(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6840268号
(P6840268)
(45)発行日　令和3年3月10日(2021.3.10)　(24)登録日　令和3年2月18日(2021.2.18)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 675Z
G06Q 20/38 (2012.01)　　H04L 9/00 675B
　　H04L 9/00 675C
　　G06Q 20/38 310

請求項の数 13　(全 28 頁)

(21)出願番号　特願2019-559290(P2019-559290)
(86)(22)出願日　平成31年1月31日(2019.1.31)
(65)公表番号　特表2020-526053(P2020-526053A)
(43)公表日　令和2年8月27日(2020.8.27)
(86)国際出願番号　PCT/CN2019/074057
(87)国際公開番号　WO2019/072317
(87)国際公開日　平成31年4月18日(2019.4.18)
審査請求日　令和1年12月25日(2019.12.25)

早期審査対象出願

(73)特許権者　520015461
アドバンスド　ニュー　テクノロジーズ　カンパニー　リミテッド
英国領ケイマン諸島　グランド　ケイマン　ケーワイ１－９００８　ジョージ　タウン　ホスピタル　ロード　２７　ケイマン　コーポレート　センター
(74)代理人　100188558
弁理士　飯田　雅人
(74)代理人　100205785
弁理士　▲高▼橋　史生

最終頁に続く

(54)【発明の名称】ブロックチェーンネットワーク内の資産間取引

(57)【特許請求の範囲】
【請求項１】
ブロックチェーンネットワークにおけるプライベート資産間取引のためのコンピュータ実装方法であって、1つまたは複数のプロセッサによって実行され、かつ、
前記ブロックチェーンネットワークにおける第1のノードによって、かつボウネイ-ゴー-ニッシム(BGN)暗号化を使用して、第1の値と、第2の値とに基づいて暗号文を生成するステップであって、
前記第2の値は、前記第1の値の準同型乗算と、前記ブロックチェーンネットワークにおける第2のノードによって提供される暗号化された為替レートとに基づいて決定され、
前記暗号文および前記暗号化された為替レートは同一の楕円曲線上にある、ステップと、
前記第1のノードによって前記第2のノードに、前記第1の値および前記暗号文を送信するステップと、
前記第1のノードによって、かつ前記第2のノードから、前記為替レートを明かすことなくゼロ知識証明(ZKP)ルーチンで前記為替レートを検証するために使用できるデータの集合を備える第1の証拠集合を受信するステップと、
前記第1のノードによって、前記暗号文が前記第1のノードのBGN公開鍵によって暗号化されていることを、前記ZKPルーチンを使用して、検証するために使用できるデータの集合を備える第2の証拠集合を生成するステップと、
前記第1のノードによって、前記第1のノードから前記第2のノードへの前記第1の値の移

転のための前記第1のノードと前記第2のノードとの間の第1のトランザクション、および前記第2のノードから第3のノードへの前記第2の値の移転のための前記第2のノードと前記第3のノードとの間の第2のトランザクションを備えるトランザクションを定義するステップと、

前記第1のノードによって、前記トランザクションであって、前記第1の証拠集合および前記第2の証拠集合に基づいて検証される、前記トランザクションの検証および実行のために前記ブロックチェーンネットワークの少なくとも1つのコンセンサスノードに前記トランザクションを送信し、そして前記トランザクションの検証に応じて、前記第1のトランザクションおよび前記第2のトランザクションを実行して、前記第1のノードの残高を前記第1の値だけ減少させ、前記第2のノードの第1の残高を前記第1の値だけ増加させ、前記第2のノードの第2の残高を前記第2の値だけ減少させ、そして前記第3のノードの残高を前記第2の値だけ増加させるステップと

を含む、方法。

【請求項２】

前記第1の証拠集合が、前記第1の値、前記第1のノードによって提供される一対の乱数、および前記暗号文に基づいて前記第2のノードによって提供される、請求項1に記載の方法。

【請求項３】

前記少なくとも1つのコンセンサスノードによって前記トランザクションを検証するステップが、前記第1のノードのデジタル署名および前記第2のノードのデジタル署名を検証するステップを含む、請求項1に記載の方法。

【請求項４】

前記少なくとも1つのコンセンサスノードによって前記トランザクションを検証するステップが、前記第1のノードによって提供される第1の範囲証明および前記第2のノードによって提供される第2の範囲証明を検証するステップを含む、請求項1に記載の方法。

【請求項５】

前記第1の範囲証明が、前記第1の値がゼロより大きいこと、および前記第1のノードの前記残高が前記第1の値以上であることを証明するZKPを備える、請求項4に記載の方法。

【請求項６】

前記第2の範囲証明が、前記第2のノードの前記第2の残高が前記第2の値以上であることを証明するZKPを備える、請求項4に記載の方法。

【請求項７】

前記トランザクションが、BGN暗号化を使用して生成される暗号文の集合を備えるデータ集合であって、前記少なくとも1つのコンセンサスノードによって前記トランザクションを検証するために使用される、データ集合をさらに備える、請求項1に記載の方法。

【請求項８】

前記第1のノードによって、前記ブロックチェーンネットワークのサブチェーンチャネルを通じて前記第2のノードから前記為替レートを受信するステップをさらに含む、請求項1に記載の方法。

【請求項９】

前記暗号文のうちの少なくとも1つの暗号文が、ペダーセンコミットメントを使用して提供される、請求項1に記載の方法。

【請求項１０】

前記第1の証拠集合の前記データの集合が、第1のデータ値および第2のデータ値であって、前記第2のノードのBGN公開鍵を生成するために使用されるパラメータに基づいて各々が決定される、第1のデータ値および第2のデータ値を備える、請求項1に記載の方法。

