(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6697008号
(P6697008)
(45)発行日　令和2年5月20日(2020.5.20)　(24)登録日　令和2年4月27日(2020.4.27)

(51)Int.Cl.　F I
G06Q 40/04 (2012.01)　G06Q 40/04

請求項の数 22　(全 29 頁)

(21)出願番号　特願2017-564775(P2017-564775)
(86)(22)出願日　平成28年3月4日(2016.3.4)
(65)公表番号　特表2018-507501(P2018-507501A)
(43)公表日　平成30年3月15日(2018.3.15)
(86)国際出願番号　PCT/US2016/021069
(87)国際公開番号　WO2016/141361
(87)国際公開日　平成28年9月9日(2016.9.9)
審査請求日　平成31年3月1日(2019.3.1)
(31)優先権主張番号　14/639,895
(32)優先日　平成27年3月5日(2015.3.5)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　517309766
ゴールドマン　サックス　アンド　カンパニー　エルエルシー
アメリカ合衆国　ニューヨーク州　１０２８２，ニューヨーク，ウエスト　ストリート　２００
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介

最終頁に続く

(54)【発明の名称】取引の部分的認可に基づいて分散元帳を更新するシステム及び方法

(57)【特許請求の範囲】
【請求項１】
制御回路により実行される方法であって、
分散元帳に記憶された複数のデータアカウントから選択されたデータアカウントを修正する要求を受信することであって、前記選択されたデータアカウントは少なくとも１つの資産に関連付けられた少なくとも１つの値を記憶する、ことと、
前記受信した要求と前記少なくとも１つの資産とに基づいて複数の認可サーバを識別することであって、前記複数の認可サーバは、前記要求を実行できるかを認可する、ことと、
前記複数の認可サーバが前記要求を認可することに応答して前記分散元帳を修正することであって、前記複数の認可サーバの各々が、前記分散元帳の冗長コピーを記憶するように構成される、ことと、
前記分散元帳の少なくとも１つの修正された部分を前記複数の認可サーバの各々に送信することであって、前記複数の認可サーバの各々が、そのそれぞれの前記分散元帳の冗長コピーを、前記分散元帳の前記少なくとも１つの修正された部分で更新するように構成される、ことと、
前記複数の認可サーバを制御して、前記要求を含む取引を認可することに関連付けられた処理負荷を前記複数の認可サーバ間で分散させることであって、前記複数の認可サーバの各々における前記分散元帳の前記冗長コピーは、前記分散元帳の部分的な冗長コピーである、ことと、

を含む方法。
【請求項２】
前記分散元帳内の前記複数のデータアカウントを別様に暗号化することであって、第１のタイプの資産のデータにアクセスするために前記複数の認可サーバにより使用される復号処理は、第２のタイプの資産のデータにアクセスすることに使用できない、こと
をさらに含む請求項１に記載の方法。
【請求項３】
前記分散元帳は、支払い取引又は預入れ取引を処理するように修正され、
前記少なくとも１つの資産は、証券に対応し、
前記複数の認可サーバは、前記証券の発行当局に属する、
請求項１に記載の方法。
【請求項４】
前記証券の前記発行当局は、通貨を発行する中央銀行又は債券を発行する債券発行者のプロキシである、請求項３に記載の方法。
【請求項５】
前記複数の認可サーバは第１の認可者を集合的に形成し、前記少なくとも１つの資産は第１の資産及び第２の資産を含み、当該方法は、
前記受信した要求に基づいて第２の認可者のアイデンティティを決定することであって、前記第２の認可者は、前記第２の資産について前記要求を認可するように構成される、こと
をさらに含む請求項１に記載の方法。
【請求項６】
前記受信した要求は前記複数のデータアカウントの中のいくつかのデータアカウントに対する修正を含み、前記複数の認可サーバは複数の認可者のうちの第１の認可者を集合的に形成し、前記複数の認可者の各々が異なる資産に関連付けられ、当該方法は、
前記受信した要求に基づいて前記複数の認可者についての複数のアイデンティティを決定することであって、前記複数の認可者の各々が前記要求を認可するように構成される、こと
をさらに含む請求項１に記載の方法。
【請求項７】
前記複数の認可サーバは、前記要求を認可すべきかを、
前記選択されたアカウント及び前記少なくとも１つの資産について、公開された残高を前記分散元帳から取り出すことと、
保留の及び予約された支払いに関連付けられたシャドウ残高により前記公開された残高を低減することにより利用可能残高を計算することと、
前記利用可能残高が前記要求の取引額より大きいか又は等しいとき、前記要求を承認することと、
前記利用可能残高が前記要求の前記取引額より小さいとき、前記要求を拒否することと、
に基づいて決定するように構成される、請求項１に記載の方法。
【請求項８】
前記複数の認可サーバは、前記保留の及び予約された支払いに関連付けられた前記シャドウ残高と前記分散元帳の前記冗長コピーとを記憶するように構成される、請求項７に記載の方法。
【請求項９】
前記複数の認可サーバは、前記要求を認可すべきかを、
前記選択されたアカウントに関連付けられた当事者が前記要求を実行することを許可されているかを確認すること
に基づいて決定するように構成される、請求項１に記載の方法。
【請求項１０】

前記分散元帳の前記冗長コピーは、前記複数の認可サーバが前記少なくとも１つの資産とは異なる資産のデータにアクセスすることを防止するように暗号化される、請求項１に記載の方法。

【請求項１１】

前記分散元帳は、外国為替取引を処理するように修正され、

前記第１の資産は第１の通貨に対応し、前記第２の資産は第２の通貨に対応し、

前記第１の認可者は、前記第１の通貨の第１の発行当局に対応する複数のコンピューティング装置を含み、前記第２の認可者は、前記第２の通貨の第２の発行当局に対応する少なくとも１つの第２のコンピューティング装置を含む、

請求項５に記載の方法。

【請求項１２】

複数のアカウントを有する分散元帳を記憶するように構成されたメモリと、

前記複数のアカウントから選択されたアカウントを修正する要求を受信することであって、前記選択されたアカウントは少なくとも１つの資産に関連付けられ、

前記受信した要求に基づいて少なくとも１つの資産に関連付けられた複数の認可サーバのアイデンティティを決定することであって、前記複数の認可サーバは前記要求を認可するように構成され、

前記複数の認可サーバが前記要求を認可することに応答して前記分散元帳を修正することであって、前記複数の認可サーバの各々が、前記分散元帳の冗長コピーを記憶するように構成され、

前記分散元帳の少なくとも１つの修正された部分を前記複数の認可サーバの各々に送信することであって、前記複数の認可サーバの各々が、そのそれぞれの前記分散元帳の冗長コピーを、前記分散元帳の前記少なくとも１つの修正された部分で更新するように構成され、

前記複数の認可サーバを制御して、前記要求を含む取引を認可することに関連付けられた処理負荷を前記複数の認可サーバ間で分散させることであって、前記複数の認可サーバの各々における前記分散元帳の前記冗長コピーは、前記分散元帳の部分的な冗長コピーである

ように構成された制御回路と、

を含むシステム。

【請求項１３】

前記制御回路は、

前記分散元帳内の前記複数のアカウントを別様に暗号化し、第１のタイプの資産のデータにアクセスするために前記複数の認可サーバにより使用される復号処理は、第２のタイプの資産のデータにアクセスすることに使用できない

ようにさらに構成される、請求項１２に記載のシステム。

【請求項１４】

前記分散元帳は、支払い取引又は預入れ取引を処理するように修正され、

前記少なくとも１つの資産は、証券に対応し、

前記複数の認可サーバは、前記証券の発行当局に属する、

請求項１２に記載のシステム。

【請求項１５】

前記証券の前記発行当局は、通貨を発行する中央銀行又は債券を発行する債券発行者のプロキシである、請求項１４に記載のシステム。

【請求項１６】

前記複数の認可サーバは第１の認可者を集合的に形成し、前記少なくとも１つの資産は第１の資産及び第２の資産を含み、前記制御回路は、

前記受信した要求に基づいて第２の認可者のアイデンティティを決定することであって、前記第２の認可者は、前記第２の資産について前記要求を認可するように構成される

ようにさらに構成される、請求項１２に記載のシステム。

【請求項１７】
前記受信した要求は前記複数のアカウントの中のいくつかのアカウントに対する修正を含み、前記複数の認可サーバは複数の認可者のうちの第１の認可者を集合的に形成し、前記複数の認可者の各々が異なる資産に関連付けられ、前記制御回路は、
前記受信した要求に基づいて前記複数の認可者についての複数のアイデンティティを決定することであって、前記複数の認可者の各々が前記要求を認可するように構成される
ようにさらに構成される、請求項１２に記載のシステム。
【請求項１８】
前記複数の認可サーバは、前記要求を認可すべきかを、
前記選択されたアカウント及び前記少なくとも１つの資産について、公開された残高を前記分散元帳から取り出し、
保留の及び予約された支払いに関連付けられたシャドウ残高により前記公開された残高を低減することにより利用可能残高を計算し、
前記利用可能残高が前記要求の取引額より大きいか又は等しいとき、前記要求を承認し、
前記利用可能残高が前記要求の前記取引額より小さいとき、前記要求を拒否する
ように構成されることにより決定するように構成される、請求項１２に記載のシステム。
【請求項１９】
前記複数の認可サーバは、前記保留の及び予約された支払いに関連付けられた前記シャドウ残高と前記分散元帳の前記冗長コピーとを記憶するように構成される、請求項１８に記載のシステム。
【請求項２０】
前記複数の認可サーバは、前記要求を認可すべきかを、
前記選択されたアカウントに関連付けられた当事者が前記要求を実行することを許可されているかを確認する
ように構成されることにより決定するように構成される、請求項１２に記載のシステム。
【請求項２１】
前記分散元帳の前記冗長コピーは、前記複数の認可サーバが前記少なくとも１つの資産とは異なる資産のデータにアクセスすることを防止するように暗号化される、請求項１２に記載のシステム。
【請求項２２】
前記分散元帳は、外国為替取引を処理するように修正され、
前記第１の資産は第１の通貨に対応し、前記第２の資産は第２の通貨に対応し、
前記第１の認可者は、前記第１の通貨の第１の発行当局に対応する複数のコンピューティング装置を含み、前記第２の認可者は、前記第２の通貨の第２の発行当局に対応する少なくとも１つの第２のコンピューティング装置を含む、
請求項１６に記載のシステム。
【発明の詳細な説明】
【背景技術】
【０００１】
金融取引の処理は、特に外国為替市場において、実質的な決済リスクを伴う可能性がある。なぜならば、こうした取引は２つの部分を一般に含むからである。例えば、第１の当事者がユーロと引き換えに第２の当事者からある額の米国ドルを購入する取引は、２つの部分で処理されることがあり、すなわち、（ｉ）第１の当事者から第２の当事者へのユーロの移転、及び（ｉｉ）第２の当事者から第１の当事者への米国ドルの移転である。信頼された第三者がいない場合、こうした外国為替取引の２つの部分は、様々な処理時間、タイムゾーン差、又は他のファクタに起因して、異なる時間に処理される。取引の双方の部分が完了されるまで、取引のうち自己の部分を完了しており、しかしまだ他方の当事者か

ら資金を受け取っていない当事者は、リスクにさらされる。なぜならば、他方の当事者がその義務を怠る可能性があるからである。上記リスクは「ヘルシュタット」リスクとして知られる。

【０００２】

外国為替取引に関連付けられたヘルシュタットリスクを軽減するために、取引は、信頼された第三者（例えば、ＣＬＳ）が決済することがある。信頼された第三者は、そのメンバ機関（例えば、商業銀行）からの取引を受け入れ、一方の当事者の資金を他方の当事者もまたその資金を提供するまで一時的に保持し、それから、取引のすべての部分を一緒に処理する。信頼された第三者は、ゆえに、取引がその全体を処理されるか、あるいはまったく処理されないかのいずれかであることを確保する。さらに、信頼された第三者は、資金が特定の取引に対して予約され、無関係の取引に使用できないことを保証することができる。取引を処理することについての上記の「全か無か」のアプローチは、「原子的決済」又は「支払い対支払い」として知られる。しかしながら、信頼された第三者の使用は、必ずしも、所与の営業日にわたり取引が決済する所定の順序を確立しない。ＦＸ市場において、現在の慣例は、特定の日に対してスケジュールされた取引はその日の間に任意の時間に決済することができ、このことは、当事者が十分な資金を維持して、取引が処理される順序にかかわらず資金が利用可能であることを確保することを必要とする。より悪いケースのシナリオのための予算の必要は、このいわゆる日中流動性（intraday liquidity）要件を満たすために大量の資金が取っておかれることを必要とする可能性がある。

【０００３】

日中流動性要件は、新しい取引が開始される前に取引が決済するようにリアルタイム近くで取引を処理することにより、低減することができる。従来のバンキングシステムにおいて、このことは、不可能ではないにしても実現するのが困難である。なぜならば、支払いが複数の秘密の元帳をとおして移動する必要があり、ゆえに遅延を被るからである。暗号通貨、例えばビットコイン（Bitcoin）又はリップル（Ripple）などは、すべての参加者について単一の元帳に取引記録を保持し、ゆえに、順番に、及び従来のバンキングシステムと比較して速く、取引を処理することができる。例えば、リップルはおよそ数秒の間に、ビットコインはおよそ数時間の間に、取引を典型的に処理する。しかしながら、これらシステムは、プライバシーの観点で大幅な不利益に悩まされる。なぜならば、これらは、分散サーバに記憶された公的にアクセス可能な元帳内に残高及び取引記録を維持するからである。この透過性は、多くの当事者が元帳に適用された変更を観察及び承認することを可能にすることにより、記録の正確さを維持するのに役立つ。例えば、単独の悪意ある行為者がいくつかのサーバ上の記録を偽造することができる可能性がある一方、公的に利用可能な元帳の広い散布は、こうした悪意ある行為者が十分な元帳コピーを変造することを防止する可能性がある。元帳の広い分散は、記録の正確さのために望ましいことがあるが、この公的な可用性は、それが当事者の流動性を供給する意欲を低減する可能性があり、卸売市場参加者の制御された可視性をサポートする望みに反する。例えば、流動性を提供することに関連付けられたコストが、マーケットメーカーに対して増加する可能性がある。なぜならば、取引が十分に可視であり、このことは、マーケットメーカーが取引に関連付けられたリスクをヘッジする前に他の当事者がその挙動を変更することを可能にするからである。実際、このことは、取引が公開されるとすぐに市場がマーケットメーカーに反して動くことを意味する。顧客とマーケットメーカーとの双方がこのことを知っているため、予期されるさらなるコストがマーケットメーカーから顧客に渡される。上記理由で、大きい取引における買い手又は売り手のいずれも、即時の公開に関心を有さない。大抵の規制された証券取引所は、少なくともいくつかのトレードの遅延した公開を許容するルールを有する。マーケットメーカーに反して動く慣例は略奪的トレーディングとして知られ、2005年8月の“The Journal of Finance”vol. LX, No.4に公開されたMarkus K. Brunnermeier及びLasse H. Pedersen著の学術論文“Predatory Trading”に詳細に論じられており、上記論文は本明細書においてその全体を参照により援用される。

