(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6925346号
(P6925346)
(45)発行日　令和3年8月25日(2021.8.25)　(24)登録日　令和3年8月5日(2021.8.5)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 675Z
G09C 1/00 (2006.01)　　H04L 9/00 675B
　　G09C 1/00 640D

請求項の数 26　(全 40 頁)

(21)出願番号　特願2018-539398(P2018-539398)
(86)(22)出願日　平成29年2月14日(2017.2.14)
(65)公表番号　特表2019-506075(P2019-506075A)
(43)公表日　平成31年2月28日(2019.2.28)
(86)国際出願番号　PCT/IB2017/050818
(87)国際公開番号　WO2017/145003
(87)国際公開日　平成29年8月31日(2017.8.31)
審査請求日　令和2年1月15日(2020.1.15)
(31)優先権主張番号　1603123.9
(32)優先日　平成28年2月23日(2016.2.23)
(33)優先権主張国・地域又は機関
英国(GB)
(31)優先権主張番号　1603125.4
(32)優先日　平成28年2月23日(2016.2.23)
(33)優先権主張国・地域又は機関
英国(GB)

(73)特許権者　318001991
エヌチェーン　ホールディングス　リミテッド
NCHAIN HOLDINGS LIMITED
アンティグア・バーブーダ、　セントジョンズ、　４４　チャーチ　ストリート、　フィッツジェラルド　ハウス
Fitzgerald House, 44 Church Street, St. John's, Antigua and Barbuda (AG)
(74)代理人　100107766
弁理士　伊東　忠重

最終頁に続く

(54)【発明の名称】ブロックチェーンベースのトークナイゼーションを用いた交換

(57)【特許請求の範囲】
【請求項１】
第１ユーザと第２ユーザとの間でエンティティの交換を実行するためのコンピュータで実施される方法であって、
第１コンピュータによって、出力（ＵＴＸＯ）を含む第１インビテーショントランザクション（Ｔｘ）を生成するステップ、を含み、
前記第１インビテーショントランザクションは、
ｉ）暗号化され、電子的に移転可能なデジタルアセット、および、
ｉｉ）第１スクリプトの第１スクリプトハッシュであり、
メタデータの第１セットであり、
－交換されるエンティティの指示、および、
－前記交換のための条件の第１セット、
を含む、メタデータの第１セットと、
前記第１ユーザに関連付けられた第１ユーザの公開鍵（Ｐ１Ａ）と、
を含む、第１スクリプトの第１スクリプトハッシュ、
と関連付けられている、
方法。
【請求項２】
前記方法は、さらに、
前記第１インビテーショントランザクションを生成する前に、第２コンピュータによっ

て、前記交換を実行するための第１インビテーションを、第１ユーザから受け取るステップであり、
　前記第１インビテーションは、インビテーションと関連付けられた前記メタデータの第１セットを含み、
　前記メタデータの第１セットは、交換されるエンティティの指示と、前記交換のための条件の第１セットとを含む、ステップと、
　前記第１スクリプトを生成するステップであり、該第１スクリプトは、
　前記メタデータの第１セットと、
　前記第１ユーザに関連付けられた第１ユーザの公開鍵（Ｐ１Ａ）であり、前記第１ユーザの公開鍵（Ｐ１Ａ）は第１ユーザの秘密鍵（Ｖ１Ａ）との暗号ペアである、第１ユーザの公開鍵と、
　第１の第三者と関連付けられた第１の第三者公開鍵（Ｐ１Ｔ）であり、前記第１の第三者公開鍵（Ｐ１Ｔ）は第１の第三者秘密鍵（Ｖ１Ｔ）との暗号ペアである、第１の第三者公開鍵と、
　を含む、ステップと、
　前記第１スクリプトハッシュを生成するために前記第１スクリプトをハッシュ化するステップと、
　前記第１スクリプトおよび前記第１スクリプトハッシュを、第１ネットワークを介して送付するステップと、
　ピアツーピア（Ｐ２Ｐ）分散型台帳に包含するために、前記第１インビテーショントランザクションを、第２ネットワークを介して送付するステップであり、
　前記第１インビテーショントランザクションは、移転されることになる、暗号化され電子的に移転可能なデジタルアセットの第１量の指示と、前記第１スクリプトハッシュとを含む、ステップと、
　を含む、請求項１に記載の方法。
【請求項３】
　前記第１ネットワークを介して送付するステップは、
　第１ネットワークにわたり分散された分散ハッシュテーブル（ＤＨＴ）において前記第１スクリプトおよび前記第１スクリプトハッシュを発行するステップ、を含む、
　請求項２に記載の方法。
【請求項４】
　前記方法は、さらに、
　第２ユーザからの交換を実行するための第２インビテーションを、通信ネットワークを介して受け取るステップであり、
　前記第２インビテーションは、インビテーションに関連付けされたメタデータの第２セットを含み、
　前記メタデータの第２セットは、交換されるエンティティの指示および前記交換のための条件の第２セットを含み、
　前記条件の第２セットのうち１つまたはそれ以上は、前記条件の第１セットのうち１つまたはそれ以上と一致している、ステップと、
　第２スクリプトを生成するステップであり、該第２スクリプトは、
　前記メタデータの第２セットと、
　前記第２ユーザに関連付けられた第２ユーザの公開鍵（Ｐ２Ａ）であり、前記第２ユーザの公開鍵（Ｐ２Ａ）は第２ユーザの秘密鍵（Ｖ２Ａ）との暗号ペアである、第２ユーザの公開鍵と、
　第２の第三者と関連付けられた第２の第三者公開鍵（Ｐ２Ｔ）であり、前記第２の第三者公開鍵（Ｐ２Ｔ）は第２の第三者秘密鍵（Ｖ２Ｔ）との暗号ペアである、第２の第三者公開鍵と、
　を含む、ステップと、
　第２スクリプトハッシュを生成するために前記第２スクリプトをハッシュ化するステッ

プと、
前記Ｐ２Ｐ分散型台帳に包含するために、第２インビテーショントランザクションを、前記第２ネットワークにおいて、ブロードキャストするステップであり、
前記第２インビテーショントランザクションは、移転されることになる、暗号化され電子的に移転可能なデジタルアセットの第２量の指示と、前記第２スクリプトハッシュとを含む、ステップと、
を含む、請求項２に記載の方法。
【請求項５】
前記方法は、さらに、
前記第２スクリプトと前記第２スクリプトハッシュとを、第３ネットワークにおいて、送付するステップ、
を含む、請求項４に記載の方法。
【請求項６】
前記第１ネットワークと前記第３ネットワークは同一のネットワークであり、かつ、
前記第３ネットワークにおいて、送付する前記ステップは、前記ＤＨＴにおいて前記第２スクリプトと前記第２スクリプトハッシュとを発行するステップ、を含む、
請求項５に記載の方法。
【請求項７】
前記方法は、さらに、
前記Ｐ２Ｐ分散型台帳に包含するために、第１交換トランザクションを生成するステップであり、該第１交換トランザクションは、
前記第１スクリプトと、
前記第１ユーザの秘密鍵（Ｖ１Ａ）と、
前記第１の第三者秘密鍵（Ｖ１Ｔ）と、
前記第１インビテーショントランザクションの出力から提供される第１入力と、
前記第２ユーザに対して移転されることになる第１エンティティの第１量を指示する第１出力と、
を含む、ステップと、
前記第１交換トランザクションを、前記第２ネットワークにおいて、ブロードキャストするステップと、
を含む、請求項４乃至６いずれか一項に記載の方法。
【請求項８】
前記方法は、さらに、
前記Ｐ２Ｐ分散型台帳に包含するために、第２交換トランザクションを生成するステップであり、該第２交換トランザクションは、
前記第２スクリプトと、
前記第２ユーザの秘密鍵（Ｖ２Ａ）と、
前記第２の第三者秘密鍵（Ｖ２Ｔ）と、
前記第２インビテーショントランザクションの出力から提供される第２入力と、
前記第１ユーザに対して移転されることになる第２エンティティの第２量を指示する第２出力と、
を含む、ステップと、
前記第２交換トランザクションを、前記第２ネットワークにおいて、ブロードキャストするステップと、
を含む、請求項７に記載の方法。
【請求項９】
前記方法は、さらに、
前記Ｐ２Ｐ分散型台帳に包含するために、第１交換トランザクションを生成するステップであり、該第１交換トランザクションは、
前記第１スクリプトと、

前記第１ユーザの秘密鍵（Ｖ１Ａ）と、
前記第１の第三者秘密鍵（Ｖ１Ｔ）と、
前記第２スクリプトと、
前記第２ユーザの秘密鍵（Ｖ２Ａ）と、
前記第２の第三者秘密鍵（Ｖ２Ｔ）と、
前記第１インビテーショントランザクションの出力から提供される第１入力と、
前記第２インビテーショントランザクションの出力から提供される第２入力と、
前記第２ユーザに対して移転されることになる第１エンティティの第１量を指示する第１出力と、
前記第１ユーザに対して移転されることになる第２エンティティの第２量を指示する第２出力と、
を含む、ステップと、
前記第１交換トランザクションを、前記第２ネットワークにおいて、ブロードキャストするステップと、
を含む、請求項４乃至６いずれか一項に記載の方法。
【請求項１０】
前記第１交換トランザクションを生成するステップは、
前記第１ユーザの秘密鍵（Ｖ１Ａ）を用いて署名するために、前記第１ユーザに対して、前記第１スクリプトを送付するステップと、
前記第１ユーザから、前記第１ユーザの秘密鍵（Ｖ１Ａ）を用いて署名された前記第１スクリプトを受け取るステップと、
前記第１の第三者秘密鍵（Ｖ１Ｔ）を用いて署名するために、署名された前記第１スクリプトを送付するステップと、
前記第１の第三者から、前記第１の第三者秘密鍵（Ｖ１Ｔ）を用いて署名された前記第１スクリプトを受け取るステップと、
を含む、請求項７または９に記載の方法。
【請求項１１】
前記第１交換トランザクションを生成するステップは、
前記第２ユーザの秘密鍵（Ｖ２Ａ）を用いて署名するために、前記第２ユーザに対して、前記第１スクリプトを送付するステップと、
前記第２ユーザから、前記第２ユーザの秘密鍵（Ｖ２Ａ）を用いて署名された前記第１スクリプトを受け取るステップと、
前記第２の第三者秘密鍵（Ｖ２Ｔ）を用いて署名するために、前記第２の第三者に対して、前記第１スクリプトを送付するステップと、
前記第２の第三者から、前記第２の第三者秘密鍵（Ｖ２Ｔ）を用いて署名された前記第１スクリプトを受け取るステップと、
を含む、請求項９に従属する場合の請求項１０に記載の方法。
【請求項１２】
前記第２交換トランザクションを生成するステップは、
前記第２ユーザの秘密鍵（Ｖ２Ａ）を用いて署名するために、前記第２ユーザに対して、前記第２スクリプトを送付するステップと、
前記第２ユーザから、前記第２ユーザの秘密鍵（Ｖ２Ａ）を用いて署名された前記第２スクリプトを受け取るステップと、
前記第２の第三者秘密鍵（Ｖ２Ｔ）を用いて署名するために、前記第２の第三者に対して、前記第２スクリプトを送付するステップと、
前記第２の第三者から、前記第２の第三者秘密鍵（Ｖ２Ｔ）を用いて署名された前記第２スクリプトを受け取るステップと、
を含む、請求項８に記載の方法。
【請求項１３】
前記方法は、さらに、

前記第１交換トランザクション及び／又は前記第２交換トランザクションを生成するステップまたはブロードキャストするステップの前に、前記第１ユーザと前記第２ユーザのうち１人またはそれ以上に対して交換を受諾するためのプロンプトを送付するステップ、を含む、
請求項７乃至１２いずれか一項に記載の方法。
【請求項１４】
前記第１ネットワークを介して送付するステップは、
前記第１スクリプトと前記第１スクリプトハッシュとを前記第２ユーザに対して送付するステップ、を含む、
請求項４乃至１３いずれか一項に記載の方法。
【請求項１５】
前記Ｐ２Ｐ分散型台帳は、ビットコインブロックチェーンである、
請求項１乃至１４いずれか一項に記載の方法。
【請求項１６】
前記第１の第三者は、エスクローサービスプロバイダまたはトークン発行者であり、かつ／あるいは、前記第２の第三者は、エスクローサービスプロバイダまたはトークン発行者である、
請求項１乃至１５いずれか一項に記載の方法。
【請求項１７】
前記方法は、さらに、
前記第１の第三者に対して前記第１の第三者の公開鍵についてリクエストを送付するステップと、
前記第１の第三者から前記第１の第三者の公開鍵を受け取るステップと、
を含む、請求項１乃至１６いずれか一項に記載の方法。
【請求項１８】
前記方法は、さらに、
前記第２の第三者に対して前記第２の第三者の公開鍵についてリクエストを送付するステップと、
前記第２の第三者から前記第２の第三者の公開鍵を受け取るステップと、
を含む、請求項１乃至１７いずれか一項に記載の方法。
【請求項１９】
前記第１インビテーショントランザクション、前記第２インビテーショントランザクション、前記第１交換トランザクション、および前記第２交換トランザクションのうち１つまたはそれ以上は、ペイツースクリプトハッシュ（Ｐ２ＳＨ）トランザクションである、
請求項１乃至１８いずれか一項に記載の方法。
【請求項２０】
第１スクリプトハッシュおよび第２スクリプトハッシュのうち１つまたはそれ以上は、ベース５８（Ｂａｓｅ５８）で符号化されている、
請求項１乃至１９いずれか一項に記載の方法。
【請求項２１】
前記第１エンティティ及び／又は前記第２エンティティは、
ａ）ビットコイン、
ｂ）コントラクト、
ｃ）商品、
ｄ）サービス、
のうちの１つである、
請求項１乃至２０いずれか一項に記載の方法。
【請求項２２】
前記コントラクトは、
ａ）不換通貨、

ｂ）不動産権利書、
ｃ）チケット、
ｄ）商品、
ｅ）サービス、
のうちの１つまたはそれ以上に対するものである、
請求項２１に記載の方法。
【請求項２３】
前記条件の第１セット及び／又は前記条件の第２セットは、
ａ）前記交換に関する１つまたはそれ以上の価格における１つまたはそれ以上の限度範囲、
ｂ）交換レート、
ｃ）前記第１インビテーションの遂行に対する締め切り、
ｄ）前記交換を行うための地理的領域における制限、
のうち１つまたはそれ以上を含む、
請求項１乃至２１いずれか一項に記載の方法。
【請求項２４】
前記メタデータの第１セット及び／又は前記メタデータの第２セットは、引き換えスクリプトにおいて提供される、
請求項１乃至２１いずれか一項に記載の方法。
【請求項２５】
前記メタデータの第１セット及び／又は前記メタデータの第２セットは、暗号鍵のためのロケーションとしてブロックチェーンプロトコルにおいて指定されたロケーションにおいてスクリプトの中で提供される、
請求項１乃至２１いずれか一項に記載の方法。
【請求項２６】
実行されると、請求項１乃至２３いずれか一項に記載の方法を実行するように動作可能であるインタラクションを保管しているコンピュータで読取り可能な記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、分散型、ピアツーピア台帳（peer-to-peer　ledgers）に関し、特には、ブロックチェーン技術に関する。本発明は、また、部分的にトークナイゼーション（tokenisation）とセキュリティ技術、および、ブロックチェーンを介してエンティティ及び／又はエンティティの所有権を移転するためのセキュア（secure）なメカニズム、に関する。本発明は、ブロックチェーンにわたり異なる当事者間でセキュアなトランザクションを実行する方法を含み得る。
【背景技術】
【０００２】
ブロックチェーンは、ブロック、次にトランザクションを構成するもの、で構成されたコンピュータベースの分権的な、分散システムとして実装されるピアツーピアの電子台帳である。各トランザクションは、ブロックチェーンシステムにおける参加者間のデジタルアセットの制御の移転（transfer）を符号化（encode）するデータ構造であり、そして、少なくとも１つの入力と少なくとも１つの出力を含んでいる。各ブロックは、前のブロックのハッシュを含んでおり、ブロックは一緒に連鎖されて（chained）、その最初からブロックチェーンに対して書き込まれてきた全てのトランザクションに係る永続的で、変更不可能なレコードを作成する。トランザクションは、入力と出力の中に埋め込まれた（embedded）スクリプト（scripts）として知られている小さいプログラムを含んでおり、トランザクションの出力が、どのように又は誰によってアクセスされ得るかを特定している。ビットコイン（Bitcoin）プラットフォームにおいて、これらのスクリプトはスタックベース（stack-based）のスクリプト言語を使用して記述されている。

