装置に、
ブローカディーラから、買入取引と売却取引をマッチさせる要求を受信するステップであって、
前記買入取引が、前記１つまたは複数のデジタル取引品目の額に対応した総額で前記１つまたは複数のデジタル取引品目を取得するための買入注文を含み、前記売却取引が、前記総額で前記１つまたは複数のデジタル取引品目を売却するための売却注文を含み、
前記買入取引が、前記買入注文を識別する第１のアドレス指定アカウントに対応した関連付けられた第１のサインを有し、前記売却取引が、前記売却注文を識別する第２のアドレス指定アカウントに対応した関連付けられた第２のサインを有し、前記第１のアドレス指定アカウントが、第１の顧客に関連付けられ、前記第２のアドレス指定アカウントが、第２の顧客に関連付けられ、前記総額が、前記第１の顧客に関連付けられた第３のアドレス指定アカウントに関連付けられ、前記１つまたは複数のデジタル取引品目が、前記第２の顧客に関連付けられた第４のアドレス指定アカウントに関連付けられる、ステップと、
前記買入取引を前記第３のアドレス指定アカウントへ、前記売却取引を第４のアドレス

指定アカウントへマッピングするステップと、
暗号化取引所へ、前記買入取引を委託するために前記第１のサインおよび前記第２のサインを含むマッチ要求回答を送信するステップと、
前記買入取引および前記売却取引を確定し、清算するために、前記第１のアドレス指定アカウントへ前記１つまたは複数のデジタル品目を転送し、前記第２のアドレス指定アカウントへ前記総額を転送するステップとを実行させる命令のセットを含む、非一時的コンピュータ可読記憶媒体。
【発明の詳細な説明】
【発明の詳細な説明】
【０００１】
関連出願の相互参照
[0001]本出願は、その全体があらゆる目的のために、参照により本明細書に組み込まれる、「ＣＲＹＰＴＯ　ＩＮＴＥＧＲＡＴＩＯＮ　ＰＬＡＴＦＯＲＭ（暗号化統合プラットフォーム）」と題する、２０１５年２月９日に出願された米国仮出願第６２／１１３，９３１号、の優先権および利益を主張する。
【技術分野】
【０００２】
[0002]本開示の多様な実施形態は、一般に商取引に関する。より具体的には、本開示の多様な実施形態は、分散化され、暗号化された（「ｃｒｙｐｔｏ」）技法を使用して、資産、負債、商品、および／または通貨などのデジタル取引品目（digital transactional items）を商取引するためのシステムおよび方法に関する。
【背景技術】
【０００３】
[0003]最近は世界中で暗号化通貨（たとえば、ビットコイン）の採用が増加しており、該増加は、既存の商取引システムに課題を発生させている。たとえば、市場のデータと所有権データとは、別々に格納される。さらに、既存の商取引システムは、デジタル取引品目を商取引する商取引システムと互換性のない、商取引前通信および実行のためのプロトコルを使用する。
【発明の概要】
【課題を解決するための手段】
【０００４】
[0004]本開示は、既存の商取引システムのこれらおよびその他の制限を解決し、その他の利益を提供するが、以下の説明によって当業者にはより明確になるであろう。
[0005]本開示の実施形態は、添付図面の使用によって示され、説明される。
【図面の簡単な説明】
【０００５】
【図１】[0006]本開示の多様な実施形態によるネットワークベースの操作環境の一例を示す図である。
【図２】[0007]本開示の１つまたは複数の実施形態による暗号化統合プラットフォーム内の構成要素セットを示す図である。
【図３】[0008]デジタル取引品目の商取引で使用される構成要素の相互作用を示す図である。
【図４】[0009]暗号化統合プラットフォームの構造を示す図である。
【図５】[0010]ブローカディーラ（broker-dealer）の観点からのデジタル取引品目を商取引するプロセスを示すフローチャートである。
【図６】[0011]デジタル取引品目を商取引するプロセスを示すフローチャートである。
【図７】[0012]デジタル取引品目を商取引するプロセスを示すフローチャートである。
【図８】[0013]顧客がデジタル取引品目を商取引できるようにするために暗号化統合プラットフォームに顧客を統合するプロセスを示す図である。
【図９】[0014]デジタル取引品目を商取引する注文を作成するプロセスを示す図である。

【図１０】[0015]デジタル取引品目を取得する(purchase)注文を受信し、処理するプロセスを示す図である。
【図１１】[0016]デジタル取引品目を売却する注文を受信し、処理するプロセスを示す図である。
【図１２】[0017]デジタル取引品目を売却または取得する取引を取り消すプロセスを示す図である。
【図１３】[0018]デジタル取引品目の取得または売却の取引を確定し、清算するプロセスを示す図である。
【図１４】[0019]本開示のいくつかの実施形態が利用され得るコンピュータシステムの一例を示す図である。
【発明を実施するための形態】
【０００６】
[0020]本開示の多様な実施形態は、一般にデジタル取引品目の商取引に関し、より詳細には、有価証券などのデジタル資産に関する。より具体的には、本開示の多様な実施形態は、分散化され、暗号化された技法、および詳細には暗号化統合プラットフォームを使用してデジタル有価証券を商取引するためのシステムおよび方法に関する。暗号化統合プラットフォームは、暗号化（「ｃｒｙｐｔｏ」）売買（すなわち、デジタル取引品目を商取引する売買）に基づいて、デジタル資産、負債商品、および／または通貨（たとえば、デジタル有価証券、有価証券のデジタル利息、暗号化通貨）などのデジタル取引品目を、資本金のデジタル表現（たとえば、トークン、現金、暗号化通貨などの現金等価物）などの他のデジタル取引品目と商取引する注文をブローカディーラから受信し、その注文を暗号化注文へと変換する。
【０００７】
[0021]暗号化統合プラットフォームは、暗号化取引所から市場情報を収集し、取引に関わるデジタル資産または負債の暗号化市場での最良の価格を検索するルータとしてはたらく。マッチング注文の前に、暗号化統合プラットフォームは、デジタル取引品目（すなわち、買入注文のための資本金、および売却注文のためのデジタル資産または負債）の両方を確保し、取引へ暗号化サインする。マッチング可能性のある注文がいったん検索され、暗号化統合プラットフォームは、資本金およびデジタル資産／負債が、商取引に利用可能であることを確認し（たとえば、買主および売主によって所有されるアドレス指定アカウントに関連付けられる）、資本金およびデジタル資産または負債を対応するアドレス指定アカウントに関連付けることによって取引を即時に清算し、確定する。
【０００８】
[0022]暗号化統合プラットフォームの利点は、保証された確定、所有権の透明性および容易な金銭の移動、ならびに確実な確定を含む。取引へ暗号化サインすることは、認証、権限付与、および来歴を保証する。
【０００９】
[0023]暗号化統合プラットフォームは、他のもの中でも、従来の商取引システムとデジタル取引品目を商取引する暗号化取引所との間のインタフェースを提供する。それを実行する際、暗号化統合プラットフォームは、ブローカディーラ、代替商取引システム（ＡＴＳ）、および取引所間の、商取引および通信用のプロトコルを使用し、暗号化技法を利用して商取引が完了できるようにメッセージを変換する。たとえば、１つのプロトコルが、財務情報交換プロトコル、すなわち「ＦＩＸ」プロトコルである。暗号化統合プラットフォームによって、ブローカディーラは、本明細書で説明したテクノロジーを従来の商取引システムの最後尾に統合することができ、従来の商取引システムが暗号化取引所で使用できる。したがって、暗号化統合プラットフォームによって、より多くの企業が、資本金を利用する機会を享受できるようになり、より多くの投資家が、参加企業の株を利用する機会を享受できるようになる。ＦＩＸプロトコルでのメッセージは、本開示内の多くの実施例で使用される。しかし、暗号化統合プラットフォームは、ＦＩＸプロトコル以外のプロトコルでのメッセージを受信し、変換することができ、暗号化技法を使用して完了するこ

とができる。

【００１０】

[0024]暗号化統合プラットフォームは、暗号化台帳または分散化された台帳（たとえば、ブロックチェーン（ｂｌｏｃｋ　ｃｈａｉｎｓ））を使用して、売買されようとしているデジタル取引品目の所有権および可用性を確認する。暗号化統合プラットフォームまたはその構成要素は、有価証券発行人によって、有価証券の新規公募および他の証券取引委員会（ＳＥＣ）登録の公募を処理するために使用されてもよいし、一般人によって、流通市場取引でそれらの有価証券を商取引するために使用されてもよい。

【００１１】

[0025]暗号化取引所で商取引されるデジタル取引品目は、当技術分野でよく知られている公開キー暗号化法および双方向暗号化などの暗号化技法を使用する他の所有者へ、転送されてもよい。公開キー暗号化法は、ある１つのキーペアを必要とし、この２つのキーは、正確にリンクされる。１つのキーは、公開キーであり、ピアツーピアネットワークにおいてノード間で自由に共有される。他方のキーは、プライベートキーであり、公開共有されない。公開キーは、普通文を暗号化するために、またデジタルサインを確認するために使用される。プライベートキーは、暗号化文を復号化するために、また取引にデジタルサインするために使用される。取引メッセージは、送信者の同一性を認証するために送信者のプライベートキーによってデジタルサインされてもよい。次に、送信者のデジタルサインされた取引メッセージは、送信者が取引の開始者であることを確認するために、送信者の公開キーを使用して復号化されてもよい。

【００１２】

[0026]デジタル取引品目の所有権は、ネットワークノードによって維持される分散化された台帳内の所有権登記に基づいてもよい。分散化された台帳（たとえば、ビットコインのブロックチェーン）は、各デジタル取引品目の所有権の各変化のための登記を記録し、キーペアに正確にリンクされてもよい。デジタル資産またはデジタル負債を売却するために、取引メッセージは（たとえば、パケットまたは他のデータ構造で）、ピアツーピアネットワークでノードに配信されてもよい。取引メッセージは、売主のプライベートキーで、サインすることができ、デジタル資産またはデジタル負債の表題の連鎖の履歴、転送される株または品目の数、および取得者の公開キーに基づくアドレスなどの情報を含んでもよい。ネットワーク内のノードの大部分が、送信者が表題の適切な連鎖を有することに同意するとき、所有権は、取得者に変えられ、台帳は、取引を表示するために更新される。

【００１３】

[0027]暗号化商取引システム（すなわち、暗号化取引所においてデジタル資産または負債を商取引するシステム）を従来の商取引システムへ統合化することは、本開示が議論する課題を発生させる。たとえば、本開示は、デジタル資産または負債を商取引するための注文が従来のシステムによって提出されるプロセスを導入する。別の実施例では、本開示は、元々従来のシステム内へ収容された暗号化商取引注文が、元々の注文と同一の存在（entity）によって認可されることを保証するプロセスを紹介する。さらに、本開示は、非共有プライベートキーおよび共有公開キーに基づいた暗号化取引をマッチ（match）させるためのシステムおよび方法を導入する。

【００１４】

[0028]本明細書で導入される技法は、特定目的のハードウェア（たとえば回路）として、ソフトウェアおよび／またはファームウェアを使用して適切にプログラムされたプログラマブル回路として、あるいは特定目的およびプログラマブル回路の組合せとして、実施されることができる。したがって、実施形態は、プロセスを実行するようにコンピュータ（または他の電子装置）をプログラムするために使用し得る命令を内部に格納した機械可読媒体を含んでもよい。機械可読媒体は、たとえば、フロッピーディスク、光ディスク、コンパクトディスク読み出し専用メモリ（ＣＤ－ＲＯＭ）、磁気光ディスク、読み出し専用メモリ（ＲＯＭ）、ランダムアクセスメモリ（ＲＡＭ）、消去可能プログラム可能読み出し専用メモリ（ＥＰＲＯＭ）、電子的消去可能プログラム可能読み出し専用メモリ（Ｅ

ＥＰＲＯＭ）、磁気もしくは光カード、フラッシュメモリ、または電子命令を格納するのに適した他のタイプの媒体／機械可読媒体を含んでもよい。

【００１５】

[0029]図１は、本開示のいくつかの実施形態が使用され得る、ネットワークベースの操作環境１００の一例を示す。図１に示すように、操作環境１００は、１つまたは複数のコンピュータデバイス１１０Ａ～１１０Ｍ（携帯デバイス、携帯電話、タブレットコンピュータ、携帯型媒体デバイス、携帯ゲームデバイス、車両ベースコンピュータ、専用端末、公開端末、デスクトップまたはラップトップコンピュータ、キオスクなど）上で実行されているアプリケーション１０５Ａ～１０５Ｎを含む。いくつかの実施形態では、アプリケーション１０５Ａ～１０５Ｎは、注文を発生させること、およびコンピュータデバイス上に格納されまたは遠隔地に格納され得るアカウント残高をチェックすることなどの、操作を実行するために使用される。これらのコンピュータデバイスは、ネットワーク１２０を介して暗号化統合プラットフォーム１２５およびブローカディーラ１１５に接続することによって通信データを受信および送信するための機構を含むことができる。

【００１６】

[0030]コンピュータデバイス１１０Ａ～１１０Ｍは、ネットワーク１２０を介してブローカディーラ１１５および暗号化統合プラットフォーム１２５と通信するように構成される。いくつかの実施形態では、コンピュータデバイス１１０Ａ～１１０Ｍは、暗号化統合プラットフォーム１２５に情報を回収または提出することができ、暗号化統合プラットフォーム１２５およびブローカディーラ１１５によって回収されたカスタマイズされたコンテンツを有する１つまたは複数のアプリケーションを実行する。たとえば、コンピュータデバイス１１０Ａ～１１０Ｍは各々、ブラウザアプリケーションまたはカスタマイズされたクライアントを実行して、コンピュータデバイス１１０Ａ～１１０Ｍの間での、ならびに暗号化統合プラットフォーム１２５およびブローカディーラ１１５の間の対話を可能にする。