【０００４】

暗号元帳システム、例えばビットコイン及びリップルなどが、特定の実世界当事者に帰するのに容易でない無作為アカウント番号を使用することにより特定の当事者のアイデンティティを難読化することができる一方、大手金融機関（例えば、中央銀行）は、こうした難読化単体に頼ることはできない。なぜならば、大手金融機関の取引の純粋なサイズ及びボリュームが、そのアイデンティティを一般市場に明らかにする可能性があるからである。さらに、既存の暗号取引システム、例えばビットコイン又はリップルなどは、反マネーロンダリング（ＡＭＬ）を取り締まることで規制者を支援する設計されたアイデンティティチェックを欠いている。

【０００５】

結果として、関与する当事者のプライバシーを犠牲にすることなくビットコインやリップルのように迅速に取引を処理することができる新しいシステム及び方法の必要がある。

【０００６】

関連出願の相互参照

本出願は、2015年3月5日に申請された米国特許出願第14/639,895号に対する優先権を主張し、上記出願はその全体を本明細書において参照により援用される。

【発明の概要】

【０００７】

開示されるシステム及び方法は、分散された元帳のコピーを暗号認証手法に基づいて維持及び更新する複数のサーバを含む分散コンピュータネットワークに一般に向けられる。より詳細に、システム及び方法は、実質的にリアルタイムで行われる通貨交換などの交換又は他タイプの交換を追跡する。上記目的のために、システムは、個々を許可し、資産（例えば、規制された通貨）のいくらかの額を表すアカウントを上記個々に関連付ける。システムは、分散元帳の冗長コピー内に維持されるアカウント残高を調整することにより、２つ以上の許可された個々間で、実質的にリアルタイムで、単一の資産内における支払いを実行し、あるいは２つ以上の資産を交換する。さらに、システムは、秘密の及びセキュアな形式で交換を手配して、第三者が交換処理の前又は間に交換を観察すること（又は、元帳残高を調整すること）を防止する。

【０００８】

本明細書に説明されるシステム及び方法は、元帳を制御する元帳管理サーバを含み、支払い又は外国通貨交換取引がリアルタイム又は実質的にリアルタイムで発生することを可能にする。システムは、確認されたアカウント保持者とそれぞれのアカウント保持者により保持される各資産の残高とを記録するデータテーブルを作成する。システムは、資産発行当局をさらに記録する。各資産発行当局は、アカウント保持者の１つ以上により保持される特定の資産の供給を制御する当局（又は、該当局のプロキシ）である。システムは、認可処理を含み、該認可処理は、各アカウント保持者のアカウントに対するビュー／承認アクセスを各資産発行当局に提供し、しかしそのアクセスを、上記アカウントのうち上記発行当局により発行される資産における残高を記録する部分に制限する。

【０００９】

システムは、アカウント情報及びアカウント残高を含むデータテーブルの冗長コピーを、元帳管理サーバにおいて、及び資産発行当局に関連付けられた資産認可サーバにおいて記憶する。データテーブルの分散された記憶は、元帳のデータテーブル内に記憶された情報を偽造する試みからのさらなる保護を提供し、なぜならば、２つ以上のサーバが危険にさらされる必要があることになるからである。システムは、認証手法を使用して、識別情報を確認し、顧客確認（know-your-customer）（ＫＹＣ）又は反マネーロンダリング（anti-money laundering）（ＡＭＬ）チェックを実行する。システムは、暗号コードを使用して、データメッセージにアペンドされた電子署名を、署名した当事者の公開鍵を用いて上記電子署名とデータメッセージを処理することから取得されるハッシュとを比較することによって認証する。

【００１０】

アカウント保持者は、クライアント装置、例えばパーソナルコンピュータ、ラップトッ

プ、スマートフォン、又は他の適切なタイプの装置などをとおして、システムに取引を提出することができる。ユーザ入力に応答して、クライアント装置は、例えば第１の当事者から第２の当事者への、移転されるべき取引額を含むデータメッセージを生成することができる。取引は、単一の資産、又は、外国為替取引の場合と同様に複数の資産に関与することがある。クライアント装置は、取引の処理を制御する元帳管理サーバに直接、データメッセージを送信することができる。クライアント装置はさらに、他のサーバ、例えば商業銀行により維持されるサーバなどにデータメッセージを送信してもよく、これらサーバは、次に、元帳管理サーバにメッセージをリレーすることができる。データメッセージは、クライアント装置によりアペンドされた電子署名を含むことができる。上記電子署名を元帳管理サーバが処理して、データメッセージがクライアント装置から送信され、かつそれぞれのアカウント保持者により許可されたことを確認することができる。電子署名を確認することに応答して、元帳管理サーバは、プロセッサを用いて、取引に関連付けられた資産を識別し、利用可能残高をチェックし、ＫＹＣ認可を実行することができる。例えば、第１の当事者がユーロと交換で第２の当事者から米国ドルを購入する外国為替取引のデータメッセージは、「米国ドル」及び「ユーロ」それぞれにおける取引額を含むことがある。取引に関連付けられた資産を決定することに追加で、元帳管理サーバは、プロセッサをさらに用いて、取引を認可する資産認可サーバのセットを識別することができる。例えば、資産認可サーバの各々は、取引に関与する特定の資産の発行当局に関連付けられることができる。資産認可サーバのセットを識別することに応答して、元帳管理サーバは、取引データに基づいてデータメッセージを作成し、それを資産認可サーバの各々に送信する。データメッセージを作成することの一部として、元帳管理サーバは電子署名をアペンドすることができ、上記電子署名を資産認可サーバの各々が使用して、データメッセージが元帳管理サーバにより送信されたことを確認することができる。

【００１１】

所与の資産に関連付けられた資産認可サーバは、上記所与の資産のための元帳内に含まれるアカウント残高の冗長記録を作成し、記憶する。冗長記録を資産認可サーバが用いて、元帳管理サーバとは独立してアカウント保持者の残高を確認することができる。元帳管理サーバから取引に対応するデータメッセージを受信することに応答して、資産認可サーバは、プロセッサを用いて、その記録に記憶されたアカウント残高とデータメッセージ内に提供される取引額と比較することができる。アカウント残高が取引額より大きい場合（すなわち、十分な資金が利用可能である場合）、資産認可サーバは、取引の処理を継続することができる。そうでない場合、資産認可サーバは、データメッセージを元帳管理サーバに伝達して、取引が拒否されるべきであると示すことができる。資産認可サーバは、データメッセージに電子署名をアペンドすることができ、上記電子署名を元帳管理サーバが使用して、データメッセージの信ぴょう性を確認することができる。

【００１２】

資産認可サーバが、データメッセージに含まれるすべてのアカウント保持者について、及びそれが責任を負うすべての資産について、アカウント残高が取引額より大きいか又は等しいと決定する場合、資産認可サーバは、取引が処理されるように継続すると同時に、該資産認可サーバに記憶されたアカウント残高を修正して、取引額に等しい残高を予約する。例えば、資産認可サーバは、別個のデータ構造を採用して、現在の又は保留している取引に関連付けられた支払い額を更新することができる。利用可能残高の一部分を予約して「シャドウ残高」を取得することにより、資産認可サーバは、「二重支出」又は「リプレイ」の見込みを低減することができる。上記二重支出又はリプレイは、利用可能残高を更新するより速く取引を処理するシステムにおいて発生する可能性がある。こうしたシステムでは、利用可能残高を個々には満たすが累積的には超える詐欺取引が承認される可能性があり、なぜならば、システムが取引と取引との間に利用可能残高を更新しない可能性があるからである。資産認可サーバは、取引が処理されるように継続すると同時にシャドウ残高を維持することによってこうした二重支出を除外するのに役立つ。

【００１３】

元帳管理サーバは、規制要件に従ってＫＹＣチェックをさらに実行することできる。元帳管理サーバは、例えば、商業銀行などのＫＹＣ認可者から署名されたメッセージにおいて上記ＫＹＣ許可の指標を受信すると、上記指標を編集し、ルックアップテーブル内に記憶することができる。いくつかの態様において、ＫＹＣ許可は、信頼のチェーン（chain of trust）に基づくことができる。例えば、元帳管理サーバは、対応するＫＹＣ認可者がクライアントを信頼することを示し、元帳管理サーバ（又は、取引に関与する資産に関連付けられた資産認可者）が上記ＫＹＣ認可者を同様に信頼する場合、ＫＹＣ許可を受け入れるように決定することができる。元帳管理サーバが、取引の当事者のうちいずれかが有効なＫＹＣ許可に関連付けられていないと決定する場合、元帳管理サーバは、取引を拒否し、対応する署名されたメッセージを取引に関与する当事者に提供することができる。

【００１４】

２つ以上の資産に関与する取引について、元帳管理サーバは、取引に関与する各資産の資産認可サーバから別個のデータメッセージを受信する。メッセージの受信に応答して、元帳管理サーバは、取引が（例えば、不十分な資金に起因して）拒否されるべきであるとの指標をデータメッセージのうち１つ以上が含むかを決定する。データメッセージのうち少なくとも１つがこうした拒否を含む場合、元帳管理サーバは、取引をその全体で拒否し、取引に関与するいかなる当事者の元帳アカウント残高も更新しない。逆には、資産認可サーバから受信されるデータメッセージのすべてが、取引が承認されるべきであるとの指標を含む場合、元帳管理サーバは、その暗号化された元帳のコピー内に維持されるアカウント残高を更新する。

【００１５】

元帳管理サーバは、更新された元帳のうちの部分を資産認可サーバにデータメッセージの形式で送信する。特定の資産認可サーバに送信されるデータメッセージは、上記特定の資産認可サーバにより維持される資産において保持されるアカウントの残高のみ含むことができる。例えば、米国ドルの認可サーバは、更新された元帳のうち、米国ドルにおけるアカウントに対応する部分のみ送信されることができる。データメッセージは、更新された元帳に組み込まれている完了した取引のリストをそのそれぞれの一意識別子及び取引額と一緒にさらに含んでもよい。データメッセージを受信することに応答して、資産認可サーバは、その記録を、上記完了した取引のリストに基づいて、予約された及び保留している支払いの記録及びアカウント残高を修正することによって更新することができる。例えば、資産認可サーバは、完了した取引の取引額をシャドウ残高から除去することができ、なぜならば、完了した取引は、更新された元帳内に含まれるアカウント残高内に今や反映されているからである。資産認可サーバはさらに、上記取引のリストに含まれる取引に対応するステータス指標を更新して、上記取引が完了しており、もはや保留していないことを表すことができる。元帳管理サーバから資産認可サーバへのアカウント残高の周期的な伝達は、元帳管理サーバと資産認可サーバとにおいて別個に維持される暗号化された元帳の分散された及び冗長なコピーが一貫性のあるままであることを確保するのに役立つ。

【００１６】

要約すると、本明細書に説明されるシステム及び方法は、実質的にリアルタイムで動作することができるシステムアーキテクチャを提供することにより、現在の交換処理において生じる大幅な時間遅延の問題に対処する。システム及び方法は、交換処理のコンポーネントの、ＫＹＣ標準を満足することができるアイデンティティチェックを行うことにより、現在の交換処理に参加する当事者のアイデンティティ確認の欠如の問題にさらに対処する。システム及び方法は、アカウント残高又は取引に関する情報を知り又はその他の方法でアクセスする必要がない第三者に対して上記情報を開示する問題にさらに対処し、これにより、現在の交換処理と比較して取引を行うコストを低減することができる。

【００１７】

本開示の実施形態に従い、複数のアカウントを有するデータテーブルを実質的にリアルタイムで修正するシステム及び方法が提供される。システム及び方法は、複数のデータア

カウントから選択されたデータアカウントを修正する要求を受信することができ、選択されたアカウントは少なくとも１つの資産を含み、上記の受信した要求と上記少なくとも１つの資産とに基づいて認可者のアイデンティティを決定することができ、認可者は要求を実質的にリアルタイムで認可するように構成される。システム及び方法は、さらに、認可者が要求を認可する場合、データテーブルを実質的にリアルタイムで修正することができる。

【００１８】

いくつかの実装において、認可者は、第１の認可者であり得、少なくとも１つの資産は、第１の及び第２の資産を含むことができる。システム及び方法は、受信した要求に基づいて第２の認可者のアイデンティティを決定することをさらに含むことができ、第２の認可者は、第２の資産について実質的にリアルタイムで要求を認可する。