【０００３】
トランザクション（Tx）がブロックチェーンに対して書き込まれるためには、トランザクションが「検証される（”validated”）」必要がある。ネットワークノード（マイナ（miner））は、各トランザクションが有効であることを保証するための作業を実行し、無効なトランザクションはネットワークから拒否されている。ノード上にインストールされたソフトウェアクライアントは、ロックおよびロック解除スクリプト（locking and unlocking scripts）を実行することによって、未使用トランザクション（unspent transaction、UTXO）においてこの検証作業を実施する。ロックおよびロック解除スクリプトの実行が真（TRUE）であると評価された場合に、トランザクションは有効（valid）であり、そして、トランザクションがブロックチェーンに対して書き込まれる。従って、トランザクションがブロックチェーンに対して書き込まれるためには、ｉ）トランザクションを受け取る最初のノードによって検証される必要があり、－トランザクションが検証された場合に、ノードはネットワークにおける他のノードに対してトランザクションをリレーし（relay）、そして、ｉｉ）マイナによって構築された新しいブロックに対して追加され、かつ、ｉｉｉ）採掘（mined）、すなわち過去のトランザクションの公開台帳に対して追加されることを要する。

【０００４】
ブロックチェーン技術は、仮想通貨（cryptocurrency）実装の使用について最も広く知られているが、デジタル起業家（entrepreneur）は、新しいシステムを実施するために、ビットコインが基づいている暗号化セキュリティシステムとブロックチェーンに保管できるデータと両方の使用について探求を始めている。ブロックチェーンが、仮想通貨の領域に限定されない自動化されたタスクおよびプロセスについて使用され得るとすれば、非常に有利であろう。そうしたソリューションは、ブロックチェーンの利点（例えば、イベントの永続的で、改ざん防止（tamper proof）な記録、分散化処理、等）を利用することができるだろうし、一方で、それらのアプリケーションにおいてはより汎用性（versatile）がある。

【０００５】
現在の研究の１つの領域は、「スマートコントラクト（”smart contracts”）」の実装のためにブロックチェーンを使用することである。これらは、マシンで読取り可能な契約または同意の条件（condition）の実行を自動化するようにデザインされたコンピュータプログラムである。自然言語で書かれるであろう従来の契約とは異なり、スマートコントラクトは、結果を生成するために入力を処理することができるルールを含むマシンで実行可能なプログラムであり、次いで、その結果に応じて実行されるべきアクションを生じさせることができる。

【０００６】
ブロックチェーン関連の別の関心領域は、ブロックチェーンを介して現実世界のエンティティ（real-world entities）を表現し、かつ、移転するための「トークン（”tokens”）」（または「カラードコイン（”coloured coin”）」）の使用である。潜在的に機密扱い又は秘密のアイテムは、識別可能（discernable）な意味または価値を持たないトークンによって表すことができる。トークンは、従って、識別子（identifier）として機能し、現実世界のアイテムをブロックチェーンから参照できるようにする。トークナイゼーション（tokenisation）技術は、セキュリティ、匿名性、およびクロスプラットフォームのコンプライアンスが重要である多くの異なるタイプのコンテキスト（contexts）に関して使用され得る。そうしたアプリケーションの領域の１つは金融用途（financial applications）であるが、本発明は金融取引に関する使用について限定されるものではない。

【０００７】
この文書においては、我々は、電子、コンピュータベース、分散型台帳に係る全ての形態を含むように、用語「ブロックチェーン（”blockchain”）」を使用している。これらは、コンセンサスベースのブロックチェーンおよびトランザクションチェーン技術に限定

されるわけではないが、パーミッションと非パーミッション台帳（permissioned and un-permissioned ledgers）、共有台帳、および、その変形を含んでいる。ビットコイン技術の最も広く知られているアプリケーションは、ビットコイン台帳（Bitcoin ledger）であるが、他のブロックチェーン実装がオファーされ、かつ、開発されてきている。ここにおいては、便宜および説明目的のためにビットコインが参照され得るが、本発明は、ビットコインのブロックチェーンを伴う使用に限定されるものではなく、かつ、代替的なブロックチェーン実装およびプロトコルも本発明の範囲内に在ることに留意すべきである。

【発明の概要】

【０００８】

本発明は、添付の請求項において定義されるものである。

【０００９】

本発明は、ブロックチェーンを介したアセットのセキュアな制御（control）、及び／又は、移転（transfer）、もしくは交換（exchange）のためのソリューションを提供することができる。ここにおいて、用語「エンティティ（”entity”）」は、「アセット（”asset”）」と互換的に使用されてよい。追加的または代替的に、本発明は、アセットの所有権（ownership）の制御及び／又は移転を可能にし得る。これは、スマートコントラクトといった、デジタルまたは仮想アセット、もしくは、現実世界／物理的なアセットであってよい。アセットは、ライセンスといった権利または使用権、もしくは、あるタイプのプロパティに関するある種の権利であってよい。本発明は、この制御または移転を促進するために、トークナイゼーション技術を使用することができる。本発明は、暗号鍵（cryptographic keys）の使用を組み込んで、移転／交換がセキュアな方法で実行されることを可能にし得る。一方で、根底にあるブロックチェーンプロトコルのあらゆる変更も必要としていない。本発明は、ブロックチェーントランザクション（Tx）に関連するスクリプトの中にメタデータを埋め込むための技術を使用することができる。

【００１０】

本発明は、特に、電子的移転のためのメモリ使用の強化された最適化、ハッシュ技術の使用を通じて改善されたセキュリティおよびデータ完全性、信頼できる第三者の必要性を排除することを通じて改善されたセキュリティ、および、強化されたデータの匿名性、を提供する。本発明は、また、異種または別個の当事者が、本発明によって提供される新規な方法及び／又はアーキテクチャを介して、互いを識別し、かつ／あるいは、データ交換することを可能にする改善された通信メカニズムも提供することができる。この利点のリストは、限定的または網羅的ではない。

【００１１】

本発明は、種々の別個で、かつ、分離したコンピュータベースのリソースに係る相互作用（interaction）および相互通信（inter-communication）を必要とし得る。１つまたはそれ以上のユーザデバイス、および、ブロックチェーン関連のソフトウェアおよびプロトコルを実行するように構成されたコンピューティングノードを含む、分散コンピュータシステム（ブロックチェーン）、といったものである。

【００１２】

本発明は、エンティティの交換を実行するコンピュータ実装方法を提供することができる。交換は、第１ユーザと第２ユーザとの間で行われてよく、コンピュータネットワークを介して行われる交換であってよい。ネットワークは、ブロックチェーン実装のネットワークであってよい。用語「ユーザ（”user”）」は、人間のユーザまたはコンピュータベースのリソースを参照し得る。本発明は、交換、もしくは、２つまたはそれ以上のエンティティを制御するための交換制御方法を提供することができる。それは、デジタルエンティティの交換のためのトークナイゼーション方法を提供することができる。本発明は、ブロックチェーン実装方法として説明することができる。

本方法は、出力（ＵＴＸＯ）を含む第１インビテーション（Ｔｘ）を生成するステップを

含んでよく、第１インビテーションは、
ｉ）仮想通貨、例えばビットコイン、の量、および、
ｉｉ）スクリプトのハッシュであり、スクリプトは、
－交換されるエンティティの指示、および、
－交換のための条件の第１セット、
を含む、メタデータの第１セットと、
第１ユーザに関連付けられた公開鍵（Ｐ１Ａ）と、
を含む、スクリプトのハッシュ、
と関連付けられている。
スクリプトは、また、第三者と関連付けされた暗号鍵を含んでよい。

【００１３】
追加的または代替的に、本方法は、以下のステップを含んでよい。
交換を実行するための第１インビテーションを、第１ユーザから受け取るステップであり、第１インビテーションは、インビテーションと関連付けられた前記メタデータの第１セットを含み、ここで、メタデータの第１セットは、交換されるエンティティの指示と、交換のための条件の第１セットとを含む、ステップ、及び／又は、
第１スクリプトを生成するステップであり、第１スクリプトは、メタデータの第１セットと、第１ユーザに関連付けられた第１ユーザの公開鍵（Ｐ１Ａ）であり、ここで第１ユーザの公開鍵（Ｐ１Ａ）は、第１ユーザの秘密鍵（Ｖ１Ａ）との暗号ペアである、第１ユーザの公開鍵と、第１の第三者と関連付けられた第１の第三者公開鍵（Ｐ１Ｔ）であり、ここで第１の第三者公開鍵（Ｐ１Ｔ）は、第１の第三者秘密鍵（Ｖ１Ｔ）との暗号ペアである、第１の第三者公開鍵とを含む、ステップ、及び／又は、
第１スクリプトハッシュを生成するために第１スクリプトをハッシュ化するステップ、第１スクリプトおよび第１スクリプトハッシュを第１ネットワークを介して送付するステップ、及び／又は、
ピアツーピア（Ｐ２Ｐ）分散型台帳に包含するために、第１インビテーショントランザクションを、第２ネットワークを介して送付するステップであり、第１インビテーショントランザクションは、移転されることになる、暗号化され電子的に移転可能なデジタルアセットの第１量の指示と、第１スクリプトハッシュとを含む、ステップ。

従って、（引き換え）スクリプトのハッシュは、ブロックチェーントランザクションの中で提供されてよく、または、ブロックチェーントランザクションに関連付けられてよい。これは、ビットコインプロトコルに従ったP2SHトランザクション、または、別のブロックチェーンプロトコルにおける別の機能的に同等なトランザクションタイプであってよい。スクリプトのハッシュは、ハッシュテーブルまたは他のストレージリソースに対するルックアップキーとして機能し得る。このストレージリソースは、インビテーションのパブリックドメインリポジトリであってよい。ストレージリソースは、ルックアップキー（すなわち、ハッシュ）、および、組み合わせて、インビテーションを定義するメタデータからの全てのフィールドを含むことができる。ルックアップキーは、レコードの残りのハッシュ、すなわち連結されたメタデータ値のハッシュであってよい。好ましい実施形態において、メタデータは、トークンと関連付けられたコントラクトのロケーションに対するポインタまたは他の参照を含んでよい。コントラクトは、別個のストレージリソースの中に格納されてよい。インビテーション（ストレージリソースにおけるメタデータによって定義される）は、ハッシュを介してブロックチェーントランザクションに対してリンクされてよい。

本発明によって多くの利点が提供され、そのうちのいくつかがここで説明される。最初に、交換に関する情報は分散型台帳においてセキュアに埋め込まれたメタデータの中に含まれるため、交換は、ピアツーピアベースでセキュアに実行され、それによって信頼できる第三者を不要としている。このことは、次に、サービスプロバイダといった任意の第三者

によって保持される交換に対する両当事者に関して大量の機密情報が必要となることを回避し、次に、危険にさらされている第三者のセキュリティに関するリスクを回避する。この利点は、トランザクションの匿名性を維持しながらも、また提供されている。第１スクリプトはハッシュされているので、スクリプトの対応するハッシュ値における変化を伴うことなく、メタデータの値を変更することは実行不可能な程度に難しいだろう。このことは、また、トランザクションの条件が当事者によって検証できるようにする。それらは公に利用可能な分散型台帳においてロックされているからであり、それはトランザクションの整合性を信頼できるものにしている。利点は、また、第１メタデータを第１スクリプトにおいて公開鍵のために利用可能な１つまたはそれ以上の場所に埋め込むことができることも提供し、進行をブロックするのとは対照的に、それによって、メタデータを処理するのに適していないノードが別のノードに対してスクリプトを単に送付することを可能している。このことは、次に、関連するトランザクションの計算効率を改善する。さらなる利点が提供され、制御データをメタデータの中に組み込むことができる。例えば、会合場所に対するチケット、もしくは、旅行チケットまたバウチャーを表すトークンの場合の、バリアに対するアクセスコードである。メタデータは、また、ポインタが示す交換の詳細のオフブロックリポジトリ（off-block repository）を含むこともでき、それによって、関連トランザクションの処理に使用されるメモリ及び／又は処理リソースを少なくすることができる。なおもさらなる、トークンを分割することができるという別の利点が提供され、２つまたはそれ以上のトランザクション出力を可能にしている。その各々は、トークン化、または、非トークン化された電子的に移転可能なデジタルアセットに関連し得る。

【００１４】

第１ネットワークを介して送付するステップは、第１ネットワークにわたり分散された分散ハッシュテーブル（distributed hash table、DHT）上で第１スクリプトと第１スクリプトハッシュを発行するステップを含んでよい。

【００１５】

P2P分散型台帳は、ビットコインブロックチェーンであってよい。代替的に、P2P分散型台帳は、別の仮想通貨台帳またはブロックチェーンであってよい。

【００１６】

好ましくは、本方法は、さらに、

第２ユーザからの交換を実行するための第２インビテーションを、通信ネットワークを介して受け取るステップであり、第２インビテーションはインビテーションに関連付けされたメタデータの第２セットを含み、ここでメタデータの第２セットは、交換されるエンティティの指示および交換のための条件の第２セットを含み、条件の第２セットのうち１つまたはそれ以上は条件の第１セットのうち１つまたはそれ以上と一致している、ステップと、

第２スクリプトを生成するステップであり、第２スクリプトは、メタデータの第２セットと、第２ユーザに関連付けられた第２ユーザの公開鍵（Ｐ２Ａ）であり、ここで第２ユーザの公開鍵（Ｐ２Ａ）は第２ユーザの秘密鍵（Ｖ２Ａ）との暗号ペアである、第２ユーザの公開鍵と、第２の第三者と関連付けられた第２の第三者公開鍵（Ｐ２Ｔ）であり、ここで第２の第三者公開鍵（Ｐ２Ｔ）は第２の第三者秘密鍵（Ｖ２Ｔ）との暗号ペアである、第２の第三者公開鍵とを含む、ステップと、

第２スクリプトハッシュを生成するために第２スクリプトをハッシュ化するステップと、Ｐ２Ｐ分散型台帳に包含するために、第２インビテーショントランザクションを、第２ネットワークにおいて、ブロードキャストするステップであり、第２インビテーショントランザクションは、移転されることになる、暗号化され電子的に移転可能なデジタルアセットの第２量の指示と第２スクリプトハッシュとを含む、ステップを含む。

【００１７】

第２スクリプトと第２スクリプトハッシュは、第３ネットワークを介して送付されてよい。有利なことに、このことは、第２スクリプトと第２スクリプトハッシュをP2P DHTにおいて発行することを含む。そうすることで、第２インビテーションの記録を提供するこ

とができる。代替的に、第２スクリプトと第２スクリプトハッシュは、ウェブサイトにおいて発行されてよく、または、個人的に保管されてよい。第１および第３ネットワークは同じネットワークであってよい。同様に、第１および第２ネットワーク、及び／又は、第２および第３ネットワークは、同じネットワークであってよい。

