(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7553055号
(P7553055)

(45)発行日　令和6年9月18日(2024.9.18)

(24)登録日　令和6年9月9日(2024.9.9)

(51)国際特許分類

Ｈ０４Ｌ　9/32　(2006.01)	Ｈ０４Ｌ	9/32	２００Ｚ
Ｇ０６Ｆ　21/64　(2013.01)	Ｇ０６Ｆ	21/64	
Ｇ０６Ｆ　21/44　(2013.01)	Ｇ０６Ｆ	21/44	

ＦＩ

請求項の数　12　（全68頁）

(21)出願番号　特願2021-559657(P2021-559657)
(86)(22)出願日　令和2年3月27日(2020.3.27)
(65)公表番号　特表2022-528711(P2022-528711A)
(43)公表日　令和4年6月15日(2022.6.15)
(86)国際出願番号　PCT/IB2020/052935
(87)国際公開番号　WO2020/212784
(87)国際公開日　令和2年10月22日(2020.10.22)
審査請求日　令和5年2月28日(2023.2.28)
(31)優先権主張番号　16/384,696
(32)優先日　平成31年4月15日(2019.4.15)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　1907180.2
(32)優先日　令和1年5月21日(2019.5.21)
最終頁に続く

(73)特許権者　318001991
エヌチェーン ライセンシング アーゲー
スイス・６３００・ツーク・グラーフェナウヴェーク・６
(74)代理人　100107766
弁理士　伊東 忠重
(74)代理人　100070150
弁理士　伊東 忠彦
(74)代理人　100135079
弁理士　宮崎 修
(72)発明者　ミー，アンディ
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
最終頁に続く

(54)【発明の名称】　分散台帳に関連付けられた宛先アドレッシング

(57)【特許請求の範囲】

【請求項１】

分散台帳に関連付けられたトランザクションに対する１つ以上のクライアントの第１支払いサービスのための能力を更新する、コンピュータにより実施される方法であって、前記方法は、前記第１支払いサービスに関連付けられたプロセッサにおいて、

前記第１支払いサービスに関連付けられた機械可読リソースを更新するステップであって、前記機械可読リソースは、前記第１支払いサービスに関連付けられた予測可能な又は知られている位置で提供され又はそこからアクセス可能である、ステップを含み、

前記機械可読リソースは、

前記１つ以上のクライアントの中のクライアント毎に前記第１支払いサービスを実施することを担うホストコンピューティングリソースに関連付けられた少なくとも１つの識別子であって、各クライアントは該クライアントに固有であるエイリアス及び公開鍵に関連付けられる、１つ以上の識別子と、

前記第１支払いサービスによりサポートされる少なくとも１つの能力に関連付けられたエントリであって、各能力は前記第１支払いサービスに関連付けられた前記１つ以上のクライアントのためのそれぞれの能力を実施するプロトコル又は命令に関連付けられる、エントリと、

前記エイリアスに関連付けられた公開アドレスにアクセスする又はそれを取得するための１つ以上の命令及び／又は仕様であって、前記公開アドレスは前記エイリアスに関連付けられたトランザクションを実現するために使用される、１つ以上の命令及び／又は仕様

と、
を含み、
更新する前記ステップは、前記第１支払いサービスによりサポートされる少なくとも１つの更なる能力を追加するステップを含み、
前記少なくとも１つの更なる能力は、
エイリアスの支払先を要求する支払人エンティティの検証であって、前記１つ以上のクライアントの中の所与のクライアントは前記エイリアスに関連付けられる、検証、及び／又は、
支払人エンティティからの要求の非同時性処理であって、前記要求はエイリアスの支払先に関連付けられ、前記１つ以上のクライアントの中の所与のクライアントは前記エイリアスに関連付けられる、非同時性処理と、
を含む、方法。
【請求項２】
支払人エンティティから、エイリアスに関連付けられた要求を受信するステップであって、前記要求は、前記第１支払いサービスに関連付けられた前記１つ以上のクライアントの中の受取人クライアントの支払先に関連し、前記受取人クライアントは前記要求の中の前記エイリアスに関連付けられる、ステップと、
前記第１支払いサービスによりサポートされる少なくとも１つの能力に基づき、前記支払人エンティティを検証するステップであって、前記少なくとも１つの能力は、前記第１支払いサービスに関連付けられた前記機械可読リソースに含まれる、ステップと、
を含み、
前記検証するステップは、
前記支払人エンティティに関連付けられた公開鍵を取得するステップと、
前記支払人エンティティからの前記要求に基づき、所定の条件が満たされるかどうかを決定するステップと、
を含み、
前記所定の条件が満たされるという決定に基づき、
前記支払人エンティティ及び／又は前記支払人エンティティに関連付けられた前記要求を検証するステップと、
前記受取人クライアントの前記支払先に関連付けられたアウトプットスクリプトを生成するステップと、
前記支払人エンティティへ前記アウトプットスクリプトを送信するステップであって、前記アウトプットスクリプトは前記分散台帳のトランザクションに埋め込むために提供される、ステップと、
を含む、請求項１に記載の方法。
【請求項３】
前記所定の条件が満たされないという決定に基づき、前記方法は、前記支払人エンティティから受信した要求を拒否する応答を生成し及び／又は送信するステップを含む請求項２に記載の方法。
【請求項４】
前記支払人エンティティからの前記エイリアスに関連付けられた前記要求は、以下：
前記要求が前記支払人エンティティにより送信された日時を示すタイムスタンプ、及び／又は、
前記支払人エンティティの前記公開鍵に関連付けられたデジタル署名、及び／又は、
前記要求のためのワンタイムトークン、
を含むHTTP　POST要求である、請求項２～３のいずれか一項に記載の方法。
【請求項５】
所定の条件は、
前記要求に含まれる前記タイムスタンプが前記第１支払いサービスによる前記要求の受信時間の所定の期間内にあることを検証すること、及び／又は、

前記要求の中の前記デジタル署名が前記支払人エンティティの取得された公開鍵に関連することを検証すること、及び／又は、
前記ワンタイムトークンが前の要求のために使用されていないことを検証すること、
を含む、請求項４に記載の方法。
【請求項６】
前記所定の期間は最大２分である、請求項５に記載の方法。
【請求項７】
前記アウトプットスクリプトを送信する前記ステップは、
前記受取人クライアントの公開鍵に関連付けられたデジタル署名を前記アウトプットスクリプトに適用するステップと、
前記支払人エンティティへ、署名済みアウトプットスクリプトを送信するステップと、
を含む、請求項２～６のいずれか一項に記載の方法。
【請求項８】
前記支払人エンティティは、支払人エンティティ支払いサービスに関連付けられ、前記支払人エンティティ支払いサービスに関連付けられたエイリアスを割り当てられ、前記エイリアスは前記支払人エンティティから前記第１支払いサービスへの要求に含まれ、
前記支払人エンティティに関連付けられた公開鍵を取得する前記ステップは、
前記支払人エンティティ支払いサービスに関連付けられた位置から機械可読リソースにアクセスするステップと、
前記機械可読リソースの中の公開鍵基盤（PKI）要求テンプレートに基づき、及び前記支払人エンティティの前記エイリアスに基づき、HTTP GET要求を送信するステップと、
応答して、前記エイリアスに関連付けられた前記公開鍵を取得するステップと、
を含む、請求項２～７のいずれか一項に記載の方法。
【請求項９】
前記支払人エンティティ支払いサービスは、前記第１支払いサービスと異なる第２支払いサービスである、請求項８に記載の方法。
【請求項１０】
前記支払人エンティティ支払いサービスは、前記第１支払いサービスである、請求項８に記載の方法。
【請求項１１】
コンピューティング装置又はシステムであって、
少なくとも１つのプロセッサと、
実行可能命令を含むメモリであって、前記実行可能命令は、前記少なくとも１つのプロセッサによる実行の結果として、前記コンピューティング装置又はシステムに請求項１～１０のいずれか一項に記載のコンピュータにより実施される方法を実行させる、メモリと、
を含むコンピューティング装置又はシステム。
【請求項１２】
実行可能命令を記憶した非一時的コンピュータ可読記憶媒体であって、前記実行可能命令は、システム又はコンピューティング装置のプロセッサにより実行された結果として、前記システム又はコンピューティング装置に、請求項１～１０のいずれか一項に記載のコンピュータにより実施される方法を実行させる、非一時的コンピュータ可読記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、概して、分散台帳に関連付けられたトランザクションを実現する方法及びシステムに関し、特に、１つ以上のデジタルウォレットのための宛先アドレッシングのための方法に関する。本開示は、特に、限定ではないが、受取人から支払人へデジタルアセット移転又は支払いを実現する方法を提供することに適する。
【背景技術】
【０００２】

本願明細書では、私たちは、全ての形式の電子的な、コンピュータに基づく、分散型台帳を包含するために用語「ブロックチェーン」を使用する。これらは、総意に基づくブロックチェーン及びトランザクションチェーン技術、許可及び未許可台帳、共有台帳、並びにこれらの変形を含む。他のブロックチェーン実装が提案され開発されているが、ブロックチェーン技術の最も広く知られているアプリケーションは、Bitcoin台帳である。Bitcoinは、ここでは、便宜上及び説明の目的で参照されることがあるが、本開示はBitcoinブロックチェーンと共に使用することに限定されず、代替のブロックチェーン実装及びプロトコルが本開示の範囲に包含されることに留意すべきである。用語「ユーザ」は、ここでは、人間又はプロセッサに基づくリソースを表してよい。用語「Bitcoin」は、本願明細書では、Bitcoinプロトコルから派生した又はその変形である任意のプロトコルを含むと考えられる。

【０００３】

ブロックチェーンは、コンピュータに基づく非集中型の分散型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り、ブロックにより構成され、ブロックはまたトランザクションにより構成される。各トランザクションは、ブロックチェーンシステムの中の参加者間でデジタルアセットの制御の移転を符号化するデータ構造であり、少なくとも１つのインプット及び少なくとも１つのアウトプットを含む。各ブロックは前のブロックのハッシュを含み、これらのブロックは一緒に繋げられて、起源以来ブロックチェーンに書き込まれている全てのトランザクションの永久的な変更不可能な記録を生成する。トランザクションは、スクリプトとして知られている小さなプログラムを含む。スクリプトは、それらのインプット及びアウトプットを埋め込まれ、トランザクションのアウトプットがどのように及び誰によりアクセス可能であるかを指定する。Bitcoinプラットフォームでは、これらのスクリプトはスタックに基づくスクリプト言語を用いて記述される。

【０００４】

トランザクションがブロックチェーンに書き込まれるためには、検証されなければならない。ネットワークノード（マイナー）は、無効なトランザクションがネットワークから拒否され、各トランザクションが有効であることを保証するために作業を実行する。ノードにインストールされたソフトウェアクライアントは、未使用トランザクション（unspent transaction, UTXO）のロック及びアンロックスクリプトを実行することにより、UTXOに対してこの検証作業を実行する。ロック及びアンロックスクリプトの実行が真（TRUE）と評価する場合、トランザクションは有効であり、トランザクションはブロックチェーンに書き込まれる。従って、トランザクションがブロックチェーンに書き込まれるためには、（ｉ）トランザクションを受信した第１ノードにより検証され、トランザクションが有効な場合には、ノードが該トランザクションをネットワーク内の他のノードに中継する、（ｉｉ）マイナーにより構築された新しいブロックに追加される、（ｉｉｉ）マイニングされる、つまり過去のトランザクションの公開台帳に追加される、ことが必要である。

【０００５】

UTXOとしてブロックチェーンに格納されると、ユーザは、関連する暗号通貨の制御を、別のトランザクション内のインプットに関連付けられた別のアドレスへ移転できる。これは、デジタル暗号通貨ウォレットを用いて度々行われる。このデジタルウォレットは、装置、物理媒体、プログラム、モバイル端末上のアプリケーション（アプリ）、又はインターネットのようなネットワーク上のドメインに関連付けられたリモートにホスティングされたサービスであってよい。デジタルウォレットは、公開及び秘密鍵を格納し、ユーザに関連付けられたアセット等の所有権を追跡し、暗号通貨を受信し又は使用するために使用できる。暗号通貨自体はデジタルウォレットの中に存在しない。Bitcoin及びそれから派生した暗号通貨では、暗号通貨は、公衆に利用可能な台帳、つまりブロックチェーン内で、非中央型に格納及び維持される。知られている暗号通貨ウォレットの種々の形式があり、このようなウォレットのネットワークは、BitcoinSV（BSV）ウォレットのエコシステム（ecosystem）のようなエコシステムと呼ばれる。

【０００６】

現在、ユーザ間、つまりAliceからBobへのBSV、暗号通貨支払いを実現するために、Aliceが、彼女の（秘密及び公開）暗号鍵に関連付けられたデジタルウォレットを有する必要があり、暗号通貨を送信するためのBobの公開アドレス、つまりBobのデジタルウォレットアドレスを知っている必要がある。エンティティに関連付けられた公開アドレス、ここではデジタルウォレットは、通常、アドレス生成プログラムにより自動的に生成される。これらの公開アドレスは、暗号通貨ネットワークにより認識される、トランザクションのために使用される特定のフォーマットの数字列である。例えば、これらは、BSVに基づく暗号通貨ネットワークのためのBitcoinアドレスであってよい。これは、エンティティに関連付けられた非対称秘密／鍵ペアの公開鍵又は公開鍵のハッシュと呼ぶことができる。公開アドレスは公に共有でき、その結果、他のユーザは暗号通貨の支払いをどこへ送信すべきかが分かる。しかしながら、BSVウォレットエコシステム又は他の暗号通貨ウォレットにより認識され使用される公開アドレスは、次のような形式である：

１７Ｄｘ２ｉＡｎＧＷＰＪＣｄｑＶｖＲＦｒ４５ｖＬ９ＹｖＴ８６ＴＤｓｎ

【０００７】

従って、Aliceは、Bobへ暗号通貨を送信するために、このタイプのアドレスを知り又は提供される必要がある。更に、異なるタイプのトランザクションのために、１種類より多くのアドレスが、エンティティ又はウォレットにより使用されることがあり、これらのアドレスは、ブロックチェーンに書き込まれる１つのトランザクションを実現するために１回だけ使用できる。明らかに、これらの公開アドレスは、ユーザフレンドリではなく又はユーザにとって簡単ではなく、或いは覚えやすくない、従って、トランザクションのためのこれらの公開アドレス又は鍵は、トランザクション毎に識別され又は取得され又は導出される必要があり、更に、別のエンティティへの暗号通貨支払いを行いたいエンティティにより特定の期間の間、格納され／キャッシュされる必要がある場合がある。

【０００８】

従って、ブロックチェーンが耐タンパ性及び永久記録のような利点を提供するので、データ及びイベントを記録するためにブロックチェーン技術を使用することが望ましいが、暗号通貨支払いのための宛先アドレスを識別し又は確立する際に困難がある。これは、ウォレットエコシステムにおいて認識されるこれらのアドレスの実施可能なフォーマットが、単純又はユーザフレンドリではないためである。このフォーマットの１つの理由は、デジタル支払いネットワークに渡り適用される公衆IPアドレスのための特定の命名プロトコルと共に、それに合わせたセキュリティである可能性がある。別の理由は、Bitcoinブロックチェーンが、ブロックに構築されるトランザクション（Tx）にデータを各伊能するためである。ブロックチェーンから関連データを識別し、そしてアクセスすることは、トランザクションに関連するエンティティの（秘密鍵にリンクされた）公開アドレスに基づく。本開示は、暗号通貨エコシステムのための改良された宛先識別及び／又は支払いアドレッシングのための態様及び実施形態を提供することにより、これらの技術的懸念を解決する。

【０００９】

本願明細書を通じて、用語「含む」又は「有する」のような変形（comprise、includes、comprises、comprising）は、記載された要素、整数若しくはステップ、又は要素、整数若しくはステップのグループを意味すると理解されるが、任意の他の要素、整数若しくはステップ、又は要素、整数若しくはステップのグループを排除しない。

【発明の概要】

【００１０】

本開示は、分散台帳のためのトランザクションに関連付けられた方法、装置、及び／又はシステムに関する。幾つかの実施形態では、本開示は、受信者エンティティ又は受取人エンティティのエイリアスに関連付けられた要求に対し、送信者エンティティ又は支払人エンティティ検証を実行する方法に関する。これは、要求が、支払人エンティティ、又は支払人エンティティに関連付けられた支払いサービスのようなアドレッシング処理／プロトコル若しくはメカニズムから生じたことをチェックすることを確立することである。実

施形態は、支払人エンティティから要求を送信するステップを含み、要求は受取人エンティティのエイリアスに基づく。実施形態は、要求に含まれるタイムスタンプ及びデジタル署名に基づき、支払人エンティティを検証するステップを含む。検証の成功に応答して、受取人エンティティに関連付けられたアウトプットスクリプトが支払人エンティティに提供される。このアウトプットスクリプトは、トランザクションを生成するために使用されてよく、トランザクションは分散台帳に格納され又はそれにポストされる（post）。

【００１１】

他の実施形態では、本開示は、支払人エンティティにより送信された要求の非同時性又は不連続又は遅延した処理を実施する方法に関する。本実施形態は、支払人エンティティから要求を送信するステップを含み、要求は受取人エンティティのエイリアスに基づく。実施形態は、支払人エンティティへ、通常、要求に固有のトークンの形式で、要求の受信の肯定応答を提供するステップを含む。通知が、要求に関する受取人エンティティへ送信されてよい。この通知は、受取人クライアントが利用不可能である又はオフラインであるときでも、つまりネットワーク若しくはインターネット接続を有しないで、送信される。その結果、該通知は、受取人クライアントがオンラインに戻るとき、受信されアクセスできる。受取人クライアントが要求を認可すると、実施形態は、受取人クライアントに関連付けられたアウトプットスクリプトを生成し及び／又は支払人エンティティに提供するステップを含み、アウトプットスクリプトは、トークンに基づき正しい要求に創刊される。アウトプットスクリプトは、次に、トランザクションを生成するために使用でき、トランザクションは分散台帳に格納され又はそれに記入される（post）。

【００１２】

本開示の更に関連する態様及び実施形態は、以下の詳細な説明において説明される。ここに議論される態様及び実施形態の組合せは、本開示に従い実施されてよい。

【００１３】

１つ以上のプロセッサを含む１つ以上のコンピューティング装置又はシステムは、上述の実施形態を実施するための、コンピュータ可読命令、つまりプログラムを実行するために提供されてよい。

【図面の簡単な説明】

【００１４】

本開示の態様及び実施形態は、単なる例を用いて及び添付の図面を参照して以下に説明される。

【図１】本開示の第１の態様による、支払いサービスを含むようディレクトリを更新する方法を示すフロー図である。

【図２Ａ】支払いサービスの１つ以上のプロセッサにより実施される、支払いサービスを担うホストを識別する方法を示すフロー図である。

【図２Ｂ】支払いクライアントエンティティの１つ以上のプロセッサにより実施される、支払いサービスを担うホストを識別する方法を示すフロー図である。

【図３Ａ】本開示の第２の態様による、支払いサービスの１つ以上のプロセッサにより実施される、エイリアスに関連付けられた公開アドレスを識別する方法を示すフロー図である。

【図３Ｂ】本開示の第２の態様による、支払いクライアントエンティティの１つ以上のプロセッサにより実施される、エイリアスに関連付けられた公開アドレスを識別する方法を示すフロー図である。

【図４】公開鍵基盤シーケンスを示すフロー図である。

【図５Ａ】本開示の第３の態様による、支払いサービスの１つ以上のプロセッサにより実施される、宛先アドレッシングの方法を示すフロー図である。

【図５Ｂ】本開示の第３の態様による、支払いクライアントエンティティの１つ以上のプロセッサにより実施される、宛先アドレッシングの方法を示すフロー図である。

【図６】支払先エンドポイント解決シーケンスを示すフロー図である。

【図７】支払いサービスに関連付けられた能力を更新する方法を示すフロー図である。

【図８】本開示の第４の態様による、支払いサービスの１つ以上のプロセッサにより実施される、支払人エンティティを検証する方法を示すフロー図である。
【図９】本開示の第４の態様による、支払人エンティティの１つ以上のプロセッサにより実施される、支払人エンティティを検証する方法を示すフロー図である。
【図１０】本開示の第５の態様による、支払いサービスの１つ以上のプロセッサにより実施される、非同時性要求処理の方法を示すフロー図である。
【図１１】本開示の第５の態様による、支払人エンティティの１つ以上のプロセッサにより実施される、非同時性要求処理の方法を示すフロー図である。
【図１２】本開示の第５の態様による、受取人クライアントの１つ以上のプロセッサにより実施される、非同時性要求処理の方法を示すフロー図である。
【図１３】支払いサービスのクライアントに関連付けられた公開鍵を検証する処理を示すフロー図である。
【図１４】種々の実施形態が実装できるコンピューティング環境を示す概略図である。
【発明を実施するための形態】
【００１５】
添付の請求の範囲は、以下に詳細に議論される第４及び第５の態様に関連するが、第１、第２、及び第３の態様についての詳細な議論は、請求される態様及び本開示の関連する実施形態の全体及び完全な理解を読者に提供するためにここに提供される。
【００１６】
本開示の第１の態様によると、分散台帳に関連付けられたトランザクションのための１つ以上のクライアントに対するアドレッシング処理又はプロトコルを実施する、コンピュータにより実施される方法が提供される。アドレッシング処理は、１つ以上のクライアントに対する支払いサービスとして参照される。これは、本開示の幾つかの態様及び実施形態が、あるエンティティから別のエンティティへの、暗号通貨のようなデジタルアセットの移転に関連付けられたトランザクションに関するからである。しかしながら、用語「支払いサービス（payment service）」は、デジタルアセットの支払いのためのメカニズムに限定されると考えられるべきではなく、任意のエンティティ又はクライアントが別のエンティティ又はクライアントへ要求を送信する又はそれと通信するためのアドレッシングメカニズムを実現するエンティティ又は処理（プロセス、process）として考えられる。ここで、このような通信は、分散台帳、つまりブロックチェーンに格納され、又は関連付けられ、又は提出されてよい。用語「サービス」は、機能にアクセスし又は操作したいと望む１つ以上のコンピューティング装置により使用される及び１つ以上のコンピューティング装置のための、及び／又はそのような機能にアクセスすることを要求する１つ以上の処理又はプロトコル又は機能の提供として理解される。
【００１７】
同様に、用語「支払人（payer）」は、支払いを行うエンティティに限定されると考えられるべきではなく、要求又は通信又はトランザクション要求の送信側として理解される。用語「受取人（payee）」も同様に、送信側からの要求又は通信の受信側として理解される。単に本開示の態様及び実施形態の説明を容易にするために、用語「支払いサービス（payment service）」、「支払いクライアント（payer client）」、「受取人クライアント（payee client）」は、以下を通じて使用されるが、限定的に考えられるべきではなく、上述を包含する。
【００１８】
第１の態様の方法は、所与のクライアントのためのエイリアスを提供するステップを含み、エイリアスは所与のクライアントに固有であり、エイリアスはネットワーク識別子を含み又はそれに関連する。方法は、次に、エイリアスをディレクトリ内のネットワーク識別子に関連付けるステップを含む。この関連付けは、ディレクトリ内のネットワーク識別子に基づきサービスレコードを生成するステップにより達成される。サービスレコードは、次に、支払いサービスがネットワーク識別子に関連付けられたネットワーク又はドメイン、及び支払いサービスを担うホストコンピューティングリソースの位置により提供され

ることを示すために更新される。ここで、ホストコンピューティングリソースは、エイリアスに関連するトランザクションに関する要求の受信に応答して、エイリアスに関連付けられたクライアントの識別を実現するよう構成される。

【００１９】

幾つかの実施形態では、上述の１つ以上のクライアントは、コンピューティングリソース、コンピューティングリソースに関連付けられたユーザ端末又はアプリケーションのような１つ以上のエンティティに関連する。幾つかの実施形態では、各クライアントは、デジタルウォレットであってよく、又はデジタルウォレットに関連付けられたエンティティ、例えばインストールされたデジタルウォレットのためのデジタルウォレット若しくはアプリケーションを有するユーザ端末であってよい。本開示の態様及び実施形態はデジタルウォレットに関連するが、理解されるべきことに、デジタルウォレット又はそのための別個のアプリケーションを有しないが、デジタルウォレットとして又はそれと共に又はそれと同様に動作する機能を提供するよう構成されるクライアントエンティティも、本開示の範囲内にある。単に説明を容易にするために、以下の説明は、デジタルウォレット（デジタルウォレットに関連付けられたクライアントエンティティ）に関連するが、本開示は、デジタルウォレットを有するクライアントエンティティのみに限定されない。

【００２０】

第１の態様において上述した１つ以上のデジタルウォレットは、時に複数のBitcoinBSV暗号通貨ウォレットのウォレットエコシステムのようなデジタルウォレットのエコシステムと呼ばれるネットワーク内の複数のデジタルウォレットのうちの１つである。他の実施形態では、ウォレットは、ウォレットのネットワークの部分でなくてよく、単にドメインに関連付けられた別個の独立したエンティティであってよい。いずれの場合にも、ネットワーク識別子は、ネットワークのドメイン名、例えばnchain.comであってよく又はそれを含んでよい。幾つかの実施形態では、ディレクトリは、DNS（Domain naming system）のような公開型、つまりアクセス可能及び／又は非中央型システムであってよく、グローバルディレクトリと呼ばれてよい。ホストコンピューティングリソースの位置は、ネットワークの支払いサービスの提供を担うサーバの位置であってよい。例えば、これは、エンドポイントURI（universal resource identifier）であってよく、ウェブサーバのURL（universal resource location）を含んでよく、そこから支払いサービスが他のエンティティによりアクセスされてよい。例えば、他のエンティティは、ネットワーク識別子、１つ以上の支払いサーバ若しくはクライアントエンティティ、又は支払いアプリケーションに関連付けられたネットワークの部分であってよい又はそうでなくてよいデジタルウォレットであってよい。

【００２１】

有利なことに、第１の態様は、１つ以上のデジタルウォレットのドメインオーナが、ワンタイムアクティビティとして、つまりサービスレコード（SRVレコード）の生成により、デジタルウォレットに関連付けられた要求側（支払人、payer)エンティティから宛先（受取人、payee）エンティティへの支払いトランザクションのようなトランザクションを実現するための１つ以上の機能を管理する支払いサービスを使用することを可能にする。サービスのエンドポイントを識別するためのDNS内のサービスレコードはよく知られているが、このようなレコードは、ブロックチェーンに関連付けられた支払いトランザクションを可能にするために使用され又は構成されていない。

【００２２】

有利なことに、上述の態様は、受取人エンティティ又は受取人に関連付けられたデジタルウォレットをアドレス指定するために、支払いトランザクションに関する要求が、エイリアスを用いて生成されることを可能にする。従って、要求側（支払人エンティティ）は、分散台帳のための暗号通貨トランザクションを成し遂げる又は構成するために、デジタルウォレットのための複雑な公開アドレス、つまり１７Dx２iAnGWPJCdqVvRFr４５vL９YvT８６TDsnを知り、取得し又は保存する／キャッシュする必要がない。その結果、暗号通貨支払いがこのウォレットに対して行うことができる。ネットワークの又はそれに関

連する、受取人にとって記憶しやすいエイリアス、例えば受取人の電子メールアドレス（name@domain.com）に関連し得るものが、支払いトランザクションを要求するために要求側エンティティにより知られ又は送信される必要があるだけである。エンティティを識別する他のフォーマットも、エイリアスとして使用されてよい。この種のエイリアスアドレッシングは、支払先のアドレスを解決するための遙かに簡単でユーザフレンドリな技術を提供する。幾つかの実施形態では、ネットワーク識別子がエイリアスの中で明示されない場合でも、エイリアスがネットワーク識別子に関連付けられる限り、つまりディレクトリ又はデータベースの検索により、これは、エイリアスに関連付けられた支払いサービスを識別するのに十分である。