【００１９】

いくつかの実装において、データテーブルは、支払い取引又は預入れ取引を処理するように修正され、少なくとも１つの資産は、通貨又は債券に対応し、認可者は、通貨又は債券の発行当局である。いくつかの態様において、通貨又は債券の発行当局は、通貨を発行する中央銀行又は債券を発行する債券保持者のプロキシである。いくつかの実装において、データテーブルは、外国為替取引を処理するように修正され、第１の資産は第１の通貨に対応し、第２の資産は第２の通貨に対応する。さらに、第１の認可者は、第１の通貨の第１の発行当局に対応し、第２の認可者は、第２の通貨の第２の発行当局に対応する。他の実装において、受信した要求は、複数のアカウントの中のいくつかのアカウントに対する修正を含み、認可者は、複数の認可者のうちの第１の認可者であり、複数の認可者の各々が、異なる資産に関連付けられる。さらに、システム及び方法は、受信した要求に基づいて複数の認可者についての複数のアイデンティティを決定することを含み、複数の認可者の各々は、要求を実質的にリアルタイムで認可する。

【００２０】

いくつかの実装において、システム及び方法は、データテーブル内の複数のアカウントを別様に暗号化することができ、したがって、第１の認可者により第１の資産のデータにアクセスするのに使用される復号処理は、第２の資産のデータにアクセスするのに使用することはできない。

【００２１】

いくつかの実装において、認可者は、要求を認可すべきかどうかを、アカウント及び少なくとも１つの資産についてデータテーブルから公開された残高を取り出すことと、保留の及び予約された支払いに関連付けられたシャドウ残高により公開された残高を低減することにより利用可能残高を計算することと、によって決定することができる。システム及び方法は、さらに、利用可能残高が要求の取引額より大きいか又は等しいとき、要求を承認し、利用可能残高が要求の取引額より小さいとき、要求を拒否することができる。いくつかの実装において、認可者は、保留の及び予約された支払いに関連付けられたシャドウ残高とデータテーブルの冗長コピーとを記憶する。

【００２２】

いくつかの実装において、認可者は、要求を認可すべきかどうかを、アカウントに関連付けられた当事者が要求を実行することを許可されているかどうかを確認することに基づいて決定する。

【００２３】

いくつかの実装において、認可者は、データテーブルの冗長コピーを記憶し、システム及び方法は、データテーブルを修正することに応答してデータテーブルの修正された部分を認可者に送信することをさらに含む。いくつかの実装において、データテーブルの冗長コピーは、認可者が上記少なくとも１つの資産とは異なる資産のものであるデータにアクセスことを防止するように暗号化される。

【図面の簡単な説明】

【００２４】

例示を目的として、いくつかの実施形態が下記の図面内に説明される。
【図１】分散元帳を維持及び更新する分散コンピュータシステムのブロック図である。
【図２】可視性制限を例示する分散元帳の図である。
【図３】元帳管理ネットワークのブロック図である。
【図４】元帳残高及びアカウント情報を分散元帳内に記憶する一例示的なデータ構造を表す。
【図５】分散元帳の部分的な冗長コピーを各々記憶する認可サーバから受信されたデータメッセージに基づいて、上記元帳を更新する処理のフローチャートである。
【図６】公開鍵及び秘密鍵を用いた認証方法の概略である。
【図７】元帳管理サーバ７０２及び２つの資産認可サーバにより取引を処理するフローチャートである。
【発明を実施するための形態】
【００２５】
下記の説明において、例示の目的で複数の詳細が説明される。しかしながら、本明細書に説明される実施形態はこうした特定の詳細の使用なく実施できることを当業者は認識するであろう。他の例において、不要な詳細で本説明を分かりにくくしないように、良く知られる構造及び装置はブロック図形式内に示されない。
【００２６】
図１は、分散された元帳を維持及び更新する分散されたコンピュータシステム１００の一例示的なブロック図である。コンピュータシステム１００は、元帳管理サーバ１０２、アカウントオペレータサーバ１２０、資産認可サーバ１３０、１３２、及び１４２、プロキシ認可サーバ１４０、並びにＫＹＣ認可サーバ１５０を含む。元帳管理サーバ１０２は、クライアント１１２～１１６に直接接続されてもよく、アカウントオペレータサーバ１２０をとおしてクライアント１２２～１２６に接続されてもよい。１つの例において、コンピュータシステム１００のサーバは、適切なネットワークインターフェースをとおして互いに接続されるスタンドアロンサーバであり得る。別の例において、コンピュータシステム１００は、クラウドベースのコンピューティング環境内に実装されてもよい。その場合、コンピュータシステム１００のサーバは各々、１つ以上の物理サーバ上で稼働する仮想マシンとして実装されることがある。
【００２７】
クライアント１１２～１１６（一般に、クライアント１１２）及びクライアント１２２～１２６（一般に、クライアント１２２）は、アカウント保持者が上記分散元帳に記憶された残高（balances）にアクセスするのに用いることができる。クライアント１１２は、パーソナルコンピュータ、ラップトップ、スマートフォン、又は任意の他の適切なコンピューティング装置であり得る。クライアント１１２は、プロセッサ及び記憶回路を含み、記憶回路は、クライアント１１２がアカウントオペレータサーバ１２０又は元帳管理サーバ１０２との間で（例えば、データメッセージの形式の）情報を交換することを可能にするソフトウェア又は他の命令を記憶する。１つの例において、アカウントオペレータサーバ１２０をとおしてクライアント１２２を元帳管理サーバ１０２に結合することはシステム１００のスケーラビリティを向上させる可能性があり、なぜならば、アカウントオペレータよりさらに多くのクライアントが存在する可能性があるからである。
【００２８】
クライアント１２２は、クライアント１２２に関連付けられたアカウント保持者のアカウント残高を記憶することができる。別法として、又は追加的に、クライアント１２２は、アカウントオペレータサーバ１２０にアカウント残高を記憶させてもよい。１つの例において、クライアント１２２は、アカウントオペレータサーバ１２０に排他的にアカウント情報を記憶することができ、なぜならば、クライアント１２２は窃盗に対して脆弱である可能性があり（例えば、クライアント１２２がモバイル装置である場合）、あるいは（ハッキングをとおして）不法にアクセスされ又は（例えば、ソフトウェアウィルスでの感染により）改竄されることのより高い機会を有する可能性があるからである。アカウント

オペレータサーバ１２０は、プロセッサ及び記憶回路を含み、アカウント保持者ごとのアカウント情報を記憶し、分散元帳に保持されるアカウント残高をアカウント保持者により維持される従来的な銀行アカウント（例えば、当座預金又は普通預金（savings）口座）に関連付けることができる。例えば、アカウントオペレータサーバ１２０は、商業銀行サーバであり得る。

【００２９】

元帳管理サーバ１０２は、分散元帳のマスタコピーを記憶し、このマスタコピーには、システム１００におけるすべてのアカウント保持者のアカウント残高が含まれる。各アカウント保持者のアカウントは、複数の資産における残高を含むことができる。元帳管理サーバ１０２は、プロセッサを用いて、クライアント１２２から（可能性として、アカウントオペレータサーバ１２０をとおして）データメッセージの形式で受信した取引を処理することができる。取引は、単一の資産又は複数の資産に関与することがある（例えば、外国為替（foreign exchange）取引の場合、双方の通貨である２つの資産が存在することになる）。元帳管理サーバ１０２は、資産認可サーバ１３０及び１３２（一般に、資産認可サーバ１３０）に結合することができ、元帳管理サーバ１０２による取引の処理には、元帳管理サーバ１０２と資産認可サーバ１３０とにおけるデータメッセージの交換を含むことができる。

【００３０】

資産認可サーバ１３０は、プロセッサと、分散元帳の冗長コピーを記憶するように構成された記憶回路とを含むことができる。冗長コピーの記憶は、元帳のロバスト性、信頼性、及びセキュリティを向上させる可能性がある。なぜならば、暗号化された分散元帳により記憶されたアカウント残高を偽造し、あるいはその他の方法で変造するためには、冗長コピーのうち複数が修正される必要があることになるからである。元帳管理サーバ１０２及び資産認可サーバ１３０が互いに独立して動作するとき、双方のサーバを危険にさらすタスクは、より困難にされる。

【００３１】

元帳の分散されたコピーでアカウント残高が一般市場に対して可視にされることを回避するために、元帳管理サーバ１０２及び資産認可サーバ１３０は、記憶された元帳に対する読み出し又は書き込みアクセスを得るのにユーザ名及びパスワード、２ファクタの認証、又は他の適切な形式のアクセス制御を必要とすることにより、記憶された元帳への可視性をさらに制御することができる。さらに、元帳管理サーバ１０２が分散元帳に対するフルアクセスを有することができると同時に、資産認可サーバ１３０は、元帳のうち、資産認可サーバ１３０により認可される（validated）特定資産のアカウント残高を含む部分に対するアクセスのみ付与されることができる。例えば、認可サーバ１３０及び１３２の各々が、ある資産（例えば、米国ドル若しくはユーロなどの不換通貨、ビットコイン若しくはリップルなどの暗号通貨、又は任意の他の適切なタイプの資産、例えば債券など）に関連付けられ、上記資産の発行当局（issuing authority）（例えば、上記通貨の中央銀行、又は債券の債券発行者）により操作されることができる。上記シナリオにおいて、資産認可サーバ１３０は、システム１００の元帳に記憶された資産の各単位が、対応する資産認可者（asset validator）により保持又は制御される資産の「現実の（real-life）」単位で裏付けられる（backed）ことを確保することができる。ゆえに、元帳は、一般市場に対して機密の取引情報を明らかにすることなく、所与の資産の供給を監督する規制者に対して透過的であることにより、顧客の信用を維持することができる。

【００３２】

元帳管理サーバ１０２との間でデータメッセージを実質的にリアルタイムで交換する資産認可サーバを提供することを、すべての資産発行当局が選びはしないことが可能である。こうした資産について、プロキシ（proxy）が、プロキシ認可サーバ１４０によって取引を認可することができる。プロキシ認可サーバ１４０は、資産認可サーバ１３０及び１３２と同様であり得る。しかしながら、プロキシ認可サーバ１４０は資産発行当局により制御されないので、プロキシ認可サーバ１４０は、システム１００の元帳に記憶された資

産の各単位が資産の「現実の」単位で裏付けられることを直接確保することができない可能性がある。クライアントの信用を増大させるために、プロキシ認可サーバ１４０は、資産認可サーバ１４２にさらに接続することができ、資産認可サーバ１４２は、それぞれの資産発行当局により制御される。資産認可サーバ１４２は、分散元帳を記憶又は制御することができないと同時に、資産認可サーバ１４２は、プロキシ認可サーバ１４０により維持される組み合わせられた元帳残高がエスクローアカウント内の対応する「現実の」資金で裏付けられることを確認する（verify）ように構成されることができる。資産認可サーバ１４２は、エスクローアカウント内に保持される資金の量をリアルタイムで制御することができ、エスクローアカウント内の残高を資産の供給及び需要に基づいて連続的に更新することができる。プロキシ認可サーバ１４０は、エスクローアカウント内の資金を元帳内のアカウント残高にリアルタイムで関連付けるように構成されることができ、そのため、プロキシ認可サーバ１４０及び資産認可サーバ１４２の組み合わせられた動作が、元帳内における残高の、それぞれの資産の「現実の」単位と同様の１対１対応を提供する。

【００３３】

元帳管理サーバ１０２及び資産認可サーバ１３０は、アカウントオペレータサーバ１２０に結合することができる。アカウントオペレータサーバ１２０は、プロセッサ及び記憶回路を用いて、クライアント（例えば、クライアント１２２～１２６）のために元帳アカウント情報を顧客情報にリンクすることができる。元帳管理サーバ１０２は、ＫＹＣ認可サーバ１５０にさらに結合することができる。ＫＹＣ認可サーバ１５０は、ＫＹＣ情報を含む電子記録を作成及び記憶することができ、ＫＹＣ情報は、例えば、税識別番号、当座若しくは普通預金アカウント番号、パスポート若しくは運転者免許番号、又は任意の他の適切な形式の個人識別などである。元帳管理サーバ１０２は、データメッセージを交換することにより、ＫＹＣ認可サーバ１５０により記憶されたＫＹＣ情報にアクセスすることができる。例えば、元帳管理サーバ１０２は、取引の当事者（parties）の指標を含むメッセージを、ＫＹＣ認可サーバ１５０に対して、データメッセージの信ぴょう性を確認する情報（例えば、元帳管理サーバ１０２の電子署名）と共に送信することができる。メッセージの受信に応答して、ＫＹＣ認可サーバ１５０は、データメッセージに含まれるアカウント情報に基づいて顧客記録にアクセスすることができ、ＫＹＣステータスを取り出すことができる。ＫＹＣ認可サーバ１５０は、プロセッサを用いて、元帳管理サーバ１０２から受信した要求に応答してデータメッセージを準備することができ、それをＫＹＣ認可サーバ１５０の電子署名と共に元帳管理サーバ１０２に送信することができる。元帳管理サーバ１０２及び資産認可サーバ１３０はリアルタイムで又は各取引ごとにＫＹＣ情報にアクセスする必要はないことに留意することが重要である。例えば、元帳管理サーバ１０２は、クライアント１１２のために取得されたＫＹＣ情報を記憶し、その情報を使用してＫＹＣチェックを実行することができる。このことに応じて、ＫＹＣ認可サーバ１５０と元帳管理サーバ１０２との間で交換される前述されたデータメッセージは毎取引ごとに必要ではなく、このことは、取引を処理するのに必要とされる時間を低減するのに役立つ。

【００３４】

図２は、可視性制限を例示する分散された元帳２００の図を示す。例示のために、元帳２００は表として図示され、クライアントごとの元帳アカウント残高を含む行２１０と、異なる資産に対応する列２１２とを含む。各クライアントについて、元帳２００は、資産ごとに少なくとも１つの元帳アカウント残高を含む。例えば、クライアントＡに関連付けられたアカウント保持者は、A_{USD}米国ドル、A_{EUR}ユーロ、A_{GBP}ポンド、及びA_{JPY}日本円のアカウント残高を有する。いくつかのクライアントは、利用可能な資産のサブセットのアカウント残高のみ維持することがある。元帳２００に記憶された記録は、特定資産が使用されていないとの指標を含むことができる。例えば、クライアントＢは、米国ドルの元帳アカウント残高を有し、しかしユーロのアカウント残高を有さない。ゼロ残高を関連付けてクライアントＢがその所与の資産に関与する取引を一般に実行しないことを示すことに代わって、予約された値が元帳２００に記憶されてもよい。いくつかの態様において、別の予約された値を使用して、クライアントが（例えば、規制又はＡＭＬ