【００１８】

第１ネットワークを介して送付するステップは、第１スクリプトと第１スクリプトハッシュとを第２ユーザに対して送付するステップを含んでよい。

【００１９】

本法は、さらに、Ｐ２Ｐ分散型台帳に包含するために第１交換トランザクションを生成するステップであり、第１交換トランザクションは、第１スクリプトと、第１ユーザの秘密鍵（Ｖ１Ａ）と、第１の第三者秘密鍵（Ｖ１Ｔ）と、第１インビテーショントランザクションの出力から提供される第１入力と、第２ユーザに対して移転されることになる第１エンティティの第１量を指示する第１出力とを含むステップと、記第１交換トランザクションを、第２ネットワークにおいて、ブロードキャストするステップを含む。

追加的または代替的に、本方法は、さらに、

Ｐ２Ｐ分散型台帳に包含するために、第２交換トランザクションを生成するステップであり、第２交換トランザクションは、第２スクリプトと、第２ユーザの秘密鍵（Ｖ２Ａ）と、第２の第三者秘密鍵（Ｖ２Ｔ）と、第２インビテーショントランザクションの出力から提供される第２入力と、第１ユーザに対して移転されることになる第２エンティティの第２量を指示する第２出力とを含むステップと、第２交換トランザクションを、第２ネットワークにおいて、ブロードキャストするステップを含む。

【００２０】

代替的に、交換のための単一のトランザクションが存在してもよい。それとして、本方法は、Ｐ２Ｐ分散型台帳に包含するために、第１交換トランザクションを生成するステップであり、第１交換トランザクションは、第１スクリプトと、第１ユーザの秘密鍵（Ｖ１Ａ）と、第１の第三者秘密鍵（Ｖ１Ｔ）と、第２スクリプトと、第２ユーザの秘密鍵（Ｖ２Ａ）と、第２の第三者秘密鍵（Ｖ２Ｔ）と、第１インビテーショントランザクションの出力から提供される第１入力と、記第２インビテーショントランザクションの出力から提供される第２入力と、第２ユーザに対して移転されることになる第１エンティティの第１量を指示する第１出力と、第１ユーザに対して移転されることになる第２エンティティの第２量を指示する第２出力とを含むステップと、

第１交換トランザクションを、第２ネットワークにおいて、ブロードキャストするステップを含む。

【００２１】

第１交換トランザクションを生成するステップは、第１ユーザの秘密鍵（Ｖ１Ａ）を用いて署名するために第１ユーザに対して第１スクリプトを送付するステップと、第１ユーザから第１ユーザの秘密鍵（Ｖ１Ａ）を用いて署名された第１スクリプトを受け取るステップと、第１の第三者秘密鍵（Ｖ１Ｔ）を用いて署名するために署名された第１スクリプトを送付するステップと、第１の第三者から第１の第三者秘密鍵（Ｖ１Ｔ）を用いて署名された前記第１スクリプトを受け取るステップを含む。

【００２２】

代替的に、第１交換トランザクションを生成するステップは、第２ユーザの秘密鍵（Ｖ２Ａ）を用いて署名するために第２ユーザに対して第１スクリプトを送付するステップと、第２ユーザから第２ユーザの秘密鍵（Ｖ２Ａ）を用いて署名された第１スクリプトを受け取るステップと、第２の第三者秘密鍵（Ｖ２Ｔ）を用いて署名するために第２の第三者に対して第１スクリプトを送付するステップと、第２の第三者から第２の第三者秘密鍵（Ｖ２Ｔ）を用いて署名された第１スクリプトを受け取るステップを含む。

【００２３】

第２交換トランザクションを生成するステップは、第２ユーザの秘密鍵（Ｖ２Ａ）を用いて署名するために第２ユーザに対して第２スクリプトを送付するステップと、第２ユー

ザから第２ユーザの秘密鍵（Ｖ２Ａ）を用いて署名された第２スクリプトを受け取るステップと、第２の第三者秘密鍵（Ｖ２Ｔ）を用いて署名するために第２の第三者に対して第２スクリプトを送付するステップと、第２の第三者から第２の第三者秘密鍵（Ｖ２Ｔ）を用いて署名された第２スクリプトを受け取るステップを含む。

【００２４】

本方法は、さらに、第１交換トランザクション及び／又は第２交換トランザクションを生成するステップまたはブロードキャストするステップの前に、第１ユーザと第２ユーザのうち１人またはそれ以上に対してプロンプトを送付するステップを含む。

【００２５】

第１の第三者は、エスクローサービスプロバイダまたはトークン発行者であってよい。第２の第三者は、エスクローサービスプロバイダまたはトークン発行者であってよい。

【００２６】

本方法は、さらに、第１の第三者に対して第１の第三者の公開鍵についてリクエストを送付するステップと、第１の第三者から第１の第三者の公開鍵を受け取るステップと、を含む。

【００２７】

本方法は、さらに、第２の第三者に対して第２の第三者の公開鍵についてリクエストを送付するステップと、第２の第三者から第２の第三者の公開鍵を受け取るステップを含む。

【００２８】

第１トランザクション、第２トランザクション、第３トランザクション、および第４トランザクションのうち１つまたはそれ以上は、ペイツースクリプトハッシュ（Ｐ２ＳＨ）トランザクションである。

【００２９】

第１引き換えスクリプトのハッシュおよび第２引き換えスクリプトのハッシュのうち１つまたはそれ以上は、ベース５８（Ｂａｓｅ５８）で符号化されているか、もしくは、ＳＨＡ－２５６ハッシュであってよい。

【００３０】

交換されるエンティティは、ビットコイン、コントラクト、商品、またはサービスであってよい。ここで、第１及び／又は第２エンティティは、コントラクトであり、コントラクトは、不換通貨、不動産権利書、チケット、商品、サービス、または５つ全ての組み合わせに対するものであってよい。

【００３１】

交換のための条件は、交換に関する１つまたはそれ以上の価格における１つまたはそれ以上の限度範囲、交換レート、第１インビテーションの遂行に対する締め切り、及び／又は、交換を行うための地理的領域における制限、を含んでよい。

【００３２】

本発明の実施形態は、（ブロックチェーン）トランザクションの中にメタデータを埋め込むための技術を含むことができ、

アセット（Ｂ１）に関する出力（ＴｘＯ）および引き換えスクリプトのハッシュを有するブロックチェーントランザクション（Ｔｘ）を生成するステップ、を含み、

トークン化されたエンティティの表現、または参照であるトークンを含むメタデータと、

少なくとも１つの（好ましくは２つまたはそれ以上の）公開暗号鍵、を含む。

デジタルアセット（Ｂ１）は、仮想通貨、例えばビットコインの量であってよい。引き換えスクリプトは、トランザクション出力ＴｘＯのロックスクリプトにおいて提供されてよい。メタデータは、暗号鍵のロケーションとしてブロックチェーンプロトコルにおいて指定されたロケーションにおける引き換えスクリプトの中で提供されてよい。このことは、根底にあるブロックチェーンプロトコルに対するあらゆる変更を必要とすることなくメタ

データを移転できるという利点を提供する。プロトコルを操作するノードは、暗号鍵の代わりにメタデータの使用について依存しない（agnostic）だろう。

本方法は、さらに、トランザクションＴｘをブロックチェーンに提出するステップを含んでよい。実際には、仮想通貨（Ｂ１）は、従って、トークンに関連してブロックチェーンにおいてロックされてよい。仮想通貨（Ｂ１）の量は、出力ＴｘＯのためのロックスクリプトの要求を満たすロック解除スクリプトの提供の際だけに費やす（引き換える）ことができる。
特には、ハッシュされた場合に、ＴｘＯのロックスクリプトにおいて提供されるハッシュと一致する引き換えスクリプトが提示される必要がある。出力ＴｘＯに対するロックスクリプトは、（メタデータにおいて）トークンを次いで有する引き換えスクリプトのハッシュを含むので、仮想通貨（Ｂ１）はトークンと関連付けされる。正しいロック解除（引き換え）スクリプトが一旦提示されると、仮想通貨（Ｂ１）の所有権は、引き換え当事者またはユーザに対して移転、すなわち、費やされる。

【００３３】

本発明は、上述の任意の方法を実施するように配置され、かつ、構成されたコンピュータ実装システムを提供することができる。１つの態様または実施形態に関連して上述された任意の特徴は、あらゆる他の実施形態または態様に関して使用することができる。本発明の方法に関連して言及されたあらゆる特徴は、対応する実施システムについて同様に適用することができ、その逆も同様である。

【図面の簡単な説明】

【００３４】

本発明の実施形態が、添付の図面を参照して、非限定的な実施例だけによって、これから説明される

【図１】図１は、本発明の一つの実施形態に従った、システムの模式図である。

【図２】図２は、図１に係るシステムのユーザによって実行されるプロセスのフローチャートである。

【図３】図３は、交換サービスプロバイダによって実行されるプロセスを説明するフローチャートである。

【図４】図４は、交換サービスプロバイダによって生成されるインビテーション（invitation）のためのメタデータフォーマットを説明する表である。

【図５】図５は、交換サービスプロバイダによって生成されるインビテーションのためのメタデータフォーマットを説明する表である。

【図６】図６は、図１に係るシステムの２人またはそれ以上のユーザからのインビテーションを一致させる（matching）プロセスを説明するフローチャートである。

【図７】図７は、図１に係るシステムに対する複数の当事者間における複数のトランザクションのためのトランザクションテーブルである。

【図８】図８は、図１に係るシステムに対する当事者間におけるトランザクションを説明する取引図である。

【図９】図９は、図１に係るシステムに対する複数の当事者間における複数のトランザクションのためのトランザクションテーブルである。

【図１０】図１０は、図１に係るシステムに対する複数の当事者間における複数のトランザクションのためのトランザクションテーブルである。

【図１１Ａ】図１１Ａは、図１に係るシステムに対する２人の当事者間におけるトランザクションのためのトランザクションテーブルである。

【図１１Ｂ】図１１Ｂは、図１に係るシステムに対する２人の当事者間におけるトランザクションのためのトランザクションテーブルである。

【図１１Ｃ】図１１Ｃは、図１に係るシステムに対する２人の当事者間におけるトランザクションのためのトランザクションテーブルである。

【発明を実施するための形態】

【００３５】
別の人の銀行口座への支払い又は外貨両替といった、一般的な金融取引（financial transaction）を実行する最先端の方法は、取引手数料および時間遅延の両方においてコストを招く。対照的に、ビットコインといった電子通貨における取引は、はるかに速いレート（rate）で（すなわち、数日ではなく数分）、そして、非常に低いコスト（取引き毎に数十ドルではなく数セントのオーダー）で処理することができる。
【００３６】
金融上および非金融上の両方において、日常の取引（day-to-day transactions）に係る恒久的な記録を実行して、保持する、より迅速かつ安価な方法に対する必要性が存在している。本発明は、金融アプリケーションとの使用または利点に限定されなるものではないことに留意することが重要である。代わりに、本発明は、一般的に、ビットコインブロックチェーンといった、P2P分散型台帳を利用するための方法および装置に関し、当事者があらゆるタイプの価値エンティティ（entity of value）を提供し、要求し、そして、交換することを可能にする。ここにおいて説明される方法は、エンティティの交換を実行するためのインビテーション（invitation）（または、オーダー（order））エントリー（entry）を可能にする。インビテーションの受諾（acceptance）について実際の交換に係るエンアクトメント（enactment）も同様である。実施形態は、従って、保持されるべき交換プロセスに係る全てのステップの恒久的な記録を提供する。さらに、プロセスにおける各段階（オファー、受諾、および交換）は、仮想通貨のトランザクションにおいて使用されるものと同様な暗号化ロック技術（locking techniques）を使用してセキュアにすることができる。ここにおいて説明される方法は、また、あらゆるタイプのエンティティを交換するために使用することもできる。そうしたエンティティの実施例は、これらに限定されるわけではないが、ビットコイン、不換通貨（fiat currencies）、コントラクト、商品（goods）、およびサービスを含んでいる。「仮想通貨（”cryptocurrency”）」により、これに限定されるわけではないが、ビットコインといった、暗号化された電子的に移転可能なデジタルアセットを意味している。
ブロックチェーン技術の使用を取り込んでいるCoinffeine（http://www.coinffeine.com/）といった交換が、当技術分野で知られている。しかしながら、そうした従来技術の構成（arrangement）は、未だに従来のモデルに依拠しており、そして、また、動作するために、第三者ソース、エスクロー（escrows）、および、他のマルチ通貨非銀行口座／プロセッサにも依拠している。これらの既知の構成は、（本発明による）技術革新および暗号技術を通じてではなく、むしろ、ビジネスモデルを通じて分散化（decentalisation）を達成している。
【００３７】
本発明は、トークナイゼーション技術（tokenisation techniques）の使用を組み込んでいる。コントラクトは、トークン（tokens）によるシステムを使用して交換することができる。まとめると、トークンは、契約を表す交換可能なエンティティである。コントラクトは、いくつかの形式のうち１つをとることができる。例えば、コントラクトは、保有者に権利を授与し、または、財産の所有権を示すことができる。トークンの値は、契約上で特定されてよく、そして、「ペッグ率（”pegging rate”）」を介して根底にあるBTC量に対してリンクされる。トークンは、ビットコインプロトコルといった仮想通貨プロトコルを使用する新規なタイプのトランザクションを介して交換可能である。トランザクションにおけるビットコイン値は、デジタル形式において権利契約（a rights contract）を表しているトークンとして動作する。契約自体は、ブロックチェーン上に保管されてよく、または、公にアクセス可能なオフブロックのロケーションに保存されてよく、もしくは、特定の実施形態に応じて、契約に対する当事者によって個人的に保持されてよい。契約がブロックチェーン上に保管されていない場合に、ブロックチェーントランザクション（Tx）は、一意の（unique）ポインタ、識別子、または契約に対する他の参照を保管することができる。
【００３８】

トークンは、分割可能（divisible）であり得る。分割可能なトークンとは、トランザクション出力における値をより小さい量へと細分化することができるものであり、値は複数の新たなトークンにわたり割り当てることができる。分割可能なトークンの実施例は、不換通貨のためのトークン、または、競走馬、不動産、等におけるシェア（shares）のためのトークンを含んでいる。分割可能なコントラクトは、非ゼロ（non-zero）ペッグ率を特定するものとして定義され得る。別の言葉で言えば、トークン値は、根底にあるビットコイン値に対して結び付けられている。代替的に、トークンは、分割不可能（non- divisible）であってよい。分割不可能なトークンは、保有者の権利を固定値において特定するコントラクトであり、例えば、家または豪州ドル＄１０００を引き換えるためのコントラクトである。分割不可能なトークンは、従って、根底にあるビットコインの値に対してリンクされていない。

【００３９】

トークンは、有効であるようにトークン発行者によってデジタル署名（digitally signed）される必要がある。発行者は、例えば、不動産権利の登記局（Registrar of Title deeds）といった機関であってよい。発行者は、支払いの見返りにトークンをユーザに対して発行することができる。そのトークンは、次いで、コントラクトが、不換通貨を引き換える権利であるか、またはサービスを実行させる権利であるかにかかわらず、トークンに対してリンクされたコントラクトを行使する権利をユーザに与えることができる。

【００４０】

上記に従ったトークンの実施は、以下のものを含んでいる。

・コントラクトの発行者によるトランザクション出力（UTXO）のBTC値に対してペッグされた（pegged）不換通貨トークン（fiat currency token）。例えば、「このトークンの支払人（spender）（ビットコイントランザクション出力UTXO）は、１０００サトシ（satoshis）毎に１シェア（１０セント）のレートでカナダドル（CAD）のこのトークンの任意の一部を引き換える（redeem）権利がある」。

・シンジケートの複数のメンバーによって所有されている競走馬。

・所有権が権利証書（a title deed）によるものである任意のアイテム。例えば、家または他の財産がこのようにして取り扱うことができるだろう。

・コンサートチケットを表す電子契約。これは本質的に分割不可能である。

・無記名債券（bearer bond）（分割不可能）

・商品／サービスに添付されている一意の識別子（バーコードまたはRFIDといったもの）。使用される場合に、この識別子は未だに好ましくは承認されたエンティティの署名によって有効にされる。署名がないと、より安全性が低い「商品／サービス（”goods/service”）」カテゴリへと分類される（以降に説明される）。