【００２３】

幾つかの実施形態では、方法は、エイリアスに関連付けられたトランザクションに関する要求側エンティティからの要求に応答して、エイリアスに基づきディレクトリの検索を実行するステップを含む。トランザクションに関する要求は、分散台帳、つまりブロックチェーンにポストされる（post）べきトランザクションを生成し又は構成するために必要な情報に対する要求を表す。従って、この要求は、ブロックチェーントランザクション自体を生成せず、単に将来のトランザクションに対する又はそれに関する単なる要求、つまり、将来にブロックチェーンにポストされるべきトランザクションを生成するための情報に対するオフブロック要求である。これは、ブロックチェーンのための将来のトランザクションについての要求であると理解される。参照を容易にするために、以下の説明は、このステップを説明するためにトランザクションについての要求を議論する。この要求はブロックチェーンのための将来のトランザクションに関連することが理解される。方法は、ネットワーク識別子に関連するディレクトリ内の支払いサービスについてのサービスレコードを識別するステップと、支払いサービスのためのホストコンピューティングリソースの位置を返すステップと、を含む。返された位置に基づき、エイリアスに関連付けられたデジタルウォレットに関連付けられた公開アドレスが決定できる。これは、幾つかの実施形態では、分散台帳、つまりBitcoinブロックチェーンのための将来のトランザクションに関連付けられてよい公開アドレスに対応する。幾つかの実施形態では、ホストコンピューティングリソースの位置を返すステップは、ターゲット及びポートペアを返すステップを含む。ここで、ターゲットは、ホストコンピューティングリソースの識別子を含み、ポートは、支払いサービスにより使用されるインターネットプロトコル通信ポートの識別子を含む。

【００２４】

有利なことに、これは、受取人エンティティのエイリアスだけに基づき、支払いサービスを提供することを担うホストの発見を可能にし、受取人エンティティへの支払いトランザクションを実現する。それにより、デジタル台帳のための支払いトランザクションの支払いアドレッシングを有意に簡略化する。ホストが特定されると、デジタルウォレットはネットワーク又はネットワーク識別子に関連付けられ、それにより支払いサービスに関連付けられるので、受取人エンティティのクライアント又はデジタルウォレットに関連付けられた公開アドレスが、決定できる。ここで言及される用語「公開アドレス」は、デジタルウォレット又はクライアントのアイデンティティ又はアドレスに関連し、幾つかの実施形態では、分散台帳のための１つ以上の（将来の）トランザクションに関連する。幾つかの実施形態では、公開アドレスは、クライアント又はデジタルウォレットの支払いアドレス又は宛先アドレスであってよい。他の実施形態では、公開アドレスは、支払い又は宛先アドレスを導出するために使用されてよい。この公開アドレスは、同じであってよく、又はデジタルウォレットに関連付けられたトランザクション毎に異なってよい。

【００２５】

幾つかの実施形態では、本開示の第１の態様による方法は、支払いクライアントエンティティにおいて実施される方法を含む。これは、暗号通貨のためのデジタルウォレットに関連付けられた要求側エンティティであってよい。この場合、支払いクライアントエンティティにより実施される方法は、要求側エンティティから、トランザクションについての

要求を送信するステップを含み、要求はエイリアスに関連付けられる。方法は、支払いサービスに関連付けられたホストコンピューティングリソースの位置を取得するステップを含み、位置は、ディレクトリの検索において識別されるネットワーク識別子に関連するサービスレコードに基づく。方法は、次に、エイリアスに関連付けられたデジタルウォレットの公開アドレスを受信するステップを含み、公開アドレスは、以後、要求されたトランザクションにおいて使用される。

【００２６】

幾つかの実施形態では、ホストコンピューティングリソースは、１つ以上のデジタルウォレットに関連付けられたネットワーク識別子と異なる支払いネットワークに関連付けられ、ネットワーク識別子に関連付けられたドメインに登録された複数のエンティティのための支払いサービスは、支払いネットワークに関連付けられたドメインに委任される（delegated）。

【００２７】

有利なことに、これは、ネットワークが、エイリアスに基づく支払いを、完全に異なるドメインに関連付けられた第三者ネットワークにより管理され及び提供されるよう委任することを可能にする。

【００２８】

代替の実施形態では、ホストコンピューティングリソースは、ネットワーク識別子のドメインと同じドメインに関連付けられる。代替として、ドメインオーナは、ネットワーク内で支払いサービスを実施することを選択してよい。この場合、サービスレコードの中のエンドポイント識別子は、（デジタルウォレットの）ネットワークと同じドメインに設定され又はそれを参照するよう更新される。有利なことに、エイリアスに基づく支払いサービスを担うホスト又はエンドポイントを示すためにサービスレコードを使用することは、デジタルウォレット又はデジタルウォレットのネットワークについて支払いサービスプロバイダを追加又は変更することを直接的にする。サービスレコードが更新されると、要求又はルックアップ検索は、新しいホスト位置がサービスレコード内で示されれば、シームレスに継続できる。

【００２９】

第２の態様によると、本開示は、分散台帳を使用するトランザクションのための、１つ以上のデジタルウォレットのために支払いサービスを実施する、コンピュータにより実施される方法に関し、当該方法は、支払いサービスに関連付けられた機械可読リソースを生成するステップであって、機械可読リソースは、１つ以上のデジタルウォレット（又はネットワーク）内のデジタルウォレット毎に、支払いサービスを実施することを担うホストコンピューティングリソースのエンドポイント識別子を含み、各デジタルウォレットはエイリアスに関連付けられる、ステップを含む。機械可読リソースは、支払いサービスによりサポートされる複数の能力の中の少なくとも１つの能力に関連付けられたエントリを更に含む。機械可読リソースは、エイリアスに関連付けられたトランザクションを実現するための公開アドレス又は位置又は１つ以上のリソースにアクセスするための命令及び／又は仕様を更に含む。方法は、支払いサービスのためのホストコンピューティングリソースに関連付けられた予測可能な又は知られている位置にある機械可読リソースを提供するステップを更に含む。

【００３０】

幾つかの実施形態では、各能力は、名称及び値ペアとして、機械可読リソースの中で指定される。幾つかの実施形態では、能力は、一部又は全部のトランザクションについての受取人エンティティ又は支払人エンティティ検証、トランザクションの複数のデジタル署名のための機能、受取人エンティティ又は支払先認可及び／又は電子メールに基づく支払いトランザクションを含み、その結果支払いクライアントは電子メール等を介してトランザクションスクリプトを取得してよい。

【００３１】

有利なことに、第２の態様は、１つ以上のデジタルウォレットのために実施される所与

の支払いサービスに関連付けられた１つ以上の能力又は機能を発見する手段を提供する。第１の態様と同様に、要求側エンティティにより要求されるのは、支払人又は宛先エンティティのエイリアス、つまり受取人のデジタルウォレットに関連付けられたエイリアスだけである。従って、ユーザフレンドリな簡略化されたアドレッシングメカニズムを提供する。この利点は、デジタルウォレットのために実施される支払いサービスにより提供される機能又は能力を指定する公衆アクセス可能な機械可読リソースの提供により保証される。受取人エンティティのエイリアスのみの知識に基づき支払いサービスの能力を発見するこの第２の態様は、デジタルウォレットに関連付けられた支払人エンティティが、移転の要求が行われる前に、エイリアスに対する支払いを行うとき、トランザクションのための能力又は機能がサポートされることを保証したいと望む場合に、特に有用である。特定の機能は、分散台帳に関連付けられた暗号通貨支払いトランザクションを実現するため、例えば支払いサービスに関連付けられた少なくとも１つのエンドポイント識別子を特定するため、又はPKI（public key infrastructure）等に基づくセキュア通信メカニズムを実施するための鍵と考えられる。これらの機能は、多くの場合、機械可読リソースの中の能力エントリと別個に指定される。有利なことに、能力エントリは、利用可能な全部のサポートする機能の仕様、つまりレコードの提供を可能にする。例えば、検証の特定のタイプ、指定されたタイプのトランザクション又はネットワークのための追加セキュリティ、暗号化のレベル、サポートされるPKIアーキテクチャのタイプ、アドレッシングのレベル、等を構成するための詳細事項は、能力オブジェクトの中で提供されてよい。従って、要求側エンティティは、エイリアスに関連付けられた要求される能力が先ず要求側エンティティのリソースと互換性があること、次にエイリアスの支払いサービスに関連付けられた機械可読リソースにアクセスすることによりエイリアスを有する任意のトランザクションに提供されることを、発見し保証できる。

【００３２】

幾つかの実施形態では、第２の態様の方法は、第１の態様及び上述の関連する実施形態による支払いサービスに関連付けられたほすとの位置を決定するステップを含む。従って、機械可読リソース内のエンドポイント識別子は、次に、決定したホスト位置に関連して取得される。

【００３３】

有利なことに、本実施形態は、先ず、ディレクトリ、つまりサービスレコードのDNSのルックアップに基づきホストの発見を可能にし、続いて、支払いサービスによりサポートされる１つ以上の機能の能力発見を可能にする。従って、エイリアスに関連付けられた支払いトランザクションについての要求を受信すると、エイリアス内のネットワーク識別子に一致するサービスレコードが識別され、これは、ホストの位置を提供し、またエンドポイント識別子を取得可能にする。第２の態様による能力発見は、次に、機械可読リソースないのエンドポイント識別子に基づき実行される。

【００３４】

ホスト発見のための第１の態様による方法は、第２の態様に従い機械可読リソースに基づく能力発見が実行される前に、実行され得る多くのホスト発見方法のうちのほんの１つであることが理解される。従って、第１の態様は、第２の態様と独立して実行可能であり、逆も同様である。好適な実装は、上述のホスト及び能力発見の両方を含んでよいが、この組合せは、エイリアスに関連付けられた支払いサービスの能力を確立するために必須ではない。ホスト発見の他の方法も、ホスト位置を識別するための第１の態様におけるサービスレコードの使用に加えて、第２の態様と互換性があってよい。例えば、ホスト位置の指定されたネットワークパスにおけるテキストに基づくレコードが、第１の態様で議論したサービスレコードに基づく実装の代わりに使用されてよい。更に、エンドポイント識別子を解決するホスト発見は、幾つかの実施形態では例えばホストの位置が容易に発見可能である又は公開されている、又は１つ以上のデジタルウォレットと同じドメインに関連付けられている場合に、第２の態様では一緒にスキップされてよい。

【００３５】

従って、以下の説明される実施形態は、第２の態様のみに基づくか、又は上述の第１及び第２の態様の組合せに基づくと理解される。

【００３６】

幾つかの実施形態では、エイリアスに関連付けられたトランザクションについての要求側エンティティからの要求を受信することに応答して、方法は、ネットワーク識別子に基づき、エイリアスに関連付けられた支払いサービスを識別するステップを更に含む。次に、支払いサービスを識別することに基づき、方法は、予測可能な又は知られているネットワーク位置から機械可読リソースにアクセスするステップを含む。要求されたトランザクションのために必要な１つ以上の能力が機械可読リソース内に存在するかどうかを決定すると、方法は、支払いサービスのためのホストコンピューティングリソースのエンドポイント識別子を返すステップと、これに基づき、機械可読リソース内の命令及び／又は仕様のうちの１つ以上に従い、エイリアスに関連付けられた公開アドレスを取得するステップと、を含む。

【００３７】

有利なことに、上述の実施形態は、エイリアスのみを知り、受取人エンティティに連絡ｓルための更なる情報を知らずに、エイリアスに関連付けられた公開アドレスを取得することを可能にする。更に、機械可読リソース内の１つ以上の能力が要求側エンティティ又はトランザクションの１つ以上の要件に従うことを決定するために、公開アドレスは、支払いサービスに関連付けられた機械可読リソースからエンドポイント識別子に基づき取得される。これは、それによって、エイリアスだけを有するエンティティの公開アドレスを取得しそれにより開始するためのシームレスな、簡略化された、ユーザフレンドリな技術を提供する。

【００３８】

上述の実施形態は、要求側クライアント支払いエンティティ、つまり支払いの要求を生成する支払人エンティティにおいて実施されてもよい。この場合、方法は、トランザクションについての要求を要求側エンティティから送信するステップを含み、要求はエイリアスに関連付けられる。方法は、支払いサービスに関連付けられた位置から機械可読リソースにアクセスするステップを含み、支払いサービスはエイリアス内のネットワーク識別子に基づき識別され、機械可読リソースは、第２の態様について上述したように生成される。次に、要求されたトランザクションのために必要な１つ以上の能力が機械可読リソース内に存在するかどうかを識別することに基づき、要求側エンティティは、エイリアスに関連付けられた支払いサービスのためにホストコンピューティングリソースのエンドポイント識別子を受信する。方法は、機械可読リソース内の命令及び／又は仕様のうちの１つ以上を用いて、エイリアスに関連付けられた公開アドレスを取得するステップを含む。

【００３９】

幾つかの実施形態では、各デジタルウォレットは、ネットワーク内の支払いサービスのために登録されたユーザ又はエンティティに関連付けられ、各デジタルウォレットは、分散台帳上のトランザクションのための非対称暗号鍵ペアの公開鍵及び秘密鍵に関連付けられた暗号通貨ウォレットである」。幾つかの実施形態では、公開アドレスを取得するステップは、エイリアスに関連付けられたデジタルウォレットの公開鍵を取得するステップを含む。幾つかの実施形態では、エイリアスに関連付けられた公開アドレスは、エイリアスに関連付けられたデジタルウォレットの公開鍵の暗号ハッシュに基づく。関連する実施形態では、デジタルウォレットの公開鍵は、楕円曲線デジタル署名アルゴリズム（elliptic curve digital signature algorithm (ECDSA)）公開鍵であり、公開鍵は、分散台帳に前に格納された又はそれにポストされた任意のトランザクションの部分ではない。

【００４０】

幾つかの実施形態では、能力発見の第２の態様に関連して、機械可読リソース内の命令及び／又は仕様はエイリアスに関連付けられた公開鍵を取得する後続のステップを含む。これらのステップは、PKI（public key infrastructure）エンドポイント識別子について、機械可読リソースからPKI要求テンプレートを取得するステップを含む。次に、完全

なPKI要求を生成するために、エイリアス及びネットワーク識別子は、テンプレートに含まれる。次に、エイリアスに関連付けられた公開鍵を取得するために、完全なPKI要求に基づき、HTTP GET要求が送信される。

【００４１】

関連する幾つかの実施形態では、能力発見の第２の態様に関連して、PKIに関連する機械可読リソース内の命令及び／又は仕様は、公開鍵が、所与の支払いクライアントについて、依然として有効なアイデンティティ鍵であることをチェックし又は検証するための命令を含む。言い換えると、本実施形態は、所与の公開鍵のオーナを検証することに関する。幾つかの実施形態では、チェックされるべき公開鍵は、同じ又は異なるトランザクションに関連して、上述の実施形態に基づき前に取得された公開鍵に関連する。幾つかの実施形態では、チェックされるべき公開鍵は、将来の使用のために１つ以上の支払いクライアントによりキャッシュされ又は格納されてよい公開鍵に関連する。幾つかの実施形態では、公開鍵の検証は、公開鍵が取得され又は検証されてから、設定された時間期間が経過した場合に、実行されてよい。幾つかの実施形態では、この検証は自動的にトリガされてよい。このような検証のための方法のステップは、このような検証のためのエンドポイント識別子のために、機械可読リソースから公開鍵検証要求テンプレートを取得するステップを含む。幾つかの実施形態では、これは、上述のPKIエンドポイント識別子であってよい。完全な公開鍵検証要求を生成するために、エイリアス及びネットワーク識別子は、テンプレートに含まれる。次に、エイリアスに関連付けられた公開鍵が依然として有効であることを証明するために、完全な公開鍵検証要求に基づき、HTTP GET要求が送信される。幾つかの実施形態では、生成されたこの要求に応答して、エイリアスに関連付けられた公開鍵が実際に正しいかどうか、つまり、要求内の公開鍵がエイリアスに関連付けられた現在の公開鍵と一致するかどうかが、「真」又は「偽」、又は「１」又は「０」を示すことにより示される。

【００４２】

有利なことに、上述の実施形態は、支払いクライアントにかつて関連付けられた可能性のある古い、無視された、又は廃棄された鍵、及び支払いエンティティにより、例えばPKI要求テンプレートに基づき取得された有効性が、悪用される、又は１つ以上のクライアント又はデジタルウォレットへ送信されないことを保証するので、支払いサービスについてのセキュリティ、精度、並びに信頼性を向上する。公開鍵検証又は公開鍵のオーナの妥当性確認のためのこのような要求は、支払いエンティティにより意図されるトランザクションの重要性又は機密性に依存して設定された間隔で、つまり２４時間毎に又は毎週、又は支払いサービスに関連付けられたクライアントの公開鍵が最後に取得され又は検証されたときから特定の時間量が経過した後に、自動的に実行できる。この自動的又は定期的検証は、現在の鍵だけがトランザクションに使用されることを保証し、支払いエンティティに提供された任意の公開鍵に関する情報の新鮮さも保証する。他の実施形態では、検証は、単に、要求又は検証の要求を行う支払いエンティティにより設定された１つ以上の要件に基づき実行されてよい。公開鍵検証についてのこのような上述の実施形態は、所与のエイリアスの公開鍵が時間と共に変化し得る場合に特に有用である。これは、古い鍵を用いて署名されたデータを検証しようとするとき、これらの古い鍵がセキュアに取得された場合でも、以上に議論したように、取得した公開鍵が実際に正しいユーザ、つまりエイリアスに関連付けられたクライアントに属するかどうかを確かめることが不可能なので、厄介である。

【００４３】

理解されるべきことに、上述の命令及び／又は仕様は、支払いサービスに関連付けられた機械可読リソース内に存在するが、命令は、支払いクライアントエンティティに関連付けられた１つ以上のコンピューティングリソース又はアプリケーションにより実行されることを目的としてよい。これらの命令を実行する１つ以上のコンピューティングリソースは、支払いクライアントエンティティのデジタルウォレットにインストールされた又はそれに関連付けられた支払いクライアントアプリケーションに関連付けられてよい。

【００４４】
有利なことに、支払いサービスに関連付けられた機械可読文書（document、ドキュメント）の提供は、知られているエイリアスを利用して、受取人エンティティの公開鍵を取得するための、支払いサービスに対する、指定されたフォーマットの適切な要求を生成することを可能にする。該公開鍵は、分散台帳のためのトランザクションに署名するために必要とされる。
【００４５】
幾つかの実施形態では、機械可読リソースの知られている又は予測可能な位置は、エンドポイント識別子、支払いサービスにより使用されるインターネットプロトコル通信ポート、及び／又は公衆アクセス可能なよく知られたドメインレポジトリに含まれる支払いサービスの構成仕様、のうちの少なくとも１つに基づく。有利なことに、以上は、機械可読リソースが、ネットワーク識別子に関連付けられた支払いサービス又はドメイン名のいずれかに基づき容易に位置を特定することを可能にする。
【００４６】
幾つかの実施形態では、機械可読リソースは、JSON（Java Script Object Notation）フォーマットを用いて生成される。これは、JSONが、第一に機械可読言語であるが、更に人間にとって読み書きが容易である軽量なデータ交換フォーマットであるため、有利である。それは、機械にとってパースし及び生成することが容易であり、それにより、機械可読リソースを生成するのに利用的なデータ交換言語である。
【００４７】
第３の態様では、本開示は、支払先アドレッシングのための技術を提供する。この第３の態様は、機械可読リソースが支払先をアドレス指定することを解決するために、つまり支払いを送信するために使用されるので、能力発見の第２の態様に関連する。任意で、第３の態様は、ホスト発見の第１の態様も含んでよいが、これは、ホスト発見の他の手段も本開示の第３の態様と組み合わせて使用されてよいので、品質的ではない。
【００４８】
本開示の第３の態様は、上述の第２の態様におけるエイリアスに関連付けられた公開アドレスを取得するステップが、エイリアスに関連付けられた受取人エンティティの支払先を取得するステップを更に含み、支払先は、支払人エンティティからエイリアスへの暗号通貨支払いを行うためのトランザクションを構成する際に使用される、ステップを含む、方法を提供する。第３の態様に従いトランザクションを構成するステップは、支払いサービスを識別することに基づき、機械可読リソースにアクセスするステップを含む。この後に、機械可読ドキュメント内の１つ以上の命令及び／又は仕様に基づき、支払先エンドポイント識別子を返すステップが続く。支払人エンティティからのトランザクションに関する支払いの詳細が次に取得される。支払いの詳細は、少なくとも、受取人エンティティのデジタルウォレットに関連付けられたエイリアス、及び受取人に支払われるべき暗号通貨額を含む。支払いの詳細を支払人エンティティの暗号鍵に関連付けるデジタル署名が次に取得される。エイリアスに関連付けられた支払先エンドポイント識別子に関連付けられたアウトプットスクリプトは、次に、支払人エンティティに提供するために生成される。アウトプットスクリプトは、分散台帳のための支払いトランザクションの中に埋め込まれるために提供される。
【００４９】
有利なことに、第３の態様はエイリアスに関連付けられたデジタルウォレットのアウトプットスクリプトの受信が得られることを可能にし、それにより、デジタル台帳に包含するのに適切なフォーマットのトランザクションの構成を自動的に可能にする。これは、単に受取人のエイリアスの知識に基づき、残りの詳細は、支払いサービスを担うホストに関連付けられた機械可読リソースから確立される。更に、エイリアスの知識と共にトランザクションに含まれるべき準備のできたアウトプットスクリプトの提供を可能にすることは、それだけで、デジタルウォレットのための支払いアドレッシングの技術に基づき、全体的に簡略化された、シームレスな、効率的な、自動的な、実装の容易な、ユーザフレンド

リなエイリアスを提供する。

【００５０】

第３の態様の方法は、トランザクションを要求する支払いクライアントエンティティに関連付けられたデジタルウォレット又はアプリケーション又はプロセッサのような、支払いクライアントエンティティにおいて又はそれにより実装されてもよい。この場合、トランザクションを構成する方法は、トランザクションについての要求を支払人エンティティから送信するステップを含み、要求はエイリアスに関連付けられる。方法は、支払いサービスに関連付けられた位置から機械可読リソースにアクセスするステップと、機械可読リソース内の１つ以上の命令及び／又は仕様に基づき支払先エンドポイント識別子を受信するステップと、を含む。支払人エンティティは、次に、トランザクションに関する支払いの詳細を提供する。支払いの詳細は、受取人エンティティのデジタルウォレットに関連付けられたエイリアス、及び受取人に支払われるべき暗号通貨額を含む。方法は、支払いの詳細を暗号鍵に関連付けるデジタル署名を提供するステップと、エイリアスに関連付けられた支払先エンドポイント識別子に関連付けられたアウトプットスクリプトを受信するステップと、を含む。アウトプットスクリプトは、次に、分散台帳のための支払いトランザクションの中に埋め込まれる。

【００５１】

幾つかの実施形態では、第３の態様の方法は、支払先エンドポイント識別子の機械可読リソースから支払先要求テンプレートを取得するステップを含む。エイリアス及びネットワーク識別子は、次に、完全な支払先要求を生成するためにテンプレートに含まれる。HTTP POST要求は、次に、エイリアスに関連付けられた支払先エンドポイント識別子を取得するために、完全な支払先要求に基づき生成される。

【００５２】

理解されるべきことに、これらの命令は、支払いサービスに関連付けられた機械可読リソース内に存在するが、命令は、支払いクライアントエンティティに関連付けられた１つ以上のコンピューティングリソース又はアプリケーションにより実行されることも目的としてよい。これらの命令を実行する１つ以上のコンピューティングリソースは、支払いクライアントエンティティに関連付けられたデジタルウォレットと共にインストールされた又はそれに関連付けられた支払いクライアントアプリケーションに関連付けられてよい。

【００５３】

有利なことに、支払いサービスに関連付けられた機械可読文書（document、ドキュメント）の提供は、知られているエイリアスを利用して、支払先エンドポイント識別子又はURIを取得するための、支払いサービスに対する、指定されたフォーマットの要求を生成することを可能にする。その結果、これは、分散台帳のためのトランザクションの構成において使用されてよい。

【００５４】

幾つかの実施形態では、エイリアス及び支払人エンティティの公開アドレスは、それぞれ、受取人エンティティ及び支払人エンティティに関連付けられたそれぞれのデジタルウォレットの公開鍵を含み、デジタル署名が、トランザクションを要求する支払人エンティティのアイデンティティを検証するために使用される。幾つかの関連する実施形態では、受取人エンティティ及び支払人エンティティの両者に関連付けられたデジタル署名は、トランザクションが分散台帳に格納される又はポストされる前に、それぞれのエンティティの検証のために要求される。

【００５５】

幾つかの実施形態では、エイリアスは、ネットワーク内のデジタルウォレットに関連付けられた支払いハンドル（handle）と呼ばれる。

【００５６】

第４の態様では、本開示は、支払いクライアント、つまり、暗号通貨支払いを別の支払いクライアント、つまり受取人エンティティに対して行うことを望む支払人エンティティを検証する技術を提供する。第４の態様は、第２の態様の機械可読リソースが支払人エン

ティティ検証を実施するために使用されるので、能力発見の第２の態様に関連する。幾つかの実施形態では、第４の態様は、支払先アドレッシングの第３の態様に関連し、支払先アドレッシングを実施する追加又は関連技術を提供する。

【００５７】

第４の態様は、Bitcoinブロックチェーンのような分散台帳に関連付けられたトランザクションのための１つ以上のクライアントのための支払いサービスを実施する、コンピュータにより実施される方法に関する。第１の実装では、方法は、支払いサービスに関連付けられた１つ以上のプロセッサにより実行される。方法は、支払いサービスに関連付けられた機械可読リソースを更新するステップを含む。幾つかの実施形態におけるこの機械可読リソースは、第３の態様に関して上述した通りであり、支払いサービスに関連付けられた予測可能な又はよく知られた位置において提供され又はそこからアクセスされる。従って、第２の態様で議論したように、機械可読リソースは、１つ以上のクライアントの中の各クライアントのために支払いサービスの実施を担うホストコンピューティングリソースに関連付けられた少なくとも１つの識別子を含み、各クライアントは、エイリアスに関連付けられ、エイリアスは、クライアント固有である。機械可読リソースは、支払いサービスによりサポートされる少なくとも１つの能力に関連付けられたエンティティも含み、各能力は、支払いサービスのクライアントのためにそれぞれの能力を実施するプロトコル又は命令に関連付けられる。機械可読リソースは、エイリアスに関連付けられ公開アドレスにアクセスする又は取得するための命令及び／又は仕様も含み、公開アドレスは、エイリアスに関連付けられたトランザクションを実現するために使用される。

【００５８】

第４の態様では、機械可読リソースを更新するステップは、支払いサービスによりサポートされる少なくとも１つの更なる能力を追加するステップを含み、少なくとも１つの更なる能力は、１つ以上のクライアントの中の所与のクライアントのエイリアスの支払先を要求する支払人エンティティがエイリアスに関連付けられるかの検証、及び／又は、支払人エンティティからの要求の非同時性処理、を含み、要求は、エイリアスに関連付けられた１つ以上のクライアントの中の所与のクライアントのエイリアスの支払先に関連付けられる。

【００５９】

第４の態様は、幾つかの実施形態ではそれぞれがデジタルウォレットに関連付けられてよい１つ以上のクライアントのために実施される所与の支払いサービスに関連付けられた１つ以上の能力又は機能を発見する上述の第２の態様に関連する全部の利点を提供する。第２の態様と同様に、要求側エンティティ、つまり支払人エンティティにより要求されるのは、受取人のデジタルウォレットに関連付けられたエイリアスだけである。従って、ユーザフレンドリな簡略化されたアドレッシングメカニズムを提供し、このようなクライアントによるトランザクションに関わりたいと望む任意のエンティティにより容易に派遣できる方法で、支払人エンティティに関連付けられたクライアントにより利用可能な又はサポートされる全部のサポート機能又は能力のレコードを提供する。

【００６０】

第４の態様の第１の実装により提供される更なる利点は、支払いサービスによりサポートされるべき１つ以上の新しい能力の提供又は追加を容易にすることである。支払いサービスに関連付けられた予測可能な又はよく知られた公衆アクセス可能な位置において提供される機械可読リソースを更新することにより、追加される新しい能力が自動的に展開され又は支払いサービスのクライアントに適用可能になり、要求側エンティティは、機械可読リソースがアクセスされるとき、このような新しい能力がサポートされることを確立することもできる。従って、新しい又は更新された能力は、直接発見され、支払いサービスに関連付けられた１つ以上の支払いクライアントによる将来のトランザクションに関連する１つ以上の要求を処理するために適用できる。