規制に起因して）ある資産の取引を実行するのを許されていないことを示してもよい。例えば、クライアントＣが、日本円に関与する元帳取引を実行することを許されないことがあり、このことは、元帳内の対応するエントリ内で「Ｘ」で表される。

【００３５】

図１に関連して論じられたように、システム１００は、規制者により認可され、しかし市場に対して不透明であり得る取引の、迅速な処理を提供する。元帳２００の編成は、システム１００により強制される可視性制限を例示する。例えば、元帳管理サーバ１０２が、元帳２００に対してその全体にアクセスを有することができると同時に、資産認可者は、該資産認可者により認可される特定資産に属する元帳アカウント残高に対しての、制限されたアクセスを有することがある。例えば、米国ドルの資産認可者（例えば、資産認可者１３０）は、元帳部分２０２に対するアクセスのみ有することができる。同様に、日本円の資産認可者（例えば、資産認可者１３２）は、元帳部分２０４に対するアクセスのみ有することができる。一方、特定アカウント保持者に対応するクライアントは、該クライアントに関連付けられたすべての元帳アカウント残高、例えば元帳部分２０６などに対するアクセスを有することができ、元帳部分２０６には、米国ドル、ポンド、及び日本円における元帳アカウント残高が含まれる。

【００３６】

いくつかの態様において、クライアントＡは、クライアントＤとの取引、例えば外国為替取引などを開始することができる。例えば、クライアントＡは、D'_{JPY}日本円と引き換えにクライアントＤからA'_{USD}を購入することができる。この取引は、２つの通貨、すなわち米国ドル及び日本円に関与する。元帳管理サーバ１０２は、クライアントＡ及びＤから、取引を要求する別個のデータメッセージを受信することができ、取引の処理を制御することができる。そのようなものとして、元帳管理サーバ１０２は、クライアントＡ及びＤの元帳アカウント残高に対する完全なアクセスを有することができる。しかしながら、資産認可サーバ１３０及び１３２は、元帳のうちの部分に対するアクセスしか有することができない。例えば、資産認可サーバ１３０は、取引のうち米国ドル部分を認可することができ、ゆえに、元帳アカウント残高A_{USD}及びD_{USD}を含む元帳部分２０２にアクセスすることができる。同様に、資産認可サーバ１３２は、取引のうち日本円部分を認可することができ、ゆえに、元帳アカウント残高A_{JPY}及びD_{JPY}を含む元帳部分２０４にアクセスすることができる。

【００３７】

図３は、元帳管理ネットワーク３００のブロック図である。元帳管理ネットワーク３００は、元帳管理サーバ３１０、資産認可サーバ３３０、アカウントオペレータサーバ３４０、及びＫＹＣ認可サーバ３６０を含む。元帳管理サーバ３１０及び資産認可サーバ３３０は、データメッセージを交換して、可視性制約にさらされる分散された元帳２００の冗長コピーを維持する。上記可視性制約は、規制者により必要とされる透過性を可能にすると同時に、元帳アカウント残高をその他の方法では一般市場に対してアクセス不可能にする。元帳管理サーバ３１０は、取引の処理を制御し、資産認可サーバ３３０との間でデータメッセージを交換して、取引の信ぴょう性及び正確さを確認する。元帳管理サーバ３１０が資産認可サーバ３３０から取引を承認するデータメッセージを受信しない限り、元帳管理サーバ３１０は取引を承認することができない。いくつかの態様において、資産認可サーバ３３０による上記認可は、資産認可サーバ３３０に関連付けられた資産の発行当局により制御される資産の単位との１対１対応を元帳アカウント残高が有することを提供する。同様に、元帳管理サーバ３１０は、ＫＹＣ認可サーバ３６０にデータメッセージを送信して、取引に関与する当事者のＫＹＣステータスの認可を要求することができる。しかしながら、元帳管理ネットワーク３００は、ＫＹＣ情報が各取引について確認されることを必要としなくてもよい。例えば、ＫＹＣ情報は、元帳管理サーバ３１０及び資産認可サーバ３３０に記憶され、所定の時間にのみ（例えば、ＫＹＣ認可サーバ３６０との間でデータを交換することにより）更新されてもよい。ＫＹＣ情報の更新は、元帳管理サーバ３１０により要求されてもよく、あるいは、ＫＹＣ認可サーバ３６０により元帳管理サーバ

３１０に対してプッシュされてもよい。
【００３８】
元帳管理サーバ３１０は、処理サーバ３２４及びネットワークインターフェース３１６を含み、これらの双方がバス３２６に接続される。ネットワークインターフェース３１６は、元帳管理サーバ３１０と資産認可サーバ３３０とアカウントオペレータサーバ３４０とＫＹＣ認可サーバ３６０とにおけるデータメッセージの交換を可能にすることができる。ネットワークインターフェース３１６は、クライアント１１２との間で直接データメッセージを交換するのにさらに使用されてもよい。処理サーバ３２４は、元帳管理サーバ１３０により実行される処理及びデータ交換を制御することができる。処理サーバ３２４は、認証及び暗号化回路をさらに含み、データメッセージに関連付けられた署名を認可し、元帳２００がさらされるアクセス制約を強制することができる。バス３２６は、資産認可者データベース３２０、ＫＹＣステータスデータベース３２２、及びアクセス制御回路３１８にさらに結合される。アクセス制御回路３１８は、ウォレットデータベース３１２及び残高データベース３１４に対するアクセスを制限する。
【００３９】
いくつかの態様において、資産認可者データベース３２０は、バス３２６に直接結合され、なぜならば、元帳管理サーバ３１０が、アクセス制限なく資産認可者データベース３２０に記憶された情報をアクセス可能にするためである。対照的に、アクセス制御回路３１８は、ウォレットデータベース３１２及び残高データベース３１４に記憶された情報に対するアクセスを制御することができる。いくつかの態様において、資産認可者データベース３２０は、資産ごとの資産認可サーバ（例えば、資産認可サーバ３３０）のポインタ、ネットワークアドレス、又は他の適切な識別のリストを記憶する。
【００４０】
取引を処理することの一部として、元帳管理サーバ３１０は、取引に関与する各資産について、少なくとも１つの認可サーバからの認可を要求する。しかしながら、複数の資産認可サーバが資産ごとに提供されてもよい。複数の資産認可サーバが利用可能であるとき、資産認可サーバ３３０は、取引の処理を複数の資産認可サーバ間で分散することができる。複数の資産認可サーバは、分散された元帳の多数の冗長コピーをさらに記憶してもよい。多数の冗長コピーは、悪意ある行為者又は詐欺の取引に対する元帳管理ネットワーク３００の回復力をさらに強化する可能性がある。
【００４１】
元帳管理サーバ３１０は、ウォレットデータベース３１２及び残高データベース３１４をさらに含み、これらは、元帳管理サーバ３１０により維持される元帳アカウント残高のコピーを記憶するように構成される。いくつかの実施形態において、ウォレットデータベース３１２は、所与のクライアントにより保持されるすべての資産を、他の識別情報、例えば従来の銀行アカウント番号及び暗号コード（例えば、クライアントの公開鍵）と一緒に記憶することができる。資産ごとにクライアントにより保持される元帳残高は、残高データベース３１４に記憶することができ、このことは図４に関連して論じられる。他の実施形態において、ウォレットデータベース３１２及び残高データベース３１４は、組み合わせられ、クライアントごとに、資産と対応するアカウント残高との双方を共通のデータ構造に記憶してもよい。元帳管理サーバ３１０は、アクセス制御回路３１８を用いることにより、ウォレットデータベース３１２及び残高データベース３１４に記憶された情報に対するアクセスを制限することができる。アクセス制御回路３１８は、特定クライアントのアクセスを、該特定クライアントに関連付けられたアカウント保持者により保持されるアカウントに限定することができる。アクセス制御回路３１８は、データベースに対するアクセスを提供する前にユーザ名及びパスワード又は２ファクタの認証を必要とすることにより、上記アクセス制限を提供することができる。元帳管理サーバ３１０もまた、ウォレットデータベース３１２及び残高データベース３１４に対するフルアクセスを有してもよい。しかしながら、アクセス制御回路３１８は、ウォレットデータベース３１２及び残高データベース３１４により記憶された元帳残高が一般市場に対してアクセス不可能であ

ることを確保することができる。

【００４２】

元帳管理サーバ３１０は、ＫＹＣステータスデータベース３２２を含む。元帳管理サーバは、処理サーバ３２４を用いて、クライアントごと又はアカウントごとにＫＹＣステータス情報（例えば、クライアントのアカウントが有効であるか、あるいは無効であるかを識別する情報）を記憶することができる。元帳管理サーバ３１０は、ＫＹＣステータスデータベース３２２を利用して、取引が処理されるたびにＫＹＣ認可サーバ３６０との間でＫＹＣデータを交換する必要を除去することができる。むしろ、元帳管理サーバ３１０は、所定の時間にＫＹＣ認可サーバ３６０との間でデータメッセージを交換することによってＫＹＣステータスデータベース３２２を更新し、しかしそうでない場合は、取引を処理することの一部として実質的にリアルタイムでＫＹＣステータスデータベース３２２からＫＹＣステータス情報を取り出すことができる。いくつかの実施形態において、資産認可サーバ３３０は、元帳管理サーバ３１０と同様の方法でＫＹＣステータス情報を記憶することができる。例えば、資産認可サーバ３３０は、処理サーバ３３４を用いて、クライアントごと又はアカウントごとにＫＹＣステータス情報を記憶することができ、元帳管理サーバ３３０から受信した取引を承認する前にＫＹＣステータス確認を実行することができる。元帳管理サーバ３１０と同様に、資産認可サーバ３３０は、（各取引についてＫＹＣ認可サーバ３６０との間でデータメッセージを交換するよりも）記憶されたステータス情報を用いて、取引を処理するのにかかる時間を低減することができる。

【００４３】

元帳管理サーバ３１０と同様に、資産認可サーバ３３０は、ネットワークインターフェース３３２及び処理サーバ３３４を含み、これらの双方がバス３３９に接続される。バス３３９は、資産残高データベース３３６、保留残高（pending balance）データベース３３７、及び予約残高（reserved balance）データベース３３８にさらに結合される。元帳管理サーバ３１０と同様に、ネットワークインターフェース３３２を使用して、元帳管理サーバ３１０及びアカウントオペレータサーバ３４０との間でデータメッセージを交換することができる。いくつかの態様において、ネットワークインターフェース３３２は、さらなる資産認可サーバに結合されてもよい。元帳管理サーバ３１０又は資産認可サーバ３３０は、さらなる資産認可サーバを制御し、取引に関連付けられた負荷をさらなる資産認可サーバ間で分散することができる。さらなる資産認可サーバは、許可されていない取引からのさらなる保護をさらに提供することができ、なぜならば、さらなる資産認可サーバの各々は、分散された元帳の冗長コピーを記憶することができるからである。処理サーバ３３４は、元帳管理ネットワーク３００内の他のサーバから受信したデータメッセージを認証するのに用いられてもよい。

【００４４】

資産残高データベース３３６、保留残高データベース３３７、及び予約残高データベース３３８は、元帳２００の部分的コピーを記憶することができ、上記部分的コピーには、資産認可サーバ３３０により認可される資産の元帳アカウント残高が含まれる。例えば、資産認可サーバ３３０が米国ドルにおけるすべての取引を認可する場合、資産残高データベース３３６、保留残高データベース３３７、及び予約残高データベース３３８は、米国ドルにおけるすべての元帳アカウント残高を記憶することになる。しかしながら、上記の場合、資産認可サーバ３３０は、ユーロ又は日本円などの他の資産における元帳アカウント残高に対するアクセスを有さないことになる。いくつかの態様において、資産残高データベース３３６は、資産認可サーバ３３０により事前に承認されており、かつ取引の完了が元帳更新の一部として元帳管理サーバ３１０により報告された取引について、元帳アカウント残高のコピーを記憶することができる。さらに、予約残高データベース３３８は、資産認可サーバ３３０により承認されており、しかし元帳管理サーバ３１０により完了としてまだ報告されていない支払い残高を、記憶することができる。各アカウント残高について、入ってくる支払いでなく出ていく支払いのみが記録されてもよく、ゆえに、保留残高データベース３３８内の残高は非負でありうる。同様に、保留残高データベース３３７

は、資産認可サーバ３３０により認可され、かつ元帳管理サーバ３１０により署名されており、しかし更新された資産残高データベースにまだ含まれていない支払いについて、残高を記憶することができる。

【００４５】

保留残高データベース３３７及び予約残高データベース３３８は一緒に、「二重支出」又は「リプレイ」を防止するのに役立つ。保留残高データベース３３７及び予約残高データベース３３８に記憶された情報を用いて、資産認可サーバ３３０は、資産残高データベース３３６内に維持される公開された元帳残高を、保留残高データベース３３７に記憶された金額（例えば、保留中の支払いの合計和）により、及び予約残高データベース３３８に記憶された金額（例えば、予約された支払いの合計和）により低減することができる。結果として生じる残高は「シャドウ残高（shadow　balance）」として知られ、この残高は、資産認可サーバ３３０により処理されており、しかし更新された元帳コピー内で元帳管理サーバ３１０により「完了」としてまだ報告されていない取引について説明する。結果として、（例えば、立て続けに複数の取引を提出することによる）「二重支出する」試みは防止され、なぜならば、資産認可サーバ３３０が、各取引を認可することに応答して「シャドウ残高」を更新するからである。

