

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5116920号
(P5116920)

(45) 発行日 平成25年1月9日(2013.1.9)

(24) 登録日 平成24年10月26日(2012.10.26)

(51) Int.Cl.

F 1

G06Q 20/06 (2012.01)
G06Q 20/10 (2012.01)G06F 17/60 41 O E
G06F 17/60 234 S

請求項の数 40 (全 26 頁)

(21) 出願番号	特願2000-615945 (P2000-615945)
(86) (22) 出願日	平成12年4月28日 (2000.4.28)
(65) 公表番号	特表2002-543532 (P2002-543532A)
(43) 公表日	平成14年12月17日 (2002.12.17)
(86) 國際出願番号	PCT/US2000/011732
(87) 國際公開番号	W02000/067177
(87) 國際公開日	平成12年11月9日 (2000.11.9)
審査請求日	平成19年2月19日 (2007.2.19)
審判番号	不服2010-29264 (P2010-29264/J1)
審判請求日	平成22年12月24日 (2010.12.24)
(31) 優先権主張番号	60/131,785
(32) 優先日	平成11年4月30日 (1999.4.30)
(33) 優先権主張国	米国(US)
(31) 優先権主張番号	60/144,633
(32) 優先日	平成11年7月19日 (1999.7.19)
(33) 優先権主張国	米国(US)

(73) 特許権者	501416254 ペイパル, インコーポレイテッド アメリカ合衆国 カリフォルニア 951 31, サン ホセ, ノース 1エステ ィー ストリート 2211
(74) 代理人	100078282 弁理士 山本 秀策
(74) 代理人	100062409 弁理士 安村 高明
(74) 代理人	100113413 弁理士 森下 夏樹
(72) 発明者	レブチン, マックス アメリカ合衆国 カリフォルニア 943 06, パロ アルト, グラント アベ ニュー ナンバーキュー 469 最終頁に続く

(54) 【発明の名称】分散型ユーザ間で価値を電子的に交換するためのシステムおよび方法

(57) 【特許請求の範囲】

【請求項 1】

分散型価値交換システムにおける情報処理デバイスの動作方法であって、前記情報処理デバイスは、前記分散型価値交換システムにおける複数のユーザの間で価値交換を行うことを容易にし、

前記情報処理デバイスは、

前記複数のユーザと通信するように構成された通信手段と、

複数の登録ユーザに対して提供される複数の口座を格納するように構成された格納手段であって、前記複数の口座は、前記分散型価値交換システムにおける価値を含み、前記複数の口座の各々は、口座残高を格納することが可能である、格納手段と、

処理手段と

を含み、

前記動作方法は、

前記処理手段が、第1のユーザに対する口座を前記分散型価値交換システムに登録するステップであって、前記登録することは、前記第1のユーザの識別情報を前記格納手段に格納することによって行われ、前記第1のユーザの識別情報は、電子登録の間に、前記第1のユーザによって前記情報処理デバイスに通信される、ステップと、

前記通信手段が、前記格納手段に格納するために、前記第1のユーザから第1の通信情報を受信するステップであって、前記第1の通信情報は、第2のユーザの既存の識別子と、前記第1のユーザと前記第2のユーザとの間で交換されるべき価値とを含み、前記第2

10

20

のユーザの既存の識別子は、前記分散型価値交換システムから独立して前記第2のユーザとの通信を可能にする、ステップと、

前記処理手段が、前記第2のユーザが前記価値交換システムに登録されているかどうかを決定するステップと

前記通信手段が、前記価値交換システムに登録するように、前記第2のユーザに命令を送信し、前記処理手段が、前記第2のユーザから受信された前記命令に対する応答に基づいて、前記第2のユーザに対する、カスタマイズされたアクセスのレベルを有する口座を前記分散型価値交換システムに登録するステップであって、前記カスタマイズされたアクセスのレベルは、前記命令に応答して前記第2のユーザから受信された情報の量に基づいており、前記命令を送信するステップは、前記第2のユーザが前記価値交換システムに登録されていないということを前記処理手段が決定した場合に実行される、ステップと、10

前記通信手段が、前記格納されている第1の通信情報に基づいて、第2の通信情報を前記第2のユーザに送信するステップであって、前記第2の通信情報は、交換されるべき価値を含む、ステップと、

前記処理手段が、前記通信された交換されるべき価値に基づいて、前記第1のユーザの口座と前記第2のユーザとの間で価値交換を開始するステップと

を含む、動作方法。

【請求項2】

前記処理手段が、第2のユーザに対する口座を前記分散型価値交換システムに登録するステップは、前記第2のユーザの既存の識別子を、前記格納手段に格納することを含む、20請求項1に記載の動作方法。

【請求項3】

前記処理手段が、前記第1のユーザの口座と前記第2のユーザとの間で前記通信された価値を転送するステップをさらに含む、請求項1に記載の動作方法。

【請求項4】

前記第1のユーザと前記第2のユーザとの間で交換されるべき前記通信された価値は、換金可能な証書の形式で前記第2のユーザによって受信可能である、請求項3に記載の動作方法。

【請求項5】

前記第1のユーザと前記第2のユーザとの間で交換されるべき前記通信された価値は、30デビットカードを介して、前記第2のユーザによって受信可能である、請求項3に記載の動作方法。

【請求項6】

前記第1のユーザと前記第2のユーザとの間で交換されるべき前記通信された価値は、前記第2のユーザによって受信可能であり、かつ、取引証明書に含まれ、

前記方法は、

前記処理手段が、前記第1のユーザと前記第2のユーザとの間で交換されるべき前記通信された価値を第3のユーザに転送するステップをさらに含む、請求項3に記載の動作方法。

【請求項7】

前記第2のユーザの既存の識別子は、電話番号である、請求項1に記載の動作方法。40

【請求項8】

前記第2のユーザの既存の識別子は、電子メールアドレスである、請求項1に記載の動作方法。

【請求項9】

前記第1の通信情報を受信するステップは、

前記分散型価値交換システムにおける前記第1のユーザのモバイルクライアントデバイスが、前記第1のユーザの口座と前記第2のユーザの口座との間の価値交換を開始するステップと、

前記モバイルクライアントデバイスが、前記第1のユーザと前記分散型価値交換シス50テ

ムとの間の接続を確立するステップと、

前記モバイルクライアントデバイスが、前記第1のユーザと前記第2のユーザとの間で交換されるべき価値を前記情報処理デバイスに送信するステップと
をさらに含む、請求項1に記載の動作方法。

【請求項10】

前記価値交換を開始するステップは、

前記第1のユーザの前記モバイルクライアントデバイスと前記第2のユーザのモバイルクライアントデバイスとの間に通信リンクを確立することを含む、請求項9に記載の動作方法。

【請求項11】

前記第1の通信情報は、モバイル通信デバイスを用いて前記第1のユーザによって前記通信手段に通信される、請求項1に記載の動作方法。

【請求項12】

前記モバイル通信デバイスは、携帯情報端末機器である、請求項11に記載の動作方法。

【請求項13】

前記モバイル通信デバイスは、電話である、請求項11に記載の動作方法。

【請求項14】

前記モバイル通信デバイスは、送受信可能なポケットベルである、請求項11に記載の動作方法。

【請求項15】

前記第1の通信情報は、無線ネットワークを介して、前記モバイル通信デバイスから受信される、請求項11に記載の動作方法。

【請求項16】

前記モバイル通信デバイスは、切断可能なデバイスである、請求項11に記載の動作方法。

【請求項17】

前記処理手段が、前記第1のユーザと前記第2のユーザとの間で交換されるべき前記通信された価値を第1の形式から第2の形式に変換するステップをさらに含む、請求項1に記載の動作方法。

【請求項18】

前記第1の形式は、第1の通貨であり、前記第2の形式は、第2の通貨である、請求項17に記載の動作方法。

【請求項19】

前記処理手段が、前記第1のユーザと前記第2のユーザとの間で交換されるべき前記通信された価値を、前記価値交換が完了するまで第三者預託当事者に第三者預託して保持するステップをさらに含む、請求項1に記載の動作方法。

【請求項20】

非対称暗号方式が、前記価値交換を安全に行うために適用される、請求項1に記載の動作方法。

【請求項21】

分散型取引システムにおける情報処理デバイスの動作方法であって、前記情報処理デバイスは、前記分散型取引システムにおける複数のユーザの間で価値交換を行うことを容易にし、

前記情報処理デバイスは、

前記複数のユーザと通信するように構成された通信手段と、

複数の登録ユーザに対して提供される複数の口座を格納するように構成された格納手段であって、前記複数の口座は、前記分散型取引システムにおける価値を含み、前記複数の口座の各々は、口座残高を格納することが可能である、格納手段と、

処理手段と

10

20

30

40

50

を含み、

前記情報処理デバイスは、

前記通信手段が、価値を第2のユーザと交換するための命令を第1のユーザから受信するステップであって、前記第1のユーザは、前記分散型取引システムの登録ユーザであり、前記命令は、前記第2のユーザの既存の識別子と、前記第1のユーザと前記第2のユーザとの間で交換されるべき価値とを含み、前記第2のユーザの既存の識別子は、前記分散型取引システムから独立して前記第2のユーザとの通信を可能にする、ステップと、

前記通信手段が、前記第2のユーザに前記価値交換を通知するステップと、

前記処理手段が、前記第2のユーザが前記価値交換システムに登録されているかどうかを決定し、前記第2のユーザが前記分散型取引システムに登録されていないということを前記処理手段が決定した場合に、前記通信手段が、前記価値交換システムに登録するよう前に、前記第2のユーザに命令を送信し、前記処理手段が、前記第2のユーザから受信された前記命令に対する応答に基づいて、前記格納手段に格納するために、前記第2のユーザに対する、カスタマイズされたアクセスのレベルを有する口座を作成することによって、前記第2のユーザを前記分散型取引システムに登録するステップであって、前記カスタマイズされたアクセスのレベルは、前記命令に応答して前記第2のユーザから受信された情報の量に基づいている、ステップと、

前記処理手段が、前記第1のユーザの口座と前記第2のユーザの口座との間で価値を転送するステップと

を実行する、動作方法。

10

【請求項22】

前記識別子は、電子メールアドレスである、請求項21に記載の動作方法。

【請求項23】

前記既存の識別子は、電話番号である、請求項21に記載の動作方法。

【請求項24】

前記命令は、前記第1のユーザによって操作されるモバイル通信デバイスを介して受信される、請求項21に記載の動作方法。

【請求項25】

命令を格納したコンピュータ読み取り可能な格納媒体であって、前記命令がコンピュータによって実行されると、前記命令は、分散型価値交換システムにおける複数のユーザの間で価値交換を行うことを容易にする方法を実行することを前記コンピュータに行わせ、

前記コンピュータは、

前記複数のユーザと通信するように構成された通信手段と、

複数の登録ユーザに対して提供される複数の口座を格納するように構成された格納手段であって、前記複数の口座は、前記分散型価値交換システムにおける価値を含み、前記複数の口座の各々は、口座残高を格納することが可能である、格納手段と、

処理手段と

を含み、

前記コンピュータは、

前記処理手段が、第1のユーザに対する口座を前記分散型価値交換システムに登録するステップであって、前記登録することは、前記第1のユーザの識別情報を前記格納手段に格納することによって行われ、前記第1のユーザの識別情報は、電子登録の間に、前記第1のユーザによって前記コンピュータに通信される、ステップと、