【００１７】

[0031]ブローカディーラ１１５は、彼ら自身のアカウントのために、または彼らの顧客の代理で、資産（たとえば、有価証券、投資信託など）を商取引するビジネスに従事する存在（すなわち、実在する人間、企業、または他の組織）である。顧客の代理で注文の商取引を実行するとき、その存在はブローカとして振る舞う。それ自身のアカウントでの商取引を実行するとき、その存在はディーラとして振る舞う。ブローカディーラ１１５は、コンピュータデバイス１１０Ａ～１１０Ｍで注文を受信してもよく、彼ら自身の注文を作成してもよい。ブローカディーラ１１５は注文を、ネットワーク１２０を通して暗号化統合プラットフォーム１２５へ通知してもよい。ブローカディーラ１１５によって送信される注文は、ＦＩＸプロトコル、あるいは他のプロトコルおよび／またはフォーマットを使用してもよい。

【００１８】

[0032]暗号化統合プラットフォーム１２５は、１つまたは複数のサーバ上で実行されてもよく、デジタル取引品目の商取引に使用され得る。いくつかの実施形態では、図に示すように、暗号化統合プラットフォーム１２５は、暗号化アダプタ１３０、暗号化ブリッジ１３５、および暗号化マッチング構成要素１４０を含む。

【００１９】

[0033]暗号化アダプタ１３０は、ブローカディーラ１１５から、およびいくつかの実施形態では直接コンピュータデバイス１１０Ａ～１１０Ｍから、デジタル取引品目を商取引するための注文を受信する。注文は、一般にブローカディーラ１１５によって使用される従来のプロトコル／フォーマットで暗号化アダプタ１３０によって受信される（たとえば、ＦＩＸメッセージ）。暗号化アダプタ１３０は、注文を暗号化取引へ変換し、暗号化台帳１６０を使用して注文の資産および資本金の所有権を確認し、暗号化取引に暗号化サインして資産および資本金を転送し、暗号化取引が同一の顧客によって認可されたことを確認し、ＦＩＸ注文を認可する。暗号化ブリッジ１３５は、暗号化取引所１５５からブロー

カディーラ１１５へ、市場データを収集し、提供する。暗号化マッチング構成要素１４０は、デジタル資産の買入および売却注文をマッチさせ、注文を実行し、ブローカディーラ１１５へ既存のブローカディーラのフォーマットで実行報告を返信する。したがって、暗号化統合プラットフォーム１２５が、現在のブローカディーラ１１５の操作にシームレスに統合され、ブローカディーラ１１５は、公開またはプライベートキー、台帳、およびブロックチェーンの知識を持たずに、暗号化取引所１５５で有価証券を商取引することができる。

【００２０】

[0034]暗号化統合プラットフォーム１２５は、ネットワーク１４５を通して、１つまたは複数のＡＴＳ１５０、暗号化取引所１５５、および暗号化台帳１６０と通信可能に結合される。

【００２１】

[0035]ネットワーク１２０およびネットワーク１４５は、同一のネットワークまたは独立したネットワークであってもよく、有線および／または無線通信システムを使用したローカルエリアおよび／またはワイドエリアネットワークの任意の組合せであってもよい。ネットワーク１２０またはネットワーク１４５のどちらかは、以下のプロトコル／技術のいずれかまたはそれ以外のものであっても、またはそれらを使用してもよく、それらには、イーサネット（登録商標）、ＩＥＥＥ８０２．１１またはＷｉ－Ｆｉ、ワールドワイド・インターオペラビリティ・フォー・マイクロウェーブ・アクセス（ＷｉＭＡＸ）、セルラー電気通信（たとえば、３Ｇ、４Ｇ、５Ｇ）、ＣＤＭＡ、ケーブル、デジタル加入者回線（ＤＳＬ）などがある。同様に、ネットワーク１２０およびネットワーク１４５上で使用されるネットワークプロトコルは、マルチ・プロトコル・ラベル・スイッチング（ＭＰＬＳ）、伝送制御プロトコル／インターネット・プロトコル（ＴＣＰ／ＩＰ）、ユーザー・データグラム・プロトコル（ＵＤＰ）、ハイパー・テキスト・トランスポート・プロトコル（ＨＴＴＰ）、シンプル・メール転送プロトコル（ＳＭＴＰ）、およびファイル転送プロトコル（ＦＴＰ）を含んでもよい。ネットワーク１２０およびネットワーク１４５を介した交換されたデータは、ハイパーテキスト・マークアップ言語（ＨＴＭＬ）または拡張可能マークアップ言語（ＸＭＬ）を含む技術、言語および／または書式を使用して表現されてもよい。加えて、全てまたはいくつかのリンクは、セキュア・ソケット・レイヤ（ＳＳＬ）、トランスポート層セキュリティ（ＴＬＳ）、およびインターネット・プロトコル・セキュリティ（Ｉｐｓｅｃ）などの従来の暗号化技術を使用して暗号化されてもよい。

【００２２】

[0036]ＡＴＳ１５０は、売主と買主のマッチングによる取引のための相手方を探す非交換性の商取引システムである。ＡＴＳ１５０は、従来の証券取引所の代替物である。ＡＴＳ１５０の例は、電気通信ネットワーク（ＥＣＮ）、交差ネットワーク、ダークプール、およびコールマーケットを含む。ＡＴＳ１５０は、暗号化統合プラットフォーム１２５からデジタルサインされたＦＩＸ注文を受信し、デジタル資産を商取引するために売買注文がマッチする可能性のある一対を見つけ、注文の状態を記録する注文台帳の状態を収容する。

【００２３】

[0037]暗号化取引所１５５は、株式、債券、または通貨のデジタル分担所有などのデジタル取引品目を商取引する取引所である。株式のデジタル分担所有は、従来の取引所に上場される有価証券と同一の株式のクラスであり得る。暗号化取引所１５５でのデジタル取引品目の所有権は、暗号化台帳１６０などの１つまたは複数の分散化された台帳上に記録され得る。暗号化取引所１５５は、暗号化統合プラットフォーム１２５からデジタルサインされた暗号化取引（たとえば、注文、取消し）を受信する。

【００２４】

[0038]暗号化台帳１６０は、資本金と交換されるデジタル資産または負債の売却などの経済上の取引を記録する。暗号化台帳１６０は、ユニット毎に様々である。たとえば、ビ

ットコインは、ブロックチェーンと呼ばれる分散化された公開台帳を使用する。暗号化台帳１６０が、暗号化統合プラットフォーム１２５から適切なキーを使用してサインされた取引を受信し、取引がネットワークのノードによって確認されたとき、暗号化台帳１６０は、取引を記録する（たとえば、ブロックチェーンを台帳内に付加する）ことによって、デジタル取引品目を適切なアドレス（たとえば、適切なウォレット）に移動させる。

【００２５】

[0039]多様なデータ記憶装置は、デジタル有価証券、ユーザ情報、および他のデータの記憶およびそれらへのアクセスを管理するために使用され得る。データ記憶装置は、暗号化台帳１６０などの分散化されたデータ記憶装置であってもよい。データ記憶装置は、データベーススキーマで決定されるクラスを使用して設計された集積体セットのデータリポジトリであってもよい。データ記憶装置は、データ記憶できるフラットファイルをさらに含んでもよい。暗号化統合プラットフォーム１２５および／または他のサーバは、データ記憶装置からのデータを収集し、かつ／またはそれらにアクセスしてもよい。

【００２６】

[0040]図２は、本開示の１つまたは複数の実施形態による暗号化統合プラットフォーム１２５内の構成要素セットを示す図である。図２で示した本実施形態によれば、暗号化統合プラットフォームは、メモリ２０５、１つまたは複数のプロセッサ２１０、暗号化アダプタ２１５、暗号化ブリッジ２２０、および暗号化マッチング構成要素２２５を含み得る。他の実施形態は、他のモジュール、アプリケーション、および／または構成要素と共に、それらのモジュールおよび構成要素のいくつか、または全てを含んでもよいし、あるいはそれらを含まなくてもよい。さらにまた、いくつかの実施形態は、２つ以上のこれらのモジュールおよび構成要素を単独のモジュールに組み入れてもよく、および／または１つまたは複数のこれらのモジュールの機能性の一部分を異なるモジュールと結合させてもよい。たとえば、ある実施形態では、暗号化ブリッジ２２０および暗号化マッチング構成要素２２５は、単独の構成要素へと組み合わされてもよい。

【００２７】

[0041]メモリ２０５は、情報を記憶するために使用される、任意のデバイス、機構、集中データ構造であり得る。本開示のいくつかの実施形態によれば、メモリ２０５は、たとえば、任意のタイプの揮発性メモリ、不揮発性メモリ、およびダイナミックメモリであってもよく、またはそれらを含んでもよい。たとえば、メモリ２０５は、ランダムアクセスメモリ、メモリ記憶装置、光メモリ装置、磁気媒体、フロッピーディスク、磁気テープ、ハードドライブ、消去可能プログラム可能読み出し専用メモリ（ＥＰＲＯＭ）、電気的消去可能プログラム可能読み出し専用メモリ（ＥＥＰＲＯＭ）、コンパクトディスク、ＤＶＤ、および／または類似のものであってもよい。いくつかの実施形態によれば、メモリ２０５は、１つまたは複数のディスクドライブ、フラッシュドライブ、１つまたは複数のデータベース、１つまたは複数の表、１つまたは複数のファイル、ローカルキャッシュメモリ、プロセッサキャッシュメモリ、リレーショナルデータベース、フラットデータベース、および／または類似のものを含んでもよい。加えて、当業者ならば、メモリ２０５として使用できる情報記憶用の多くの追加デバイスおよび技法を理解されよう。

【００２８】

[0042]メモリ２０５は、プロセッサ２１０上で１つまたは複数のアプリケーションまたはモジュールを実行するための命令を記憶するために使用されてもよい。たとえば、メモリ２０５は、暗号化アダプタ２１５、暗号化ブリッジ２２０、および暗号化マッチング構成要素２２５の機能性を実行するために必要な命令の全てまたはいくつかを収容する１つまたは複数の実施形態で使用され得る。

【００２９】

暗号化アダプタ

[0043]暗号化アダプタ２１５は、ブローカディーラと暗号化取引所との間のインタフェースとしてはたらく。暗号化アダプタ２１５は、暗号化取引所からブローカディーラへ市場データを提供するために、暗号化ブリッジ２２０と通信する。暗号化アダプタ２１５は

また、ブローカディーラによって提供される顧客識別子を記憶し、２つの独立したキーペアを発生させることによって、新しい顧客を統合する。各キーペアは、１つのプライベートキーおよび１つの公開キーを有する。キーペアの２つは、正確にリンクされている。キーペアの公開キーは、セキュリティに妥協せずに公開されることができ、キーペアのプライベートキーは、メッセージを読むことまたはデジタルサインを実行することを認可されていないいずれの人へも公開されてはいけない。

【００３０】

[0044]２つのキーペアは、顧客識別子に関連付けられた２つのアドレス指定アカウントを作成するために使用される。アドレス指定アカウントは、「ウォレット」と呼ばれることがある。両方のウォレットとも、デジタルアカウントを表す。第１のウォレットは、本明細書中で顧客ポートフォリオウォレットとしてしばしば言及されるが、デジタル資産および負債（たとえば、株式のデジタル分担所有）ならびにデジタル資本金（たとえば、デジタル化ドル、トークン、暗号化通貨）などのデジタル取引品目を記憶する。いくつかの実施形態では、顧客識別子に関連付けられた顧客は、ウォレット用のキーペアを所有するが、暗号化アダプタ２１５が、顧客の代理で取引を完了させるためにキーペアを使用することを認可する。別の実施形態では、暗号化アダプタ２１５または第三者が、顧客ポートフォリオウォレットを所有する。第２のウォレットは、本明細書中で顧客委託ウォレットとしてしばしば言及されるが、顧客が買入または売却注文で申し込み、まだ完了していないデジタル取引回数を記憶する（たとえば、「委託された」資産または資本金）。暗号化アダプタ２１５は、顧客委託ウォレット用のキーを所有するか、または顧客委託ウォレットへのキーを使用することを認可される。いくつかの実施形態では、多くの異なる顧客ポートフォリオウォレットおよび顧客委託ウォレットキーを含む、ペアレントウォレットが作成されてもよい。ペアレントウォレットは、異なる公開台帳用のキーを含み、それによってブローカディーラに１つのマスタアカウントを提供してもよい。

【００３１】

[0045]暗号化アダプタ２１５は、ブローカディーラから、ウォレットの残高を獲得する要求を受信してもよい。顧客識別子を使用して、暗号化アダプタ２１５は、正しい顧客ポートフォリオウォレットおよび顧客委託ウォレットを識別してもよい。暗号化アダプタ２１５は、１つまたは複数の暗号化台帳から各ウォレットの残高を獲得するために、顧客ポートフォリオウォレットおよび顧客委託ウォレット用に対応する公開キーを使用してもよい。

【００３２】

[0046]暗号化アダプタ２１５は、ブローカディーラからの、顧客識別子に関連付けられた買入、売却、または取消し注文を含むＦＩＸ注文メッセージ（または同様のメッセージ）を受信してもよい。注文が、買入注文の場合、ＦＩＸ注文メッセージは、ブローカディーラが取引用に預金された米ドル（または、他の通貨）を有することを示す。したがって、暗号化アダプタ２１５は、顧客からの資本金が、商取引を確定するために特化してブローカディーラのもとに保管されていることの表現を発行する。この表現は、ブローカディーラからのデジタル負債またはＩＯＵであってもよい。そのようなデジタル表現は、顧客ポートフォリオウォレットに、記憶されるか、または関連付けられてもよい。いくつかの実施形態では、資本金は、ブローカディーラのウォレット（すなわち、アドレス指定アカウント）から顧客ポートフォリオウォレットへ暗号化通貨取引を介して送信されてもよい。