【００４６】

元帳管理サーバ３１０と同様に、ＫＹＣ認可サーバ３６０は、ネットワークインターフェース３６２及び処理サーバ３６４を含み、これらの双方がバス３６９に接続される。ＫＹＣ認可サーバ３６０は、ネットワークインターフェース３６２を使用して、元帳管理サーバ３１０及び資産認可サーバ３３０との間でデータメッセージを交換することができる。処理サーバ３６４が、元帳管理ネットワーク３００内の他のサーバから受信した又は送信されたデータメッセージを認証することができる。ＫＹＣ認可サーバ３６０はＫＹＣデータベース３６６をさらに含み、ＫＹＣデータベース３６６は顧客識別を記憶することができる。ＫＹＣデータベース３６６に記憶された情報は、ＫＹＣ要件の準拠を確保するのに使用されてもよい。例えば、所定の時間に、元帳管理サーバ３１０はデータメッセージをＫＹＣ認可サーバ３６０に送信して、当事者のＫＹＣステータスを確認することができる。ＫＹＣ認可サーバ３６０は、関連するＫＹＣステータスをＫＹＣデータベース３６６に記憶することができる。元帳管理サーバ３１０からの要求に応答して、ＫＹＣ認可サーバ３６０は、クライアント識別子（例えば、クライアントの公開鍵）に基づいてＫＹＣデータベース３６６を検索し、クライアントの現在のＫＹＣステータスを取り出すことができる。ＫＹＣ認可サーバ３６０は、それから、データメッセージを元帳管理サーバ３１０に伝達して返すことができる。ＫＹＣステータスは、毎取引についてリアルタイムにチェックされる必要はないことが留意されるべきである。むしろ、元帳管理サーバ３１０及び資産認可サーバ３３０は、所定の時間にＫＹＣ情報にアクセスし、ローカルに記憶されたステータスを取引の処理に使用することができる。

【００４７】

元帳管理サーバ３１０と同様に、アカウントオペレータサーバ３４０は、ネットワークインターフェース３４２及び処理サーバ３４４を含むことができ、これらの双方がバス３４９に接続される。アカウントオペレータサーバ３４０は、元帳アカウント残高に関する情報が当事者の関連付けられたクライアント（例えば、クライアント１１２）上よりむしろアカウントオペレータサーバ３４０上に維持されることを好む当事者について、アカウントプロセッサの役割を果たすことができる。上記シナリオにおいて、アカウントオペレータサーバ３４０は、本質的に、前述された処理をクライアントの代わりに供給する。アカウントオペレータサーバ３４０は、元帳アカウント残高に関する情報をアカウントデータベース３４６に記憶することができる。いくつかの実施形態において、アカウントオペレータサーバ３４０及びＫＹＣ認可サーバ３６０は、組み合わせられ、単一のサーバアーキテクチャ内に実装されてもよい。

【００４８】

いくつかの実施形態において、元帳管理サーバ３１０及び資産認可サーバ３３０により

記憶される分散元帳の冗長コピーは、暗号化された形式で記憶することができる。元帳管理サーバ３１０は、分散された暗号化された元帳への可視性を、元帳のうちの部分を別様にエンコードする暗号化処理を採用することによって制御することができ、そのため、元帳の第１の部分に対するアクセスを可能にする復号処理は、元帳の第２の部分にアクセスするのに使用することはできない。例えば、元帳管理サーバ３１０は、第１の資産（例えば、米国ドル）に対応する残高を、第１の資産認可サーバ（例えば、連邦準備銀行（Federal Reserve）のサーバ）により使用される復号処理のみが上記残高を復号することができるように、暗号化することができる。同時に、元帳管理サーバ３１０は、第２の資産（例えば、ユーロ）に対応する残高を、第１の資産認可サーバ（例えば、連邦準備銀行のサーバ）により使用される復号処理が第２の資産の上記残高を復号することができず、しかし第１の資産に対応する残高のみ復号することができるように、暗号化することができる。いくつかの態様において、元帳管理サーバ３１０及び資産認可サーバ３３０は、分散された暗号化された元帳のコピーを交換して、元帳が元帳管理ネットワーク３００内のサーバにわたり一貫性のあることを確保することができる。資産認可サーバは、分散された暗号化された元帳のうちの部分にのみアクセスすることができ得るが、例えば、元帳管理サーバ３１０の故障に対する記録保持又は向上したロバスト性のために、元帳のコピーをその全体で交換することが望ましい可能性がある。

【００４９】

図４は、分散された元帳に元帳残高及びアカウント情報を記憶する一例示的なデータ構造４００を表す。データ構造４００は、ウォレットテーブル４１０、ＫＹＣ認可者テーブル４４０、及び資産テーブル４５０を含む。ウォレットテーブル４１０はデータブロックのリストを含み、上記データブロックの各々が、特定のクライアント、例えばクライアント４１０ａ～４１０ｃなどに関連付けられた元帳残高を記憶する。ウォレットテーブル４１０内にエントリを有する各クライアントについて、ウォレットテーブル４１０のデータブロック（例えば、クライアント４１０ｃのデータブロック）が、公開鍵４１２、資産４１４、アカウント情報４１６、アカウントごと（per-account）残高４１８、ＫＹＣ承認ステータス４２０、及び暗号署名されたＫＹＣ承認メッセージのコピー、並びに、アカウント４１６に関する取引を処理するのに必要とされ得る任意のさらなる署名のリストのための付加的（extra）署名フィールド４２２を含むことができる。公開鍵４１２は、元帳管理ネットワーク３００にわたりサーバが使用して、クライアント又はサーバから受信するメッセージの信ぴょう性を確認することができる。資産４１４は、クライアントが元帳残高を維持する１つ以上の通貨又は他の資産を示すことができる。アカウント情報４１６は、従来的な銀行アカウント情報（例えば、当座預金若しくは普通預金口座、又は証券（securities）の保管口座に対応する）を含むことができ、資産ごとにいくつかのアカウントが可能であり得る。通貨には、米国ドル又はユーロなどの不換通貨、さらに暗号通貨（例えば、ビットコイン又はリップル）などの他タイプの通貨、又は任意の他の適切な形式の通貨又は資産を含むことができる。データブロック４１０ｃは、各アカウント４１６に関連付けられた元帳残高４１８を記憶することができる。いくつかの態様において、別個の残高テーブルが元帳内に維持されてもよく、データブロック４１０ｃに組み込まれなくてもよい。いくつかの実施形態において、データブロック４１０ｃとは別個に残高テーブルを維持することは有益であり得、なぜならば、このことは、データブロック４１０ｃと比較して残高テーブルに、より粒度の細かいアクセス制限、例えばより高いレベルのプライバシーなどを提供するからである。データブロック４１０ｃは、アカウントごとＫＹＣステータス４２０をさらに含むことができ、アカウントごとＫＹＣステータス４２０は、リストにされた承認されたＫＹＣ認可者４４４のうちの１つによりアカウント４１６がＫＹＣ準拠として確認されたかどうかの指標と、さらに、参照ＫＹＣ認可者テーブル４４０の認可者のＩＤとを含む。例えば、データブロック４１０ｃに関連付けられた特定のクライアントについて、「シティバンク」が米国ドルにおけるアカウントのうち１つのＫＹＣ認可者であり得、「ドイツ銀行」がユーロにおけるアカウントのうち１つのＫＹＣ認可者であり得るなどである。さらに、データブロック４１０ｃは、Ｃ．Ｃ．取引リスト４２４

、取引に関して知らされる（例えば、カーボンコピーされる）必要がある付加的な当事者のアイデンティティを記憶するフィールドを含むことができる。Ｃ．Ｃ．取引リスト４２４は、図４に示されるように、クライアントごとに記憶することができる。その場合、ある取引について通知される当事者は、クライアントのアカウントのうちいずれが取引に関与するかに依存しない。Ｃ．Ｃ．取引リスト４２４は、さらに、アカウントごとに（例えば、アカウント情報４１６の一部として）記憶されてもよい。その場合、クライアントのアカウントのうちいずれが取引に関与するかに依存して、異なる当事者が取引について通知されることができる。Ｃ．Ｃ．取引リスト４２４内のエントリは、通知をされるべき当事者を具体的に識別することができ、取引に関連付けられたさらなる識別子を含むことができる。

【００５０】

アカウントごとＫＹＣステータス４２０は、ＫＹＣ認可者テーブル４４０内に列挙されたＫＹＣ認可者４４４により確立されることができる。さらに、ＫＹＣ認可者テーブル４４０はポインタ４４２を含むことができ、ポインタ４４２は、ＫＹＣ認可者リスト４４４内に列挙された各ＫＹＣ認可者を識別することができる。各ＫＹＣ認可者４４４は、対応する資産４５２のための資産テーブル４５０内の資産認可者４５４（例えば、中央銀行）により承認されることができる。資産テーブル４５０は、各資産認可者４５４について、公開鍵４５５を記憶することができ、公開鍵４５５を他の当事者が用いて、資産認可者４５４から受信したデータメッセージの信ぴょう性を確認することができる。さらに、資産テーブル４５０は、ポインタ４４２にリンクされたポインタのリスト４５６を含み、そのため、あらゆる認可者４５４が、資産４５２のための、ＫＹＣ認可者４４４内の承認されたＫＹＣ認可者のグループにリンクされることができる。例えば、米国ドルについて、連邦準備銀行が、資産認可者としての役割を果たすことができ、バンクオブアメリカ及びシティバンクが、承認されたＫＹＣエージェントの中にあり得る。いくつかの態様において、資産テーブル４５０は、特定のクライアント又はデータブロック４１０ｃにリンクされないグローバルなデータ構造であり得る。ＫＹＣ認可者テーブル４４０は、各ＫＹＣ認可者４４４について、公開鍵４４５を記憶することができ、公開鍵４４５を他の当事者が用いて、ＫＹＣ認可者４４４から受信したデータメッセージの信ぴょう性を確認することができる。

【００５１】

図５は、分散された元帳の部分的な、冗長なコピーを各々記憶する認可サーバから受信したデータメッセージに基づいて、上記元帳を更新する処理５００のフローチャートを示す。処理５００は、ステップ５０２において、取引に関与する当事者（例えば、クライアント１１２又は１２２）から入力を受信することができ、処理５００の残りのステップは、元帳管理ネットワーク３００が実行することができる。図３に関連して論じられたように、取引の成功した処理は、資産認可サーバ（例えば、資産認可サーバ３３０）からの認可と（例えば、ＫＹＣ認可サーバ３６０からの）ＫＹＣ確認とを元帳管理サーバ１０２に受信させることができる。

【００５２】

処理５００は、ステップ５０２において、取引における当事者であるクライアントから認証要求を受信することによって開始することができる。元帳管理ネットワーク３００に対するクライアントのアクセスは、２ファクタ認証メカニズムにより、あるいはユーザ名及びパスワードを提供することにより保護することができる。いくつかの態様において、ユーザ名は、クライアント（例えば、クライアント１１２）を具体的に識別することができ、分散元帳内のクライアントのアカウントにリンクされることができる。クライアントがその取引要求を備えたデータメッセージを提出するのに使用する認証手順及びインターフェースは、特別に設計されたアプリケーションプログラムインターフェース（ＡＰＩ）の一部であり得る。クライアントが元帳管理ネットワーク３００に対するアクセスを獲得すると、元帳管理ネットワーク３００にアクセスするためにクライアントにより使用されるＡＰＩは、要求された取引に関する情報、例えば取引に関与する資産、移転又は交換さ

れるべき元帳残高などと、取引を処理するのに必要とされる任意の他の関連情報とを、クライアントから収集することができ、記憶することができる。いくつかの態様において、例えば、取引が複数のクライアントに関与する外国為替取引などにおいて、クライアントは、他の手段により（例えば、音声で、電子メールで、あるいは従来の外国為替取引又は処理プラットフォームをとおして）取引の一部であることを事前に同意されている他の当事者に関する情報（例えば、そのそれぞれの公開鍵又はアカウント情報）をさらに入力することができる。取引に関与するクライアントの各々は、そのそれぞれの署名をデータメッセージに個々にアペンドする（append）ことができる。署名は、取引要求に関連付けられた当事者と取引詳細とを識別する。クライアントは、そのそれぞれの署名を、前述のクライアントにより要求された取引の詳細に対応するデータをハッシュすることにより、それから、結果として生じるハッシュをクライアントの秘密鍵を用いて暗号化して暗号化された署名を取得することにより、生成することができる。このことは、図６に関連してより詳細に説明される。

【００５３】

ステップ５０４において、処理５００は、元帳管理サーバ３１０により認証されているクライアントによる複数の取引要求を受信することができる。元帳管理サーバ３１０と、ＡＰＩをとおして元帳管理サーバ３１０にアクセスするクライアント装置との間の接続は、従来的な認証プロトコル（例えば、「Ｏａｕｔｈ」プロトコル）を用いて認証することができる。処理５００は、ステップ５０６において、取引要求に関連付けられた各当事者の署名を認可することができる。処理５００は、各クライアントの署名の有効性を、署名を復号してハッシュを取得することにより決定することができる。ハッシュは、それから、データメッセージとは独立して取得される別のハッシュと比較することができる。このことは、図６に関連して説明される。