前記通信手段が、前記格納手段に格納するために、前記第1のユーザから第1の通信情報を受信するステップであって、前記第1の通信情報は、第2のユーザの既存の識別子と、前記第1のユーザと前記第2のユーザとの間で交換されるべき価値とを含み、前記第2のユーザの既存の識別子は、前記分散型価値交換システムから独立して前記第2のユーザとの通信を可能にする、ステップと、

前記通信手段が、前記格納されている第1の通信情報に基づいて、第2の通信情報を前記第2のユーザに送信するステップであって、前記第2の通信情報は、交換されるべき価

20

30

40

50

値を含む、ステップと、

前記処理手段が、前記第2のユーザが前記価値交換システムに登録されているかどうかを決定し、前記第2のユーザが前記分散型取引システムに登録されていないということを前記処理手段が決定した場合に、前記通信手段が、前記価値交換システムに登録するよう前に、前記第2のユーザに命令を送信し、前記処理手段が、前記第2のユーザから受信された前記命令に対する応答に基づいて、前記格納手段に格納するために、前記第2のユーザに対する、カスタマイズされたアクセスのレベルを有する口座を作成することによって、前記第2のユーザを前記分散型取引システムに登録するステップであって、前記カスタマイズされたアクセスのレベルは、前記ユーザに送信された前記命令に応答にして前記第2のユーザから受信された情報の量に基づいている、ステップと、

10

前記処理手段が、前記通信された交換されるべき価値に基づいて、前記第1のユーザの口座と前記第2のユーザとの間で価値交換を開始するステップと

を実行する、コンピュータ読み取り可能な格納媒体。

【請求項26】

命令を格納したコンピュータ読み取り可能な格納媒体であって、前記命令がコンピュータによって実行されると、前記命令は、分散型取引システムにおける複数のユーザの間で価値交換を行うことを容易にする方法を実行することを前記コンピュータに行わせ、

前記コンピュータは、

前記複数のユーザと通信するように構成された通信手段と、

複数の登録ユーザに対して提供される複数の口座を格納するように構成された格納手段であって、前記複数の口座は、前記価値交換システムにおける価値を含み、前記複数の口座の各々は、口座残高を格納することが可能である、格納手段と、

20

処理手段と

を含み、

前記方法は、

前記通信手段が、価値を第2のユーザと交換するための命令を第1のユーザから受信するステップであって、前記第1のユーザは、前記分散型取引システムの登録ユーザであり、前記命令は、第2のユーザの既存の識別子と、前記第1のユーザと前記第2のユーザとの間で交換されるべき価値とを含み、前記第2のユーザの既存の識別子は、前記分散型取引システムから独立して前記第2のユーザとの通信を可能にする、ステップと、

30

前記通信手段が、前記第2のユーザに前記価値交換を通知するステップと、

前記処理手段が、前記第2のユーザが前記価値交換システムに登録されているかどうかを決定し、前記第2のユーザが前記分散型取引システムに登録されていないということを前記処理手段が決定した場合に、前記通信手段が、前記価値交換システムに登録する前に、前記第2のユーザに命令を送信し、前記処理手段が、前記格納手段に格納するために、前記第2のユーザに対する、カスタマイズされたアクセスのレベルを有する口座を作成することによって、前記第2のユーザを前記分散型取引システムに登録するステップであって、前記カスタマイズされたアクセスのレベルは、前記ユーザに送信された前記命令に応答して前記第2のユーザから受信された情報の量に基づいている、ステップと、

前記処理手段が、前記第1のユーザの口座と前記第2のユーザの口座との間で価値を転送するステップと

40

を含む、コンピュータ読み取り可能な格納媒体。

【請求項27】

分散型取引システムを介して複数のユーザの間で価値交換を行うことを容易にするコンピュータ実装方法であって、

前記コンピュータは、

前記複数のユーザと通信するように構成された通信手段と、

複数の登録ユーザに対して提供される複数の口座を格納するように構成された格納手段であって、前記複数の口座は、前記分散型取引システムにおける価値を含み、前記複数の口座の各々は、口座残高を格納することが可能である、格納手段と、

50

处理手段と

を含み、

前記方法は、

前記通信手段が、格納のために、第2のユーザに通知することなく、前記分散型取引システムに送信した第1のユーザから、価値交換取引を示す第1の情報を受信するステップであって、前記第1のユーザは、前記システムに登録されており、前記第2のユーザは、前記システムに登録されておらず、前記取引は、前記第2のユーザに関連し、前記取引は、前記第2のユーザの既存の識別子と、前記第1のユーザと前記第2のユーザとの間で交換されるべき価値とをさらに含み、前記第2のユーザの既存の識別子は、前記分散型取引システムから独立して前記第2のユーザとの通信を可能にする、ステップと、

前記通信手段を用いて前記第2のユーザに前記価値交換を電子的に通知するステップと、前記処理手段が、前記第2のユーザが前記分散型取引システムに登録されていないということを決定し、前記第2のユーザが前記分散型取引システムに登録されていないということを前記処理手段が決定した場合に、前記通信手段が、前記分散型取引システムに登録するように、前記第2のユーザに命令を送信するステップと、

前記第2のユーザから受信された前記送信された命令に対する応答に基づいて、前記処理手段が、前記第2のユーザを前記分散型取引システムに登録するステップであって、前記処理手段は、前記第2のユーザを前記分散型取引システムの前記格納手段に格納されている、カスタマイズされたアクセスのレベルを有する口座に割り当てることによって、前記第2のユーザを前記分散型取引システムに登録し、前記カスタマイズされたアクセスのレベルは、前記命令に応答して前記第2のユーザから受信された情報の量に基づいている、ステップと、

前記処理手段が、前記交換されるべき価値に基づいて借方または貸方に記入するよう¹、前記第1のユーザおよび前記第2のユーザに関連付けられて格納されている口座情報を処理することによって、交換されるべき価値を交換するステップと

を含む、方法。

【請求項 28】

命令を格納したコンピュータ読み取り可能な格納媒体であって、前記命令がコンピュータによって実行されると、前記命令は、分散型取引システムを介して複数のユーザの間で価値交換を行うことを容易にする方法を実行することを前記コンピュータに行わせ、

前記コンピュータは、

前記複数のユーザと通信するように構成された通信手段と、

複数の登録ユーザに対して提供される複数の口座を格納するように構成された格納手段であって、前記複数の口座は、前記分散型取引システムにおける価値を含み、前記複数の口座の各々は、口座残高を格納することが可能である、格納手段と、

処理手段と

を含み、

前記方法は、

前記通信手段が、格納のために、第2のユーザに通知することなく、前記分散型取引システムに送信した第1のユーザから、価値交換取引を示す第1の情報を受信するステップであって、前記第1のユーザは、前記システムに登録されており、前記第2のユーザは、前記システムに登録されておらず、前記取引は、前記第2のユーザに関連し、前記取引は、前記第2のユーザの既存の識別子と、前記第1のユーザと前記第2のユーザとの間で交換されるべき価値とをさらに含み、前記第2のユーザの既存の識別子は、前記分散型取引システムから独立して前記第2のユーザとの通信を可能にする、ステップと、

前記通信手段を用いて前記第2のユーザに前記価値交換を電子的に通知するステップと

前記処理手段が、前記第2のユーザが前記分散型取引システムに登録されていないということを決定し、前記第2のユーザが前記分散型取引システムに登録されていないということを上に前記処理手段が決定した場合に、前記通信手段が、前記分散型取引システムに登録

するように、前記第2のユーザに命令を送信するステップと、

前記第2のユーザから受信された前記送信された命令に対する応答に基づいて、前記処理手段が、前記第2のユーザを前記分散型取引システムに登録するステップであって、前記処理手段は、前記第2のユーザを前記分散型取引システムの前記格納手段に格納されている、カスタマイズされたアクセスのレベルを有する口座に割り当てることによって、前記第2のユーザを前記分散型取引システムに登録し、前記カスタマイズされたアクセスのレベルは、前記命令に応答して前記第2のユーザから受信された情報の量に基づいている、ステップと、

前記処理手段が、前記交換されるべき価値に基づいて借方または貸方に記入するよう¹⁰に、前記第1のユーザおよび前記第2のユーザに関連付けられて格納されている口座情報を処理することによって、交換されるべき価値を交換するステップと

を含む、コンピュータ読み取り可能な格納媒体。

【請求項29】

前記第2のユーザの既存の識別子は、前記第2のユーザの電子メールアドレスであり、前記第2のユーザは、前記電子メールアドレスによってのみ識別可能であり、

前記第2のユーザが前記分散型価値交換システムに登録されていない場合には、前記第2の通信情報は、どのように登録するかを示す前記第2のユーザのための詳細をさらに含み、

前記方法は、前記処理手段が、前記第1のユーザの口座と前記第2のユーザとの間で前記通信された価値を転送するステップをさらに含む、請求項1に記載の動作方法。²⁰

【請求項30】

前記処理手段が、預託された価値に基づいて前記第1のユーザに関連付けられて格納されている口座情報を調整するステップをさらに含み、前記預託された価値は、前記通信手段によって前記第1のユーザから受信され、前記預託された価値は、クレジットカードによって提供され、

前記調整するステップは、前記受信するステップの前に実行される、請求項29に記載の動作方法。

【請求項31】

前記処理手段が、預託された価値に基づいて前記第1のユーザに関連付けられて格納されている口座情報を調整するステップをさらに含み、前記預託された価値は、前記通信手段によって前記第1のユーザから受信され、前記預託された価値は、電子小切手によって提供され。³⁰

前記調整するステップは、前記受信するステップの前に実行される、請求項29に記載の動作方法。

【請求項32】

前記処理手段が、預託された価値に基づいて前記第1のユーザに関連付けられて格納されている口座情報を調整するステップをさらに含み、前記預託された価値は、前記通信手段によって前記第1のユーザから受信され、前記預託された価値は、A C H(自動精算所)によって提供され、

前記調整するステップは、前記受信するステップの前に実行される、請求項29に記載の動作方法。⁴⁰

【請求項33】

前記転送するステップは、前記要求の通知を前記第2のユーザに送信するステップの前に実行される、請求項29に記載の動作方法。

【請求項34】

前記転送するステップは、前記要求の通知を前記第2のユーザに送信するステップの後に実行される、請求項29に記載の動作方法。

【請求項35】

前記既存の識別子は、電子メールアドレスである、請求項1に記載の方法。

【請求項36】

10

20

30

40

50

前記既存の識別子は、電話番号である、請求項 1 に記載の方法。

【請求項 3 7】

前記通信手段は、前記第 1 のユーザによって操作されるコンピュータから、前記第 1 の情報を受信する、請求項 1 に記載の方法。

【請求項 3 8】

前記通信手段は、前記第 1 のユーザによって操作されるモバイル通信デバイスから、前記第 1 の情報を受信する、請求項 1 に記載の方法。

【請求項 3 9】

前記カスタマイズされたアクセスのレベルは、前記第 2 のユーザから受信された命令に対する応答において提供される検証された情報の量にさらに基づいている、請求項 1 に記載の動作方法。10

【請求項 4 0】

前記カスタマイズされたアクセスのレベルは、前記第 2 のユーザがより多くの価値に関する取引を行うことが可能なより高いアクセスのレベルを含む、請求項 1 に記載の動作方法。

【発明の詳細な説明】

【0 0 0 1】

(背景)