【００３３】

[0047]暗号化アダプタ２１５は、デジタル負債をソースアカウント（すなわち、顧客ポートフォリオウォレット）から行先アカウント（すなわち、顧客委託ウォレット）へ転送するための情報を含む買入注文用の暗号化委託取引（すなわち、暗号化取引所でのデジタル資産または負債の売買に関係する取引）を作成し、顧客ポートフォリオウォレットのプライベートキーを使用して暗号化委託取引にサインする。暗号化委託取引は、ＵＳＤトークン、顧客識別子、および／または委託ウォレットの公開キーを含んでもよい。取引が、

暗号化アダプタ２１５によってサインされ、ネットワークノードによって確認された後、ＵＳＤトークンの顧客委託ウォレットへの転送が完了し、取引は、暗号化台帳内で更新される。

【００３４】

[0048]暗号化委託取引の作成に加えて、暗号化アダプタ２１５は、ＦＩＸ注文取引を作成する。ＦＩＸ注文取引を作成するために、暗号化アダプタ２１５は、非暗号化ＦＩＸ注文を伴い、顧客識別子を使用して１組のウォレットおよびキーへ顧客をマッピングし、顧客ポートフォリオウォレットのプライベートキーを使用してＦＩＸ取引を作成し、それにサインする。ＦＩＸ取引は、暗号化注文取引のアウトプット、具体的には取引識別子または暗号化取引注文のハッシュ、によって強化される。ＦＩＸ注文取引は、メッセージタイプ（たとえば、買入、売却）、注文識別子、資本金取引のハッシュ、リターンアカウント、および公開キーを含み得る。ＦＩＸ注文取引をＡＴＳへ送信する前に、ＦＩＸ注文取引を認可するサインと暗号化委託取引を認可するサインが比較される。サインが一致する場合、注文はＡＴＳへ送信される。したがって、同一のプライベートキーを使用してＦＩＸ注文取引および暗号化注文取引にサインすることによって、暗号化アダプタ２１５は、注文が同一の存在に由来することを正確に確かめることができる。これにより、攻撃者による公開台帳の監視、および委託注文の背景で出現する詐欺的な注文を作成しようとすることを防止する。

【００３５】

[0049]暗号化アダプタ２１５は、マッチする可能性のある売却注文を見つけるために、サインされたＦＩＸ注文取引をＡＴＳへ送る。暗号化アダプタ２１５は、サインされた暗号化委託取引を暗号化ブリッジ２２０へ送信し、最終的には、マッチした売却注文を見つけるために、サインされた暗号化委託取引を暗号化取引所へ送る。下記で説明するように、暗号化ブリッジ２２０は、ＦＩＸ注文取引および暗号化委託取引でのサインを比較する。公開キー暗号化法は、サインが一致したかどうかを判定するために使用され得る。暗号化アダプタ２１５はまた、ブローカディーラに買入注文が保留されたことを知らせるブローカディーラへの実行報告を作成し、配信する。暗号化アダプタ２１５はまた、暗号化アダプタ２１５がブローカディーラへ転送した実行報告を暗号化マッチング構成要素２２５から受信する。

【００３６】

[0050]暗号化アダプタ２１５は、買入注文とほとんど同一の方法で売却注文を処理するが、デジタル有価証券がそれを発行する機関によって裏付けられることから、暗号化アダプタ２１５がＵＳＤトークンまたは他のデジタル表現を発行しないことは除かれる。

【００３７】

[0051]暗号化アダプタ２１５は、ブローカディーラからの取消し注文を受信する。暗号化アダプタ２１５は、取消し注文要求を受信し、顧客識別子を顧客委託ウォレットにマッピングする。１つまたは複数の暗号化台帳からウォレット残高を獲得した後、暗号化アダプタは、ＦＩＸ取消し取引を作成し、顧客委託ウォレットプライベートキーを使用してこの取引にサインする。暗号化アダプタ２１５は、ＦＩＸ取消し取引が、最初の暗号化注文取引と同一のプライベートキーによってサインされたことを確認した後（たとえば、公開キー暗号化法を使用して）、暗号化取消し取引注文は、作成される。暗号化アダプタ２１５は、暗号化台帳による資本金または資産の顧客ポートフォリオウォレットへの転送を実施するために、顧客委託ウォレットプライベートキーを使用して暗号化取消し取引にサインする。暗号化取消し取引にサインすることで、取消し注文に由来する存在が実行することを認可されたことを保証する。これにより、攻撃者による先回り取引するための注文の不正な除去を防止する。

【００３８】

暗号化ブリッジ

[0052]暗号化ブリッジ２２０は、暗号化アダプタ２１５から暗号化取引所での市場データの要求を受信する。暗号化ブリッジ２２０は、暗号化取引所から情報を収集し、取引に

関わる有価証券の暗号化市場での最良の価格を検索するルータとしてはたらく。暗号化ブリッジは、暗号化台帳を監視することによってデータを収集し、公開台帳上で見ることができる注文情報に署名することによって、注文台帳の現在のスナップショットを生成することができる。暗号化取引所は、異なる分散化された台帳を有してもよい。暗号化ブリッジ２２０は、異なる分散化された台帳を正規化することによって、ブローカディーラのための単一のインタフェースをさらに提供する。たとえば、多様な分散化された台帳が、使用されてもよく、これらの分散化された台帳は、異なる関連付けられたキーと共に異なるアプリケーションのプログラミングインタフェースを有してもよい。暗号化ブリッジ２２０は、全ての分散化された台帳からのデータにアクセスし、１つの標準フォーマットのデータを提供する。したがって、ブローカディーラは、他のものの中でも、異種のウォレットおよびキー生成、委託された取引、残高の回収を扱うことなしに、暗号化取引所へ自由にアクセスできる。

【００３９】

暗号化マッチング構成要素

[0053]暗号化マッチング構成要素２２５は、マッチする可能性のある一対である２つの委託注文（すなわち、デジタル取引品目が、顧客委託ウォレットへ転送されている注文）を識別するＡＴＳからマッチ要求を受信する。マッチ要求は、各委託取引のための注文識別子を含む。暗号化マッチング構成要素２２５は、注文識別子を委託顧客ポートフォリオウォレットへ注文毎にマッピングする。暗号化マッチング構成要素２２５は、暗号化台帳から顧客委託ウォレットの残高を獲得し、売却側からは、資産または負債が利用可能であり、取引が委託され、買入側からは、資本金が利用可能であり、取引が委託されることを保証する。暗号化マッチング構成要素は、要求回答をマッチさせ、相手方のハッシュ、または顧客ポートフォリオウォレットからのサインを含む。暗号化マッチング構成要素は続いて、顧客委託ウォレットから差し引くこと、および相手方のハッシュまたは顧客ポートフォリオウォレットからのサインを使用して、各々の側の顧客ポートフォリオウォレットに記入することによって、取引を確定し、清算する。

【００４０】

[0054]図３は、デジタル資産の商取引で使用される構成要素の相互作用を示す図である。図３に示すように、顧客（３０２、３０４、３０６、３０８、３１０、３１２、３１４、３１６）は、ブローカディーラ（３１８、３２０）と連係する。ブローカディーラは、顧客から従来の取引所での非デジタル資産または負債を商取引するための注文と同様に、暗号化取引所（３３２、３３４）でのデジタル資産または負債を商取引するための注文もまた受信する。注文がデジタル取引品目を商取引することを伴う場合、注文は、ＦＩＸ注文などのブローカディーラ用の標準フォーマットで、暗号化アダプタ（３２２）へ送られる。暗号化技法を使用して、暗号化アダプタ（３２２）は、顧客ポートフォリオウォレットから顧客委託ウォレットへ、注文に対応したデジタル取引品目を転送し、このことで、「サインされた暗号化取引」が作成される。サインされた暗号化取引は、暗号化ブリッジ（３２８）へ送信される。次に、暗号化アダプタ（３２２）は、１つまたは複数のＡＴＳ（３２４、３２６）へ送信されるＦＩＸ取引注文を作成し、これにサインする。暗号化アダプタ（３２２）は、暗号化サインを比較することで、ＦＩＸ取引および暗号化取引が同一の署名人（party）によって認可されたことを確認する。

【００４１】

[0055]サインがマッチするかを推定するために、暗号化マッチング構成要素（３３０）は、ＡＴＳ（３２４、３２６）のうちの１つ、または暗号化取引所（３３２、３３４）のうちの１つから、注文のマッチする可能性のある一対を受信する。いくつかの実施形態では、注文は、１つ以上のＡＴＳ、または１つ以上の暗号化取引所へ送信されてもよい。暗号化マッチング構成要素は、デジタル取引品目が、利用可能であり、取引を即時に清算し、確定することを確認する。

【００４２】

[0056]図４は、暗号化統合プラットフォーム１２５の構造を示す図である。示したよう

に、ブローカディーラ（４０２）は、１つまたは複数のネットワーク（４０４、４０６）を介して暗号化統合プラットフォーム１２５（４０８、４１０、４１２）と通信する。暗号化統合プラットフォーム１２５は、１つまたは複数のネットワーク（４１４）を介して暗号化台帳（４１６、４１８）と通信する。デジタル取引品目を取得または売却する、または注文を取り消す注文は、いったんブローカディーラ（４０２）によって受信されると、アダプタ（４０８）は、ＡＴＳおよび暗号化取引所（cryptographic exchange）へ送信される、従来のシステム上の取引を作成する。ウォレットキーを含む情報、ユーザ情報、および取引が作成され、データベース（４２０、４２２、４２４）内、および多様な分散化された台帳（４１６、４１８）上に記憶される。資産が確認され、顧客委託ウォレット内へ移動され、取引はサインされる。市場データは、ブロックチェーンなどの分散化された公開台帳から収集される。複数の暗号化台帳（４１６、４１８）で示したように、取引は、取引を記録するために使用される分散化された台帳のタイプに対して断定的でない。ブリッジ（４１０）は、多様な暗号化取引所からの市場データを正規化する。注文は、マッチング構成要素（４１２）内でマッチされる。

【００４３】

[0057]図５は、暗号化統合プラットフォームを使用して、ブローカディーラの観点からのデジタル資産を商取引するプロセス５００を示すフローチャートである。受信操作５０２は、ブローカディーラのコンピュータデバイスにおける顧客から注文を受信する。注文は、１つまたは複数のデジタル取引品目の買入または売却の注文、または既存の注文を取り消す注文を含んでもよい。受信した注文に基づいて、ブローカディーラは、ＦＩＸプロトコル（または他のプロトコル）内に注文メッセージを作成し、その注文を送信操作５０４で暗号化統合プラットフォームへ送信してもよい。暗号化統合プラットフォームが、顧客アカウント残高（すなわち、顧客ポートフォリオウォレットおよび顧客委託ウォレットの残高）を調べ、注文するデジタル資本金または資産を委託した後、ブローカディーラは、受信操作５０６で注文の状態（たとえば、注文保留、注文実行、注文取消し）を含む実行報告を受信する。実行報告は、ブローカディーラが通常の売買で発生する商取引から受信する同一のフォーマットで提供される。

【００４４】

[0058]図６は、暗号化統合プラットフォームの観点からのデジタル取引品目を商取引するプロセス６００を示すフローチャートである。いくつかの実施形態では、図６で実行される操作は、暗号化アダプタによって実行され得る。いくつかの実施形態では、より少ない、またはより多い操作が実行されてもよく、あるいは、操作が異なる順序で実行されてもよい。

【００４５】

[0059]作成操作６０２は、顧客のための、第１のアドレス指定アカウント（たとえば、顧客ポートフォリオウォレット）、および第２のアドレス指定アカウント（たとえば、顧客委託ウォレット）を作成する。第１および第２のアドレス指定アカウントは、関連付けられたキーペアを各々有してもよく、両方が、顧客識別子に関連付けられてもよい。顧客によって所有される多様なデジタル取引品目は、第１および第２のアドレス指定アカウントに関連付けられてもよい。受信操作６０４は、デジタル有価証券などのデジタル取引品目の買入または売却の注文を受信する。

【００４６】

[0060]サイン操作６０６は、第１のアドレス指定アカウントに関連付けられたプライベートキーを使用して、第１の取引に電子サインし、デジタル取引品目を第１のアドレス指定アカウントから第２のアドレス指定アカウントへ転送する。サイン操作６０６はさらに、第１のアドレス指定アカウントのプライベートキーを使用して第２の取引に電子サインしてもよい。確認操作６０８は、第１の取引が第２の取引と同一のプライベートキーを使用してサインされたことを確認する。認可操作６１０は、第１の取引が、第２の取引と同一のプライベートキーを使用してサインされたことを確認した後、暗号化取引所でのデジタル取引品目の申し込みを認可する。

