(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7620733号
(P7620733)

(45)発行日　令和7年1月23日(2025.1.23)

(24)登録日　令和7年1月15日(2025.1.15)

(51)国際特許分類		FI		
H04L 9/32 (2006.01)		H04L	9/32	200Z
G06Q 20/06 (2012.01)		G06Q	20/06	

請求項の数　16　（全28頁）

(21)出願番号　特願2023-577760(P2023-577760)
(86)(22)出願日　令和4年6月17日(2022.6.17)
(65)公表番号　特表2024-525174(P2024-525174A)
(43)公表日　令和6年7月10日(2024.7.10)
(86)国際出願番号　PCT/SG2022/050420
(87)国際公開番号　WO2022/265581
(87)国際公開日　令和4年12月22日(2022.12.22)
審査請求日　令和6年1月29日(2024.1.29)
(31)優先権主張番号　17/350,646
(32)優先日　令和3年6月17日(2021.6.17)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　517187728
マスターカード アジア パシフィック ピーティーイー リミテッド
Ｍａｓｔｅｒｃａｒｄ Ａｓｉａ／Ｐａｃｉｆｉｃ Ｐｔｅ．Ｌｔｄ．
シンガポール国 １８９３５２ シンガポール フレイザー ストリート ３ デュオ タワー ナンバー１７－２１／２８
(74)代理人　100147485
弁理士　杉村 憲司
(74)代理人　230118913
弁護士　杉村 光嗣
(74)代理人　100224683
弁理士　齋藤 詩織
(72)発明者　スリナス ラヴィナサン

最終頁に続く

(54)【発明の名称】　ハッシュロックを使用して、仲介された相互台帳ステーブルコインのアトミックスワップのための方法及びシステム

(57)【特許請求の範囲】

【請求項１】

アトミックスワップを仲介するための方法であって、

処理サーバの受信機によって、第１のコンピューティング装置からスワップ要求を受信することであって、前記スワップ要求は、少なくとも、第１のブロックチェーンに関連付けられた第１のアドレスと、第２のブロックチェーンに関連付けられたネットワーク識別子とを含む、ことと、

前記処理サーバのプロセッサによって、少なくとも、前記ネットワーク識別子と、前記第２のブロックチェーンに関連付けられた第２のアドレスとに基づいて、第２のコンピューティング装置を識別することと、

前記処理サーバの前記プロセッサによって、証明値とハッシュロックとを生成することであって、前記ハッシュロックは少なくとも前記証明値を使用して生成される、ことと、

前記処理サーバの送信機によって、（ｉ）少なくとも、前記ハッシュロックと前記第２のアドレスとを前記第１のコンピューティング装置に、及び（ｉｉ）少なくとも、前記ハッシュロックと前記第１のアドレスとを前記第２のコンピューティング装置に、送信することと、

前記処理サーバの前記プロセッサによって、前記第１のアドレスへの第１の通貨額の転送のために前記第１のブロックチェーンに掲示された第１のブロックチェーントランザクションと、前記第２のアドレスへの第２の通貨額の転送のために前記第２のブロックチェーンに掲示された第２のブロックチェーントランザクションと、を検証することと、

前記処理サーバの前記送信機によって、少なくとも前記証明値を、前記第１のブロックチェーンに関連付けられた第１のブロックチェーンノードと、前記第２のブロックチェーンに関連付けられた第２のブロックチェーンノードと、に送信することと、
を含む、方法。
【請求項２】
請求項１に記載の方法において、前記第２のコンピューティング装置は、前記スワップ要求において識別される、方法。
【請求項３】
請求項１に記載の方法において、前記第２のコンピューティング装置を識別することは、
前記処理サーバの前記プロセッサによって、前記ネットワーク識別子に基づいて、複数の追加のコンピューティング装置の各々についての識別子を識別することと、
前記処理サーバの前記送信機によって、前記複数の追加のコンピューティング装置の各々についての前記識別子を前記第１のコンピューティング装置に送信することと、
前記処理サーバの前記受信機によって、前記第１のコンピューティング装置から、前記第２のコンピューティング装置に関連付けられた識別子を受信することと、
を含む、方法。
【請求項４】
請求項１に記載の方法において、前記スワップ要求は、前記第１の通貨額と前記第２の通貨額とを含む、方法。
【請求項５】
請求項１に記載の方法において、前記第１の通貨額と前記第２の通貨額とは、同じ額である、方法。
【請求項６】
請求項１に記載の方法において、
前記処理サーバの前記受信機によって、前記第２のコンピューティング装置から、前記第１のブロックチェーントランザクションに関連付けられた第１の通知データを受信することと、
前記処理サーバの前記受信機によって、前記第１のコンピューティング装置から、前記第２のブロックチェーントランザクションに関連付けられた第２の通知データを受信することと、
をさらに含む、方法。
【請求項７】
請求項６に記載の方法において、
前記第１の通知データと前記第２の通知データとは、前記第１のブロックチェーントランザクションと前記第２のブロックチェーントランザクションとを検証する前に受信され、
前記第１のブロックチェーントランザクションは、前記第１の通知データを使用して検証され、
前記第２のブロックチェーントランザクションは、前記第２の通知データを使用して検証される、方法。
【請求項８】
請求項１に記載の方法において、
前記処理サーバの前記プロセッサによって、少なくとも、前記第１の通貨額と、前記第２のコンピューティング装置に関連付けられた為替レートとに基づいて、前記第２の通貨額を計算すること、
をさらに含む、方法。
【請求項９】
アトミックスワップを仲介するためのシステムであって、
第１のコンピューティング装置と、
第２のコンピューティング装置と、
処理サーバと、を含み、前記処理サーバは、

前記第１のコンピューティング装置からスワップ要求を受信する受信機であって、前記スワップ要求は、少なくとも、第１のブロックチェーンに関連付けられた第１のアドレスと、第２のブロックチェーンに関連付けられたネットワーク識別子とを含む、受信機と、
プロセッサであって、
少なくとも、前記ネットワーク識別子と、前記第２のブロックチェーンに関連付けられた第２のアドレスとに基づいて、前記第２のコンピューティング装置を識別することと、
証明値とハッシュロックとを生成することと、を実行し、前記ハッシュロックは、少なくとも前記証明値を使用して生成される、プロセッサと、
（ｉ）少なくとも、前記ハッシュロックと前記第２のアドレスとを前記第１のコンピューティング装置に、及び（ｉｉ）少なくとも、前記ハッシュロックと前記第１のアドレスとを前記第２のコンピューティング装置に、送信する送信機と、を含み、
前記処理サーバの前記プロセッサは、前記第１のアドレスへの第１の通貨額の転送のために前記第１のブロックチェーンに掲示された第１のブロックチェーントランザクションと、前記第２のアドレスへの第２の通貨額の転送のために前記第２のブロックチェーンに掲示された第２のブロックチェーントランザクションと、をさらに検証し、
前記処理サーバの前記送信機は、少なくとも前記証明値を、前記第１のブロックチェーンに関連付けられた第１のブロックチェーンノードと、前記第２のブロックチェーンに関連付けられた第２のブロックチェーンノードと、にさらに送信する、システム。
【請求項１０】
請求項９に記載のシステムにおいて、前記第２のコンピューティング装置は、前記スワップ要求において識別される、システム。
【請求項１１】
請求項９に記載のシステムにおいて、前記第２のコンピューティング装置を識別することは、
前記処理サーバの前記プロセッサによって、前記ネットワーク識別子に基づいて、複数の追加のコンピューティング装置の各々についての識別子を識別することと、
前記処理サーバの前記送信機によって、前記複数の追加のコンピューティング装置の各々についての前記識別子を前記第１のコンピューティング装置に送信することと、
前記処理サーバの前記受信機によって、前記第１のコンピューティング装置から、前記第２のコンピューティング装置に関連付けられた識別子を受信することと、
を含む、システム。
【請求項１２】
請求項９に記載のシステムにおいて、前記スワップ要求は、前記第１の通貨額と前記第２の通貨額とを含む、システム。
【請求項１３】
請求項９に記載のシステムにおいて、前記第１の通貨額と前記第２の通貨額とは、同じ額である、システム。
【請求項１４】
請求項９に記載のシステムにおいて、前記処理サーバの前記受信機は、
前記第２のコンピューティング装置から、前記第１のブロックチェーントランザクションに関連付けられた第１の通知データと、
前記第１のコンピューティング装置から、前記第２のブロックチェーントランザクションに関連付けられた第２の通知データと、
をさらに受信する、システム。
【請求項１５】
請求項１４に記載のシステムにおいて、
前記第１の通知データと前記第２の通知データとは、前記第１のブロックチェーントランザクションと前記第２のブロックチェーントランザクションとを検証する前に受信され、
前記第１のブロックチェーントランザクションは前記第１の通知データを使用して検証され、

前記第２のブロックチェーントランザクションは前記第２の通知データを使用して検証される、システム。
【請求項１６】
請求項９に記載のシステムにおいて、前記処理サーバの前記プロセッサは、少なくとも、前記第１の通貨額と、前記第２のコンピューティング装置に関連付けられた為替レートとに基づいて、前記第２の通貨額をさらに計算する、システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、アトミックスワップの仲介に関する。本開示は、具体的には、仲介処理を使用して、アトミックスワップとハッシュロックとを使用して、別々のブロックチェーン台帳にわたって通貨をスワップすることを可能にすることに関する。
【背景技術】
【０００２】
ブロックチェーンは、暗号通貨を用いて決済トランザクションを行う際に使用するための記憶機構として最初に作成された。ブロックチェーンを使用することは、分散化、分散コンピューティング、トランザクションに関する透明性、さらにトランザクションに関与する個人又はエンティティに関する匿名性を提供すること、などの多くの利点を提供する。ブロックチェーンのより一般的な態様の１つは、それが不変の記録であることである。チェーンの一部であるすべてのトランザクションは、その内に格納され、特にチェーンがより長くなり、ブロックチェーンネットワークがより多くのノードを追加するにつれて、計算要件及び帯域幅制限のために変更されることができない。
【０００３】
ブロックチェーンの人気及び汎用性は、各々が独自の固有なデジタル通貨を利用する多数のブロックチェーンをもたらした。ブロックチェーンに関心のある多くのユーザ及びエンティティは、さまざまな理由で、複数のブロックチェーンに参加することに関心があることを見出し得る。結果として、そのようなユーザは、１つのブロックチェーン通貨を別のブロックチェーン通貨に交換すること、又は両方が異なる通貨を利用する別のユーザとのトランザクションに参加すること、に関心を有することがあり得る。伝統的に、そのようなトランザクションには２つの方法がある。第１は、取引所サービスを利用することである。これは、ユーザに秘密鍵を取引所に譲り渡すことを要求するか、又は両当事者に通貨を取引所に転送させるかのいずれかである。しかしながら、多くの当事者は、秘密鍵を譲り渡すこと、又はすべての資金を第三者に任せること、に関わる危険性のために、取引所を使用することに伴うどちらの選択肢にも警戒感を抱くことがある。第２の従来の方法は、アトミックスワップの使用である。アトミックスワップは、ハッシュロックを利用して、両当事者が通貨を受け取るであろう、又は当事者が受け取らないであろうについてのいずれかを確実にする。しかしながら、アトミックスワップは典型的には、両方のブロックチェーンが同じハッシュ化方法論を利用することを必要とし、両当事者が、アトミックスワップを達成するために必要とされるハッシュを生成して利用することが可能であることを必要とする。
【０００４】
したがって、従来のブロックチェーンウォレット機能を使用して当事者が自由に参加することができ、関与するブロックチェーンによって使用されるハッシュ方法論に依存しない、アトミックスワップを実行するための技術的改善が必要とされている。
【発明の概要】
【０００５】
本開示は、アトミックスワップを仲介するためのシステム及び方法の説明を提供する。処理サーバは、ハッシュロックに必要なデータを生成する。このデータは、使用される証明値を含む。処理サーバは、アドレスとハッシュロックとを両当事者に提供することによって、アトミックスワップに関与する両当事者の仲介として働く。当事者は、処理サーバ