本発明は、コンピュータシステムおよび通信の分野に関する。より詳細には、システムおよび方法が、計算機器を通して分散型ユーザ間の価値の交換を促進するために提供される。20

【0 0 0 2】

多くの人々の間の価値を転送し、または交換する既存の方法は、多くの欠点を有する。例えば、現金の使用は、定期的な補充が必要であるし、両替をする必要が生じ、窃盗または紛失の可能性があり得、そして現金の支払いおよび受領に関しての記録をつける内蔵または容易な方法がない。同様に、小切手は偽造され得るし、単に原始的な記録管理（例えば、小切手の控え）を提供するだけであり、人はうっかりと当座資金を引き出しすぎ得る。クレジットカードは、現金と小切手に関する問題のいくつかを軽減し得るが、2人以上の個人間の支払いを行ったり、価値を交換するためには使用され得ない。

【0 0 0 3】

さらに、既存の価値交換取引が形式張っているために、その取引を完了することを非能率または困難にし得る。例えば、お金を別の人の銀行または他の金融口座へ転送するのに、人はその別の人の銀行口座番号を知る必要があり得る。その別の人がある、そのような情報を漏らすのは気が進まないことがあり得ることは理解できる。

【0 0 0 4】

従って、必要とされていることは、既存の手段および技術のすべての短所なしに、価値転送を可能にするためのシステムおよび方法である。例えば、価値交換取引が、他のもっと敏感な情報ではなく、人の既知または通常の識別子（例えば、電子メールアドレス、電話番号）を使用して行われ得ることが望まれる。

【0 0 0 5】

(要旨)

本発明の1実施形態において、分散型価値交換システムを使用して2人以上の人々の間で価値交換を行うためのシステムおよび方法が提供される。

【0 0 0 6】

この実施形態において、システムは、システムユーザとして人または他のエンティティ（例えば、職業）を登録し、登録ユーザであり得るまたはあり得ない人との価値交換取引を、人が行い得るために構成された1つ以上のシステムサーバを含み得る。ユーザは次にクライアント計算機器（例えば、ハンドヘルド、パームトップ、またはデスクトップのコンピュータ、ウェブ可能電話、送受信可能ポケットベル）を使用して、価値交換を開始または行う。価値交換は、システムとオンライン（例えば、システムに接続された）中に、才50

フライン中に、別のユーザのデバイスと（例えば、無線接続を通して）接続中に、行われ得る。取引が、システムに提示されると、システムは、まだ取引に気付いていない取引当事者を通知し、取引を清算するまたは終了し、そしてユーザの口座残高を適切に調整するよう試みる。

【0007】

通信サーバは、（例えば、有線のおよび／または無線の）接続を、登録ユーザになることを望んでいる人から受信するよう構成され得る。同期サーバは、ユーザのクライアントデバイスのシステムとの同期を促進するよう構成され得る。同期中、ユーザのデバイスは、取引をシステムに提示し、新規な取引または清算された取引についての情報を受信し、システム上の口座情報をクライアントデバイス上の情報と同期させ得る。セキュリティサーバは、おそらく非対称および／または対称暗号技術を使用してセキュリティ手順を実施するよう構成され得る。金融サーバは、他のシステムサーバおよび外部金融機関とインタラクトし、ユーザが価値をシステムに注入し、そして価値をシステムから引き出すことを可能にする。1つ以上のデータベースは、ユーザのための口座情報（例えば、口座情報、取引詳細）を格納し、そしてシステムの活動を調整することを助け得る。

10

【0008】

価値交換を行う1方法において、人はシステムに登録し、口座がその人のために作られ、システムのソフトウェアは、クライアントデバイスへダウンロードされる。ユーザは次に、クライアントがシステムに接続している接続していないに関係なく、クライアント上で取引を行い得る。接続されていない場合は、クライアントは取引詳細を格納し、そして同期目的のために後でシステムに接続される場合は、取引をシステムへアップロードし、そして他のユーザによって開始された取引を受信し得る。各取引は、交換される取引および価値に対する別の当事者の識別子を含み得る。本発明の1実施形態において、取引当事者は、電子メールアドレス、電話番号、社会保障番号などのシステム外で意味を有する識別子によって識別され得る。従って、ユーザが、人の適切な識別子を知っている限り、ユーザは、登録ユーザでない人と取引を開始し得る。

20

【0009】

システムが、ユーザによって開始された新しい取引を受信すると、システムは、開始ユーザによって提供された識別子を使用して、他の当事者と接続するよう試みる。別の当事者が登録ユーザである場合は、システムはまた、その当事者と接続する他の方法を知り得る。まだユーザでない当事者について、その当事者は、システムに接続し、登録し、そして取引を完了するよう求められる。

30

【0010】

価値転送のほとんどとなる手段もシステムに関連し得る。ユーザは、クレジットカード、小切手、現金、電子口座振替、直接預け入れ、などを通して自分のシステム口座へ価値を導入し得る。価値は、同じまたは類似のプロセスを使用してシステムから引き出され得る。取引当事者間で交換される価値は、（例えば、米国のドルや他の通貨で表される）貨幣であり得る、またはクレジット、アフィニティポイント、頻繁に飛行機に乗る人のマイル数、交換券、交換ポイントなどのいくつかの他の形を有し得る。

40

【0011】

（詳細な説明）

次の説明は、当業者が本発明を行いそして使用することを可能にするために与えられ、そして本発明の詳細な適用およびその要求に関連して提供される。開示された実施形態への様々な改変は、当業者に容易に明らかであり、本明細書中に規定される一般的原則は、本発明の意図および範囲から逸脱することなく他の実施形態および適用に適用され得る。従って、本発明は、示される実施形態に制限される意図はなく、本明細書中に開示される原則および特徴と一致する最も広い範囲と一致する意図のものである。

【0012】

本発明の本実施形態が、例示的に実施されるプログラム環境は、汎用のコンピュータ、またはハンドヘルドコンピュータなどの特殊目的デバイスを構成する。（例えば、プロセッ

50

サ、メモリ、データ格納、ディスプレイ、有線／無線通信性能)などのデバイスの詳細は、明瞭であるために省略される。

【0013】

本発明の技術は、様々な技術を使用して実施され得ることも理解される必要がある。例えば、本明細書中に記載される方法は、コンピュータシステム上で実行するソフトウェアにおいて実現され、またはマイクロプロセッサあるいは他の特別に設計されたアプリケーション特定集積回路、プログラム可能論理デバイス、またはそれらの様々な組合せのいずれかを利用するハードウェアにおいて実施され得る。詳細には、本明細書中に記載される方法は、搬送波、ディスクドライブ、またはコンピュータ読み出し可能媒体などの格納媒体上に常駐する一連のコンピュータ実行可能な命令によって実施され得る。例示的な形の搬送波は、ローカルネットワーク、またはインターネットなどの公的にアクセス可能なネットワークによってデジタルデータストリームを伝える電気的、電磁的、または光学的信号の形態を取り得る。10

【0014】

(導入)

本発明の1実施形態において、クライアント計算機器を使用して2人以上の人々の間の価値の交換を促進するためのシステムおよび方法が提供される。交換される価値は、(いずれかの通貨を使用して)実在の貨幣であり得、またはクレジット、デビット、割り引き、交換券、証明書、マイレージ(例えば、頻繁に飛行機に乗る人のマイル数)などの他の形態を取り得る。交換取引を行うために使用される計算デバイスは、本来ポータブルであってもよいし、なくてもよい、そして有線および無線の両方を含む事実上すべての通信媒体を使用し得る。本実施形態の1つのインプリメーションは、少なくとも一人のユーザが、ハンドヘルドまたはパームトップのコンピュータ、スマート電話、送受信可能ポケットベルなどのポータブル計算デバイスを使用する。本実施形態に適切な計算デバイスは、ネットワーク化されたパーソナルコンピュータなどの別のデバイス(例えば、システムサーバ)と常にリンクしたまま、通信状態であり得る、あるいは例えば携帯情報端末機器(PDA)のような切断可能であり得る。従って、価値交換取引は、他のシステム構成要素と接続または切断中に、オフラインまたはオンラインで行われ得る。20

【0015】

本発明の本実施形態によるシステムは、価値交換を促進するよう構成された少なくとも1つの高アクセス可能なコンピュータサーバを含む。例示的に、別の当事者と価値交換または価値転送を開始したいユーザは、前もってサーバと登録される(例えば、口座がサーバ上にユーザのために確立される)。他の当事者は、取引が開始されるまたはシステムと通信される時に登録ユーザであってもよいし、なくてもよい。30

【0016】

本発明の本実施形態による価値交換を行う1つの方法において、交換に関わるエンティティは、意味を有する、または電子メールアドレス、電話番号、社会保障番号などのシステム外の物を使用する識別子によって認識され得る。例示的に、各々そのような識別子は、1人の人間または1つのエンティティと関連するだけで、従って責任を促進する。しかし、別の方針において、多くのユーザまたは口座が識別子と関連し得る。40

【0017】

価値交換を行う方法の1実現において、システムの登録ユーザは、電子メールアドレスによってその当事者をシステムに対して識別することによって未登録の当事者との交換を開始する。登録ユーザは、価値の形式(例えば、金銭の量、クレジットまたはアフィニティポイントの数)、転送を実行する日付、未登録当事者の名前などの価値交換の様々な詳細を提供し得る。システムは次に、未登録の当事者(例えば、提供された電子メールアドレスを介して)と接続を試み、その当事者に価値交換を通知し、開始ユーザを識別し、そして未登録の当事者をサーバに接続して、交換を終了するよう依頼する。未登録の当事者は、取引を終了するためにシステムに登録するよう要求され得る。例えば、価値交換が未登録のユーザの利益に対して存在する場合は、未登録のユーザは、価値を使用してさらに別50

の当事者と交換を行うために、システムに価値を残すことを望み得る。または、未登録の当事者は、登録されずに、システムが取引を終了可能なだけの十分な情報（例えば、クレジットカードの番号、住所）のみを提供することを許され得る。

【0018】

本発明の異なる実施形態において、価値交換は、交換される価値を借りているまたは借りられている人によって開始され得る。さらに、交換される価値は、事実上どのような形でもあり得るし、そして／または本来変換され得る。例えば、第一のユーザによって保持されそして第二のユーザによって受け入れられる金銭の量あるいはクレジットまたは交換券は、商品またはサービスと交換されて第一のユーザから第二のユーザへ転送され得る。または、価値は、1つの通貨から別の通貨へ、あるいは、実在の金銭から商人とのクレジット、頻繁な飛行機に乗る人のマイル数、または他の価値によって表されるものまで変動し得る。従って、ユーザは、通貨またはシステム（例えば、ユーザ間の取引のため）内でのみ使用されるポイントを含む、多くの異なる形式の価値で、商品またはサービスに対して支払い得る。

【0019】

システムはまた、ユーザに普通の銀行の操作（例えば、引き出し、預け入れ、振り替え）、株取引、電子チケット発券などの実行を可能にするよう構成され得る。本発明の別の実施形態において、第三の当事者が、取引が終了するまで、価値を第三者預託として保持するために関わり得る。

【0020】

価値は、現金、小切手、デビット、または現在使用されているまたはビジネス界で受け入れられている事実上いかなる他の方法を介して、システムへ導入され（そしてユーザの口座へ振り込まれ（credit））得る。価値は、これらの形式および類似の形式でシステムから出て行き得る。