【００４７】
[0061]図７は、暗号化統合プラットフォームの観点からのデジタル取引品目を商取引するプロセス７００を示すフローチャートである。いくつかの実施形態では、図７で実行される操作は、暗号化マッチング構成要素によって実行され得る。いくつかの実施形態では、より少ない、またはより多い操作が実行されてもよく、あるいは、操作が異なる順序で実行されてもよい。
【００４８】
[0062]受信操作７０２は、買入取引と売却取引をマッチさせる要求を受信する。買入取引は、デジタル取引品目を指定された総額だけ（たとえば、デジタル取引品目の額に対応した総額）取得する買入注文を含んでもよく、売却取引は、デジタル取引品目をある総額だけ売却する、売却注文を含んでもよい。デジタル取引品目を取得する顧客は、２つのアドレス指定アカウント、すなわち第１の顧客ポートフォリオウォレットおよび第１の顧客委託ウォレットを有してもよい。デジタル取引品目を売却する顧客もまた、２つのアドレス指定アカウント、すなわち第２の顧客ポートフォリオウォレットおよび第２の顧客委託ウォレットを有してもよい。
【００４９】
[0063]買入取引は、買入注文を識別する第１のアドレス指定アカウント（たとえば、第１の顧客ポートフォリオウォレット）に対応する、関連付けられた第１のサインを含み得る。売却取引は、売却注文を識別する第２のアドレス指定アカウント（たとえば、第２の顧客ポートフォリオウォレット）に対応した関連付けられた第２のサインを含み得る。資本金の総額は、第１の顧客に関連付けられた第３のアドレス指定アカウント（たとえば、第１の顧客委託ウォレット）に関連付けられてもよく、１つまたは複数のデジタル取引品目は、第２の顧客に関連付けられた第４のアドレス指定アカウント（たとえば、第２の顧客委託ウォレット）に関連付けられてもよい。
【００５０】
[0064]マッピング操作７０４は、買入取引を第３のアドレス指定アカウント（たとえば、第１の顧客委託ウォレット）に、売却取引を第４のアドレス指定アカウント（たとえば、第２の顧客委託ウォレット）にマッピングする。
【００５１】
[0065]送信操作７０６は、マッチ要求回答を暗号化取引所へ送信する。マッチ要求は、買入取引を委託するための、第１のサインおよび第２のサインを含み得る。転送操作７０８は、デジタル取引品目を第１のアドレス指定アカウント（たとえば、第１の顧客ポートフォリオウォレット）へ転送する。転送操作７１０は、買入取引および売却取引を確定し、清算するために、総額を第２のアドレス指定アカウント（たとえば、第２の顧客ポートフォリオウォレット）へ転送する。
【００５２】
顧客の作成
[0066]図８は、顧客がデジタル有価証券を商取引できるようにするために暗号化統合プラットフォームに新しい顧客を統合するプロセス８００を示す。ユーザのサインアップ（８０２）のとき、ブローカディーラは、ユーザインタフェース（「ＵＩ」）を介して、氏名、銀行口座情報、および顧客によって所有される有価証券などの顧客データを収集する（８０４）。顧客データは、顧客からデータを受信し（８０８）、顧客の同一性を確認する（８１０）、Ｋｎｏｗ　Ｙｏｕｒ　Ｃｕｓｔｏｍｅｒ（「ＫＹＣ］）プロセス（または、他のプロセス）で、確認されてもよい（８０６）。ＫＹＣプロセスは、外部のベンダーによって、または、ブローカディーラによって履行されてもよい。顧客の同一性が確認された場合、ブローカディーラは、ブローカディーラのシステム内に顧客を作成する（８１２）。ブローカディーラは、顧客識別番号または顧客の他の識別子などの顧客識別子を割り当てる。
【００５３】
[0067]ブローカディーラが、顧客識別子を顧客へ、いったん割り当てた後、顧客識別子

および顧客データは、顧客識別子および顧客データが１つまたは複数のデータベースに記憶されている暗号化アダプタへ送信されてもよい（８１４）。暗号化アダプタは、顧客用のキーペア（たとえば、公開キーおよびプライベートキーのペア）を生成してもよく（８１６）、そのキーペアおよび顧客識別子に関連付けられた顧客ポートフォリオウォレットを作成してもよい（８１６）。顧客ポートフォリオウォレットは、顧客によって所有される、資本金（たとえば、デジタルの通貨または通貨の表現）、およびデジタル資産または負債（たとえば、株式のデジタル分担所有）などの任意のデジタル取引品目を保持し得る（すなわち、関連付けられ得る）。

【００５４】

[0068]さらに、キーペアの第２のセット、ならびにそのキーペアの第２のセットおよび顧客識別子に関連付けられた第２のデジタルウォレットが作成される（８１８）。顧客委託ウォレットは、将来の注文で委託されるデジタル取引品目を確保するために、エスクロウアカウント（escrow account）と同じように、使用されてもよい。顧客ポートフォリオウォレットおよび顧客委託ウォレットの残高は、分散化された台帳に記録され、キーペアを使用してアクセスされ得る。いくつかの実施形態では、第三者が、顧客ポートフォリオウォレットおよび顧客委託ウォレットを作成し、対応するキーペアを生成することを委任されてもよい。顧客ポートフォリオウォレットおよび顧客委託ウォレットがいったん作成されると、暗号化アダプタは、ブローカディーラへ顧客が順調に作成されたことを知らせる（８２０）。ブローカディーラは、顧客が順調に作成されたことの知らせを受信する（８２２）。

【００５５】

注文の作成

[0069]図９は、デジタル有価証券を商取引する注文を作成するプロセス９００を示す。顧客は、ユーザインタフェース（「ＵＩ」）を介してブローカディーラにログインしてもよい。顧客がログインすると（９０２）、ブローカディーラは、暗号化レベル１データ（すなわち、１つまたは複数の有価証券の最新の買入呼値および売却指値などの、暗号化取引所での有価証券商取引のための市場データ）を要求することができる（９０４）。このタイプのデータは、トレーダによって将来の商取引の買入、買入呼値、および売却指値の決定のために使用され得る。暗号化レベル１データの要求は、１つまたは複数の暗号化取引所からデータを収集する暗号化ブリッジ（９０６）へ送られる。暗号化ブリッジは、暗号化取引所から暗号化レベル１データを回収し（９０８、９１０）、そのデータを正規化して、ブローカディーラの既存のシステムによって使用されるフォーマットでの暗号化レベル１データを作成する（９１２）。いくつかの実施形態では、ブローカディーラは、ある期間中に発生した注文の履歴などの追加の市場データを提供する、暗号化レベル２データなどの追加のデータを要求する。暗号化ブリッジは、ブローカディーラのインタフェースに利用可能な暗号化レベル１データを、発行、送信、またはその他の場合は作成する（９１４）。

【００５６】

[0070]ブローカディーラは、顧客ポートフォリオウォレットおよび顧客委託ウォレットの資産（すなわち、有価証券およびデジタル資本金）の残高を要求してもよい（９１６）。暗号化アダプタは次に、ブローカディーラによって送信された顧客識別子を使用して、顧客識別子を顧客ポートフォリオウォレットおよび顧客委託ウォレットにマッピングする（９１８）。顧客ポートフォリオウォレットデータおよび顧客委託ウォレットデータは、現在の通常の商取引システムの取引所によって所有されるデータベース（たとえば、ニューヨーク証券取引所は、それの商取引データを所有する）とは対照的に、分散化された暗号化台帳を使用して記録される（９１８）。したがって、ブローカディーラへウォレットデータを提供するために、暗号化アダプタは、暗号化台帳からウォレットデータを収集する。

【００５７】

[0071]顧客ウォレットおよび／または顧客委託ウォレットの残高を決定するために、分

散化された台帳は、顧客ポートフォリオウォレットおよび／または顧客委託ウォレットのそれぞれのためのキーペアを使用して検索される（９２０、９２２）。残高がいったん決定されると（９２４）、暗号化アダプタは次に、ブローカディーラのユーザインタフェースへ、確定された残高を含む顧客ポートフォリオウォレットおよび顧客委託ウォレットの両方の、デジタル資本金およびデジタル資産を含む残高を提供する（９２６）。ブローカディーラは、顧客ポートフォリオウォレットおよび／または顧客委託ウォレットに関連付けられた残高を表示してもよく（９２８）、次に顧客から買入または売却注文を受信してもよい（９３０）。ブローカディーラは、注文が買入注文（９３０、９３２）か売却注文（９３０、９３４）かを判定してもよい。

【００５８】

買入注文処理

[0072]図１０は、デジタル資産、負債、または他のデジタル取引品目を取得する注文を受信し、処理するプロセス１０００を示す。ブローカディーラは、買入注文を受信し（１００２）、顧客ポートフォリオウォレットの残高に基づいて、顧客が取得を成立させる購買力を有するかを判定する。顧客が取得を成立させる購買力を有するかを推定するために、ブローカディーラは、注文を顧客と対応して確認し（１００４）、ブローカディーラが顧客のために預金した現金または現金等価物で予約を配置する（１００６）。次に、ブローカディーラは、ＦＩＸ注文メッセージまたは同等の注文メッセージなどの、商取引前の通信および商取引実行のための従来の商取引プロトコルを使用して、注文メッセージを作成する（１００８）。本実施例の目的のために、ＦＩＸ注文メッセージは、使用される。

【００５９】

[0073]暗号化アダプタが、ＦＩＸ注文メッセージを受信するとき、暗号化アダプタは、顧客識別子を顧客ポートフォリオウォレットおよび顧客委託ウォレットの両方にマッピングする（１０１０）。次に、暗号化アダプタは、顧客からの現金が商取引（すなわち、通常は資産価格によって量が増加する総額の、ブローカディーラからのデジタル負債またはＩＯＵ）を確定するために特化して、ブローカディーラに保持されていることを表現する、ＵＳＤトークンなどの資本金のデジタル表現を作成する（１０１２）。暗号化アダプタは、ブローカディーラの代理で顧客ポートフォリオウォレットへトークンを発行し、これは分散化された台帳に記録される（１０１４、１０１６）。

【００６０】

[0074]その後、暗号化アダプタは、このときＵＳＤトークを含む顧客ポートフォリオウォレット残高、および暗号化台帳からの顧客委託ウォレット残高を回収する（１０１８）。暗号化台帳は、残高を検索し、その残高を暗号化アダプタに提供する（１０２０、１０２２）。暗号化アダプタは、注文のための残高が利用可能であるか判定する（１０２４）。残高が十分である場合、暗号化アダプタは、顧客委託ウォレットのＵＳＤトークンを転送するために、顧客ポートフォリオウォレット用の顧客のプライベートキーを使用して暗号化委託取引を作成し、それにサインする（１０２６）。暗号化委託取引は、そのアドレスがＵＳＤトークンを顧客ポートフォリオウォレットへ送信するために使用される記録、ＵＳＤトークンの総額、および顧客委託ウォレットのアドレスなどの情報を含む。サインされた暗号化委託取引を受信し、それを確認した後、暗号化台帳は、取引を記録することによって、ＵＳＤトークンを顧客委託ウォレット内に移動させ（１０２８）、その記録が暗号化アダプタに提供される（１０３０）。ＵＳＤトークンは、取引の確定または取り消しのどちらかが決定されるまでの間、委託ウォレット内に留まる。

【００６１】

[0075]ＵＳＤトークンが、いったん顧客ポートフォリオウォレットから顧客委託ウォレットへ移動されると（１０３２）、暗号化アダプタは、ＦＩＸ注文取引（最終的にＡＴＳへ送信される）を作成し、顧客ポートフォリオウォレット用のプライベートキーを使用してＦＩＸ注文取引にサインする（１０３４）。暗号化アダプタは、暗号化委託取引からのサインと、ＦＩＸ注文取引からのサインを比較し、サインが一致するか判定する（１０３６）。暗号化アダプタは、サインが一致するか判定するために、非対称公開キー暗号化法

を使用してもよい。

【００６２】

[0076]ＦＩＸ注文取引が、暗号化委託取引にサインした同一の署名人によってサインされたことを確認することによって、暗号化統合プラットフォームは、ＦＩＸ注文取引が暗号化委託取引に関連付けられており、したがってデジタル資本金が取引に利用可能であることの確実性を提供できる。さらに、委託注文は公開情報であり、それゆえ一般人は、注文が委託残高を有することを知ることができる。

【００６３】

[0077]委託取引からのサインが、ＦＩＸ注文取引からのサインと一致する場合、ＡＴＳおよび／または暗号化取引所は、注文を申し込み（１０３８）、注文識別子を含む実行報告を作成する（１０４０）。暗号化アダプタは、注文識別子を暗号化委託取引のハッシュにマッピングする（１０４２）。次に、注文が順調に申し込まれたかを推定するために（１０４４）、暗号化アダプタは、注文が保留中であること示す実行報告を作成し、その実行報告をブローカディーラに発行する（１０４６）。ブローカディーラは、注文が順調に保留中であることを反映するために、そのシステムを更新してもよい（１０４８）。図に示すように、暗号化統合プラットフォームによって、ブローカディーラが、暗号化取引所で単にＦＩＸ注文メッセージを送信することで商取引できるようになる。

【００６４】

売却注文処理

[0078]図１１は、暗号化取引所で、デジタル資産、デジタル負債、または他のデジタル取引品目を売却する注文を受信し、処理するプロセス１１００を示す。売却する注文のプロセスは、資産を取得する注文のプロセスと同様であるが１つの例外をもち、すなわち、資産が企業のネットワークで裏付けられるので、デジタル負債を作成する必要がない。

【００６５】

[0079]ブローカディーラは、売却注文を受信し（１１０２）、暗号化アダプタによって提供された顧客ポートフォリオウォレットの残高に基づいて、顧客が売却する資産を所有するかを判定する。顧客が売却する資産を所有するかを推定するために、ブローカディーラは、注文を顧客と対応して確認する（１１０４）。次に、ブローカディーラは、商取引前の通信および商取引実行のためのＦＩＸ注文メッセージまたは同等の注文メッセージを作成する（１１０６）。本実施例の目的のために、ＦＩＸ注文メッセージは、使用される。

【００６６】

[0080]暗号化アダプタが、ＦＩＸ注文メッセージを受信するとき、暗号化アダプタは、顧客識別子を顧客ポートフォリオウォレットおよび顧客委託ウォレットにマッピングする（１１０８）。次に、暗号化アダプタは、暗号化台帳から顧客ポートフォリオウォレット残高および顧客委託ウォレット残高を収集する（１１１０、１１１２、１１１４）。売却するデジタル資産または負債が、顧客ポートフォリオウォレットに関連付けられているか推定するために（１１１６）、暗号化アダプタは、顧客ポートフォリオウォレット用のプライベートキーを使用して、暗号化委託取引を作成し、暗号化委託取引にサインする（１１１８）。暗号化委託取引は、そのアドレスがデジタル資産を顧客ポートフォリオウォレットへ送信するために使用される記録、商取引を委託されている資産の総額、および顧客委託ウォレットのアドレスを含んでもよい。サインされた暗号化委託取引が受信され、確認された後、暗号化台帳は、資産を顧客委託ウォレット内へ移動させ（１１２０）、取引回答を作成する（１１２２）。資産は、取引の確定または取り消しのどちらかが決定されるまでの間、顧客委託ウォレット内に留まる。