によって提供されるハッシュロックとアドレスとを使用して、必要なトランザクションを行う。処理サーバは、両方のトランザクションが適切なブロックチェーンに掲示(post)されたことを検証し、次に、証明値を提供して、ブロックチェーンにハッシュロックを解放させ、それによって、当事者に資金を解放する。処理サーバを使用することは、両当事者が、ハッシュロック自体を生成する必要なく、又は他の当事者と通信することさえしなくても、アトミックスワップを利用することを可能にする。これは、より容易な実行と、より大きな安全性とを提供する。その結果、関係する当事者にとってより安全でより実行し易い、改良されたアトミックスワップがもたらされる。

【０００６】

アトミックスワップを仲介するための方法は、処理サーバの受信機によって、第１のコンピューティング装置からスワップ要求を受信することであって、前記スワップ要求は、少なくとも、第１のブロックチェーンに関連付けられた第１のアドレスと、第２のブロックチェーンに関連付けられたネットワーク識別子とを含む、ことと、前記処理サーバのプロセッサによって、少なくとも、前記ネットワーク識別子と、前記第２のブロックチェーンに関連付けられた第２のアドレスとに基づいて、第２のコンピューティング装置を識別することと、前記処理サーバの前記プロセッサによって、証明値とハッシュロックとを生成することであって、前記ハッシュロックは少なくとも前記証明値を使用して生成される、ことと、前記処理サーバの送信機によって、（ｉ）少なくとも、前記ハッシュロックと前記第２のアドレスとを前記第１のコンピューティング装置に、及び（ｉｉ）少なくとも、前記ハッシュロックと前記第１のアドレスとを前記第２のコンピューティング装置に、送信することと、前記処理サーバの前記プロセッサによって、前記第１のアドレスへの第１の通貨額の転送のために前記第１のブロックチェーンに掲示された第１のブロックチェーントランザクションと、前記第２のアドレスへの第２の通貨額の転送のために前記第２のブロックチェーンに掲示された第２のブロックチェーントランザクションと、を検証することと、前記処理サーバの前記送信機によって、少なくとも前記証明値を、前記第１のブロックチェーンに関連付けられた第１のブロックチェーンノードと、前記第２のブロックチェーンに関連付けられた第２のブロックチェーンノードと、に送信することと、を含む。

【０００７】

アトミックスワップを仲介するためのシステムは、第１のコンピューティング装置と、第２のコンピューティング装置と、処理サーバと、を含み、前記処理サーバは、前記第１のコンピューティング装置からスワップ要求を受信する受信機あって、前記スワップ要求は、少なくとも、第１のブロックチェーンに関連付けられた第１のアドレスと、第２のブロックチェーンに関連付けられたネットワーク識別子とを含む、受信機と、プロセッサであって、少なくとも、前記ネットワーク識別子と、前記第２のブロックチェーンに関連付けられた第２のアドレスとに基づいて、前記第２のコンピューティング装置を識別することと、証明値とハッシュロックとを生成することと、を実行し、前記ハッシュロックは、少なくとも前記証明値を使用して生成される、プロセッサと、（ｉ）少なくとも、前記ハッシュロックと前記第２のアドレスとを前記第１のコンピューティング装置に、及び（ｉｉ）少なくとも、前記ハッシュロックと前記第１のアドレスとを前記第２のコンピューティング装置に、送信する送信機と、を含み、前記処理サーバの前記プロセッサは、前記第１のアドレスへの第１の通貨額の転送のために前記第１のブロックチェーンに掲示された第１のブロックチェーントランザクションと、前記第２のアドレスへの第２の通貨額の転送のために前記第２のブロックチェーンに掲示された第２のブロックチェーントランザクションと、をさらに検証し、前記処理サーバの前記送信機は、少なくとも前記証明値を、前記第１のブロックチェーンに関連付けられた第１のブロックチェーンノードと、前記第２のブロックチェーンに関連付けられた第２のブロックチェーンノードと、にさらに送信する。

【０００８】

本開示の範囲は、添付の図面と併せて読まれるとき、例示的な実施形態の以下の詳細な

説明から最もよく理解される。図面に含まれるのは、以下の図である。
【図面の簡単な説明】
【０００９】
【図１】例示的な実施形態による、アトミックスワップを仲介するための高位レベルのシステムアーキテクチャを示すブロック図である。
【図２】例示的な実施形態による、アトミックスワップを仲介するための図１のシステムの処理サーバを示すブロック図である。
【図３Ａ】例示的な実施形態による、図１のシステムにおいて、仲介されたアトミックスワップを実行するための処理を示すフロー図である。
【図３Ｂ】例示的な実施形態による、図１のシステムにおいて、仲介されたアトミックスワップを実行するための処理を示すフロー図である。
【図４】例示的な実施形態による、アトミックスワップを仲介するための例示的な方法を示すフローチャートである。
【図５】例示的な実施形態によるコンピュータシステムアーキテクチャを示すブロック図である。
【発明を実施するための形態】
【００１０】
本開示のさらなる適用分野は、以下に提供される詳細な説明から明らかになるであろう。例示的な実施形態の詳細な説明は、例示の目的のみを意図するものであり、したがって、必ずしも本開示の範囲を限定することを意図するものではないことを理解されたい。
【００１１】
用語集
ブロックチェーン－ブロックチェーンに基づく通貨のすべてのトランザクションの公開台帳。１つ以上のコンピューティング装置はブロックチェーンネットワークを含むことができる。これにより、ブロックチェーン内のブロックの一部として、トランザクションを処理及び記録するように構成されることができる。ブロックが完成されると、ブロックはブロックチェーンに追加され、トランザクション記録がこれにより更新される。多くの事例では、ブロックチェーンは、時系列順のトランザクション台帳とすることができる、又はブロックチェーンネットワークによる使用に適し得る任意の他の順序で提示されることができる。ある構成では、ブロックチェーン内に記録されたトランザクションは、宛先アドレス及び通貨額を含むことができ、ブロックチェーンは、どのくらいの通貨が特定のアドレスに帰属可能であるかを記録する。ある事例では、あるトランザクションは、金融、他のトランザクションは、金融ではない、又はトランザクションは、送信元アドレス、タイムスタンプなどの追加の若しくは異なる情報を含み得る。ある実施形態では、ブロックチェーンは、さらに又は代替として、その操作者によるものでさえ改竄及び修正に対して強固にされたデータ記録の連続的に増大する一覧を維持する分散データベース内に配置される、又は配置される必要があるトランザクションの形態として、ほぼ任意の種類のデータを含むことができる。ある実施形態では、ブロックチェーンは、作業の証明(proof of work)及び／又はそれに関連付けられる任意の他の適切な検証技術を介して、ブロックチェーンネットワークによって確認され、検証されることができる。ある場合では、所与のトランザクションに関するデータは、トランザクションデータに付加されたトランザクションの直接的な一部ではない追加のデータをさらに含むことができる。ある事例では、ブロックチェーン内にそのようなデータを含めることは、トランザクションを構成することができる。そのような事例では、ブロックチェーンは、特定のデジタル通貨、仮想通貨、フィアット（不換）通貨、又は他の種類の通貨に直接関連付けられないとすることができる。
【００１２】
アトミックスワップを仲介するためのシステム
図１は、仲介を利用して２つのブロックチェーン間のアトミックスワップを実行するためのシステム１００を示す。

【００１３】
システム１００は、ブロックチェーンネットワーク１０６ａ及び１０６ｂとして図１に示される、２つの異なるブロックチェーンネットワーク１０６の間で生じるアトミックスワップを可能にするように構成されることができる。各ブロックチェーンネットワーク１０６は、複数の異なるブロックチェーンノードから構成されることができる。ある実施形態では、１つ以上のブロックチェーンノードは、ブロックチェーンネットワーク１０６ａ及び１０６ｂの両方を含む２つ以上のブロックチェーンネットワーク１０６内のノードとすることができる。各ブロックチェーンノードは、以下でより詳細に論じられ、図５に示されるようなコンピューティングシステムとすることができる。コンピューティングシステムは、ブロックチェーンの処理及び管理に関連した機能を実行するように構成される。この機能は、ブロックチェーンデータ値の生成と、提案されたブロックチェーントランザクションの検証と、デジタル署名の検証と、新しいブロックの生成と、新しいブロックの検証と、ブロックチェーンの複製の維持とを含む。

【００１４】
ブロックチェーンは、少なくとも複数のブロックから構成される分散台帳とすることができる。各ブロックは、少なくとも、ブロックヘッダと、１つ以上のデータ値とを含むことができる。各ブロックヘッダは、少なくとも、タイムスタンプと、ブロック参照値と、データ参照値とを含むことができる。タイムスタンプは、ブロックヘッダが生成された時間とすることができ、任意の適切な方法（例えば、ＵＮＩＸタイムスタンプ、日時型(DateTime)など）を使用して表されることができる。ブロック参照値は、ブロックチェーン内のより前のブロックを（例えば、タイムスタンプに基づいて）参照する値とすることができる。ある実施形態では、ブロックヘッダ内のブロック参照値は、それぞれのブロックの前にごく最近追加されたブロックのブロックヘッダへの参照とすることができる。例示的な実施形態では、ブロック参照値は、ごく最近追加されたブロックのブロックヘッダのハッシュ化を介して生成されたハッシュ値とすることができる。データ参照値は同様に、ブロックヘッダを含むブロック内に格納された１つ以上のデータ値への参照とすることができる。例示的な実施形態では、データ参照値は、１つ以上のデータ値のハッシュ化を介して生成されたハッシュ値とすることができる。例えば、ブロック参照値は、１つ以上のデータ値を使用して生成されたマークルツリーのルートとすることができる。

【００１５】
各ブロックヘッダ内のブロック参照値及びデータ参照値の使用は、ブロックチェーンが不変であることをもたらすことができる。何らかのデータ値への修正を試みると、そのブロックについて新しいデータ参照値の生成が必要になり、それによって、後続のブロックのブロック参照値が新たに生成されることが必要になり、さらに、すべての後続のブロック内に新しいブロック参照値を生成することが必要になる。これは、変更を永続的にするために、新しいブロックを生成して新しいブロックをブロックチェーンに追加する前に、ブロックチェーンネットワーク１０６内のすべての単一のブロックチェーンノードにおいて実行され、更新されなければならない。不可能ではないにしても、計算上及び通信上の制限は、そのような修正を非常に困難にし、したがって、ブロックチェーンを不変にすることができる。

【００１６】
ある実施形態では、ブロックチェーンは、２つの異なるブロックチェーンウォレット間で行われるブロックチェーントランザクションに関する情報を格納するために使用されることができる。ブロックチェーンウォレットは、暗号鍵ペアのうちの秘密鍵を含むことができる。これは、ブロックチェーントランザクションの支払人による承認として機能するデジタル署名を生成するために使用される。デジタル署名は、暗号鍵ペアのうちの公開鍵を使用して、ブロックチェーンネットワーク１０６によって検証されることができる。ある場合では、用語「ブロックチェーンウォレット」は、特に秘密鍵を指すことができる。他の場合では、用語「ブロックチェーンウォレット」は、ブロックチェーントランザクションにおいて使用するための秘密鍵を格納するコンピューティング装置（例えば、処理サ