【0021】

本発明の別の実施形態において、本明細書中に記載される分散型システムは、価値交換以外の通信の形式のために使用され得る。例えば、1つの別の実施形態において、システムは、多くのユーザ間にソフトウェアを広めるかまたは普及させるために使用され得る。例示的に、登録システムのユーザは、次に未登録の人にシステムのソフトウェアを提供し得、それによってそのユーザが取引を行い得る。好都合なことには、ソフトウェアは、有線または無線の通信を使用してユーザのクライアントデバイス間で送信され得る。

【0022】

（価値転送を促進するためのシステムの1実施形態）

図1は、本発明の1実施形態による価値転送を促進するための例示的なシステムを示す。本発明の別の実施形態は、例示されたシステムの構成要素の任意のサブセットも構成し得る。

【0023】

図1のシステムは、中央データベース102を含み、データベースは価値交換取引を促進するために使用される様々な情報を格納するよう構成される。例示的に、データベース102に格納された情報は、システムの登録ユーザのための口座、および取引に参加しているか、または取引に参加するよう依頼された未登録のユーザに関する様々な情報を含む。登録および／または未登録のユーザについてのユーザ情報は、ユーザ識別子（例えば、名前、電子メールアドレス、電話番号、ネットワークアドレス、物理アドレス）、取引記録、1つ以上の異なる形式の口座残高（例えば、お金、頻繁に飛行機に乗る人のマイル数、お店のクレジット、アフィニティポイント、引換券、クーポン、割り引き）、好適な通信方法（例えば、電子メール、ワイヤレスボイス）、セキュリティデータなどを含み得る。

【0024】

図1のシステムにおいて、データベース102は、通信サーバ104、同期サーバ106、金融サーバ108、およびおそらくセキュリティサーバ110によってアクセスされる

10

20

30

40

50

。この実施形態において、通信サーバ104および／または他のシステムサーバが、通信ネットワーク120を通して1つ以上のユーザとインタラクトするよう構成される。例えば、通信サーバ104は、ウェブサーバ、電話スイッチ、DSLAM（ディジタル加入者ラインアクセスマルチプレクサ等）であり得、またはそれらを含み得る。

【0025】

インターネット上のウェブサイトなどの、通信サーバ104によってホストされるネットワークの存在は、新規なユーザそしておそらく既存のユーザにとってシステムへの主要なアクセスポイントとしての役立ち得る。例示的に、ユーザは、登録後システムにアクセスするための口座名およびパスワードを与えられる。他の形式のセキュリティ（例えば、デイジタル証明書、バイオメトリックデバイス）は、本発明の他の実施形態で使用され得る。
10

【0026】

本発明の1実施形態において、ユーザは、通信サーバ104から自分の計算機器のためのソフトウェアをダウンロードし得る。詳細には、通信サーバ104は、人がシステムに登録し、口座情報にアクセスおよび／または口座情報を改変し、取引を行い、および取引を終了することを可能にし得る。しかし、ユーザは、取引を開始または清算できる前に、システムに登録するよう要求され得る。

【0027】

例示された実施形態において、同期サーバ106は、システム上に格納された情報をユーザのクライアント計算機器およびローカルに格納されたデータと同期するよう構成される。例示的に、ユーザは、同期サーバに接続し、ユーザに関する取引（例えば、価値交換）の詳細をアップロードおよび／またはダウンロードし得る。同期セッション中、ユーザのクライアントは、（例えば、清算された取引を反映する）最新の口座情報を受信し得、追加の資金をユーザに請求し（例えば、クレジットカードに課金（charge）する、または銀行口座から資金を転送することによって）、顧客サービスにアクセスする、取引の状態を検証する、新しい取引を開始するなどを行うよう、システムを認定し得る。
20

【0028】

金融サーバ108は、1つ以上の金融機関とインターフェースをとるよう構成され、金融機関は、本発明の1実施形態において、システムの外部に位置し得る。従って、金融サーバは、クレジットカード会社、銀行（従来の銀行およびオンラインの銀行を含む）、および適切な形式で価値を扱いまたは処理する他のエンティティとインタラクトし得る。詳細には、金融サーバは、ACH（自動精算所）を通して資金を転送するように構成され得る。金融サーバ108は、ユーザのシステム口座残高が、所定のしきい値を下回る、あるいは上回る場合、外部金融機関のユーザの口座への請求を自動的に生成し、または貸方に記入するよう構成され得る。さらに、システムが、金融サーバ108を通してユーザに代わってアクセスし得る外部の価値は、ユーザが行い得る取引の数または取引における価値の量に影響を及ぼし得る。
30

【0029】

セキュリティサーバ110は、データベース102、通信サーバ104、同期サーバ106、および金融サーバ108のうち1つ以上と共同し、価値交換および価値交換に関する実行についてのセキュリティを適用、保証、または実施し得る。本発明の1実施形態において、ディジタル署名は、セキュリティ方式の大きな役割を果たし得る。DSA（ディジタル署名アルゴリズム）、その変種（例えば、ECDSAすなわち椭円カーブDSA）、RSAまたは他のディジタル署名プロトコルが、使用され得る。DES（ディジタル暗号化規格）などの対称暗号方式もまた、同じまたは異なる実施形態において適用され得る。メッセージの認証コードは、システムとユーザとの間で交換されるメッセージの完全さおよび認証を検証するために使用され得る。
40

【0030】

本発明の本実施形態において、公開鍵暗号化技術が、暗号的に検証可能な取引を生成し、およびその債務履行拒否を防ぐために、ディジタル証明書とともに使用され得る。対称暗
50

号方式は、（例えば、ユーザクライアントデバイスおよび／またはシステムに関する）データの安全な格納のために使用され得る。

【0031】

例示的に、価値交換システムを行う組織は、証明当局 (Certificate Authority) として振る舞い、そして個人のユーザを証明し得る。一方証明されたユーザは、今度は、個人の取引を証明し得る。証明されたユーザは、価値交換取引において使用のための身元証明書が発行され得る。

【0032】

身元証明書は、ユーザの名前、電子メールアドレス（または電話番号あるいは社会保障番号などのユーザを識別する他の重要な識別子）、口座番号、または名前などの情報を含み得る。例示的に、身元証明書はまた、ユーザの公開鍵を含み、公開鍵は、ユーザによって行われる取引の認証を検証するために使用され得る。10

【0033】

個人のユーザは、自分が行うまたは開始する取引についての取引証明書を生成し、そしてシステムは、（例えば、同期中に）ユーザの公開鍵でその証明書を認証する。取引証明書は、交換される価値、取引に対する別の当事者の識別子、（必要または所望なら）他の詳細を含み得、そしてユーザの秘密鍵で署名され得る。1実施形態において、ユーザのクライアント計算機器は、ユーザ登録中に公開／秘密鍵の対を生成し、そして秘密鍵が、クライアントデバイス上にのみ保持される。

【0034】

例示されたシステムは、様々なタイプの通信媒体を通してユーザと通信し得る。通信ネットワーク120は、従って、従来の有線ネットワーク（例えばインターネット）、および／またはポータブルコンピュータ（例えば、パームトップまたはハンドヘルド）、スマート（例えば、ウェブ使用可能な）電話、送受信可能なポケットベル、などのポータブルデバイスによって使用可能な無線ネットワークを含み得る。従って、ユーザは、クライアントコンピュータ122a、ポータブルクライアントコンピュータまたはディジタルアシスタント122b、無線電話122c、および／または通信サーバ104および／または同期サーバ106と通信可能な他のデバイスなどのデバイスを動作させることによって、システムとインタラクトし得る。例示的に、ポータブルクライアントコンピュータ122bは、独立しておよび自立して、システムと価値交換を行う、またはシステムへ価値交換を通信するよう構成され得る。または、別の実施形態において、ポータブルクライアントコンピュータ122bは、切断モードで交換の詳細を記録し、次に別の計算機器（例えばコンピュータ122a）に接続される（例えば、ドッキングされる）と、交換を完了するためにシステムへその詳細を転送する、および／またはシステムと同期するよう動作され得る。20

【0035】

価値交換取引に参加するために、ユーザによって使用されるポータブルクライアントデバイスは、システムとインタラクトするための一連の命令を組み込み得る。例えば、本発明の1実施形態において、ユーザのクライアントデバイスは、システムに接続中および／またはシステムから切断中に、ユーザが自分の口座残高にアクセスすることが可能なウォレット適用を含む。例示的に、本発明のこの実施形態において、ユーザのデバイスは、定期的に同期サーバ106に接続する。そのような接続中に、ユーザのデバイスは、サーバと通信し、新しい取引情報（例えば、ユーザに関する新しい価値交換の詳細）を送信および受信し、および／または、更新された口座情報（例えば、終了された取引を反映するため）を受信する。ユーザはまた、価値交換システムの外部のシステムまたは機関への価値転送または価値交換システムの外部のシステムからの価値転送などの、自分の口座に関する他の活動を公認または行い得る。40

【0036】

（価値交換を行う1方法）

本発明の1実施形態において、価値交換取引は、システムサーバ（図1の通信サーバ1050

4、同期サーバ106)または別の当事者のクライアントと接続または切断中に、1人のユーザ(例えば、自分のクライアントデバイスで)によって行われ得る。詳細には、本発明の1実施形態において、ユーザは、取引をシステムに提示することによって開始し、次にシステムは別の参加者に通知し、そしておそらく他の参加者をシステムに登録することによって、取引を終了する動作を行う。しかし、別の実施形態において、取引は、2つの(またはそれ以上の)当事者間の直接通信において行われ得、その後取引の詳細がシステムサーバの1つへ提示される。この別の実施形態において、少なくとも1つの(例えば価値が転送される)当事者が、システムと登録される必要があり得る。

【0037】

例示的に、システムが、関係する当事者の1つからの取引について知り、他の参加者を識別し、そして価値の転送方法を決定するまで、取引は終了すなわち完了し得ない。取引の終了は、1つの当事者(例えば、第一の口座および/または形式で)から第二の当事者(例えば、別の口座および/または形式で)へ価値の実際の転送を含み得る。取引が終了され得る前に、取引に対する当事者は、システムと登録され、および/または所定の情報(例えば、当事者を識別する、当事者の身元を検証する、価値を当事者へまたは当事者から転送する方法を決定する)を提供する必要があり得る。

10

【0038】

このセクションにおいて、1つ以上的方法が、2つ以上の当事者間で価値交換を実行するための図1に示されたような価値交換システムを使用するために説明される。本発明の範囲を逸脱することなく、当事者が使用し得る様々なタイプの計算機器、および/または異なるシステムまたは取引構成について、このセクションで説明される方法および手順は、変更または改変され得る。

20

【0039】

本発明の1実施形態において、図1のシステムは、2人以上に関する金融取引を促進するまたは行うためのシステムとして考察され得る。例示的に、取引において少なくとも1人が、システムとすでに登録されており(例えば、口座を有する)、そして価値を転送する少なくとも1つの形式またはコンジット(conduit)が存在する。しかし、好都合には、登録ユーザは、未登録の当事者と取引を開始し得る、未登録の当事者は、電子メールアドレス、電話番号、IP(インターネットプロトコル)アドレスなどの既存の識別子でシステムに対して識別され得る。従って、この実施形態において、未登録のユーザ(および/または登録ユーザ)に関連する識別子はすでに重要性を有し、またはシステム外の物を使用し得る。従って、その識別子は、それらの識別子を通してまたはそれらの識別子で到達し得るある程度の保証が存在し得る。