【００５４】

処理５００が、署名が有効であると決定する場合、処理５００は、ステップ５０８において、取引の処理が任意のさらなる署名を必要とし得るかを決定することができる。例えば、図４に関連して説明されたようにデータブロック４１０ｃの付加的署名フィールド４２２内に付加的な署名を追加することにより、特定の個々により要求された取引を他の当事者が確かめることを、所与のクライアントのＫＹＣポリシーが必要としてもよい。さらなる署名が必要とされる場合、元帳管理サーバ３１０は、処理５００を継続する前に、ステップ５１０においてさらなる署名を収集し、認可することができる。元帳管理サーバ３１０は、取引の当事者のうちいずれかがその署名をまだ提供していないかをさらにチェックすることができる。例えば、取引は複数のクライアントに関与することがあり、ステップ５０４において、署名されたデータメッセージを上記クライアントのすべてが提供しなくてもよい。したがって、元帳管理サーバ３１０は、要求された取引のタイプを識別し、任意の不足している署名のための要求を送信することができる。例えば、取引が複数のクライアントに関与する外国為替取引において、ＡＰＩを用いてクライアントにより送信される取引情報は、取引に加わることができる他の当事者に関する情報をさらに含む。いくつかの実施形態において、これら当事者は、他の手段により（例えば、音声で、電子メールで、あるいは従来の外国為替取引又は処理プラットフォームをとおして）取引の一部であることを事前に同意されており、取引における他の参加者に知られている。ステップ５１０において、元帳管理サーバ３１０は、Ｃ．Ｃ．取引リスト４２４内に参加者のアイデンティティを、及び付加的署名４２２内にその署名を追加することができる。これらデータテーブルは、複数当事者取引を要求する最初のクライアントからのデータがステップ５０４において元帳管理サーバ３１０により受信され、認証されるとき、埋められることが始まってもよい。それから、付加的署名テーブル４２２は未完了としてマーク付けされ、Ｃ．Ｃ．取引リスト４２４内に列挙された当事者のアイデンティティは、上記当事者がシステムにログインし、同じ取引のための要求を提出するとき、付加的署名テーブル４２２に対して１つずつチェックされ、マッチされる。すべての当事者が取引に同意したとき、付加的署名テーブル４２２は完了としてマーク付けされ、処理５００は、次のステップに

継続する。元帳管理サーバ３１０は、取引におけるすべての当事者が該取引の一部であることに同意する、ステップ５１０のための時間のウィンドウを設定するハードウェア又はソフトウェア制御を用いて、タイムアウトメカニズムを実装してもよい。こうして、処理５００は、取引に関与する当事者のすべてが該取引の一部であることの許可を与え、同じ取引に加わる他の当事者を相互に認めていることを確認することができる。

【００５５】

取引に対するすべての必要な署名を要求した後、処理５００は、ステップ５１１において、当事者間の取引をマッチさせることができる。例えば、元帳管理サーバ３１０は、外国為替取引を、第２の資産と交換に第１の資産を売る取引を提出した当事者を識別することによって処理することができる。元帳管理サーバ３１０は、上記当事者の取引を処理し、該取引を、第１の資産と交換に第２の資産を売ろうとする別の当事者により受信された別の取引とマッチさせることができる。いくつかの場合、当事者間で取引をマッチさせることは必要でない場合があり、例えば、支払い取引について、又は、２以上の当事者が取引を実行することにあらかじめ同意している取引について、などである。

【００５６】

処理５００は、ステップ５１２において、各クライアントのＫＹＣステータスをチェックすることができる。いくつかの態様において、上記ＫＹＣチェックは、法律により義務付けられてもよく、元帳管理サーバ３１０は、分散元帳に対するいかなる修正も承認する前に上記ＫＹＣチェックを実行するように構成されることができる。ＫＹＣチェックを完了するために、元帳管理サーバ３１０は、元帳内の各クライアントアカウントにリンクされた銀行アカウント詳細がＫＹＣ認可者により確認され、署名されていることをチェックすることができる。承認されたＫＹＣ認可者のリストは、（元帳管理サーバ３１０により維持される）ＫＹＣステータスデータベース３２２に記憶することができる。図４に関連して論じられた、資産テーブル４５０及びＫＹＣ認可者テーブル４４０と同様のデータ構造が使用されてもよい。

【００５７】

処理５００は、ステップ５１４において、すべての当事者のＫＹＣステータスが有効であるかどうかを決定することができる。当事者のいずれかが無効なＫＹＣステータスに関連付けられている場合、処理５００は、取引を全体として拒否することができ、当事者の元帳アカウント残高のいずれも更新されるのを防止することができる。そうでない場合、処理５００は、ステップ５１７において、元帳管理サーバ３１０に記憶された元帳残高が取引の支払い額より大きいか又は等しいかどうかを決定することができる。元帳管理サーバ３１０が、元帳残高が十分であると決定する場合、処理５００は、ステップ５１８において取引に署名することと、取引詳細を有するデータメッセージを資産認可者（例えば、資産認可サーバ３３０）に転送することとを、元帳管理サーバ３１０にさせる。逆に、元帳管理サーバ３１０が、元帳残高が支払い額より小さいと決定する場合、取引は拒否され得る。いくつかの態様において、元帳管理サーバ３１０は、いずれの資産認可サーバに取引が転送される必要があるかを決定することができる。例えば、元帳管理サーバ３１０は、資産認可者のリスト（例えば、資産認可者テーブル４５０）を記憶するデータベースを含むことができる。元帳管理サーバ３１０は、取引に関与する資産を決定し、取引詳細を有するデータメッセージを、資産テーブル４５０から取得される資産認可者に転送することができる。

【００５８】

ステップ５２０において、処理５００は、取引に関連付けられた資産認可者から承認又は拒否のいずれかを受信することができる。資産認可者による取引の承認メカニズムは、取引に関与する双方のクライアントの署名の認可と、元帳管理サーバ３１０に関連付けられた署名の認可とを含むことができる。上記署名が認可された後、資産認可サーバは、各クライアントの現在利用可能な残高又は「シャドウ残高」に対して、提案された取引額を比較することができる。所与の資産についてのクライアントのシャドウ残高は、該クライアントの最後に公開された資産元帳残高から、「保留している」又は「予約されている」

としてマーク付けされたすべての支払いの累積残高を引いた額に対応することができる。保留支払いは、元帳管理サーバ３１０から受信された最新の元帳残高更新に含まれていない、完全に署名され、承認された出ていく支払いに対応することができる。予約支払いは、部分的に署名され、まだ元帳管理サーバ３１０により承認されていない、出ていく支払いに対応することができる。シャドウ残高が、要求された取引をカバーするのに十分である場合、上記取引に必要とされる額が「予約された」額に追加され、二重支出又は「リプレイ」が防止される。資産認可サーバは、規制又は法律により必要に応じて任意のさらなる非公開チェックをさらに実行することができる。さらに、資産認可サーバは、さらなるレイヤのＫＹＣ認可を実行してもよい。このポイントで、すべてのチェックが通過する場合、資産認可サーバは取引に署名し、それを元帳管理サーバに転送する。

【００５９】

ステップ５２２において、処理５００は、資産認可サーバのうちいずれかが取引を拒否したかどうか、又はＫＹＣチェックのうちいずれかかが失敗したかを決定することができる。そうである場合には、処理５００は、ステップ５２４において、取引が拒否されるべきであると決定することができる。逆には、処理５００は、取引が承認に対して適格であると決定することができる。処理５００は、それから、ステップ５２６において、取引が承認され、かつ元帳内における公開のためにマーク付けされるべきであるかどうかを決定することができる。

【００６０】

元帳管理サーバ３１０は、資産認可サーバから受信された完全に承認されたメッセージを処理してこれらを新しいバージョンの元帳に含める合意処理を採用することができる。元帳管理サーバ３１０は、合意処理を周期的に実行することができる。１つの例において、元帳管理サーバ３１０により実行される合意処理は、資産認可サーバから受信されたメッセージのすべてが上記取引を含めることを承認する場合、上記取引を含めるように決定することができる。そうでない場合、合意処理が、メッセージのうち少なくとも１つが上記取引を拒否することを決定する場合、提案された新しい元帳はその全体で拒否され、処理は、更新された取引セットで繰り返されることができる。別の例において、元帳管理サーバ３１０により実行される合意処理は、資産認可サーバから受信されるデータメッセージのうち少なくともある割合が新しい元帳を承認することのみ必要としてもよい。例えば、合意処理は、各資産の資産認可サーバから受信されるメッセージのうち８０％より多くが取引を承認する場合、その資産の新しい元帳が承認されるべきであると決定することができる。新しい元帳内に含まれるべき取引の候補リストにおいて、あらゆる取引が、関連付けられた「取引ＩＤ」を有することができ、署名された取引メッセージのハッシュと一緒に列挙されることができる。このハッシュを資産認可サーバが使用して、該資産認可サーバが承認している取引と迅速に比較し、取引におけるすべての参加者（例えば、クライアント及び認可者）と取引の額及び資産とを識別することができる。１つの例において、新しい元帳に同意する処理を、資産認可者の各々における分散元帳に対する更新を統合するのに使用して、例えば、完了した取引について「保留」又は「予約」ステータスを除去し、資産残高データベース３３６を更新することができる。

【００６１】

ステップ５１８と５２０との間に、処理５００は、反マネーロンダリング（ＡＭＬ）チェックをさらに実行してもよい。例えば、資産認可サーバ（例えば、資産認可サーバ３３０）は、処理サーバ３３４を用いて、取引ヒストリを収集し、アカウント活動に関する統計データを生成することができる。資産認可サーバ３３０は、検出処理をさらに使用して、収集されたデータを解析し、疑わしいパターン又は他タイプの不規則なアカウント活動にマッチする活動にフラグを立てることができる。疑わしいとして活動にフラグを立てることに応答して、資産認可サーバ３３０は警告メッセージを生成することができる。警告メッセージは、影響されるアカウントのＫＹＣステータスを「承認されていない」に変更させ、ゆえに、このアカウントに関連する取引が承認されることをブロックすることができる。

【００６２】
処理５００は、知る必要に応じて（on a need-to-know basis）元帳を公開することができる。本開示の重要な一態様は、取引を認可するのに必要な透過性を規制者に提供すると同時に、センシティブな情報を一般市場に明らかにすることなく分散された元帳を維持する元帳管理ネットワーク３００の能力である。いくつかの態様において、完全な元帳は元帳管理サーバ３１０により記憶され、冗長な部分的コピーが資産及びＫＹＣ認可者により保持される。元帳管理サーバ３１０において及び資産認可サーバにおいて記憶される分散元帳の冗長コピーに含まれるデータは、同期されて保たれる。資産認可サーバと元帳管理サーバとの間の通信に必要とされる回路は、元帳における取引公開と、認可者により保たれる部分的フラグメントを用いた完全な元帳の横断的認可の処理との間の、レイテンシを回避するように設計されることができる。いくつかの実施形態において、元帳の完全冗長コピーさえも資産認可サーバ及び元帳管理サーバにより記憶され、ゆえに、外部干渉又はシステム全体の機能不全のリスクを低減することができる。認証手法は、資産認可サーバが分散元帳のうちそのそれぞれの部分にのみアクセスすることができると同時に、元帳残高に対するフルアクセスが元帳管理サーバでのみ利用可能であることを提供することができる。

【００６３】
図６は、２つの相互関連した高レベルブロック図６００及び６５０を示し、これらは連帯で、取引を認証する処理を説明する。図６００は、第２の認証する当事者からの認証を求める当事者により署名されたデータを生成するのに使用される手順を詳述する。図６００は、認証されるべき元データ６０２と、元データを処理してハッシュ６０６を作り出すハッシュ関数６０４と、秘密暗号化鍵６０８で生成された暗号化された署名６１０と、暗号化された署名６１０を元データ６０２にアペンドした結果生じる新しいデータ構造６１２とを含む。

【００６４】
図６００に説明される、署名されたデータの生成は、元データ６０２をハッシュすることで開始することができる。ハッシュすることは、ハッシュ関数６０４に基づいて実行され、ハッシュ関数６０４は、取引詳細を入力データとしてとり、一意文字列のデータ（ハッシュ）６０６を出力する。ハッシュは、それから、取引を認証する当事者にのみ知られている秘密鍵６０８を用いて、従来的な暗号化方法により（例えば、ＲＳＡ暗号化を用いて）暗号化される。秘密鍵６０８を用いて、暗号化された署名６１０に対応するデータの文字列が生成される。署名６１０は、それから、元データ６０２の末尾にアペンドされてもよく、あるいはヘッダとして含まれてもよい。結果として生じる署名されたデータ６１２は、データ６１２の起点を認証しようとする当事者に送信される。

【００６５】
図６５０は、図６００において説明された処理により生成される署名されたデータ６１２を認証する当事者が従う認証手順を説明する。図６５０は、取引の元データ６５４を含む受信された署名されたデータ６５２と、図６００に従って生成された暗号化された署名６５６とを含む。図６５０は、署名６５６の復号に使用される公開鍵６６０と、ハッシュ関数６５８と、下記で説明される２つの別のメカニズムにより生成される２つのハッシュ６５８及び６６４とをさらに含む。

【００６６】
認証当事者により受信される署名されたデータ６５２は、２つのフラグメントに分けられる。第１のデータフラグメント６５４は、認証を求める上記当事者により請求された取引を説明する元データに対応する。第２のフラグメントは、暗号化された署名６５６である。いったん分離されると、取引データ６５４はハッシュ関数６５８によりハッシュされ、ハッシュ関数６５８は、暗号化された署名６１０を生成するのに図６００で使用されたハッシュ関数６０４と同一である。このことは、ハッシュ６６２を作り出す。暗号化された署名６５６は、認証当事者に所有されている公開鍵６６０を用いて復号され、従来の暗号化手法に従う公開鍵６６０は、秘密鍵６０８にリンクされる。公開鍵を用いた署名の復

号は第２のハッシュ６６４を作り出し、第２のハッシュ６６４はハッシュ６６２と比較される。６６２と６６４とが同一である場合、認証は成功である。このことが当てはまらない場合、認証処理は無効としてマーク付けされ、要求された取引は拒否される。

【００６７】

図７は、元帳管理サーバ７０２と２つの資産認可サーバの資産認可サーバ７０４及び７０６とにより取引を処理するフローチャート７００である。これら認可サーバは、２つの異なる資産について取引を認可することができる。例えば、資産認可サーバ７０４は、米国ドルにおける取引を認可することができ、資産認可サーバ７０６は、ユーロにおける取引を認可することができる。資産認可サーバ７０４及び７０６は、取引が正しく認証されていることを確認することにより、及び、取引額が保留の又は予約された支払いだけ低減されたアカウント内の利用可能残高を下回ることを決定することにより、取引を認可することができる。フローチャート７００は、外国為替トレードの、例えば米国ドル及びユーロの処理を例示する。図７において、時間が垂直軸に沿って（矢印により表されて）組み込まれ、元帳管理ネットワーク内のサーバ間におけるデータ交換のタイミングを示している。フローチャート７００に表されるステップは、図５のステップ５０８及び５１０に関連して論じられたように取引に関与する当事者の署名を認可することに応答して実行される。