ーバ１０２、第１の参加者装置１０８、又は第２の参加者装置１１０）を指すことができる。例えば、各コンピューティング装置は、それぞれの暗号鍵ペアについて独自の秘密鍵を各々有することができ、それぞれ、ブロックチェーンネットワークに関連付けられたブロックチェーンとのトランザクションの際に使用するためのブロックチェーンウォレットとすることができる。コンピューティング装置は、ブロックチェーンウォレットを格納して利用するのに適した任意の種類の装置とすることができ、例えば、デスクトップコンピュータ、ラップトップコンピュータ、ノートブックコンピュータ、タブレットコンピュータ、携帯電話、スマートフォン、スマートウォッチ、スマートテレビ、装着型コンピューティング装置、埋め込み型コンピューティング装置などである。

【００１７】

ブロックチェーン内に格納された各ブロックチェーンデータ値は、適用可能な場合、ブロックチェーントランザクション又は他のデータの記憶に対応することができる。ブロックチェーントランザクションは、少なくとも、送信者の秘密鍵を使用して生成される、通貨の送信者（例えば、第１の参加者装置１０８）のデジタル署名と、受信者の公開鍵を使用して生成される、通貨の受信者（例えば、第２の参加者装置１１０）のブロックチェーンアドレスと、転送されるブロックチェーン通貨額又は格納される他のデータと、から構成されることができる。通貨とは別のデータ記憶のために使用されるブロックチェーンの場合、通貨額は、そのような他のデータによって置き換えられることができる。また、あるブロックチェーントランザクションでは、トランザクションは、ブロックチェーン通貨が現在格納される（例えば、デジタル署名がそのような通貨へのアクセスを証明する）、送信者の１つ以上のブロックチェーンアドレスと、送信者によって保持される任意の変更のために送信者の公開鍵を使用して生成されるアドレスと、を含むことができる。将来のトランザクションにおいて使用され得る、暗号通貨が送信されたアドレスは「出力」アドレスと呼ばれ、これは、各アドレスが前のブロックチェーントランザクションの出力を捕捉するために以前に使用されたものであり、「未使用トランザクション」とも呼ばれ、これはその通貨が依然として未使用である前のトランザクションにおいてアドレスに送信された通貨があるためである。また、ある場合では、ブロックチェーントランザクションは、トランザクションを検証する際のエンティティによる使用のために、送信者の公開鍵を含むことができる。ブロックチェーントランザクションの従来の処理のために、そのようなデータは、送信者又は受信者のいずれかによって、ブロックチェーンネットワーク１０６内のブロックチェーンノードに提供されることができる。ノードは、送信者のウォレットの暗号鍵ペア内の公開鍵を使用してデジタル署名を検証することができる。また、ノードは、（例えば、未使用トランザクションがまだ使用されておらず、送信者のウォレットに関連付けられたアドレスに送信された）送信者の資金へのアクセス、トランザクションの「確認」として知られる処理、を検証し、次に、ブロックチェーントランザクションを新しいブロック内に含むことができる。新しいブロックは、従来のブロックチェーン実装では、ブロックチェーンに追加され、ブロックチェーンネットワーク１０６内のブロックチェーンノードのすべてに分散される前に、ブロックチェーンネットワーク１０６内の他のノードによって検証されることができる。ブロックチェーンデータ値がブロックチェーントランザクションに関連されないが、代わりに他の種類のデータの記憶に関連され得る場合、ブロックチェーンデータ値は、依然として、デジタル署名の検証を含む、又は、デジタル署名の検証を伴うことができる。

【００１８】

システム１００は、処理サーバ１０２を含むことができる。処理サーバ１０２は、以下でより詳細に論じられるように、アトミックスワップを実行するために、第１の参加者装置１０８と第２の参加者装置１１０との間の仲介として働いて、本明細書では第１のブロックチェーンと呼ばれる第１のブロックチェーンネットワーク１０６ａに関連付けられたブロックチェーン内のブロックチェーン通貨を、本明細書では第２のブロックチェーンと呼ばれる第２のブロックチェーンネットワーク１０６ｂに関連付けられたブロックチェーン内のブロックチェーン通貨と交換するように構成されることができる。処理を開始する

ために、第１の参加者装置１０８は、任意の適切な通信ネットワーク及び方法を使用して、スワップ要求を処理サーバ１０２に提出することができる。例えば、第１の参加者装置１０８は、処理サーバ１０２にスワップ要求を提出するように構成されたアプリケーションプログラムを含むことができる、スワップ要求を提出することができるウェブサイトにアクセスすることができる、又は処理サーバ１０２に関連付けられたアプリケーションプログラミングインタフェースにアクセスすることができる。

【００１９】

スワップ要求は、第１の参加者装置１０８が（例えば、第１のブロックチェーンにおいて）通貨を受け取ることを望むブロックチェーン上の宛先アドレスを少なくとも含むことができる。この宛先アドレスは、本明細書では第１のアドレスと呼ばれることができる。宛先アドレスは、第１の参加者装置１０８によって、ブロックチェーンウォレットを使用して生成されることができる。例えば、第１のブロックチェーンに関連付けられた暗号鍵ペアの公開鍵を用いてアドレスを生成することによって、行われる。スワップ要求はまた、通貨額を含むことができる。この通貨額は、第１の参加者装置１０８に関連付けられたユーザが、第２のブロックチェーン上で転送することを望む、又は第１のブロックチェーン上で受け取ることを望むブロックチェーン通貨の額とすることができる。ある場合では、スワップ要求は、両方の通貨額、すなわち、ユーザが第２のブロックチェーン上でどのくらいの額を転送することを望むか、及びユーザが第１のブロックチェーン上でどのくらいの額を受け取ることを望むか、を含むことができる。他の場合では、以下で論じられるように、１つの通貨額のみが提供されることができる。他の額は、ブロックチェーンネットワーク１０６と第２の参加者装置１１０との両方に依存し得る為替レートなどに基づいて、決定されることができる。ある実施形態では、スワップ要求はまた、第１のブロックチェーン及び／又は第２のブロックチェーンについての識別子を含むことができる。この識別子は、それぞれのブロックチェーン、関連付けられたブロックチェーンネットワーク１０６、又はそれぞれのブロックチェーンによって使用されるブロックチェーン通貨に関連付けられた一意の識別値とすることができる。スワップ要求がそのような識別子を含まない場合、処理サーバ１０２は、含まれる通貨額に基づいてブロックチェーン及び／又はブロックチェーンネットワーク１０６を識別するように構成されることができる（例えば、通貨自体が指定される場合、それは、処理サーバ１０２によって、適切なブロックチェーンを識別するために使用されることができる）。

【００２０】

処理サーバ１０２は、スワップ要求を受信することができ、スワップ要求内に含まれるデータに基づいて、アトミックスワップに関与する両方のブロックチェーンネットワーク１０６を識別することができる。ある実施形態では、スワップ要求は、第２の参加者装置１１０を識別することができる。これは例えば、第２の参加者装置１１０についての装置識別子又は連絡先情報を含むことによって行われ、連絡先情報は、電話番号、媒体アクセス制御アドレス、インターネットプロトコルアドレス、シリアル番号、又は他の一意の値などである。他の実施形態では、第１の参加者装置１０８は、第２の参加者装置１１０を識別することなく、スワップ要求を処理サーバ１０２に提出することができる。そのような実施形態では、処理サーバ１０２は、第１の参加者装置１０８が、アトミックスワップを実行する第２の参加者装置１１０を見つけることを支援することができる。

【００２１】

そのような実施形態では、第２の参加者装置１１０としてアトミックスワップに参加することに関心がある任意の装置（これは、例えば、第１の参加者装置１０８を含み得る）は、処理サーバ１０２に登録することができる。登録は、処理サーバ１０２に、装置に関連付けられた装置識別子と、（例えば、識別値を介して、）装置が、ブロックチェーンウォレットを有し、ブロックチェーン通貨を受け取る及び／又はブロックチェーン通貨を転送する用意があり得るブロックチェーンネットワーク１０６の一覧と、を提供することを含むことができる。ある事例では、登録する装置はまた、装置が登録している１つ以上のネットワークについての公開鍵を提供することができる。その結果、処理サーバ１０２は

、受け取るアドレスを生成して、仲介されたアトミックスワップ中に装置が実行する必要があり得る動作を低減することを可能にする。ある場合では、登録された装置は、ブロックチェーン上の現在の残高の更新を提供することができる。この装置は、通貨を転送する用意がある。この通貨は、処理サーバ１０２内のその装置の登録データ内に保持されることができる。

【００２２】

処理サーバ１０２が、第１の参加者装置１０８のために、第２の参加者装置１１０を見つけることを支援する場合、処理サーバ１０２は、第２のブロックチェーン上でブロックチェーン通貨を受け取り、第１のブロックチェーン上でブロックチェーン通貨を転送する、登録されたすべての装置を識別することができる。登録された装置の通貨残高が格納される場合、処理サーバ１０２は、スワップ要求において提供された通貨額に基づいて、十分な残高を有する装置のみを識別することができる。ある場合では、登録された各装置は、第２の参加者装置１１０としてアトミックスワップに参加することに伴う所望の為替レート又は手数料を有することができる。そのような場合、処理サーバ１０２は、第１の参加者装置によって望まれるアトミックスワップを達成するために必要となり得る通貨額を計算することができる。

【００２３】

処理サーバ１０２が適格な装置を識別すると、処理サーバ１０２は、例えば受信されたスワップ要求に応答して、適切な通信ネットワーク及び方法を使用して、識別された装置の一覧を第１の参加者装置１０８に送信することができる。手数料又は為替レートが適格な装置にわたって異なり得る場合、一覧は、付随する手数料、為替レート、第１の参加者装置１０８が受信することになるであろう、第１のブロックチェーンにおける通貨額、及び／又は第１の参加者装置１０８が適格な装置の各々について転送しなければならない、第２のブロックチェーンにおける通貨の額、を含むことができる。次に、第１の参加者装置１０８に関連付けられたユーザは、第２の参加者装置１１０として機能する適格な装置のうちの１つを選択して、適切な通信ネットワーク及び方法を使用して、選択を処理サーバ１０２に提出することができる。

【００２４】

処理サーバ１０２は、第２の参加者装置１１０についての選択を受信することができ、また、第１のブロックチェーンと第２のブロックチェーンとの両方についての通貨額を決定するために必要とすることができる任意の追加の計算を実行することができる。処理サーバ１０２が、第２のブロックチェーン上の選択された第２の参加者装置１１０についての公開鍵を格納させることができる場合、処理サーバ１０２は、第２の参加者装置１１０について、第２のブロックチェーン内で通貨を受け取るために使用される宛先アドレスを生成することができる。処理サーバ１０２が公開鍵を有しない場合、処理サーバ１０２は、宛先アドレスの要求を、選択された第２の参加者装置１１０に提出することができる。要求は、第２のブロックチェーンについての識別子を少なくとも含むことができ、第１のブロックチェーン又は第２のブロックチェーンについての通貨額、使用される為替レート及び／又は手数料など、第２の参加者装置１１０によって望まれる任意の追加情報を含むことができる。次に、第２の参加者装置１１０は、受信された識別子を使用して適切なブロックチェーンウォレットを識別し、それぞれの暗号鍵ペアの公開鍵を使用して第２のブロックチェーンについての宛先アドレスを生成することができる。第２の参加者装置１１０は、適切な通信ネットワーク及び方法を使用して、宛先アドレスを処理サーバ１０２に電子的に送り返すことができる。

【００２５】

処理サーバ１０２は、アトミックスワップのための処理を開始する準備をすることができる。処理を開始するために、処理サーバ１０２は、ハッシュロックの証明値として使用される値を生成することができる。値は、トランザクションに固有の一意の値とすることができる。値は、ランダムに又は擬似ランダムに生成されることができる、第１の参加者装置１０８と第２の参加者装置１１０とに関する情報に基づいて（例えば、第１のアドレ