【００６１】

幾つかの実施形態では、上述の追加された又は更なる能力に加えて、更なる能力、又は

実際には元の生成された能力が真（オン、又は１）又は偽（オフ、又は０）かを指定するための指示があってよい。このトグル機能は、支払いサービスが機械可読リソース内で指定された能力のうちの１つ以上を、特定のタイプのトランザクションについて実施すること又はしないこと、又は特定の期間の間、この実施値を相応して設定することを可能にするので、有利である。従って、支払人エンティティのような任意の支払いエンティティは、特定の能力が要求に関連するタイプのトランザクションについて、又は要求が生成されている時間において、実際に実施されるかどうかをチェックできる。例えば、要求側支払いクライアント、つまりこの場合には支払人エンティティが、このような能力に関するメッセージ又は命令をサポートしない又は応答できないクライアントである場合、要求は取り下げられ又は単に送信されなくてよい。

【００６２】

第４の態様の第２の実装は、また、支払いサービスに関連付けられた１つ以上のプロセッサにより実行される。ここで、分散台帳に関連付けられたトランザクションを実現するための支払いサービスを実施する、コンピュータにより実施される方法が提供され、ここで、エイリアスが支払いサービスに関連付けられた１つ以上のクライアントの中のクライアントのために提供され、エイリアスはクライアントに固有である。方法は、支払人エンティティからエイリアスに関連付けられた要求を受信するステップを含み、要求は、支払いサービスに関連付けられた１つ以上のクライアントの中の受取人クライアントの支払先に関連し、受取人クライアントは、要求内のエイリアスに関連付けられる。幾つかの実施形態では、この要求は、支払先テンプレートを用いて上述の図６に関連する説明に基づき生成されるHTTP　POST要求である。方法は、次に、支払いサービスによりサポートされる少なくとも１つの能力に基づき支払人エンティティを検証するステップを含む。ここで、少なくとも１つの能力は、支払いサービスに関連付けられた機械可読リソースを用いて識別される。幾つかの実施形態では、機械可読リソースがどのようにアクセスされるか、及びサポートされる能力がどのように発見され実施されるかは、既に上述した第２の態様と一致する。従って、幾つかの実施形態では、少なくとも１つの能力は、第２の態様に基づき元々生成された能力であってよく、又は上述の第４の態様の第１の実装に基づき追加された更なる能力であってよい。方法の検証するステップは、支払人エンティティに関連付けられた公開鍵を取得するステップを含む。幾つかの実施形態では、このステップは、図４に関連して上述したような、つまりHTTP　GET要求を送信することによる、PKIのための機械可読リソースないの命令及び／又は仕様に基づいてよい。方法は、支払人エンティティからの要求に基づき、所定の条件が満たされるかどうかを決定するステップを含む。幾つかの実施形態では、所定の条件は、単一の条件であってよく、又は満たされるべき複数の条件であってよい。

【００６３】

所定の条件が満たされると決定された場合、支払人エンティティは有効であると考えられる。つまり支払人エンティティ検証が成功する。幾つかの実施形態では、この検証は、支払人エンティティのアイデンティティを検証する又は確認するステップを含んでよい。幾つかの実施形態では、この検証は、支払人エンティティのアイデンティティに加えて、要求の有効性を検証する又は確認するステップを含んでよい。方法は、次に、エイリアスに関連付けられた受取人クライアントの支払先に関連付けられたアウトプットスクリプトを生成するステップを含む。幾つかの実施形態では、アウトプットスクリプトの生成は、受取人のエイリアスに関連し、図５Ａに関して上述した方法で生成されてよい（この図のステップ５１２ａに関連する上述の議論を参照する）。一旦生成されると、アウトプットスクリプトは、分散台帳のためのトランザクションに埋め込むために、支払人エンティティに提供される。トランザクションは、このアウトプットスクリプトに基づき分散台帳のために構成される。

【００６４】

幾つかの実施形態では、所定の条件（又はこのような条件のうちの１つ以上）が満たされないと決定されてよい。この場合、方法は、機械可読ドキュメント内の能力により実施

されるとき、支払人エンティティが有効ではなかったので、支払人エンティティから受信した要求を拒否する応答を生成するステップを含む。幾つかの実施形態では、この拒否応答は支払人エンティティへ送信され、一方で、他の実施形態では、拒否応答は、単にレコードのために生成され送信されない。この場合、要求は、単に応答されず又は認可されないままであってよい。

【００６５】

第２の態様及び第３の態様に関連付けられた利点に追加して、第２の実装の上述の方法は、別のエンティティ、つまり支払人エンティティからの支払いトランザクションのための要求を処理するときに、支払人検証能力をサポートする又は実施する支払いサービスに関連付けられた支払いクライアント又はエンティティのためのセキュリティ及び信頼性を向上する。これは、要求側エンティティの認証を確立するために、つまりアイデンティティを検証することにより、及び相応して支払人エンティティにより送信された要求を検証することにより、支払人エンティティが、少なくとも１つの所定の条件に基づき検証されなければならないからである。従って、支払いサービスの支払いクライアントは、要求が真正であること、及び実際に支払いエンティティから生じたこと、任意の他の悪意あるパーティ又はエンティティからではないこと、を保証されてよい。

【００６６】

幾つかの実施形態では、要求は、要求が支払人エンティティにより送信された日時を示すタイムスタンプ、及び／又は支払人エンティティの公開鍵に関連付けられたデジタル署名、及び／又はワンタイムトークンを含む。上述の少なくとも１つは、要求内に存在する。幾つかの実施形態では、デジタル署名は、タイムスタンプ又はワンタイムトークンのいずれかと一緒に、常に存在する。幾つかの場合には、タイムスタンプ及びトークンの両方が、デジタル署名により署名された要求内に存在してよい。

【００６７】

幾つかの実施形態では、タイムスタンプが要求内に存在するとき、所定の条件は、要求に含まれるタイムスタンプが、受取人クライアントに関連付けられた支払いサービスによる要求の受信時間の所定の期間内にあることを検証することを含む。幾つかの実施形態では、所定の期間は最大で２分である。この２分の期間は、異なるエンティティ内のクロック同士の同期問題のために、妥当な遅延バッファを許容するために選択される。理解されるべきことに、この期間は２分に限定されず、要求されるアプリケーション及び実装に依存して更に長くてよい。通常、２分は、受け入れ可能な時間差バッファであり、幾つかの場合には、アプリケーション又は実装が特に重要であり又は時間に敏感な特性である場合には、更に短くてよい。日時は、送信／受信の日／時を記録するために、いずれかのエンティティに関連付けられたクロックにより記録されてよい。

【００６８】

幾つかの実施形態では、デジタル署名が要求内に存在するとき、所定の条件は、要求内のデジタル署名が支払人エンティティの取得された公開鍵に対応することを検証することを含む。幾つかの実施形態では、これは、署名済み要求内の署名が、取得された公開鍵に基づき検証され又はチェックできることをチェックすることを含む。幾つかの実施形態では、署名は、支払人エンティティのための非対称又は暗号鍵ペアの秘密鍵に基づき適用され、これは、同じ鍵ペアの公開鍵のみを用いて検証され又は暗号解除できる。幾つかの実施形態では、検証は、公開鍵が、古い又は使用されていない鍵ではなく、支払人エンティティの依然として有効なアイデンティティ鍵であるかどうかを知るためにチェックすることも含んでよい。これは、公開鍵が幾らかの前の時間に取得された可能性があるとき、又は公開鍵が周期的に変更されるが、該変更が起こる直前に鍵が取得された場合に、関連してよい。

【００６９】

幾つかの実施形態では、ワンタイムトークンが要求内に存在するとき、所定の条件は、トークンが任意の前の要求内で使用されていないことを検証することを含む。幾つかの実施形態では、これは、前の要求に含まれた全部のワンタイムトークンのレコードを維持す

ることを含む。その結果、このレコードは、現在の要求内のトークンが前に使用されていないことを確立するために使用されてよい。例えば、使い捨て（single－use）トークンを発行する方式は、トークンが発行される度にカウンタを単調増加させる方式が使用されてよい。

【００７０】

上述の実施形態は、有利なことに、要求が、支払人エンティティからの署名、タイムスタンプ、及び／又はワンタイムトークン、のうちの１つ以上を含むことを要求する。その結果、これらは、支払人エンティティ、及びメッセージ、つまりこのエンティティから送信された要求を検証するために使用されてよい。有利なことに、署名を検証することにより、これが既に取得された支払人エンティティの公開鍵を使用して暗号解除又は検証できることをチェックするために、支払いサービスは、要求の発生元が実際に支払人エンティティであることを確認することができる。従って、支払人エンティティのアイデンティティが検証できる。

【００７１】

有利なことに、要求のタイムスタンプが所定の期間内であることを検証することにより、メッセージ応答攻撃の範囲を限定することにより、セキュリティ及び信頼性が更に向上される。悪意あるパーティが傍受し同じメッセージを１回以上返信して宛先又は受取人クライアント又は実際にメッセージが悪意あるパーティではなく支払人エンティティから送信されている支払いサービスを混乱させようとするとき、メッセージ応答攻撃又は中間者攻撃（Man in the Middle attack）が生じ得る。それにより、受取人クライアント又は支払いサービスにメッセージに応答するよう促し、元々メッセージを送信した真正な支払人エンティティではなく悪意あるエンティティへと行く又はそれへのアクセスを提供し得る。例えば、単純なアプリケーションログイン画面実装は、ユーザからのユーザ名及びパスワードのような機密情報をキャプチャし得る。このデータがキャプチャされた場合、攻撃者は、単純にキャプチャした機密情報を幾らか後の時点で再提示することにより、ユーザとしてアプリケーションにログインできる。ユーザ名及びパスワードが両方とも有効なままであるとき、攻撃者はアクセスを許可されるだろう。従って、本開示では、受信のタイミングが要求自体の中のタイムスタンプの小さな期間内であることをチェックすることにより、これは、キャプチャされた要求の再生に成功するウインドウを狭め、従って、このような型の攻撃が防がれ、又はそれらが生じる場合に容易に検出可能である。有利なことに、ワンタイムトークンに基づく検証は、所与の要求が１回だけ処理されることを保証する。従って、要求がキャプチャされるが、要求が既に処理されたと検出された場合、該要求の後続の再生は拒否できる。例えば、ここでもユーザのログインの例を参照すると、ユーザがウェブアプリケーションのログインページにアクセスする度に、使い捨て（one－time－use）トークンが、ユーザ名及びパスワードフィールドと一緒に隠れフィールドとして埋め込まれてよい。その結果、任意の重複する又は後続の要求が同じ使い捨てトークンを特徴付ける。従って、悪意あるパーティは、例えば力ずくの試行錯誤を通じて有効なトークンを推測することができない。このようなワンタイム又は使い捨てトークンが、トークンが発行される度にカウンタを用いてインクリメントされる実施形態では、このようなカウンタはシーケンス又はシリアル番号であってよい。

【００７２】

有利なことに、使い捨てトークンをタイムスタンプ及びデジタル署名と結合することにより、再生攻撃を実行するとき、攻撃者に複数の障害を提示する。攻撃者は有効な要求をキャプチャし記録しなければならないだけでなく、最初の要求が処理されることを防ぐ必要もある。元の要求が処理されれば、使い捨てトークンが焼却され、つまり使い果たされ、もはや有効ではなくなり、再生が機能しない。これは、タイムスタンプに基づく検証に加えて、メッセージを変更することを防ぐデジタル署名も、悪意あるパーティによる再生攻撃の実施成功を非常に困難にする。

【００７３】

幾つかの実施形態では、アウトプットスクリプトを送信するステップは、受取人クライ

アントの公開鍵に関連付けられたデジタル署名をアウトプットスクリプトに適用するステップと、支払人エンティティへ、署名済みアウトプットスクリプトを送信するステップと、を含む。有利なことに、受取人エンティティの公開鍵に関連する鍵又は暗号に基づきアウトプットスクリプトを署名することにより、要求される支払先に関連付けられたアウトプットスクリプトの改ざんを防ぐ。幾つかの実施形態では、これは、受取人エンティティのための非対称又は暗号鍵ペアの秘密鍵を用いて署名を適用することを含む。その結果、署名は、同じ鍵ペアに属する公開鍵を使用してしか検証され又は暗号解除できない。

【００７４】

幾つかの実施形態では、支払人エンティティは、受取人クライアントの支払いサービスと異なる支払いサービスに関連付けられ、異なる支払いサービスに関連付けられたエイリアスを割り当てられ、エイリアスは、支払人エンティティからの要求に含まれる。他の実施形態では、支払人エンティティは前記受取人クライアントの支払いサービスと同じ支払いサービスに関連付けられ、同じ支払いサービスに関連付けられたエイリアスを割り当てられ、エイリアスは、支払人エンティティからの要求に含まれる。

【００７５】

支払人エンティティが受取人エンティティの支払いサービスと同じ又は異なる支払いサービスに関連付けられる第４の態様の実装にとって本質的ではないが、関連付けられる場合には、これは、（上述の第１～第３の態様に関連して説明されたように）公開アドレス及び支払人エンティティによりサポートされる任意の能力を発見するために、単にエイリアスに基づきアクセスされるという利点も有する。他の実施形態では、図４で説明したようなHTTP GET要求は、これが支払いエンティティの支払いサービスの機械可読リソース内のPKIテンプレートを利用するとき、支払人エンティティに関連付けられた公開鍵を取得し及び検証するために、使用できる。

【００７６】

本開示の第４の態様の第３の実装によると、上述のような支払人検証に関連する方法は、要求側クライアント支払いエンティティ、つまりこの場合には要求を行う支払人エンティティに関連して実施されてよい。方法は、エイリアスに関連付けられた要求を生成するステップを含んでよく、要求は、支払いサービスに関連付けられた１つ以上のクライアントの中の受取人クライアントの支払先に関連し、受取人クライアントは、要求内のエイリアスに関連付けられる。方法は、署名済み要求を取得するために、生成された要求に支払人エンティティの公開鍵に関連付けられたデジタル署名を適用するステップを含む。幾つかの実施形態では、これは、支払人エンティティのための非対称鍵ペアの秘密鍵により要求に署名することを含む。ここで、署名済み要求は、同じペアの公開鍵を使用して取得され又は検証され又は読み取りできる。方法は、エイリアスの支払いサービスに関連付けられた機械可読リソースにアクセスするステップを更に含む。幾つかの実施形態では、このようなアクセスは、第２の態様に関連して説明した受取人クライアントのエイリアスに基づき行われる。方法は、支払先に関連する機械可読リソース内の１つ以上の命令及び／又は仕様に基づき署名済み要求を送信するステップを含み、要求は、送信の日時を示すタイムスタンプを含む。幾つかの実施形態では、要求側支払いエンティティにより実施されるとき、要求は、図６で第３の態様に関連して議論したような支払先テンプレートに基づくHTTP POST要求であってよい。方法は、次に、要求された支払先に関連付けられたアウトプットスクリプトを受信するステップと、受信したアウトプットスクリプトを分散台帳のためのトランザクションに埋め込むステップと、を含み、トランザクションは支払人エンティティ及び受取人クライアントに関連付けられる。

【００７７】

幾つかの実施形態では、受信したアウトプットスクリプトは受取人クライアントに関連付けられた公開鍵に基づくデジタル署名を含み、方法は、先ず、図４に関連して説明したようにHTTP GET要求を用いて受取人クライアントの公開鍵を取得することにより、署名を検証するステップと、次に、デジタル署名が取得した公開鍵を用いて検証され又は暗号解除でことを検証するステップと、を含み、それにより、有利なことに、メッセージが受

取人エンティティにより初めに生成されたこと、及びアウトプットスクリプトが真正でありトランザクションを構成するために使用できることを検証する。

【００７８】

第５の態様では、本開示は、エイリアスに関連付けられた支払先のための要求の非同時性処理を実施する技術を提供する。要求は支払人エンティティ、つまり、この場合には支払人エンティティから、エイリアスに関連付けられた支払いサービスへと送信され、つまり、エイリアスは受取人クライアントに関連付けられる。要求の非同時性処理は、要求に関連する応答が直ちに又は要求を受信した短い時間の範囲内に提供されないとき、要求の遅延した処理又は不連続処理を含むと考えられてよい。これは、処理が狂った順序で行われ得るとき、つまり、場合によっては、支払いエンティティからの要求が、要求が受信された順序と同じではない順序で処理される状況もカバーする。用語「非同時性処理（asynchronous processing）」は、従って、以後、要求に対する応答の処理が要求の受信のタイミングと同期していない上述の状況の全部をカバーするために使用される。幾つかの実施形態では、このような非同時性処理は、応答又はアクションが支払いエンティティから強制的に要求されるとき、このようなエンティティが利用可能ではなく又はオフラインである、つまり要求、応答及びメッセージの転送のために使用されるインターネットのような通信ネットワークに接続されていないとき、適用されてよい。第５の態様は、第２の態様の機械可読リソースが、支払いサービスに関連付けられた支払いクライアントのためのこのような非同時性処理を可能にする能力を実装するために使用されるので、能力発見の第２の態様に関連する。第５の態様は、幾つかの実装では、支払先アドレッシングの第３の態様に関連し、非同時性であるが、支払先アドレッシングを実施する追加又は関連技術を提供する。幾つかの実施形態では、支払人検証に関連する第４の態様に関連する方法は、第５の態様に含まれてもよい。

【００７９】

第５の態様は、分散台帳に関連付けられたトランザクションのための１つ以上のクライアントのための支払いサービスを実施する、コンピュータにより実施される方法に関する。第１の実装では、方法は、支払いサービスに関連付けられた１つ以上のプロセッサにより実行され、分散台帳に関連付けられたトランザクションのための支払いサービスを実施する、コンピュータにより実施される方法に関連し、ここで、エイリアスが支払いサービスに関連付けられた１つ以上のクライアントの中のクライアントのために提供され、エイリアスはクライアントに固有である。方法は、支払人エンティティからエイリアスに関連付けられた要求を受信するステップを含み、要求は、支払いサービスに関連付けられた１つ以上のクライアントの中の受取人クライアントの支払先に関連し、受取人クライアントは、要求内のエイリアスに関連付けられる。幾つかの実施形態では、この要求は、図６に関して議論したような、支払いサービスに関連付けられた支払先テンプレートに基づくHTTP POST要求であってよい。本態様における要求の非同時性処理の実施は、支払いサービスによりサポートされる少なくとも１つの能力に基づき、少なくとも１つの能力は、支払いサービスに関連付けられた機械可読リソースを用いて識別される。幾つかの実施形態では、能力は、支払いサービスに関連付けられた予測可能な又はよく知られた位置からアクセス可能な機械可読リソースを用いて、上述の第２の態様に従い生成され又は提供される。少なくとも１つの能力は、機械可読リソースの生成のときに元々存在した能力であってよく、又は、第５の態様のために適用できる第４の態様の第１の実装に関連して上述したような更なる能力であってよい。

【００８０】

非同時性処理を実施するステップは、受信した要求に固有のトークンを生成するステップを含む。幾つかの実施形態では、このトークンは、受取人クライアントに関連する要求の受信の肯定応答として機能する。幾つかの実施形態では、トークンは、要求の識別子としても機能する。その結果、それは、そのような要求を参照し又はそれにコールバックするために使用されてよい。トークンは、次に、支払人エンティティへ送信される。幾つかの実施形態では、方法は、受取人、つまり、要求が関連する支払先に関連付けられた、ク

ライアントへ、応答の受信の通知を送信するステップを含む。この通知は、受取人クライアントに関連付けられたデジタルウォレット又はユーザ装置のメッセージ又はメールボックスアプリケーションへ送信されてよい。ここで、このような通知は、受取人クライアントがオフライン又は利用可能ではない又は応答可能ではない、つまりインターネットに接続されていない、又は単にオフにされているときでも送信されてよい。幾つかの実施形態では、受取人クライアントが動作可能であり又はオンラインであり、応答可能であるときはいつも、この応答は、要求が支払いサービスにより受信されるのを認可又は拒否する。幾つかの実施形態では、応答が、例えば２４時間又は２日間等であってよい所定の期間までに受取人クライアントにより受信されない場合、応答不可能又は認証不可能応答のような拒否と同様の応答が、生じたと考えられる。第５の態様の残りのステップは、受信した応答に基づき実行される。

【００８１】

受取人クライアントから応答として要求の認可を受信することに応答して、第５の態様の方法は、エイリアスに関連付けられた受取人クライアントの支払先に関連付けられたアウトプットスクリプトを生成するステップを含む。幾つかの実施形態では、このアウトプットスクリプトは、第３の態様の図５Ａに関して、特にステップ５１２ａに関して説明した方法で生成されてよい。方法は、次に、コールバック要求を生成するステップを含む。コールバック要求は、トークン及び生成されたアウトプットスクリプトを含む。アウトプットスクリプトは、受取人クライアントの支払先に関連付けられる。コールバック要求は、次に、支払人エンティティへ送信される。コールバック要求内で、トークンが提供される。その結果、アウトプットスクリプトは、アウトプットスクリプト内の支払先に関連して生成されたそれぞれの要求に正しく相関付けられる。アウトプットスクリプトは、分散台帳のためのトランザクションの中に埋め込まれるために提供される。

【００８２】

幾つかの実施形態では、要求の拒否が受信された、又は応答が受取人クライアントから受信されない上述の所定の期間が終了した場合、方法は、受信した要求を拒否する応答を生成するステップを含む。幾つかの実施形態では、生成された応答は、支払人エンティティへ送信されず、要求のトークンは次に単に廃棄される。他の実施形態では、コールバックメッセージが、トークン及び拒否応答に基づき生成される。これは、支払人エンティティへ送信されて、トークンに関連する要求が拒否されたことを支払人エンティティに知らせる。両方の場合に、アウトプットスクリプトは生成されない。

【００８３】

有利なことに、要求のこのような非同時性処理を実施することは、要求に対するシームレスな、正確な、不連続な、又は遅延した処理のための手段を提供する。この技術は、宛先、つまりこの場合には受取人クライアントからの応答が処理される必要があるが、受取人クライアントが動作できない又はこのような応答を提供できない実装又は状況に特に有用である。従って、上述の技術は、受取人クライアントがオフライン又は応答不可能なときでも、要求が依然として正確に処理されることを可能にする。これは、上述のようなトークンを生成すること、及び更にこのトークンを要求に関連付けることにより、達成される。問題の要求について、この同じトークンに基づくコールバックを送信することにより、要求が支払人エンティティから送信されたときから又は応答が受取人エンティティから受信されたときから経過した時間長に拘わらず、アウトプットスクリプトが、要求に関連するトランザクションに正しく関連付けられることが保証される。更に、何個の他の要求が同じ支払いサービスに関連付けられた同じ支払人エンティティから同じ又は異なる受取人エンティティへと提供されるか、又は任意の応答が受信される前にどんな順序でそれらが送信されたかに拘わらず、コールバック要求内のトークンは、アウトプットスクリプトが関連する又は応答すべき１つの要求にのみ正確に且つシームレスに相関されることを保証する。従って、要求を処理する際の遅延又は中断ではなく、処理は、同期フローの遅延又はプット（put）が全く無いかのように、正確且つシームレスに達成される。従って、有利なことに、非同時性要求処理のこのような能力を含み実施する支払いサービスの支払

いクライアントは、要求の通知が受信されるときに彼らが動作可能ではない又はオフラインである又は利用可能ではなくても、シームレス且つ信頼できる処理を享受する。

【００８４】

幾つかの実施形態では、トークンを生成することにより要求の非同時性処理を実施する又は開始するステップは、受取人クライアントに関連付けられた全部の要求について実行されてよい。この実装は、受取人クライアントがオフラインか在席かに拘わらず、先ず支払人エンティティへの肯定応答として、トークンが常に返されるので、有利である。その結果、トークンに関連付けられたこの要求のレコードが存在する。幾つかの実施形態では、トランザクションを認可する受取人クライアントからの応答が、ほぼ直ちに、例えば１０秒の所定の期間内に受信される場合、コールバック要求は直接返されてよい。この場合、トークンは、幾つかの実施形態では、要求のレコードを維持するために依然として生成されてよいが、アウトプットスクリプトを含むコールバック要求又は適用可能な場合には実際に拒否応答と共に送信されてもされなくてもよい。幾つかの実施形態では、受取人クライアントからの応答が所定の期間内に受信されない場合、トークンは、生成されなくてよい。この場合、要求／応答フローは同期的であり、コールバック要求はアウトプットスクリプトを含んでよい。有利なことに、本実施形態は、受取人クライアントがオンラインであること及び認可／拒否応答が既に受信されたことが既に確立されているとき、トークンを別個に送信することに関連するコンピューティングリソース及びネットワークリソースを節約する。

【００８５】

上述の両方の実装は、トークンに関連付けられた非同時性処理を可能にするという利点を有する。後の実装は、所定の期間が非常に短く、例えば１０秒以内又はそれより短い場合にのみ、有用である。これは、支払いサービス又は支払いエンティティを、メッセージ再生攻撃を実施する任意の悪意あるパーティから保護する。これは、支払いサービスにおいて要求が受信された直後又は直ぐにトークンを生成することにより保証される。

【００８６】

幾つかの実施形態では、トークンを送信するステップ及び／又はコールバック要求を送信するステップは、受取人クライアントの公開鍵に関連付けられたデジタル署名をトークンに適用して、署名済みトークンを取得するか、又はコールバック要求の中のアウトプットスクリプトとトークンとの組合せに適用して、署名済みコールバック要求を取得するステップと、を含み、署名済みトークン又はコールバック要求は、支払人エンティティへ返される。これは、有利なことに、トークンの内容の完全性を保護することにより、セキュリティを増大すると共に、コールバック要求が送信中に改ざんされることを防ぎ、同時に、その公開鍵に基づき受取人クライアントのアイデンティティを確認するよう機能する。幾つかの実施形態では、デジタル署名が、受取人エンティティの非対称鍵ペアの秘密鍵に基づき、トークン又はコールバック要求のいずれかに適用される。ここで、同じ鍵ペアの公開鍵のみが、秘密鍵により署名された任意のメッセージの内容を取得する又は使用する、つまり解読する又は復号するために使用できる。

【００８７】

幾つかの実施形態では、支払人エンティティは、受取人クライアントの支払いサービスと同じ又は異なる支払いサービスに関連付けられ、支払いサービスに関連付けられたエイリアスを割り当てられ、エイリアスは、支払人エンティティからの要求に含まれる。第４の態様と同様に、支払人エンティティが、受取人エンティティの支払いサービスと同じ又は異なる支払いサービスに関連付けられるかは本質的ではない。暗号通貨にアクセスし移転できるよう構成される任意のエンティティは、デジタルウォレットを実装していないものでも、支払いエンティティとして要求を生成できる。しかしながら、支払いエンティティがそのように関連付けられる場合、支払いエンティティは、公開アドレス及び支払いエンティティによりサポートされる任意の能力を発見するために、単にエンティティに基づきアクセスされるとく利点も有する（上述の第１～第３の態様に関連して説明したように）。例えば、幾つかの実施形態では、方法は、図４において説明したように、受取人エン

ティティに関連付けられた公開鍵を取得し及び検証するために、支払いエンティティの支払いサービスに基づき、HTTP GET要求を利用できる。同様に、支払いエンティティが支払いサービスに関連付けられる場合、コールバック要求は、支払先要求テンプレート、トークン、及び支払人エンティティのエイリアスに基づくHTTP POST要求であり、支払先要求テンプレートは、図６に関して説明されるように、支払人エンティティの支払いサービスに関連付けられた機械可読リソースにアクセスすることにより取得される。非同時性要求処理のために、図６のHTTP POST要求に加えて、機械可読リソース内の能力は、支払先テンプレートにトークンを含めるか、含めるための準備も含む。従って、有利なことに、支払人エンティティは、第２の態様で議論したように、単にエイリアスを使用して連絡されてよい。