・実行されるべきサービスに対する権利についての契約。これは、実際のサービス自体と同じものではなく、自分のために実行されるサービスを受ける権利だけであることに留意する。この権利は取引することができる。たとえば、シドニーの首都圏内で３時間までの芝生刈りについてマイケルマウイング（Michael's Mowing）からのクーポン券（voucher）。このクーポン券（契約書）の保有者は、クーポン券を実際のサービスについて引き換えることができる。

【００４１】

トークンは、シェア（share）の価値を指定する必要がある。例えば、１シェア＝１０セントCAD、１シェア＝１ルピア（rupia）、または、１シェア＝アイテムまたはプロパティ（競走馬、家、等）である。

【００４２】

以下に説明される実施形態は、ビットコインブロックチェーン（または、単純にブロックチェーン）におけるトランザクションを記録することについて特定的に参照することができるが、本発明は、任意のP2P分散台帳を使用して実装され得ることが正しく理解されよう。以下で、ブロックチェーンは、標準化のレベルが高いこと、および、関連する公的な文書化が大量であることだけによる簡潔性（simplicity）について本発明の態様を説明

するために使用される。

【００４３】

当技術分野においてよく知られているように、ブロックチェーンは、ネットワーク化された、参加ノード（participating nodes）にわたり分散されたトランザクション台帳である。通貨のブロックチェーンの完全コピーは、これまで通貨において実行された全てのトランザクションを含んでいる。従って、トランザクションのデータレコードに係る継続的に増加するリストが提供される。ブロックチェーン上に入力された各トランザクションは暗号化されて実施されるので、データストアノードのオペレータによってさえも、改ざん（tampering）および改訂（revision）に対してブロックチェーンが強化されている。

【００４４】

本発明の実施形態においては、一方の当事者（one party）から別の当事者へビットコイン（または、他の仮想通貨）の支払いを表すトランザクションのレコードを保管することに係るデザインされた機能において使用されることの代わりに、または、加えて、ブロックチェーンは、当事者間におけるエンティティまたはアセットの移転を可能にする新規な方法で使用されている。交換（exchange）は、一方の当事者から別の当事者へデジタルエンティティの制御及び／又は所有権を移転する。これを達成するために、本発明は、１つまたはそれ以上のエンティティに係る交換を実行するためのインビテーション（または、オーダー）を保持および記録するためのメカニズムを提供する。本発明は、従って、ブロックチェーンを介して導かれる新規で有利な通信ソリューションを提供する。

【００４５】

上述のように、任意のタイプのエンティティまたはアセットが交換可能である。これらは、物理的な、「現実世界（”real world”）」エンティティ、または、仮想的な、デジタルエンティティであってよい。交換することができるエンティティの実施例は、ビットコイン、トークン（任意のタイプの移転可能なコントラクトを表している）、および、任意のタイプの商品とサービスを含んでいる。トークンは、特定の権利を保有者に授与する契約を表すことができる。多くの例のうちのいくつかを挙げると、不換通貨（仮想銀行紙幣）について引き換えられるため、プロパティの所有権（例えば、権利証書）を示し、または、イベントに対するアクセスを認めるための権利である。商品とサービスは、多くの例のうちのいくつかを挙げると、新品または中古の製品、労働（例えば、時間によって請求されるもの）、完全な仕事（例えば、芝生の芝刈り）を含んでよい。

【００４６】

図１は、一つの実施形態に従った、P2P交換システム100のネットワーク図である。システム100は、ネットワーク102およびネットワークに対する複数の当事者を含んでいる。当事者は、交換サービスプロバイダ104、第１ユーザ106、第２ユーザ108、エスクローサービスプロバイダ（an escrow service provider）110、および、発行者112を含んでいる。より詳細に以下に説明するように、交換サービスプロバイダ104、エスクローサービスプロバイダ110、および発行者112の機能の組み合わせは、単一の当事者によって引き受けることができる。別の言葉で言えば、単一の当事者がそれぞれの機能を同時に実行することができる。加えて、そして、より詳細に以下に説明するように、交換サービスプロバイダ104およびエスクローサービスプロバイダ110は、これらのサービスプロバイダ104、110を使用することなくP2P交換システム上で完全に実行できるので、任意的である。

【００４７】

交換サービスプロバイダ104は、第１ユーザ106および第２ユーザ108を含む、複数のユーザに交換サービスを提供する。発行者112は、破線によって示されるように、ネットワーク102に対して任意的である。より詳細に以下に説明するように、発行者112は、トークンの交換が関与する場合にだけ必要とされるものである。

【００４８】

いくつかの実施形態において、ネットワーク102はインターネットである。従って、他の当事者（図示なし）がネットワーク102に対する当事者であってよい。ネットワーク102に対する全ての当事者は、ネットワーク102に対する他の全ての当事者と通信することが

できる。ネットワーク102上でホストされているのは、ピアツーピア分散ハッシュテーブル（P2P　DHT）とピアツーピア分散型台帳（P2P　DL）である。システム100において示されている当事者のいくつか又は全ては、図示されていないものと一緒に、P2P　DHTおよびP2P　DLの両方またはいずれかに対するホストノードとして動作し得ることが正しく理解されよう。

【００４９】

インビテーションの構造

　インビテーションは、様々なパラメータまたはコードを含むように構成されてよい。これらは、様々な目的のために使用することができる。例えば、より詳細に以下に説明されるような、インビテーションのマッチング（matching）である。１つまたはそれ以上の実施形態においては、以下の構造を使用することができる。

Offer-type-code	
Offer-QTY-max	これは申込者の支払トランザクションで運ばれる価値、例えばBTC、の量である。 申込者がこの値より大きいBTCを提供する場合には、それは単に申込者の最大BTC提供である。 申込者がトークン化された通貨を提供している場合、この値は、（トークナイゼーション契約で指定されたペッグ率に基づいて計算された）申込者の最大提供通貨量と同等のトークン値である。申込者が、競走馬の所有権の一部といったトークン化された他の商品を提供している場合にも同じである（契約は未だに、馬におけるシェアについてのBTCトークン値が指定するペッグ率を有する）。 申込者が物理的なアイテムを提供している場合には、このフィールドが無視される。しかし、実際のビットコインのトランザクションは必要最小限の量を運ぶだろう（すなわち、ダスト＝５４６サトシ） もちろん、消費量はトランザクションの入力に係るBTC総額を超えることはできず、よって、申込者は所有するビットコインより多くを提供することはできない。
Offer-QTY-min	
Offer-Item-ID	
Offer-Description	キーワード：これは、提供が商品／サービスであり、かつ、他の識別子（オークションサイトのカタログ番号、といったもの）が存在しない場合に、設定される必要がある条件である。
Rate-min	これは、申込者が受諾する交換の最小レートであり、（要求されるユニット）／（提供されるユニット）として慣習により表現される、 例： （１）商品におけるシェアについて提供されるBTC（競走馬の一部所有権といったもの） レート＝シェア／サトシ （注：これは、また、コンサートチケットといった分割不可能な

	トークンにも当てはまるが、この場合には１シェアだけが存在し得る） （２）BTCについて提供されるトークンシェア レート＝サトシ／シェア（例えば、サトシ／セントであり、ここで、トークンはCADといった不換金額（fiat amount）に対するものである） （３）トークンのためのトークン レート＝要求されるシェア／提供されるシェア（例えば、セント／ルピアであり、ここで、提供されるトークンはルピアを表し、そして要求されるものはCADである） これは、一貫性と利便性のための慣習であって、マッチングをより容易にすることに留意する。このレートは、トークナイゼーション契約において使用されているペッグ率に基づいて、要求されるサトシ／提供されるサトシへと容易に簡単に変換することができるだろう。
Rate-max	
Conditions	これは、別個のメタデータフィールドにおいてコード化される８個までの条件を示すコードになる。例えば： ・ 締め切り（Unix時間において） ・ ロケーション これらのメタデータフィールドのフォーマットは、条件のタイプに依存する。 オファー記述（Offer-Description）およびリクエスト記述（Request-Description）も、または条件とみなされることに留意する。要求される全ての情報は一般的に他のメタデータフィールドの中へコード化することができるため、それらは通常は必要とされない。必要な場合には、次いで、Conditionsビットフィールドにおける適切なフラグをスイッチオンすることにより存在するものとしてフラグされることを要する。
Request-type-code	
Request-item-ID	
Request-description	キーワード：これは、リクエストが商品／サービスであり、かつ、他の識別子（オークションサイトのカタログ番号といったもの）が存在しない場合に設定されることを要する条件である。
Request-QTY-max	
Request-QTY-min	

【００５０】

交換サービスプロバイダ104の１つの目的は、P2P DHTとP2P DLの両方においてインビ

テーション（またはオーダー）を置く（place）ためにユーザ106、108のためのゲートウェイを提供することである。ネットワーク102のユーザ106、108は、それ自体、P2P DHTとP2P DLの両方にインビテーションを置くことができるが、交換サービスプロバイダ104は、簡素化されたインターフェイスを提供し、インビテーションが生成される効率を改善し、かつ、当業者であれば理解するように、ビットコイン台帳といった、分散型台帳におけるトランザクションの直接的な取り扱いに関連する危険を低減する（例えば、トランザクションの喪失、等）。P2P DHTとP2P DLにおけるユーザインビテーションの発行を可能にすることに加えて、交換サービスプロバイダは、以下の追加サービスのうち１つまたはそれ以上を実行することができる。

・インビテーションのマッチング（Matching invitations）－ 上述のように、インビテーションは、ａ）ユーザが交換することを望むエンティティの詳細、ｂ）交換に添付された１つまたはそれ以上のユーザ適用オプション／条件、を含んでよい。２つのインビテーションは、それぞれのエンティティの詳細がミラーリングされており（mirrored）、かつ、２つのインビテーションの条件のうち１つまたはそれ以上が適合する場合に、一致し得る。別の言葉で言えば、第１インビテーションの中に含まれる一つまたはそれ以上のパラメータまたは特徴が、また、第２インビテーションの中にも含まれている場合に、一致が生じ得る。インビテーションにおけるパラメータ間にはいくつかの共通性が存在している。ミラーリングされたエンティティの詳細の例は、第１ユーザ（アリス（Alice））がリンゴのためにビットコインを提供し、かつ、第２ユーザ（ボブ（Bob））がビットコインのためにリンゴを提供する場合である。サービスプロバイダは、従って、交換に適応する（accommodate）ために、コンパチブルなインビテーションを合致するマッチングサービスを提供することができる。マッチングは、一致するエンティティ及び／又は条件を有する１つまたはそれ以上のインビテーションについてP2P DHTをスキャンすることを含んでよい。いくつかの実施形態において、サービスプロバイダ104は、ユーザからの要求に応じてP2P DHTをスキャンすることができる。例えば、ユーザは、サービスプロバイダ104に対して所望のインビテーションのための１つまたはそれ以上のクライテリア（criteria）を提供することができる。提供されたクライテリアに基づいて、サービスプロバイダ104は、次いで、それらのクライテリアに一致する、既にP2P DHT上に置かれているインビテーションを検索することができる。他の実施形態において、サービスプロバイダ104は、特定のユーザ要求に関係しない、一致またはほぼ一致するインビテーションについてP2P DHTを検索する、非特定的なペアリングアルゴリズム（non-specific pairing algorithm）を実装することができる。マッチングサービスは、他の第三者プロバイダによって提供されてよいことが正しく理解されよう。１つまたはそれ以上の第三者プロバイダが存在してよく、その主な目的は、上記に従ってマッチングサービスを提供し、以下に説明されるように、同様にマッチングアラートを提供することである。いくつかの実施形態において、マッチングはマッチングサービスプロバイダ（MSP）によって提供される。

１つまたはそれ以上の実施形態に従って、かつ、また上記の「インビテーションの構造」セクションに示されるテーブルを参照して、以下のようなＡとＢとの間でインビテーションのマッチングからマッチングアルゴリズムを採用することができる。

ＡのOffer-type-codeは、ＢのRequest-type-codeと一致することを要する
ＡのRequest-type-codeは、ＢのOffer-type-codeと一致することを要する
ＡのRate-min ≦ ＢのRate-max（同等の単位で表される場合）
ＡのRate-max ≧ＢのRate-min（同等の単位で表される場合）
Request-item-IDは、Offer-Item-IDと一致することを要する
ＡのRequest-QTY-min ≦ ＢのOffer-QTY-max
ＡのRequest-QTY-max ≧ ＢのOffer-QTY-min
Ａの条件は（もしあれば）、Ｂのインビテーションと適合することを要する
Ｂの条件は（もしあれば）、Ａのインビテーションと適合することを要する

本発明は、このアルゴリズムまたはその変形を実施するマシンで実行可能なルールを組み込むように構成することができる。

・アラートの一致（Match alerts）－ 一致またはほぼ一致が検出された場合に、交換サービスプロバイダ104は、電子メールによる、もしくは、電話またはタブレットアプリケーションを介するといった、既知の方法でユーザにアラートする（alert）ことができる。従って、本発明は、新規な通信またはアラートメカニズムを提供することができる。
・一致に基づく新たなインビテーション生成（Generating new invitation based on matches）－ ユーザが、置きたいと望むインビテーションまたはオーダーの詳細を提供する場合に、サービスプロバイダ104は、ユーザのオーダーの条件を満足する１つまたはそれ以上のインビテーションについてP2P DHTをスキャンすることができる。次いで、P2P DHTにおいてインビテーションのマッチングが見つかった場合に、サービスプロバイダ104は、成功した一致を促進するために、既にP2P DHT上にある識別されたインビテーションをミラーリングするインビテーションを生成することができる。P2P DL上で最終トランザクションを完了するためには、トランザクションに対する全ての当事者は、P2P DLで既に公開されているインビテーションを有する必要があることに留意する。しかしながら、全てのインビテーションがP2P DHTにおいて公開されることを要するとは限らない。この実施例において、例えば、サービスプロバイダは、インビテーションが広告される（advertised）必要が存在しないので（所望の一致が既に見つかっている）、P2P DHT上でオファーを公開する必要はない。しかしながら、例えば、最初のマッチングが失敗に終わる場合に、生成されたインビテーションは、未だにP2P DHT上に置かれてよいことが正しく理解されよう。

・トランザクションの実行（Executing transactions）－ インビテーションのペアが成功裡に一致した後で、サービスプロバイダ104は、最終トランザクションを実施するためのプロキシとして動作することができる。例えば、２つのインビテーションが一致するという判断において、サービスプロバイダ104は、実際のトランザクション、すなわち、エンティティの交換を含むトランザクションを、P2P分散型台帳に記録することができる。このプロセスは、当事者が承認を表すことなく、または、トランザクションを承認するために一人またはそれ以上の当事者を促した後で、自動的に行われてよい。 いくつかの実施形態では、インビテーションの中のメタデータは、交換が確定される前に当事者が通知されることを要するか否かを示すことができる。

・ｅウォレットサービス（eWallet services）－ 上記に加えて、サービスプロバイダ104は、また、仮想通貨の鍵、等の保持といった、従来のｅウォレットサービスを提供することもできる。

【００５１】

図１のシステム１００においては、単一のサービスプロバイダ104が示されている。しかしながら、１つまたはそれ以上の追加の交換サービスプロバイダがネットワーク102に対する当事者であってよいことが正しく理解されよう。１つ以上の交換サービスプロバイダが存在する場合に、ユーザは、例えば、サービスプロバイダの料金体系、ロケーション、互換性、等を含み得る、それらの要求に応じて交換サービスプロバイダを選択することができる。従って、所定の状況においては、一致するインビテーションを持つ２人のユーザが、異なる交換サービスプロバイダを使用してよいことが正しく理解されよう。そうした状況において、ユーザのそれぞれの交換サービスプロバイダは、交換を促進するために相互間で通信することができる。