スと第２のアドレスとから）構築されることができる、又は任意の他の適切な方法を使用して識別されることができる。証明値は、処理サーバ１０２によって生成及び／又は識別されることができるが、任意の他のデバイス、特に、第１の参加者装置１０８及び第２の参加者装置１１０、には知られていないとすることができる。次に、処理サーバ１０２は、ハッシュロックを生成することができる。ハッシュロックは、暗号鍵又は生成された他の値のスクランブルされたバージョンであり、トランザクション上に置かれると、元の暗号鍵又は他の値を使用してハッシュ値がロック解除されるまで、トランザクションの出力をロックする。システム１００では、処理サーバ１０２は、証明値を使用してハッシュロックを生成することができる。このハッシュロックは、第１の参加者装置１０８と第２の参加者装置１１０とによってなされる転送に配置されるであろう。これは、証明値を使用して処理サーバ１０２によってのみロック解除されることができる。ハッシュロックは例えば、ハッシュアルゴリズムを証明値に適用することによって生成されることができる。ある場合では、ハッシュロックはまた、第１のアドレス、第２のアドレス、第１のブロックチェーン又は第２のブロックチェーンの通貨額など、実行されるアトミックスワップに関連付けられる追加データを使用して生成されることができる。ある実施形態では、処理サーバ１０２は、例えばハッシュロックを生成するときに様々なデータを使用することによって、別個のハッシュロックを生成することができるが（これは、第２のブロックチェーン上で使用される、第１の参加者装置１０８についてのハッシュロック、及び第１のブロックチェーン上で使用される、第２の参加者装置１１０についてのハッシュロック）、両方のハッシュロックについて同じ証明値を利用することもできる。

【００２６】

ハッシュロックが生成されると、処理サーバ１０２は、参加する各装置が適切なトランザクションを実行するために必要なデータを、適切な参加する装置に電子的に送信することができる。例えば、処理サーバ１０２は、少なくとも、（例えば、第２の参加者装置１１０によって提供される）第２のブロックチェーン上の宛先アドレスと、第２のブロックチェーンの通貨額と、ハッシュロックとを第１の参加者装置１０８に送信することができる。処理サーバ１０２は、少なくとも、（例えば、スワップ要求からの）第１のブロックチェーン上の宛先アドレスと、第１のブロックチェーンの通貨額と、ハッシュロックとを第２の参加者装置１１０に送信することができる。ある事例では、処理サーバ１０２は、（例えば、スワップ要求内で、又は宛先アドレスを要求するときに）適切な参加者装置がすでに受信した可能性がある任意の冗長な情報を送信しないとすることができる。

【００２７】

参加者装置は、データを受信することができ、受信されたデータ内に示されるような通貨の転送のために、新しいブロックチェーントランザクションを適切なブロックチェーンに提出することができる。例えば、第１の参加者装置１０８は、第２の参加者装置１１０のブロックチェーンウォレットに関連付けられた宛先アドレスへの適切な通貨額の転送のために、第２のブロックチェーンについてのブロックチェーントランザクションを生成し、次に、ブロックチェーントランザクションをブロックチェーンネットワーク１０６ｂ内のブロックチェーンノードに提出することができる。第２の参加者装置１１０は、スワップ要求において提出された宛先アドレスへの適切な通貨額の転送のために、第１のブロックチェーンについての新しいブロックチェーントランザクションを生成することができ、これは、次に、ブロックチェーンネットワーク１０６ａ内のブロックチェーンノードに提出されることができる。

【００２８】

従来の方法及びシステムを使用して、両方のブロックチェーントランザクションがそれぞれのブロックチェーンに掲示されると、処理サーバ１０２は、トランザクションが掲示されたこと、及び正しいこと（例えば、適切な通貨の額が適切な宛先アドレスに転送されることを伴うこと）を検証することができる。ある実施形態では、第１の参加者装置１０８と第２の参加者装置１１０とは、トランザクションを提出した後にブロックチェーンノードから確認メッセージを受信することができる。これは例えば、ブロックチェーン上の

、提出されたブロックチェーントランザクションを格納するブロックチェーンデータ値の識別子を含むことができる。そのような実施形態では、第１の参加者装置１０８と第２の参加者装置１１０とは、第１及び第２のブロックチェーン上のブロックチェーントランザクションを識別する際に使用するために、受信された識別子及び／又は確認メッセージを処理サーバ１０２に提供することができる。他の実施形態では、処理サーバ１０２は、所望のアトミックスワップに一致するブロックチェーントランザクションを追加するために、第１のブロックチェーンと第２のブロックチェーンとの両方を監視することができる。これは、例えば各参加者装置に供給される宛先アドレスを監視することによって、行われる。

【００２９】

ブロックチェーントランザクションが識別された後、処理サーバ１０２は、各トランザクションを検証することができる。トランザクションの検証は、宛先アドレスが正確であることと、転送される通貨額が正確であることとを検証することを含むことができる。ある場合では、処理サーバ１０２はまた、ハッシュロックが、処理サーバ１０２によって以前に提供されたのと同じハッシュロックであることを検証することができる。ある実施形態では、処理サーバ１０２は、例えば暗号鍵ペアの秘密鍵を使用することによって、第１の参加者装置１０８と第２の参加者装置１１０とにハッシュロックを提供する前に、ハッシュロックにデジタル署名することができる。そのような実施形態では、処理サーバ１０２は、ブロックチェーントランザクションの検証の一部として、暗号鍵ペア内の対応する公開鍵を使用して、デジタル署名を検証することができる。ブロックチェーントランザクションの一方又は両方が検証に成功できない場合、処理サーバ１０２は、適切な参加者装置に通知することができ、修正されたブロックチェーントランザクションを提出する機会を参加者装置に提供することができる。両方のブロックチェーントランザクションの検証に成功しない場合、ハッシュロックは、処理サーバ１０２によって除去されないとすることができる。これは、トランザクションがロック解除されることを防止することができ、それによって、転送を防止することができる。ある場合では、ハッシュロックは、（例えば、スマートコントラクト、ブロックチェーンネットワーク１０６などを介して）それに関連付けられた有効期限を有することができる。ハッシュロックが有効期限内にロック解除されない場合、対応するブロックチェーントランザクションは、行われないであろう（例えば、送信者によって再度使用されることが可能な入力を用いて、又はブロックチェーンに自動的に掲示される取消トランザクション(reversal transaction)を用いて、ロックされたままであろう）。

【００３０】

両方のブロックチェーントランザクションが検証に成功する場合、処理サーバ１０２は、ハッシュロックを解放することができる。処理サーバ１０２は、証明値を、第１のブロックチェーンネットワーク１０６ａ内のブロックチェーンノードと第２のブロックチェーンネットワーク１０６ｂ内のブロックチェーンノードとに電子的に送信して、ハッシュロックを解放することができる。この証明値は、ハッシュロックを生成するためにブロックチェーンノードによって使用されることができ、一致(match)を検証して、処理サーバ１０２が、ハッシュロックを除去することを許可されることを確実にすることができる。ハッシュロックを生成するために証明値に加えて他のデータが使用された場合、追加のデータもブロックチェーンノードに送信されることができる。ブロックチェーントランザクションごとに別々のハッシュロックが生成される場合、処理サーバ１０２は、適切なデータを、それに応じて適切なブロックチェーンノードに送信することができる。ハッシュロックが除去されると、第１の参加者装置１０８と第２の参加者装置１１０との両方が、第１のブロックチェーン及び第２のブロックチェーン上でそれぞれ通貨を受信して、アトミックスワップを完了させるであろう。

【００３１】

例示的な実装形態では、処理サーバ１０２は、以下のコードを利用して、通貨額と、宛先アドレスと、証明値とを使用して作成されるハッシュロックを定義及び作成することが

できる。

【００３２】

```
class AtomicSwapContract:
    struct HashLock{
        Coin amount
        Address recipient
        byte[] hashKey
    }
    public CreateHashLock(double amount, Address recipient, byte[] hashKey){
        Coin coin = WithdrawAmountFromSenderAccount(amount)
        HashLock hashLock = new HashLock(coin, recipient, hashKey)
        PublishHashLockTransactionToSenderAccount(hashLock)
    }
}
```

【００３３】

上記の例では、hashKeyは、上述されたように処理サーバ１０２によって生成された証明値とすることができる。ハッシュロックがロック解除されるとき、処理サーバ１０２は、例示的な実装形態において以下の関数を利用することができる。

【００３４】

```
public Unlock(Address addressOfSmartContract, Address recipient, byte[] sec
retKey){
        HashLock hashLock = ReadTransactionFromSender(addressOfSmartCon
tract)
        // Ensure the recipient of the hashLock is same as provided
        assert(hashLock.recipient == recipient)
        // Ensure the hashes match, otherwise this transaction will fail
        byte[] hashOfSecretKey = Hash(secretKey)
        assert(hashLock.hashKey == hashOfSecretKey)
        // Second participant receives the amount from the first participant.
        SendTransaction(hashLock.recipient, hashLock.amount)
}
```

【００３５】

ある実施形態では、ハッシュロックとアトミックスワップとは、ブロックチェーン内に格納された自己で実行する契約とすることができるスマートコントラクトの使用を介して、ブロックチェーンによって実施されることができる。スマートコントラクトは、ブロックチェーンネットワーク１０６ごとに異なり得る異なるプログラミング言語、コード、及びプロトコルを利用することができる。一例では、ブロックチェーンネットワーク１０６は、関連付けられたブロックチェーンによって使用されるスマートコントラクトのプログラミング言語としてＳｏｌｉｄｉｔｙ（登録商標）を利用することができる。Ｓｏｌｉｄｉｔｙにおいて、上記の関数は例えば、以下のコードを使用して実行されることができる。

【００３６】

```
contract AtomicSwap {
    struct Swap {
        address sender;
        address recipient;
        uint    startTime;
        uint    duration;
        uint    amount;
        bool    active;
    }
```

```
    mapping(bytes32=〉 Swap) swaps;
    event SwapStart(address indexed sender,
                    address indexed recipient,
                    bytes32 indexed hashedSecret,
                    uint      startTime,
                    uint      duration,
                    uint      amount);
    function startSwap(address recipient, uint duration, bytes32 hashedSecre
t) public payable {
        require(! swaps[hashedSecret].active);
        require(msg.value 〉 0);
        Swap memory swap;
        swap.sender = msg.sender;
        swap.recipient = recipient;
        swap.startTime = now;
        swap.duration = duration;
        swap.amount = msg.value;
        swap.active = true;
        swaps[hashedSecret] = swap;
        emit SwapStart(swap.sender, swap.recipient, hashedSecret, swap.start
Time, swap.duration, swap.amount);
    }
    event SwapCancel(bytes32 indexed hashedSecret, uint time);
    function cancelSwap(bytes32 hashedSecret) public {
        Swap memory swap = swaps[hashedSecret];
        require(swap.sender == msg.sender);
        require(swap.active);
        require(now 〉= swap.startTime + swap.duration);
        swaps[hashedSecret].active = false;
        msg.sender.transfer(swap.amount);
        emit SwapCancel(hashedSecret, now);
    }
    event SwapComplete(bytes32 indexed hashedSecret, uint time);
    function completeSwap(bytes memory secret) public {
        bytes32 hashedSecret = keccak256(secret);
        Swap memory swap = swaps[hashedSecret];
        require(swap.recipient == msg.sender);
        require(swap.active);
        require(now 〈 swap.startTime + swap.duration);
        swaps[hashedSecret].active = false;
        msg.sender.transfer(swap.amount);
        emit SwapComplete(hashedSecret, now);
    }
    // auxilary function to get swap info
    function getSwapInfo(bytes32 hashedSecret) public view
        returns(address sender,
                address recipient,
                uint   startTime,
                uint   duration,
                uint   amount,
```

```
            bool    active) {
        Swap memory swap = swaps[hashedSecret];
        sender = swap.sender;
        recipient = swap.recipient;
        startTime = swap.startTime;
        duration = swap.duration;
        amount = swap.amount;
        active = swap.active;
    }

    // auxilary function to help calculate the hashed secret on chain
    function hashSecret(bytes memory secret) public pure returns(bytes32){
        return keccak256(secret);
    }
}
```