【００８８】

本開示の第５の態様の第２の実装によると、上述のような非同時性処理に関連する方法は、要求側クライアント支払いエンティティ、つまり要求を行う支払人エンティティに関連して又はそのために実施されてよい。この場合、方法は、エイリアスに関連付けられた要求を生成するステップを含んでよく、要求は、支払いサービスに関連付けられた１つ以上のクライアントの中の受取人クライアントの支払先に関連し、受取人クライアントは、要求内のエイリアスに関連付けられる。方法は、支払先に関連する機械可読リソースからアクセスされる１つ以上の命令及び／又は仕様に基づき要求を送信するステップを含み、機械可読リソースは支払いサービスに関連付けられる。幾つかの実施形態では、このようなアクセスは、第２の態様に関連して上述した技術に基づく。方法は、支払いサービスからトークンを受信するステップを含み、トークンは要求に固有でありデジタル署名に関連付けられる。方法は、トークンに関連付けられたデジタル署名が受取人クライアントの公開鍵に関連付けられることを検証するステップを含む。上述のように、幾つかの実施形態における署名は、受取人クライアントの非対称鍵ペアの秘密鍵を用いて適用され、その結果、トークンは、該ペアの公開鍵を使用してのみ検証され又は暗号解除できる。検証が成功することに応答して、方法は、トークンに基づき、要求に関連付けられたレコードを更新するステップを含む。幾つかの実施形態では、レコードは、支払人エンティティ自体、又は支払人エンティティに関連付けられた支払いサービスに関連付けられてよく、又は、支払人エンティティに関連付けられた装置又はクラウドにリモートに格納されたレコードに基づいてよい。方法は、コールバック要求を受信するステップを含み、コールバック要求は、トークン及び要求された支払先に関連するアウトプットスクリプトを含み、コールバック要求はデジタル署名に関連付けられる。デジタル署名は、トークンについて上述した通りであってよい。方法は、コールバック要求に関連付けられたデジタル署名が、受取人クライアントの公開鍵に対応することを検証するステップを含み、この検証が成功することに応答して、コールバック要求内のトークンを更新されたレコードに相関させるステップを更に含む。正しい要求に相関されると、コールバック要求内のアウトプットスクリプトは、次に、分散台帳のためのトランザクションに埋め込まれ、トランザクションは支払人エンティティ及び受取人エンティティに関連付けられる。

【００８９】

第５の態様の第１の実装について上述した利点は、第２の実装に等しく適用される。更に、要求に固有のトークンが、支払人エンティティのような支払いクライアントに提供される場合、このエンティティは、有利なことに、多くの他のメッセージがエンティティにより送信され／受信される場合でも、それぞれの要求に関連する応答が受信される前に、トランザクション又はメッセージのリスト又は集合を検索する必要無しに、該エンティティから生じたトランザクションに関連する要求を容易に特定できる。

【００９０】

幾つかの実施形態では、受信したトークン又はコールバック要求は、受取人クライアントの公開鍵に関連付けられたデジタル署名を含み、デジタル署名を検証するステップは、公開鍵を取得し、取得した公開鍵が署名済みトークン及びアウトプットスクリプトを検証するために使用される公開鍵に対応することをチェックすることを含む。幾つかの実施形

態では、公開鍵を取得するステップは、図４に関連して説明したように、機械可読リソース内のPKI（public key infrastructure）要求テンプレートを用いてHTTP GET要求を送信することに基づく。

【００９１】

幾つかの実施形態では、方法は、上述の第４の態様の第３の実装による、支払人クライアントにより実施され又はそれにより実施されるような支払人検証に関連する能力に関連付けられる。

【００９２】

本開示の第４の態様の第３の実装によると、上述の非同時性処理に関連する方法は、宛先支払人クライアント、つまり要求が向けられる受取人クライアントに関連して実施されてよい。この場合の方法は、受取人クライアントにより、エイリアスに関連付けられた要求を受信するステップを含み、要求は、支払いサービスに関連付けられた１つ以上のクライアントの中の受取人クライアントの支払先に関連し、受取人クライアントは、要求内のエイリアスに関連付けられる。支払人クライアントがオンラインである又は受信した要求に応答できるとき、要求は受取人からのこのようなインプットが処理されることを要求するので、受取人クライアントは、要求を認可又は拒否してよく、該認可又は拒否に基づき、支払いサービスへ応答を送信する。

【００９３】

幾つかの実施形態では、通知は、要求側支払人クライアントの指示、要求されるトランザクションに関連するタイプ及び／又は額、のような要求の詳細を含んでよい。幾つかの実施形態では、通知は、受取人クライアントのデジタルウォレットに関連付けられたコンピューティング装置又はディスプレイ端末上で、受取人クライアントに提示されてよい。幾つかの実施形態では、方法は、コンピューティング装置又はディスプレイ端末のユーザインタフェース上で相互作用する又は要求を認可する又は拒否するためのデータを入力するステップを含んでよい。幾つかの実施形態では、認可又は拒否は、コンピューティング装置において相互作用又は任意の明示的なアクションを要求せずに、受取人クライアントにより自動的に提供されてよい。幾つかの実施形態では、受取人クライアントは、特定のプロパティ又は支払人エンティティ又は支払人エンティティエイリアスに関連付けられた要求を許可する又は許可しない１つ以上のレコード又はリストを含み又はそれに関連付けられてよい。例えば、要求がホワイトリスト内にある支払人エンティティからである場合、受取人クライアントがオンラインになると直ぐに、ホワイトリストがチェックされ、認可が送信される。同様に、支払人エンティティがブラックリスト内にある場合、拒否が自動的に送信される。リストは、要求のタイプ又は額、等のような、要求の他のプロパティに関連付けられることが可能である。応答が提供されると、要求の処理は、第５の態様の第１及び／又は第２の実装毎に、処理される。

【００９４】

第４の態様に関連する例示的なシナリオは、分散台帳のためのトランザクションに関連付けられた方法を含み、該方法は、支払人エンティティから受取人エンティティへ要求を送信するステップを含み、要求は、受取人エンティティのためのエイリアスを含み又はそれにアドレッシングされる。ここで、要求は、受取人エンティティに関連付けられた支払いサービスにより受信される。支払いサービスは、要求に含まれるタイムスタンプ及び署名に基づき、支払人エンティティを検証する。検証の成功に応答して、受取人エンティティに関連付けられたアウトプットスクリプトが、アウトプットスクリプトに基づきトランザクションを生成するために、支払人エンティティへ送信される。このトランザクションは、分散台帳へとポストされる。

【００９５】

第５の態様に関連する例示的なシナリオは、分散台帳のためのトランザクションに関連付けられた方法を含み、該方法は、支払人エンティティから受取人エンティティへ要求を送信するステップを含み、要求は、受取人エンティティのためのエイリアスに基づく。ここで、要求は、支払人エンティティに関連付けられた支払いサービスにより受信される。

トークンの形式の要求の受信の肯定応答が、支払人エンティティに提供される。要求に関連する通知は、受取人エンティティに提供される。受取人エンティティがオンラインである又は利用可能であるとき、受取人エンティティは、ユーザインタフェースと相互作用することにより、通知内で要求を認可し又は拒否する。受取人エンティティからの認可に応答して、受取人エンティティに関連付けられたアウトプットスクリプトが、アウトプットスクリプトに基づきトランザクションを生成するために、支払人エンティティへ送信される。トランザクションは、分散台帳へとポストされる。

【００９６】

本開示の更なる態様は要求側エンティティからネットワーク内のデジタルウォレットに関連付けられたエイリアスへの支払いトランザクションを要求するためのプレフィックスを構成する方法に関する。その結果、プレフィックス及びエイリアスを含む要求側エンティティからの要求の受信に応答して、本開示の上述の第１～第５の態様のうちの１つ以上が、支払いサービスによりエイリアスに基づき自動的に実行されてよい。

【００９７】

有利なことに、この更なる態様は、要求側エンティティに知られている受取人エンティティのエイリアスに続いて例えば「payto:」又は「bsvto:」のような単にプレフィックスの提示により、上述の態様及び実施形態を自動的にトリガすることを可能にする。このプレフィックスは、有利なことに、上述の態様及び実施形態のうちの１つ以上に基づき、支払いトランザクションについての要求が生成され支払いサービスへ送信されることを可能にする。要求側エンティティが必要なことは、知られているエイリアスをプレフィックスに追加することだけである。

【００９８】

本開示は、プロセッサと、プロセッサによる実行の結果として、コンピューティング装置に本願明細書に記載のコンピュータにより実施される方法のいずれかの態様又は実施形態を実行させる可能命令を含むメモリと、を含むコンピューティング装置も提供する。本開示は、上述の任意の態様又は実施形態を実施するよう一緒に動作可能な複数のこのような装置を含むシステムも提供する。

【００９９】

本開示は、実行可能命令を記憶した非一時的コンピュータ可読記憶媒体であって、実行可能命令は、コンピューティング装置又はシステムのプロセッサにより実行された結果として、コンピューティング装置又はシステムに、少なくとも本願明細書に記載のコンピュータにより実施される方法の１つの態様又は実施形態を実行させる、非一時的コンピュータ可読記憶媒体も提供する。

【０１００】

幾つかの特定の実施形態は、添付の図面を参照して例示のためにここで説明される。ここで同様の参照符号は同様の機能を示す。

【０１０１】

図１は、本開示の第１の態様に関し、エイリアスに関連付けられた１つ以上のデジタルウォレットのための支払いサービスを実施する方法を示す。図１では、方法は、支払いサービスの提供に関連付けられた１つ以上のプロセッサにより実施されると理解される。本開示では、支払いサービスは、以下に説明する機能を実行する１つ以上の実行可能なルール又はプロトコルであってよい。ウォレットは、デジタルウォレットのネットワークの中のものであってよく、又は分散台帳に関連付けられたトランザクションのための個別の独立型暗号通貨ウォレットであってよい。例えば、方法は、BSV暗号通貨のためのBitcoinウォレットのネットワーク内で実施されてよい。説明を簡単に及び理解を容易にするために、デジタルウォレットのネットワーク内のデジタルウォレットに関連付けられたエイリアス（alias）は、以下では、図の説明の中で参照される。しかしながら、上述のように、本開示は、ネットワーク内の他のウォレットに接続されるデジタルウォレットに多くの場合に限定されない。

【０１０２】

ステップ１０２は、デジタルウォレットのネットワーク内の所与のデジタルウォレットにエイリアスを割り当てる又は提供することに関連する。これは、デジタルウォレットに関連付けられたそれぞれの公開アドレスとのエイリアスのマッピング又は相関を提供することに関連する。その結果、エイリアスは、公開アドレスの代わりに使用できる。このような割り当ては、例えば特定の支払いクライアント又はエンティティがネットワークに署名するときに行われてよい。この点で、「エイリアス：公開アドレス」のペアは、ウォレット毎に提供されてよい。エイリアスは、特定のウォレットにユニークであり、ネットワークのドメイン名のようなネットワーク識別子、又は該ネットワークを識別する名称のいずれかを含む。例えば、エイリアスは、clientname@domainname.comのような、よく知られた電子メールのフォーマットであってよい。ここで、clientnameは、Alice又はBobのような、デジタルウォレットのネットワークに署名する又は登録される単なる個人又は会社の名称又は識別子であってよい。domainnameは、組織又はドメインオーナ、例えば「nChain」を示す。この場合、Aliceのエイリアスは、alice@nchain.comである。Bobが、本開示の１つ以上の態様及び／又は実施形態を実施するドメイン名「notnchain」を有するデジタルウォレットの異なるネットワークに署名する場合、Bobのエイリアスはbob@notnchain.comとして割り当てられてよい。エイリアスがネットワーク識別子に関連付けられる限り、AliceNC又はBobBSV等のような他のエイリアスフォーマットも使用されてよい。

【０１０３】

ステップ１０４は、ディレクトリ内のネットワーク識別子に基づき支払いサービスのサービスレコードを生成することに関する。このステップは、ディレクトリ内の支払いサービスを提供するネットワーク識別子にエイリアスを関連付けるために必要である。ここで参照されるディレクトリは、通常、開放型である、つまりあらゆるユーザにより公衆アクセス可能な、非集中型ディレクトリである。例えば、DNSのようなグローバルディレクトリが使用できる。これは、非集中型であり開放型であり、従って、インターネットを介してどこからでも任意のエンティティ又はユーザによりアクセス可能である。開放型のアクセス可能な非集中型ディレクトリは好適な実装であるが、本開示はこれに限定されない。幾つかの実施形態では、参照されるディレクトリは、集中型ディレクトリであってもよい。他の実施形態では、ディレクトリは、閉じられたディレクトリ、つまり、ネットワーク又はサービスに登録されたユーザ又はエンティティがアクセス可能なものであってよい。以下では、説明を容易にするために、説明の中でDNSのようなグローバルディレクトリが言及される。他のタイプのディレクトリも本開示の範囲内にあることが、当業者により理解される。

【０１０４】

例えば、エイリアスが、上述のフォーマットのインプット又は要求の中で提供されるとき、支払いがエイリアスを使用して行われるかどうかを識別するために、DNSのようなディレクトリが検索される（caDNSルックアップ）。支払いサービスに基づくエイリアスをサポートしないネットワーク又はドメインに関連付けられたエイリアスが、入力された場合、この状況は、以下の実装のうちの１つ又は組合せを用いて処理されてよい。ある実装では、エイリアスを使用する支払いは行うことができないことを示す結果は、DNSにより返されない。サービスレコードが存在しない場合、要求側エンティティは、分散台帳に関連付けられた任意のトランザクションが生成され得る前に、他の知られている技術により公開アドレスを取得しなければならない。別の実装では、例えば、サービスがネットワーク識別子としてdameドメインにより提供されるとき、返される結果は、エイリアスに関連付けられるネットワーク又はドメインに責任のあるホストの位置であってよい。例えば、上述の例に基づき、エイリアス内のネットワーク識別子に関連付けられた支払いサービスのサービスレコードがディレクトリ内に存在しない場合、ドメイン「nchain」に責任のあるホストの位置又はURIが提供されてよく、又は要求側エンティティがドメイン「nchain」のためのホストへ向けられてよい。従って、エイリアス内で示されたドメインに責任のあるホストは、要求を更に処理してよい。

【０１０５】
ステップ１０６は、ステップ１０４で生成されたサービスレコードを更新すること、又はそれに、ネットワーク識別子により関連付けられたネットワーク又はドメインにより提供される支払いサービスを示すエントリ又はフィールドを含むことに関する。DNS内のサービスレコードを更新するステップは、nchain.comのような特定のネットワーク識別子が、特定の支払いサービス、例えば「bsvpay」又は「bsvalias」として識別されるサービスを提供する又は使用することを示す。この更新するステップは、DNSルックアップを実行するエンティティに、識別された支払いサービスが、つまり「bsvalias」を考慮して、nChainドメインに関連付けられたエイリアスに対して支払いトランザクションを実行できることを示す。
【０１０６】
ステップ１０８は、ステップ１０６で示された支払いサービスに責任のあるホストコンピューティングリソースの位置を示すために、サービスレコードを更新するステップに関する。従って、支払いサービスがデジタルウォレットのネットワークへの異なるネットワーク又はドメインに関連付けられた場合、サービスレコード内のこのエントリは、サービスを担うホストコンピュータ又はサーバのウェブサーバ位置又はIPアドレスを指すだろう。上述の例から続けて、bsvalias支払いサービスが別個のネットワーク又は別個のドメイン（bsvalias.com）に関連付けられた場合、bsvalias.comのホストサーバを特定する位置又は命令は、サービスレコード内で示される。これは、エイリアスに関連付けられたデジタルウォレットの識別を実現するよう構成されるホストコンピューティングリソースがどこで見付かるかを識別するためである。
【０１０７】
指定されたサービスのためのサーバの位置を定義するDNS内のサービスレコード（srv record）の例は、以下に示される。
【０１０８】
支払いサービス（bsvalias）に関連するドメイン名（nchain）のサービスレコードは、以下の形式で、以下のようなフィールド又はエントリを有してよい：
・service：所望のサービスの記号名。
・proto：所望のサービスのトランスポートプロトコル、これは、通常、TCP（transmission control protocol）又はUDP（User datagram protocol）である。
・name：このレコードが有効であるドメイン名、ドットで終わる。
・TTL：標準的なDNS存続時間フィールドであり、レコードに関連する終了期間又は期限を設定する。
・class：標準的なDNSクラスフィールドである。
・priority：目標ホストの優先度である。
・weight：同じ優先度を有するレコードについての相対的重みである。
・port：サービスが発見されるべきTCP又はUDPポートである。
・target：サービスを提供する機械の標準的ホスト名である。
【０１０９】
例えば、nchainのドメインオーナは、以下のパラメータを有するSRV（service）レコードを生成してよい。

【表１】

Parameter	Value
Service	_bsvalias
Proto	_tcp
Name	nchain
TTL	3600 (for example)
Class	IN
Priority	10
Weight	10
Port	443
Target	payment-services.nchain.com

図２Ａ及び２Ｂは、支払いサービスを担うホストを識別する方法を示すフロー図である。図２Ａは、支払いサービスに関連付けられた１つ以上のプロセッサにより実施される方法を示す。図２Ｂは、支払いクライアントエンティティに関連付けられた１つ以上のプロセッサにより実施される方法を示す。

【０１１０】

図２Ａのステップ２０２ａで、ホストサービスは、エイリアスに関連付けられたトランザクションの要求側エンティティから要求を受信する。この要求は、要求側エンティティのコンピューティング装置のインタフェース、つまり、インストールされているデジタルウォレットからの入力の形式であってよい。例えば、要求は、支払人エンティティからのalice@nchain.comへの支払い（payto）を示す要求を含んでよい。

【０１１１】

ステップ２０４ａで、ステップ２０２ａにおける要求又は入力に応答して、グローバルディレクトリの検索又はルックアップ、例えばDNSルックアップが、入力されたエイリアスに基づき実行される。これは、エイリアス内のネットワーク識別子に関連するグローバルディレクトリ内の支払いサービスのサービスレコードを特定することである。従って、図１について上述した同じ例を用いて、このステップは、エイリアス内のネットワーク識別子の中でnchainが受信されたので、上述のようにドメインnchainのサービスレコードを識別する。nchainについてのこのサービスレコードは、次に、bsvaliasがnchainのために使用される支払いサービスであることを識別する。

【０１１２】

ステップ２０６ａで、サービスレコード、従って支払いサービス、つまりbsvaliasが識別されると、支払いサービスのためのホストコンピューティングリソースの位置が取得される。幾つかの実施形態では、これは、要求側エンティティへ返される。上述の例では、ホストのこの位置は、nchainのsrvレコードの中のtarget:portペアに対応する。target:portペアは、サービスbsvaliasを担うホストが使用する又は動作する位置を提供する。

【０１１３】

ステップ２０８ａで、ステップ２０６ａで取得したホストの位置、つまりtarget:portペアに基づき、エイリアスに関連付けられたデジタルウォレットの公開アドレスが決定されてよい。幾つかの実施形態では、これは、例えば図１に関連して議論された、支払いサ

ービス又はネットワークに署名するときのマッピングに基づいてよい。公開アドレスが取得されると、これは、デジタルウォレット間のBitcoinブロックチェーントランザクションのために使用できる。

【０１１４】

図２Bは、上述のように、図２Ａに対応するステップに関連するが、支払人又は要求側エンティティのコンピューティング装置又はデジタルウォレットにおいて実施される。

【０１１５】

従って、ステップ２０２ｂは、要求側エンティティからのトランザクションについての要求を送信することに関連し、要求はエイリアスに関連付けられる。

【０１１６】

ステップ２０６ｂは、支払いサービスに関連付けられたホストコンピューティングリソースの位置を取得するステップに関連し、位置は、ネットワーク識別子に関連するサービスレコードに基づく。これは、例えば、図２Ａのステップ２０４ａ及び２０６ａで実行される。従って、ここで取得された位置は、「bsvalias」支払いサービスのホストのtarget:portペアである。

【０１１７】

ステップ２０８ｂで、エイリアスに関連付けられたデジタルウォレットの公開アドレスが取得される。その結果、これは、デジタル台帳に関連付けられたトランザクションのために使用されてよい。

【０１１８】

図３Ａ及び３Ｂは、トランザクションのための要求内のエイリアスに関連付けられた公開アドレスを識別するための、本開示の第２の態様による方法を示すフロー図である。図３Ａは、支払いサービスに関連付けられた１つ以上のプロセッサにより実施される方法を示す。図３Ｂは、支払いクライアントエンティティに関連付けられた１つ以上のプロセッサにより実施される方法を示す。

【０１１９】

図３Ａのステップ３０２ａで、機械可読リソースが、支払いサービスのために生成される。機械可読リソースは、支払いサービスにより提供される又はサポートされる機能又は能力、及び／又はこれらの能力を利用する任意の命令が識別できることを保証するために提供される。従って、この処理は、支払いサービスに関連する能力発見と呼ばれる。従って、機械可読ドキュメントが、能力発見処理のために生成される。これにより、サービスを使用し又は要求したいと望む支払いクライアントエンティティ又はデジタルウォレット又はアプリケーションは、支払いサービスのサポートされる機能、及び支払いサービスの使用に関連する任意のそれぞれのエンドポイント及び構成を学習し又は発見できる。幾つかの実施形態では、機械可読リソースは、予め生成され支払いサービスに関連付けられて保存されたファイル又はドキュメントであり、つまり静的ドキュメントである。幾つかの実施形態では、例えば、エンタープライズ級のサービス実装では、機械可読リソースは、動的であってよく、例えばウェブサーバ上に保存される静的ファイルとしてではなく、オンデマンドで生成できる。有利なことに、このように動的に生成されるリソースは、サービス展開、移行、保守、及び実行されることを要求される任意のアップグレードにおける簡略化を提供する。

【０１２０】

幾つかの実施形態では、軽量なデータ交換フォーマットであるJSON（JavaScript Object Notation）が、機械可読リソースを生成するために使用される。JSONは、完全に言語独立のテキストフォーマットである画、C、C++、C#、Java、JavaScript、Perl、Python、及び他の多くを含む、Cファミリ言語に慣れているプログラマに親しみのある慣習を使用する。これらのプロパティは、JSONを理想的なデータ交換言語にする。更に、JSONは、２つの構造、つまり名称／値ペアの集合、及び値の順序付きリスト、の上に構築される。多くの言語では、これは、配列、ベクトル、リスト、又はシーケンスにより実現される。これらは汎用的なデータ構造であるので、事実上、全ての近年のプログラミング言語

は、それぞれそれらをサポートする。従って、JSONはこれらの同じ構造に基づく他のプログラミング言語と交換可能なデータフォーマットを提供するので、JSONを機械可読リソースのために使用することは望ましい。

【０１２１】

機械可読リソースは、支払いサービスに関する以下の情報を含んでよい：

支払いサービスを実施する責任のあるホストコンピューティングリソースに関連付けられた少なくとも１つのエンドポイント識別子。これは、支払いサービスの１つ以上の機能を担うサーバ又はコンピューティングリソースの位置、つまりtarget:portペアであってよい。

【０１２２】

支払いサービスによりサポートされる複数の能力の中の少なくとも１つの能力に関連付けられたエントリ。これは、要求側エンティティ又は支払人エンティティ検証、トランザクションのための複数のデジタル署名、トランザクションのための受取人エンティティ又は支払先認可、及び／又はトランザクションが分散台帳へポストされる前にエイリアスに関連付けられた電子メールアドレスへ送信されるようにする電子メールに基づく支払いトランザクション、要求又は応答に関連する支払人及び／又は受取人コールバック機能、等のような、支払いサービスによりサポートされ得る１つ以上の機能であってよい。

【０１２３】

エイリアスに関連付けられたエンティティ又はデジタルウォレットによりトランザクションを実現するために使用され得る、（デジタルウォレットのエンティティの）公開アドレスにアクセスするための命令及び／又は仕様。幾つかの実施形態では、公開アドレスにアクセスすることは、エイリアスに基づき、支払いサービスに関連付けられた１つ以上のリソース又はURIにアクセスすることを含む。幾つかの実施形態では、取得されると、公開アドレスは、分散台帳のためのトランザクションの構成において使用されるアウトプットスクリプトの中で使用されてよい。幾つかの実施形態では、公開アドレスにアクセスすることは、PKI手順に基づきエンティティの公開鍵を解決すること、及び支払先、つまり受取人デジタルウォレットを解決することを含んでよい。

【０１２４】

例えば、機械可読リソースは、支払いサービス「bsvalias」のための以下のファイル又はエントリを示してよい：

【数１】

```
{
  "bsvalias": “version …”
  "capabilities": {…
    "pki": "https://bsvalias.example.org/ {name} @ {domain.tld}/id",
    "paymentDestination": https://bsvalias.example.org/ {name} @ {domain.tld}/payment-destination"
  }
}
```

【０１２５】

テンプレート値{name}及び{domain.tld}は、エイリアスフォーマット〈name〉@〈domain〉.〈tld〉の成分を表す。ここで、tldは、.com又は.org又は.co.uk等のような最上位ドメインである。要求側エンティティ又は支払いクライアントは、テンプレートをエイリアスで置き換えてよい。従って、上述の例では、これは、alice@nchain.comである。

【０１２６】

ステップ３０４ａで、支払いサービスに関連付けられた予測可能な又は知られている位置に、機械可読リソースを格納するステップに関する。例えば、支払いサービス「bsvalias」「のための支払いサービスオペレータ又はプロセッサは、ステップ３０２ａにおいて上述したＪＳＯＮフォーマットのテキストドキュメントの生成に続いて、以下の位置においてドキュメントを提供してよい：

https://〈host－discovery－target〉:〈host－discovery－port〉/.well－known/bsvalias

【０１２７】

よく知られた予測可能な位置においてJSONフォーマットのドキュメントを提供することは、有用である。その結果、それは、（例えばネットワーク識別子に基づき）支払いサービスを認識する全てのエンティティにより公衆アクセス可能である。上述の例示的な位置は、IANA（Internet Assigned Numbers Authority）のWell－Known URIリソースに基づく。従って、機械可読リソースは、支払いサービスbsvaliasに関連する発見能力のために、ウェブサーバ上の予測可能な位置に置かれる。

【０１２８】

ステップ３０６ａで、支払いクライアントエンティティからのトランザクションについての要求が受信され、要求は支払いが向けられるべきエイリアスを含む。上述の例から続けて、これは、payto:alice@nchain.comのような要求を含む。

【０１２９】

ステップ３０８ａで、エイリアスに関連付けられた支払いサービスが識別される。これは、エイリアス内のネットワーク識別子、つまりnchainに基づく。この識別子、つまりbsvaliasに関連付けられた支払いサービスは、このステップで識別される。サービスレコードを識別するための第１の態様によるホスト発見は、これの前に実行されてもよいが、これは、図３に示した実施形態では、本質的ではない。例えば、データベースに格納されたマッピング、又はサービス発見処理に基づくテキストドキュメントは、第１の態様におけるサービスレコードの代わりに、bsvaliasのホストを識別するために使用されてもよい。

【０１３０】

ステップ３１０ａで、識別された支払いサービスに基づき、支払いサービスの機械可読リソースは、予測可能な又は知られているネットワーク位置からアクセスされる。例えば、サービスbsvaliasのためのJSONドキュメントは、ステップ３０４ａで指定されたようなよく知られた位置から取得される。

【０１３１】

ステップ３１２ａは、要求されたトランザクションの１つ以上の能力が機械可読リソース内に存在するかどうかを決定する。このステップは、サポートされる能力に関連する１つ以上のエントリが要求のために適切かどうかを識別するステップを含む。例えば、これは、共通能力が要求側クライアントエンティティの支払いサービスによりサポートされるかどうか、及びbsvaliasのためのJSONドキュメント内の能力、つまり受取人alice@nchain.comの支払いサービス、をチェックすることを含んでよい。幾つかの場合には、要求側エンティティにより追加能力が指定されず又は要求されなくてよい。この場合、支払いトランザクションは、共通能力が存在するか否かに拘わらず進行できる。

【０１３２】

ステップ３１４ａで、機械可読リソースがトランザクションのための少なくとも１つのサポートされる能力を有すると仮定すると（これが要求側エンティティにより指定された場合）、これが識別されると、支払いサービスのホストコンピューティングリソースに関連付けられたエンドポイント識別子が、機械可読リソースから返される。上述の例では、これは、bsvaliasに責任のあるホストの位置であってよい。次に、支払いサービス「bsvalias」のための機械可読リソース内の命令及び／又は仕様のうちの１つ以上を用いて、エイリアスに関連付けられたデジタルウォレットのための公開アドレスが取得できる。

【０１３３】

図３Ｂは、上述のように、図３Ａに対応するステップに関連するが、支払人又は要求側

エンティティのコンピューティング装置又はデジタルウォレットにおいて実施される。

【０１３４】

従って、ステップ３０６ｂは、要求側エンティティからのトランザクションについての要求を送信することに関連し、要求はエイリアスに関連付けられ、つまり上述の例に続き、payto:alice@nchain.comを送信することに関連する。