【００５２】

交換サービスプロバイダ104に加えて、エスクローサービスプロバイダ110（または、略してエスクロー）が、ネットワーク102における当事者であってよい。エスクローサービスプロバイダ110は、取引が決済されるまでユーザのオファーを保持すること（すなわち

、提供された金額が留保されている）、または、所定の条件下において、オーダーをキャンセルし、かつ、インビテーションにおいて提供されたものを何でも返却すること、を可能にする。エスクローサービスプロバイダ110は、トランザクションについてエスクローサービスを提供するために、トランザクションの２人の当事者によって信頼される、中立的な第三者として機能する。従って、システムにより、ユーザは、最終トランザクションに参加することができ、オファーを行うユーザが、提供された金額を（ビットコインまたはトークンで）を満足できるという保証を有することができる。

【００５３】

交換サービスプロバイダと同様に、１つ以上のエスクローがネットワーク104に対する当事者であってよい。P2P交換システム100のユーザは、また、１つのエスクロープロバイダを使用する場合に、どのエスクロープロバイダを使用するか選択することもできる。いくつかの実施形態において、エスクロー110のサービスは、交換サービスプロバイダ104のサービスの中に組み込まれてよく、または、その逆も同様である。そうした場合には、別個のエスクローが必要とされないことがある。

【００５４】

上記に加えて、システム100は、また、発行者112も含んでよい。発行者112は、トランザクションがトークンの交換を含む場合に、関与することができる。そうした状況において、プロセスは、トークンに署名する発行者を取り込んでいる。トークンの移転を取り込んでいるそれぞれのトランザクションは、好ましくは、発行者112を含んでいる。ここにおいて説明される実施形態において、発行者の署名は、インビテーショントランザクションにおいて要求され、そこではトークンが提供されて、エスクローにおいて保持される。発行者の署名は、また、交換トランザクションにおいても要求され、そこでは相手方（counterparty）に対してトークンの支払いが行われる。

【００５５】

本開示の実施形態の重要な態様は、ビットコイン交換トランザクション（または、仮想通貨トランザクション）において交換を実行するためのインビテーションに関するメタデータを埋め込むための能力（ability）であり、同様に、ビットコインまたは他の仮想通貨トランザクションにおいて、実際の交換に関するメタデータを埋め込むための能力である。ここにおいて説明される実施形態は、以下に説明するように、そうしたメタデータの埋め込みを可能にするために、マルチシグネチャ（multi-signature）ペイツースクリプトハッシュ（pay to script hash、P2SH）タイプのトランザクションを使用する。

【００５６】

（ｉ）一般的なP2SHにおける引き換えスクリプト（Redeem script in P2SH in general）

背景として、ビットコインプロトコルの標準的なペイツースクリプトハッシュ方法において、引き換えスクリプトは以下の形式をとる：

<NumSigs PubK1 PubK2 ... PubK15 NumKeys OP_CHECKMULTISIG>

ここで、

NumSigsは、トランザクションをロック解除するための引き換えスクリプトを満足するために要求される有効な署名の数「m」である。

PubK1、PubK2、・・・、PubK15は、トランザクションをロック解除する署名に対応する公開鍵（public keys）である（最大１５個までの公開鍵）。

NumKeysは、公開鍵の数「n」である"（１５個以下でなければならない）。

【００５７】

上記の引き換えスクリプトを償還するためには、公開鍵に対応する少なくとも「m」個の署名が必要とされる。いくつかの実施においては、公開鍵の順序が重要であり、そして、署名（signing）のための「n」個の署名のうち「m」個の署名が、順番に行われなければならない。例えば、「m」が２であり、公開鍵の数「n」が１５であるとする。２個の署名が使用のために利用可能であるとすると、例えばSig1（PubK1に対応しているもの）とSig15（PubK15に対応しているもの）、引き換えスクリプトは、最初にSig1によって署名さ

れ、その後でSig15によって署名されなければならない。

【００５８】

（ｉｉ）P2SHにおけるメタデータの埋め込み（Embedding metadata in P2SHl）

本発明者は、引き換えスクリプトにおいて公開鍵のために利用可能な１５か所のうち１つまたはそれ以上において、メタデータがP2SHの中に埋め込まれ得ることを認識した。

【００５９】

例えば、P2SHは以下の形式をとる：

<NumSigs Metadata1 Metadata2 ... PubK1 PubK2 ... NumKeys OP_CHECKMULTISIG>

ここで、

NumSigsは、トランザクションをロック解除するための引き換えスクリプトを満足するために要求される有効な署名の数「m」である。

Metadata1とMetadata2は、それぞれ、公開鍵に代わるメタデータを含んでいる。

PubK1とPubK2は、実際の公開鍵である。そして、

NumKeysは、メタデータと公開鍵（１５個以下でなければならない）によって取られる位置の総数である。

【００６０】

引き換えスクリプトの中に、インビテーションの条件、トークンに関連するコントラクトの詳細、及び／又は、交換に関連する他の情報に対応するメタデータを置くことによって、そうした情報のハッシュは、P2P分散型台帳の中に含まれる。この埋め込み方法は、次のように要約できる。

仮想通貨の一部に関する出力（Tx0）および引き換えスクリプトのハッシュを有するブロックチェーントランザクション（Tx）を生成することであり、Txは、

トークン化されたエンティティの表現、または参照である、トークンを含むメタデータ、および、

少なくとも１つ（好ましくは２つまたはそれ以上の）公開暗号鍵、を含む。

トークン化されたエンティティは、交換に関するコントラクト及び／又は他のエンティティとすることができる。メタデータは、暗号鍵のためのプロトコルによって指定されたロケーションにおいて提供される。

【００６１】

このように、本発明の実施形態におけるマルチシグネチャP2SHビットコイントランザクションの使用は、いくつかの利点を提供する。第１に、それは、インビテーショントランザクションがメタデータペイロードを運ぶ（carry）ことを可能にする。第２に、それは、交換トランザクションにおけるエスクローサービスの利用を促進する。第３に、交換においてトークンが移転されるロケーションで、それにより、交換トランザクションは、交換される１つまたはそれ以上のトークンに関するメタデータを運ぶことができる。また、根底にあるブロックチェーンプロトコルは、メタデータがトランザクションを介して送付されているという事実には関わらない（agnostic）。従って、この情報を伝達するためにブロックチェーンプロトコルに対する変更は必要とされない。

【００６２】

メタデータは、インビテーショントランザクションにおいてオファー（offer）またはリクエスト（request）を記述している記載またはキーワードを含んでよい。メタデータは、また、インビテーションに関する条件も含んでよい。例えば、インビテーションに締め切り日付を添付することができる。締め切りは、それまでにオーダーが遂行されねばならない時間及び／又は日付を指定することができる。インビテーショントランザクションを用いて締め切り条件が提供される場合には、同じBTC量を費やし、かつ、交換が行われる締め切りを表すロック時間（locktime）を含んでいる、取り消し（cancellation）トランザクションが生成されてよい。取り消しトランザクションは、ロックタイムまでP2P DL上に配信されることを防ぐことができる。締め切りまでに交換が行われない場合には、取り消しトランザクションがP2P DLに対して追加され、そして、支払人（payer）及び／

又はサービスプロバイダに効果的に払い戻される。締め切りが終了する以前に交換が行われた場合に、交換トランザクションはその量（amount）を費やし、時間ロックされた取り消しトランザクションに先立ってP2P DLにヒットする二重支払い（double-spend）を創出し、それにより、取り消しトランザクションをブロックしている。いくつかの実施形態においては、メタデータは、締め切りを含まなくてよいが、その代わりに、取り消しトランザクションは、元のインビテーショントランザクションを取り消すことについて単に責任を負うことができる。代替的に、締め切りメタデータ条件は、取り消しトランザクションの支払い（spending）を自動的に引き起こさなくてよい。別の言葉で言えば、締め切りは支払人の管理下に残る柔軟な締め切りであってよい。この締め切りは、従って、単にそれが失効することを許可し、かつ、遅れて一致するインビテーションを依然として受け入れる当事者によって拡張されてよい。同様に、サービスプロバイダは、未使用のままである場合に、期限切れのオーダーとの照合を依然として試みてよい。

【００６３】

インビテーショントランザクションを置く（placing）のと同時に取り消しトランザクションをロックする代わりに、ユーザは、締め切りの後まで待つことができ、そして、そう望む場合には、取り消しトランザクションを手動で入力することができる。

【００６４】

条件は、また、例えば、トランザクションブロードキャストのロケーションが指定された座標のＸメートル以内にある場合には、トランザクションがP2P DHT上にだけブロードキャストされること、を指定することができる１つまたはそれ以上のロケーション条件（location conditions）を含むこともできる。このことは、トランザクションが指定されたロケーション、例えば、ボブのコーヒーショップ、でだけ行われることを保証する。

【００６５】

ユーザが自分の新しい条件を作成し、そして、以前に使用されていない条件コードにそれらに割り当てることによって、条件のリストにそれらを追加することを可能にするファシリティ（facility）が存在し得る。このファシリティは、乱用に抵抗することができる。例えば、各サービスプロバイダは、単に関連する条件コードと一緒に条件の独自のテーブルを公開することができ、そして、システム100の他の当事者は、同じコーディングを採用することを選択することができ、かつ、また、それ自身の新しいコーディングを追加することもできる。次いで、例えば、条件コードの再使用のせいで紛争が発生した場合に、紛争は、サービスプロバイダまたはシステム100の他のユーザによって解決され得るものである。

【００６６】

本発明の実施に係るいくつかの例が、第１ユーザ106（ここにおいてはアリス（Allice）と呼ばれる）と第２ユーザ（ここにおいてはボブ（Bob）と呼ばれる）との間のトランザクションの例としてこれから説明される。この例において、トランザクションは、ビットコインについてトークン化されたカナダドルの交換である。

【００６７】

インビテーションを知らせること（Posting an invitation）

【００６８】

第１実施例において、アリスは、ビットコインについてトークン化されたカナダドル（CAD）をいくらか購入したい。彼女の関心を広告するために、アリスは、例えば、ウェブインターフェイス、もしくは、タブレットまたは携帯電話上で動作するアップ（app）を介して、交換サービスプロバイダ104にコンタクトする。図２に示されるように、ステップ２０２において、アリスは、サービスプロバイダ104のウェブインターフェイスへとログインする。ステップ２０４と２０６において、アリスは、次いで、彼女のインビテーションの詳細をサービスプロバイダに対して送付する。交換されるエンティティ（ビットコインについてトークン化されたCAD）と交換の条件、およびサービスプロバイダによって提供される任意の選択されたオプションを含むものである。アリスは、例えば、有効なインビテーションへとサービスプロバイダ104によって次いで翻訳され得る通常の言語を使

用して、サービスプロバイダ104によってホストされているインターフェイスの中へこの情報を入力することができ、または、代替的に、アリスは、事前選択オプション（pre-selecting options）例えば、ドロップダウン選択メニューを介して、簡単に情報を入力することができる。

【００６９】

ステップ２０８において、アリスは、彼女の選択に基づいてサービスプロバイダ104によって生成され、かつ、アリスが交換したいと望むエンティティに関する情報およびインビテーションに関する任意の条件を含む、引き換えスクリプト（redeem script）をサービスプロバイダ104から受け取る。アリスは特定のサービスプロバイダ104を使用するように契約（signed up）しているので、サービスプロバイダ104は、既にアリスの公開鍵（public key）を持ち得る。代替的に、アリスは、最初の選択の最中か、または、サービスプロバイダ104からの要求に応じてかのいずれかで、サービスプロバイダ104に対して彼女の公開鍵を提供することができる。

【００７０】

アリスは、ステップ２１０において、彼女の公開鍵に対する暗号ペア（cryptographic pair）である、彼女の秘密鍵を使用して引き換えスクリプトに署名し、そして、ステップ２１２において、配布されるように、署名された引き換えスクリプトをサービスプロバイダ104へ送り返す。このプロセスは、それ自体がサービスプロバイダ104によって提供され得る、アップの使用によってサポートされてよい。

【００７１】

図３に示されるフローチャート300は、サービスプロバイダ104によって実行される対応するプロセスを説明している。ステップ３０２において、サービスプロバイダ104は、アリスからのインビテーションの詳細を受け取り、そして、ステップ３０４において、アリスの公開鍵、エンティティの詳細、およびインビテーションの条件を使用して、引き換えスクリプトを生成する。引き換えスクリプトは、P2SHビットコイントランザクションについて適したフォーマットであってよい。インビテーションの詳細は、マルチシグロック解除スクリプト（multisig unlocking script）において通常使用されている３２バイトの公開鍵の代わりに（in place of）、メタデータフィールドにおいて保管されてよい。図４は、一つの実施形態に従って、アリスのインビテーションについてメタデータのフォーマットを示している。インビテーションにおいて、アリスは、トークン化されたCADを要求し、そして、見返りに、４００CAD／ビットコイン以上のレートでビットコインを提供する。より詳細に以下に説明するように、図４は、また、インビテーションに対して追加することができる締め切り条件（deadline condition）も示している。締め切り条件は、インビテーションに基づいて、交換が確定されていない場合に締め切りにおいてインビテーションが取り消されるようにすることができる。

【００７２】

引き換えスクリプトは、次いで、署名のためにアリスへ送付される。アリスから署名された引き換えスクリプトを受け取ると、ステップ３０８において、サービスプロバイダ104は、署名された引き換えスクリプトのハッシュを生成する。

【００７３】

サービスプロバイダ104は、２つの方法でハッシュを使用する。第１に、ステップ３１０において、サービスプロバイダ104は、公に利用可能なP2P DHTにおけるハッシュと共にインビテーションの詳細をリストする。上述のように、この表はトレント技術（torrent technique）を採用しているので、集中化されるのではなく、むしろ分散されており、そして、従って、公にアクセス可能なままであり、かつ、偽和（adulteration）から安全である。他のサービスプロバイダ104は、次いで、インビテーションにアクセスし、そして、彼ら自身のサイトにおいてリストすることができる（実際には、サービスプロバイダ104は、単にハッシュテーブルを唯一のリポジトリとして使用し、そして、インビテーションに係る自身のローカルデータベースを維持する必要さえない。）

【００７４】

ハッシュが使用される第２の方法は、ステップ３１２において、ビットコイントランザクションのロッキングスクリプト（locking script）を作成することである。このトランザクションは、ロック解除するために２つの署名を必要とするP2SHスクリプトに対してアリスのビットコインのある量を費やす。アリスの署名、および、指定されたエスクローサービスプロバイダ110（上述のように、サービスプロバイダ104と同じエンティティであっても、なくてもよい）の署名である。このトランザクションの目的は、二重（twofold）である。第１に、インビテーションがP2P DL上に記録される（logged）。任意のユーザまたはそのサービスプロバイダは、（一致するハッシュ値を介して）P2P DL上に一致するトランザクションが存在することを保証することによって、P2P DHT上のインビテーションが正当（legitimate）であることを確認することができる。第２に、トランザクションは、アリスがインビテーションにおいて成したコミットメントを「ロック（”lock”）」する。トークン化されたCADの交換においてアリスが提供するビットコインの量は、オーダートランザクションによって費やされる量である。従って、オーダーは十分な資金（funds）によって裏付けされていることを確認することができる。

【００７５】

一致するインビテーションのペアリング（Pairing matching invitations）

【００７６】

第２の実施例において、ボブは、彼のBTCについてトークン化されたCADのいくらかを売りたい、そして、アリスによって使用されておりサービスプロバイダ104と同じか又は異なるサービスプロバイダのいずれかを使用して、彼自身のインビテーションを独立的にリストしている。ボブのオーダーも、図２および図３を参照して説明したように、ハッシュテーブルにおいてリストされ、そして、P2P DLトランザクションの中に埋め込まれている。ボブのインビテーションのメタデータが、図５において示されている。