【００３７】

上記の例では、Swapは、実行されるアトミックスワップのデータについての構成とすることができる。SwapStartは、両方のトランザクションについてのハッシュロックを生成するために呼び出されることができる。SwapCancelは、アトミックスワップが停止され、トランザクションの公開に成功しない場合（例えば、参加者装置のうちの１つによる検証失敗又は撤回のため）、使用されることができる。SwapCompleteは、ハッシュロックを除去するために使用されることができ、両方のトランザクションを完了させることができる。getSwapInfoは、アトミックスワップの現在の状態を識別するために使用されることができる。これは例えば、処理サーバ１０２が２つのブロックチェーントランザクションの検証を待っている間、有効期限を確認する(check)ことができる。上記のコードは、一例であり、Ｓｏｌｉｄｉｔｙ又は任意の他のプログラミング言語を使用して本明細書で論じられる方法及びシステムのすべての実装を網羅し得るものではないことが、当業者には明らかであろう。

【００３８】

本明細書で論じられる方法及びシステムは、処理サーバ１０２によるアトミックスワップの仲介を提供する。本明細書で論じられる方法でアトミックスワップを仲介することによって、第１の参加者装置１０８は、自身の秘密鍵又は公開鍵を譲り渡すことなく、又は第２の参加者装置１１０を識別することさえなく（これは、代わりに処理サーバ１０２によって識別されることができるからである）、望まれるスワップを有することができる。加えて、トランザクションは、ハッシュロックを担当する仲介として処理サーバ１０２と共に、両方のブロックチェーン上で独立して行われるので、アトミックスワップは、ブロックチェーンネットワーク１０６間のハッシュ化方法論及び他の技術的差異に関わらず実行されることができる。結果として、本明細書で論じられる方法及びシステムは、仲介と本明細書で論じられる処理との使用によって、参加者の利便性及び安全も向上させながら、より汎用性の高いアトミックスワップを提供する。

【００３９】

処理サーバ

図２は、システム１００内の処理サーバ１０２などの処理サーバ１０２の一実施形態を示す。図２に示される処理サーバ１０２の実施形態は、例示としてのみ提供され、本明細書で論じられるような機能を実行するのに適した処理サーバ１０２のすべての可能な構成を網羅し得るものではないことが、当業者には明らかであろう。例えば、図５に示され、以下でより詳細に論じられるコンピュータシステム５００は、処理サーバ１０２の適切な構成とすることができる。

【００４０】

処理サーバ１０２は、受信装置２０２を含むことができる。受信装置２０２は、１つ以

上のネットワークプロトコルを介して１つ以上のネットワークにわたってデータを受信するように構成されることができる。ある事例では、１つ以上の通信方法を介して、ブロックチェーンノードと、第１の参加者装置１０８と、第２の参加者装置１１０と、他のシステム及びエンティティとからデータを受信するように構成されることができる。この通信方法は、無線周波数、構内通信網、無線エリアネットワーク、セルラー通信ネットワーク、Ｂｌｕｅｔｏｏｔｈ、インターネットなどである。ある実施形態では、受信装置２０２は、複数の装置から構成されることができる。これは、例えば、異なるネットワークを介してデータを受信するための異なる受信装置であり、構内通信網を介してデータを受信するための第１の受信装置及びインターネットを介してデータを受信するための第２の受信装置などである。受信装置２０２は、電子的に送信されたデータ信号を受信することができる。データは、データ信号に重ねられる、又は符号化されることができ、受信装置２０２によるデータ信号の受信を介して、復号される、構文解析される、読み込まれる、又は取得されることができる。ある事例では、受信装置２０２は、受信されたデータ信号を構文解析して、重ねられたデータを取得するために、構文解析モジュールを含むことができる。例えば、受信装置２０２は、パーサプログラムを含むことができる。パーサプログラムは、受信して、受信されたデータ信号を、本明細書で説明される方法及びシステムを実行するために処理装置によって実行される機能のための使用可能な入力に変換するように構成される。

【００４１】

受信装置２０２は、ブロックチェーンノードによって電子的に送信されるデータ信号を受信するように構成されることができる。これは、ブロックチェーンデータ値、ブロック、ブロックチェーントランザクションデータなどに重ねられる、又は符号化されることができる。受信装置２０２はまた、第１の参加者装置１０８によって電子的に送信されるデータ信号を受信するように構成されることができる。これは、スワップ要求、宛先アドレス、トランザクション識別子、登録データなどに重ねられる、又は符号化されることができる。受信装置２０２はまた、第２の参加者装置１１０によって電子的に送信されるデータ信号を受信するように構成されることができる。これは、登録データ、宛先アドレス、手数料、為替レート、ネットワーク識別子、トランザクション識別子などに重ねられる、又は符号化されることができる。

【００４２】

処理サーバ１０２はまた、通信モジュール２０４を含むことができる。通信モジュール２０４は、本明細書で論じられる機能を実行する際に使用するために、モジュールと、エンジンと、データベースと、記憶部と、処理サーバ１０２の他の構成要素との間でデータを送信するように構成されることができる。通信モジュール２０４は、１つ以上の通信種別から構成されることができ、コンピューティング装置内の通信のための様々な通信方法を利用することができる。例えば、通信モジュール２０４は、バス、コンタクトピンコネクタ、電線などから構成されることができる。また、ある実施形態では、通信モジュール２０４は、処理サーバ１０２の内部構成要素と、外部接続データベース、表示装置、入力装置などの処理サーバ１０２の外部構成要素との間で通信するように構成されることができる。また、処理サーバ１０２は、処理装置を含むことができる。処理装置は、当業者には明らかであるように、本明細書で論じられる処理サーバ１０２の機能を実行するように構成されることができる。ある実施形態では、処理装置は、クエリモジュール２１４、生成モジュール２１６、検証モジュール２１８など、処理装置の１つ以上の機能を実行するように特別に構成された複数のエンジン及び／又はモジュールを含む、及び／又はそれらから構成されることができる。本明細書で使用される場合、用語「モジュール」は、入力を受信し、入力を使用して１つ以上の処理を実行し、出力を提供するように特にプログラムされた、ハードウェア上で実行されるソフトウェア又はハードウェアとすることができる。様々なモジュールによって実行される入力、出力、及び処理は、本開示に基づいて当業者には明らかであろう。

【００４３】

処理サーバ１０２は、口座データベース２０６を含むことができる。口座データベース２０６は、適切なデータ記憶フォーマット及びスキーマを使用して、複数の口座プロファイル２０８を格納するように構成されることができる。口座データベース２０６は、格納された構造化データ集合の記憶、識別、修正、更新、アクセスなどのために構造化クエリ言語を利用する関係データベースとすることができる。各口座プロファイル２０８は、上述したように、例えばアトミックスワップにおいて第２の参加者装置１１０として働くように登録された任意の装置についての、１つ以上の登録された口座に関連したデータを格納するように構成された構造化データ集合とすることができる。例えば、口座プロファイル２０８は、第２の参加者装置１１０に関連付けられることができ、第２の参加者装置１１０としてのその装置の識別とアトミックスワップへの参加とのために必要なデータを格納することができる。例えば、口座プロファイル２０８は、装置識別子、各ブロックチェーンネットワーク１０６についての識別子を含むことができる。関連付けられた装置は、通貨を受信することができる。或いは、関連付けられた装置は、通貨、関連付けられた装置が通貨を転送することができる任意のブロックチェーン内の通貨残高、関連付けられた装置が通貨、連絡先情報、手数料、為替レートなどを受信することができるブロックチェーンについての暗号鍵ペアの公開鍵、を転送することができる。

【００４４】

処理サーバ１０２はまた、ブロックチェーンデータ２１０を含むことができる。これは、処理サーバ１０２の記憶部２１２内に格納されることができる、若しくは処理サーバ１０２内の別個の領域内に格納されることができる、又はそれによってアクセス可能とすることができる。ブロックチェーンデータ２１０は、ブロックチェーンを含むことができる。これは、複数のブロックから構成されることができ、ブロックチェーンネットワーク１０６に関連付けられることができる。ブロックチェーンデータ２１０は、さらに又は代替として、処理サーバ１０２によって使用されることができる、１つ以上のブロックチェーンウォレットに関連付けられた任意のデータを含むことができる。このデータは例えば、暗号鍵ペア、未使用トランザクション出力、デジタル資産額、ブロックチェーンネットワーク１０６についてのネットワーク識別子、スマートコントラクト、署名生成アルゴリズム、暗号化アルゴリズム、第三者サービスについての通信情報などである。

【００４５】

処理サーバ１０２はまた、記憶部２１２を含むことができる。記憶部２１２は、公開鍵及び秘密鍵、対称鍵などの、本明細書で論じられる機能を実行する際に処理サーバ１０２によって使用されるためのデータを格納するように構成されることができる。記憶部２１２は、適切なデータフォーマット方法及びスキーマを使用してデータを格納するように構成されることができ、読取り専用メモリ、ランダムアクセスメモリなどの任意の適切な種類のメモリとすることができる。例えば、記憶部２１２は、暗号鍵及びアルゴリズムと、通信プロトコル及び規格と、データフォーマット規格及びプロトコルと、処理装置のモジュール及びアプリケーションプログラムについてのプログラムコードと、当業者には明らかであるような、本明細書で開示される機能の実行の際に処理サーバ１０２によって使用されるのに適し得る他のデータと、を含むことができる。ある実施形態では、記憶部２１２は、関係データベースから構成されることができる、又はそれを含むことができる。関係データベースは、格納された構造化データ集合の記憶、識別、修正、更新、アクセスなどのために構造化クエリ言語を利用する。記憶部２１２は例えば、暗号鍵、ソルト、ナンス、他のコンピューティングシステムについての通信情報、生成アルゴリズム、暗号鍵ペア、通貨額の算出のためのアルゴリズム、為替レート、ブロックチェーンネットワーク１０６についての識別子などを格納するように構成されることができる。

【００４６】

処理サーバ１０２は、クエリモジュール２１４を含むことができる。クエリモジュール２１４は、データベース上でクエリを実行して、情報を識別するように構成されることができる。クエリモジュール２１４は、１つ以上のデータ値又はクエリ文字列を受信することができ、処理サーバ１０２の口座データベース２０６などの、示されたデータベース上

で、それに基づくクエリ文字列を実行して、格納された情報を識別することができる。次に、クエリモジュール２１４は、必要に応じて、識別された情報を、処理サーバ１０２の適切なエンジン又はモジュールに出力することができる。クエリモジュール２１４は例えば、口座データベース２０６上でクエリを実行して、第１の参加者装置１０８によって要求されたアトミックスワップの第２の参加者装置１１０として働く資格があり得るすべての登録された装置を見つけることができる。これは例えば、スワップ要求内に含まれるネットワーク識別子に基づいて行われることができる。

【００４７】

処理サーバ１０２はまた、生成モジュール２１６を含むことができる。生成モジュール２１６は、本明細書で論じられる機能を実行する際に処理サーバ１０２によって使用されるためのデータを生成するように構成されることができる。生成モジュール２１６は、入力として命令を受信することができ、命令に基づいてデータを生成することができ、生成されたデータを処理サーバ１０２の１つ以上のモジュールに出力することができる。例えば、生成モジュール２１６は、暗号鍵ペアを生成する、デジタル署名を生成する、ブロックチェーンデータ値を生成するなどを実行するように構成されることができる。生成モジュール２１６はまた、証明値とハッシュロックとを生成することと、処理サーバ１０２によって生成されたハッシュロックの除去のために必要な任意のデータを生成することと、を実行するように構成されることができる。