【０１３５】

ステップ３１０ｂで、エイリアス内のネットワーク識別子に基づく支払いサービスの識別に続き、例えば、図３Ａのステップ３０８ａにおいて説明したように、例えば図３Ａのステップ３０４ａにおいて説明したように、このステップは、要求側クライアントにより、識別された支払いサービスに関連付けられたよく知られた位置から機械可読リソースにアクセスするステップを含む。

【０１３６】

ステップ３１２ａは、要求側エンティティが、要求されたトランザクションの１つ以上の能力が機械可読リソース内に存在するかどうかを決定する。このステップは、図３Ａのステップ３１２ａと同様に、共通の又は指定されたサポートされる能力に関連する１つ以上のエントリが、要求されたトランザクションのために適切である又は必要であるかどうかを識別するために、JSONドキュメントをチェックするステップを含む。

【０１３７】

ステップ３１３ｂで、１つ以上の能力が機械可読リソース内に存在するかどうかを識別することに基づき、要求側クライアントは、支払いサービスのためのホストコンピューティングリソースに関連付けられたエンドポイント識別子、つまりサービスbsvaliasのためのホスト位置、を受信する。

【０１３８】

ステップ３１４ｂで、要求側クライアントは、次に、エイリアスに関連付けられた公開アドレスを取得する。これは、機械可読リソース内の命令及び／又は仕様のうちの１つ以上に従い機能を実行する要求側クライアントにより取得できる。

【０１３９】

図４は、エイリアスに関連付けられた暗号鍵を取得するPKI（public key infrastructure）技術を実施する第２の態様の機械可読リソース内で指定される命令の例示的なシーケンスを示す。

【０１４０】

ステップ４０２で、機械可読リソースからのPKI要求テンプレートは、支払いサービスに関連付けられた機械可読リソースから取得されなければならない。このテンプレートは、幾つかの実施形態では、PKIエンドポイント識別子を要求するためのテンプレートである。これは、支払いクライアントエンティティの公開鍵を識別し及び／又は検証するために構成される、支払いサービスのコンピューティングリソースのURIである。例えば、上述の例から続けると、テンプレートは以下であってよい：

"pki": "https://bsvalias.example.org/{name}@{domain.tld}/id

【０１４１】

ステップ４０４で、テンプレートが受信されると、エイリアス及び関連するネットワーク識別子は、テンプレートの適切なフィールドに含まれ又は代用されて、完全なPKI要求を生成する。例えば、テンプレート値{name}及び{domain.tld}は、エイリアス、つまり〈name〉@〈domain〉.〈tld〉のコンポーネントを表し、機械可読リソースに基づき完全な要求を発行する前に、代入されなければならない。このステップの結果は、「bsvalias」のPKIエンドポイント識別子の提供である。

【０１４２】

ステップ４０６で、HTTP GET要求が、ステップ４０４で取得されたPKIエンドポイント識別子に基づき生成される。

【０１４３】

ステップ４０８で、エイリアスに関連付けられた公開鍵は、次に、ステップ４０６で生

成された要求に応答して取得できる。多くの場合に、公開鍵は、オンチェーントランザクションの部分として使用されていない、安定した楕円曲線デジタル署名アルゴリズム（elliptic curve digital signature algorithm（ECDSA））公開鍵である。有効なエイリアスのための要求、つまり、支払いサービスに関連付けられ公開鍵を割り当てられたものが受信された場合、支払いサービスのPKIに責任のあるホストからの応答メッセージは、以下のフォーマットで公開鍵を返してよい。

【数２】

```
{
   "bsvalias": "1.0",
   "alias": "<name>@<domain>.<tld>",
   "pubkey": "..."
}
```

【０１４４】

ECDSA公開鍵は、secp２５６k１曲線上の有効な点であり、圧縮され、１６進符号化される。これは、「pubkey」文字列が６６バイト長（３３バイトの２進数、各バイトが２個の１６進文字として符号化される）であることを意味する。

【表２】

Start	Length	Value
00	02	"Odd/even" indicator, either “02” or “03”
02	64	Elliptic curve point x-coordinate

【０１４５】

要求が有効ではないエイリアスに基づく場合、つまり、支払いサービス及び／又は公開鍵に関連付けられていないものである場合、応答メッセージは、エラーが生じたこと、又は要求されたリソースが見付からない、又は利用可能ではない、又は認可されていないことを示す。

【０１４６】

図５Ａ及び５Ｂは、トランザクションのための要求内のエイリアスに関連付けられた支払先を識別するための、本開示の第３の態様による方法を示すフロー図である。支払先は、分散台帳のためのトランザクションを構成する際に使用される。図５Ａは、支払いサービスに関連付けられた１つ以上のプロセッサにより実施される方法を示す。図５Ｂは、支払いクライアントエンティティに関連付けられた１つ以上のプロセッサにより実施される方法を示す。幾つかの実施形態では、支払先を取得するステップは、図３A及び３Bにおけるエイリアスに関連付けられた公開鍵を取得ことに基づき又はその部分である。幾つかの実施形態では、支払先エンドポイント識別子は、アウトプットスクリプト内に符号化されるべき又は含まれるべきアドレスに関連し、その結果、トランザクションは、このアドレスに基づきブロックチェーンのために構成されてよい。幾つかの実施形態では、支払先エンドポイント識別子は、上述の公開アドレスと同じである。他の実施形態では、支払先エンドポイント識別子は、エイリアスに関連付けられた公開アドレスと異なってよく、又はデジタルウォレットのための公開アドレスの部分であってよく又はそれに関連付けられてよい。幾つかの実施形態では、エイリアスに関連付けられた公開アドレス及び／又は支払先エンドポイント識別子は、静的又は動的に割り当てられてよい。

【０１４７】

図５Ａのステップ５０２ａは、エイリアスの中の支払いサービスを識別するステップに続き、支払いサービスの機械可読リソースにアクセスするステップに関連する。支払いサービスのアイデンティティは、機械可読リソースの位置と共に、図１、３Ａ及び／又は３Ｂに関連して上述したように取得できる。

【０１４８】

ステップ５０４ａで、支払先エンドポイント識別子は、機械可読ドキュメント内の１つ以上の命令及び／又は仕様を用いて、機械可読リソースから取得される。このエンドポイントは、エイリアスに関連付けられたデジタルウォレットの支払先エンドポイントを解決するよう構成される支払いサービスのコンピューティングリソース又はサーバのＵＲＩであってよい。

【０１４９】

ステップ５０６ａで、支払いトランザクションの支払いの詳細は、支払いエンティティから取得される。例えば、これは、少なくとも、受取人エンティティのデジタルウォレットに関連付けられたエイリアス、及び受取人に支払われるべき暗号通貨の額を含んでよい。これは、支払人エンティティのコンピューティングリソース又はアプリケーションに関連付けられたインタフェースを用いて提供されてよい。

【０１５０】

ステップ５０８ａで、ステップ５０６ａにおける支払いの詳細を有する要求のためのデジタル署名、及び支払人エンティティに関連付けられた暗号鍵が、取得される。トランザクションに関連する要求に関連するこの署名は、多くの場合、要求側、つまり支払人エンティティの秘密鍵を用いて適用される。

【０１５１】

ステップ５１０ａで、デジタル署名が検証されてよく、その結果、支払人エンティティのアイデンティティが認証できる。これは、１つ以上の知られている技術を用いて実行されてよい。幾つかの実施形態では、ECDSA鍵が使用されると仮定すると、例えば図４のPKIシーケンスを用いて取得された支払人エンティティの公開鍵は、署名するエンティティ（支払人エンティティ）のアイデンティティを検証するために使用できる。検証が失敗した場合、デジタル署名は、もう一度提供される必要があってよく、又は１つ以上のエラーメッセージが生成され得る。

【０１５２】

ステップ５１２ａで、ステップ５１０ａにおいて検証の成功が出力されることに続き、エイリアスに関連付けられた支払先エンドポイント識別子に基づくアウトプットスクリプトが、生成される。このアウトプットスクリプトは、分散台帳のためのトランザクションの中の支払先を自動的に解決するために、分散台帳のための支払いトランザクションに埋め込むために提供される。

【０１５３】

例えば、分散台帳、つまりBitcoinブロックチェーンのｔまえのトランザクションの構成のために返されるアウトプットスクリプトは、次式に従ってよい：

【数３】

```
{
   "output": "..."
}
```

【０１５４】

アウトプットフィールドの値は、１６進符号化Bitcoinスクリプトであってよく、支払いトランザクションの構成中に、支払人エンティティがこれを使用する。

【０１５５】

種々の可能なタイプのアウトプットスクリプトが生成されてよいが、説明を容易にする

ために、Ｐ２ＰＫＨ（Ｐａｙ ｔｏ Ｐｕｂｌｉｃ Ｋｅｙ Ｈａｓｈ）アウトプットスクリプト生成が以下の例で議論される。

【０１５６】

次式の公開鍵を有する鍵ペアが与えられると：

【数４】

027c1404c3ecb034053e6dd90bc68f7933284559c7d0763367584195a8796d9b0e

【０１５７】

同じもののＰ２ＰＫＨアウトプットスクリプトは次式のように１６進符号化されてよい：

【数５】

76a9140806efc8bedc8afb37bf484f352e6f79bff1458c88ac

【０１５８】

これは、以下のように分解できる：

【数６】

```
76              ; OP_DUP
a9              ; OP_HASH160
14              ; Push the next 20 bytes on to the stack
08 06 ef c8; ripemd160 (sha256 (compressed_public_key))
be dc 8a fb
37 bf 48 4f
35 2e 6f 79
bf f1 45 8c
88              ; OP_EQUALVERIFY
ac              ; OP_CHECKSIG
```

【０１５９】

サービス応答本体、つまり、ステップ５１２ａにおけるトランザクションに埋め込むためのスクリプトは、従って以下の通りである：

【数７】

```
{
   "output": "76a9140806efc8bedc8afb37bf484f352e6f79bff1458c88ac"
}
```

【０１６０】

図５Ｂは、上述のように、図５Ａに対応するステップに関連するが、支払人又は要求側エンティティのコンピューティング装置又はデジタルウォレットにおいて実施される。

【０１６１】

ステップ５０２ｂで、支払人エンティティからのトランザクションについての要求であって、該要求はエイリアスに関連付けられる要求に基づき、機械可読リソースは、支払い

サービスに関連付けられた位置から支払人エンティティによりアクセスされる。
【０１６２】
ステップ５０４ｂで、機械可読ドキュメント内の１つ以上の命令及び／又は仕様に基づく支払先エンドポイント識別子が、受取人エンティティにより取得される。
【０１６３】
ステップ５０６ｂは、トランザクションに関する支払いの詳細を送信する又は提供するステップに関連する。支払いの詳細は、受取人エンティティのデジタルウォレットに関連付けられたエイリアス、及び受取人に支払われるべき暗号通貨額を含む。
【０１６４】
ステップ５０８ｂ及び５１０ｂは、支払人エンティティが、支払いの詳細を暗号鍵に関連付けるために、デジタル署名を提供するステップに関連し、その後に、図５Ａの対応するステップで議論したような検証が続く。
【０１６５】
ステップ５１２ｂは、エイリアスに関連付けられた支払先エンドポイント識別子に基づき、支払人エンティティによりアウトプットスクリプトを受信するステップに関連する。これは、上述の図５Ａに関連して説明された。
【０１６６】
ステップ５１４ｂは、受信したアウトプットスクリプトをトランザクションに埋め込むことにより、支払人エンティティにより分散台帳のための支払いトランザクションを構成するステップに関連する。
【０１６７】
図６は、デジタルウォレットのためのエイリアスに関連付けられた支払先エンドポイント解決シーケンスを実施する、機械可読リソース内で指定される命令の例示的なシーケンスを示す。
【０１６８】
ステップ６０２で、機械可読リソースからの支払先要求テンプレートは、支払いサービスに関連付けられた機械可読リソースから取得される。幾つかの実施形態では、これは、図５Ａ及び５Ｂで議論した支払先エンドポイント識別子を要求するためのテンプレートである。例えば、支払いサービスbsvaliasについての上述の例から続けると、テンプレートは以下であってよい：
"paymentDestination":https://bsvalias.example.org/{name}@{domain.tld}/payment－destination
【０１６９】
ステップ６０２でテンプレートが受信されると、ステップ６０４で、エイリアス及び関連するネットワーク識別子は、テンプレートの適切なフィールドに含まれ又は代用されて、完全な支払先要求を生成する。例えば、テンプレート値{name}及び{domain.tld}は、目標エイリアス、つまり〈name〉@〈domain〉.〈tld〉のコンポーネントを表し、機械可読リソースに基づき完全な要求を発行する前に、代入されなければならない。このステップの結果は、支払先エンドポイント識別子の提供であり、これは、幾つかの実施形態では、エイリアスに関連付けられたアウトプットトランザクションの生成のために使用されるべき支払いアドレスを識別する責任のあるコンピューティングリソースのURIであってよい。
【０１７０】
ステップ６０６で、HTTP　POST要求が、ステップ６０４で取得された支払先エンドポイント識別子に基づき生成される。
【０１７１】
ステップ６０８で、エイリアスに関連する、支払先エンドポイント識別子に基づくアウトプットスクリプトが返される。これは、また、図５A及び５Bで議論したように、分散台帳のための支払いトランザクションの構成において使用される。
【０１７２】

上述の第３の態様に関連する幾つかの実施形態では、第３の態様による支払先についての要求（例えば、ステップ５０２ａ、５０２ｂに関連する要求、又は上述の図６のPOST要求）の本体は、アプリケーション／jsonのコンテンツタイプを示してよい。これは、要求を生成する又は完成させるためのテンプレートが、支払いサービス、つまりbsvaliasのための機械可読リソースに基づくからである。幾つかの実施形態では、上述のように（例えば、図６を参照、）支払人エンティティからの要求は、要求内の受取人エンティティのエイリアスを識別することに加えて、以下のスキーマに従ってよい。

【数８】

```
{
    "payerName": "FirstName LastName",
    "payerHandle ": "<alias>@<domain.tld>",
    "dt": "<ISO-8601 timestamp>",
    "amount of cryptocurrency": 550,
    "purpose": "message to payee",
    "signature": "<compact Bitcoin message signature>"
}
```

【０１７３】

上述のスキーマのフィールドは、以下の表に簡単に説明され、幾つかのフィールドの更なる説明は後述される。

【表３】

Field		Description
payerName		人間により読み取り可能な支払人表示名
payerHandle		支払人エンティティ又は支払人のデジタルウォレットに関連付けられたエイリアス
dt		ISO-8601 フォーマットのタイムスタンプ（以下を参照）のような好適な又は容認されるフォーマットのタイムスタンプ
amount		支払人が受取人クライアントエンティティへ移転しようとする、BSV(Satoshis)又は Ethereum 又は他の Bitcoin 又は IBM チェーン等のような暗号通貨の額
purpose		支払いの目的の人間により読み取り可能な説明、つまり、会費支払いのため、未払いの残高を明確にするため、等
signature		これは、軽量な Bitcoin メッセージ署名である（以下を参照）

【０１７４】

幾つかの実施形態では、受取人エンティティのエイリアスを含むことに加えて、上述のスキーマの中でpayerHandleとして識別されるフィールドが存在すれば、又は要求に関連付けられれば、十分である。幾つかの実施形態では、支払人エンティティ又は支払人クライアントに関連付けられたデジタルウォレットが支払いトランザクションのためのエイリアスを有しない場合、このpayerHandleは単に支払人の公開識別子又はＩＰ又はBitcoinアドレスに関連付けられてよい。以下では、本開示におけるpayerHandleは、支払人クラ

イアントエンティティに関連付けられたエイリアスであるとして説明される。従って、このような実施形態では、支払人エンティティはエイリアスを有し、該エイリアスに基づき支払いトランザクションを実現する支払いサービスに関連付けられる。支払人の支払いサービスは、受取人の支払いサービスと同じ又は異なってよい。

【０１７５】

幾つかの実施形態では、上述の表の中で「dt」により示されるタイムスタンプフィールド、及びpayerHandleは、要求のためのスキーマの中で必要とされてよい。他の実施形態では、タイムスタンプ、payerHandle、並びに署名フィールドは、特定の要求について、又は受取人クライアントに関連付けられた機械可読リソース内に存在し得る１つ以上の能力に従い動作するために、要求されてよい。

【０１７６】

残りのフィールドは、要求の機能又は動作が関連する限り、任意である場合がある。しかしながら、多くの状況では、通常は量が示される（これは０であっても）。しかし、任意的フィールド又は任意的フィールドのゼロでない値は、それが知られている場合、又は情報が支払いエンティティ、つまりこの場合には支払人エンティティに利用可能である場合に、要求内に存在してよい。タイムスタンプ及び署名フィールドは、機械可読リソース内で指定される特定の支払いサービス能力について必須であると考えられてよく、以下に説明される。

【０１７７】

タイムスタンプフィールド「dt」は、支払人が支払先要求を開始した時点で、受け入れられた標準ISO－８６０１フォーマットの現在時刻を含んでよい。JavaScriptから、これは、JSON.stringify()のような機械可読リソースに関連するコマンド又は命令を用いて構成できる。例えば、これは、以下を返してよい：

【数９】

```
let now = JSON.stringify ({'now': new Date ()});

Which may yield for example:

{
   "now": "2013-10-21T13:28:06.419Z"
}
```

【０１７８】

幾つかの実施形態では、署名フィールドは、メッセージに署名し及びメッセージ署名を検証する支払いエンティティ又はクライアントの能力に基づいてよい。この機能は、多くの場合に、基本的に、標準的なECDSAの実装であるが、整数r及びsについて(r,s)署名ペアを有し、クライアントが、公開鍵に対して直接ではなく、Ｐ２PKHアドレス（公開鍵のハッシュ）に対してメッセージ署名を検証できるようにするために提供される追加情報がある。

【０１７９】

幾つかの実施形態では、署名は、この場合には上述の要求であるメッセージのdouble－SHA２５６ハッシュに対して計算された未処理（raw）(r,s)フィールドであってよい。例えばMoneyButtonのBSVライブラリのような既存のBitcoinクライアントライブラリ、又は他の同様の暗号通貨ライブラリを利用するために、既存の署名及び検証プロトコルが幾つかの実施形態について適切であり得る。

【０１８０】

幾つかの実施形態では、MoneyButton BSVライブラリの実装は、支払先要求に含まれる署名に対する標準的なメッセージダイジェスト構成及び署名符号化方法として指名される。署名されるべきメッセージ又は要求は、（BSVライブラリのソースコードの中で文書

化され得るように）Bitcoin署名方式の伝統的な又は知られているプリアンブルで開始してよく、その後に、フィールドpayerHandleとdtと、任意的に、上述の例示的なスキーマで議論した量及び目的フィールドとのUnicode Transformation Format－８－bit(UTF８)ストリング連結が続く。

【０１８１】

要求内の量の指定に関して、上述のスキーマに基づき、幾つかの実施形態では、以下のルールが適用されてよい。

【０１８２】

量が存在する場合、それはストリングに変換される（先行するゼロを有しない）。

【０１８３】

量が存在しない場合、ストリング「０」が使用される。

【０１８４】

目的が存在しない場合、空ストリング「」が使用される（事実上、目的がメッセージ内に含まれない）。

【０１８５】

図７は、支払いサービスのための能力を更新する方法を示すフロー図である。この方法は、上述の第２～第５の態様のうちの１つ以上に適用可能である。この図は、第４の態様の第１の実装に関連して上述した、支払いサービスに関連付けられた１つ以上のプロセッサにより実施される方法に関する。

【０１８６】

ステップ７０２で、前述の態様の例で上述したようなbsvaliasのような支払いサービスに関連付けられた機械可読リソースがアクセスされる。このようなアクセスは、支払いサービスに責任のあるホストにより行われてよい。幾つかの実施形態では、更新又は変更を行うためのアクセスは、責任のあるホストに限定されてよい。

【０１８７】

幾つかの実施形態では、機械可読リソースは、生成されたものであり、第２の態様に関して上述したように、支払いサービスの１つ以上の支払いクライアントのためのエイリアスに基づき支払いサービスに関連付けられたよく知られた位置からアクセスされ得る。これは、図３Ａ及び３Ｂに関して詳細に説明される。

【０１８８】

ステップ７０４で、以下で支払いサービスによりサポートされる少なくとも１つの更なる能力（従って、このような能力はそれに関連付けられた全ての支払いクライアントに提供される）が、機械可読リソースに追加される。このような追加は、支払いサービスに責任のあるホストにより行われてよい。第２の態様に関して議論したように、機械可読リソース内の能力又はエントリは、支払いサービスに関連付けられた１つ以上のクライアントのためにそれぞれの能力を実施するための、従うべき１つ以上のプロトコルのセット、又は仕様若しくは実行可能ファイル若しくは命令である。クライアントは、トランザクションに関与する支払人又は受取人エンティティ又はノードのような、支払いエンティティである。

【０１８９】

幾つかの実施形態では、このステップにおける更新は、単に、能力の実施に関する値又はフィールドを変更することであってよい。従って、支払いサービスbsvaliasが既に機械可読ドキュメント内の能力仕様を有するが、能力が未だbsvaliasによりそのクライアントに展開される準備ができていないために、値が「偽」又は「０」に設定される場合、又は終了されるべき変更又はバージョン更新が実行中である場合、これを「真」又は「１」に更新することは、このステップの更新であると考えられる。

【０１９０】

例えば、支払いサービスbsvaliasが、bsvaliasに関連付けられた全部のクライアント又はデジタルウォレットについて全部の将来の暗号通貨トランザクションに対する以後の支払人検証をサポートするよう、新しい能力を追加するために、のための（第２の態様で上

述したように、JSONフォーマットである）機械可読リソースは、支払人検証能力のための以下のエントリ又はスキーマを含むよう更新されてよい。

【数１０】

```
enforcement:
{
  "bsvalias": "1.0",
  "capabilities": {
    "name: payervalidation “or “ref: c318d09ed403” {……}
“value: true”
  }
}
```

【０１９１】

パスcapabilities.payervalidation、又はc３１８d０９ed４０３等のような任意の他の識別子は、それにより、機械可読リソースに含まれ、幾つかの実施形態では、支払人検証が実施されることを識別するために値「真」に設定される。この能力は、第４の態様に関連して更に議論される。

【０１９２】

幾つかの実施形態では、値フィールドが存在しない。この場合、上述のエントリ又はスキーマの包含は、支払人検証が実施されることを意味するために十分であってよい。幾つかの実施形態では、値フィールドが存在する場合、「真」以外の任意の値は、「偽」と等価であると考えられてよく、支払人検証が実施されないことを示す。

【０１９３】

同様に、非同時性要求処理のような別の能力が、ステップ７０４における更新の間に、支払人検証と別個に又はそれに加えて追加される場合、以下のエントリが、bsvaliasのための機械可読リソース内で非同時性処理のサポートの宣言を含むために追加される：

【数１１】

```
{
  "bsvalias": "1.0",
  "capabilities": {
    "name: asynchronous request processing” or “ref: da377cdc9ae7": {…….
      "call-back":  "https://bsvalias.example.org/  {name}  @  {domain.tld}/payment-
destination-response"
    }
  }
}
```

【０１９４】

非同時性要求処理のためのJSONドキュメント内のcapabilities.da３７７cdc９ae７パス又はオブジェクトは、値フィールドを含まない。この例では、単に上述の仕様を追加することにより、この能力は、以後にbsvaliasによりサポートされると理解される。以上は、入ってくる（incoming）支払先コールバック要求を含むテンプレートエンドポイントU

RIを有するコールバックプロパティも含む。これは、第５の態様に関連して更に議論される。

【０１９５】

図８は、第４の態様による、bsvaliasのような支払いサービスのための支払人エンティティ検証を実施する方法を示すフロー図である。この方法は、能力が支払いサービスによりそのクライアントのために実施されるとき、図７で上述された支払人検証のための能力エントリにおいて指定される１つ以上の命令又はプロトコル又はルールに基づき実施される。この方法は、上述の第２の態様及び第３の態様のうちの１つ以上に関連し、第４の態様の第２の実装に関連して上述した、支払いサービスに関連付けられた１つ以上のプロセッサにより実施される方法に関する。

【０１９６】

ステップ８０２で、要求が受信され、要求は、支払人エンティティからであり、支払いサービスに関連付けられた支払先エンティティのエイリアスに関連付けられる。

【０１９７】

例えば、要求は、エイリアス「alice@nchain.com」を含んでよく、前述の例から続けると、そのようなエイリアスに関連付けられた支払いエンティティ又はデジタルウォレットの支払いサービスは、bsvaliasである。従って、以後、このエイリアスのためのデジタルウォレットは、（この支払いエンティティがbsvaliasのクライアントであることを識別するために）受取人クライアントと呼ばれる。要求を送信する支払人エンティティは、支払いサービスに関連付けられてもそうでなくてもよい。この場合、支払人エンティティは、単に、暗号通貨トランザクションのための、その公開アドレスにより識別される。支払人エンティティが受取人クライアントと同じ支払いサービスに関連付けられる場合、それは、エイリアス「bob@nchain.com」を用いて表すことができる。支払人エンティティは、支払いサービス、つまり、それ自体の能力エンティティを指定する異なる機械可読リソースを有する支払いサービス「notbsvalias」に基づき、全く異なるエイリアスに関連付けられることも可能である。この場合、支払人エンティティのエイリアスは「bob@notnchain.com」であってよい。

【０１９８】

以後、第４及び第５の実施形態の全部の実装及び実施形態のために説明を容易にするために、エイリアス「bob@nchain.com」は、受取人クライアントと同じ支払いサービス、つまりbsvaliasに関連付けられた、従って同じJSONドキュメント又は機械可読リソースに基づく能力の同じセットを実施する支払人エンティティのエイリアスと考えられる。しかしながら、本開示が以上に説明したような実装に限定されないことが理解される。

【０１９９】

幾つかの実施形態では、この要求は、図６に関して説明したような、bsvaliasのための支払先要求テンプレートに関連付けられたHTTP　POST要求に基づいてよい。

【０２００】

ステップ８０４で、支払人エンティティに関連付けられた公開鍵は、bsvalias支払いサービスに関連付けられた１つ以上のプロセッサにより取得される。これは、図４に関して説明したように、bsvaliasのための機械可読リソースに基づくHTTP　GET要求を用いて取得されてよい。

【０２０１】

ステップ８０６で、１つ以上の所定の条件が、alice@nchain.comについてbsvaliasにより実施される支払人検証能力について満たされるかどうかが決定される。この図で議論された実施形態では、２つの条件が評価され、最初の１つは支払人エンティティのための公開鍵検証である。しかしながら、上述のように、所定の条件は、単にこれらの条件に基づいてよく、又は（ワンタイムトークンに基づくような）追加条件を含んでよい。議論される本願の実施形態では、要求は、bob@nchain.comの秘密鍵によりデジタル署名されるべきである。これは、bob@nchain.comの秘密鍵にリンクされた公開鍵と共にのみ使用でき、つまり同じ暗号鍵ペアの部分である。その結果、要求は、公開鍵を用いて読み取られ

、つまり検証され又は取得され又は復号できる。従って、このステップで、bob@nchain.comからの要求の中のデジタル署名がステップ８０４で取得された公開鍵により検証されるかどうかがチェックされる。

【０２０２】

要求がデジタル署名を含まない場合、又はデジタル署名がステップ８０４で取得した公開鍵を用いて検証できない場合、これは、要求が支払人エンティティに関連付けられていないデジタル署名を含むことを意味する。要求は、従って、ステップ８１０で支払人エンティティのアイデンティティが無効であるので又は検証できないので、拒否される。幾つかの実施形態では、要求が拒否された又は認可されない又は許可されないことを示す応答が、支払人エンティティのために生成されてよい。上述のように、これは、支払人エンティティのアイデンティティ、及び要求の内容の完全性が上述のステップに基づき検証できるので、支払いサービスのクライアントに関連するトランザクションのセキュリティ及び信頼性を向上する。適用されるデジタル署名は、幾つかの実施形態では、支払先に関連付けられた要求の例示的なスキーマに関連して上述したような軽量なBitcoinメッセージ署名に基づいてよい。