【００７７】

図６を参照すると、アリスとボブのオーダーをマッチングするプロセス400が説明されている。この例において、サービスプロバイダ104が、そのプロセスを実行するものとして説明されている。しかしながら、任意の交換サービスプロバイダ、または、実際には、他の任意の適切な第三者が、プロセス400を実行し得ることが正しく理解されよう。

【００７８】

交換サービスプロバイダ104は、アリスとボブのインビテーション間における完全な一致または部分的な一致を識別するように動作可能なマッチングアルゴリズムを実行することができる。ステップ４０２において、交換サービスプロバイダ104は、エンティティの詳細をマッチングするために、P2P DHTをスキャンする。スキャンの最中に、サービスプロバイダ104は、アリスとボブのインビテーションに係るエンティティの詳細の間における一致をチェックする。ステップ４０４において一致が見つからない場合に、次いで、プロセスは、ステップ４０２まで戻り、そして、交換サービスプロバイダ104は、エンティティの詳細のマッチングのためにP2P DHTをスキャンし続ける。ステップ４０４において一致が見つかった場合、プロセス400は、ステップ４０６を続けて、アリスとボブのインビテーションそれぞれの１つまたはそれ以上の条件の間における一致についてチェックが行われる。ステップ４０６で一致が見つからない場合に、プロセスはステップ４０２へ戻る。１つまたはそれ以上の条件の間における一致が見つかった場合に、次いで、プロセスはステップ４０８へ移動し、そこで、交換サービスプロバイダ104は、アリスとボブとの間のトランザクションを作成し、そして、確定するように試みる。

【００７９】

ポジティブな一致（positive matching）が確認されるためには、ステップ４０６において、２つのインビテーションにおける全ての条件の直接的な一致が要求されなくてよい。実際に、プロセス400は、条件のいくつかが一致することを要求するだけであってよい。追加的または代替的に、１つまたはそれ以上の条件が完全に一致する必要はない。例えば、比較されている条件が各条件においてオファーされる交換レートである場合に、プロセス400は、レートが互いに既定の閾値範囲内にあれば、ポジティブな一致を確認するこ

とができる。例えば、アリスが４×１０$^{-5}$トークン化CAD／サトシ（tokenised CAD/satoshi）の最小レート条件をオファーしており、かつ、ボブの同様な最小オファーレートが３．９×１０$^{-5}$トークン化CAD／サトシである場合には、ボブの提示レートがアリスのオリジナルの要件を十分に満たすものではないとしても、プロセスは、それでも条件の一致を確認し得る。そうした状況においては、一致に際して、アリスには受け入れるためのオプションが与えられてよい。ボブの同様な最小オファーレートが４．１×１０$^{-5}$トークン化CAD／サトシである場合には、条件が満足されることが正しく理解されよう。別の例において、条件は、オファーおよび要求においてオファーされる商品およびサービスに対するそれぞれの値であってよい。プロセス400は、２つの値が互いに既定の閾値範囲内にあれば、ポジティブな一致を再び確認することができる。いずれの場合にも、既定の閾値範囲は、例えば、オファー値または要求値に係る計数値（discrete value）またはパーセンテージであってよい。

【００８０】

前述のように、ボブとアリスのインビテーションそれぞれ又は両方のトランザクションメタデータは、さらに、１つまたはそれ以上のロケーション条件を含んでよく、例えば、トランザクションブロードキャスト（transactional broadcast）のロケーションが指定された座標のＸメートル以内である場合にトランザクションがP2P DHT上にのみブロードキャストされることを指定することができる。このことは、トランザクションが指定されたロケーション、例えばボブのコーヒーショップ、おいてのみ行われることを保証する。

【００８１】

一旦、一致が見い出され、かつ、トランザクションを完了する以前に、１つまたはそれ以上の介在するステップ（intervening steps）が実行されてよい。これらは、一致が見い出されたことの当事者に対するアラートを含んでよく、進行することを彼らが望んでいるということを確認するためのリクエスト、等が後に続く。例えば、上述のように、条件が１人またはそれ以上のユーザによって完全ではないがほぼ満足される場合には、それでも一致は記録されるが、全ての当事者がインビテーションの条件に満足するまで確定されなくてよい。このプロセスは、条件について最終合意を交渉するためのカウンターオファー（counter offers）をもたらし得るものであり、次いで、上述のプロセスに従ってさらなるインビテーションの生成をもたらし得る。

【００８２】

最終的な交換は、各インビテーショントランザクションの出力を費やす１つまたはそれ以上のビットコイントランザクションを作成することによって実行することができる。本発明者は、トランザクションを完了するいくつかの新規な方法を見い出した。これらに限定されるわけではないが、トランザクションに関与するユーザ、交換されるエンティティ、およびトランザクションに関与するサービスプロバイダと発行者、を含む状況に依存し得るものである。これらの方法のうちいくつかの実施例が以下に説明される。

【００８３】

図２から図６までを参照して上述された実施例から続いて、アリス－ボブおよびボブ－アリスについて別々のトランザクションのためのトランザクションテーブル500が図７に示されており、そして、トランザクションフローの概略図600が図８に示されている。図４と図５に示されるメタデータ値と同様に、トランザクションテーブル500において提供される値は、例としてだけ示されるものである。この例においては、アリスのインビテーショントランザクションにおける彼女のビットコインはボブに対して費やされ、そして、ボブのインビテーショントランザクションにおける彼のCADトークン化ビットコインはアリスに対して費やされる。

【００８４】

最初にアリス－ボブのトランザクションを参照すると、このトランザクションの入力602は、アリスのインビテーションと共にP2P DL上に置かれたインビテーショントランザクションの出力から提供されている。第１トランザクションと同様に、アリスとエスクローサービスプロバイダ110の両方によって入力スクリプトが署名される（アリスはトランザ

クションが進行することを喜ぶと仮定している）。スクリプトは、費やされたビットコイン（spent bitcoins）をロック解除し、ａ）トークン化CADに対する見返りの彼の支払いとしてボブに対して（604）、ｂ）交換に対する支払いとして交換サービスプロバイダ104に対して（606）、およびｃ）もしあれば、お釣り（change）としてアリスに対して（608）、出力することができる。

【００８５】

これからボブ－アリスのトランザクションを参照すると、このトランザクションは２つの入力を有している。トランザクションの第１入力610は、ボブのインビテーションと共にP2P DL上に置かれたインビテーショントランザクションの出力から提供されている。このトランザクションに対する入力はトークン化されているため、入力スクリプトはボブとトークン発行者の両方によって署名される必要がある。この状況において、トークン発行者は、また、エスクローとしても動作し、それにより、ボブ（および、任的にアリス）がトランザクションに満足するまで資金を保留している。署名されたスクリプトは費やされたトークンをロック解除し、次いで、ａ）BTXに対する見返りの支払いとしてアリスに対して（612）、およびｂ）アリスに対して送付された値より少ないオリジナルのトークン値に対するお釣りトークン（change token）としてボブに戻って（614）、出力することができる。第２入力616は、ボブの以前のビットコイントランザクションからのものである。この入力は、ロック解除され、そして、ａ）交換に対する支払いとしてサービスプロバイダ104に対して、ｂ）交換トランザクションに対する料金（fee）としてビットコインマイナに対して、およびｃ）サービスプロバイダ104の料金とマイナの料金より少ないオリジナルのビットコイン入力値の値に対するビットコインでのお釣り（change）としてボブに対して、出力される。

【００８６】

各トランザクションに対するサービスプロバイダ104の料金は、トランザクションの値のスライス（slice）であってよい。代替的または追加的に、料金は、２つのインビテーションにおいて示された対応するレート条件間に広がる交換レートのスライスであってよい。例えば、オファーされたレートがオーバーラップする場合に、サービスプロバイダ104は、交換に係る両面をそれぞれの提示レート（asking rate）で遂行し、そして、差を料金として保持することができる。代替的または追加的に、サービスプロバイダ104によって、フラットな料金（サトシ、トークン化された通貨、またはその他におけるもの）が取られてよい。

【００８７】

一旦トランザクションが完了すると、ボブとアリスのそれぞれのサービスプロバイダは、P2P DHTから彼らのインビテーションのエントリを削除し、または、オリジナルのエントリを無効にするさらなるエントリを入力することができる。例えば、サービスプロバイダは、エントリが支払トランザクション（spend transaction）に対応するので、P2P DHT上にそのエントリを単に残すことができる。これは、インビテーションが、もはや有効でないことを意味する。代替的に、サービスプロバイダは、費やされたことを示すフィールドを用いてトランザクションをマークすることができる。これは、特定のエントリに対応するDHTにおける個別のフィールドであってよいが、インビテーションと関連付けられた実際のメタデータは変更しない（このことは、スクリプトハッシュ（script hash）が未だにトランザクションにおけるハッシュと一致することを保証し得る）。代替的に、サービスプロバイダは、P2P DHTからエントリを削除することができる。しかしながら、P2P DHTの利点は、システム100を使用するトランザクションの永続的な監査制御（audit control）である。望ましくは、従って、P2P DHTからのエントリの削除が防止され、もしくは、エントリのレコードを維持するために削除されたエントリがアーカイブされる。一つの例においては、削除されたエントリがアーカイブされる。

【００８８】

上記の例のトランザクションにおいて、パズル（puzzle）は交換されない。別の言葉で言えば、２つのトランザクション（アリス－ボブとボブ－アリス）は完全に分離された、

別々のものである。しかしながら、ある場合には、２つのトランザクションについて有効または無効のいずれかであることが望ましい。図９は、アリスのトランザクション（アリス－ ボブ）においてパズルが交換される代替的なトランザクションの例を示している。そうすることによって、２つのトランザクションは一緒にロックされ、他方を費やすことなく、一方を費やすことはできない。このことは、相手方のトランザクションも通過することなく、一方の当事者から別の当事者へのトランザクションが通過することを防止する。

【００８９】

上記の２つの例においては、交換を完了するために２つのビットコイントランザクションが実行されている。可能であれば、しかしながら、上記の２つのトランザクションを単一のビットコイントランザクションへと統合することが望ましい。そうすることは、交換の２つの部分を一緒に自動的にロックし、かつ、トランザクションのためにアリスとボブによって支払われる全体の手数料の削減につながる。

【００９０】

図１０は、アリスとボブとの間の単一のトランザクションに対するトランザクションテーブル700を示している。交換のためのトランザクションフローは、以前の２つの実施例と同じである、つまり図６に示されているものである。しかしながら、交換は、単一のマルチ入力－マルチ出力（multi-input-multi-output、MIMO）トランザクションへと統合されている。図８においては、２つの別個の料金が交換サービスプロバイダ104に対して支払われることに留意する。しかしながら、ボブとアリスの両方について交換サービスプロバイダ104が同じである場合に、これら２つの料金は、ボブ、アリス、またはボブとアリスの両方によって支払われる、単一のトランザクションへと統合され得る。

【００９１】

２つ以上の当事者を含むトランザクション

【００９２】

上記のトランザクションは、２つのエンティティ間における交換に関するものである。しかしながら、いくつかの例においては、２つより多いエンティティが交換に関与し得ることが正しく理解されよう。例えば、以下のシナリオを考えてみる。アリスはビットコインをリンゴと交換したいが、最低でも１０００個のリンゴしか受け入れない。ボブは、リンゴをビットコインと交換したいが、５００個のリンゴしか供給できない。キャロルは、リンゴをビットコインと交換したいが、６００個のリンゴしか供給できない。こうした状況において、アリスのインビテーションの条件は、ボブまたはキャロルによって個別には満足することができない。しかしながら、一緒に、ボブとキャロルは１１００個のリンゴを持っており、そして、アリスのインビテーションを満足することができる。

【００９３】

別の実施例において、アリスはトークン化CADをトークン化GBPと交換したいし、ボブはトークン化GBPをトークン化AUDと交換したいし、そして、キャロルはトークン化CADをトークン化AUDと交換したい。３人の当事者のあらゆる２人の間に直接的な一致は存在しないが、組み合わされて、インビテーションのそれぞれを満足することができる。－アリスのトークン化CADがキャロルのところへ行き、ボブのトークン化GBPがアリスのところへ行き、そして、キャロルのトークン化AUDがボブのところへ行くことができる。図１１Ａから図１１Ｃは、アリス、ボブ、およびキャロルの間におけるトランザクションのための例示的なトランザクションテーブルを示している。

【００９４】

図１１Ａを最初に参照すると、アリスからキャロルへの支払いについてトランザクションテーブルが示されている。アリスは１５００ドルのトークン化CADを有しており、そして、ボブからのトークン化GBP５００を必要としている。トランザクションは、トークン化CAD１０００をアリスからキャロルに対して支払い、そして、アリスは彼女自身に残りのトークン化CAD５００（１５００－１０００）を支払う。標準BTC（regular BTC）を使用して、アリスは、サービスプロバイダの料金（図１１Ａに示すような定額料金であって

よく、または、移転の価値に応じた料金であってよい）を支払うことができ、そして、お釣りからマイナ（miner）のための１０００サトシを差し引いたものを彼女自身に支払う。

【００９５】

図１１Ｂをこれから参照すると、ボブからアリスへのトークン化GBPの支払いについてトランザクションテーブルが示されている。ボブはトークン化GBP７５０を有しており、そして、キャロルからのトークン化AUDを必要としている。トランザクションは、トークン化GBP５００をボブからアリスに対して支払い、そして、ボブは彼自身に残りのトークン化GBP２５０（７５０－５００）を支払う。標準BTCを使用して、ボブは、サービスプロバイダの料金（図１１Ｂに示すような定額料金であってよく、または、移転の価値に応じた料金であってよい）を支払うことができ、そして、お釣りからマイナのための１０００サトシを差し引いたものを彼自身に支払う。

【００９６】

図１１Ｃをこれから参照すると、キャロルからボブへのトークン化AUDの支払いについてトランザクションテーブルが示されている。キャロルはトークン化AUD１５００を有しており、そして、アリスからのトークン化CADを必要としている。トランザクションは、トークン化AUD１０００をキャロルからボブに対して支払い、そして、キャロルは彼女自身に残りのトークン化AUD５００（１５００－１０００）を支払う。標準BTCを使用して、キャロルは、サービスプロバイダの料金（図１１Ｃに示すような定額料金であってよく、または、移転の価値に応じた料金であってよい）を支払うことができ、そして、お釣りからマイナのための１０００サトシを差し引いたものを彼自身に支払う。

交換が２つまたはそれ以上の別個のトランザクション（例えば、１：アリスがボブに対して移転し、そして、２：ボブがアリスに対して移転する）から成る場合には、全ての当事者が自身の資格（entitlement）を受け取るか又は誰も受け取らないかのいずれかであることを保証するように、トランザクションがリンクされてよいことが正しく理解されよう。これは、以下の条件を満足することによって達成することができる（２人の当事者、ＡとＢ、の例を使用するが、３人またはそれ以上の当事者まで容易に拡張可能である）：ＡからＢへ移転するトランザクション出力が存在し、かつ、Ｂによって費やすことができるのは、同時に、ＢからＡへ移転するトランザクション出力も存在し、かつ、Ａによって費やすことができる場合だけであり、逆もまた同様である。当事者ＡとＢは、アリスとボブだけでなく、各トランザクションのために必要とされる一式の署名者を参照する（例えば、トークン発行者、エスクロー、等を含む）ことに留意する。

【００９７】

ユーザからの選択の受け取り

【００９８】

図６を参照して上述した例示的な交換の変形においては、オーダーのマッチングのためにP2P DHTを解析する（parsing）サービスプロバイダの代わりに、現在のユーザ自身が現在のインビテーションを見るためにP2P DHTをスキャンまたはブラウズ（browse）することができる。ブラウジングは、交換サービスプロバイダ104といった、第三者によって促進されてよい。第三者は、インターフェイスを提供することができ、ユーザは、興味を持ち得るインビテーションについて、その中で閲覧、スキャン、および検索することができる。