【００４８】

処理サーバ１０２はまた、検証モジュール２１８を含むことができる。検証モジュール２１８は、本明細書で論じられる機能の一部として、処理サーバ１０２のための検証を実行するように構成されることができる。検証モジュール２１８は、入力として命令を受信することができ（これは、検証を実行する際に使用されるデータも含み得る）、要求に応じて検証を実行することができ、検証の結果を処理サーバ１０２の別のモジュール又はエンジンに出力することができる。検証モジュール２１８は例えば、適切な署名生成アルゴリズム及び鍵を使用してデジタル署名を検証することと、ブロックチェーントランザクションを検証することと、スマートコントラクトを検証することと、ハッシュロックを検証することと、などを実行するように構成されることができる。

【００４９】

処理サーバ１０２はまた、送信装置２２０を含むことができる。送信装置２２０は、１つ以上のネットワークプロトコルを介して１つ以上のネットワークにわたってデータを送信するように構成されることができる。ある事例では、送信装置２２０は、１つ以上の通信方法を介して、ブロックチェーンノードと、第１の参加者装置１０８と、第２の参加者装置１１０と、他のエンティティとにデータを送信するように構成されることができる。この通信方法は、構内通信網、無線エリアネットワーク、セルラー通信、Ｂｌｕｅｔｏｏｔｈ、無線周波数、インターネットなどである。ある実施形態では、送信装置２２０は、複数の装置から構成されることができる。これは、例えば、異なるネットワークを介してデータを送信するための異なる送信装置であり、構内通信網を介してデータを送信するための第１の送信装置及びインターネットを介してデータを送信するための第２の送信装置などである。送信装置２２０は、受信するコンピューティング装置によって構文解析され得る、データが重ねられたデータ信号を電子的に送信することができる。ある事例では、送信装置２２０は、データを、送信に適したデータ信号に重ねる、符号化する、又はフォーマットするための１つ以上のモジュールを含むことができる。

【００５０】

送信装置２２０は、データ信号をブロックチェーンノードに電子的に送信するように構成されることができる。これは、ハッシュロック、ハッシュロックの除去のためのデータ、ブロック又はブロックチェーンデータ値の要求などに重ねられる、又は符号化されることができる。送信装置２２０はまた、第１の参加者装置１０８にデータ信号を電子的に送信するように構成されることができる。これは、アドレスの要求、適格な第２の参加者装置１１０の一覧、通貨額、手数料、為替レート、新しいブロックチェーントランザクショ

ンについてのデータ、通知などに重ねられる、又は符号化されることができる。送信装置２２０は、データ信号を第２の参加者装置１１０に電子的に送信するように構成されることができる。これは、宛先アドレス又は通貨額のデータの要求、新しいブロックチェーントランザクションについてのデータ、通知、更新された通貨残高の要求などに重ねられる、又は符号化されることができる。

【００５１】

仲介されたアトミックスワップを実行するための処理

図３Ａ及び図３Ｂは、処理サーバ１０２によって仲介され、第１の参加者装置１０８と第２の参加者装置１１０とが関与する、図１のシステム１００においてアトミックスワップを実行するための処理を示す。

【００５２】

ステップ３０２において、第２の参加者装置１１０は、登録データを処理サーバ１０２に電子的に送信することによって、アトミックスワップへの参加について処理サーバ１０２に登録することができる。登録データは例えば、第２の参加者装置１１０についての装置識別子及び／又は連絡先情報と、第２の参加者装置１１０が通貨を受け入れる用意があるブロックチェーンについての識別子の一覧と、第２の参加者装置が通貨を転送する用意があるブロックチェーンについての識別子の一覧と、を含むことができる。ステップ３０４において、処理サーバ１０２の受信装置２０２は、第２の参加者装置１１０から登録データを受信することができる。ステップ３０６において、処理サーバ１０２のクエリモジュール２１４は、処理サーバ１０２の口座データベース２０６上でクエリを実行して、受信された装置登録データを含む、第２の参加者装置１１０のための新しい口座プロファイル２０８をそこに挿入することができる。

【００５３】

ステップ３０８において、第１の参加者装置１０８は、適切な通信ネットワーク及び方法を使用して、アトミックスワップの要求を処理サーバ１０２に提出することができる。スワップ要求は、少なくとも、第１の参加者装置１０８が通貨を受け取ることを望む第１のブロックチェーンの宛先アドレスと、第１の参加者装置１０８が第１のブロックチェーン上で受け取ることを望む通貨額と、第１の参加者装置１０８が通貨を転送する用意がある第２のブロックチェーンの１つ以上の識別子と、を含むことができる。ステップ３１０において、処理サーバ１０２の受信装置２０２は、スワップ要求を受信することができる。

【００５４】

ステップ３１２において、処理サーバ１０２のクエリモジュール２１４は、処理サーバ１０２の口座データベース２０６上でクエリを実行して、アトミックスワップにおいて第２の参加者装置１１０として働くのに適し得る任意の登録された装置の口座プロファイル２０８を識別することができる。これは例えば、口座プロファイル２０８が、関連付けられる装置が通貨を転送する用意があるものとして第１のブロックチェーンの指示を含むかどうか、及び関連付けられる装置が通貨を受け取る用意があるものとして第２のブロックチェーンのうちの１つの指示を含むかどうか、を確認するために検査することによって、行われる。ある実施形態では、処理サーバ１０２は、複数の適格な装置を識別することができ、第１の参加者装置１０８から、装置のうちの１つの選択を要求することができる。図３Ａ及び図３Ｂに示される例では、処理サーバ１０２は、第２の参加者装置１１０装置を適格として識別し、それに応じて処理を進めることができる。ステップ３１２の一部として、処理サーバ１０２は、第２のブロックチェーン上の第２の参加者装置１１０についての宛先アドレスを識別することができる（例えば、処理サーバ１０２、第１の参加者装置１０８、又は第２の参加者装置１１０によって、すべての適格な第２のブロックチェーンから選択される）。これは例えば、（例えば、口座データベース２０８内に格納された、第２のブロックチェーンについての公開鍵を使用して生成モジュール２１６を介して）宛先アドレスを生成することによって、又は第２のブロックチェーンについて、第２の参加者装置１１０から宛先アドレスを要求することによって、行われる。

【００５５】

ステップ３１４において、処理サーバ１０２の生成モジュール２１６は、ハッシュロックにおいて使用される証明値を生成することができる。証明値は、任意の適切な方法を使用して生成又は識別されることができ、第１の参加者装置１０８によって要求されるアトミックスワップに対して一意とすることができる。ステップ３１６において、処理サーバ１０２の生成モジュール２１６は、例えば証明値にハッシュアルゴリズムを適用することによって、少なくとも証明値を使用してハッシュロックを生成することができる。ハッシュロックは、結果として得られるハッシュ値である。ステップ３１８において、処理サーバ１０２の送信装置２２０は、第１の参加者装置１０８と第２の参加者装置１１０との両方に、ハッシュロックと適切なトランザクションデータとを電子的に送信することができる。第１の参加者装置１０８は、ハッシュロックと、第２の参加者装置１１０の第２のブロックチェーンについての宛先アドレスと、第２のブロックチェーンの通貨額と、を送信されることができる。第２の参加者装置１１０は、ハッシュロックと、第１の参加者装置１０８の第１のブロックチェーンについての宛先アドレスと、第１のブロックチェーンの通貨額と、を送信されることができる。

【００５６】

ステップ３２０において、第１の参加者装置１０８は、ハッシュロックと、宛先アドレスと、通貨額とを処理サーバ１０２から受信することができる。ステップ３２２において、従来の方法及びシステムを使用して、第１の参加者装置１０８は、第１の参加者装置１０８が所有する（例えば、通貨額を扱う）１つ以上の適切なトランザクション出力を使用して、受信された通貨額を、受信された宛先アドレスに転送するために、第２のブロックチェーンネットワーク１０６ｂ内のブロックチェーンノードに新しいブロックチェーントランザクションを提出することができる。ブロックチェーントランザクションは、第１の参加者装置１０８によって送信されるハッシュロックによって、又は新しいブロックチェーントランザクションが提出される前に処理サーバ１０２によってブロックチェーンネットワーク１０６ｂに個別に提出されることによって、ハッシュロックされることができる。第１の参加者装置１０８は、新しいブロックチェーントランザクションが、確認に成功したこと、新しいブロックに追加されたこと、第２のブロックチェーンに掲示されたことの通知として、トランザクション識別子をブロックチェーンノードから受信することができる。ステップ３２４において、第１の参加者装置１０８は、ブロックチェーントランザクションが掲示に成功したことを処理サーバ１０２に通知する際に、トランザクション識別子を電子的に送信することができる。

【００５７】

ステップ３２６において、第２の参加者装置１１０は、ハッシュロックと、宛先アドレスと、通貨額とを処理サーバ１０２から受信することができる。ステップ３２８において、従来の方法及びシステムを使用して、第２の参加者装置１１０は、第２の参加者装置１１０が所有する（例えば、通貨額を扱う）１つ以上の適切なトランザクション出力を使用して、受信された通貨額を、受信された宛先アドレスに転送するために、第１のブロックチェーンネットワーク１０６ａ内のブロックチェーンノードに新しいブロックチェーントランザクションを提出することができる。ブロックチェーントランザクションは、第２の参加者装置１１０によって送信されるハッシュロックによって、又は新しいブロックチェーントランザクションが提出される前に処理サーバ１０２によってブロックチェーンネットワーク１０６ａに個別に提出されることによって、ハッシュロックされることができる。第２の参加者装置１１０は、新しいブロックチェーントランザクションが、確認に成功したことと、新しいブロックに追加されたことと、第２のブロックチェーンに掲示されたこととの通知として、トランザクション識別子をブロックチェーンノードから受信することができる。ステップ３３０において、第２の参加者装置１１０は、ブロックチェーントランザクションが掲示に成功したことを処理サーバ１０２に通知する際に、トランザクション識別子を電子的に送信することができる。

【００５８】

ステップ３３２において、処理サーバ１０２の受信装置２０２は、第１の参加者装置１

０８と第２の参加者装置１１０との両方から、両方のブロックチェーントランザクションについて、トランザクション識別子を受信することができる。ステップ３３４において、処理サーバ１０２は、両方のブロックチェーントランザクションを識別することができる。これは例えば、処理サーバ１０２内に格納されたブロックチェーンデータ２１０内で、又は受信されたトランザクション識別子を使用して、適切なブロックチェーンネットワーク１０６からブロックチェーンデータ値を要求することによって、実行される。ステップ３３６において、処理サーバ１０２の検証モジュール２１８は、両方のブロックチェーントランザクションを検証することができる。各ブロックチェーントランザクションは、宛先アドレスと通貨額とが正しいことを保証することによって、及びハッシュロックが適切であり、適当であり、まだ期限切れでないことを検証することによって、検証モジュール２１８により検証されることができる。トランザクションが検証に成功すると、ステップ３３８において、処理サーバ１０２の送信装置２２０は、第１のブロックチェーンネットワーク１０６ａと第２のブロックチェーンネットワーク１０６ｂとの両方におけるブロックチェーンノードに証明値を電子的に送信して、両方のブロックチェーントランザクション上のハッシュロックの除去を要求することができる。ハッシュロックが除去されると、第１の参加者装置１０８と第２の参加者装置１１０とは、適切なブロックチェーン上で通貨を受け取ることができ、アトミックスワップが完了することができる。