30

【0040】

しかし、一旦システムに認識される(例えば、システムに登録する)と、ユーザは、価値交換、ならびにポータブル、準ポータブル、および他の計算機器を使用する他の取引を行い得る。詳細には、システムでユーザは、自分のクライアントデバイスから直接的に(例えば、互換性装備されたデバイスを有する別のユーザまたは人へ)、または間接的に(例えば、システムサーバに取引を記述または提示し、次に別の取引当事者を通知することによって)、安全な取引を行い得る。

40

【0041】

例示的に、直接転送において、当事者は後の債務履行拒否を防ぐために、暗号トークンを交換し、そしてシステムに対して取引を認証し得る。一旦システムが、少なくとも1当事者によって取引を通知されたら、取引は終了され得る。間接的な転送において、開始ユーザに代わって、別の当事者と(例えば、電子メールまたは電話で)連絡し得、そして当事者がまだ登録されていない場合、自分の転送または交換を受信しおよび/または行うために、その当事者にシステムと登録するよう依頼し得る。本発明の1実施形態において、依頼された当事者は、もちろん、システムと登録することなく、取引の自分の役割を充足する(例えば、お金または他の価値を受け取るまたは支払う)ことができ得る。例えば、依頼された当事者は、従来の形式(例えば、小切手、クレジットカード、デビットカード)

50

でシステムへ支払いを送り、またはシステムから支払いを受け取り得る。

【0042】

次に図2を参照して、本発明の1実施形態による間接的な価値交換取引を行う例示的な方法が示されている。示された方法は、図1に示されたシステムでの使用に適切である。

【0043】

状態200において、第一のユーザ（ユーザ1）は、システムに登録し、その1方法は、次のセクションで説明される。例示的に、登録プロセスの一部として、ユーザ1は、自分の名前および住居／郵便住所、重要な識別子（例えば、電子メールアドレス、電話番号、社会保障番号）、および適切な金融情報を提供する。ユーザ1によって提供された金融データは、個人の取引のため、および／または取引の価値が所定の制限を越える場合に、貸方に記入されるかまたは請求されるクレジットカードまたは銀行口座を含み得る。詳細には、ユーザは、自分に関する金融データ、つまり個人情報（例えば、住所）が検証され得る程度などに基づいて、どれだけの価値をシステムを通して転送できるかについての制限を割り当てられ得る。制限は、ユーザが、所定の時間に関係し得る未清算の取引の大きさまたは数に影響を及ぼし得る。

10

【0044】

登録ユーザは、システム内に口座番号または他の識別子を割り当てられ得る。しかし、上述したように、当事者は、当事者と関連する外部の重要な識別子（例えば、電子メールアドレス、電話番号）を特定することによって取引に含まれ得る。ユーザ1は、別の計算機器（例えば、システムサーバ）と通信する性能を有する事実上すべての形式のクライアントデバイス（例えば、ハンドヘルドまたはパームトップのコンピュータ、デスクトップ、ウェブ使用可能電話）を使用して、システムと登録し、そして取引を行い得る。

20

【0045】

本発明の現在説明された実施形態において、ディジタル証明書は、登録プロセスの一部として、ユーザ1について生成され、またはユーザ1によって提供される。例示的に、ユーザ1について生成された証明書は、ユーザ1の名前ならびに電子メールアドレス（あるいは他の重要な識別子）およびシステムによって署名された公開鍵が含まれ、これら全ては、前にユーザ1に割り当てられたまたはユーザ1によって選択されたコード（例えば、個人識別番号すなわちPIN）によって暗号化される。後のセクションで説明されるユーザを登録する1方法において、公開／秘密対の暗号鍵が（例えば、ユーザのクライアントまたはセキュリティサーバ110によって）生成され、そして秘密鍵は、クライアント、またはユーザによって動作される他のコンピュータシステムによってのみ保持される。

30

【0046】

状態202において、ユーザ1は、システムによって提供されるソフトウェアを使用してクライアントに取引を入力する。例示的に、ユーザ1が価値価値および転送される価値価値を交換したい当事者（例えば、ユーザ2）の電子メールアドレス、電話番号、または他の識別子をユーザ1は入力するだけである。この実施形態において、価値はいずれの方向にも（すなわち、ユーザ1からまたはユーザ1へ）流れ得る。ユーザ1が転送し得る（価値がユーザ2へ流れる場合）価値の量は、自分のシステムの口座残高に制限され得る。この量は、要求されまたは開始されたがまだ清算されていないいずれの他の転送によって（他のユーザに対して）減少され得る（例えば、クライアントがシステムと同期する場合にクライアント上に格納されそして更新され得る）。しかし、ユーザ1が、他の支払い取り決めを（例えば、クレジットカード、電子口座振替を通して）提供する場合は、ユーザ1は、口座残高を越えることができ得る。

40

【0047】

ユーザ1は、取引を入力する前にクライアントシステムソフトウェアを起動させるために、セキュリティコード（例えば、個人識別番号またはパスワード）を入力することを要求される。例示的に、不正確なコードが所定の回数（例えば、10回）入力された場合、取引を入力する性能は、使用不能となり得、ユーザ1は、クライアントソフトウェアを再使用可能にするために（以下で説明されるように）システムと接続するか、またはシステム

50

と同期するよう要求され得る。

【0048】

ソフトウェアは、ユーザ1が価値交換取引を前に行ったすべての当事者のリストを維持し得る。その場合にユーザ1は、ユーザ2がリストに含まれている場合は、ユーザ2の識別子をただ単に選択し得る。ユーザ1によって使用されるクライアントシステムソフトウェアは、多くの取引選択を提供し得る。例えば、ユーザ1はまた、ユーザ2へ（またはユーザ2から）の一方だけの取引を開始しし得る。ユーザ1のクライアントおよびユーザ2のクライアントが、直接的な（例えば、無線の）通信が可能である場合は、ユーザ1はまた、相互の取引を開始し得る。またさらに、ユーザ1は、クライアントシステムソフトウェアをユーザ2のクライアントデバイスへ送信し得る。しかし、この場合、ユーザ2は、ユーザ2がシステムに登録する（そして口座を開く）まで別の当事者に価値を転送不可能であり得る。10

【0049】

クライアントに取引を入力後しばらくして、状態204において、ユーザ1は、同期サーバ106と同期する。詳細には、ユーザ1は、自分のクライアントを同期サーバと接続するために必要なすべてのコマンドまたは動作を開始する。クライアントは、おそらく無線接続を通して、あるいは任意の数の仲介デバイスまたは媒体を通して、（例えば、インターネット）直接接続でき得る。詳細には、ユーザ1のクライアントがポータブルデバイスである場合は、同期サーバ106へ接続を開始するために、ユーザ1は、そのデバイスとドッキングするか、そうでなければそのデバイスを別のコンピュータシステムへ接続する。20

【0050】

同期は、定期的に（30日ごとに少なくとも1回）要求され得る。この要求が充足されない場合、クライアントソフトウェアは、自動的にユーザ1が支払いを行うことまたは取引を開始することを防ぎ得る。さらに、クライアントに取引を入力後一定の期間（例えば、30日）内にユーザ1のクライアントが同期しない場合は、ユーザ1のクライアント上で行われる取引は自動的に取り消されまたは破棄され得る。

【0051】

本発明の1実施形態による典型的なプロセスにおいて、ユーザ1のクライアントは、同期サーバ106と接続し、自分のシステム口座番号（および／または電子メールアドレス、電話番号または他の重要な識別子）によってユーザ1を識別する。サーバは、ユーザ1についてのユーザ記録を（例えば、データベース102中に）位置させ、ユーザに割り当てられたまたはユーザに関連するコード（例えばPIN）を取り出す。ユーザ1に関連するおよび同期中ユーザ1へ送信されるディジタル証明書は次に、このコードで暗号化される。このディジタル証明書は、ユーザ1が登録された時に生成された証明であり得る。しかし、例示的に、ディジタル証明書は、他のユーザによってシステムに報告されたユーザ1に関する取引についての1つ以上の取引証明で増大され得る。ディジタル証明はまた、新しいコード（例えば、PIN）をユーザ1へ送信するために使用され得る。30

【0052】

ユーザ1についてシステム上に格納されたディジタル証明が存在しない場合は、同期サーバは、ユーザ1のパスワードおよび電子メールアドレス（または他の識別子）を要求する。この情報が検証された場合は、新しい鍵の対が生成され、そして新しいディジタル証明が発行される。40

【0053】

最初の同期接続が確立された後、クライアントは、現在の取引（およびクライアントが格納し、まだ送信していない他の取引）をサーバへ送信する。取引は、上記で説明されたように、ディジタル取引証明を使用して送信され得る。ユーザ1の全ての前の取引が清算した（例えば、前の取引において別の当事者がシステムに接続しそして取引を受け入れることができた）場合、クライアントは通知され、この場合取引はクライアントから取り除かれ得る。サーバは次に、ある基準（例えば、日付、時間、他の当事者、取引の価値、価値50

転送の方向)に従って、未清算の取引を優先させ得る。

【0054】

ユーザのクライアント(および/またはシステムサーバ)は、ユーザによって行われたおよび/またはユーザに関する取引を記録する取引ログを維持し得る。次に、ユーザが取引を開始する場合ログの入力が行われる。クライアントがシステムサーバから(例えば、同期中に)知る各取引(例えば、別の当事者によって開始された)についてもログの入力が行われ得る。入力は、関連した取引が清算後削除されるか、またはアーカイブされ得る。

。

【0055】

本発明の1方法において、口座残高が、同期プロセス中変更される。詳細には、ユーザ1の口座は、ユーザ1から離れて転送されている全ての価値について借方に記入される。しかし、逆に、価値転送に対して他の当事者がその転送と同期する、そうでなければ認めるまたは承認するまで(例えば、取引が清算するまで)ユーザ1の口座は、ユーザ1によって開始された入来の価値転送について貸方に記入され得ない。ユーザ1のシステムの口座が、転送(例えば、ユーザ2へ)を行うだけの十分な残高を有する場合、クレジットカードまたは他の価値のストリームは、それらをカバーするために(例えば、金融サーバ108によって)傍受され得る。

【0056】

従って、状態204において、一旦ユーザ1が同期サーバに接続すると、取引は、まだ提示されていないすべての他の取引と共にシステムへ通信される。代わって、同期サーバは、クライアントにすべての終了された取引を通知し、そしてユーザ1を含む、他の当事者によって開始された取引をダウンロードする。従って、状態204の同期プロセスは、ユーザ1が当事者である様々な取引で、ユーザ1のクライアントおよびシステムを更新することを含み得る。システムサーバおよび/またはクライアント上の口座残高は、同期プロセス中またはその後でそれに従って変更され得る。

【0057】

状態206において、システムサーバ(例えば、同期サーバ106)は、ユーザ1/ユーザ2の取引の詳細(例えば、ユーザ2の識別子および転送される価値を含む)を受信する。価値交換が、ユーザ1からユーザ2である場合、ユーザ1の口座は、転送の量によって自動的に借方に記入され得る。このことで、請求は、ユーザ1に関連するクレジットカードまたは銀行口座へ要求され得る。しかし、例示的に示された実施形態において、口座の更新は手順の後の段階まで延期され得る。