【００６８】

フローチャート７００において、元帳管理ネットワークのサーバは、元帳管理サーバ７０２、資産認可サーバ７０４、及び資産認可サーバ７０６により表され、これらの各々が、入力を認可して取引の処理及び承認を決定することを提供することができる。処理７００の異なるサーバ間におけるメッセージの交換は、図３に例示されたネットワークアーキテクチャに基づいて実装することができる。具体的に、元帳管理サーバ７０２と資産認可サーバ７０４及び７０６との間のメッセージの交換のために、ネットワークインターフェース３１６、３３２、及び３４２の回路が２段階認証処理６００との組み合わせで使用されてもよい。ネットワークインターフェースの回路は、マシンツーマシン認証プロトコル、例えば「Ｏａｕｔｈ」などと関連して動作して、サーバ間の通信への外部干渉を防止することができる。このことは、元帳管理サーバ７０２と資産管理サーバ７０４と資産管理サーバ７０６とのあり得る大きい地理的広がりを仮定すると重要であり得る。

【００６９】

処理５００のステップ５０８及び５１０が実行された後、元帳管理サーバ７０２は、ステップ７０８において、取引に関連付けられた資産を決定する。上記資産のリストが識別されると、リストは資産テーブル４５０と比較されて、取引において交換されるべき各資産の資産認可サーバのアイデンティティを決定することができる。図５に関連して論じられたステップ５１７と同様に、元帳管理サーバ７０２は、元帳管理サーバ７０２に記憶された元帳残高が取引に必要とされる支払額より大きいか又は等しいかどうかをさらに決定することができる。元帳管理サーバ７０２が、残高が十分でないと決定する場合、元帳管理サーバ７０２は、取引を拒否することができる。そうでない場合、元帳管理サーバ７０２は、ステップ７１０において取引に署名し、それを「認可を保留している」としてマーク付けすることができる。図６において説明された署名処理６００は、元帳管理サーバ７０２により実行されてもよい。上記の場合におけるデータブロック６０２は、署名されたデータブロック６５２をヘッダとして含むことができ、このデータブロックは、クライアントが取引を要求するのに使用した装置内で実行されるＡＰＩにより送信されることができる。上記データブロックは、図６の処理６００により説明されたように元帳管理サーバ７０２によりステップ７１０において署名されることができ、取引は「認可を保留している」としてマーク付けされることができる。

【００７０】

元帳管理サーバ７０２は、通貨テーブル４５０に指定されたマッピングに従い、及び図３に説明されるネットワークアーキテクチャを用いて、ステップ７０８において元帳管理サーバ７０２により内部的に決定され得る資産認可者に取引情報を送信することができる

。情報がステップ７１２において資産認可サーバ７０４（例えば、米国ドル取引を認可するサーバ）により受信されると、クライアントの署名と元帳管理サーバ７０２の署名とが復号され、確認される。署名の復号及び認可と、取引を説明するデータの完全性の確認とは、図６に説明される処理６５０に従うことができる。

【００７１】

それから、資産認可サーバ７０４は、ステップ７１６において、クライアントの所与の資産のシャドウ残高を算出する。クライアントごと資産ごとのシャドウ残高は、「最新の公開された元帳残高」として表される、所与のクライアントの元帳内の最後に公開された資産残高のうち、承認され、認可され、完全に署名されており、しかし最後に公開された分散された元帳に含まれていない支払いである「保留している取引」の額を引き、完了したとしてマーク付けされておらず、しかし部分的に署名されている取引である「予約された」取引の額を引いた、残高である。保留の及び予約された取引は、最後の取引のＩＤを含む更新された元帳が元帳管理サーバ７０２により公開されると、ローカル元帳残高に移動することができる。

【００７２】

ステップ７１８において、資産認可サーバ７０４は、ステップ７１６において算出されたシャドウ残高が要求された取引の額より大きいかを決定する。その場合、資産認可サーバ７０４は、取引が継続することを可能にする。

【００７３】

ステップ７２０において、シャドウ残高が現在の取引の額より大きいか又は等しい場合、資産認可サーバ７０４はローカル資産元帳を更新して、取引額を予約し、シャドウ残高を更新する。シャドウ残高の迅速な又は即時の更新は、「二重支出」又は「リプレイ」試行に対する重要な予防手段であり得る。

【００７４】

ステップ７２２において、資産認可サーバ７０７（上記例においてＵＳＤである）のローカル元帳を更新した後、資産認可サーバ７０４は、認可承認メッセージに署名し、元帳管理サーバ７０２に送信する。承認メッセージは、資産認可処理を成功としてマーク付けする認容（acknowledgment）フラグを含むことができる。

【００７５】

７１０において、第２のメッセージが元帳管理サーバ７０２により資産認可サーバ７０６に送信される。上記例において、資産認可サーバ７０６は、取引のうちユーロ部分を認可するサーバであり得る。資産認可サーバ７０６により実行されるステップ７２４～７３０は、資産認可サーバ７０４により実行されるステップ７１２～７１８と同様であり得る。上記例において、資産認可サーバ７０６により実行されるステップ７３０は、ユーロにおけるクライアントのシャドウ残高が要求された取引の額より小さいことを決定することができる。この決定に応答して、資産認可サーバ７０６は、拒否メッセージに署名し、元帳管理サーバ７０２に送信することができる。

【００７６】

資産認可サーバ７０４からの承認メッセージ及び資産認可サーバ７０６からの拒否メッセージを受信した後、元帳管理サーバ７０２は、合意が達せられなかったと決定し、取引を拒否する。すべての資産認可サーバが取引を認可した別のシナリオにおいて、取引は、図５の議論と関連してステップ５２６で説明されたように「公開を保留している」としてマーク付けされる。

【００７７】

本開示のいくつかの実施形態は、本明細書における教示に従いプログラムされた従来の汎用目的の又は特化されたデジタルコンピュータ又はマイクロプロセッサを用いて便利に実装することができ、このことは、コンピュータ分野における当業者に明らかであろう。適切なソフトウェアコーディングを、本明細書における教示に基づいてプログラマが準備することができ、このことは、ソフトウェア分野における当業者に明らかであろう。いくつかの実施形態は、特定用途向け集積回路の準備により、又は従来のコンポーネント回路

の適切なネットワークを相互接続することにより実装されてもよく、このことは、当業者に容易に明らかになるであろう。情報及び信号が、様々な種々のテクノロジー及び手法のうち任意のものを用いて表現され得ることを当業者は理解するであろう。例えば、上記説明の全体をとおして参照され得るデータ、命令、要求、情報、信号、ビット、シンボル、及びチップは、電圧、電流、電磁波、磁場若しくは磁気粒子、光場若しくは光学粒子、又はこれらのうち任意の組み合わせにより表すことができる。いくつかの実施形態は、既存の並列の、分散コンピュータ処理及び分散データストレージフレームワーク（例えば、Ｈａｄｏｏｐ）を用いて実装することができる。

【００７８】

いくつかの実施形態は、命令を記憶させたコンピュータ読取可能媒体を含むコンピュータプログラム製品を含み、上記命令は、（例えば、プロセッサにより）実行されると、本明細書に説明される方法、手法、又は実施形態を実行し、コンピュータ読取可能媒体は、本明細書に説明される方法、手法、又は実施形態の様々なステップを実行する命令セットを含む。コンピュータ読取可能媒体には、命令を記憶させた記憶媒体を含むことができ、上記命令を使用して、実施形態の処理のうち任意のものを実行するようにコンピュータを制御し、あるいは上記実行をコンピュータにさせることができる。記憶媒体には、フロッピーディスク、ミニディスク（ＭＤ）、光ディスク、ＤＶＤ、ＣＤ－ＲＯＭ、マイクロドライブ、及び磁気光ディスクを含む任意タイプのディスク、ＲＯＭ、ＲＡＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、ＤＲＡＭ、ＶＲＡＭ、フラッシュメモリデバイス（フラッシュカードを含む）、磁気若しくは光学カード、ナノシステム（分子メモリＩＣを含む）、ＲＡＩＤ装置、リモートデータストレージ／アーカイブ／ウェアハウジング、又は、命令及び／又はデータを記憶するのに適した任意の他タイプの媒体又は装置を限定なく含むことができる。さらに、記憶媒体は、異なるタイプの媒体、例えばフラッシュ媒体及びディスク媒体などにわたりデータを記憶するハイブリッドシステムであってもよい。場合により、上記異なる媒体は、ハイブリッドストレージ集合に編成されてもよい。いくつかの実施形態において、種々の媒体タイプが、他の媒体タイプより優先されてもよい。例えば、フラッシュ媒体がハードディスク記憶媒体より優先されて、データを記憶し、あるいはデータを供給してもよく、あるいは、異なる作業負荷が、それぞれの作業負荷の特性に場合により基づいて、異なる媒体タイプによりサポートされてもよい。さらに、システムは、本明細書に説明される記憶動作を実行するように構成されたモジュールに編成され、ブレード上にサポートされてもよい。

【００７９】

コンピュータ読取可能媒体のうち任意のものに記憶され、いくつかの実施形態は、汎用目的の又は特化されたコンピュータ又はマイクロプロセッサのハードウェアを制御することとコンピュータ又はマイクロプロセッサが一実施形態の結果を用いて人間のユーザ及び／又は他のメカニズムと対話することを可能にすることとの双方のためのソフトウェア命令を含む。上記ソフトウェアには、デバイスドライバ、オペレーティングシステム、及びユーザアプリケーションを限定なく含むことができる。究極的に、上記コンピュータ読取可能媒体は、本明細書に説明される実施形態を実行するソフトウェア命令をさらに含む。汎用目的の／特化されたコンピュータ又はマイクロプロセッサのプログラミング（ソフトウェア）に含まれるのは、いくつかの実施形態を実装するソフトウェアモジュールである。

【００８０】

本明細書に説明される実施形態の様々な例示的な論理ブロック、モジュール、回路、手法、又は方法ステップは、電子ハードウェア、コンピュータソフトウェア、又は双方の組み合わせとして実装できることを当業者はさらに十分理解するであろう。ハードウェア及びソフトウェアのこの互換性を示すために、様々な例示的コンポーネント、ブロック、モジュール、回路、及びステップが、その機能性の観点で一般的に本明細書に説明されている。上記機能性がハードウェアとして実装されるかソフトウェアとして実装されるかは、システム全体に課される具体的な用途及び設計制約に依存する。当業者は、説明された機

能性を各々の具体的な用途のために様々な方法で実装することができるが、こうした実装判断は、本明細書に説明される実施形態からの逸脱を引き起こすと解釈されるべきではない。

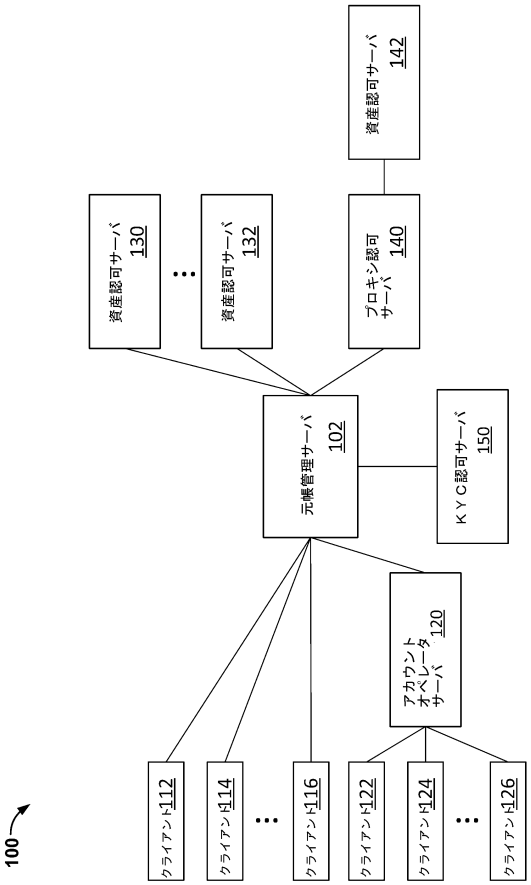
【００８１】

本明細書に開示される実施形態と関連して説明される様々な例示的な論理ブロック、モジュール、及び回路は、本明細書に説明される機能を実行するように設計された汎用目的プロセッサ、デジタルシグナルプロセッサ（ＤＳＰ）、特定用途向け集積回路（ＡＳＩＣ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）若しくは他のプログラマブル論理デバイス、ディスクリートゲート若しくはトランジスタロジック、ディスクリートハードウェアコンポーネント、又はこれらのうち任意の組み合わせで実装し、あるいは実行することができる。汎用目的プロセッサはマイクロプロセッサであり得るが、代替において、プロセッサは任意の従来的プロセッサ、コントローラ、マイクロコントローラ、又はステートマシンであってもよい。プロセッサはさらに、コンピューティング装置の組み合わせで実装されてもよく、例えば、ＤＳＰとマイクロプロセッサとの組み合わせ、複数のマイクロプロセッサ、ＤＳＰコアと関連した１つ以上のマイクロプロセッサ、又は任意の他のこうした構成である。