【００５９】

アトミックスワップの仲介のための例示的な方法

図４は、第三者の処理サーバによるアトミックスワップの仲介のための方法４００を示す。

【００６０】

ステップ４０２において、スワップ要求は、処理サーバ（例えば、処理サーバ１０２）の受信機（例えば、受信装置２０２）によって、第１のコンピューティング装置（例えば、第１の参加者装置１０８）から受信されることができる。スワップ要求は、少なくとも、第１のブロックチェーンに関連付けられた第１のアドレスと、第２のブロックチェーンに関連付けられたネットワーク識別子と、を含む。ステップ４０４において、処理サーバのプロセッサ（例えば、クエリモジュール２１４）は、少なくとも、ネットワーク識別子と第２のブロックチェーンに関連付けられた第２のアドレスとに基づいて、第２のコンピューティング装置（例えば、第２の参加者装置１１０）を識別することができる。ステップ４０６において、証明値とハッシュロックとは、処理サーバのプロセッサ（例えば、生成モジュール２１６）によって生成されることができる。ハッシュロックは、少なくとも証明値を使用して生成される。

【００６１】

ステップ４０８において、処理サーバの送信機（例えば、送信装置２２０）は、（ｉ）少なくとも、ハッシュロックと第２のアドレスとを第１のコンピューティング装置に、（ｉｉ）少なくとも、ハッシュロックと第１のアドレスとを第２のコンピューティング装置に、送信することができる。ステップ４１０において、処理サーバのプロセッサ（例えば、検証モジュール２１８）は、第１のアドレスへの第１の通貨額の転送のために第１のブロックチェーンに掲示された第１のブロックチェーントランザクションと、第２のアドレスへの第２の通貨額の転送のために第２のブロックチェーンに提示された第２のブロックチェーントランザクションと、を検証することができる。ステップ４１２において、処理サーバの送信機は、少なくとも証明値を、第１のブロックチェーンに関連付けられた第１のブロックチェーンノードと、第２のブロックチェーンに関連付けられた第２のブロックチェーンノードとに送信することができる。

【００６２】

一実施形態では、第２のコンピューティング装置は、スワップ要求において識別されることができる。ある実施形態では、第２のコンピューティング装置を識別することは、処理サーバのプロセッサによって、ネットワーク識別子に基づいて、複数の追加のコンピューティング装置の各々についての識別子を識別することと、処理サーバの送信機によって

、複数の追加のコンピューティング装置の各々についての識別子を第１のコンピューティング装置に送信することと、処理サーバの受信機によって、第２のコンピューティング装置に関連付けられた識別子を第１のコンピューティング装置から受信することと、を含むことができる。一実施形態では、スワップ要求は、第１の通貨額と第２の通貨額とを含むことができる。ある実施形態では、第１の通貨額と第２の通貨額とは、同じ額とすることができる。

【００６３】

一実施形態では、方法４００は、処理サーバの受信機によって、第１のブロックチェーントランザクションに関連付けられた第１の通知データを第２のコンピューティング装置から受信することと、処理サーバの受信機によって、第２のブロックチェーントランザクションに関連付けられた第２の通知データを第１のコンピューティング装置から受信することと、をさらに含むことができる。さらなる実施形態では、第１の通知データと第２の通知データとは、第１のブロックチェーントランザクションと第２のブロックチェーントランザクションとを検証する前に受信されることができ、第１のブロックチェーントランザクションは、第１の通知データを使用して検証されることができ、第２のブロックチェーントランザクションは、第２の通知データを使用して検証されることができる。ある実施形態では、方法４００はまた、処理サーバのプロセッサによって、少なくとも、第１の通貨額と、第２のコンピューティング装置に関連付けられた為替レートとに基づいて、第２の通貨額を計算することを含むことができる。

【００６４】

コンピュータシステムアーキテクチャ

図５は、本開示の実施形態又はその一部がコンピュータ可読コードとして実装されることができるコンピュータシステム５００を示す。例えば、図１及び図２の処理サーバ１０２は、格納された命令を有するハードウェア、非一時的コンピュータ可読媒体、又はそれらの組み合わせを使用して、コンピュータシステム５００において実装されることができ、１つ以上のコンピュータシステム又は他の処理システムにおいて実装されることができる。ハードウェアは、図３Ａ、図３Ｂ、及び図４の方法を実施するために使用されるモジュール及び構成要素を具体化することができる。

【００６５】

プログラマブルロジックが使用される場合、そのようなロジックは、実行可能ソフトウェアコードによって構成された市販の処理プラットフォーム上で実行して、特定の目的のコンピュータ又は特別の目的の装置（例えば、プログラマブルロジックアレイ、特定用途向け集積回路など）になることができる。当業者は、開示された主題の実施形態が様々なコンピュータシステム構成を用いて実施され得ることを理解することができる。このコンピュータシステム構成は、マルチコアマルチプロセッサシステム、ミニコンピュータ、メインフレームコンピュータ、分散機能を用いてリンク又はクラスタ化されたコンピュータ、ならびに仮想的に任意の装置に埋め込まれ得るパーペイシブ又は小型コンピュータを含む。例えば、少なくとも１つのプロセッサ装置と記憶部とが、上述の実施形態を実装するために使用されることができる。

【００６６】

本明細書で論じられるプロセッサユニット又は装置は、単一のプロセッサ、複数のプロセッサ、又はそれらの組み合わせとすることができる。プロセッサ装置は、１つ以上のプロセッサ「コア」を有することができる。本明細書で論じられるような用語「コンピュータプログラム媒体」、「非一時的コンピュータ可読媒体」、及び「コンピュータ使用可能媒体」は、概して、取り外し可能記憶ユニット５１８、取り外し可能記憶ユニット５２２、及びハードディスクドライブ５１２にインストールされたハードディスクなどの有形媒体を指すために使用される。

【００６７】

本開示の様々な実施形態は、この例示的なコンピュータシステム５００に関して説明される。この説明を読んだ後、他のコンピュータシステム及び／又はコンピュータアーキテ

クチャを使用して、どのように本開示を実施するかが当業者には明らかになるであろう。動作は連続的な処理として説明されることができるが、動作の一部は、実際には、並列に、同時に、及び／又は分散環境において、単一又はマルチプロセッサ機械によるアクセスのためにローカルに又は遠隔に格納されたプログラムコードを用いて、実行されることができる。追加として、ある実施形態では、動作の順序が、開示される主題の趣旨から逸脱することなく、再構成されることができる。

【００６８】

プロセッサ装置５０４は、本明細書で論じられる機能を実行するように特に構成された専用又は汎用プロセッサ装置とすることができる。プロセッサ装置５０４は、通信インフラストラクチャ５０６に接続されることができる。これは、例えば、バス、メッセージキュー、ネットワーク、マルチコアメッセージパッシング方式などである。ネットワークは、本明細書で開示されるような機能を実行するのに適した任意のネットワークとすることができ、構内通信網（ＬＡＮ）、広域通信網（ＷＡＮ）、無線ネットワーク（例えば、ＷｉＦｉ）、移動体通信網、衛星ネットワーク、インターネット、光ファイバ、同軸ケーブル、赤外線、無線周波数（ＲＦ）、又はそれらの任意の組合せを含むことができる。他の適切なネットワークの種類及び構成は、当業者には明らかであろう。また、コンピュータシステム５００は、主記憶部５０８（例えば、ランダムアクセスメモリ、読み取り専用メモリなど）を含むことができ、補助記憶部５１０も含むことができる。補助記憶部５１０は、ハードディスクドライブ５１２と取り外し可能記憶ドライブ５１４とを含むことができる。これは、例えば、フロッピーディスクドライブ、磁気テープドライブ、光ディスクドライブ、フラッシュメモリなどである。

【００６９】

取り外し可能記憶ドライブ５１４は、周知の方法で、取り外し可能記憶ユニット５１８から読み取り、及び／又はそれに書き込むことができる。取り外し可能記憶ユニット５１８は、取り外し可能記憶ドライブ５１４によって読み書きされ得る取り外し可能記憶媒体を含むことができる。例えば、取り外し可能記憶ドライブ５１４がフロッピーディスクドライブ又はユニバーサルシリアルバスポートである場合、取り外し可能記憶ユニット５１８は、それぞれ、フロッピーディスク又はポータブルフラッシュドライブとすることができる。一実施形態では、取り外し可能記憶ユニット５１８は、非一時的コンピュータ可読記録媒体とすることができる。

【００７０】

ある実施形態では、補助記憶部５１０は、コンピュータプログラム又は他の命令をコンピュータシステム５００内に読み込むことを可能にするための代替手段、例えば、取り外し可能記憶ユニット５２２及びインタフェース５２０を含むことができる。そのような手段の例は、プログラムカートリッジ及びカートリッジインタフェース（例えば、ビデオゲームシステムに見られるようなもの）と、取り外し可能メモリチップ（例えば、ＥＥＰＲＯＭ、ＰＲＯＭなど）及び関連付けられたソケットと、当業者には明らかであるような他の取り外し可能記憶ユニット５２２及びインタフェース５２０とを含むことができる。

【００７１】

コンピュータシステム５００（例えば、主記憶部５０８及び／又は補助記憶部５１０）内に格納されたデータは、任意の種類の適切なコンピュータ可読媒体上に格納されることができる。これは例えば、光学記憶装置（例えば、コンパクトディスク、デジタル多用途ディスク、ブルーレイディスクなど）又は磁気テープ記憶装置（例えば、ハードディスクドライブ）である。データは、任意の種類の適切なデータベース構成において構成されることができる。これは、例えば、関係データベース、構造化クエリ言語（ＳＱＬ）データベース、分散データベース、オブジェクトデータベースなどである。適切な構成及び記憶装置の種類は、当業者には明らかであろう。

【００７２】

コンピュータシステム５００はまた、通信インタフェース５２４を含むことができる。通信インタフェース５２４は、ソフトウェア及びデータを、コンピュータシステム５００

と外部装置との間で転送することを可能にするように構成されることができる。例示的な通信インタフェース５２４は、モデム、ネットワークインタフェース（例えば、イーサネットカード）、通信ポート、ＰＣＭＣＩＡスロット及びカードなどを含むことができる。通信インタフェース５２４を介して転送されたソフトウェア及びデータは、信号の形態とすることができ、これは、電子信号、電磁信号、光信号、又は当業者には明らかであるような他の信号とすることができる。信号は、通信経路５２６を介して伝わることができる。これは、信号を搬送するように構成されることができ、電線、ケーブル、光ファイバ、電話回線、携帯電話リンク、無線周波数リンクなどを使用して実装されることができる。

【００７３】

コンピュータシステム５００は、表示インタフェース５０２をさらに含むことができる。表示インタフェース５０２は、データを、コンピュータシステム５００と外部表示装置５３０との間で転送することを可能にするように構成されることができる。例示的な表示インタフェース５０２は、高解像度マルチメディアインタフェース（ＨＤＭＩ）、デジタルビジュアルインタフェース（ＤＶＩ）、ビデオグラフィックスアレイ（ＶＧＡ）などを含むことができる。表示装置５３０は、コンピュータシステム５００の表示インタフェース５０２を介して送信されるデータを表示するための任意の適切な種類の表示装置とすることができる。この表示装置は、陰極線管（ＣＲＴ）表示装置、液晶表示装置（ＬＣＤ）、発光ダイオード（ＬＥＤ）表示装置、静電タッチ表示装置、薄膜トランジスタ（ＴＦＴ）表示装置などを含む。

【００７４】

コンピュータプログラム媒体及びコンピュータ使用可能媒体は、主記憶部５０８及び補助記憶部５１０などの記憶部を指すことができ、これは、メモリ半導体（例えば、ＤＲＡＭなど）とすることができる。これらのコンピュータプログラム製品は、コンピュータシステム５００にソフトウェアを提供するための手段とすることができる。コンピュータプログラム（例えば、コンピュータ制御ロジック）は、主記憶部５０８及び／又は補助記憶部５１０内に格納されることができる。また、コンピュータプログラムは、通信インタフェース５２４を介して受信されることができる。そのようなコンピュータプログラムは、実行されると、コンピュータシステム５００が本明細書で論じられるような本方法を実施することを可能にすることができる。特に、コンピュータプログラムは、実行されると、プロセッサ装置５０４が、本明細書で論じられるような、図３Ａと、図３Ｂと、図４とによって示された方法を実施することを可能にすることができる。したがって、そのようなコンピュータプログラムは、コンピュータシステム５００の制御装置を表すことができる。本開示がソフトウェアを使用して実装される場合、ソフトウェアは、コンピュータプログラム製品内に格納され、取り外し可能記憶ドライブ５１４、インタフェース５２０、及びハードディスクドライブ５１２、又は通信インタフェース５２４を使用してコンピュータシステム５００内に読み込まれることができる。