【請求項１１】

前記第2の証拠集合の前記データの集合が、暗号文の集合と、各値が前記暗号文の集合のハッシュに基づく値の集合とを備える、請求項1に記載の方法。

【請求項１２】

ブロックチェーンネットワークにおけるプライベート資産間取引のための命令が符号化された1つまたは複数のコンピュータ可読記憶媒体であって、前記命令が、1つまたは複数のプロセッサによって実行可能であり、かつ前記1つまたは複数のプロセッサに、請求項1乃至11のいずれか1項に記載の方法を実行させる、
1つまたは複数のコンピュータ可読記憶媒体。
【請求項１３】
1つまたは複数のプロセッサと、
前記1つまたは複数のプロセッサに結合され、かつブロックチェーンネットワークにおけるプライベート資産間取引のための命令が記憶された1つまたは複数のコンピュータ可読メモリと
を備え、前記命令が前記1つまたは複数のプロセッサによって実行可能であり、かつ前記1つまたは複数のプロセッサに、請求項1乃至11のいずれか1項に記載の方法を実行させる、
システム。
【発明の詳細な説明】
【背景技術】
【０００１】
分散型台帳システム(DLS)は、コンセンサスネットワークおよび/またはブロックチェーンネットワークとも称することができ、参加エンティティが安全かつ不変にデータを格納することを可能にする。DLSは、いかなる特定のユースケースにも関係せず一般的にブロックチェーンネットワークと称される。ブロックチェーンネットワークの種類例には、パブリックブロックチェーンネットワーク、プライベートブロックチェーンネットワークおよびコンソーシアムブロックチェーンネットワークを含むことができる。パブリックブロックチェーンネットワークは、全てのエンティティがDLSを使用してコンセンサスプロセスに参加するように開かれている。プライベートブロックチェーンネットワークは、読出しおよび書込み許可を中央で制御する、特定のエンティティのために提供される。コンソーシアムブロックチェーンネットワークは、コンセンサスプロセスを制御する、選択された一群のエンティティのために提供され、かつアクセス制御層を含む。
【０００２】
ブロックチェーンネットワークは、通貨などのデジタル資産の移転および交換を通じて価値を取引するために使用できる。ブロックチェーンネットワークの1つのノードから別のノードにデジタル資産を移転することによって、異なる数種類のデジタル資産がブロックチェーンネットワーク内で交換できる。一部の事例では、ブロックチェーンネットワーク内でデジタル資産を移転することは、為替レートに基づく一種類のデジタル資産の第2の種類のデジタル資産との交換を要する。
【０００３】
ブロックチェーンネットワークの参加者は、しかしながら、コンセンサスノードを含め、他の参加者がトランザクションの詳細(例えば、トランザクション金額、為替レート)に気づかないように、自分のトランザクションのプライバシーを所望するかもしれない。プライバシーを提供するために、暗号化方式が使用できる。しかしながら、一部の暗号化方式は、準同型乗算などの乗算演算をサポートしない。一部の暗号化方式がそのような乗算演算をサポートするが、それらは単一の乗算演算だけに限定される。これは、例えば、為替レートを含む資産間トランザクションの参加者の、為替レートのプライバシーを守る能力を抑制する。
【発明の概要】
【課題を解決するための手段】
【０００４】
本明細書の実装例は、ブロックチェーンネットワーク内で通貨を移転するためのコンピュータ実装方法を含む。より詳細には、本明細書の実装例は、暗号化トランザクションデータおよび暗号化為替レートを使用するブロックチェーンネットワーク内の資産間トランザクションに向けられる。

【０００５】
一部の実装例では、行為が、ブロックチェーンネットワークにおける第1のノードによって、かつボウネイ-ゴー-ニッシム(Boneh-Goh-Nissim:BGN)暗号化を使用して、第1の値と、第1の値およびブロックチェーンネットワークにおける第2のノードによって提供される為替レートに基づいて決定される第2の値とに基づいて暗号文を生成することと、第1のノードによって第2のノードに、第1の値および暗号文を送信することと、第1のノードによって、かつ第2のノードから、為替レートを明かすことなくゼロ知識証明(ZKP)ルーチンで為替レートを検証するために使用できるデータの集合を含む第1の証拠集合を受信することと、第1のノードによって、暗号文が第1のノードのBGN公開鍵によって暗号化されていることを、ZKPルーチンを使用して、検証するために使用できるデータの集合を含む第2の証拠集合を生成することと、第1のノードによって、第1のノードから第2のノードへの第1の値の移転のための第1のノードと第2のノードとの間の第1のトランザクション、および第2のノードから第3のノードへの第2の値の移転のための第2のノードと第3のノードとの間の第2のトランザクションを含むトランザクションを定義することと、第1のノードによって、トランザクションであり、第1の証拠集合および第2の証拠集合に基づいて検証される、トランザクションの検証および実行のためにブロックチェーンネットワークの少なくとも1つのコンセンサスノードにトランザクションを送信し、そしてトランザクションの検証に応じて、第1のトランザクションおよび第2のトランザクションを実行して、第1のノードの残高を第1の値だけ減少させ、第2のノードの第1の残高を第1の値だけ増加させ、第2のノードの第2の残高を第2の値だけ減少させ、そして第3のノードの残高を第2の値だけ増加させることとを含む。他の実装例は、対応するシステム、装置、およびコンピュータ記憶デバイスに符号化される、本方法の行為を行うように構成された、コンピュータプログラムを含む。