【0058】

状態208において、システムは、ユーザ2に取引を通知しようと試みる。この実施形態において、システムは、ユーザ1によって(例えば、自動化された電子メールメッセージまたはボイスメッセージを生成することによって)提示された識別子を使用する。しかし、ユーザ2が登録システムユーザである場合は、ユーザ2の口座は、ユーザ2が取引通信を受信する異なる好適な方法を有するかどうかを判定するために調査され得る。ユーザ2が登録ユーザでない場合は、自動化されたメッセージは、ユーザ2が価値を受信するために行わなければならないことに関する詳細を含む。例えば、通信サーバ104によってホストされるシステムウェブサイトは、識別され得、そしてユーザ2は、サイトに接続し、そして登録するよう依頼され得る。

【0059】

状態210において、この状態は状態208と同時に生じ得るが、システムは、ユーザ2が登録ユーザかどうかを判定する。登録ユーザである場合は、ユーザ2は、登録する必要はなく、そして手順は状態214に続く。

【0060】

しかし、状態212において、ユーザ2は、ユーザ1と取引の時に登録されていず、従つて、特に価値がユーザ2からユーザ1へ転送される必要がある場合は、取引が終了され得る前に登録するよう要求され得る。システムに登録することによって、ユーザ2は、価値

10

20

30

40

50

を伝達するための事実上任意の通常の手段（例えば、クレジットカード、小切手、デビットカード、電子口座振替）を使用して取引価値を受信し、または提示し得る。しかし、本発明の1つの実施形態において、ユーザ2は、登録するよう要求され得ない。詳細には、この別の実施形態において、ユーザ2は、システムへの1回限りの支払い、またはシステムから1回限りの引き出しが（例えば、クレジットカードまたは小切手で）でき得る。

【0061】

状態214において、ユーザ2は、取引を受け入れまたは認める。ユーザ2が、未登録の当事者であり、システムからの依頼に応答して登録する場合に、受理が意味され得る。状態214は、価値がユーザ2からユーザ1へ転送される必要のある取引についてのみ要求され得る。言い換えると、第一のユーザが、価値を別のユーザへ転送するため取引を開始する場合に、他のユーザの認証は必要であり得ない。しかし、第一のユーザが、価値を別のユーザから受信するために取引を開始する場合は、取引を終了する前に他のユーザからの承認を受ける必要があり得る。

10

【0062】

状態216において、取引は、取引の価値に従って、ユーザ1およびユーザ2についてのシステムの口座残高を変更することによって終了する。加えて、他の当事者に価値を提供するユーザは、取引をカバーするためにシステムへ追加の価値を注入する必要があり得る。従って、金融サーバ108は、ユーザのクレジットカードに請求し、電子口座振替を行い、または他の行動をとり得る。さらに、ユーザの口座残高について制限すなわち最高限度がある場合、金融サーバは、ユーザのクレジットカード、デビットカード、銀行口座などに価値を貸方に記入し得る。

20

【0063】

状態218において、ユーザ1およびユーザ2についてのクライアントデバイスは、取引（および、おそらく他の取引）に従って更新される。しかし、ユーザ1またはユーザ2が、その時にシステムから切断されている場合は、次に接続するときに、そのデバイスが（例えば、同期サーバ106によって）最新にされ得る。状態218の後、例示された手順は終了する。

【0064】

本発明の本実施形態において、ユーザ1は、新しいユーザをシステムに導入することでアフィニティポイントまたはある他の報奨を与えられ得る。詳細には、ユーザ2が、ユーザ1がシステムに取引を提示したときに登録ユーザでなかった場合は、ユーザ1は、ユーザ2がシステムから取引通知に応答して登録する場合、報奨を受け得る。

30

【0065】

図2に示され、上記で説明した本発明の実施形態は、図1に示されたようなシステムと価値交換を行う単なる1方法である。この方法は、様々なタイプのクライアントデバイス、通信媒体および通信シーケンスの使用に適応するために容易に改変され得る。詳細には、前の方法は、登録ユーザと未登録当事者との間に、2つ以上の登録ユーザ間に、または価値が交換される事実上すべての環境において、価値交換を行うために、説明されたように、あるいは少し変更されて、適用され得る。

【0066】

図3は、モバイルクライアントデバイス上で1人のユーザによって行われる間接的な価値交換の1形式を示す。図3において、ユーザAは、自分のデバイスクライアントAで価値交換を入力する。取引は次に、おそらく同期プロセス中に、システムサーバへ提示される。（ユーザAが最大の価値を転送するよう公認されている場合）価値の量は、ユーザAの口座から取り除かれ、そしてユーザAのクライアントデバイスは、自分の新しい口座残高で更新される。ユーザAの口座残高が最低限のレベルを下回る、または要求された交換を完了するために転送が必要な場合は、追加の資金または価値が、銀行、クレジットカード、ACH、またはユーザAと関連する他の金融源から回収される。価値は、ユーザBの口座に預けられ、ユーザBがまだ登録ユーザでない場合は、ユーザBの口座を作りよう要求し得る。

40

50

【 0 0 6 7 】

本発明の1実施形態において、取引の価値は、第三者預託に保持され得る。この実施形態において、取引を開始するユーザは、価値を第三者預託にされる選択を選ぶ。このユーザが、支払者（例えば、価値が転送される当事者）である場合、ユーザの口座は、取引がシステムに通信されるとすぐ、借方に記入され得るが、特定された受領者へ貸方を記入される代わりに、第三者預託口座に保持される。例示的に、価値受領者は、価値は第三者預託に保持されていること、そしておそらくそれを譲渡するための条件を通知される。システムは、資金が受領者へ転送され、または支払者へ戻される前に、両当事者が合意することを要求し得る。システムは、債務不履行によって、当事者から反対がない場合は、ある一定の期間後、転送を完了するよう、または逆に、1つまたは両方の当事者が、特定の期間内に取引を認めない場合は、取引を取り消すよう、構成され得る。10

【 0 0 6 8 】

次のサブセクションは、上記で説明したものと異なる環境または状況において価値交換を行う方法を説明する。

【 0 0 6 9 】**(オンラインの価値交換を行う)**

価値交換を行う1つの別の方法において、ユーザは、（例えば、デスクトップまたは無線のクライアントから）インターネット接続を通して価値交換システム（例えば図1のシステム）に接続する。この方法において、図1の通信サーバ104は、システムのためのウェブサイトをホストするウェブサーバを含む。取引を開始したいユーザは、通信サーバ104に接続し、ユーザ名、口座名、または他の識別子（例えば、電子メールアドレス、電話番号）およびパスワードを提供することによって必要なセキュリティ要求を充足する。この実施形態の1つの別の方法において、ユーザに暗号認証またはセキュリティトークンを提供するよう要求する暗号セキュリティ手段が実施され得る。20

【 0 0 7 0 】

ユーザは、別の当事者の識別子（例えば、電子メールアドレス、電話番号、社会保障番号、口座名）を転送される取引および価値に提供することによってオンラインの形式を完了する。また、ユーザは、価値が自分から他の当事者へ、またはその逆に転送される必要があるかを特定し得る。システムとユーザのインターフェイス（例えば、ユーザが接続するまたはログインする場合にユーザに与えられるウェブページ）は、ユーザに対して個人化され得る。詳細には、ユーザが過去に取引をした当事者の識別子は、すぐに選択するために利用可能であり得り、その場合、ユーザは、識別子を記憶しまたは入力する必要はないが、その代わり、リストから1つ識別子を選択し得る。30

【 0 0 7 1 】

他の当事者がすでに登録システムユーザである場合、システムは次に、続いて価値転送を行い得る。例示的に、価値が開始ユーザから他の当事者へ流れる場合は、システムは、取引を完了または終了するために、他の当事者の承認または公認を要求し得ない。システムは、単に取引の通知を（例えば電子メールを介して）当事者へ送信し得る。対照的に、価値が、他の当事者から開始ユーザへ流れる場合は、システムは、終了前に他の当事者の承認を要求し得る。取引の価値が、開始ユーザから他の当事者へ流れる場合は、ユーザの口座は、取引が終了する前（例えば、他の当事者が取引を受け入れる前）でも転送される量によって借方に記入され得る。40

【 0 0 7 2 】

他の当事者が登録システムユーザでない場合は、システムは、開始ユーザによって提供される識別子を使用することによって、当事者に未決済の取引を通知する。通知は、従って電子メールを介して送信され得る。例示的に、通知は、取引を開始したユーザを識別し、他の当事者に取引の量を伝え、そして取引を完了する方法／場所（例えば、ウェブページまたはウェブサイト）を特定する。価値を受信し、または開始ユーザによって要求された価値を提示するために、他の当事者は次に、システムに接続し、そして登録する。新しいユーザを登録する方法は、次のセクションで説明される。50

【 0 0 7 3 】

オフラインの取引（例えば、切断可能なポータブル計算機器を使用して）と異なり、取引をオンラインで行う場合は、ユーザは、リアルタイムで口座情報にアクセスし、および／または取引を終了でき得る。

【 0 0 7 4 】

このサブセクションにおいて説明された本発明の方法は、有線または無線の接続を介してのインターネットを通して、（有線のまたは無線の）電話接続を通して、システムと同時のリンクを確立し、そして維持し得るクライアントに関する適用に適切である。

【 0 0 7 5 】

（直接（クライアントからクライアントへの）価値交換を行う）

10

本発明の1つの別の実施形態において、2つの当事者が、価値交換を行うために自分のクライアント計算機器を使用する方法が提供される。2つの当事者が取引を行っている間にシステムから切断される場合は、取引後、そのうちの1人または両者が取引を（例えば、図1のシステムの通信サーバ104または同期サーバ106を介して）システムに提示する。この方法は、モバイル計算機器、および別のクライアントと（例えば、有線または無線の通信媒体を介して）直接通信し得るスマートつまりウェブ使用可能な電話の使用に特に適している。

【 0 0 7 6 】

クライアントからクライアントへの取引を行う選択は、ユーザにとって利用可能ないくつかの選択のただ1つの選択であり得る。例えば、クライアントデバイス上にインストールされたシステムソフトウェアはまた、1人のユーザが、システムソフトウェアを別のユーザへ送信し、一方だけの取引（例えば、図2と関連して上記で説明されたように）を行い、そのユーザの口座残高（クライアントが同期されるたびに更新される）または取引ログを見る、計算器を使用する、などを行ひ得る。

20

【 0 0 7 7 】

ユーザが、クライアントからクライアントの取引を行うことを選択する場合は、ユーザのクライアントは、別のクライアントとの接続を確立するよう自動的に試み得る。クライアントは、無線または有線のモードでそのような接続をするよう構成され得る。

【 0 0 7 8 】

この方法において、各ユーザは、自分の計算機器を起動し、そしてその計算機器の1つは、インストールされたシステムソフトウェアを動作し、他のユーザへまたは他のユーザから支払いを開始する。このことは、ユーザに個人識別番号（PIN）を入力し、ソフトウェアを起動するよう要求し得る。他のユーザのクライアントは次に、特に取引の価値が、他のユーザから最初のユーザへ転送される必要のある場合は、ユーザに取引を受け入れるか、断るかを促し得る。1人のユーザだけがソフトウェアをインストールされた場合は、ソフトウェアは、取引の一部として、または取引の先駆けとして、他のユーザのデバイス上に送信およびインストールされ得る。