【００７５】

プロセッサ装置５０４は、コンピュータシステム５００の機能を実行するように構成された１つ以上のモジュール又はエンジンを含むことができる。モジュール又はエンジンの各々は、ハードウェアを使用して実装されることができ、ある事例では、主記憶部５０８又は補助記憶部５１０内に格納されたプログラムコード及び／又はプログラムに対応するようなソフトウェアも利用することができる。そのような事例では、プログラムコードは、コンピュータシステム５００のハードウェアによる実行の前に、プロセッサ装置５０４によって、（例えば、コンパイルするモジュール又はエンジンによって）コンパイルされることができる。例えば、プログラムコードは、プロセッサ装置５０４及び／又はコンピュータシステム５００の任意の追加のハードウェア構成要素による実行のために、アセンブリ言語又は機械コードなどの低水準言語に翻訳されるプログラミング言語で書かれたソースコードとすることができる。コンパイルする処理は、字句解析と、前処理と、構文解析と、意味解析と、構文指向翻訳と、コード生成と、コード最適化と、コンピュータシステム５００を制御して本明細書で開示される機能を実行するのに適した低水準言語へのプ

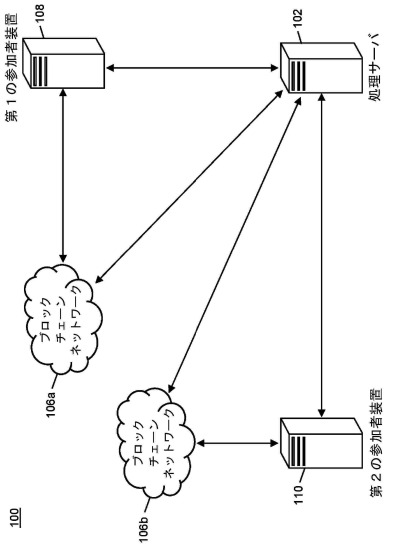
ログラムコードの翻訳に適し得る任意の他の技術と、の使用を含むことができる。そのような処理の結果、コンピュータシステム５００は、上述の機能を実行するように一意にプログラムされた、特別に構成されたコンピュータシステム５００となることが当業者には明らかであろう。

【００７６】

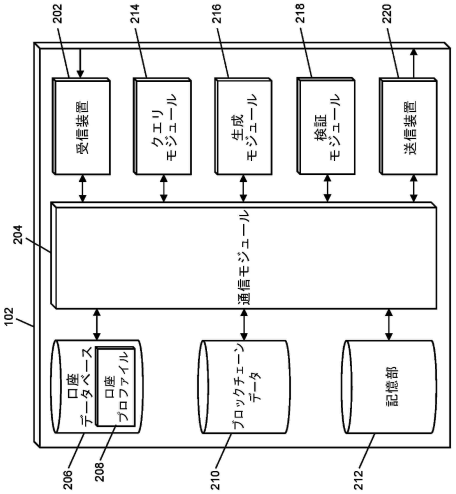
本開示と一致する技法は、とりわけ、アトミックスワップを仲介するための特徴、システム、及び方法を提供する。開示されたシステム及び方法の様々な例示的な実施形態が上記説明されたが、それらは、限定ではなく、例示のみを目的として提示されたことを理解されたい。それは、網羅的ではなく、開示された厳密な形態に本開示を限定しない。上記の教示に照らして、修正及び変形が可能であり、又は、修正及び変形は、広さ若しくは範囲から逸脱することなく、本開示の実施から得られることができる。

【図面】

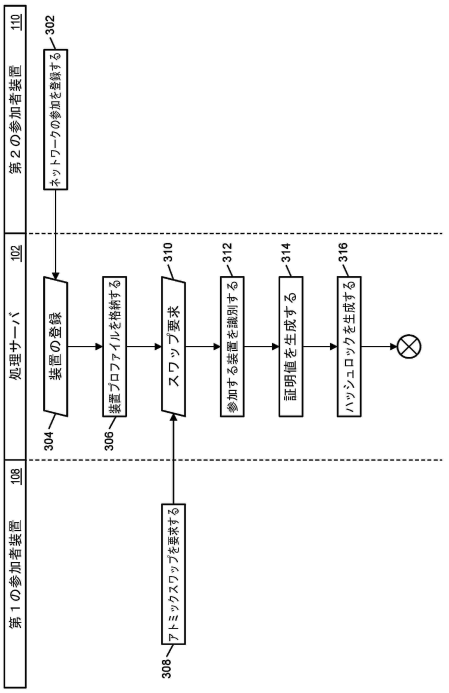
【図１】



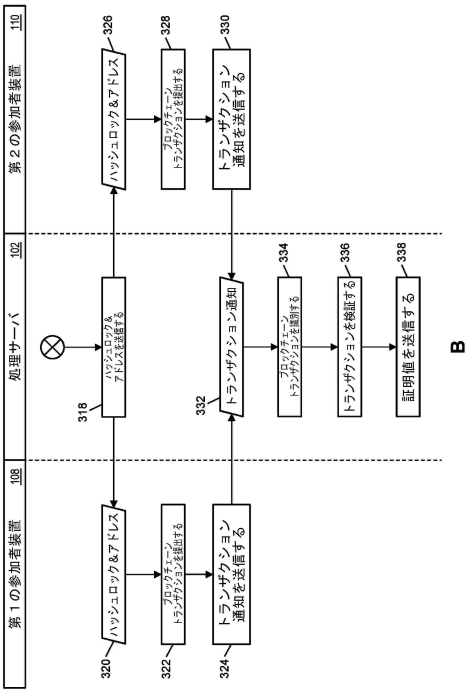
【図２】



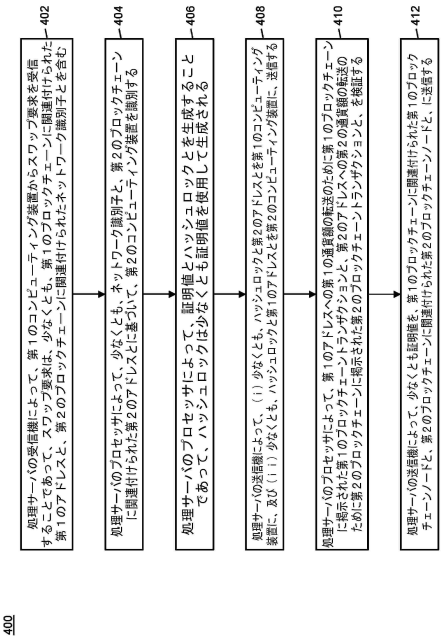
【図３Ａ】



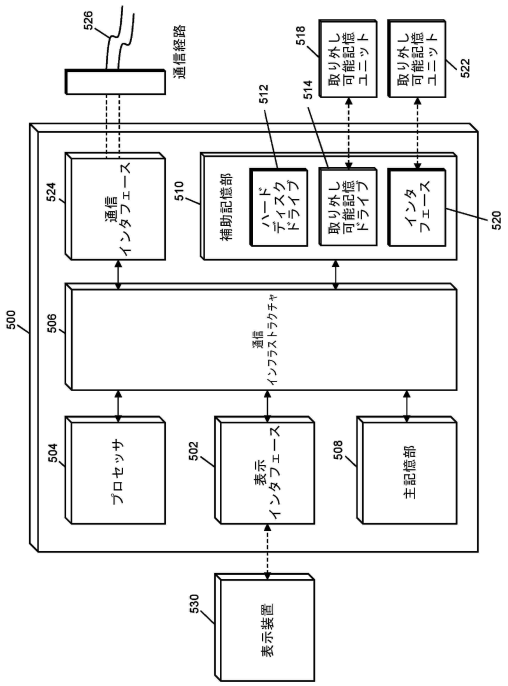
【図３Ｂ】



【図４】


402
処理サーバの受信機によって、第１のコンピューティング装置からスワップ要求を受信することであって、スワップ要求は、少なくとも、第１のブロックチェーンに関連付けられた第１のアドレスと、第２のブロックチェーンに関連付けられたネットワーク識別子とを含む
404
処理サーバのプロセッサによって、少なくとも、ネットワーク識別子と、第２のブロックチェーンに関連付けられた第２のアドレスに基づいて、第２のコンピューティング装置を識別する
406
処理サーバのプロセッサによって、証明値とハッシュロックとを生成することであって、ハッシュロックは少なくとも証明値を使用して生成される
408
処理サーバの送信機によって、（ｉ）少なくとも、ハッシュロックと第２のアドレスと第１のコンピューティング装置に、及び（ｉｉ）少なくとも、ハッシュロックと第１のアドレスと第２のコンピューティング装置に、送信する
410
処理サーバのプロセッサによって、第１のアドレスへの第１の通貨額の転送のために第１のブロックチェーンに掲示された第１のブロックチェーントランザクションと、第２のアドレスへの第２の通貨額の転送のために第２のブロックチェーンに掲示された第２のブロックチェーントランザクションと、を検証する
412
処理サーバの送信機によって、少なくとも証明値を、第１のブロックチェーンに関連付けられた第１のブロックチェーンノードと、第２のブロックチェーンに関連付けられた第２のブロックチェーンノードと、に送信する
400

【図５】


526
通信経路
518
取り外し可能記憶ユニット
522
取り外し可能記憶ユニット
512
514
524
通信インタフェース
510
補助記憶部
ハードディスクドライブ
取り外し可能記憶ドライブ
インタフェース
520
500
506
通信インフラストラクチャ
504
プロセッサ
502
表示インタフェース
508
主記憶部
530
表示装置

フロントページの続き

シンガポール国 ５３２９８０ シンガポール ブアンコク クレセント ９８０ビー ナンバー０３－７７
(72)発明者 ドンハオ フアン
シンガポール国 ０９８６４１ シンガポール カリビアン アット ケッペル ベイ ケッペル ベイ ドライブ １２ ナンバー０３－１４
(72)発明者 ハンコン グアン
シンガポール国 ５９６２３０ シンガポール ヒュム アヴェニュー ５２エイ ナンバー０９－０３
(72)発明者 カール チェン
シンガポール国 １４００５１ シンガポール ストラスモア アヴェニュー ５１ ナンバー０６－１９３
(72)発明者 フォック ホアン ロン レー
シンガポール国 １４３０６１ シンガポール ストラスモア アヴェニュー ブロック ６１ ナンバー０５－２０
(72)発明者 ウェイミン マ
シンガポール国 ３１０２３４ シンガポール ロロン ８ トア パヨー ２３４ ナンバー１２－２７０

審査官 行田 悦資

(56)参考文献
特開２０２０－０４８１６１（ＪＰ，Ａ）
米国特許出願公開第２０２０／００９８０４２（ＵＳ，Ａ１）
米国特許出願公開第２０１９／０１５６３０１（ＵＳ，Ａ１）
福岡 尊 ほか，ブロックチェーンによる取引の秘匿とその検証方法の提案，２０２１年 暗号と情報セキュリティシンポジウム予稿集，日本，電子情報通信学会，2021年01月19日，pp.1-8
BENTOV, I. et al.，Tesseract: Real-Time Cryptocurrency Exchange Using Trusted Hardware，CCS'19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security，ACM，2019年11月06日，pp.1521-1538，〈DOI:10.1145/3319535.3363221〉

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０６Ｑ ２０／０６