【０００６】
これらおよび他の実装例は各々以下の特徴の1つまたは複数を任意選択で含んでよい:第1の証拠集合が、第1の値、第1のノードによって提供される一対の乱数、および暗号文に基づいて第2のノードによって提供される;少なくとも1つのコンセンサスノードによってトランザクションを検証することが、第1のノードのデジタル署名および第2のノードのデジタル署名を検証することを含む;少なくとも1つのコンセンサスノードによってトランザクションを検証することが、第1のノードによって提供される第1の範囲証明および第2のノードによって提供される第2の範囲証明を検証することを含む;第1の範囲証明が、第1の値がゼロより大きいこと、および第1のノードの残高が第1の値以上であることを証明するZKPを含む;第2の範囲証明が、第2のノードの第2の残高が第2の値以上であることを証明するZKPを含む;トランザクションが、少なくとも部分的にBGN暗号化に基づいて生成される暗号文の集合を含むデータ集合であり、少なくとも1つのコンセンサスノードによってトランザクションを検証するために使用される、データ集合をさらに含む;行為が、第1のノードによって、ブロックチェーンネットワークのサブチェーンチャネルを通じて第2のノードから為替レートを受信することをさらに含む;暗号文のうちの少なくとも1つの暗号文が、ペダーセンコミットメント(Pedersen Commitment)を使用して提供される;第1の証拠集合のデータの集合が、第1のデータ値および第2のデータ値であり、第2のノードのBGN公開鍵を生成するために使用されるパラメータに基づいて各々が決定される、第1のデータ値および第2のデータ値を含む;ならびに第2の証拠集合のデータの集合が、暗号文の集合と、各値が少なくとも部分的に暗号文の集合のハッシュに基づく値の集合とを含む。

【０００７】
本明細書は、1つまたは複数のプロセッサに結合され、かつ1つまたは複数のプロセッサによって実行されると、1つまたは複数のプロセッサに本明細書で提供される方法の実装例に従う動作を行わせる命令が記憶された、1つまたは複数の非一時的コンピュータ可読記憶媒体も提供する。

【０００８】
本明細書は、本明細書で提供される方法を実装するためのシステムをさらに提供する。

本システムは、1つまたは複数のプロセッサと、1つまたは複数のプロセッサによって実行されると、1つまたは複数のプロセッサに本明細書で提供される方法の実装例に従う動作を行わせる命令が記憶された、1つまたは複数のプロセッサに結合されるコンピュータ可読記憶媒体とを含む。

【０００９】

本明細書に従う方法が本明細書に記載される態様および特徴のいかなる組合せも含んでよいことが認識される。すなわち、本明細書に従う方法は、本明細書に具体的に記載される態様および特徴の組合せに限定されるのではなく、提供される態様および特徴のいかなる組合せも含む。

【００１０】

本明細書の1つまたは複数の実装例の詳細が添付の図面および以下の説明に明らかにされる。本明細書の他の特徴および利点は同説明および図面から、ならびに請求項から明らかであろう。

【図面の簡単な説明】

【００１１】

【図１】本明細書の実装例を実行するために使用できる環境の一例を描く。

【図２】本明細書の実装例に従う概念アーキテクチャの一例を描く。

【図３】本明細書の実装例に従う資産間取引プラットフォームの一例を描く。

【図４】本明細書の実装例に従う資産間トランザクションを実行するための信号図の一例を描く。

【図５】本明細書の実装例に従って実行できるプロセスの一例を描く。

【図６】本明細書の実装例に従う装置のモジュールの例を描く。

【発明を実施するための形態】

【００１２】

様々な図面における同様の参照記号は同様の要素を示す。

【００１３】

本明細書の実装例は、ブロックチェーンネットワーク内で資産を移転するためのコンピュータ実装方法を含む。より詳細には、本明細書の実装例は、暗号化トランザクションデータおよび暗号化為替レートを使用するブロックチェーンネットワーク内の資産間トランザクションに向けられる。

【００１４】

本明細書の実装例のための更なる背景を提供するため、かつ上記提示したように、分散型台帳システム(DLS)は、コンセンサスネットワーク(例えば、ピアツーピアノードから構成される)およびブロックチェーンネットワークとも称することができ、参加エンティティが安全かつ不変にトランザクションを行ってデータを格納することを可能にする。用語ブロックチェーンが一般に特定のネットワークおよび/またはユースケースと関連付けられるが、ブロックチェーンは本明細書では、いかなる特定のユースケースにも関係なくDLS一般を指すために使用される。

【００１５】

ブロックチェーンは、トランザクションが不変であるようにトランザクションを記憶するデータ構造である。このように、ブロックチェーンに記録されたトランザクションは確実で信頼できる。ブロックチェーンは1つまたは複数のブロックを含む。チェーンにおける各ブロックは、チェーンにおけるそれの直前の以前のブロックの暗号ハッシュを含むことによってその以前のブロックにリンクされる。各ブロックは、タイムスタンプ、それ自身の暗号ハッシュ、および1つまたは複数のトランザクションも含む。トランザクションは、ブロックチェーンネットワークのノードによって既に検証されており、マークルツリーへハッシュおよび符号化される。マークルツリーは、ツリーのリーフノードにおけるデータがハッシュされ、そしてツリーの各ブランチにおける全てのハッシュがブランチのルートで連結されるデータ構造である。このプロセスはツリー全体のルートまでツリーを上がり続け、そこでツリーにおける全てのデータを表すハッシュを記憶する。ツリーに記憶