【００６７】

[0081]資産が、いったん顧客ポートフォリオウォレットから顧客委託ウォレットへ順調に移動されると（１１２４）、暗号化アダプタは、ＦＩＸ注文取引を作成し、顧客委託ウォレット用のプライベートキーを使用してＦＩＸ注文取引にサインする。（１１２６）。暗号化アダプタは、委託取引からのサインと、ＦＩＸ注文取引からのサインを比較し、サ

インが一致するか判定する（１１２８）。上で説明したように、非対称公開キー暗号化法は、サインが一致したことを保証するために使用され得る。

【００６８】

[0082]ＦＩＸ注文取引が、暗号化委託取引と同一の署名人によってサインされたことを確認することによって、暗号化統合プラットフォームは、ＦＩＸ注文取引が委託取引に関連付けられており、したがって資産が取引に利用可能であることの確実性を提供できる。

【００６９】

[0083]委託取引からのサインが、ＦＩＸ注文取引からのサインと一致する場合、暗号化取引所は、注文を申し込み（１１３０）、注文識別子を含む実行報告を作成する（１１３２）。暗号化アダプタは、注文識別子を暗号化委託取引のハッシュにマッピングする（１１３４）。次に、成功を推定するために（１１３６）、暗号化アダプタは、注文が保留中であること示す実行報告を作成し、その実行報告をブローカディーラに発行する（１１３８）。ブローカディーラは、注文が順調に保留中であることを表示するために、そのシステムを更新してもよい（１１４０）。

【００７０】

取消し注文処理

[0084]図１２は、デジタル取引品目を売却または取得する取引を取り消すプロセス１２００を示す。取消し注文が成立した場合、売却または取得を保留している顧客委託ウォレット内のデジタル取引品目（たとえば、資産またはデジタル資本金）は、顧客ポートフォリオウォレットへ戻される。デジタル取引品目が、顧客委託ウォレットへまだ移動されていない場合は、取消し注文は、デジタル取引品目が顧客委託ウォレットへ移動されないことを保証する。暗号化統合プラットフォームは、取消しが最初のＦＩＸ取引にサインした同一の存在によって注文されたことを証明することによる、注文の取り消しに備える。

【００７１】

[0085]ブローカディーラは、注文を取り消す要求を受信し（１２０２）、顧客識別子を含むその要求を、暗号化アダプタへ送信する（１２０４）。暗号化アダプタが、注文を取り消す要求を受信するとき、暗号化アダプタは、顧客識別子を顧客ポートフォリオウォレットおよび顧客委託ウォレットにマッピングする（１２０６）。次に、暗号化アダプタは、暗号化台帳への問い合わせによって、顧客ポートフォリオウォレット残高および顧客委託ウォレット残高を確認する（１２０８、１２１０）。暗号化台帳は、顧客のウォレット残高を検索し（１２１０）、回答を暗号化アダプタに提供する（１２１２）。

【００７２】

[0086]次に、暗号化アダプタは、取消し注文の内容が顧客委託ウォレット（すなわち、売却され得る資産、または取得のために使用され得るデジタル通貨）内にあるかを判定する（１２１４）。取消し注文の内容が顧客委託ウォレット内にない場合（すなわち、注文が既に、確定プロセスの一部にある）、取消し注文は実行されない。取消し注文の内容が顧客委託ウォレット内にある場合、暗号化アダプタは、ＦＩＸ取消し取引を作成し、デジタル資本金または資産を顧客委託ウォレット内へ転送した最初の注文にサインするために使用したプライベートキー（すなわち、顧客ポートフォリオウォレット用のプライベートキー）を使用してＦＩＸ取消し取引にサインする（１２１６）。最初の注文は、暗号化マッチング構成要素および／または暗号化注文取引によって戻される注文識別子によって識別される。

【００７３】

[0087]次に、暗号化アダプタは、注文に関連付けられた暗号化委託取引からのサインと、ＦＩＸ取消し取引からのサインを比較し、サインが一致するか判定する（１２１８）。暗号化取消し取引からのサインと、ＦＩＸ取消し取引からのサインとが一致する場合、暗号化取引所は、注文を取り消し、注文識別子を含む実行報告を作成する（１２２０）。暗号化取引所は、暗号化アダプタのための実行報告１２２２を作成する。暗号化アダプタは、注文識別子を暗号化取消し取引のハッシュにマッピングする（１２２４）。次に、暗号化取引所での注文の順調な取消しを推定するために（１２２６）、暗号化アダプタは、取

消し注文およびデジタル資本金または資産を顧客委託ウォレット内に転送する注文にサインするために使用したプライベートキー（すなわち、顧客委託ウォレット用のプライベートキー）を使用して、暗号化取消し取引を作成し、それにサインする（１２２８）。暗号化台帳は、デジタル資本金または資産を顧客委託ウォレットから顧客ポートフォリオウォレット内へ移動し（１２３０）、取引回答を作成する（１２３２）。成功を推定するために（１２３４）、暗号化アダプタは次に、注文が取り消されたことを示す実行報告を作成し、その実行報告をブローカディーラに発行する（１２３６）。ブローカディーラは次に、そのシステムを、注文の順調な取消しに対応して更新する（１２３８）。

【００７４】

マッチング注文

[0088]図１３は、デジタル資産の取得または売却の取引を確定し、清算するプロセス１３００を示す。ＡＴＳは、委託買入注文と委託売却注文との間のマッチする可能性のある一対を識別し（１３０２）、マッチする可能性のある一対が本当にマッチすること（すなわち、各注文識別子に関連付けられたウォレット残高が利用可能であること）を確認するために、マッチ要求を暗号化マッチング構成要素へ送信する（１３０４）。

【００７５】

[0089]暗号化マッチング構成要素は、マッチ要求を受信し（１３０６）、注文識別子を各委託ウォレットにマッピングし（１３０８）、買入注文および売却注文の両方に関連付けられた顧客委託ウォレット残高について、暗号化台帳に問い合わせる（１３１０）。暗号化台帳は、残高を回収し（１３１２）、残高回答を作成し（１３１４）、その残高回答を暗号化マッチング構成要素に提供する（１３１６）。暗号化マッチング構成要素は、残高が利用可能であることを確認する（１３１８）。顧客委託ウォレット内に対応する買入および売却の残高が存在することを推定するために、暗号化マッチング構成要素は、注文をマッチさせるマッチ要求を作成する（１３２０）。マッチ要求は、相手方の顧客ポートフォリオウォレットのためのサイン、および／または最初の注文を識別する各注文のための相手方のハッシュを含み、台帳上に公開し分散化される（１３２０）。たとえば、売却注文用のハッシュは、資産を顧客ポートフォリオウォレットから顧客委託ウォレットへと移動するときに、作成される識別子である。同様に、買入注文用のハッシュは、ＵＳＤトークンを委託状態へと移動させた取引中に、作成される識別子である。

【００７６】

[0090]暗号化取引所が、マッチする一対を示すマッチ要求回答をいったん受信すると、暗号化取引所は、取引をマッチさせ、資産／資本金の売買を各相手方の顧客ポートフォリオウォレットに記録することによってマッチされた取引を委託し（１３２２）、暗号化ブリッジに送られブローカディーラに通知される注文実行を作成する（１３３０）。同時に、またはほぼ同時に、暗号化マッチング構成要素は、相手方のハッシュを使用した取引を確定し、清算する（１３２４）。取引の確定および清算は、取得または売却する顧客の委託ウォレットからデジタル資本金または資産をそれぞれ差し引くことと（１３２６）、および取得または売却する顧客ポートフォリオウォレットに資産およびデジタル資本金をそれぞれ記入することと（１３２８）を含む。暗号化取引所は、注文実行を、暗号化ブリッジへ送り（１３３２）、それが順調な取引の結果をブローカディーラへ送る（１３３４）。

【００７７】

[0091]多様な本開示の実施形態が、以下に説明される。

実施形態１

コンピュータによって、各々が共通の識別子を有し、かつ各々がある１人の第１の顧客に関連付けられる、第１のアドレス指定アカウントおよび第２のアドレス指定アカウントを作成するステップと、

リモートのコンピュータデバイスから、前記第１のアドレス指定アカウントに関連付けられた１つまたは複数のデジタル取引品目を売買するための注文を受信するステップであって、前記注文が前記共通の識別子に関連付けられている、ステップと、

前記第１のアドレス指定アカウントに関連付けられたプライベートキーを使用して、第１の取引に電子サインし、前記第１のアドレス指定アカウントから前記第２のアドレス指定アカウントへ前記１つまたは複数のデジタル取引品目を転送するステップと、
前記第１のアドレス指定アカウントに関連付けられた前記プライベートキーを使用して、第２の取引に電子サインするステップと、
前記第１の取引が、前記第２の取引と同一のプライベートキーを使用してサインされたことを確認するステップと、
暗号化取引所での前記注文の申し込みを、前記第１の取引が、前記第２の取引と同一のプライベートキーを使用してサインされたことの確認に基づいて、認可するステップと
を含む、コンピュータ化された方法。
実施形態２
前記第２のアドレス指定アカウントが、第２の公開キーおよび第２のプライベートキーを含む第２のキーペアに関連付けられる、実施形態１に記載のコンピュータ化された方法。
実施形態３
分散化された台帳から、前記注文に関連付けられた前記１つまたは複数のデジタル取引品目が、前記第１の公開キーを使用することによって前記第１のアドレス指定アカウントに関連付けられることの確認を受信するステップと、
前記注文に関連付けられた前記１つまたは複数のデジタル取引品目が、前記第１のアドレス指定アカウントに関連付けられることの確認の受信に基づいて、前記第１の取引および前記第２の取引を作成するステップと
をさらに含む、実施形態１に記載のコンピュータ化された方法。
実施形態４
分散化された台帳に、前記第１のアドレス指定アカウントおよび前記第２のアドレス指定アカウントとの残高を通知するステップをさらに含む、実施形態１に記載のコンピュータ化された方法。
実施形態５
前記注文が、デジタル資産またはデジタル負債を取得するための注文である、実施形態１に記載のコンピュータ化された方法であって、
前記リモートのコンピュータデバイスから、資本金で前記デジタル資産または前記デジタル負債を取得できることを示す情報を受信するステップであって、前記１つまたは複数のデジタル取引品目が、前記資本金のデジタル表現である、ステップと、
前記資本金の前記デジタル表現を、前記１つまたは複数のデジタル取引品目として、前記第１のアドレス指定アカウントに関連付けるステップとをさらに含む、コンピュータ化された方法。
実施形態６
前記注文が、前記１つまたは複数のデジタル取引品目を売却するための注文であって、前記１つまたは複数のデジタル取引品目が、１つまたは複数のデジタル資産または１つまたは複数のデジタル負債である、実施形態１に記載のコンピュータ化された方法であって、
前記リモートのコンピュータデバイスから、前記１つまたは複数のデジタル資産に対応した資産、または前記１つまたは複数のデジタル負債に対応した負債が、売却できることを示す情報を受信するステップをさらに含む、コンピュータ化された方法。
実施形態７
第３のアドレス指定アカウントを作成するステップをさらに含む、実施形態１に記載のコンピュータ化された方法であって、前記第３のデジタルアドレス指定アカウントが、前記第１のアドレス指定アカウントに関連付けられた第１のキーペアと、前記第２のアドレス指定アカウントに関連付けられた第２のキーペアとを含む、コンピュータ化された方法。
実施形態８

前記第１の取引を作成するステップであって、前記第１の取引が、前記１つまたは複数のデジタル取引品目、前記識別子、および前記第２のアドレス指定アカウントの公開キーのうちの少なくとも１つを含む、ステップと、
前記第１の取引のハッシュを作成するステップと、
前記第２の取引を作成するステップであって、前記第２の取引が、前記注文のタイプ、前記識別子、前記第２のアドレス指定アカウントの公開キー、および前記第１の取引の前記ハッシュのうちの少なくとも１つを含む、ステップとをさらに含む、実施形態１に記載のコンピュータ化された方法。
実施形態９
前記暗号化取引所へ前記第１の取引を送信するステップと、
代替の商取引システムへ前記第２の取引を送信するステップとをさらに含む、実施形態１に記載のコンピュータ化された方法。
実施形態１０
前記注文が前記暗号化取引所での第２の注文にマッチしたことの通知を受信するステップと、
実行報告を作成するステップとをさらに含む、実施形態９に記載のコンピュータ化された方法。
実施形態１１
前記第１のアドレス指定アカウントが、顧客ポートフォリオアカウントであり、前記第２のアドレス指定アカウントが、顧客委託アカウントである、実施形態１に記載のコンピュータ化された方法。
実施形態１２
前記第１の取引が、前記第１の取引の額に対応した総額内の資本金または前記第１の取引の前記額に対応した前記総額内の前記資本金の表示、および前記第１のアドレス指定アカウントの公開キーのうちの少なくとも１つを含み、前記第２の取引が、前記第２のアドレス指定アカウントの公開キー、前記注文のタイプ、前記識別子、前記第２のアドレス指定アカウントの公開キー、および前記第１の取引のハッシュのうちの少なくとも１つを含む、実施形態１に記載のコンピュータ化された方法。
実施形態１３
ブローカディーラから、買入取引と売却取引をマッチさせる要求を受信するステップであって、
前記買入取引が、前記１つまたは複数のデジタル取引品目の額に対応した総額で前記１つまたは複数のデジタル取引品目を取得するための買入注文を含み、前記売却取引が、前記総額で前記１つまたは複数のデジタル取引品目を売却するための売却注文を含み、
前記買入取引が、前記買入注文を識別する第１のアドレス指定アカウントに対応した関連付けられた第１のサインを有し、前記売却取引が、前記売却注文を識別する第２のアドレス指定アカウントに対応した関連付けられた第２のサインを有し、前記第１のアドレス指定アカウントが、第１の顧客に関連付けられ、前記第２のアドレス指定アカウントが、第２の顧客に関連付けられ、前記総額が、前記第１の顧客に関連付けられた第３のアドレス指定アカウントに関連付けられ、前記１つまたは複数のデジタル取引品目が、前記第２の顧客に関連付けられた第４のアドレス指定アカウントに関連付けられる、ステップと、
コンピュータによって、前記買入取引を前記第３のアドレス指定アカウントへ、前記売却取引を前記第４のアドレス指定アカウントへマッピングするステップと、
暗号化取引所へ、前記買入取引を委託するために前記第１のサインおよび前記第２のサインを含むマッチ要求回答を送信するステップと、
前記買入取引および前記売却取引を確定し、清算するために、前記第１のアドレス指定アカウントへ前記１つまたは複数のデジタル取引品目を転送し、前記第２のアドレス指定アカウントへ前記総額を転送するステップとを含む、コンピュータ化された方法。
実施形態１４