【０２０３】

ステップ８０６の結果が、支払人エンティティbob@nchain.comについてステップ８０４で取得された公開鍵に基づき、要求内のデジタル署名が検証されたことである場合、これは、要求が支払人エンティティbob@nchain.comから調整された（ordinated from）ことを確認する。ステップ８０８で、次に、要求が、支払人検証能力の上述の２つの所定の条件のうちの２つ目を満たすかどうかが決定される。ステップ８０８の２つ目の条件は、要求が、支払いサービスにおける受信時間の所定の期間内にあるタイムスタンプを含むかどうかをチェックする。受信時間は、支払いサービスのクロックに基づく。この期間は、支払人検証の能力の中で設定されてよい。例えば、この所定の期間は、同期及びメッセージ送信タイミングの問題又は遅延のための幾らかの時間を許容するために、２分であってよい。他の期間も可能であってよく、このステップは２分の期間に限定されない。

【０２０４】

要求がタイムスタンプを含まない場合、又はタイムスタンプが所定の期間内にない場合、ステップ８２０で、支払人エンティティからの要求は、拒否され又は無効であると考えられる。上述のように、これは、タイムスタンプを検証することによりメッセージ再生攻撃又は中間者攻撃に対して支払システムのクライアントを保護することにより、セキュリティ及び信頼性を向上する。従って、第３の態様に関連して上述した要求スキーマは、支払人検証能力が本実施形態に従い実施される場合、少なくとも「dt」及び「signature」フィールドを含む。他の実施形態では、上述の条件のうちの１つの適合又は充足は、支払人検証のためには十分であるが、多くの場合には両方の条件が満たされることが望ましい。

【０２０５】

ステップ８１２で、両方の条件が満たされる場合、つまり、デジタル署名が取得した公開鍵に関連する場合、且つタイムスタンプが所定の期間内にある場合、支払人エンティティは検証に成功したと考えられ、それにより、支払先についての要求が処理できることを示す。

【０２０６】

ステップ８１４で、次に、受取人クライアントのエイリアス、つまりalice@nchain.comの支払先に関連付けられたアウトプットスクリプトが、生成される。これは、図５Ａに関連して議論したアウトプットスクリプトの生成と同様であってよい。

【０２０７】

ステップ８１６で、受取人クライアントに関連付けられたデジタル署名が、アウトプットスクリプトに適用される。ステップ８０６で支払人エンティティについて上述した署名と同様に、ここで、alice@nchain.comのための暗号鍵ペアの秘密鍵が、アウトプットスクリプトに署名するために使用され、同じ鍵ペアの公開鍵を用いて取得できるようにする。これは、アウトプットスクリプトが送信中に改ざんされないことを保証し、支払人エン

ティティがアウトプットスクリプトの生成元を確認することを助ける。
【０２０８】
従って、送信されるアウトプットスクリプトのためのスキーマは以下であってよい：
【数１２】

```
{
   "output": "...",
   "signature": "<compact Bitcoin message signature>"
}
```

【０２０９】
ステップ８１８で、署名済みアウトプットスクリプトは、支払人エンティティbob@nchain.comへ送信される。ここで、一旦復号され又は取得され又は検証されると、このアウトプットスクリプトは、分散台帳のためのトランザクションに埋め込むことができる。
【０２１０】
図９は、支払いサービスに関連付けられた１つ以上の支払いエンティティクライアントのために支払人検証の能力を実施することに関する第４の態様の第３の実装による方法を示すフローチャートである。この場合には、示された方法は、要求側エンティティである支払人エンティティに関連付けられた１つ以上のプロセッサにより実行される。従って、方法は、図８で議論した第４の態様の第１の実装に関連するが、同じ例から続けて、支払人エンティティ、つまりbob@nchain.comによる実施に関係する。
【０２１１】
ステップ９０２で、エイリアスに関連付けられた要求が生成され、要求は、bsvalias支払いサービスに関連付けられた１つ以上のクライアントの中の受取人クライアント、つまりalice@nchain.comの支払先に関連する。ここで、要求は受取人クライアントのエイリアスを含む。
【０２１２】
ステップ９０４で、支払人エンティティbob@nchain.comの公開鍵に関連付けられたデジタル署名が、要求に適用される。デジタル署名を適用する処理は、図８のステップ８０６又は８１６に関して、又は要求スキーマを議論した上述の第３の態様で説明した軽量なBitcoinメッセージに関連して上述したものと同様であるが、ここでは、署名は支払人エンティティの鍵、つまり上述の例ではbob@nchain.comの秘密鍵を用いて適用される。
【０２１３】
ステップ９０６で、支払人エンティティは、エイリアスの支払いサービスに関連付けられた機械可読リソースにアクセスする。従って、このステップでは、bsvaliasに関連するJSONドキュメント又は機械可読リソースは、エイリアスalice@nchain.comに基づきアクセスされる。このようなアクセスに関連する方法は、第２の態様に関連して上述した。
【０２１４】
ステップ９０８で、署名済み要求は、次に、支払先に関連する機械可読リソース内の１つ以上の命令及び／又は仕様に基づき、送信される。幾つかの実施形態では、要求はHTTP POST要求であり、命令及び／又は仕様は、第３の態様の図６に関して議論したような支払先要求テンプレートに基づく。要求は、幾つかの実施形態では、送信の日時を示すタイムスタンプを含む。これは、支払人エンティティ検証の能力を実施するために署名及びタイムスタンプフィールドが必要とされることを議論した図８と同様である。
【０２１５】
ステップ９１０で、alice@nchain.comのための要求された支払先に関連付けられたアウトプットスクリプトが、支払人エンティティにより受信される。図８のステップ８０６に関して上述したように、このアウトプットスクリプトは、受取人クライアントalice@nc

hain.comに関連するデジタル署名を含む。

【０２１６】

ステップ９１２で、デジタル署名が正しく検証されるか又は受取人エンティティの公開鍵に関連するかどうかがチェックされる。このために、受取人クライアントalice@nchain.comに関連付けられた公開鍵が先ず取得されなければならない。幾つかの実施形態では、これは、第２の態様の図４に関連して議論されたようなbsvalias機械可読ドキュメントを用いるHTTP GET要求に基づく。デジタル署名は、次に、この取得した公開鍵に基づき検証される。

【０２１７】

ステップ９１４で、取得した公開鍵を用いてデジタル署名が検証され又は有効にされ又は復号できた場合、アウトプットスクリプトは、改ざん又は悪意ある妨害を伴わずに、支払人エンティティから生じたと確認される。この場合、アウトプットスクリプトは、分散台帳のためのトランザクションに埋め込まれ、トランザクションは支払人エンティティ及び受取人クライアントに関連付けられる。

【０２１８】

他方で、デジタル署名が取得した公開鍵に関連しない場合、又はアウトプットスクリプトが取得した公開鍵を用いて取得できない場合、ステップ９１６で、アウトプットスクリプトは拒否され、トランザクションは構成されず、送信者、つまりここでは受取人クライアントalice@nchain.comのアイデンティティも、スクリプトのコンテンツの完全性も、確認できない。

【０２１９】

図１０は、bsvaliasのような支払いサービスのための非同時性要求処理（又は遅延又は不連続処理）を実施する方法を示すフロー図である。この方法は、能力が支払いサービスによりそのクライアントのために実施されるとき、図７で上述された非同時性要求処理のための能力エントリにおいて指定される１つ以上の命令又はプロトコル又はルールに基づき実施される。この方法は、上述の第２、第３、又は第４の態様のうちの１つ以上に関連する。この図は、第５の態様の第１の実装に関連して上述した、支払いサービスに関連付けられた１つ以上のプロセッサにより実施される方法に関する。

【０２２０】

ステップ１００２で、支払人エンティティからのエイリアスに関連付けられた要求が受信され、要求は、支払いサービスに関連付けられた受取人クライアントの支払先に関連する。前述の例から続けて、支払人エンティティbob@nchain.comからの要求は、エイリアスalice@nchain.com（受取人クライアント）を含むことが理解され、ここでalice@nchain.comは支払いサービスbsvaliasに関連付けられる。幾つかの実施形態では、要求は、bsvaliasの機械可読リソースに基づく支払先要求テンプレートを使用する第３の態様の図６に関して説明したように、HTTP POST要求である。

【０２２１】

ステップ１００４で、受信された要求に固有のトークンが生成される。幾つかの実施形態では、トークンは、乱数生成器に基づくもののような、ユニークな識別子である。ここで、どの２つの要求も決して同じトークンを割り当てられない。トークンは、要求に関連する特定のシード又は関数に基づいてよい。幾つかの実施形態では、このトークンは、要求自体の１つ以上のコンポーネントのハッシュ値であってよい。

【０２２２】

ステップ１００６で、このトークンは、支払人エンティティへ送信され、ちょうど受信の肯定応答のようなものである。本実施形態では、トークンは、alice@nchain.comのような支払いクライアントについて受信された全部の要求について生成されると理解され、ここで、支払いサービスbsvaliasは、非同時性要求処理能力を実施する。他の実施形態では、そのようなトークンが生成されるのは、受取人クライアントが所定の時間期間の間、つまり要求の通知を受信した後の５又は１０分間に応答しない場合のみであってよい。幾つかの実施形態では、第４の態様に関して上述したように、デジタル署名は、生成元及び

トークンのセキュリティ及び完全性を保証するために、受取人エンティティ、つまりalice@nchain.comの公開鍵に基づき適用されてよい。トークンを含む、支払人エンティティへ送信される内容についてのスキーマは、以下であってよい：

【数１３】

```
{
   "token": "…",
   "signature": "…"
}
```

【０２２３】

ステップ１００８で、受信した要求に関する通知が、受取人クライアントalice@nchain.comへ送信される。これは、支払人クライアントが、通知を送信するときに、インターネットに接続されていない又はオフラインである又は電源断である又は非動作中である又は応答しないときでも送信されてよい。

【０２２４】

ステップ１０１０で、alice@nchain.comが、通信端末上のユーザインタフェース又は指示子を用いて通知を認可又は拒否したかが決定され、相応して、これを示す応答をbsvaliasへ送信する。受取人エンティティからのこの応答は、通知を送信してから直ちに又は幾らかの時間の後に到着してよい。例えば、本実施形態では最大で２日間も可能であるが、非活性化の期間は更に長くてもよいので、本開示はこれに限定されない。

【０２２５】

要求の拒否が受取人クライアントからの応答として受信された場合、ステップ１０１８で、要求について拒否通知又はレコードが生成される。幾つかの実施形態では、ステップ１１２０で、結果、つまり拒否通知は、支払人クライアントへ送信される。通知は、この拒否が要求に関連して単に記録されれば十分である幾つかの他の状況では、送信されなくてよい。

【０２２６】

ステップ１０１２で、要求の認可が受信された場合、受取人クライアントalice@nchain.comの支払先に関連付けられたアウトプットスクリプトが生成される。アウトプットスクリプトを生成するステップは、第３の態様の図５Ａに関連して説明したものと同様であってよい。

【０２２７】

ステップ１０１４で、トークン及び生成されたアウトプットスクリプトを含むコールバック要求が生成される。これは、bob@nchain.com又はalice@nchain.comに関連して処理された他のメッセージ又は要求の数の範囲又は時間に拘わらず、アウトプットスクリプトを正しい要求に相関させるために使用できるユニークなトークンの存在のために、コールバック要求と呼ばれる。幾つかの実施形態では、このコールバック要求は、署名されてよく、つまり、alice@nchain.comの公開鍵に基づき検証可能なデジタル署名を適用される。幾つかの実施形態では、コールバック要求は、第３の態様の図６で議論したようなHTTP POST要求に基づいてよいが、図７に関して議論した非同時性要求処理能力に関連付けられたテンプレートでトークンの更なる提供を有する。これは、alice@nchain.com及びbob@nchain.comのための支払いサービスであるbsvaliasの機械可読リソースから取得されてよいが、支払人エンティティは異なる支払いサービスを有してよい。例えば、非同時性処理の能力エントリは、以下であってよい：

【数１４】

```
{
  "bsvalias": "1.0",
  "capabilities": {
    "da377cdc9ae7": {
      "call-back": "https://bsvalias.example.org/ {name} @ {domain.tld}/payment-destination-response"
    }
  }
}
```

【０２２８】
従って、ここで、この能力のための識別子は、capabilities.da３７７cdc９ae７オブジェクトへの参照であってよい。これは、支払先要求コールバックのためのテンプレートエンドポイントURIを有するコールバックプロパティを含む。従って、コールバック要求は、これに、幾つかの実施形態では、図６の支払先要求テンプレートに基づく。
【０２２９】
ステップ１０１６で、コールバック要求は、トークン及びアウトプットスクリプトと一緒に支払人エンティティに提供される。トークンは、アウトプットスクリプトを要求に相関させるために使用され、更にこの相関のために、アウトプットスクリプトは、分散台帳のためのトランザクションに埋め込むことができる。コールバック要求のスキーマは、以下であってよい：
【数１５】

```
{
  "token": "...",
  "output": "...",
  "signature": "..."
}
```

【０２３０】
トークンは、ここで、ステップ１００６で送信されたのと同じトークンである。
【０２３１】
図１１は、支払いサービスに関連付けられた１つ以上の支払いエンティティクライアントのために非同時性要求処理の能力を実施することに関する第５の態様の第２の実装による方法を示すフローチャートである。この場合には、示された方法は、要求側エンティティである支払人エンティティに関連付けられた１つ以上のプロセッサにより実行される。従って、方法は、図１０で議論した第５の態様の第１の実装に関連するが、同じ例から続けて、支払人エンティティ、つまりbob@nchain.comによる実施に関係する。幾つかの実施形態では、支払人エンティティ検証の能力を実施する図９に関連して議論した方法も含まれてよい。
【０２３２】
ステップ１１０２で、エイリアスに関連付けられた要求が生成され、要求は、支払いサービスbsvaliasに関連付けられた１つ以上のクライアントの中の受取人クライアント、つ

まりalice@nchain.comの支払先に関連する。ここで、要求は受取人クライアントのエイリアスを含む。幾つかの実施形態では、特に第４の態様の支払人検証の能力も実施される場合に、この要求は、要求スキーマにおいて上述したような署名を含むようデジタル署名されてよい。生成されると、この要求は、支払人エンティティbob@nchain.comにより、受取人クライアントalice@nchain.comのbsvalias支払いサービスへ送信される。要求は、第３の態様の図６に関連して議論したHTTP　POST要求を用いて送信されてよい。

【０２３３】

ステップ１１０４で、トークンは、支払人エンティティbob@nchain.comのためのデジタルウォレット又は装置の１つ以上のプロセッサにより、支払いサービスbsvaliasから受信される。このトークンは、幾つかの実施形態では、図１０のステップ１００４及び１００６で生成されたトークンと同じ又はそれに関連してよい。従って、トークンは要求に固有であり、alice@nchain.comの公開鍵に基づき検証可能なデジタル署名に関連付けられる。

【０２３４】

ステップ１１０６で、トークンに関連付けられたデジタル署名が受取人クライアントalice@nchain.comの公開鍵に関連するかどうかが決定され又は検証される。幾つかの実施形態では、このような検証は、例えばbsvaliasの機械可読リソース内のPKIテンプレートを用いてHTTP　GET要求に基づき、公開鍵を取得するステップと、取得した鍵がトークンを取得するためにデジタル署名を取得し又は暗号解除し又は復号するために使用できる（通常は同じ鍵ペアの秘密鍵を用いて適用される）デジタル署名に関連することを検証するステップと、を含む。

【０２３５】

デジタル署名がalice@nchain.comの取得した公開鍵を用いて検証できない場合、トークンはステップ１１１０で拒否され、要求は処理されない。

【０２３６】

デジタル署名が検証に成功した場合、ステップ１１０８で、支払人エンティティbob@nchain.comに関連するレコード又はデータベースが更新され、その結果、トークンはそれぞれの要求にリンクされる。これは、このトークンに関連付けられた任意の更なるメッセージ又は要求が非同期的方法で後の時間に受信されるとき、この要求が正しく且つ素早く識別できるようにするためである。このようなレコードは、支払人エンティティに関連付けられた１つ以上のメモリモジュール内にローカルに格納されてよく、又はサーバに、若しくは支払人エンティティの支払いサービスに関連付けて格納されてよい。従って、レコードは、支払人エンティティbob@nchain.comに関連付けられる限り、更新の前及び後のどこかで配置又は格納されてよい。

【０２３７】

ステップ１１１２で、コールバック要求が、受取人クライアントalice@nchain.comのbsvalias支払いサービスから受信される。このコールバック要求は、受取人クライアントが要求を認可した後に、従って、このような認可がbsvaliasにより受信されるとき及びそれと同期せずに又はその順序で到着した後に、提供される。コールバック要求は、ステップ１１０４と同じトークンを含み、要求に応答してアウトプットスクリプトも含み、このアウトプットスクリプトは、alice@nchain.comのための要求された支払先に関連付けられる。コールバック要求は、図１０のステップ１０１４で生成されたコールバック要求と同様であってよく、また、デジタル署名に関連付けられる。このコールバック要求は、支払人エンティティbob@nchain.comの支払いサービスbsvaliasのために機械可読リソース内のテンプレートに基づくHTTP　POST要求であってよい。

【０２３８】

ステップ１１１４で、コールバック要求内のデジタル署名が検証される。このような検証は、ステップ１１０６で議論した処理と同様であってよい。一旦検証されると、アウトプットスクリプト及びトークンが取得できる。

【０２３９】

alice@nchain.comの公開鍵に基づく検証が失敗した場合、コールバック要求は拒否され、ステップ１１２０でアウトプットスクリプトは生成されない。

【０２４０】

ステップ１１１４での検証が成功した場合、トークン及びアウトプットスクリプトが、支払人エンティティにより取得される。ステップ１１１６で、コールバック要求内のトークンは、ステップ１１０８で議論した更新されたレコード内のそれぞれの要求と相関される。従って、これは、正しい要求を、トークンを用いてアウトプットスクリプトと照合することを可能にする。

【０２４１】

要求がトークンに基づき更新されたレコード内で識別されると、アウトプットスクリプトは、ステップ１１１８で、分散台帳のために支払人エンティティによりトランザクションを構成するために使用でき、トランザクションは支払人エンティティ及び受取人クライアントに関連付けられる。

【０２４２】

図１２は、支払いサービスに関連付けられた１つ以上の支払いエンティティクライアントのために非同時性要求処理の能力を実施することに関する第５の態様の第３の実装による方法を示すフローチャートである。この場合には、示された方法は、宛先エンティティである支払人エンティティに関連付けられた１つ以上のプロセッサにより実行される。従って、方法は、図１０で議論した第５の態様の第１の実装に関連するが、同じ例から続けて、受取人クライアント、つまりalice@nchain.comによる実施に関係する。

【０２４３】

ステップ１２０２で、受取人クライアントのエイリアスに関連付けられた要求に関連する通知が受信される。上述の実施形態と同様に、受信した通知に関連する要求は、受取人クライアントalice@nchain.comの支払先に関連する。この通知は、受取人クライアントの支払いサービスbsvaliasにより送信される。受取人クライアントがオフラインである又は利用可能ではない又は電源断である場合、再びオンライン又は動作状態になると、この通知は、alice@nchain.comのためのデジタルウォレットに関連付けられたインタフェース上で提供される。

【０２４４】

ステップ１２０４で、受取人クライアントは、認可又は拒否するために、通知と相互作用する。このような相互作用は、ユーザインタフェース上のボタン又は表示されたオブジェクトをクリックすることにより、又は受取人クライアントのユーザインタフェースに関連付けられた入力インタフェース上の鍵の特定の組合せを使用して応答が認可又は拒否のうちの１つでることを示すことによってよい。

【０２４５】

ステップ１２０６で、応答が認可のものである場合、これは、支払いサービスbsvaliasにより送信される。ステップ１２０８で、代わりに応答が拒否のものである場合、このような拒否応答がbsvaliasへ送信されるから、或いは、代わりに、所定の期間の終了まで、例えば２日間、受取人が単に応答しないままであり、その後に、支払いサービスが単に通知が応答されなかったこと又は認可されなかったことを記録する。幾つかの実施形態では、これは、次に、図１０のステップ１０１８及び１０２０で拒否を促す。

【０２４６】

図１３は、公開鍵検証を実施するための上述のbsvaliasのような支払いサービスに関連付けられた機械可読リソース内で指定された命令の例示的なシーケンスを示す。これは、或いは、エイリアスに関連付けられた暗号鍵のための公開鍵オーナ検証技術と呼ばれる。これは、要求内の鍵が実際にエイリアス又は支払いエンティティ又はエイリアスに関連付けられたデジタルウォレットに関連することをチェックする能力に基づく。多くの場合、チェックされるべき鍵は、公開鍵のオーナを検証するために、秘密鍵を更に含む非対称鍵ペアの公開鍵である。この公開鍵は、要求を送信する支払いエンティティ又はクライアントにより既に知られている又は予め取得若しくはキャッシュされていてよい。図１３に関

連して議論した実施形態は、上述の本開示の第２～第５の態様のいずれかに含まれ又はそれに関連してよい。

【０２４７】

ステップ１３０２で、公開鍵検証要求テンプレートは支払いサービスに関連付けられた機械可読リソースから取得される。このテンプレートは、鍵検証又は検証エンドポイント識別子を要求するためのテンプレートである。これは、支払いエンティティの鍵を識別し及び／又は検証するために構成される、支払いサービスのコンピューティングリソースのURIである。例えば、上述の例から続けると、テンプレートは公開鍵オーナ検証エンドポイントに関連するbsvaliasのための機械可読リソース内の以下の能力又は命令に基づいてよい：

【数１６】

```
{
   "bsvalias": "1.0",
   "capabilities": {
      "ref: a9f510c16bde": "https://example.bsvalias.tld/api/ {name} @ {domain.tld}/
{pubkey}"
   }
}
```

【０２４８】

本例では、capabilities.a９f５１０c１６bdeの参照は、「public key（公開鍵）」のオーナシップを検証するためのテンプレートURLである。公開鍵は、既に、図４で議論した方法を用いて取得されていてよい。

【０２４９】

ステップ１３０２でテンプレートが受信されると、ステップ１３０４で、宛先エンティティのエイリアス、つまり受取人クライアント又は支払人エンティティは、テンプレートの適切なフィールドに含まれ又は代用されて、完全な公開鍵検証要求を生成する。これは、鍵検証要求とも呼ばれてよい。例えば、テンプレート値{name}及び{domain.tld}は、エイリアス、つまり〈name〉@〈domain〉.〈tld〉のコンポーネントを表し、機械可読リソース、つまり受取人クライアントのエイリアスalice@nchain.comに基づき完全な要求を発行する前に、代入されなければならない。このステップの結果は、alice@nchain.comの支払いサービス、つまりbsvaliasの公開鍵検証エンドポイント識別子の提供である。

【０２５０】

ステップ１３０６で、HTTP GET要求が、ステップ１３０４で取得されたエンドポイント識別子に基づき生成される。

【０２５１】

ステップ１３０８で、エイリアスに関連付けられた応答は、次に、ステップ１３０６で生成されたGET要求に応答して取得される。多くの場合、これは、単に、公開鍵が一致したこと又は要求内で示されたエイリアスについて検証されたことの指示であってよい。幾つかの実施形態では、検証の処理は、支払いサービスbsvaliasの全ての暗号鍵及び鍵ペアを管理することに関連付けられた鍵管理サーバにより行われてよい。例えば、鍵管理サーバは、bsvalias支払いサービスのクライアント毎の全部の現在の及び有効な公開鍵の詳細を含む最新のレコード又はルックアップテーブルを維持してよい。上述のように、及び図４に関連して、公開鍵は、ECDSA（elliptic curve digital signature algorithm）公開鍵であってよい。

【０２５２】

要求内の鍵が、要求内のエイリアスについて有効である、つまり、鍵のオーナが実際に

要求内のエイリアスに関連付けられた支払いエンティティである場合、支払いサービスの公開鍵検証を担うホストからの応答は、以下のフォーマットであってよい：

【数１７】

```
{
   "alias": <name@domain.tld> in the received request,
   "pubkey": <pubkey> in the received request,
   "match": true
}
```

【０２５３】

要求内の「pubkey」が要求内のエイリアスについて有効ではない、つまり、該エイリアスに関連付けられないものである、又は過去に有効であったかも知れないが少なくとも該エイリアスについてもはや有効ではない場合、応答メッセージ内の「match」フィールドは、値「偽」を示してよい。幾つかの実施形態では、この場合の応答は、単に、エラーが生じたこと、又は要求されたリソースが見付からない若しくは利用可能ではない若しくは認可されていないことを示してよい。

【０２５４】

図１４を参照すると、本開示の少なくとも一実施形態を実施するために使用され得るコンピューティング装置２６００の説明のための簡略ブロック図が提供される。種々の実施形態で、コンピューティング装置２６００は、上述の図示のシステムのうちのいずれかを実装するために使用されてよい。例えば、コンピューティング装置２６００は、支払いサービス又は支払いクライアントエンティティに関連付けられたウェブサーバ又は１つ以上のプロセッサ又はコンピューティング装置として使用するために、つまり支払いサービスの提供を担うホストを実施するよう、又は支払人若しくは受取人支払いクライアントエンティティを実施するよう構成されてよい。従ってコンピューティング装置２６００は、ポータブルコンピューティング装置、パーソナルコンピュータ、又は任意の電子コンピューティング装置であってよい。図１４に示すように、コンピューティング装置２６００は、主メモリ２６０８及び永久記憶装置２６１０を含む記憶サブシステム２６０６と通信するよう構成され得る１つ以上のレベルのキャッシュメモリ及びメモリ制御部（集合的に２６０２とラベル付けされる）を備える１つ以上のプロセッサを含んでよい。主メモリ２６０８は、図示のように、動的ランダムアクセスメモリ（ＤＲＡＭ）２６１８及び読み出し専用メモリ（ＲＯＭ）２６２０を含み得る。記憶サブシステム２６０６及びキャッシュメモリ２６０２は、本開示で説明されたようなトランザクション及びブロックに関連付けられた詳細事項のような情報の記憶のために使用されてよい。プロセッサ２６０２は、本開示で説明されたような任意の実施形態のステップ又は機能を提供するために利用されてよい。

【０２５５】

プロセッサ２６０２は、１つ以上のユーザインタフェース入力装置２６１２、１つ以上のユーザインタフェース出力装置２６１４、及びネットワークインタフェースサブシステム２６１６とも通信できる。

【０２５６】

バスサブシステム２６０４は、コンピューティング装置２６００の種々のコンポーネント及びサブシステムが意図した通りに互いに通信できるようにするメカニズムを提供してよい。バスサブシステム２６０４は、単一のバスとして概略的に示されるが、バスサブシステムの代替の実施形態は、複数のバスを利用してよい。

【０２５７】

ネットワークインタフェースサブシステム２６１６は、他のコンピューティング装置及びネットワークへのインタフェースを提供してよい。ネットワークインタフェースサブシ

ステム２６１６は、幾つかの実施形態では、コンピューティング装置２６００の他のシステムからデータを受信し及びそれへデータを送信するインタフェースとして機能してよい。例えば、ネットワークインタフェースサブシステム２６１６は、データ技術者が、装置をネットワークに接続することを可能にする。その結果、データ技術者は、データセンタのような遠隔地にいがなら、データを装置へ送信し、データを装置から受信できる。

【０２５８】

ユーザインタフェース入力装置２６１２は、キーボード、統合型マウス、トラックボール、タッチパッド、又はグラフィックタブレットのような指示装置、スキャナ、バーコードスキャナ、ディスプレイに組み込まれたタッチスクリーン、音声認識システム、マイクロフォンのようなオーディオ入力装置、及び他の種類の入力装置のような、１つ以上のユーザ入力装置を含んでよい。通常、用語「入力装置」の使用は、コンピューティング装置２６００に情報を入力する全ての可能な種類の装置及びメカニズムを含むことを意図する。

【０２５９】

１つ以上のユーザインタフェース出力装置２６１４は、ディスプレイサブシステム、プリンタ、又は音声出力装置のような非視覚ディスプレイ、等を含んでよい。ディスプレイサブシステムは、陰極線管（ＣＲＴ）、液晶ディスプレイ（ＬＣＤ）、発光ダイオード（ＬＥＤ）ディスプレイ、又はプロジェクションのような平面装置、又は他のディスプレイ装置を含んでよい。通常、用語「出力装置」の使用は、コンピューティング装置２６００から情報を出力する全ての可能な種類の装置及びメカニズムを含むことを意図する。１つ以上のユーザインタフェース出力装置２６１４は、例えば、ユーザインタフェースを提示して、ここに記載したプロセス及び変形を実行するアプリケーションとのユーザ相互作用が適切であるとき、そのような相互作用を実現するために使用されてよい。