されたトランザクションのであるように見えるハッシュは、それがツリーの構造と一致しているかどうかを判定することによって迅速に検証できる。

【００１６】

ブロックチェーンがトランザクションを記憶するための非集中型または少なくとも部分的に非集中型データ構造であるのに対して、ブロックチェーンネットワークは、トランザクションをブロードキャスト、検証および有効化すること等によって1つまたは複数のブロックチェーンを管理、更新および維持するコンピューティングノードのネットワークである。コンソーシアムブロックチェーンネットワークは参加エンティティの間でプライベートである。コンソーシアムブロックチェーンネットワークでは、コンセンサスプロセスは、公認されたノードの集合によって制御されており、1つまたは複数のノードがそれぞれのエンティティ(例えば、金融機関、保険会社)によって運営される。例えば、10のエンティティ(例えば、金融機関、保険会社)のコンソーシアムがコンソーシアムブロックチェーンネットワークを運営でき、その各々がコンソーシアムブロックチェーンネットワークにおいて少なくとも1つのノードを運営する。したがって、コンソーシアムブロックチェーンネットワークは、参加エンティティに対するプライベートネットワークと考えることができる。一部の例では、ブロックが有効であり、ブロックチェーンに追加されるためには、各エンティティ(ノード)がブロックごとに署名しなければならない。一部の例では、ブロックが有効であり、ブロックチェーンに追加されるためには、少なくともエンティティ(ノード)の部分集合(例えば、少なくとも7のエンティティ)がブロックごとに署名しなければならない。

【００１７】

上記提示したように、ブロックチェーンネットワークは、パブリックブロックチェーンネットワーク、プライベートブロックチェーンネットワークまたはコンソーシアムブロックチェーンネットワークとして提供できる。本明細書の実装例は、コンソーシアムブロックチェーンネットワークに関して本明細書にさらに詳細に記載される。しかしながら、本明細書の実装例が任意の適切な種類のブロックチェーンネットワークで実現できることが企図される。本明細書に記載される手法がコンソーシアムブロックチェーンネットワークに関連するとして示されるが、同手法は、パブリックブロックチェーンネットワークおよびプライベートブロックチェーンネットワークを含め、他の種類のブロックチェーンネットワークでも、変更の有無にかかわらず、使用できる。

【００１８】

一般に、コンソーシアムブロックチェーンネットワークは参加エンティティの間でプライベートである。コンソーシアムブロックチェーンネットワークでは、コンセンサスプロセスは、公認されたノードの集合によって制御されており、それらはコンセンサスノードと称することができ、1つまたは複数のコンセンサスノードがそれぞれのエンティティ(例えば、金融機関、保険会社)によって運営される。例えば、10のエンティティ(例えば、金融機関、保険会社)のコンソーシアムがコンソーシアムブロックチェーンネットワークを運営でき、その各々がコンソーシアムブロックチェーンネットワークにおいて少なくとも1つのノードを運営する。

【００１９】

一部の例では、コンソーシアムブロックチェーンネットワーク内に、全てのノードにわたって複製されるブロックチェーンとしてグローバルブロックチェーンが提供される。すなわち、全てのコンセンサスノードがグローバルブロックチェーンに関しては完全状態コンセンサスに達している。コンセンサス(例えば、ブロックチェーンへのブロックの追加への合意)を達成するために、コンソーシアムブロックチェーンネットワーク内にコンセンサスプロトコルが実装される。コンセンサスプロトコル例には、限定することなく、実用的ビザンチン障害耐性(PBFT)、プルーフオブワーク(POW)、プルーフオブステーク(POS)およびプルーフオブオーソリティ(POA)を含む。

【００２０】

コンソーシアムブロックチェーンネットワークは、デジタル資産の移転および交換を行

うために使用できる。一部の事例では、デジタル資産は実世界の資産を表すことができる。一部の事例では、デジタル資産は仮想資産を表すことができる。例えば、仮想資産は実世界の価値を表すことができ、そしてそれは製品および/またはサービスを購入するために使用できる。仮想資産は、実世界の物理的資産(例えば、中国RMB、米国ドル)の代替物として提供される。コンソーシアムブロックチェーンネットワークがトランザクションを検証して不変に記録するので、コンソーシアムブロックチェーンネットワーク内でトランザクションを行うことは付加的なセキュリティを提供する。本明細書の実装例は、通貨(例えば、RMB、USD)に関して本明細書にさらに詳細に記載される。しかしながら、実装例が任意の適切なデジタル資産で実現できることが企図される。

【００２１】

図1は、本明細書の実装例を実行するために使用できる環境100の一例を描く。一部の例では、環境100は、エンティティがコンソーシアムブロックチェーンネットワーク102に参加することを可能にする。環境100は、コンピューティングデバイス106、108およびネットワーク110を含む。一部の例では、ネットワーク110は、ローカルエリアネットワーク(LAN)、ワイドエリアネットワーク(WAN)、インターネットまたはその組合せを含み、そしてウェブサイト、ユーザデバイス(例えば、コンピューティングデバイス)およびバックエンドシステムを接続する。一部の例では、ネットワーク110は有線および/または無線通信リンクを通じてアクセスできる。

【００２２】

描かれた例では、コンピューティングシステム106、108は各々、コンソーシアムブロックチェーンネットワーク102へのノードとしての参加を可能にする任意の適切なコンピューティングシステムを含むことができる。コンピューティングデバイス例には、限定することなく、サーバ、デスクトップコンピュータ、ラップトップコンピュータ、タブレットコンピューティングデバイスおよびスマートフォンを含む。一部の例では、コンピューティングシステム106、108は、コンソーシアムブロックチェーンネットワーク102と対話するための1つまたは複数のコンピュータ実装サービスをホストする。例えば、コンピューティングシステム106は、第1のエンティティ(例えば、ユーザA)が1つまたは複数の他のエンティティ(例えば、他のユーザ)とのそのトランザクションを管理するために使用するトランザクション管理システムなど、第1のエンティティのコンピュータ実装サービスをホストできる。コンピューティングシステム108は、第2のエンティティ(例えば、ユーザB)が1つまたは複数の他のエンティティ(例えば、他のユーザ)とのそのトランザクションを管理するために使用するトランザクション管理システムなど、第2のエンティティのコンピュータ実装サービスをホストできる。図1の例では、コンソーシアムブロックチェーンネットワーク102はノードのピアツーピアネットワークとして表現され、そしてコンピューティングシステム106、108はそれぞれ第1のエンティティおよび第2のエンティティのノードを提供し、それらがコンソーシアムブロックチェーンネットワーク102に参加する。