【００９９】

ユーザは、次いで、P2P DHT上で彼ら自身の将来のインビテーション（prospective invitation）を入力するプロセスをスキップすることができるが、代わりに、彼らが関心を持つオーダーと一致又はほぼ一致するインビテーションを作成することを選択することができる。

【０１００】

例えば、先の実施例に続いて、しかし、対照的に、ボブは、ブラウジングまたは検索インターフェイスを介してP2P DHT上でアリスのインビテーションを見つけることができ、

その場合に、ボブは、アリスのものと一致するように自分のインビテーションを入力することができる。ボブは、これをいくつかの方法のうちの１つで行うことができる。一つの実施例においては、オーダーを「受諾（”Accept”）」するためのアリスのオーダーを表示する機能がインターフェイス上に存在してよい。ボブが、アリスがインビテーションのために使用したのと同じ交換サービスプロバイダ104のクライアントである場合には、彼らがボブのｅウォレット（eWallet）（公開鍵、等）に既にアクセスしていることがあり、そして、従って、そうした情報に基づいて一致するオーダー（matching order）を作成することができる。それに応じて、交換サービスプロバイダ110は、インビテーションのマッチングのための引き換えスクリプトを生成し、これを署名のためにボブに対して送付し、署名された引き換えスクリプトを受け取り、そして、トランザクションのために備えてP2P DL上にオーダーを入力することができる。ボブがアリスの交換サービスプロバイダ104のクライアントでない場合には、ボブが必要とされる情報および承認（authorisation）を入力できるようにする機能が提供されてよく、次いで、サービスプロバイダがボブの一致するオーダーを作成できるようにする。図７と図８を参照して上述したのと同じプロセスが、次いで、後に続く。

【０１０１】

上記の例は、BTCをトークン化CADと交換することを説明している。しかしながら、システム100は、あらゆるタイプのトークンについて働くことが正しく理解されよう。例えば、あらゆるタイプの（すなわち、通貨契約だけでなく、任意の契約を表わしている）トークンのためのBTC、あらゆる他のタイプのトークンのための任意のタイプのトークン、商品／サービスのためのBTC、商品／サービスのためのトークン、または、商品／サービスのための商品／サービス、を含んでいる。追加的および理論的に、上記のプロセスは、BTCに対するBTCの交換へ変更することができるが、そうした交換は現実の意味（real meaning）を有さない。

【０１０２】

商品／サービスの交換

【０１０３】

商品／サービスが交換に関与する場合には、上述のトランザクションプロセスに係るわずかな変更が必要とされる。

【０１０４】

そうした場合に、（商品及び／又はサービスの）トランザクションは、交換に関わる商品またはサービスの記述（description）を含んでいる。契約書または権利証書によって表される、トークンとは異なり、記述は、契約を構成するものではない。

【０１０５】

記述は、アイテムを一意的に識別しても、しなくてもよい。例えば、物理的アイテムがトランザクションに関与する場合、その記述は、その物理的アイテムに関連付けられた一意の識別子を明示的に参照することができる。追加的または代替的に、記述メタデータ（description metadata）は、以下のうち１つまたはそれ以上を含んでよい。ａ）提供されるか、または、要求される所望のアイテムの一般的な記述、例えば、「食器洗い機、＜３ ｙｏ（”dishwasher,<3 yo”）」、ｂ）オークションウェブサイトにおける販売について特定のアイテムに対する参照、例えば、「オークションサイト上で売りに出された中古品」、ｃ）アイテムタイプの任意の数、例えば、販売のための１５枚のＴシャツを、単品として又は１５枚までの任意の数量として購買することができると広告すること、ｄ）現金（cash）への参照、任意の特定の通貨におけるもの、ｅ）労働および支払いに係る記述であり、１回の作業完了のたび、もしくは、繰返し又は時間毎の支払いを伴う通常の芝刈り（繰返し作業）のためのもの、または、ｆ）１つまたはそれ以上のキーワード、例えば「食器洗い機」。

【０１０６】

サービスに関して、サービスはトークンと同様にコントラクトによって裏付けられる。それとして、サービスはシェア（shares）へと分割可能であり、そして、分割不可能なサ

ービスは１回限りの仕事（one-time job）、すなわち、分割可能であるが単一シェア（１シェア）を有するもの、であるとみなすことができる。サービスが分割不可能である場合に、サービスはインビテーションおよび交換の目的のトークンとして取り扱われてよい。アイテムがトークンによって裏付けされている場合に、アイテムは、インビテーションおよび交換の両方の目的のトークンとして取り扱われ、そして、不換通貨（fiat currency）のためのトークンといった、他のトークンと同じ方法で交換される。

【０１０７】

一意の識別子と関連付けられた物理的アイテムを含むトランザクションの一つの実施が、これから説明される。先の実施例と同様に、この例において、アリスは、P2P DLおよびP2P DHT上にインビテーションを置くために彼女の交換プロバイダを使用する。このインビテーションは、彼女が一意の識別子ＸＹＺ１２３を有する物理的アイテム、ラファエルの傑作「十字架降架（”Deposition of Christ”）」に関連し得るもの、を２５００ＢＴＣ未満（no more than 2500BTC）で購入するという記述を含んでいる。同様に、ボブは、彼が２４００ＢＴＣ以上（no less than 2400BTC）でアイテムＸＹＺ１２３を販売するというインビテーションのマッチング（matching invitation）を置くことができる。アリスは、P2P DLを閲覧して、アイテム番号ＸＹＺ１２３を持つアイテムを見つけ、そして、この情報に基づいて一致するオーダー（matching order）を置くことができる。もしくは、代替的に、アリスは、その後に第三者、例えば交換サービスプロバイダ、によってマッチングされる一般的なインビテーションを置くことができ、そして、続いて、カタログアイテム番号と記述を含む新たなインビテーションがボブのオーダーと一致するように作成される。

【０１０８】

一意のＩＤを含むトランザクションについて、そうしたIDは、特定の交換サービスプロバイダに対してだけでなく、P2P DL全体にわたっても、永久に一意でなければならないことが正しく理解されよう。従って、一意の識別子がデバイスに対して全くの一意ではない場合（例えば、デバイスのシリアル番号）には、交換サービスプロバイダは、そのデバイスについての一意の識別子を生成することができる。各識別子がP2P DL全体に対して一意であることを保証するために、各交換サービスプロバイダは、例えば、彼らが使用する番号の前につける彼ら独自の一意のコードを有することができ、P2P DL上で広告されている製品を一意的に識別する。

【０１０９】

アリスとボブとの間で一旦合意に至ると、図７から図１０を参照して上述した例示的なトランザクションプロセスに従ってトランザクションが行われる。

【０１１０】

物理的アイテムを含むトランザクションのさらなる実施例が、これから説明される。しかしながら、この例において、アイテムは、それに関連する一意の識別子を有していない。

【０１１１】

インビテーションが複数の類似アイテムを販売するためのオファーを含む場合には、メタデータは、任意の１つのトランザクションを用いて購入することができるアイテムの最大および最小の量を記述するように要求され得る。例えば、アリスは、彼女が、トランザクション毎に少なくとも５枚、Dead Lizard 2015コンサートツアーＴシャツを、それぞれ０．０２５ＢＴＣで１５枚まで売るということを暗示する（inferring）インビテーションを置くことができる。この場合に、メタデータ値は、最小レート（０．０２５ＢＴＣ／１５アイテム）、最大量（Offer-QTY-max（15））、および最小量（Offer-QTY-min（5））を含んでよい。以下の表は、インビテーションに関連付けられたメタデータをまとめている。

Field	Sub-field	Value	コメント
A	ContractType	0x0000FF01	P2P交換オーダーを示す
	ContractPointer		実際の契約ファイルロケーションのIPv6アドレス
	OfferRequestCodes		オファータイプ(4bits)＋リクエストタイプ(4bits)を示すコード化値
	Conditions	00000011_2	ビットフィールドーメタデータフィールドにおける追加条件の存在を示すフラグ
	Rate-min	0.025	BTC/15items
	Rate-max		
C	Offer-QTY-max	15	販売毎のＴシャツの最大数量
	Offer-QTY-min	5	販売毎のＴシャツの最小数量
	Request-QTY-max		
	Request-QTY-min		
D	Offer-Item-ID	01245D2SA	アイテムに関する一意のＩＤ
	Request-item-ID		

【０１１２】
支払トランザクションにおける実際のBTC値が、次いで、交換サービスプロバイダによって計算される。このトランザクションは、実行して交換するためのインビテーションを単に表しているだけなので、トランザクションの実際の値は、例えば、ダスト（dust）ほどに小さくてよい（５４６サトシ）。代替的に、以下で説明するように、値は、インビテーションを保証するためにサービスプロバイダによって必要とされる名目額（nominal amount）であってよい（例えば、そのためアリスは引出しをしないように動機付けられる）。

【０１１３】
さらなる実施例においては、硬貨（現金）の形態における商品を交換することができる。例えば、アリスは、１５０ＢＴＣの最大購入で、カナダドル（トークンではなく硬貨（hard currency））についてビットコインを販売するインビテーションを置くことができる。インビテーションは、追加的に、彼女の店舗の住所（371 Whimsy Avenue、Brentford）だけで交換が行われなければならないというロケーション条件を含んでよい。インビテーションのマッチングを置いた後で、トランザクションを確定するために、ボブは、次いで、ビットコイントランザクションにおける支払いの代わりに、現金を引き渡すためにアリスの店に持ってきてよい。物理的な移転のためにボブとアリスがひとたび彼女の店で会うと、次いで、ボブに対するビットコインの実際のデジタルトランザクションおよびアリスに対する硬貨の移転のデジタル記録が行われてよい。

【０１１４】
他の商品／サービスと交換される商品／サービスを含むトランザクションの場合には、P2P DL上のトランザクションは、記録としてのみ存在し、当事者間のいかなる価値も交換するものではないことが正しく理解されよう（サービスプロバイダ等に対するあらゆる料金とは別に）。ユーザは、システムを使用し、そして、交換が永久に記録されるように、P2P DL上にトランザクションを入力するための名目上のサービス料（nominal service fee）を支払うように選択することができる。

【０１１５】

オリジナルのインビテーショントランザクションは、価値の移転またはイベントの記録としてではなく、インビテーションとしてのみ動作すること、に留意する。交換が物理的アイテムだけを含むように、商品間の交換（goods-for-goods exchange）が行われる場合には、最終的な交換がP2P DL上に記録される必要はない。P2P DLは、最終的な交換においていかなるトランザクションも完了することを要求されないからである。それにもかかわらず、物理的アイテムの交換に対する当事者がP2P DL上に交換を記録することを望む場合には、そうするためのマイナに対する料金を条件として、彼らは、インビテーショントランザクションを互いにそれぞれを費やすことができる。当事者がP2P DL上に最終的な交換を記録することを望まない場合には、インビテーショントランザクションを彼ら自身に戻すように費やすか、または、P2P DL上に未使用のまま残しておくことができる。

【０１１６】

商品に対するBTC、または商品に対するトークンを含む交換の場合には、BTCまたはトークンの値を移転するために、少なくとも１つのトランザクションがP2P DL上で費やされる。この場合に、商品を上乗せする（offering up）インビテーショントランザクションが、費やされてもされなくてもよい。そのインビテーショントランザクションを費やすことによって交換（商品）の価値は移転されないからである。しかしながら、再度、当事者は、移転の恒久的な記録（例えば、販売の領収書）を提供するために、それにもかかわらずトランザクションを費やすように決定することができる。

【０１１７】

上記のトランザクションにおいて費やされた金額は、特にアリスのオファーがビットコインまたはトークンではなく商品／サービスである場合に、いくつかの事例においては提供される金額を表わさないことがある。代わりに、サービスプロバイダは、商品の価値を表す金額のアリスによる「デポジット（”deposit”）」を要求するか、または、別の方法でアリスがオファーを「保証する（”guarantee”）」ことができる場合に名目上の金額だけを必要求するか、もしくは、（ｉｉｉ）サービスプロバイダ自身がアリスのためにビットコインを提供し（彼女はいくらも持っていないかもしれない）、そして、クライアントに対して料金を請求するあらゆる手段によってこの調達コスト（funding cost）をカバーすることができるだろう。

【０１１８】

上述の実施形態においては、ユーザのインビテーションがP2P DHTにおいて公開される。いくつかの実施形態においては、しかしながら、ユーザのインビテーション（例えば、スクリプトおよびスクリプトハッシュ）がウェブサイトにおいて公開され、別のユーザに対して直接的に送付されてよい。

【０１１９】

いくつかの実施形態において、ユーザのインビテーションは、サービスプロバイダによってローカルに保管されてよい。例えば、サービスプロバイダは、特定のユーザだけがユーザのインビテーションの詳細にアクセスすることができるプライベートオークションをホストすることができる。

【０１２０】

この開示が、ユーザ、発行者、商人、プロバイダ、または他のエンティティが特定のアクション（署名、発行、決定、計算、送付、受取、作成、等を含むもの）を実行することを説明する場合に、この用語は、表現の明確化のために使用される。これらのアクションは、これらのエンティティによって操作されるコンピューティングデバイスによって実行されることが理解されるべきである。

【０１２１】

署名（signing）は、暗号機能を実行することを含んでよい。暗号機能は、クリアテキストに対する入力と、秘密鍵（private key）といった、鍵に対する入力を有している。プロセッサは、署名として使用できる数字（number）または文字列（string）を計算するための関数を実行することができる。署名は、次いで、署名されたテキストを提供するた

めにクリアテキストと一緒に提供される。メッセージテキストまたは鍵が１ビット（single bit）だけ変更された場合に、署名は完全に変更される。署名を計算することは計算能力をほとんど必要としないが、所与の署名を有するメッセージを再作成することは事実上不可能である。このように、クリアテキストは、秘密鍵が利用可能である場合にだけ、変更され、そして、有効な署名を伴うことができる。さらに、他のエンティティは、公に利用可能な公開鍵を使用して署名を容易に検証することができる。

【０１２２】

ほとんどの状況において、暗号化および復号化は、暗号化されたメッセージまたはクリアテキストメッセージをそれぞれに表す出力文字列を計算するための暗号関数を実行するプロセッサを含んでいる。

【０１２３】

鍵、トークン、メタデータ、トランザクション、オファー、契約、署名、スクリプト、メタデータ、インビテーション、等は、データメモリ上に保管された数字、テキスト、または文字列として表されるデータを参照する。「ストリング（”string”）」または「イント（”int”）」タイプ、もしくは、他のタイプのプログラムコードにおける変数、または、テキストファイル、といったものである。

【０１２４】

ピアツーピア台帳の一つの実施例は、ビットコインブロックチェーンである。ビットコイン通貨における資金の移転または料金の支払いは、トランザクションから出力される資金または料金を用いてビットコインブロックチェーン上のトランザクションを作成することを含む。ビットコイントランザクションの一つの実施例は、入力トランザクションハッシュ、トランザクション量（amount）、１つまたはそれ以上の宛先（destination）、受取人（payee or payees）の公開鍵、および、入力メッセージとしての入力トランザクションおよび署名を計算するための支払人（payer）の秘密鍵を使用して作成された署名、を含んでいる。トランザクションは、入力トランザクションハッシュがビットコインブロックチェーンのコピーの中に存在すること、および、公開鍵を使用して署名が正しいこと、を確認することによって検証することができる。同じ入力トランザクションハッシュが他のロケーションで既に使用されていないことを保証するために、トランザクションはコンピューティングノードのネットワーク（「マイナ（”miners”）」に対してブロードキャストされる。マイナは、入力トランザクションハッシュが未だに接続されておらず、かつ、署名が有効である場合にだけ、ブロックチェーンにおいてトランザクションを受け入れ、そして、記録する。入力トランザクションハッシュが既に別のトランザクションに対してリンクされている場合に、マイナはトランザクションを拒否する。