【０２６０】

記憶サブシステム２６０６は、本開示の少なくとも１つの実施形態の機能を提供する基本プログラミング及びデータ構造を記憶するコンピュータ可読記憶媒体を提供してよい。アプリケーション（例えば、プログラム、コードモジュール、命令）は、１つ以上のプロセッサにより実行されると、本開示の１つ以上の実施形態の機能を提供し、記憶サブシステム２６０６に格納されてよい。これらのアプリケーションモジュール又は命令は、１つ以上のプロセッサ２６０２により実行されてよい。記憶サブシステム２６０６は、更に、本開示に従い使用されるデータを格納するレポジトリを提供する。例えば、主メモリ２６０８及びキャッシュメモリ２６０２は、プログラム及びデータのための揮発性記憶を提供できる。永久記憶装置２６１０は、プログラム及びデータの永久（不揮発性）記憶を提供でき、磁気ハードディスクドライブ、取り外し可能媒体に関連付けられた１つ以上のフロッピディスクドライブ、取り外し可能媒体に関連付けられた１つ以上の光ドライブ（例えば、ＣＤ－ＲＯＭ、又はＤＶＤ、又はＢｌｕｅ－Ｒａｙ）ドライブ、及び他の同様の記憶媒体を含んでよい。このようなプログラム及びデータは、本開示に記載した１つ以上の実施形態のステップを実行するためのプログラム、及び本開示に記載したトランザクション及びブロックに関連付けられたデータを含み得る。

【０２６１】

コンピューティング装置２６００は、ポータブルコンピュータ装置、タブレットコンピュータ、ワークステーション、又は後述する任意の他の装置を含む種々のタイプのものであってよい。さらに、コンピューティング装置２６００は、１つ以上のポート（例えば、USB、ヘッドフォンジャック、光コネクタ、等）を通じてコンピューティング装置２６００に接続可能な別の装置を含み得る。コンピューティング装置２６００に接続され得る装置は、光ファイバコネクタを受けるよう構成される複数のポートを含んでよい。従って、この装置は、光信号を、処理のために装置を接続するポートを通じてコンピューティング装置２６００に送信される電気信号に変換するよう構成されてよい。コンピュータ及びネットワークの絶えず変化する特性により、図１４に示したコンピューティング装置２６００の説明は、装置の好適な実施形態を説明する目的の特定の例としてのみ意図される。図１４に示したシステムより多くの又は少ないコンポーネントを有する多くの他の構成が可

能である。

【０２６２】

上述の実施形態は、本開示を限定するのではなく、説明すること、及び当業者は添付の特許請求の範囲により定められる本開示の範囲から逸脱することなく多くの代替的実施形態を考案できることに留意すべきである。請求項において、括弧内の任意の参照符号は、請求項を限定すると考えられるべきではない。用語「有する」及び「含む」（comprising、comprises）等は、任意の請求項又は明細書全体に列挙されたもの以外の要素又はステップの存在を排除しない。本願明細書では、「有する」は「有する又は構成される」を意味し、「含む」は「含む又は構成される」を意味する。要素の単数の参照は、そのような要素の複数の参照を排除しない。逆も同様である。本開示は、幾つかの別個の要素を含むハードウェアにより、及び適切にプログラムされたコンピュータにより、実装できる。幾つかの手段を列挙する装置クレームでは、これらの手段のうちの幾つかは、１つの同じハードウェアアイテムにより具現化されてよい。単に特定の手段が相互に異なる従属請求項に記載されるという事実は、これらの手段の組み合わせが有利に使用されないことを示さない。

【０２６３】

本開示は、ここで、第１～第３の態様に関連する以下の項に基づき議論される。これらは、ここで、請求される態様及び実施形態を一層良好に説明し、記載し、及び理解するために例示的な実施形態として提供される。

（項１）分散台帳に関連付けられたトランザクションのための１つ以上のクライアントのために支払いサービスを実施する、コンピュータにより実施される方法であって、前記方法は、

前記１つ以上のクライアントの中の所与のクライアントのためのエイリアスを提供するステップであって、前記エイリアスは前記所与のクライアントに固有であり、前記エイリアスはネットワーク識別子を含み又はそれに関連する、ステップと、

前記エイリアスを、ディレクトリ内の前記ネットワーク識別子に関連付けるステップと、

を含み、

前記関連付けるステップは、

前記ディレクトリ内の前記ネットワーク識別子に基づき、サービスレコードを生成するステップと、

前記支払いサービスが前記ネットワーク識別子に関連付けられたネットワーク又はドメインにより提供されることを示すよう、前記サービスレコードを更新するステップと、

前記支払いサービスを担うホストコンピューティングリソースの位置を示すよう、前記サービスレコードを更新するステップであって、前記ホストコンピューティングリソースは、前記エイリアスに関連するトランザクションに関する要求に応答して、前記エイリアスに関連付けられたデジタルウォレットの識別を実現するよう構成される、ステップと、

を含む、方法。

（項２）前記１つ以上のクライアントのうちの各クライアントは、デジタルウォレットに関連付けられる、項１に記載の方法。

（項３）前記エイリアスに関連付けられたトランザクションに関連する要求側エンティティからの要求に応答して、前記エイリアスに基づき前記ディレクトリの検索を実行するステップと、

前記ネットワーク識別子に関連する前記ディレクトリ内の前記支払いサービスの前記サービスレコードを識別するステップと、

前記支払いサービスのための前記ホストコンピューティングリソースの前記位置を返すステップであって、前記エイリアスに関連付けられた前記クライアントの公開アドレスは、前記返された位置に基づき決定され、前記公開アドレスは前記トランザクションの中で使用される、ステップと、

を含む項１又は２に記載の方法。

（項４）分散台帳のためのトランザクションに関連する方法であって、エイリアスが１つ

以上のクライアントの中の所与のクライアントのために提供され、前記エイリアスは前記所与のクライアントに固有であり、前記エイリアスはネットワーク識別子を含み又はそれに関連し、前記方法は、
要求側エンティティから、トランザクションに関連する要求を送信するステップであって、前記要求は前記エイリアスに関連付けられる、ステップと、
支払いサービスに関連付けられたホストコンピューティングリソースの位置を取得するステップであって、前記位置は、ディレクトリの検索において識別される前記ネットワーク識別子に関連するサービスレコードに基づく、ステップと、
を含み、
前記エイリアスに関連付けられた前記クライアントの公開アドレスは、前記位置に基づき決定され、前記公開アドレスは前記トランザクションの中で使用される、方法。
（項５）前記１つ以上のクライアントのうちの各クライアントは、デジタルウォレットに関連付けられる、項４に記載の方法。
（項６）前記ホストコンピューティングリソースの位置を返す前記ステップは、ターゲット及びポートペアを返すステップを含み、前記ターゲットは、前記ホストコンピューティングリソースの識別子を含み、前記ポートは、前記支払いサービスにより使用されるインターネットプロトコル通信ポートの識別子を含む、項１～５のいずれかに記載の方法。
（項７）前記ホストコンピューティングリソースは、前記エイリアスのネットワーク識別子に関連付けられたネットワークと異なる支払いネットワークに関連付けられ、前記ネットワークに登録された１つ以上のエンティティの前記支払いサービスは、前記支払いネットワークに関連付けられた支払いドメインに委任される（delegated to）、項１～６のいずれかに記載の方法。
（項８）前記ホストコンピューティングリソースは、支払いネットワークに関連付けられ、前記支払いネットワークの前記ドメインは、前記エイリアスの前記ネットワーク識別子に関連付けられた前記ネットワークの前記ドメインと同じである、項１～７のいずれかに記載の方法。
（項９）分散台帳に関連付けられたトランザクションのための１つ以上のクライアントのための支払いサービスを実施する、コンピュータにより実施される方法であって、前記方法は、
前記支払いサービスに関連付けられた機械可読リソースを生成するステップであって、前記機械可読リソースは、
各クライアントのための前記支払いサービスの実施を担うホストコンピューティングリソースに関連付けられた少なくとも１つのエンドポイント識別子であって、各クライアントはエイリアスに関連付けられ、前記エイリアスはネットワーク識別子を含み又はそれに関連する、少なくとも１つのエンドポイント識別子と、
前記支払いサービスによりサポートされる複数の能力の中の少なくとも１つの能力に関連付けられたエントリと、
前記エイリアスに関連付けられた公開アドレスにアクセスする又はそれを取得するための命令及び／又は仕様であって、前記公開アドレスは、前記エイリアスに関連付けられたトランザクションを実現するために使用される、命令及び／又は仕様と、
を含む、ステップと、
前記支払いサービスに関連付けられた予測可能な又知られた位置において、前記機械可読リソースを提供するステップと、
を含む方法。
（項１０）前記１つ以上のクライアントのうちの各クライアントは、デジタルウォレットに関連付けられる、項９に記載の方法。
（項１１）前記複数の能力は、以下：
支払人エンティティ又は受取人エンティティ検証、
トランザクションのための複数のデジタル署名、
トランザクションのための受取人エンティティ認可、

電子メールプロトコルに関連する支払いトランザクション、及び／又は、
コールバック要求又は応答、
のうちの１つ以上を含む、項９又は１０に記載の方法。
（項１２）項１～５のいずれか一項に記載の方法によりホストコンピューティングリソースの位置を決定するステップ、を更に含み、前記機械可読リソース内の前記エンドポイント識別子は、前記決定した位置に基づく、項９～１１のいずれかに記載の方法。
（項１３）エイリアスに関連付けられたトランザクションに関連する要求側エンティティから要求を受信することに応答して、前記方法は、
前記要求内の前記エイリアスに関連付けられた前記ネットワーク識別子に基づき、前記エイリアスに関連付けられた前記支払いサービスを識別するステップと、
前記識別された支払いサービスに基づき、前記予測可能な又は知られている位置から前記機械可読リソースにアクセスするステップと、
前記トランザクションのために必要な１つ以上の能力が前記機械可読リソース内に存在するかどうかを識別することに応答して、前記機械可読リソースから前記支払いサービスのための前記ホストコンピューティングリソースのエンドポイント識別子を返すステップと、
前記機械可読リソース内の前記命令及び／又は仕様のうちの１つ以上に基づき、前記エイリアスに関連付けられた公開アドレスを取得するステップと、
を含む方法。
（項１４）分散台帳のためのトランザクションに関連付けられた方法であって、エイリアスが１つ以上のクライアントの中の所与のクライアントのために提供され、前記エイリアスは前記所与のクライアントに固有であり、前記エイリアスはネットワーク識別子を含み又はそれに関連し、前記方法は、
要求側エンティティから、トランザクションに関連する要求を送信するステップであって、前記要求は前記エイリアスに関連付けられる、ステップと、
前記支払いサービスに関連付けられた位置から、前記機械可読リソースにアクセスするステップであって、前記支払いサービスは、前記エイリアス内の前記ネットワーク識別子に基づき識別され、前記機械可読リソースは項９に従い生成される、ステップと、
前記トランザクションのために必要な１つ以上の能力が前記機械可読リソース内に存在するかどうかを識別することに基づき、前記エイリアスに関連付けられた前記支払いサービスのための前記ホストコンピューティングリソースのエンドポイント識別子を受信するステップと、
前記機械可読リソース内の前記命令及び／又は仕様のうちの１つ以上を用いて、前記エイリアスに関連付けられた公開アドレスを取得するステップと、
を含む方法。
（項１５）各デジタルウォレットは前記ネットワーク内の前記支払いサービスについて登録されたユーザ又はエンティティに関連付けられ、各デジタルウォレットは、前記分散台帳上のトランザクションのための非対称暗号鍵ペアの公開鍵及び秘密鍵に関連付けられた暗号通貨ウォレットであり、前記公開アドレスを取得する前記ステップは、前記エイリアスに関連付けられた前記デジタルウォレットの前記公開鍵を取得するステップを含む、項１３又は１４に記載の方法。
（項１６）前記エイリアスに関連付けられた前記公開アドレスは、前記エイリアスに関連付けられた前記デジタルウォレットの前記公開鍵の暗号ハッシュに基づく、項１５に記載の方法。
（項１７）前記デジタルウォレットの前記公開鍵は、楕円曲線デジタル署名アルゴリズム（elliptic curve digital signature algorithm（ECDSA））公開鍵であり、前記公開鍵は、前記分散台帳に前に格納された又はそれにポストされた任意のトランザクションの部分ではない、項１５又は１６に記載の方法。
（項１８）前記機械可読リソースの中の前記１つ以上の命令及び／又は仕様は、
PKI（public key infrastructure）エンドポイント識別子について、前記機械可読リ

ソースからPKI要求テンプレートを取得することと、
前記エイリアス及び前記ネットワーク識別子を前記テンプレートに含めて、完全なPKI要求を生成することと、
前記エイリアスに関連付けられた公開鍵を取得するために、前記完全なPKI要求に基づき、HTTP GET要求を送信することと、
を含む、項１３～１７のいずれか一項に記載の方法。
（項１９）前記機械可読リソースの知られている又は予測可能な位置は、前記エンドポイント識別子、前記支払いサービスにより使用されるインターネットプロトコル通信ポート、及び／又は公衆アクセス可能なよく知られたドメインレポジトリに含まれる前記支払いサービスの構成仕様、のうちの少なくとも１つに基づく、項９～１８のいずれかに記載の方法。
（項２０）前記機械可読リソースは、JSON（Java Script Object Notation）フォーマットを用いて生成される、項９～１９のいずれかに記載の方法。
（項２１）前記エイリアスに関連付けられた前記公開アドレスを取得する前記ステップは、
エイリアスに関連付けられた受取人エンティティの支払先を取得するステップであって、前記支払先は、支払人エンティティから前記エイリアスへの暗号通貨支払いを行うトランザクションを構成する際に使用される、ステップを含み、
前記トランザクションを構成するステップは、
前記支払いサービスを識別することに基づき、前記機械可読リソースにアクセスするステップと、
前記機械可読ドキュメント内の１つ以上の命令及び／又は仕様に基づき、支払先エンドポイント識別子を返すステップと、
前記支払人エンティティから前記トランザクションの支払いの詳細を取得するステップであって、前記支払いの詳細は、前記受取人エンティティクライアントに関連付けられたエイリアス及び前記受取人に支払われるべき暗号通貨の額を含む、ステップと、
前記支払いの詳細を前記支払人エンティティに関連付けられた暗号鍵に関連付けられたデジタル署名を取得するステップと、
前記エイリアスに関連付けられた前記支払先エンドポイント識別子に関連付けられたアウトプットスクリプトを生成するステップであって、前記アウトプットスクリプトは、前記分散台帳のためのトランザクションに埋め込むために提供される、ステップと、
を含む、項１３～２０のいずれかに記載の方法。
（項２２）前記エイリアスに関連付けられた前記公開アドレスを取得する前記ステップは、
前記エイリアスに関連付けられた受取人エンティティの支払先を取得するステップであって、前記支払先は、支払人エンティティから前記エイリアスへの暗号通貨支払いを行うトランザクションを構成する際に使用される、ステップを含み、
前記トランザクションを構成するステップは、
前記支払人エンティティから、前記トランザクションに関する要求を送信するステップであって、前記要求は前記エイリアスに関連付けられる、ステップと、
前記支払いサービスに関連付けられた位置から前記機械可読リソースにアクセスするステップと、
前記機械可読リソース内の前記１つ以上の命令及び／又は仕様に基づき、支払先エンドポイント識別子を受信するステップと、
前記トランザクションの支払いの詳細を提供するステップであって、前記支払いの詳細は、前記受取人エンティティクライアントに関連付けられたエイリアスと前記受取人に支払われるべき暗号通貨の額とを含む、ステップと、
前記支払いの詳細を暗号鍵に関連付けるデジタル署名を提供するステップと、
前記エイリアスに関連付けられた前記支払先エンドポイント識別子に関連付けられたアウトプットスクリプトを受信するステップと、
前記分散台帳のためのトランザクションに前記受信したアウトプットスクリプトを埋め込むことにより、前記トランザクションを生成するステップと、

を含む、項１４～２０のいずれかに記載の方法。
（項２３）前記機械可読リソースの中の前記１つ以上の命令及び／又は仕様は、
支払先エンドポイント識別子について、前記機械可読リソースから支払先要求テンプレートを取得することと、
前記エイリアス及び前記ネットワーク識別子を前記テンプレートに含めて、完全な支払先要求を生成することと、
前記エイリアスに関連付けられた支払先エンドポイント識別子を取得するために、前記完全な支払先要求に基づき、HTTP　POST要求を送信することと、
を含む、項２１又は２２に記載の方法。
（項２４）前記エイリアス及び前記支払人エンティティの前記公開アドレスは、それぞれ、前記受取人エンティティ及び前記支払人エンティティに関連付けられたそれぞれのデジタルウォレットの公開鍵を含み、前記デジタル署名が、前記支払人エンティティのアイデンティティを検証するために使用される、項２１～２３のいずれかに記載の方法。
（項２５）前記支払人エンティティ及び前記受取人エンティティの両者に関連付けられたデジタル署名は、前記生成されたトランザクションが前記分散台帳に格納される又はポストされる前に、それぞれのエンティティの検証のために要求される、項２１～２４のいずれかに記載の方法。
（項２６）前記エイリアスは、クライアントに関連付けられた支払いハンドル（payment handle）である、項１～２５のいずれかに記載の方法。
（項２７）要求側エンティティからクライアントに関連付けられたエイリアスへのトランザクションに関連する要求を生成するためのプレフィックスを構成する方法であって、前記方法は、
前記プレフィックス及び前記エイリアスを含む、前記要求側エンティティからの要求を受信することに応答して、前記エイリアスに基づき項１～２６のいずれかに記載のステップをトリガするステップを含む方法。
（項２８）システムであって、
プロセッサと、
前記プロセッサによる実行の結果として、前記システムに項１～２７のいずれか一項に記載のコンピュータにより実施される方法を実行させる実行可能命令を含むメモリと、
を含むシステム。
（項２９）実行可能命令を記憶した非一時的コンピュータ可読記憶媒体であって、前記実行可能命令は、コンピュータシステムのプロセッサにより実行された結果として、前記コンピュータシステムに、項１～２８のいずれか一項に記載のコンピュータにより実施される方法を実行させる、非一時的コンピュータ可読記憶媒体。
【０２６４】
本開示は、請求される主題に関して、第４及び第５の態様に関連する以下の項に基づきここに議論される。これらの硬派、請求される態様及び実施形態を一層良好に説明し、記載し、及び理解するために提供される。
（項１）分散台帳に関連付けられたトランザクションに対する１つ以上のクライアントの支払いサービスを実施する、コンピュータにより実施される方法であって、前記方法は、
前記支払いサービスに関連付けられた機械可読リソースを更新するステップであって、前記機械可読リソースは、前記支払いサービスに関連付けられた予測可能な又は知られている位置で提供され又はそこからアクセス可能である、ステップを含み、
前記機械可読リソースは、
前記１つ以上のクライアントの中のクライアント毎に前記支払いサービスを実施することを担うホストコンピューティングリソースに関連付けられた少なくとも１つの識別子であって、各クライアントはエイリアスに関連付けられ、前記エイリアスは前記クライアントに固有である、１つ以上の識別子と、
前記支払いサービスによりサポートされる少なくとも１つの能力に関連付けられたエントリであって、各能力は前記支払いサービスに関連付けられた前記１つ以上のクライアン

トのためのそれぞれの能力を実施するプロトコル又は命令に関連付けられる、エントリと、
前記エイリアスに関連付けられた公開アドレスにアクセスする又はそれを取得するための１つ以上の命令及び／又は仕様であって、前記公開アドレスは前記エイリアスに関連付けられたトランザクションを実現するために使用される、１つ以上の命令及び／又は仕様と、
を含み、
更新する前記ステップは、前記支払いサービスによりサポートされる少なくとも１つの更なる能力を追加するステップを含み、
前記少なくとも１つの更なる能力は、
エイリアスの支払先を要求する支払人エンティティの検証であって、前記１つ以上のクライアントの中の所与のクライアントは前記エイリアスに関連付けられる、検証、及び／又は、
支払人エンティティからの要求の非同時性処理であって、前記要求はエイリアスの支払先に関連付けられ、前記１つ以上のクライアントの中の所与のクライアントは前記エイリアスに関連付けられる、非同時性処理と、
を含む、方法。
（項２）分散台帳に関連付けられたトランザクションに対する支払いサービスを実施する、コンピュータにより実施される方法であって、前記支払いサービスに関連付けられた１つ以上のクライアントの中のクライアントにエイリアスが提供され、前記エイリアスは前記クライアントに固有であり、各クライアントはそれぞれのエイリアスを提供され、前記方法は、
支払人エンティティから、エイリアスに関連付けられた要求を受信するステップであって、前記要求は、前記支払いサービスに関連付けられた前記１つ以上のクライアントの中の受取人クライアントの支払先に関連し、前記受取人クライアントは前記要求の中の前記エイリアスに関連付けられる、ステップと、
前記支払いサービスによりサポートされる少なくとも１つの能力に基づき、前記支払人エンティティを検証するステップであって、前記少なくとも１つの能力は、前記支払いサービスに関連付けられた機械可読リソースに含まれる、ステップと、
を含み、
前記検証するステップは、
前記支払人エンティティに関連付けられた公開鍵を取得するステップと、
前記支払人エンティティからの前記要求に基づき、所定の条件が満たされるかどうかを決定するステップと、
を含み、
前記所定の条件が満たされるという決定に基づき、
前記支払人エンティティ及び／又は前記支払人エンティティに関連付けられた前記要求を検証するステップと、
前記受取人クライアントの前記支払先に関連付けられたアウトプットスクリプトを生成するステップと、
前記支払人エンティティへ前記アウトプットスクリプトを送信するステップであって、前記アウトプットスクリプトは前記分散台帳のトランザクションに埋め込むために提供される、ステップと、
を含む、方法。
（項３）前記所定の条件が満たされないという決定に基づき、前記方法は、前記支払人エンティティから受信した要求を拒否する応答を生成し及び／又は送信するステップを含む項２に記載の方法。
（項４）前記受取人クライアントの前記支払いサービスは、項１に記載の方法により実施され、前記受取人クライアントの前記支払いサービスによりサポートされる前記少なくとも１つの能力は、項１の更新された機械可読リソースの中の少なくとも１つの更なる能力に基づく、項２又は３に記載の方法。

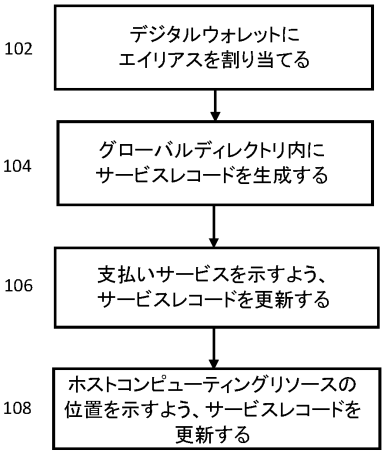
（項５）前記支払人エンティティからの前記エイリアスに関連付けられた前記要求は、以下：
前記要求が前記支払人エンティティから送信された日時を示すタイムスタンプ、及び／又は、
前記支払人エンティティの前記公開鍵に関連付けられたデジタル署名、及び／又は、
前記要求のためのワンタイムトークン、
を含むHTTP POST要求である、項２～４のいずれか一項に記載の方法。
（項６）所定の条件は、
前記要求に含まれる前記タイムスタンプが前記受取人クライアントに関連付けられた前記支払いサービスによる前記要求の受信時間の所定の期間内にあることを検証すること、及び／又は、
前記要求の中の前記デジタル署名が前記支払人エンティティの取得された公開鍵に関連することを検証すること、及び／又は、
前記ワンタイムトークンが前の要求のために使用されていないことを検証すること、
を含む、項５に記載の方法。
（項７）前記所定の期間は最大２分である、項６に記載の方法。
（項８）前記アウトプットスクリプトを送信する前記ステップは、
前記受取人クライアントの公開鍵に関連付けられたデジタル署名を前記アウトプットスクリプトに適用するステップと、
前記支払人エンティティへ、署名済みアウトプットスクリプトを送信するステップと、
を含む、項２～７のいずれか一項に記載の方法。
（項９）前記支払人エンティティは、前記受取人クライアントの前記支払いサービスと異なる支払いサービスに関連付けられ、前記異なる支払いサービスに関連付けられたエイリアスを割り当てられ、前記エイリアスは、前記支払人エンティティからの前記要求に含まれる、項１～８のいずれかに記載の方法。
（項１０）前記支払人エンティティは、前記受取人クライアントの前記支払いサービスと同じ支払いサービスに関連付けられ、前記同じ支払いサービスに関連付けられたエイリアスを割り当てられ、前記エイリアスは、前記支払人エンティティからの前記要求に含まれる、項１～９のいずれかに記載の方法。
（項１１）前記支払人エンティティに関連付けられた前記公開鍵を取得する前記ステップは、
前記支払人エンティティの前記支払いサービスに関連付けられた位置から機械可読リソースにアクセスするステップと、
前記機械可読リソースの中の公開鍵基盤（PKI）要求テンプレートに基づき、及び前記支払人エンティティの前記エイリアスに基づき、HTTP GET要求を送信するステップと、
応答して、前記エイリアスに関連付けられた前記公開鍵を取得するステップと、
を含む、項９又は１０に記載の方法。
（項１２）分散台帳のためのトランザクションに関連付けられた方法であって、支払いサービスに関連付けられた１つ以上のクライアントの中のクライアントにエイリアスが提供され、前記エイリアスは前記クライアントに固有であり、各クライアントはそれぞれのエイリアスに関連付けられ、前記方法は、
エイリアスに関連付けられた要求を生成するステップであって、前記要求は、前記支払いサービスに関連付けられた前記１つ以上のクライアントの中の受取人クライアントの支払先に関連し、前記受取人クライアントは前記要求の中の前記エイリアスに関連付けられる、ステップと、
支払人エンティティの公開鍵に関連付けられたデジタル署名を生成された要求に適用して、署名済み要求を取得するステップと、
前記エイリアスの前記支払いサービスに関連付けられた機械可読リソースにアクセスするステップと、
前記支払先に関連する前記機械可読リソースの中の１つ以上の命令及び／又は仕様に基

づき、前記署名済み要求を送信するステップであって、前記要求は送信の日時を示すタイムスタンプを含む、ステップと、
前記要求された支払先に関連付けられたアウトプットスクリプトを受信するステップと、
前記分散台帳のためのトランザクションに前記受信したアウトプットスクリプトを埋め込むステップであって、前記トランザクションは前記支払人エンティティ及び前記受取人クライアントに関連付けられる、ステップと、
を含む方法。
（項１３）前記受信したアウトプットスクリプトは、前記受取人クライアントに関連付けられた公開鍵に基づくデジタル署名を含み、前記方法は、前記署名を検証するステップであって、以下：
前記機械可読リソースの中の公開鍵基盤（PKI）要求テンプレートに基づき、及び前記受取人クライアントの前記エイリアスに基づき、HTTP GET要求を送信するステップと、
応答して、前記エイリアスに関連付けられた前記公開鍵を取得するステップと、
前記アウトプットスクリプト内の前記デジタル署名が前記受取人クライアントの前記取得した公開鍵に関連することを検証するステップと、
により前記署名を検証するステップを含む項１２に記載の方法。
（項１４）分散台帳に関連付けられたトランザクションのための支払いサービスを実施する、コンピュータにより実施される方法であって、前記支払いサービスに関連付けられた１つ以上のクライアントの中のクライアントにエイリアスが提供され、前記エイリアスは前記クライアントに固有であり、各クライアントはそれぞれのエイリアスを提供され、前記方法は、
支払人エンティティから、エイリアスに関連付けられた要求を受信するステップであって、前記要求は、前記支払いサービスに関連付けられた１つ以上のクライアントの中の受取人クライアントの支払先に関連し、前記受取人クライアントは前記要求の中の前記エイリアスに関連付けられる、ステップと、
前記支払いサービスによりサポートされる少なくとも１つの能力に基づき、前記要求の非同時性処理を実施するステップであって、前記少なくとも１つの能力は、前記支払いサービスに関連付けられた機械可読リソースを用いて識別され、前記非同時性処理は、
前記受信した要求に固有であるトークンを生成することと、
前記支払人エンティティへ前記トークンを送信することと、を含む、ステップと、
前記要求の認可を受信することに応答して、前記受取人クライアントの前記支払先に関連付けられたアウトプットスクリプトを生成するステップと、
前記トークンと前記生成されたアウトプットスクリプトとを含むコールバック要求を生成するステップと、
前記支払人エンティティへ前記コールバック要求を送信するステップであって、前記コールバック要求の中の前記アウトプットスクリプトは、前記分散台帳のためのトランザクションに埋め込むために提供される、ステップと、
を含む方法。
（項１５）前記要求の拒否を受信することに応答して、又は所定の期間が終了すると、前記方法は、前記支払人エンティティから受信した要求を拒否する応答を生成し送信するステップを含む項１４に記載の方法。
（項１６）前記受取人クライアントの前記支払いサービスは、項１に記載の方法により実施され、前記受取人クライアントの前記支払いサービスによりサポートされる前記少なくとも１つの能力は、項１の更新された機械可読リソースの中の少なくとも１つの更なる能力に基づく、項１４又は１５に記載の方法。
（項１７）前記要求の非同時性処理を実施する前記ステップは、前記受取人クライアントが、前記受取人エンティティから前記要求を受信した後に所定の期間の間、応答しない又はオフラインであることに応答して実行される、項１４～１６のいずれか一項に記載の方法。