【００２３】

図2は、本明細書の実装例に従う概念アーキテクチャ200の一例を描く。概念アーキテクチャ200は、エンティティ層202、ホストサービス層204およびブロックチェーンネットワーク層206を含む。描かれた例では、エンティティ層202は3者の参加者、参加者A、参加者Bおよび参加者Cを含み、各参加者がそれぞれのトランザクション管理システム208を有する。

【００２４】

描かれた例では、ホストサービス層204は、各トランザクション管理システム208に対するインタフェース210を含む。一部の例では、それぞれのトランザクション管理システム208は、プロトコル(例えば、ハイパーテキスト転送プロトコルセキュア(HTTPS))を使用してネットワーク(例えば、図1のネットワーク110)を通じてそれぞれのインタフェース210と通信する。一部の例では、各インタフェース210は、それぞれのトランザクション管理システム208とブロックチェーンネットワーク層206との間の通信接続を提供する。より詳細には、インタフェース210は、ブロックチェーンネットワーク層206のブロックチェーン

ネットワーク212と通信する。一部の例では、インタフェース210とブロックチェーンネットワーク層206との間の通信は、リモートプロシージャコール(RPC)を使用して行われる。一部の例では、インタフェース210は、それぞれのトランザクション管理システム208に対してブロックチェーンネットワークノードを「ホストする」。例えば、インタフェース210は、ブロックチェーンネットワーク212へのアクセスのためのアプリケーションプログラミングインタフェース(API)を提供する。

【００２５】

本明細書に記載されるように、ブロックチェーンネットワーク212は、ブロックチェーン216に情報を不変に記録する複数のノード214を含むピアツーピアネットワークとして提供される。単一のブロックチェーン216が概略的に描かれるが、ブロックチェーン216の複数のコピーが提供されて、ブロックチェーンネットワーク212にわたって維持される。例えば、各ノード214がブロックチェーンのコピーを記憶する。一部の実装例では、ブロックチェーン216は、コンソーシアムブロックチェーンネットワークに参加する2つ以上のエンティティ間で行われるトランザクションと関連する情報を記憶する。

【００２６】

ブロックチェーン(例えば、図2のブロックチェーン216)はブロックのチェーンから構成されおり、各ブロックがデータを記憶する。データ例には、2者以上の参加者間のトランザクションを表すトランザクションデータを含む。トランザクションが非限定例として本明細書に使用されるが、任意の適切なデータがブロックチェーンに記憶できる(例えば、文書、画像、ビデオ、オーディオ)ことが企図される。トランザクション例には、限定することなく、価値があるもの(例えば、資産、製品、サービス、通貨)の交換を含むことができる。トランザクションデータはブロックチェーン内に不変に記憶される。すなわち、トランザクションデータは変更できない。

【００２７】

ブロックへの記憶の前に、トランザクションデータはハッシュされる。ハッシングは、トランザクションデータ(列データとして提供される)を固定長ハッシュ値(同じく列データとして提供される)へ変換するプロセスである。ハッシュ値を非ハッシュ化してトランザクションデータを得ることは可能でない。ハッシングは、トランザクションデータの僅かな変更さえ結果として完全に異なるハッシュ値になることを保証する。さらに、上記したように、ハッシュ値は固定長である。すなわち、トランザクションデータのサイズにかかわらず、ハッシュ値の長さは固定される。ハッシングは、ハッシュ関数を通じてトランザクションデータを処理してハッシュ値を生成することを含む。ハッシュ関数例には、限定することなく、セキュアハッシュアルゴリズム(SHA)-256を含み、これは256ビットハッシュ値を出力する。

【００２８】

複数のトランザクションのトランザクションデータがハッシュされてブロックに記憶される。例えば、2つのトランザクションのハッシュ値が提供され、そしてそれら自体ハッシュされて別のハッシュを提供する。このプロセスは、ブロックに記憶されることになる全てのトランザクションに対して、単一のハッシュ値が提供されるまで繰り返される。このハッシュ値はマークルルートハッシュと称され、ブロックのヘッダに記憶される。トランザクションのいずれかの変更が結果としてそのハッシュ値の変更に、最終的に、マークルルートハッシュの変更になることになる。

【００２９】

ブロックはコンセンサスプロトコルを通じてブロックチェーンに追加される。ブロックチェーンネットワーク内の複数のノードがコンセンサスプロトコルに参加して作業を行って、ブロックをブロックチェーンに追加させる。そのようなノードはコンセンサスノードと称される。上記提示したPBFTがコンセンサスプロトコルの非限定例として使用される。コンセンサスノードは、コンセンサスプロトコルを実行してブロックチェーンにトランザクションを追加する。

【００３０】

さらに詳細に、コンセンサスノードは、ブロックヘッダを生成し、ブロックにおけるトランザクションの全てをハッシュし、そしてブロックにおける全てのトランザクションに対して単一のハッシュ値が提供される(マークルルートハッシュ)まで、ハッシュ値を対に組み合わせて更なるハッシュ値を生成する。このハッシュはブロックヘッダに追加される。コンセンサスノードは、ブロックチェーンにおける最近のブロック(すなわち、ブロックチェーンに追加された最後のブロック)のハッシュ値も決定する。コンセンサスノードは、ブロックヘッダにナンス値およびタイムスタンプも追加する。