分散化された台帳から、前記マッチ要求回答を送信する前に、前記総額が、前記第３のアドレス指定アカウントに関連付けられ、前記１つまたは複数のデジタル取引品目が、前記第４のアドレス指定アカウントに関連付けられている確認を受信するステップをさらに含む、実施形態１３に記載の方法。

実施形態１５

前記１つまたは複数のデジタル取引品目が、１つまたは複数のデジタル資産またはデジタル負債を含み、前記総額が、前記１つまたは複数のデジタル取引品目の額に対応した通貨、暗号化通貨、または前記通貨もしくは前記暗号化通貨の表示の総額を含む、実施形態１３に記載のコンピュータ化された方法。

実施形態１６

リモートのコンピュータデバイスへ、前記買入取引および前記売却取引を確定、清算した結果を公表するステップをさらに含む、実施形態１３に記載のコンピュータ化された方法。

実施形態１７

前記第１のサインが、前記第１のアドレス指定アカウントに関連付けられたプライベートキーであり、前記第２のサインが、前記第２のアドレス指定アカウントに関連付けられたプライベートキーである、実施形態１３に記載のコンピュータ化された方法。

実施形態１８

前記第１のアドレス指定アカウントが、前記第１の顧客に関連付けられた顧客ポートフォリオアカウントであり、

前記第２のアドレス指定アカウントが、前記第２の顧客に関連付けられた顧客ポートフォリオアカウントであり、

前記第３のアドレス指定アカウントが、前記第１の顧客に関連付けられた顧客委託アカウントであり、

前記第４のアドレス指定アカウントが、前記第２の顧客に関連付けられた顧客委託アカウントである、実施形態１３に記載のコンピュータ化された方法。

実施形態１９

少なくとも１つのプロセッサと、

少なくとも１つのコンピュータ可読記憶媒体であって、命令が、そこに格納され、少なくとも１つのプロセッサによって実行されるとき、前記暗号化統合システムに、

第１のアドレス指定アカウントに関連付けられた１つまたは複数のデジタル取引品目のための商取引を実行する注文を受信するステップであって、前記注文、前記第１のアドレス指定アカウント、および第２のアドレス指定アカウントは、ある１つの識別子に関連付けられた、ステップと、

前記第１のアドレス指定アカウントから前記第２のアドレス指定アカウントへ前記１つまたは複数のデジタル取引品目を転送する第１の取引を発生させるステップと、

前記注文を含む第２の取引を発生させるステップと、

前記第１の取引が、前記第２の取引と同一の署名人によって認可されたことを確認するステップと、

前記第１の取引が、前記第２の取引と同一の署名人によって認可されたことを確認した後に、暗号化取引所での前記注文の申し込みを認可するステップとを実行させる、

少なくとも１つのコンピュータ可読記憶媒体とを備える、暗号化統合システム。

実施形態２０

前記第１の取引および前記第２の取引が、同一のキーによってサインされたとき、前記第１の取引が、前記第２の取引と同一の署名人によって認可される、実施形態１９に記載の暗号化統合システム。

実施形態２１

前記キーが、前記第１のアドレス指定アカウントのプライベートキーであり、前記第２の取引が、前記第１の取引のハッシュを含む、実施形態２０に記載の暗号化統合システム。

実施形態２２
前記命令が、前記少なくとも１つのプロセッサによって実行されるとき、前記暗号化統合システムに、
前記暗号化取引所から、前記注文と第２の注文をマッチさせる要求を受信するするステップであって、前記第２の注文が、第２の識別子に関連付けられている、ステップと、
前記注文を確定し、清算するために、前記１つまたは複数のデジタル取引品目を前記第２の識別子に関連付けられたアドレス指定アカウントへ転送し、１つまたは複数の他のデジタル取引品目を前記第１のアドレス指定アカウント内に転送するステップとをさらに実行させる、実施形態１９に記載の暗号化統合システム。
実施形態２３
前記暗号化取引所へ前記第１の取引を送信するステップと、
代替の商取引システムへ前記第２の取引を送信するステップとに適合する、暗号化アダプタ構成要素をさらに備える、実施形態１９に記載の暗号化統合システム。
実施形態２４
１つまたは複数のプロセッサによって実行されるとき、装置に、
各々が共通の識別子を有し、かつ各々がある１人の第１の顧客に関連付けられる、第１のアドレス指定アカウントおよび第２のアドレス指定アカウントを作成するステップと、
前記第１のアドレス指定アカウントに関連付けられた１つまたは複数のデジタル取引品目を売買するための注文を受信するステップであって、前記注文が前記共通の識別子に関連付けられている、ステップと、
前記第１のアドレス指定アカウントに関連付けられたプライベートキーを使用して、第１の取引に電子サインし、前記第１のアドレス指定アカウントから前記第２のアドレス指定アカウントへ前記１つまたは複数のデジタル取引品目を転送するステップと、
前記第１のアドレス指定アカウントに関連付けられた前記プライベートキー、第２の取引に電子サインするステップと、
前記第１の取引が、前記第２の取引と同一のプライベートキーを使用してサインされたことを確認するステップと、
暗号化取引所での前記注文の申し込みを、前記第１の取引が、前記第２の取引と同一のプライベートキーを使用してサインされたことの確認に基づいて、認可するステップとを実行させる、命令のセットを含む非一時的コンピュータ可読記憶媒体。
実施形態２５
１つまたは複数のプロセッサによって実行されるとき、装置に、
ブローカディーラから、買入取引と売却取引をマッチさせる要求を受信するステップであって、
前記買入取引が、前記１つまたは複数のデジタル取引品目の額に対応した総額で前記１つまたは複数のデジタル取引品目を取得するための買入注文を含み、前記売却取引が、前記総額で前記１つまたは複数のデジタル取引品目を売却するための売却注文を含み、
前記買入取引が、前記買入注文を識別する第１のアドレス指定アカウントに対応した関連付けられた第１のサインを有し、前記売却取引が、前記売却注文を識別する第２のアドレス指定アカウントに対応した関連付けられた第２のサインを有し、前記第１のアドレス指定アカウントが、第１の顧客に関連付けられ、前記第２のアドレス指定アカウントが、第２の顧客に関連付けられ、前記総額が、前記第１の顧客に関連付けられた第３のアドレス指定アカウントに関連付けられ、前記１つまたは複数のデジタル取引品目が、前記第２の顧客に関連付けられた第４のアドレス指定アカウントに関連付けられる、ステップと、
前記買入取引を前記第３のアドレス指定アカウントへ、前記売却取引を第４のアドレス指定アカウントへマッピングするステップと、
暗号化取引所へ、前記買入取引を委託するために前記第１のサインおよび前記第２のサインを含むマッチ要求回答を送信するステップと、
前記買入取引および前記売却取引を確定し、清算するために、前記第１のアドレス指定

アカウントへ前記１つまたは複数のデジタル品目を転送し、前記第２のアドレス指定アカウントへ前記総額を転送するステップとを実行させる、命令のセットを含む非一時的コンピュータ可読記憶媒体。

【００７８】

コンピュータシステムの概要

[0092]本開示の実施形態は、上述した多様なステップおよび操作を含む。種々のこれらのステップおよび操作は、ハードウェア構成要素によって実行されてもよく、または機械実行可能な命令で実施されてもよく、これは、命令を含みプログラムされた汎用または専用プロセッサに、ステップを実行させるために使用されてもよい。別法として、ステップは、ハードウェア、ソフトウェア、および／またはファームウェアを組み合わせたものによって実行されてもよい。そのような、図１４は、本開示の実施形態が利用され得るコンピュータシステム１４００の一例である。本実施例によれば、コンピュータシステム１４００は、相互接続１４１０と、少なくとも１つのプロセッサ１４２０と、少なくとも１つの通信ポート１４３０と、主記憶装置１４４０と、リムーバブル記憶媒体１４５０と、リードオンリメモリ１４６０と、および大容量記憶装置１４７０とを含む。

【００７９】

[0093]プロセッサ１４２０は、任意の周知のプロセッサであってもよい。通信ポート１４３０は、たとえば、モデムベースのダイアルアップ接続での使用するためのＲＳ－２３２ポート、１０／１００イーサネットポート、または銅線もしくは光ファイバを使用したギガビットポートの任意のものであってもよいし、または、それを含んでもよい。通信ポート１４３０の種類は、ローカルエリアネットワーク（ＬＡＮ）、広域ネットワーク（ＷＡＮ）、またはコンピュータシステム１４００を接続する任意のネットワークなどのネットワークに応じて、選択されてもよい。

【００８０】

[0094]主記憶装置１４４０は、ランダムアクセスメモリ（ＲＡＭ）、または一般に当技術分野で知られている他の任意の動的記憶デバイスであってもよい。リードオンリメモリ１４６０は、プロセッサ１４２０用の命令などの静的な情報を記憶するためのプログラマブルリードオンリメモリ（ＰＲＯＭ）チップなどの、任意の静的記憶デバイスであってもよい。

【００８１】

[0095]大容量記憶装置１４７０は、情報および命令を記憶するために使用されてもよい。たとえば、ＳＣＳＩドライブのＡｄａｐｔｅｃ（登録商標）ファミリー、光ディスク、ＲＡＩＤドライブのＡｄａｐｔｅｃファミリーなどの、ＲＡＩＤなどのディスクのアレイ、または他の任意の大容量記憶装置などのハードディスクが、使用されてもよい。

【００８２】

[0096]相互接続１４１０は、１つまたは複数のバス、ブリッジ、制御装置、アダプタ、および／または二地点間接続であってもよいし、それを含んでもよい。相互接続１４１０は、他の、メモリ、記憶装置、および通信ブロックと共に、プロセッサ１４２０に通信可能に結合される。相互接続１４１０は、使用される記憶装置に応じて、ＰＣＩ／ＰＣＩ－ＸまたはＳＣＳＩに基づいたシステムバスであってもよい。

【００８３】

[0097]リムーバブル記憶媒体１４５０は、外部ハードドライブ、フロッピードライブ、コンパクトディスク・リードオンリメモリ（ＣＤ－ＲＯＭ）、書換え可能コンパクトディスク（ＣＤ－ＲＷ）、デジタルビデオディスク・リードオンリメモリ（ＤＶＤ－ＲＯＭ）のうちの任意の種類であり得る。

【００８４】

[0098]上で説明した構成要素は、いくつかの可能性の型を例示することを意図したものである。上述の実施例は、単なる例示的な実施形態であるので、それらが、一切本開示を制限してはならない。

【００８５】

用語

[0099]本出願を通して使用される、用語、略語、およびフレーズの簡単な定義を以下に示す。

【００８６】

[00100]用語の「接続された」または「結合された」、および関連する用語は、動作上の意味で使用されたものであり、直接、物理的な接続または結合に、必ずしも制限されない。したがって、たとえば、２つの装置は、直接結合されてもよいし、または１つまたは複数の中間媒体または装置を介して結合されてもよい。別の例として、複数の装置が、情報がそれらの間を通り得るよう結合され、一方で、互いの物理的接合を一切共有しない。本明細書で提供される本開示に基づいて、接続または結合が上述の定義に従って存在する種々の方法を当業者は理解されよう。

【００８７】

[00101]フレーズの「いくつかの実施形態では」、「いくつかの実施形態によれば」、「示された実施形態では」、「他の実施形態では」、「実施形態」、および類似のものは、通常、フレーズに続く具体的な特徴、構造、または特性が、少なくとも１つの本開示の実施形態に含まれ、かつ１つ以上の本開示の実施形態に含まれ得ることを意味する。加えて、そのようなフレーズは、必ずしも同一の実施形態または異なる実施形態を示さない。

【００８８】

[00102]明細書が、特徴が含まれる、または、特徴を有する「ｍａｙ（してもよい）」、「ｃａｎ（し得る）」、「ｃｏｕｌｄ（することがある）」または「ｍｉｇｈｔ（するかもしれない）」の構成要素または特徴を示す場合、その具体的な構成要素または特徴は、その特徴を含めるまたは有する必要はない。

【００８９】

[00103]用語「ｒｅｓｐｏｎｓｉｖｅ（応答する）」は、完全に、または部分的に応答することを含む。

[00104]用語「ｍｏｄｕｌｅ（モジュール）」は、ソフトウェア、ハードウェア、またはファームウェア（または、任意のそれらの組合せ）の構成要素を広く示す。モジュールは通常、有用なデータ、または他の、具体的な入力を使用した出力を発生させる、機能的な構成要素である。モジュールは、自立型であっても、そうでなくてもよい。アプリケーションプログラム（「アプリケーション」と呼ばれるものも）は、１つまたは複数のモジュールを含んでもよく、モジュールは、１つまたは複数のアプリケーションプログラムを含み得る。