30

【 0 0 7 9 】

例示的に、価値（例えば、システムソフトウェアに示されるように）を与えるユーザの口座残高は、取引が行われる場合に減少する。取引を終了することは、支払うユーザのクレジットカード、デビットカード、または請求されるシステムに価値を提供する他の方法を要求し得る（例えば、ユーザの口座残高があまりにも少ない場合）。取引は、ユーザの1人が、（例えば、同期サーバ106と同期セッション中に）取引をシステムに転送するまで終了され得ない。クライアントのソフトウェアは、ユーザが、取引の詳細（例えば、価値、他のユーザの識別子）で取引ログ中にセーブされるメモやコメントを作成することを可能にし得る。

40

【 0 0 8 0 】

直接的な価値交換を行う1方法において、互いを認証するため、および／またはシステムに、取引が有効であり、そして当事者の1人によってだまされたり、でっちあげられないことを証明するために、ユーザは、デジタル証明書（例えば、取引証明書）または

50

他のトーケンを交換し得る。

【0081】

図4は、モバイルクライアントデバイスを有する2人のユーザ間に行われる直接的な価値交換の1形式を示す。図4において、ユーザAは、自分のクライアントAからユーザBのクライアントBへ価値を電子的に転送する。取引は次に、取引当事者の1つによって、おそらく同期プロセス中にシステムサーバへ転送される。価値の量は（ユーザAが最大の価値を転送するよう公認されている場合）、ユーザAの口座から削除され、そしてユーザBの口座へ預けられる。ユーザAの口座残高が、要求された交換を完了するために、最低限のレベルを下回っている、または転送が必要である場合は、追加の資金または価値が、銀行、クレジットカード、A C H、またはユーザAに関連する他の金融源から回収され得る。ユーザのクライアントデバイスの両方が、新しい口座残高で更新される。10

【0082】

（価値交換の取消）

様々な状況において、ユーザは、価値交換を逆にしたり、取り消すことを望んだり、またはそうする必要があり得る。例えば、別の当事者と取引を行おうと試みる間に、ユーザは、不正確な識別子（存在しないメールアドレスまたは無効なメールアドレス、あるいは所望の当事者以外の人に関連する有効な電子メールアドレスなど）を提供し得る。本発明の1実施形態において、価値転送は、状況が保証されれば、行われ得ない。詳細には、交換が行われる必要がないと判定される場合は、システムは、価値転送を取り消し、価値転送を逆にし、価値転送の向きを変える（例えば、価値を第三の当事者へ転送する）、または何か別の方法で価値転送を無効にし得る。20

【0083】

ユーザによって提供される取引当事者の識別子（例えば、電子メールアドレス）が、使用不可能（例えば、無効）である場合は、ユーザは、転送を逆にするかまたは向きを変えるかどうかを特定し得、あるいはシステムが、債務不履行な活動を（例えば、価値をユーザに戻し）を適用し得る。この状況は、例えば、取引の他の当事者へ電子メール通知が配達不可能である（例えば、正しくないアドレス、当事者の電子メールサーバが利用不可能である）場合に生じ得る。

【0084】

当事者の識別子が、有効な識別子であるが、意図された当事者と関連しない場合は、状況を修正することがより難しくなり得る。例えば、取引が、すでに終了しており、そして価値が、正しくない当事者へ貸方を記入された場合は、取引は、逆にできないことがあり得る。開始ユーザは、もちろん、その当事者に接続し、そして価値を回収しようとする。30

【0085】

当事者の識別子が、有効であるが、意図した当事者と関連せず、そして取引がまだ終了していない場合は、ユーザは、価値を回収でき得る。ある期間（例えば、6ヶ月）が、清算していない取引を自動的に取り消しまたは逆にするために確立され得るし、またはその期間中にユーザが取引の取消を要求し得る。例えば、ユーザが、取引を開始し、そして6ヶ月後受領者がなお価値を請求していない場合は、システムは、自動的に転送を逆にするかまたは取り消し得る。しかし、その時間までに、開始ユーザは、取引が無効にされることを要求する必要があり得る。システムは、そうする前に正しくない当事者と連絡しようと試み得る。40

【0086】

（発明の1実施形態における新しいユーザを登録する）

前に説明したように、本発明の1実施形態において、ユーザは、システムと取引を開始または終了し得る前に価値交換システムに登録されていなければならない。このセクションは、新しいユーザを登録する1方法を説明する。その間、ユーザは、ユーザのクライアントデバイスがシステムおよび/または他のユーザのクライアントとインタラクトすることが可能なように構成されたソフトウェアをダウンロードし、またはそうでなければソフトウェアを受信し得る。50

【 0 0 8 7 】

例示的に、新しいユーザは、システムウェブサイトを通して、ウェブ使用可能電話を介して、通常のボイス電話連絡を介して、電子または通常のメールを介して、など多くの方法でシステムと登録し得る。ユーザが登録後システムを使用し得るアクセスのレベルまたは程度は、ユーザの登録方法、どれだけの情報が登録中に提供されるか、情報のうちどれだけが検証されるか、などに依存している。例えば、ユーザが提供した電話番号、電子メールアドレス、街路住所、および／または、他の情報が、すべて検証される場合は、ユーザは、より大きなシステムアクセスを与えられ、または、情報が正しくない、検証不可能、または提供されない場合よりも多くの価値が関連する取引を行い得る。

【 0 0 8 8 】

本発明の1実施形態において、可能性のある新しいユーザは、図1のシステムの通信（例えば、ウェブ）サーバ104に接続し、そして登録書式を完成する。好都合なことには、登録プロセスは、安全なモードで（例えば、SSL（Secure Sockets Layer）で）行われる。登録形式は、名前、住所（例えば、街路）、電話番号（例えば、日中の、夜間の、携帯の）などの個人情報を引き出し、または要求し得る。ユーザの口座に関連する情報も要求され得る。例えば、電子メールアドレス、社会保証番号、セキュリティ目的のために使用され得るいくつかの情報（例えば、母の旧姓）、などである。ユーザはまた、新しい口座のために使用されるパスワード、および／またはユーザのモバイルデバイス上にシステムソフトウェアを起動するためのPIN（個人識別番号）を入力するよう促され得る。例示的に、ユーザが、自分のモバイルデバイスを使用中に取引を開始または受け取りたい場合は、ユーザは、ソフトウェアが機能する前にPINを入力するよう要求され得る。

10

【 0 0 8 9 】

ユーザは、システムを使用するための具体的な条件に同意するよう要求され得る。システムは次に、ユーザによって提供される1つ以上の情報の部分を検証するよう試み得る。従って、確認の通信が、ユーザの街路住所、電子メールアドレス、モバイルデバイス、などへ送信され得る。確認の通信は、登録プロセスを完了または続けるために、ユーザがシステム（例えば、ウェブサーバ104）へ提供するよう命令されるコード（例えば、PIN）を含み得る。

20

【 0 0 9 0 】

新しいユーザが、スマート電話またはウェブ使用可能電話を使用して、システムと登録する本発明の1実施形態において、登録プロセスは、デバイスおよびそのようなデバイスの制限された表示手段に合うよう調整され得る。従って、登録情報（例えば、電話番号、名前）のいくつかは、電話または電話から受信される信号から派生し得る。そして、ユーザに要求された情報は、電話のキーパッドを通して入力されなければならない場合は、最小限に減らされ得る。

30

【 0 0 9 1 】

例示的に、システムユーザに関連する情報のいくつかは、一意であることを要求され得る。例えば、取引参加者がその電子メールアドレスによって識別され得る本発明の1実施形態において、システムは、アドレスとユーザとの間の1対1のマッピングを要求し得る。別の実施形態において、ユーザは、電話番号で識別可能であり得る。また、システムは、各電話番号を1人のユーザとのみ関連させることを可能にし得るが、内線番号は、1つの番号で到達可能な多くのユーザ間で区別するためにおそらく追加され得る。この制限の1つの理由は、価値交換参加者が、既知であるまたは既知であり得る通常の識別子を使用して、別の参加者を識別することを可能にすることである。しかし、1つの別の実施形態において、ユーザは、口座番号、またはシステムによってあるいはシステムのために生成された他の識別子によって認識され得る。別の実施形態において、いくつかのまたは全てのユーザは、多くの識別子によって識別され得る。この場合、多くのユーザは、特定の識別子（例えば、電子メールアドレス）に関連し得るが、またユーザを区別する他の識別子も有し得る。

40

50

【 0 0 9 2 】

ユーザがシステムと登録された後、ユーザは次に、資金を提供する最初の方法および／または債務不履行の方法を確立し得る。例えば、ユーザが価値を別の人へ転送する場合、または価値がユーザのシステム口座へ追加されなければならない他の時に、ユーザは、クレジットカード、銀行口座、デビットカード、または請求される他の価値源を識別し得る。ユーザのシステム活動上に置かれるシステムクレジットの量またはクレジットの制限は、ユーザが使用する価値転送の形式、ユーザの金融機関によって公認されたクレジットまたは価値転送のレベル、ユーザの個人または口座情報が検証される程度、などによって、一部または全体的に決定され得る。例えば、ユーザの街路住所が検証され得ない（例えば、ユーザが提供した住へ郵送されるコードを提示しない）、またはユーザのクレジットカードの住所が、その郵便の住所と適合しない、あるいはユーザのクレジットカードの制限が低い場合は、ユーザは、第一のシステム使用レベルに制限され得る。しかし、ユーザの個人または金融情報が検証され、および／または、そのクレジットカードの制限がかなり高い場合は、ユーザは、システムを通してはるかに多くの価値を転送することが可能であり得る。すなわち、ユーザがシステムに提供する信用、認証、検証またはセキュリティのレベルが、ユーザが与えられるシステム使用の量またはレベルに影響を及ぼし得る。10

【 0 0 9 3 】

ユーザが、貸方または借方情報を提示するまで、ユーザのシステム制限は、ゼロで維持され得、これはユーザが価値を他の当事者へ転送するよう公認されていないことを示す。しかし、ユーザは、ユーザが登録されるとすぐ、価値転送を受信でき得る。20

【 0 0 9 4 】

ユーザはまた、直接預け入れ、個人小切手、電子口座振替、などを通して、自分のシステム口座に価値を置くことができ得る。しかし、例示的に、これらの方法を介して提示される資金は、清算するまでは転送のために利用不可能である。ユーザは、価値を口座に預け入れる（そして口座から価値を回収する）多くの方法を選択し得るし、そしてそれらの方法を実施するために必要なすべての情報（例えば、銀行ルーティング、または口座番号）を提供するよう要求され得る。

【 0 0 9 5 】

ユーザが価値交換を行うことを可能にするよう構成されたソフトウェアをダウンロードおよびインストールし得る前に、登録は要求されてもよいし、されなくてもよい。ソフトウェアのダウンロードは、登録プロセスの一部であり得るし、または、ユーザが登録する前あるいは後で行われ得る。以下は、本発明の1実施形態によるソフトウェアのダウンロード／インストールプロセスの説明である。30

【 0 0 9 6 】

ソフトウェアを受信するために、ユーザはまず、クライアントデバイスを適切なサーバ（例えば、図1のシステムの通信サーバ104または同期サーバ106）に接続する。ユーザは、ソフトウェアをダウンロードする選択をし、正しいソフトウェアが提供されるために自分のデバイスを識別する必要があり得る。登録ユーザはまた、自分をシステムに識別し得る。この場合、システムは、ユーザがソフトウェアを最新にする必要があるかどうかを、（例えば、ユーザのデバイスで通信すること、またはデータベース102中の口座情報を参照することによって）自動的に判定し得る。40