【００３１】

一般に、PBFTは、ビザンチン障害(例えば、故障ノード、悪意のあるノード)に耐える実用的なビザンチン状態機械複製を提供する。これは、障害が発生するであろうと仮定する(例えば、独立ノード障害および/またはコンセンサスノードによって送られる操作メッセージの存在を仮定する)ことによってPBFTで達成される。PBFTでは、コンセンサスノードは、主コンセンサスノードおよびバックアップコンセンサスノードを含む順序で設けられる。主コンセンサスノードは定期的に変更される。トランザクションは、ブロックチェーンネットワークの世界状態に関して合意に達しているブロックチェーンネットワーク内の全てのコンセンサスノードによってブロックチェーンに追加される。このプロセスでは、コンセンサスノード間でメッセージが送信され、そして各コンセンサスノードは、メッセージが指定されたピアノードから受信されることを証明し、そしてメッセージが送信中に変更されなかったことを検証する。

【００３２】

PBFTでは、コンセンサスプロトコルは、全てのコンセンサスノードが同じ状態で開始する、複数の段階で提供される。初めに、クライアントが、サービス動作を起動する(例えば、ブロックチェーンネットワーク内でトランザクションを実行する)よう、主コンセンサスノードに要求を送る。要求を受信したことに応じて、主コンセンサスノードは、バックアップコンセンサスノードに要求をマルチキャストする。バックアップコンセンサスノードは要求を実行し、そして各々がクライアントに応答を送る。クライアントは、閾値数の応答が受信されるまで待つ。一部の例では、クライアントは、f+1個の応答が受信されるのを待ち、ここでfは、ブロックチェーンネットワーク内で許容できる障害コンセンサスノードの最大数である。最終結果は、十分な数のコンセンサスノードが、ブロックチェーンに追加されることになる記録の順に関して合意に達し、そして記録が受理または却下されることである。

【００３３】

一部のブロックチェーンネットワークでは、トランザクションのプライバシーを守るために暗号法が実装される。例えば、2つのノードがトランザクションをプライベートに保ちたければ、ブロックチェーンネットワークにおける他のノードがトランザクションの詳細を認められないように、ノードはトランザクションデータを暗号化できる。暗号法例には、限定することなく、対称暗号化および非対称暗号化を含む。対称暗号化は、暗号化(平文から暗号文を生成すること)のためにも復号化(暗号文から平文を生成すること)のためにも単一の鍵を使用する暗号化プロセスを指す。対称暗号化では、複数のノードに同じ鍵が利用可能であるので、各ノードがトランザクションデータを暗/復号化できる。

【００３４】

非対称暗号化は、各々秘密鍵および公開鍵を含む鍵ペアを使用しており、秘密鍵がそれぞれのノードだけに知られており、公開鍵がブロックチェーンネットワークにおける任意のまたは全ての他のノードに知られている。ノードが別のノードの公開鍵を使用してデータを暗号化でき、そして暗号化データはその別のノードの秘密鍵を使用して復号化できる。例えば、図2を再び参照すると、参加者Aが、参加者Bの公開鍵を使用してデータを暗号化し、そして参加者Bに暗号化データを送ることができる。参加者Bは、その秘密鍵を使用して、暗号化データ(暗号文)を復号化して元データ(平文)を抽出できる。ノードの公開鍵で暗号化されたメッセージは、ノードの秘密鍵を使用してのみ復号化できる。

【００３５】

非対称暗号化は、デジタル署名を提供するために使用されるが、それは、トランザクションの参加者がトランザクションの有効性と同様にトランザクションの他の参加者も確認することを可能にする。例えば、ノードがメッセージにデジタル署名でき、そして別のノードが、参加者Aのデジタル署名に基づいてメッセージがそのノードによって送られたことを確認できる。デジタル署名は、メッセージが転送中に改竄されていないことを保証するためにも使用できる。例えば、再び図2を参照すると、参加者Aが参加者Bにメッセージを送ることになる。参加者Aは、メッセージのハッシュを生成し、次いで、その秘密鍵を使用して、ハッシュを暗号化して暗号化ハッシュとしてデジタル署名を提供する。参加者Aは、メッセージにデジタル署名を添付し、そして参加者Bにデジタル署名付きメッセージを送る。参加者Bは、参加者Aの公開鍵を使用してデジタル署名を復号化し、そしてハッシュを抽出する。参加者Bは、メッセージをハッシュし、そして両ハッシュを比較する。両ハッシュが同じであれば、参加者Bは、メッセージが実際に参加者Aからであり、かつ改竄されなかったことを確認できる。

【００３６】

実世界の物理的通貨の移転のように、通貨のデジタル表現を効果的に移転することは、時に譲受人に第1の種類の通貨を第2の種類の通貨と交換することを要求する。例えば、第1の種類の通貨(例えば、米国ドル($))だけを有するコンソーシアムブロックチェーンネットワークの第1のメンバー(例えば、参加者A)が通貨を第2の種類の通貨(例えば、中国RMB)でコンソーシアムブロックチェーンネットワークの第2のメンバー(例えば、参加者C)に移転したいかもしれない。参加者Aが参加者Cに価値を移転するために、第1の種類の通貨の額が、参加者Cへの移転の前に第2の種類の通貨の相当価値と交換される。

【００３７】

本明細書の実装例に従って、かつ本明細書にさらに詳細に記載されるように、通貨の種類を交換することは、仲介者としてのコンソーシアムブロックチェーンネットワークの第3のメンバー(例えば、参加者B)を通して達成できる。例えば、参加者Aが参加者Bに第1の種類の通貨の額を移転し、そして参加者Bが、参加者Bによって使用される為替レート(ER)に基づいて相当価値を有する第2の種類の通貨の額を参加者Cに移転できる。一部の例では、参加者Bは、コンソーシアムブロックチェーンネットワークのメンバーに両替サービスを提供する金融機関である。