【００９０】

[00105]用語「ネットワーク」は、通常、情報交換が可能な相互接続された装置のグループを示す。ネットワークは、ローカルエリアネットワーク（ＬＡＮ）上の数台のパーソナルコンピュータと同じくらい小さくも、またはインターネット、コンピュータの世界規模のネットワークと同じ位大きくもあり得る。本明細書で使用されるように、「ネットワーク」は、一つの存在から他の存在へ情報を送信する能力を有する任意のネットワークを包含することを意図している。場合によっては、ネットワークは、複数のネットワーク、さらに、１つまたは複数のボーダーネットワーク、音声ネットワーク、広帯域ネットワーク、金融ネットワーク、サービスプロバイダネットワーク、インターネットサービスプロバイダ（ＩＳＰ）ネットワーク、および／または公衆交換電話ネットワーク（ＰＳＴＮｓ）などの、複数の異種ネットワークから構成されてもよく、多様なネットワークの間または中で通信を支援する動作が可能なゲートウェイを介して相互接続される。

【００９１】

[00106]さらに、説明のために、本開示の多様な実施形態は、コンピュータプログラム、物理的構成要素、および現代のコンピュータネットワーク内の論理相互作用の文脈で本明細書において説明した。重要なことに、これらの実施形態が、現代のコンピュータネットワークおよびプログラムに関する、本開示の多様な実施形態を説明する一方で、本明細書で説明した方法および機器は、当業者に理解されるような、他のシステム、装置、およ

びネットワークに同等に適用可能である。したがって、本開示の実施形態の図示された用途は、制限があることを意味されず、しかしむしろ実施例である。本開示の実施形態を適用可能な他のシステム、装置、およびネットワークは、たとえば、通信およびコンピュータの装置およびシステムの他のタイプを含む。より具体的には、実施形態は、携帯電話の、ネットワーク、および互換性のある装置などの通信の、システム、サービス、および装置に適用可能である。加えて、実施形態は、パーソナルコンピュータから大規模ネットワークのメインフレームおよびサーバまで全てのコンピュータ化のレベルに適用可能である。

【００９２】

[00107]結論として、本開示は、デジタル取引品目を商取引するための新規なシステム、方法、および構成を提供する。本開示の１つまたは複数の実施形態の詳細な説明を上で示したが、本開示の技術思想から変化することない多様な代替物、変形例、および等価物が、当業者には明らかであろう。たとえば、上述の本実施形態が、具体的な特徴を示しても、本開示の範囲はさらに、説明した特徴の全ては含まれない特徴および実施形態の異なる組合せを有する実施形態を含む。したがって、本開示の範囲は、請求項の範囲に含まれる全てのそのような代替物、変形例、および変形形態を、全てのその等価物と共に包含することを意図する。そのため、上の説明は、制限するものとして理解すべきでない。

【図１】

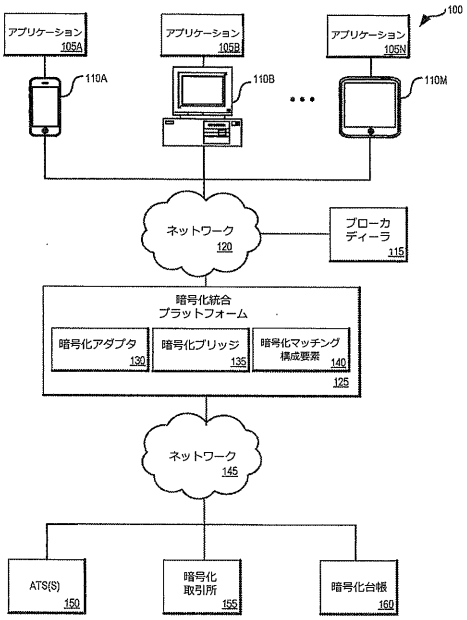


FIG. 1

【図２】

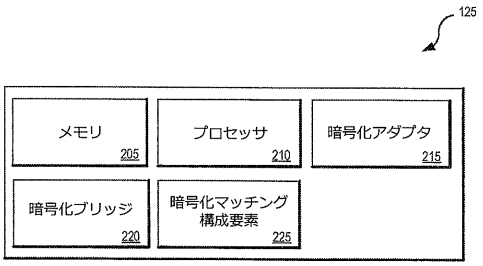


FIG. 2

【図３】

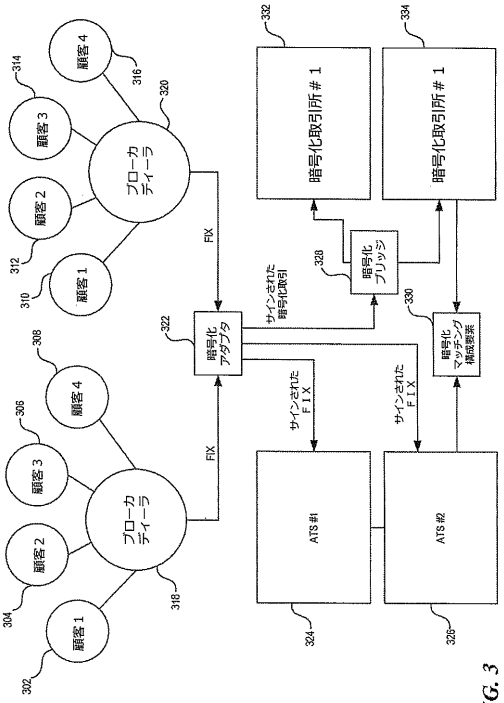


FIG. 3

【図４】

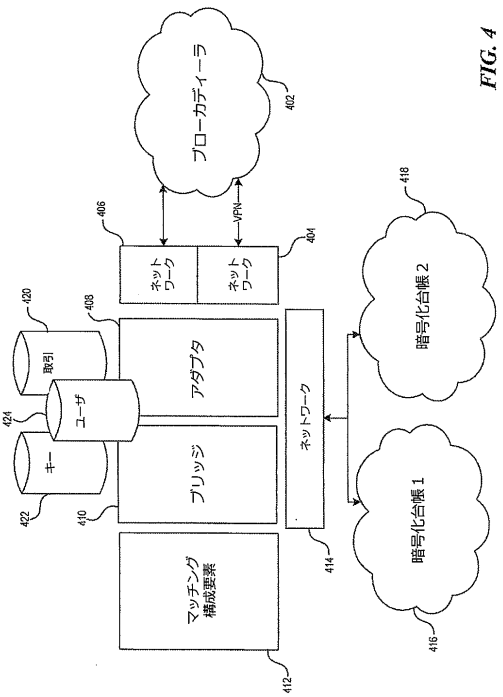


FIG. 4

【図５】

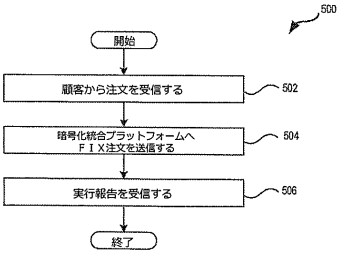
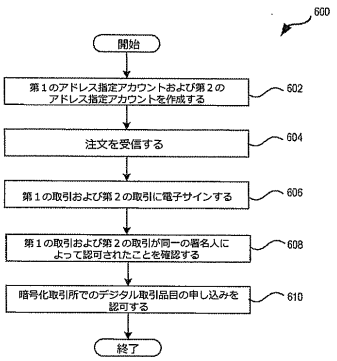