【 0 0 9 7 】

ダウンロードされるソフトウェアは、システムにアクセスするユーザの通常のまたは予想される方法に依存し得る。例えば、ユーザがポータブルデバイスを使用する場合は、ダウンロードされるソフトウェアは、システムと直接通信しおよびインタラクトできるよう特定のデバイスに調整され得る。ポータブルデバイスが、システムと通信するために別のコンピュータシステム（例えば、デスクトップまたはワークステーション、本明細書中で「コンジット」と呼ばれるコンピュータ）とドッキングされるか、そうでなければ接続されなければならない切断可能なデバイスである場合は、ダウンロードされるソフトウェアは、切断可能なデバイスおよび／または他のコンピュータシステムのためのモジュールを含50

み得る。

【 0 0 9 8 】

適切なソフトウェアは次に、ユーザのデバイスにコピーされる。ユーザのデバイスの製造者またはベンダーによっておそらく提供される他のソフトウェアは、システムのソフトウェアを完全にインストールするために動作している必要があり得る。切断可能なポータブル計算機器について、第一のソフトウェアのモジュールが、コンジットコンピュータ上にインストールされ、その後デバイスは、デバイス上の第二のモジュールをインストールするためにドッキングされ得る。第一のモジュールは、ユーザのローカルに格納されたデータおよび情報を同期サーバ106と同期するよう構成され得、一方第二のモジュールは、切断された取引を行い、その取引をコンジットコンピュータへ通信するよう構成され得る。従って、取引が、切断中にクライアントと行われた後、コンジットコンピュータへ通信され、コンジットコンピュータは次に、同期サーバ106と同期する。クライアントのソフトウェアモジュールは「ウォレット」アプリケーションとみなされ得る。10

【 0 0 9 9 】

例示的に、新しいソフトウェアがダウンロードされた後、およびユーザがポータブルデバイスを使用して価値を別の人へ転送できる前に、ユーザはシステムに認証される必要がある。従って、システムの1実施形態において、ユーザは、ユーザ名（例えば、口座名、電子メールアドレス、または他のシステム識別子）、およびパスワードを入力する。コンジットは、それを検証のためシステム（例えば、同期サーバ106、セキュリティサーバ110）へ送信する。ユーザが検証された場合、1対の暗号鍵が（例えば、コンジットコンピュータまたはセキュリティサーバ110によって）生成される。説明された本実施形態において、ユーザのコンジットコンピュータは、鍵の対を生成し、公開鍵を署名するためにシステムへ送信する。署名された鍵は、暗号化された形式で（例えば、ユーザのPINで暗号化され）返送され得る。例示的に、秘密鍵および署名された公開鍵の両方が次に、ユーザのポータブルデバイス上にのみ（すなわち、コンジット上ではなく）格納される。20

【 0 1 0 0 】

ユーザが新しいソフトウェア（新規なバージョン）をインストールする場合、未清算の取引が自動的に（同期サーバ106で）清算され、またはアーカイブされ得る。ユーザが新しいソフトウェアを異なるデバイス上にインストールする場合は、元のデバイス上のディジタル証明書は、無効にされ得る。30

【 0 1 0 1 】

本発明の実施形態の上述の説明は、例示および説明だけの目的で与えられた。説明は、網羅的である意図はなく、または開示された形式に本発明を制限する意図はない。従って、上記の開示は、本発明を制限する意図はなく、本発明の範囲は、添付の請求によって規定される。

【図面の簡単な説明】

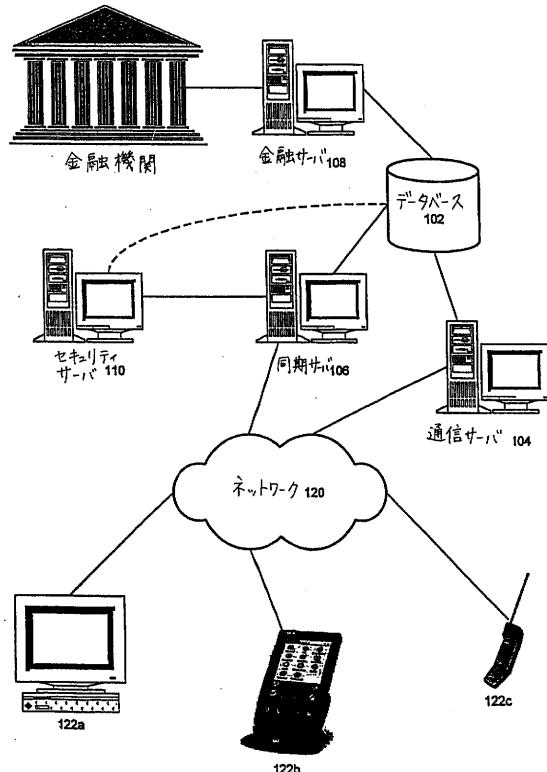
【図1】 図1は、本発明の1実施形態による価値交換取引を行うためのシステムを示すブロック図である。

【図2】 図2は、本発明の1実施形態による価値交換取引を行う1方法を示すフローチャートである。40

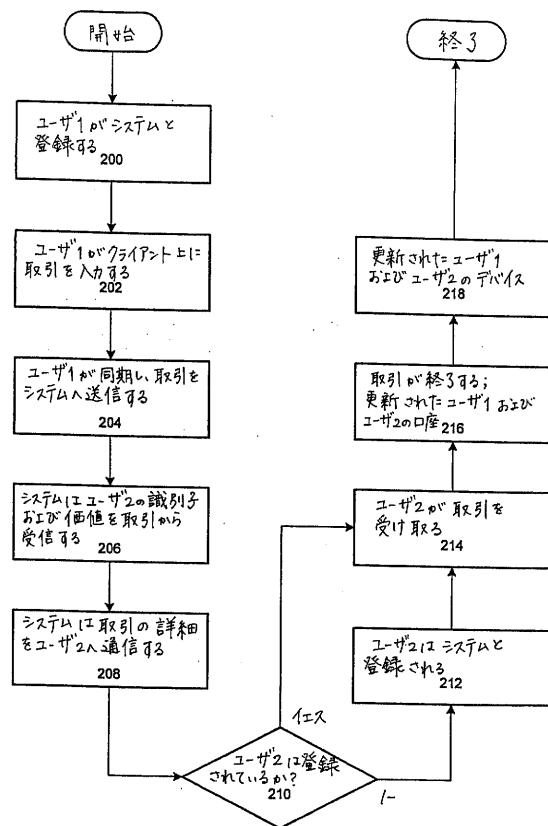
【図3】 図3は、本発明の1実施形態による、第一のユーザのモバイルクライアントデバイスで行われる第一のユーザから第二のユーザへの間接的な価値交換取引の1形態を示す。

【図4】 図4は、本発明の1実施形態による、ユーザのモバイルクライアントデバイスで行われる第一のユーザから第二のユーザへの直接的な価値交換の1形態を示す。

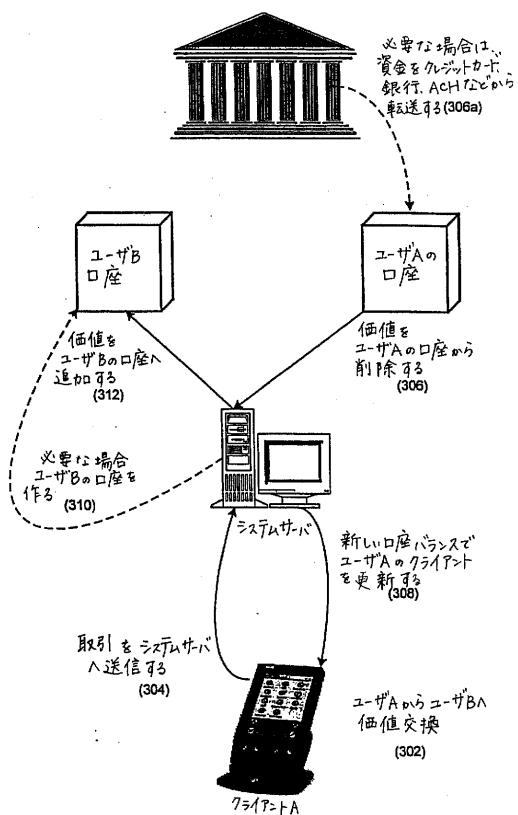
【図1】



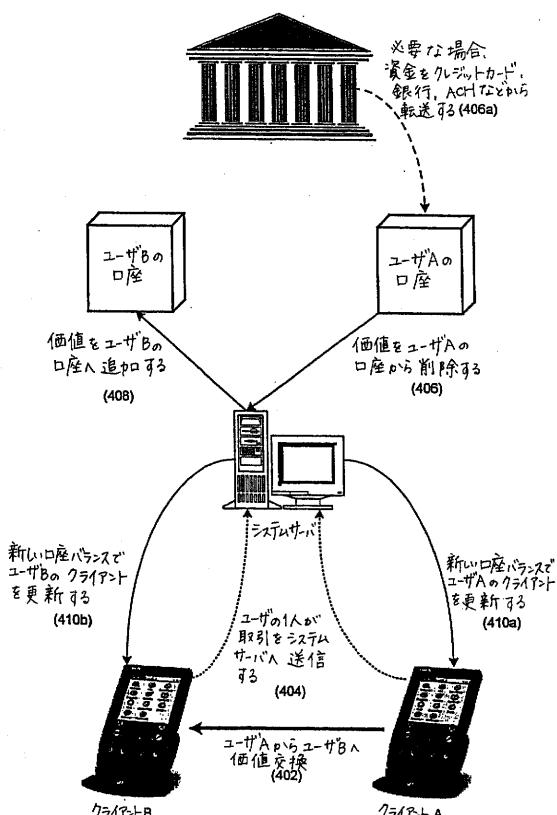
【図2】



【図3】



【図4】



フロントページの続き

(31)優先権主張番号 60/172,311

(32)優先日 平成11年12月17日(1999.12.17)

(33)優先権主張国 米国(US)

(72)発明者 ノセック , リューク

アメリカ合衆国 カリフォルニア 94306 , パロ アルト , グラント アベニュー ナン
バーピィ 469

(72)発明者 ジエル , ピーター

アメリカ合衆国 カリフォルニア 94304 , パロ アルト , オーク クリーク ドライブ
ナンバー 416 1788

(72)発明者 バニスター , スコット アラン

アメリカ合衆国 カリフォルニア 94025 , メンロ パーク , ベイ ローレル ドライブ
1480

合議体

審判長 清田 健一

審判官 松尾 俊介

審判官 須田 勝巳

(56)参考文献 國際公開第97/02539(WO,A1)

特開平09-73496(JP,A)

特開平09-185658(JP,A)

特開平10-334145(JP,A)

特開平11-15927(JP,A)

國際公開第97/22074(WO,A1)

特開平07-249073(JP,A)

特開平05-233657(JP,A)

特開平07-336286(JP,A)

特開平07-244734(JP,A)

特開平09-128468(JP,A)

特開平07-131527(JP,A)

特開平10-307885(JP,A)

米国特許第5963647(US,A)

米国特許第5677955(US,A)

米国特許第6029151(US,A)

米国特許第6039250(US,A)

(58)調査した分野(Int.Cl., DB名)

G06Q10/00-50/00