【００３８】

ブロックチェーンネットワーク内の両替に関与する当事者のプライバシーを保証するために、交換の基礎となるトランザクションデータは、ブロックチェーンネットワーク内の交換の検証および公開の前に暗号化される。一部の例では、トランザクションデータは、第1の通貨の移転額(t_1)および第1の額と交換に提供される第2の通貨の額(t_2)を含む。典型的に、検証のためにブロックチェーンに提出されるトランザクションデータは、ボウネイ-ゴー-ニッシム(BGN)暗号化などの準同型暗号化方式を使用して暗号化される。準同型暗号化方式の下で、2つ以上の暗号化データの項目が、限定することなく、合計されてよい。他の暗号化方式(例えば、ペリエ(Paillier)公開鍵暗号化(PKE))とは異なり、BGN暗号化は、2つの暗号文に対する準同型乗算(例えば、暗号化βおよび暗号化t_1の乗算)を可能にする。しかしながら、準同型暗号化を使用して暗号化されるデータ項目は単一の乗算に限定される。これは、準同型暗号化を使用して暗号化される2つのデータ項目の乗法ペアリングが、暗号化乗数とは異なる階数である暗号化積を生成するからである。

【００３９】

以下の式は、楕円曲線g上のペアリングと通常呼ばれる、乗法準同型の一回性を証明する:

$$e:g\times g\rightarrow g_1$$

ここで、乗算されている暗号化データ項目の各々は、g_1上にある乗算の積とは異なる楕円曲線g上にある。乗法準同型によって生成される暗号化データ項目は、基礎となる楕円曲線のこの変更のためさらには乗算または除算できない。加えて、乗法準同型によって生成される暗号化データ項目は、直接準同型暗号化によって生成されるデータ項目と比較でき

ない。例えば、同じ楕円曲線g上の上記の式における最初の2つの暗号化データ項目は互いと比較できるが、基礎となる楕円曲線gおよびg_1の差のため、乗法準同型によって生成される楕円曲線g_1上の第3の暗号化データ項目とは比較できない。

【００４０】

BGN暗号化では、BGN暗号化を使用することになる各参加者iには、鍵生成プロセスを通じてBGN公開鍵(PK)、秘密鍵(SK)ペア(例えば、PK_{BGN_i}、SK_{BGN_o})が提供される。鍵生成プロセスを通じて、以下が提供される:

$PK_{BGNi}=\{N,g,g_1,e,P,Q\}i$

$SK_{BGN_i}=p$

式中:

$N=pq$

p、qは大きな素数である

gは階数Nの楕円曲線

$e:g\times g\rightarrow g_1$はペアリングである

$P\in g$生成元

$Q=q\alpha P$(階数がpであるgの部分群のランダムな生成元)

$\alpha<N$

【００４１】

本明細書の背景では、準同型暗号化方式の下で、公開為替レートを伴う交換トランザクションは、移転額および/または交換額を明かすまたは公開することなくコンソーシアムブロックチェーンネットワークによって検証および記録できる。例えば、参加者Aによって交換サービス提供者参加者Bに移転される第1の通貨の額(t_1)も、第1の額と交換に参加者Bによって提供される第2の通貨の額(t_2)も準同型暗号化を使用して暗号化できる。この方式の下で、暗号化t_1も暗号化t_2も楕円曲線g上にある。暗号化移転量t_1には参加者Bの公開為替レートが乗算されて、t_1と交換に参加者Bによって提供されるべきである第2の通貨の額を決定できる。参加者Bの為替レートがこの例では公開の非暗号化値であるので、t_1および公開為替レートの積は、t_1と同じ楕円曲線g上にある暗号化データ項目である。参加者Aと参加者Bとの間の交換トランザクションは、t_1および公開為替レートの暗号化積を暗号化データ項目t_2と比較することによってブロックチェーンネットワークによって検証できる。公開為替レートが乗算されたt_1の暗号化積が暗号化データ項目t_2に等しければ、トランザクションは検証されてブロックチェーンに記録される。

【００４２】

この検証方式は、公開為替レートを伴う交換トランザクションを検証するための有効な手段を提供するが、両替サービスを提供するブロックチェーンネットワークメンバーはしばしば他のそのような提供者と競合している。結果的に、それらは、自分の為替レートがブロックチェーンネットワーク内で公開されることを望まない。したがって、ブロックチェーンネットワーク内で行われて、それによって検証される交換トランザクションに関して、トランザクションデータと同様に為替レートも暗号化されることが望ましい。

【００４３】

しかしながら、上記した検証を使用するときに、準同型暗号化に対する1回乗算の限定が、トランザクションデータも為替レートも準同型暗号化を使用して暗号化される、交換トランザクションの検証への障壁を生じさせる。例えば、参加者Aによって交換サービス提供者参加者Bに移転される第1の通貨の額(t_1)、第1の通貨の移転額が参加者Bによって交換された第2の通貨の額(t_2)、および参加者Bの為替レート(β)が各々準同型暗号化を使用して暗号化できる。この方式の下で、暗号化t_1、暗号化t_2および暗号化βは全て同じ楕円曲線g上にある。

【００４４】

上述したように、交換トランザクションに伴う為替レートが公開されるときはいつでも、交換トランザクションは、t_1および公開為替レートの積を暗号化データ項目t_2と比較することによってブロックチェーンネットワークによって検証できる。しかしながら、為替

レートが暗号化される(β)と、t_1および暗号化為替レート(β)の積は楕円曲線g_1上にあり、これはt_2の基礎となる曲線gと異なる。乗法準同型から生じるこの階数の差に基づいて、暗号化為替レート(β)が乗算されたt_1の積はt_2と比較できない。結果として、現在の検証方式の下では、トランザクションデータおよび為替レートの両方の暗号化を伴う交換トランザクションの検証はブロックチェーンネットワーク内では行えない。