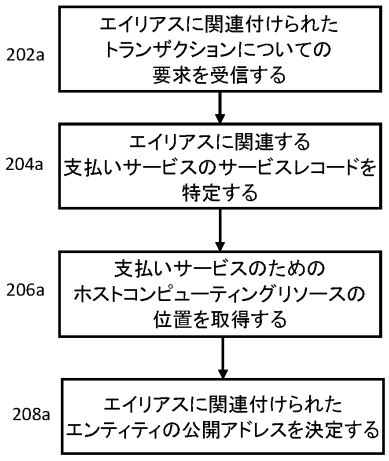
（項１８）前記受取人エンティティへ、前記要求に関する通知を送信するステップと、
前記受取人クライアントから前記要求の認可又は拒否を受信するステップと、
を更に含む項１４～１７のいずれか一項に記載の方法。
（項１９）前記トークンを送信するステップ及び／又は前記コールバック要求を送信するステップは、
前記受取人クライアントの公開鍵に関連付けられたデジタル署名を前記トークンに適用して、署名済みトークンを取得するか、又は前記コールバック要求の中の前記アウトプットスクリプトと前記トークンとの組合せに適用して、署名済みコールバック要求を取得するステップと、
前記支払人エンティティへ前記署名済みトークン又は署名済みコールバック要求を送信するステップと、
を含む、項１４～１８のいずれか一項に記載の方法。
（項２０）前記支払人エンティティは、前記受取人クライアントの前記支払いサービスと同じ又は異なる支払いサービスに関連付けられ、前記支払いサービスに関連付けられたエイリアスを割り当てられ、前記エイリアスは、前記支払人エンティティからの前記要求に含まれる、項１４～１９のいずれかに記載の方法。
（項２１）前記コールバック要求は、支払先要求テンプレート、前記トークン、及び前記支払人エンティティの前記エイリアスに基づくHTTP　POST要求であり、前記支払先要求テンプレートは、前記支払人エンティティの前記支払いサービスに関連付けられた機械可読リソースにアクセスすることにより取得される、項２０に記載の方法。
（項２２）項２～１１のいずれか一項に記載の方法に従い前記支払人エンティティを検証するステップ、を更に含む項１４～２１のいずれか一項に記載の方法。
（項２３）分散台帳のためのトランザクションに関連付けられた方法であって、支払いサービスに関連付けられた１つ以上のクライアントの中のクライアントにエイリアスが提供され、前記エイリアスは前記クライアントに固有であり、各クライアントはそれぞれのエイリアスに関連付けられ、前記方法は、
エイリアスに関連付けられた要求を生成するステップであって、前記要求は前記支払いサービスに関連付けられた前記１つ以上のクライアントの中の受取人クライアントの支払先に関連し、前記受取人クライアントは前記要求の中の前記エイリアスに関連付けられる、ステップと、
前記支払先に関連する機械可読リソースからアクセスされる１つ以上の命令及び／又は仕様に基づき、要求を送信するステップであって、前記機械可読リソースは前記支払いサービスに関連付けられる、ステップと、
前記支払いサービスからトークンを受信するステップであって、前記トークンは前記要求に固有であり、前記トークンはデジタル署名に関連付けられる、ステップと、
前記トークンに関連付けられた前記デジタル署名が前記受取人クライアントの公開鍵に関連することを検証するステップと、
検証が成功することに応答して、前記トークンに基づき前記要求に関連付けられたレコードを更新するステップと、
コールバック要求を受信するステップであって、前記コールバック要求は、前記トークンと前記要求される支払先に関連付けられたアウトプットスクリプトとを含み、前記コールバック要求はデジタル署名に関連付けられる、ステップと、
前記コールバック要求に関連付けられた前記デジタル署名が前記受取人クライアントの公開鍵に関連することを検証するステップと、
検証が成功することに応答して、前記コールバック要求の中の前記トークンを前記更新されたレコードに相関させるステップと、
前記分散台帳のためのトランザクションに前記受信したアウトプットスクリプトを埋め込むステップであって、前記トランザクションは前記支払人エンティティ及び受取人クライアントに関連付けられる、ステップと、
を含む方法。

（項２４）前記受信したトークン又はコールバック要求は、前記受取人クライアントに関連付けられた公開鍵に基づくデジタル署名を含み、前記デジタル署名を検証する前記ステップは、
前記機械可読リソースの中の公開鍵基盤（PKI）要求テンプレートに基づき、及び前記受取人クライアントの前記エイリアスに基づき、HTTP GET要求を送信するステップと、
応答して、前記エイリアスに関連付けられた前記公開鍵を取得するステップと、
前記トークン又は前記コールバック要求に関連付けられた前記デジタル署名が前記受取人クライアントの前記取得した公開鍵に関連することを検証するステップと、
を含む、項２３に記載の方法。
（項２５）前記方法は、
前記支払人エンティティを検証するための、項１２又は１３のいずれか一項に記載の方法のステップ、
を更に含む項２３及び２４のいずれか一項に記載の方法。
（項２６）分散台帳のためのトランザクションに関連付けられた方法であって、支払いサービスに関連付けられた１つ以上のクライアントの中のクライアントにエイリアスが提供され、前記エイリアスは前記クライアントに固有であり、各クライアントはそれぞれのエイリアスに関連付けられ、前記方法は、
受取人クライアントにより、エイリアスに関連付けられた要求の通知を受信するステップであって、前記要求は、前記支払いサービスに関連付けられた前記１つ以上のクライアントの中の前記受取人クライアントの支払先に関連し、前記受取人クライアントは前記要求の中の前記エイリアスに関連付けられる、ステップと、
前記受取人クライアントがオフラインであるとき、前記要求を認可又は拒否するステップであって、前記認可又は拒否は、インタフェースを用いて提供されるか、又は許可若しくは不許可要求プロパティに関連付けられた所定のレコードに基づく、ステップと、
前記認可又は拒否に基づき、前記支払いサービスに対する応答を送信するステップと、
を含む方法。
（項２７）前記要求は、項１４～２２のいずれか一項に記載の方法により前記支払いサービスにより処理される、項２６に記載の方法。
（項２８）前記支払いサービスに関連付けられた前記機械可読リソースの中の１つ以上の命令及び／又は仕様は、
PKIエンドポイント識別子について、前記機械可読リソースから公開鍵検証要求テンプレートを取得することと、
前記エイリアスを前記テンプレートに含めて、完全な公開鍵検証要求を生成することと、
前記要求の中の前記公開鍵が前記要求の中の前記エイリアスについて有効であることを検証するために、前記完全な公開鍵検証要求に基づき、HTTP GET要求を送信することと、
を含む、項１～２７のいずれか一項に記載の方法。
（項２９）コンピューティング装置又はシステムであって、
少なくとも１つのプロセッサと、
実行可能命令を含むメモリであって、実行可能命令は、前記少なくとも１つのプロセッサによる実行の結果として、前記コンピューティング装置又はシステムに項１～２８のいずれか一項に記載のコンピュータにより実施される方法を実行させる、メモリと、
を含むコンピューティング装置又はシステム。
（項３０）実行可能命令を記憶した非一時的コンピュータ可読記憶媒体であって、前記実行可能命令は、システム又はコンピューティング装置のプロセッサにより実行された結果として、前記システム又はコンピューティング装置に、項１～２８のいずれか一項に記載のコンピュータにより実施される方法を少なくとも実行させる、非一時的コンピュータ可読記憶媒体。
（項３１）分散台帳のためのトランザクションに関連付けられた方法であって、
支払人エンティティから要求を送信するステップであって、前記要求は受取人エンティ

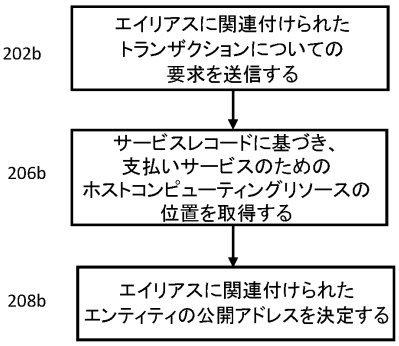
ティのエイリアスに基づく、ステップと、
前記要求に含まれるタイムスタンプ及び署名に基づき、前記支払人エンティティを検証するステップと、
検証の成功に応答して、前記支払人エンティティへアウトプットスクリプトを送信するステップと、
前記アウトプットスクリプトに基づき、トランザクションを生成するステップであって、前記トランザクションは前記分散台帳にポストされる、ステップと、
を含む方法。
（項３２）分散台帳のためのトランザクションに関連付けられた方法であって、
支払人エンティティから要求を送信するステップであって、前記要求は受取人エンティティのエイリアスに基づく、ステップと、
前記支払人エンティティへ前記要求の受信の肯定応答を提供するステップと、
前記受取人へ前記要求の通知を提供するステップと、
前記受取人エンティティがオンラインである又は利用可能であるとき、前記要求の認可を取得するステップと、
前記認可に応答して、前記支払人エンティティへアウトプットスクリプトを送信するステップと、
前記アウトプットスクリプトに基づき、トランザクションを生成するステップであって、前記トランザクションは前記分散台帳にポストされる、ステップと、
を含む方法。
（項３３）項３１に記載の方法を含む、項３２に記載の方法。
（項３４）システムであって、支払人エンティティと、受取人エンティティと、少なくとも前記受取人エンティティに関連付けられた支払いサービスとを含み、前記支払人エンティティ、受取人エンティティ、及び／又は前記支払いサービスは、それぞれ、項３１～３３のいずれか一項に記載の方法のステップを実施するためのコンピュータ可読命令を実行する少なくとも１つのプロセッサを含む、システム。
【図面】
【図１】



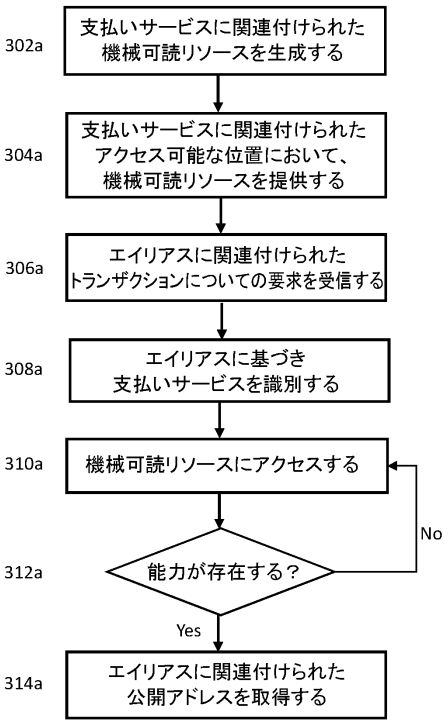
【図２Ａ】



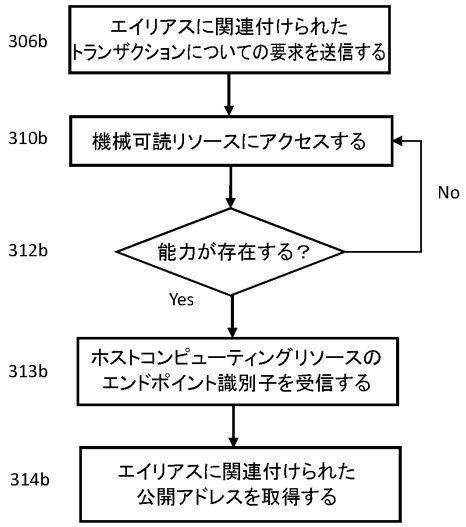
【図２Ｂ】



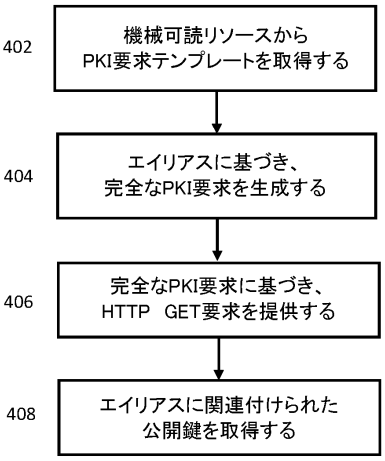
【図３Ａ】



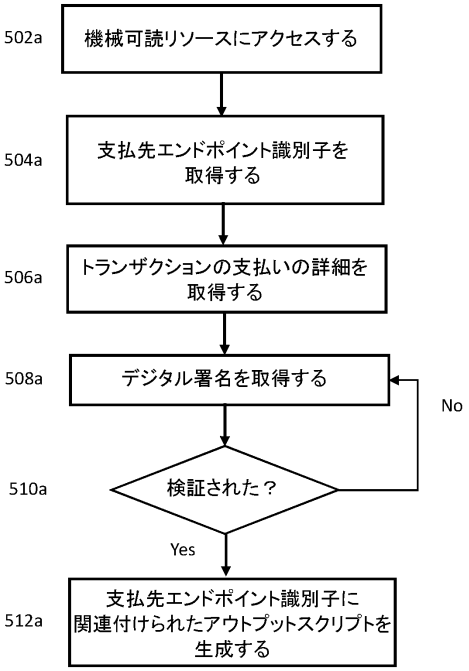
【図３Ｂ】



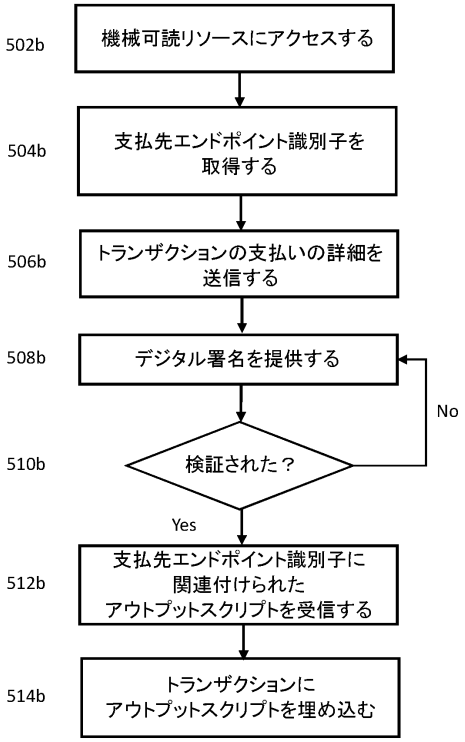
【図４】



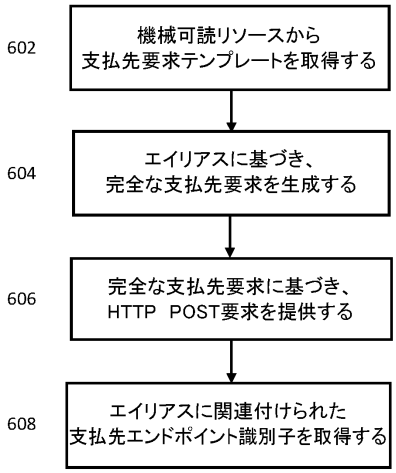
【図５Ａ】


502a
機械可読リソースにアクセスする
504a
支払先エンドポイント識別子を
取得する
506a
トランザクションの支払いの詳細を
取得する
508a
デジタル署名を取得する
No
510a
検証された？
Yes
512a
支払先エンドポイント識別子に
関連付けられたアウトプットスクリプトを
生成する

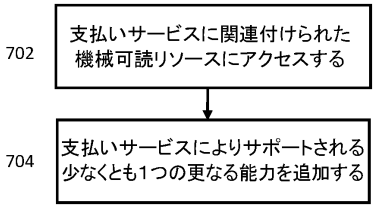
【図５Ｂ】


502b
機械可読リソースにアクセスする
504b
支払先エンドポイント識別子を
取得する
506b
トランザクションの支払いの詳細を
送信する
508b
デジタル署名を提供する
No
510b
検証された？
Yes
512b
支払先エンドポイント識別子に
関連付けられた
アウトプットスクリプトを受信する
514b
トランザクションに
アウトプットスクリプトを埋め込む

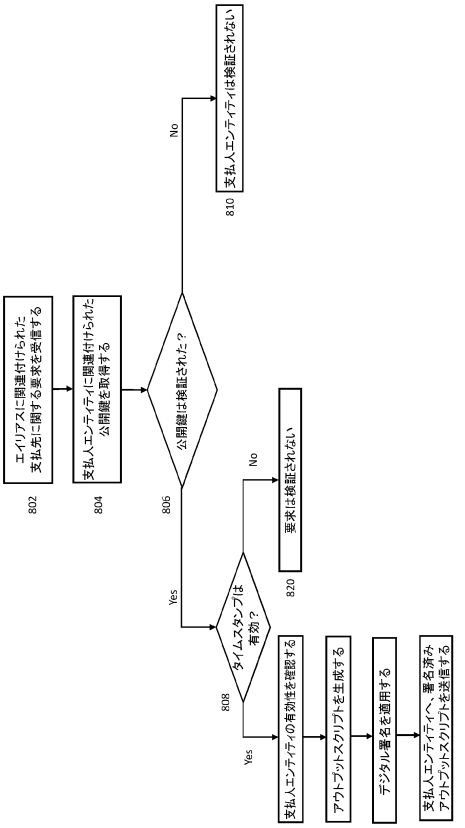
【図６】


602
機械可読リソースから
支払先要求テンプレートを取得する
604
エイリアスに基づき、
完全な支払先要求を生成する
606
完全な支払先要求に基づき、
HTTP POST要求を提供する
608
エイリアスに関連付けられた
支払先エンドポイント識別子を取得する

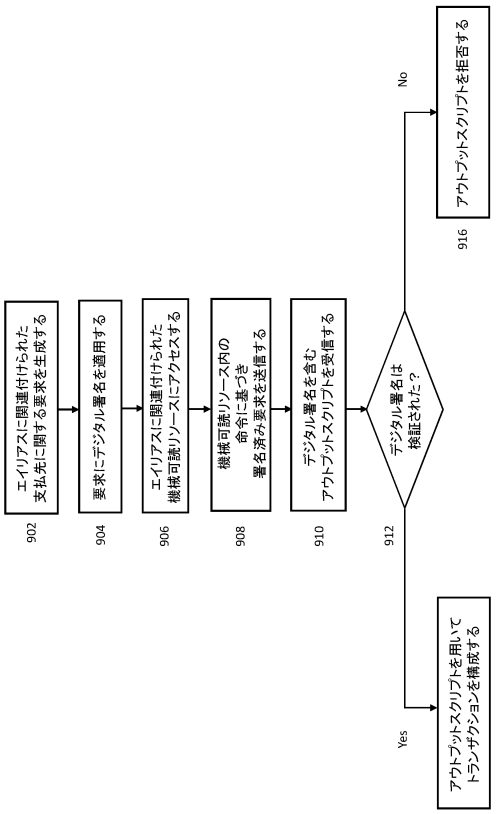
【図７】


702
支払いサービスに関連付けられた
機械可読リソースにアクセスする
704
支払いサービスによりサポートされる
少なくとも1つの更なる能力を追加する

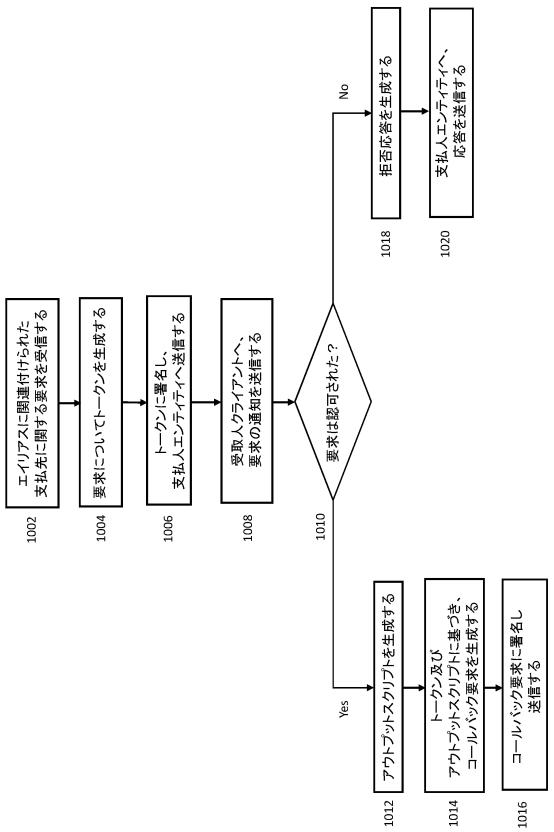
【図８】


エイリアスに関連付けられた支払先に関する要求を受信する
802
支払人エンティティに関連付けられた公開鍵を取得する
804
公開鍵は検証された？
806
No
支払人エンティティは検証されない
810
Yes
タイムスタンプは有効？
808
No
要求は検証されない
820
Yes
支払人エンティティの有効性を確認する
812
アウトプットスクリプトを生成する
814
デジタル署名を適用する
816
支払人エンティティへ、署名済みアウトプットスクリプトを送信する
818

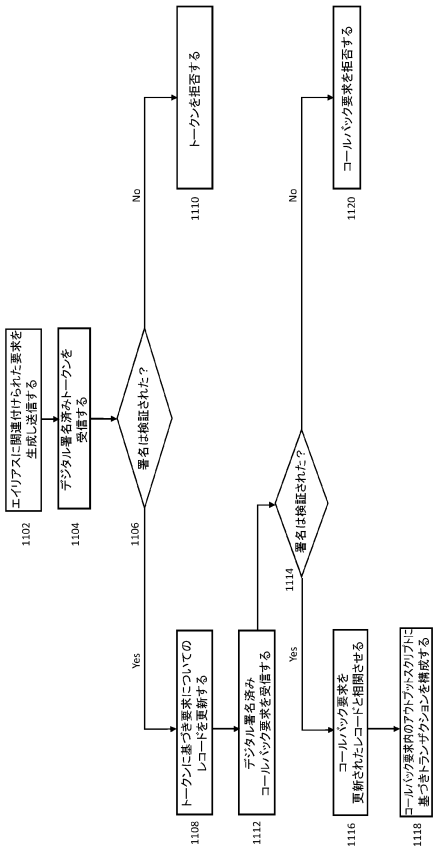
【図９】


エイリアスに関連付けられた支払先に関する要求を生成する
902
要求にデジタル署名を適用する
904
エイリアスに関連付けられた機械可読リソースにアクセスする
906
機械可読リソース内の命令に基づき署名済み要求を送信する
908
デジタル署名を含むアウトプットスクリプトを受信する
910
デジタル署名は検証された？
912
No
アウトプットスクリプトを拒否する
916
Yes
アウトプットスクリプトを用いてトランザクションを構成する
914

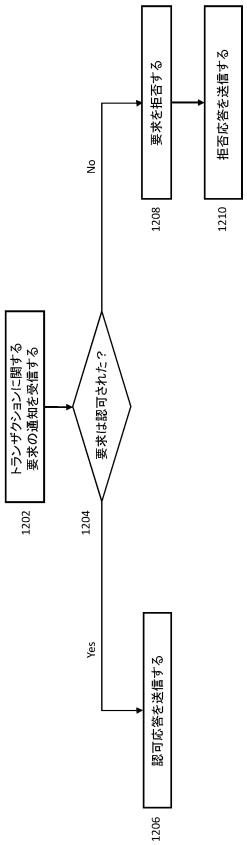
【図１０】


エイリアスに関連付けられた支払先に関する要求を受信する
1002
要求についてトークンを生成する
1004
トークンに署名し、支払人エンティティへ送信する
1006
受取人クライアントへ、要求の通知を送信する
1008
要求は認可された？
1010
No
拒否応答を生成する
1018
支払人エンティティへ、応答を送信する
1020
Yes
アウトプットスクリプトを生成する
1012
トークン及びアウトプットスクリプトに基づき、コールバック要求を生成する
1014
コールバック要求に署名し送信する
1016

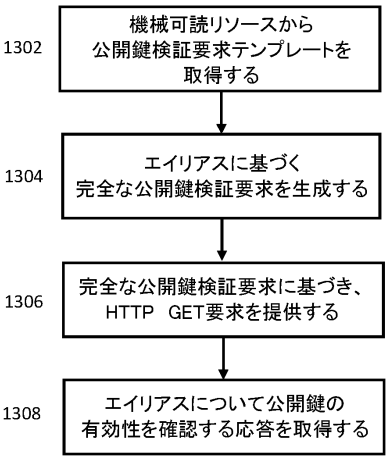
【図１１】


エイリアスに関連付けられた要求を生成し送信する
1102
デジタル署名済みトークンを受信する
1104
署名は検証された？
1106
No
トークンを拒否する
1110
Yes
トークンに基づき要求についてのレコードを更新する
1108
デジタル署名済みコールバック要求を受信する
1112
署名は検証された？
1114
No
コールバック要求を拒否する
1120
Yes
コールバック要求を更新されたレコードと相関させる
1116
コールバック要求のアウトプットスクリプトに基づきトランザクションを構成する
1118

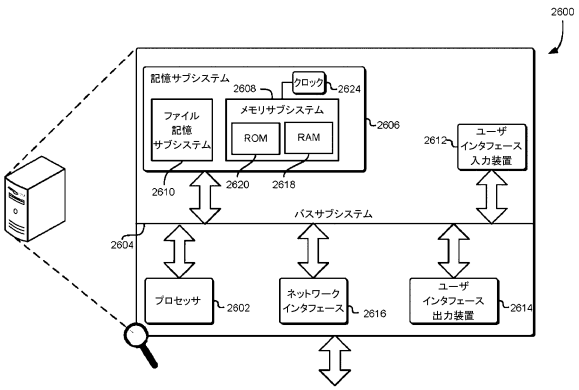
【図１２】


トランザクションに関する
要求の通知を受信する
1202
要求は認可されたか？
1204
No
要求を拒否する
1208
拒否応答を送信する
1210
Yes
認可応答を送信する
1206

【図１３】


1302
機械可読リソースから
公開鍵検証要求テンプレートを
取得する
1304
エイリアスに基づく
完全な公開鍵検証要求を生成する
1306
完全な公開鍵検証要求に基づき、
HTTP GET要求を提供する
1308
エイリアスについて公開鍵の
有効性を確認する応答を取得する

【図１４】


2600
記憶サブシステム
2608
クロック
2624
ファイル
記憶
サブシステム
メモリサブシステム
ROM
RAM
2606
2612
ユーザ
インタフェース
入力装置
2610
2620
2618
バスサブシステム
2604
プロセッサ
2602
ネットワーク
インタフェース
2616
ユーザ
インタフェース
出力装置
2614

フロントページの続き

(33)優先権主張国・地域又は機関
英国(GB)
内
審査官 青木 重徳
(56)参考文献 特表２０１６－５１９３５７（ＪＰ，Ａ）
国際公開第２０１８／１９３３４１（WO，Ａ１）
国際公開第２０１８／０８９８１５（WO，Ａ１）
国際公開第２０１９／０１４３３７（WO，Ａ１）
特許第６４４５２１１（ＪＰ，Ｂ１）
米国特許出願公開第２０１７／０２３０３５３（ＵＳ，Ａ１）
(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０６Ｆ ２１／６４
Ｇ０６Ｆ ２１／４４