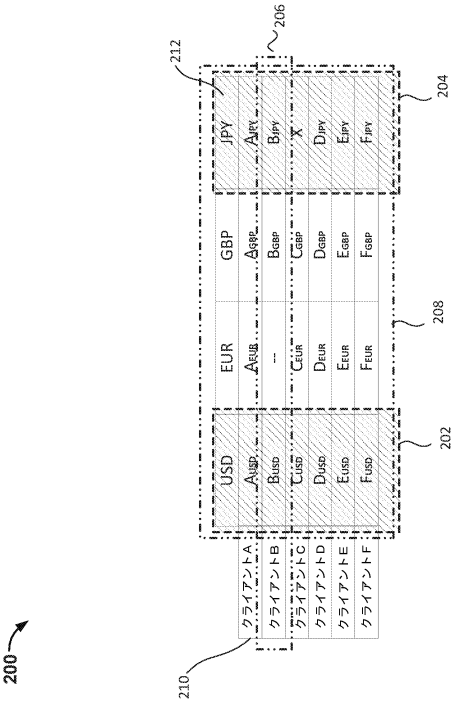
【００８２】

本明細書に開示される実施形態と関連して説明される方法の手法又はステップは、直接的にハードウェアで、プロセッサにより実行されるソフトウェアで、あるいは上記２つの組み合わせで具現化することができる。いくつかの実施形態において、本明細書に説明される任意のソフトウェアモジュール、ソフトウェアレイヤ、又はスレッドには、本明細書に説明される実施形態を実行するように構成されたファームウェア又はソフトウェア及びハードウェアを含むエンジンを含むことができる。一般に、本明細書に説明されるソフトウェアモジュール又はソフトウェアレイヤの機能は、ハードウェアで直接的に具現化されてもよく、プロセッサにより実行されるソフトウェアとして具現化されてもよく、あるいは上記２つの組み合わせとして具現化されてもよい。ソフトウェアモジュールは、ＲＡＭメモリ、フラッシュメモリ、ＲＯＭメモリ、ＥＰＲＯＭメモリ、ＥＥＰＲＯＭメモリ、レジスタ、ハードディスク、リムーバブルディスク、ＣＤ－ＲＯＭ、又は当分野において知られる任意の他形式の記憶媒体に存在することができる。一例示的な記憶媒体はプロセッサに結合され、プロセッサは記憶媒体からデータを読み出し、記憶媒体にデータを書き込むことができる。代替において、記憶媒体は、プロセッサに対して一体的であり得る。プロセッサ及び記憶媒体は、ＡＳＩＣ内に存在することができる。ＡＳＩＣは、ユーザ装置内に存在することができる。代替において、プロセッサ及び記憶媒体は、ユーザ装置内に個別のコンポーネントとして存在してもよい。

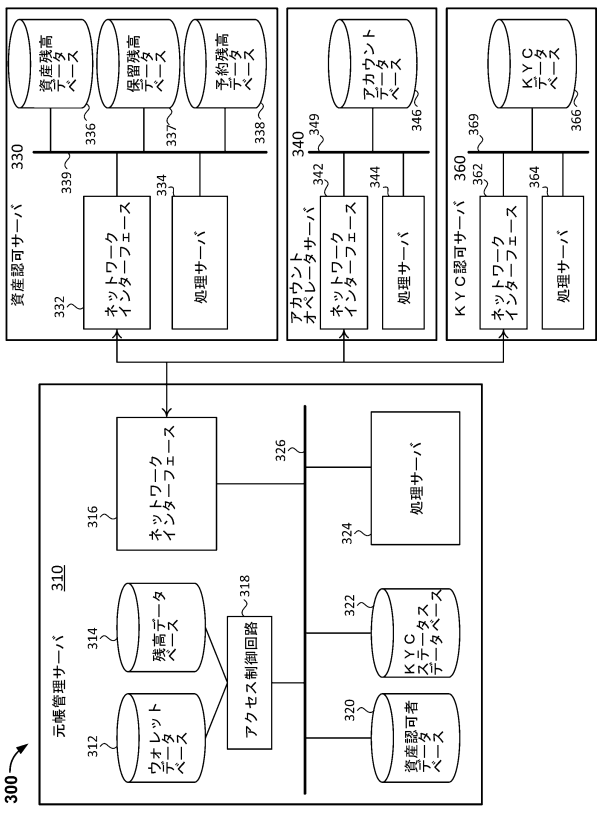
【図１】


100
資産認可サーバ 130
資産認可サーバ 132
プロキシ認可サーバ 140
資産認可サーバ 142
元帳管理サーバ 102
KYC認可サーバ 150
アカウントオペレータサーバ 120
クライアント112
クライアント114
クライアント116
クライアント122
クライアント124
クライアント126

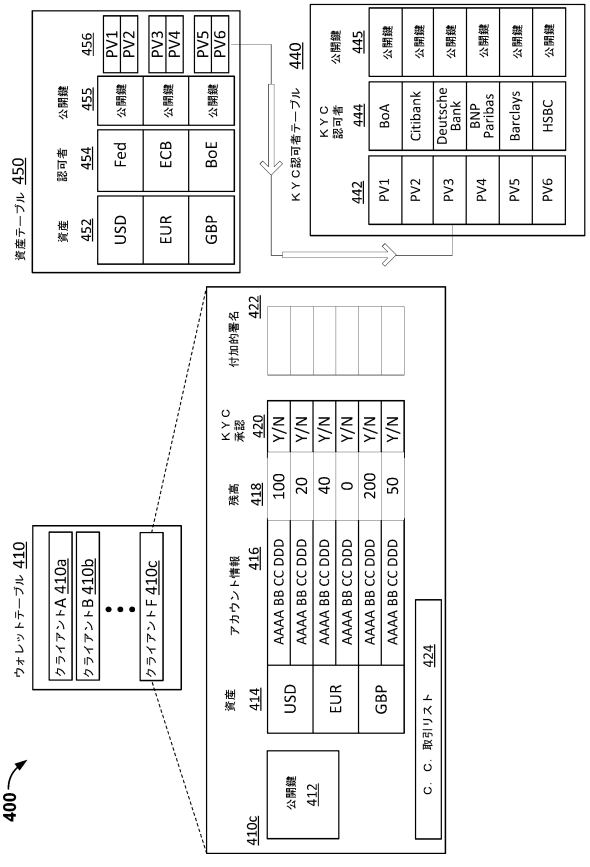
【図２】


200
210
212
206
204
208
202
USD
EUR
GBP
JPY
クライアントA
クライアントB
クライアントC
クライアントD
クライアントE
クライアントF

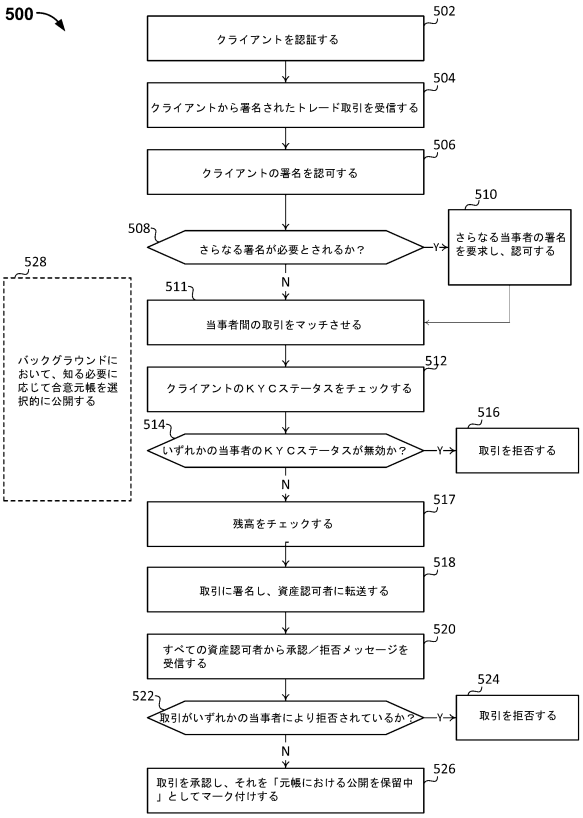
【図３】


300
元帳管理サーバ 310
資産認可サーバ 330
アカウントオペレータサーバ 340
KYC認可サーバ 360
ネットワークインターフェース
処理サーバ
資産残高データベース
保留残高データベース
予約残高データベース
アカウントデータベース
KYCデータベース
ウォレットデータベース
残高データベース
アクセス制御回路
KYCステータスデータベース
資産認可者データベース

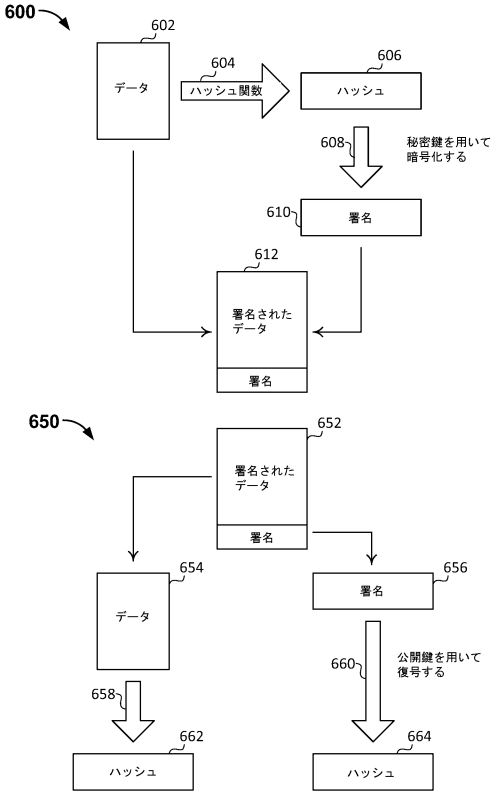
【図４】


400
資産テーブル 450
KYC認可者テーブル 440
ウォレットテーブル 410
C.C.取引リスト 424
公開鍵 412
USD
EUR
GBP
Fed
ECB
BoE
BoA
Citibank
Deutsche Bank
BNP Paribas
Barclays
HSBC
クライアントA 410a
クライアントB 410b
クライアントF 410c

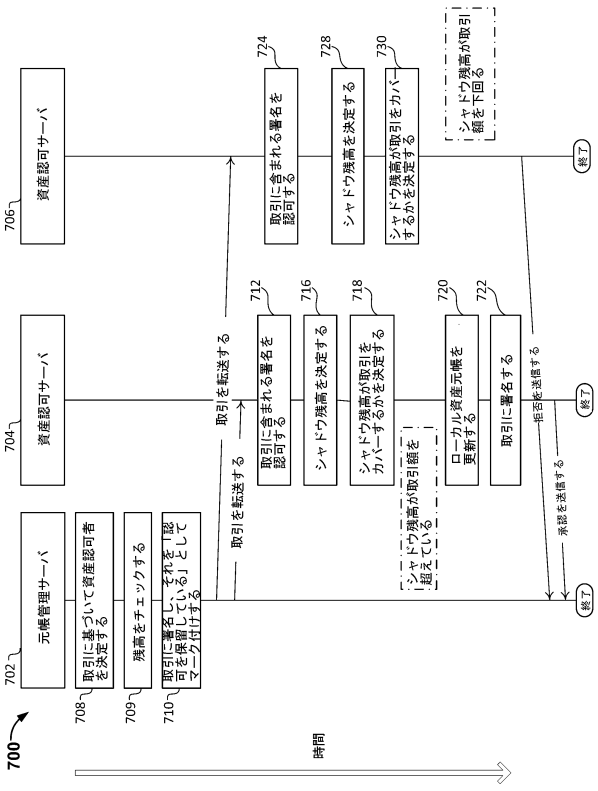
【図５】


500
クライアントを認証する
502
クライアントから署名されたトレード取引を受信する
504
クライアントの署名を認可する
506
さらなる署名が必要とされるか？
508
Y
さらなる当事者の署名を要求し、認可する
510
N
当事者間の取引をマッチさせる
511
クライアントのＫＹＣステータスをチェックする
512
いずれかの当事者のＫＹＣステータスが無効か？
514
Y
取引を拒否する
516
N
残高をチェックする
517
取引に署名し、資産認可者に転送する
518
すべての資産認可者から承認／拒否メッセージを受信する
520
取引がいずれかの当事者により拒否されているか？
522
Y
取引を拒否する
524
N
取引を承認し、それを「元帳における公開を保留中」としてマーク付けする
526
バックグラウンドにおいて、知る必要に応じて合意元帳を選択的に公開する
528

【図６】


600
データ
602
ハッシュ関数
604
ハッシュ
606
秘密鍵を用いて暗号化する
608
署名
610
署名されたデータ
612
署名
650
署名されたデータ
652
署名
データ
654
署名
656
ハッシュ関数
658
公開鍵を用いて復号する
660
ハッシュ
662
ハッシュ
664

【図７】


700
元帳管理サーバ
702
資産認可サーバ
704
資産認可サーバ
706
取引に基づいて資産認可者を決定する
708
残高をチェックする
709
取引に署名し、それを「認可を保留している」としてマーク付けする
710
取引を転送する
取引を転送する
取引に含まれる署名を認可する
712
シャドウ残高を決定する
716
シャドウ残高が取引をカバーするかを決定する
718
シャドウ残高が取引額を超えている
ローカル資産元帳を更新する
720
取引に署名する
722
拒否を送信する
承認を送信する
終了
終了
取引に含まれる署名を認可する
724
シャドウ残高を決定する
728
シャドウ残高が取引をカバーするかを決定する
730
シャドウ残高が取引額を下回る
終了
時間

フロントページの続き

(72)発明者　アーノルド，マシュー，ティモシー
イギリス国　オーエックス２５　５ピーディー　オックスフォードシャー，ローワー　ヘイフォード，ステーション　ロード，ザ　ビーチ　ハウス
(72)発明者　ナイーム，ザルタシャ
イギリス国　イー７　８エイチエヌ　ロンドン，セント　ジョージズ　スクエア　４３

審査官　鈴木　和樹

(56)参考文献　特開２０１３－０３３４０８（ＪＰ，Ａ）
特表２００６－５０５８６９（ＪＰ，Ａ）
米国特許出願公開第２００８／０２８１９０７（ＵＳ，Ａ１）
米国特許第０８８８６５７０（ＵＳ，Ｂ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　１０／００　－　９９／００