FIG. 5

【図６】



【図７】

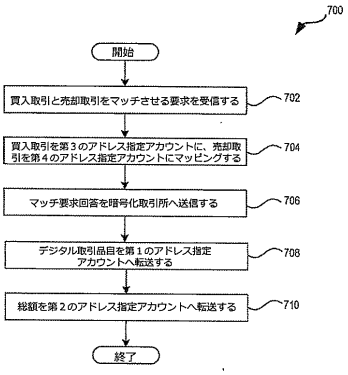


FIG. 7

【図８】

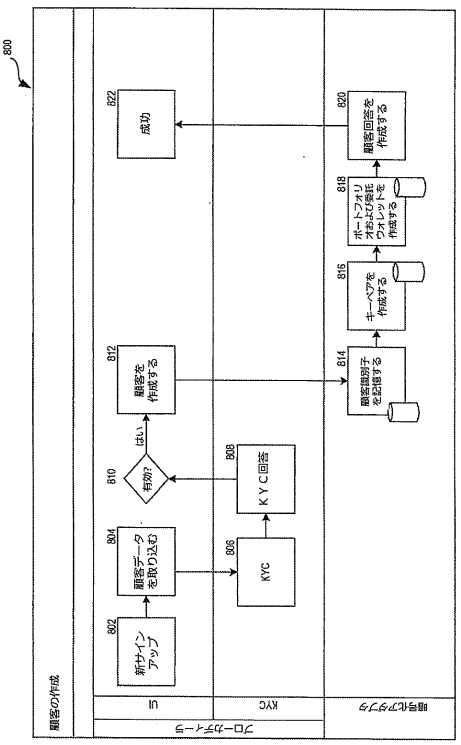


FIG. 8

【図９】

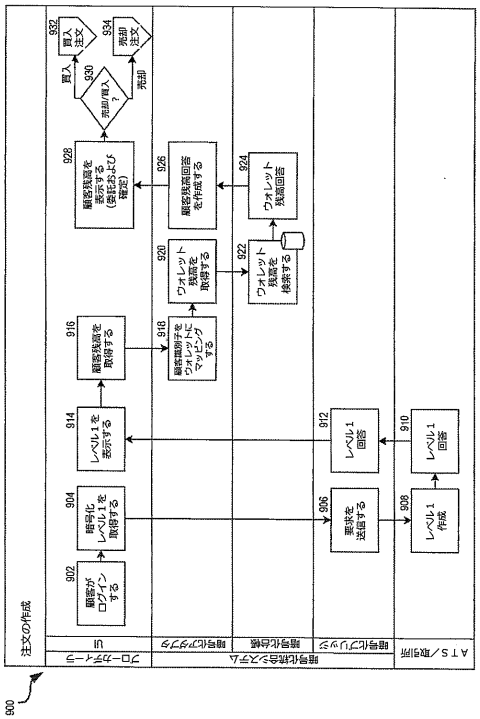


FIG. 9

【図１０】

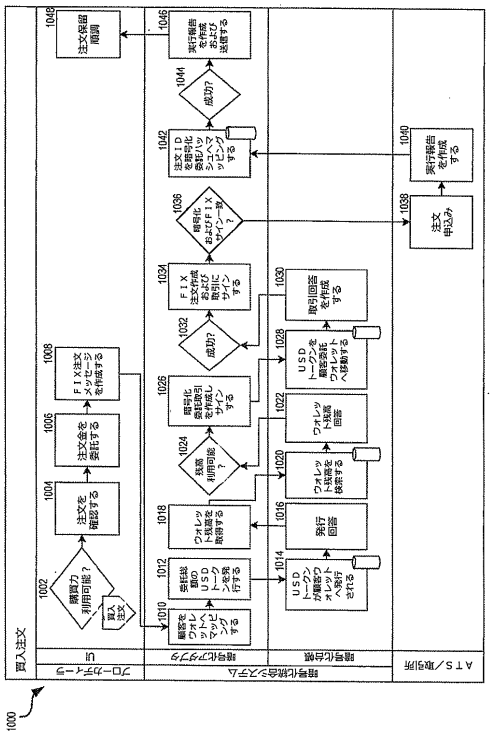


FIG. 10

【図１１】

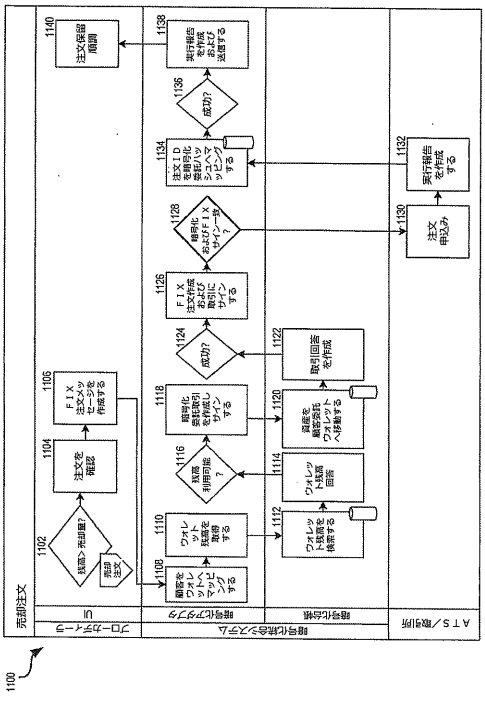


FIG. 11

【図１２】

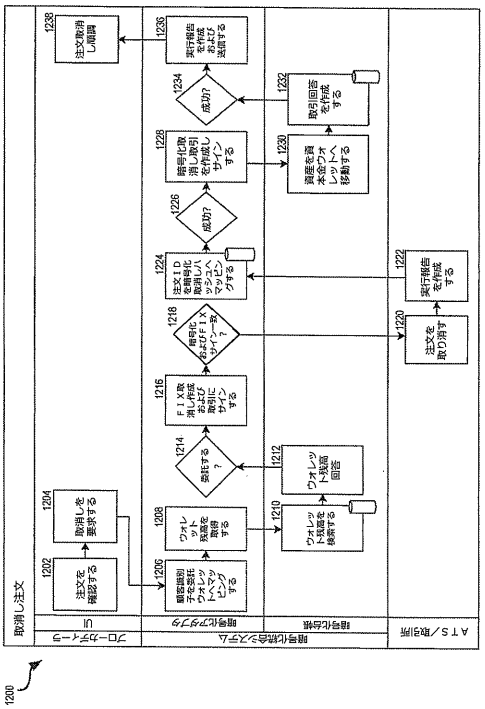


FIG. 12

【図１３】

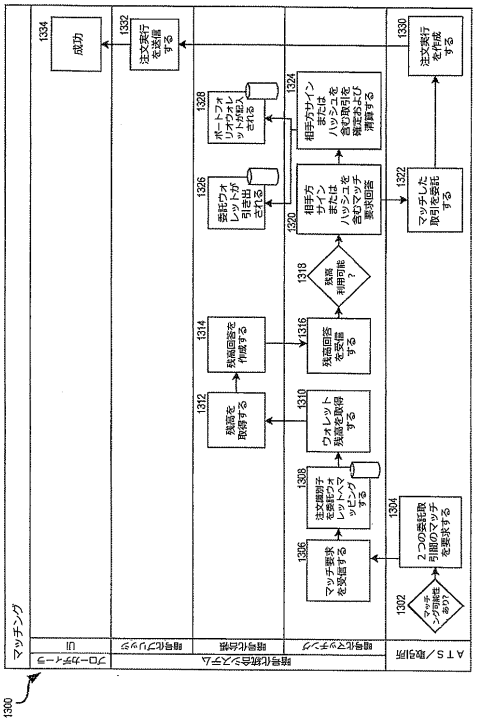


FIG. 13

【図１４】

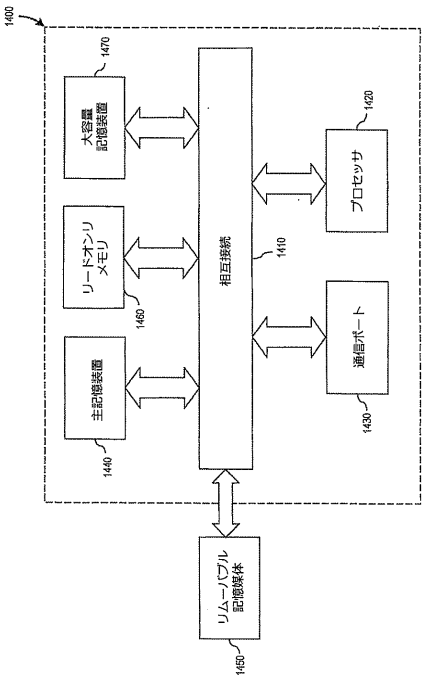


FIG. 14

【手続補正書】
【提出日】令和2年2月5日(2020.2.5)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
少なくとも１つのプロセッサと
前記少なくとも１つのプロセッサに通信可能に結合する少なくとも１つのメモリを備え、前記少なくとも１つのプロセッサは、
買入取引と売却取引をマッチさせる要求を受信するステップであって、
前記買入取引が、１つまたは複数のデジタル取引品目の額に対応した総額で前記１つまたは複数のデジタル取引品目を取得するための買入注文を含み、前記売却取引が、前記総額で前記１つまたは複数のデジタル取引品目を売却するための売却注文を含み、
前記買入取引が、前記買入注文を識別する第１のアカウントに対応した第１のプライベートキーの第１のサインを有し、前記売却取引が、前記売却注文を識別する第２のアカウントに対応した第２のプライベートキーの第２のサインを有し、前記第１のアカウントが、第１の顧客に関連付けられ、前記第２のアカウントが、第２の顧客に関連付けられ、
前記総額が、前記第１の顧客に関連付けられた第３のアカウントに関連付けられ、前記第３のアカウントに関連付けられる前記総額は、前記買入注文における使用のために委託されており、
前記１つまたは複数のデジタル取引品目が、前記第２の顧客に関連付けられた第４のアカウントに関連付けられ、前記第４のアカウントに関連付けられた前記１つまたは複数のデジタル取引品目は、前記売却注文における使用のために委託されている、ステップと、
前記買入取引を前記第３のアカウントへ、前記売却取引を前記第４のアカウントへマッピングするステップと、
暗号化取引所へ、前記買入取引を委託するために前記第１のサインおよび前記第２のサインを含むマッチ要求回答を送信するステップと、
前記買入取引および前記売却取引を確定し、清算するために、前記第２の顧客に関連付けられた前記第４のアカウントから前記第１の顧客に関連付けられた前記第１のアカウントへ前記１つまたは複数のデジタル取引品目を転送し、前記第１の顧客に関連付けられた前記第３のアカウントから前記第２の顧客に関連付けられた前記第２のアカウントへ前記総額を転送するステップと
を実行するよう構成される暗号化統合システム。
【請求項２】
前記少なくとも１つのプロセッサはさらに、
分散化された台帳から、前記マッチ要求回答を送信する前に、前記総額が、前記第３のアカウントに関連付けられ、前記１つまたは複数のデジタル取引品目が、前記第４のアカウントに関連付けられている確認を受信するステップを実行するよう構成される、請求項１に記載の暗号化統合システム。
【請求項３】
前記少なくとも１つのプロセッサはさらに、
リモートのコンピュータデバイスへ、前記買入取引および前記売却取引を確定し、清算した結果を公表するステップを実行するよう構成される、請求項１または２に記載の暗号化統合システム。
【請求項４】
コンピュータによって実行される方法であって、

ブローカディーラから、買入取引と売却取引をマッチさせる要求を受信するステップであって、

前記買入取引が、１つまたは複数のデジタル取引品目の額に対応した総額で前記１つまたは複数のデジタル取引品目を取得するための買入注文を含み、前記売却取引が、前記総額で前記１つまたは複数のデジタル取引品目を売却するための売却注文を含み、

前記買入取引が、前記買入注文を識別する第１のアカウントに対応した第１のプライベートキーの第１のサインを有し、前記売却取引が、前記売却注文を識別する第２のアカウントに対応した第２のプライベートキーの第２のサインを有し、前記第１のアカウントが、第１の顧客に関連付けられ、前記第２のアカウントが、第２の顧客に関連付けられ、

前記総額が、前記第１の顧客に関連付けられた第３のアカウントに関連付けられ、前記第３のアカウントに関連付けられる前記総額は、前記買入注文における使用のために委託されており、

前記１つまたは複数のデジタル取引品目が、前記第２の顧客に関連付けられた第４のアカウントに関連付けられ、前記第４のアカウントに関連付けられる前記１つまたは複数のデジタル取引品目は、前記売却注文における使用のために委託されている、ステップと、

コンピュータによって前記買入取引を前記第３のアカウントへ、前記売却取引を前記第４のアカウントへマッピングするステップと、

暗号化取引所へ、前記買入取引を委託するために前記第１のサインおよび前記第２のサインを含むマッチ要求回答を送信するステップと、

前記買入取引および前記売却取引を確定し、清算するために、前記第２の顧客に関連付けられた前記第４のアカウントから前記第１の顧客に関連付けられた前記第１のアカウントへ前記１つまたは複数のデジタル取引品目を転送し、前記第１の顧客に関連付けられた前記第３のアカウントから前記第２の顧客に関連付けられた前記第２のアカウントへ前記総額を転送するステップと

を備える、方法。

【請求項５】

分散化された台帳から、前記マッチ要求回答を送信する前に、前記総額が、前記第３のアカウントに関連付けられ、前記１つまたは複数のデジタル取引品目が、前記第４のアカウントに関連付けられている確認を受信するステップをさらに備える、請求項４に記載の方法。

【請求項６】

リモートのコンピュータデバイスへ、前記買入取引および前記売却取引を確定し、清算した結果を公表するステップをさらに備える、請求項４または５に記載の方法。

【請求項７】

命令のセットを含む非一時的コンピュータ可読記憶媒体であって、前記命令のセットは１つ又は複数のプロセッサにより実行されると、装置に

ブローカディーラから、買入取引と売却取引をマッチさせる要求を受信するステップであって、

前記買入取引が、１つまたは複数のデジタル取引品目の額に対応した総額で前記１つまたは複数のデジタル取引品目を取得するための買入注文を含み、前記売却取引が、前記総額で前記１つまたは複数のデジタル取引品目を売却するための売却注文を含み、

前記買入取引が、前記買入注文を識別する第１のアカウントに対応した第１のプライベートキーの第１のサインを有し、前記売却取引が、前記売却注文を識別する第２のアカウントに対応した第２のプライベートキーの第２のサインを有し、前記第１のアカウントが、第１の顧客に関連付けられ、前記第２のアカウントが、第２の顧客に関連付けられ、

前記総額が、前記第１の顧客に関連付けられた第３のアカウントに関連付けられ、前記第３のアカウントに関連付けられる前記総額は、前記買入注文における使用のために委託されており

前記１つまたは複数のデジタル取引品目が、前記第２の顧客に関連付けられた第４の

アカウントに関連付けられ、前記第４のアカウントに関連付けられる前記１つまたは複数のデジタル取引品目は、前記売却注文における使用のために委託されている、ステップと、
前記買入取引を前記第３のアカウントへ、前記売却取引を前記第４のアカウントへマッピングするステップと、
暗号化取引所へ、前記買入取引を委託するために前記第１のサインおよび前記第２のサインを含むマッチ要求回答を送信するステップと、
前記買入取引および前記売却取引を確定し、清算するために、前記第２の顧客に関連付けられた前記第４のアカウントから前記第１の顧客に関連付けられた前記第１のアカウントへ前記１つまたは複数のデジタル取引品目を転送し、前記第１の顧客に関連付けられた前記第３のアカウントから前記第２の顧客に関連付けられた前記第２のアカウントへ前記総額を転送するステップと
を実行させる、非一時的コンピュータ可読記憶媒体。
【請求項８】
請求項７に記載の非一時的コンピュータ可読記憶媒体であって、前記命令のセットは１又は複数のプロセッサにより実行されると、前記装置に
分散化された台帳から、前記マッチ要求回答を送信する前に、前記総額が、前記第３のアカウントに関連付けられ、前記１つまたは複数のデジタル取引品目が、前記第４のアカウントに関連付けられている確認を受信するステップ
を実行させる、非一時的コンピュータ可読記憶媒体。
【請求項９】
請求項７または８に記載の非一時的コンピュータ可読記憶媒体であって、前記命令のセットは１つ又は複数のプロセッサにより実行されると、前記装置に
リモートのコンピュータデバイスへ、前記買入取引および前記売却取引を確定し、清算した結果を公表させる、非一時的コンピュータ可読記憶媒体。
【請求項１０】
請求項１から請求項９のいずれか１項に記載の暗号化統合システム、方法、又は非一時的コンピュータ可読記憶媒体であって、
前記１つまたは複数のデジタル取引品目が、１つまたは複数のデジタル資産又はデジタル負債を含み、前記総額が、前記１つ又は複数のデジタル取引品目の額に対応した通貨、暗号化通貨、または前記通貨若しくは前記暗号化通貨の表示の総額を含む、暗号化統合システム、方法、又は非一時的コンピュータ可読記憶媒体。
【請求項１１】
請求項１から請求項１０のいずれか１項に記載の暗号化統合システム、方法、又は非一時的コンピュータ可読記憶媒体であって、
前記第１のアカウントが、前記第１の顧客に関連付けられた第１の顧客ポートフォリオアカウントであり、
前記第２のアカウントが、前記第２の顧客に関連付けられた第２の顧客ポートフォリオアカウントであり、
前記第３のアカウントが、前記第１の顧客に関連付けられた第１の顧客委託アカウントであり、
前記第４のアカウントが、前記第２の顧客に関連付けられた第２の顧客委託アカウントである、暗号化統合システム、方法、又は非一時的コンピュータ可読記憶媒体。
【請求項１２】
請求項１から請求項１１のいずれか１項に記載の暗号化統合システム、方法、又は非一時的コンピュータ可読記憶媒体であって、
前記１つ又は複数のデジタル取引品目はトークン化された資産を含む、暗号化統合システム、方法、又は非一時的コンピュータ可読記憶媒体。
【請求項１３】
請求項１から請求項１２のいずれか１項に記載の暗号化統合システム、方法、又は非一

時的コンピュータ可読記憶媒体であって、
前記１つ又は複数のデジタル取引品目は、トークン、現金、現金等価物、暗号化通貨、デジタル化ドル、デジタル資産、デジタル負債、デジタル株式、証券、及びデジタル資本金のうち少なくとも１つから選択される、暗号化統合システム、方法、又は非一時的コンピュータ可読記憶媒体。
【請求項１４】
請求項１から請求項１３のいずれか１項に記載の暗号化統合システム、方法、又は非一時的コンピュータ可読記憶媒体であって、
前記１つ又は複数のデジタル取引品目は、１または複数のデジタル資産又はデジタル負債を含み、前記総額は現金、暗号化通貨、又は前記１つ又は複数のデジタル取引品目の額に対応した通貨、暗号化通貨、または前記通貨若しくは前記暗号化通貨の表示の総額を含む、暗号化統合システム、方法、又は非一時的コンピュータ可読記憶媒体。

フロントページの続き

(72)発明者　ウィルキンズ，アレック
アメリカ合衆国ユタ州８４０４７，ミッドベール，ウエスト・コロシアム・ウェイ　７９９，ケア・オブ・ティー０．コム，インコーポレーテッド
(72)発明者　フィッシュ，エリック・ナサニエル
アメリカ合衆国ユタ州８４０４７，ミッドベール，ウエスト・コロシアム・ウェイ　７９９，ケア・オブ・ティー０．コム，インコーポレーテッド
(72)発明者　ラーソン，トレント・ノーマン
アメリカ合衆国ユタ州８４０４７，ミッドベール，ウエスト・コロシアム・ウェイ　７９９，ケア・オブ・ティー０．コム，インコーポレーテッド
(72)発明者　バーン，パトリック・エム
アメリカ合衆国ユタ州８４０４７，ミッドベール，ウエスト・コロシアム・ウェイ　７９９，ケア・オブ・ティー０．コム，インコーポレーテッド

Ｆターム(参考) 5L055 AA74

【外国語明細書】
2020099066000001.pdf