【０１２５】

トークンに対して仮想通貨を割り当てることは、割り当てられた仮想通貨およびトランザクションの中のメタデータフィールドにおいて表されたトークンを用いてトランザクションを作成することを含む。

【０１２６】

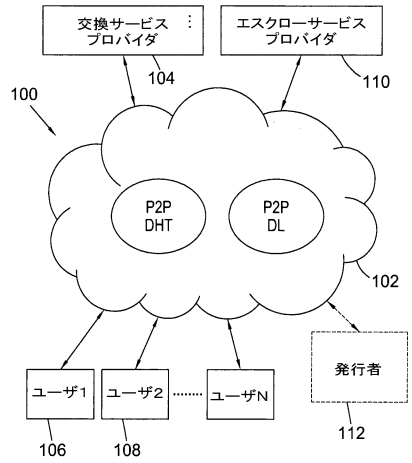
２つのアイテムが関連付けられている場合、このことは、これらのアイテム間に論理結合（logical connection）が存在していることを意味する。データベースにおいては、例えば、２つのアイテムを相互に関連付けるために、２つのアイテムに対する識別子が同じレコードの中に保管されてよい。トランザクションにおいては、２つのアイテムを相互に関連付けるために、２つのアイテムに対する識別子がトランザクション文字列の中に保管されてよい。

【０１２７】

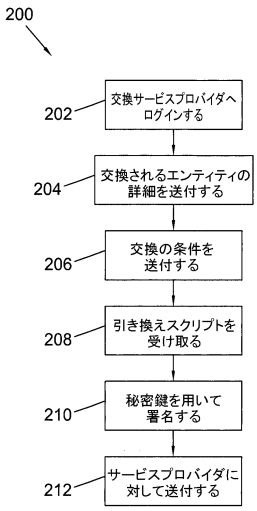
ビットコインプロトコルを使用して、スクリプトを引き換え、かつ／あるいは、トークンをロック解除することは、秘密鍵を使用してスクリプト及び／又はトランザクションの署名文字列を計算することを含んでいる。スクリプトは、異なる秘密鍵または他の条件から派生する２つ以上（more than one）の署名を必要とし得る。このトランザクションの出力は、次いで、マイナに対して提供される。

【０１２８】
別のエンティティを承認すること（authorising）は、秘密鍵を使用してトランザクションの署名文字列を計算すること、および、エンティティがトランザクションを検証するために署名を使用できるようにエンティティに対して署名文字列を提供すること、を含んでよい。
【０１２９】
他のエンティティとのアカウントを有するユーザは、電子メールアドレス、名前、および潜在的に公開鍵、といったユーザに関する情報を保管しているエンティティを含んでよい。例えば、エンティティは、SQL、OrientDB、MongoDB、または他のもの、といったデータベースを維持することができる。いくつかの例において、エンティティは、また、１つまたはそれ以上（one or more）のユーザの秘密鍵を保管することもできる。
【０１３０】
当業者であれば、本開示の広範で一般的な範囲から逸脱することなく、上述の実施形態に対して多くの変形及び／又は変更がなされ得ることが理解されよう。本実施形態は、従って、全ての点で例示的であり、かつ、限定的でないものとしてみなされるべきである。
【０１３１】
ステップ、特徴、インテジャ、混合物及び／又は化合物は、個別に又は集合的に、ここにおいて開示され、または、本出願の明細書において示されており、そして、上記のステップまたは特徴の２つまたはそれ以上のうち任意および全ての組み合わせもそうである。

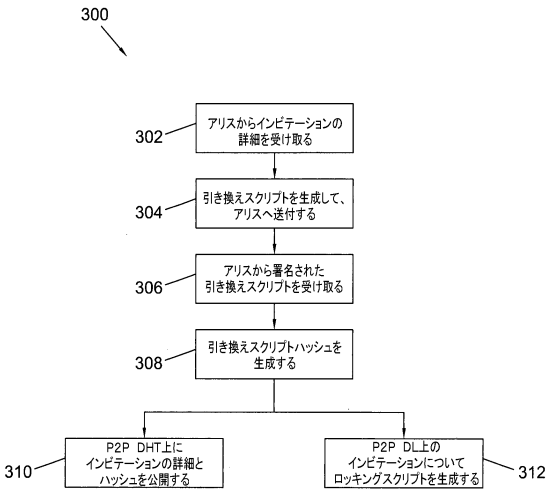
【図１】



【図２】



【図３】



【図４】

アリス

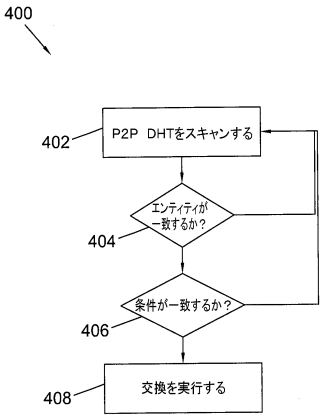
Offer:	BTC
Request:	Token
Offer-type-code	0000_2
Offer-QTY-max	NULL
Offer-QTY-min	NULL
Offer-item-ID	
Rate-min	$4.00000000 \times 10^{-5}$ shares/satoshi
Rate-max	NULL (no maximum - i.e. infinity)
Request-type-code	0001_2
Request-item-ID	CAD1234
Request-QTY-max	10000 shares
Request-QTY-min	NULL (no minimum - i.e. 0)
Offer-Deadline	midnight 31-Dec-2016
オーダーの説明	私は、$400/BTC以上のレートでBTCについてトークン化CADを$1000まで買います。締め切りは、2016年12月31日午前0時です。

【図５】

ボブ

Offer:	TOKEN
Request:	BTC
Offer-type-code	0001_2
Offer-QTY-max	15000 shares
Offer-QTY-min	NULL (no minimum - i.e. 0)
Offer-item-ID	CAD1234
Rate-min	2.43902439×10^2 satoshis/share
Rate-max	NULL (no maximum)
Request-type-code	0000_2
Request-item-ID	
Request-QTY-max	NULL
Request-QTY-min	NULL
Offer-Deadline	NULL
オーダーの説明	私は、$410/BTC未満のレートでトークン化CADを$1500まで売ります。

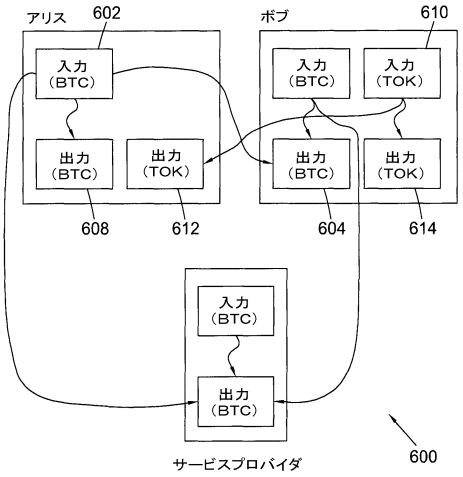
【図６】



【図７】

アリスはボブへBTCを送付する	
ALICE00040	Trancaction-ID
Version number	Version number
1	Number of inputs
ALICE00010	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Alice Sig-Escrowa < OP_2 metadataA metadataB metadataC metadataD metadataE PubK-Alice PubK-EscrowA OP_7 OP CHECKMULTSIG>	ScriptSig
Sequence number	Sequence number
3	Number of outputs
246,913,580 satoshi	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Bob hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
2,469,136 satoshi	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Server hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
3,116,284 satoshi	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Alice hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime
ボブはアリスへトークンを送付する	
BOB00030	Trancaction-ID
Version number	Version number
2	Number of inputs
BOB00010	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Bob Sig-Issuer < 2 metadata1 metadata2 PubK-Bob PubK-Issuer 4 OP_CHECKMULTSIG>	ScriptSig
Sequence number	Sequence number
BOB00010	Prev Trans Output
IDX-01	Prev Trans Output index
Script length	Script length
Sig-Bob PubK-Bob	ScriptSig
Sequence number	Sequence number
4	Number of outputs
10,000,000 satoshi	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash>OP_EQUAL	Output script
5,000,000 satoshi	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash>OP_EQUAL	Output script
10,000 satoshi	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Server hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
880,000 satoshi	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Bob hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

【図８】



【図９】

アリスはボブへBTCを送付する	
Transaction-ID	Trancaction-ID
Version number	Version number
1	Number of inputs
ALICE00010	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Alice PubK-Alice	ScriptSig
Sequence number	Sequence number
3	Prev Trans Output
246,913,580 satoshi	Prev Trans Output index
Output script length	Script length
OP_DUP OP_HASH160 <redeem script hash> OP_EQUAL	ScriptSig
2,469,136 satoshi	Sequence number
Output script length	Number of outputs
OP_DUP OP_HASH160 <PubK-Server hash> OP_EQUALVERIFY OP_CHECKSIG	Output value
50,616,284 satoshi	Output script length
Output script length	Output script
OP_DUP OP_HASH160 <PubK-Alice hash> OP_EQUALVERIFY OP_CHECKSIG	Output value
LockTime	Output script length

ボブはアリスへトークンを送付する	
Transaction-ID	Trancaction-ID
Version number	Version number
2	Number of inputs
BOB00010	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Bob Sig-Issuer < 2 metadata1 metadata2 PubK-Bob PubK-Issuer 4 OP_CHECKMULTSIG>	ScriptSig
Sequence number	Sequence number
BOB00010	Prev Trans Output
IDX-01	Prev Trans Output index
Script length	Script length
Sig-Bob PubK-Bob	ScriptSig
Sequence number	Sequence number
4	Number of outputs
10,000,000 satoshi	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash>OP_EQUAL	Output script
5,000,000 satoshi	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash>OP_EQUAL	Output script
10,000 satoshi	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Server hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
880,000 satoshi	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Bob hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

【図１０】

AB00010	Trancaction-ID
Version number	Version number
3	Number of inputs
ALICE00010	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Alice PubK-Alice	ScriptSig
Sequence number	Sequence number
BOB00010	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Bob Sig-Issuer < 2 metadata1 metadata2 PubK-Bob PubK-Issuer 4 OP_CHECKMULTSIG>	ScriptSig
Sequence number	Sequence number
BOB00010	Prev Trans Output
IDX-01	Prev Trans Output index
Script length	Script length
Sig-Bob PubK-Bob	ScriptSig
Sequence number	Sequence number
7	Number of outputs
246,913,580 satoshi	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Bob hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
2,469,136 satoshi	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Server hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
50,616,284 satoshi	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Alice hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
10,000,000 satoshi	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash>OP_EQUAL	Output script
5,000,000 satoshi	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash>OP_EQUAL	Output script
10,000 satoshi	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Server hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
880,000 satoshi	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Ali hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

Fig. 10

【図１１Ａ】

アリスはキャロルへトークンを送付する	
ALI00010	Trancaction-ID
Version number	Version number
2	Number of inputs
ALI00010	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Ali Sig-Issuer < 2 metadata1 metadata2 PubK-Ali PubK-Issuer 4 OP_CHECKMULTSIG>	ScriptSig
Sequence number	Sequence number
ALI00010	Prev Trans Output
IDX-01	Prev Trans Output index
Script length	Script length
Sig-Ali PubK-Ali	ScriptSig
Sequence number	Sequence number
4	Number of outputs
10,000,000 satoshi	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash>OP_EQUAL	Output script
5,000,000 satoshi	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash>OP_EQUAL	Output script
10,000 satoshi	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Server hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
880,000 satoshi	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Ali hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

アリスはキャロルへトークン化CADで$1000を支払う
（AUD$2/GBPのレートでボブからの彼女のGBPを期待している）。

アリスは自身に残りのトークン化CADを支払う（つまり、お釣り）＝$1500−$1000

標準（非トークン化BTC）を使用して、アリスはサービスプロバイダ料金を支払う
（例えば、フラットレート＝1000サトシ）。

標準（非トークン化BTC）を使用して、アリスはマイナのための1000を残して
900000から自身にお釣りを支払う。

【図１１Ｂ】

ボブはアリスへトークンを送付する	
BOB00030	Trancaction-ID
Version number	Version number
2	Number of inputs
BOB00010	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Bob Sig-Issuer < 2 metadata1 metadata2 PubK-Bob PubK-Issuer 4 OP_CHECKMULTSIG>	ScriptSig
Sequence number	Sequence number
BOB00010	Prev Trans Output
IDX-01	Prev Trans Output index
Script length	Script length
Sig-Bob PubK-Bob	ScriptSig
Sequence number	Sequence number
4	Number of outputs
10,000,000 satoshi	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash>OP_EQUAL	Output script
5,000,000 satoshi	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash>OP_EQUAL	Output script
10,000 satoshi	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Server hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
880,000 satoshi	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Bob hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

ボブはアリスへトークン化GBPでGBP500を支払う
（$2/GBPのレートで彼のAUDを期待している）。

ボブは自身に残りのトークン化GBPを支払う（つまり、お釣り）＝GBP750−GBP500

標準（非トークン化BTC）を使用して、ボブはサービスプロバイダ料金を支払う
（例えば、フラットレート＝1000サトシ）。

標準（非トークン化BTC）を使用して、ボブはマイナのための1000を残して
900000から自身にお釣りを支払う。

【図１１Ｃ】

キャロルはボブへトークンを送付する	
CAR00020	Trancaction-ID
Version number	Version number
2	Number of inputs
CAR00010	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Car Sig-Issuer < 2 metadata1 metadata2 PubK-Car PubK-Issuer 4 OP_CHECKMULTSIG>	ScriptSig
Sequence number	Sequence number
CAR00010	Prev Trans Output
IDX-01	Prev Trans Output index
Script length	Script length
Sig-Car PubK-Car	ScriptSig
Sequence number	Sequence number
4	Number of outputs
10,000,000 satoshi	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash>OP_EQUAL	Output script
5,000,000 satoshi	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash>OP_EQUAL	Output script
10,000 satoshi	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Server hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
880,000 satoshi	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Ali hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

キャロルはボブへトークン化AUDで$1000を支払う
（$1CAD/AUDのレートで彼女のCADを期待している）。

キャロルは自身に残りのトークン化AUDを支払う（つまり、お釣り）＝$1500−$1000

標準（非トークン化BTC）を使用して、キャロルはサービスプロバイダ料金を支払う
（例えば、フラットレート＝1000サトシ）。

標準（非トークン化BTC）を使用して、キャロルはマイナのための1000を残して
900000から自身にお釣りを支払う。

フロントページの続き

(74)代理人 100070150
弁理士 伊東 忠彦
(74)代理人 100091214
弁理士 大貫 進介
(72)発明者 ライト, クレイグ スティーヴン
イギリス国 シーエフ１０ ２エイチエイチ カーディフ チャーチル ウェイ チャーチル ハウス ７ス フロア アーカート－ダイクス アンド ロード エルエルピー 内
(72)発明者 サヴァナ, ステファヌ
イギリス国 シーエフ１０ ２エイチエイチ カーディフ チャーチル ウェイ チャーチル ハウス ７ス フロア アーカート－ダイクス アンド ロード エルエルピー 内

審査官 行田 悦資

(56)参考文献 国際公開第２０１５／１７１５８０（WO, Ａ１）
国際公開第２０１６／００７９０４（WO, Ａ１）
米国特許出願公開第２０１５／０３２４７６４（ＵＳ, Ａ１）
国際公開第２０１４／１３０２２２（WO, Ａ１）
ANTONOPOULOS, A. M., Mastering Bitcoin, ２０１４年１０月 ７日, Early release revision 6, pp.111-138, [online], [検索日：令和3年3月11日], インターネット<URL:https://ungluei t-files.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf>

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０９Ｃ １／００