【００４５】

以上の背景に鑑みて、かつ本明細書にさらに詳細に記載されるように、本明細書の実装例は、暗号化トランザクションデータおよび暗号化為替レートを使用するブロックチェーンネットワーク内の資産間取引に向けられる。より詳細には、本明細書の資産間取引プラットフォームは、プライベート(暗号化)為替レート検証が行えるトランザクションを可能にする。

【００４６】

図3は、本明細書の実装例に従う資産間取引プラットフォーム300の一例を描く。描かれた例では、資産間取引プラットフォーム例300は、それぞれのデバイス302、304、306と関連する、3者の参加者、参加者A、参加者Bおよび参加者Cを含む。資産間取引プラットフォーム例300は、サブチェーンチャネル308、ネットワーク310およびコンソーシアムブロックチェーンネットワーク312も含む。

【００４７】

一部の例では、ネットワーク310は、ローカルエリアネットワーク(LAN)、ワイドエリアネットワーク(WAN)、インターネットまたはその組合せを含み、そしてウェブサイト、ユーザデバイス(例えば、コンピューティングデバイス)およびバックエンドシステムを接続する。一部の例では、ネットワーク310は有線および/または無線通信リンクを通じてアクセスできる。

【００４８】

本明細書に記載されるように、ブロックチェーンネットワーク312は、ブロックチェーン322に情報を不変に記録する複数のノード314を含むピアツーピアネットワークとして提供される。単一のブロックチェーン322が概略的に描かれるが、ブロックチェーン322の複数のコピーが提供されて、ブロックチェーンネットワーク312にわたって維持される。例えば、各ノード314がブロックチェーン322のコピーを記憶する。一部の実装例では、ブロックチェーン322は、コンソーシアムブロックチェーンネットワーク312に参加する2つ以上のエンティティ間で行われるトランザクションと関連する情報を記憶する。一部の例では、デバイス302、304、306は、コンソーシアムブロックチェーンネットワーク312におけるそれぞれのノード314の一部である。

【００４９】

一部の実装例では、デバイス302、デバイス304およびデバイス306は、それぞれのアカウント、アカウントA316、アカウントB318およびアカウントC320を含む。一部の例では、アカウントA316、アカウントB318およびアカウントC320は金融資産を記憶する。一部の例では、アカウントA316、アカウントB318およびアカウントC320は1つまたは複数の種類の通貨の額を記憶する。

【００５０】

一部の実装例では、サブチェーンチャネル308は、コンソーシアムブロックチェーンネットワーク312の2つのメンバー間でブロックチェーンネットワーク312の外側で情報を転送するために使用できる。一部の例では、プライベート金融情報が、サブチェーンチャネル308を通じてブロックチェーンネットワーク312の外側でコンソーシアムブロックチェーンネットワーク312の1つのメンバーからコンソーシアムブロックチェーンネットワーク312の別のメンバーに転送できる。例えば、デバイス304は、サブチェーンチャネル308を通じてプライベート為替レート(β)を送信することによって、ブロックチェーンネットワーク312の外側でデバイス302に為替レートを転送できる。

【００５１】

一部の例では、コンソーシアムブロックチェーンネットワーク312の2つ以上のメンバー

間のトランザクションが検証および記録のためにブロックチェーンネットワーク312に提出できる。一部の例では、コンソーシアムブロックチェーンネットワーク312の2つ以上のメンバー間の資産(例えば、通貨)交換トランザクションが交換の検証のためにブロックチェーンネットワーク312に提出できる。一部の例では、ブロックチェーンネットワーク312に提出されるトランザクション情報は暗号化される。一部の例では、ブロックチェーンネットワーク312に提出されるトランザクション情報は準同型暗号化を使用して暗号化される。一部の例では、トランザクション情報は、為替レート、移転されることになる第1の額、および移転されることになる第2の額を含む。一部の例では、移転されることになる第2の額は、為替レートが乗算された第1の額の積に等しい。

【００５２】

図4は、本明細書の実装例に従う資産間トランザクションを実行するための信号図400の一例を描く。図4の信号図400は、アカウントA402(例えば、ブロックチェーンネットワークにおけるノード)、アカウントB404(例えば、ブロックチェーンネットワークにおけるノード)およびブロックチェーンネットワークのコンセンサスノード406を含む。一部の例では、アカウントA402およびアカウントB404は、ブロックチェーンネットワークの参加者(例えば、それぞれ、参加者Aおよび参加者B)の資産を管理するために使用される。一部の例では、アカウントA402およびアカウントB404は、それぞれ、参加者Aおよび参加者Bのデジタル資産を記憶する。一部の例では、参加者Bは金融機関である。

【００５３】

資産間トランザクションの一例が図4を参照しつつ本明細書にさらに詳細に記載される。トランザクション例では、第1の通貨(例えば、USD)での額(t_1)が、第2の通貨(例えば、RMB)での額(t_2)でアカウントAからブロックチェーンネットワークにおける別の参加者(例えば、参加者C)のアカウントに移転される。額(t_1)は、第1の通貨と第2の通貨との間のプライベート為替レート(β)を提供するアカウントB404、仲介者を使用して移転される。アカウントA402は残額(s_A)を含み、これはアカウントA402が利用可能な第1の通貨での価値の残高である。アカウントB404は第1の残額

【００５４】

【数１】

$$(s_{B_1})$$

【００５５】

を含み、これはアカウントB404が利用可能な第1の通貨での価値の残高であり、かつ第2の残額

【００５６】

【数２】

$$(s_{B_2})$$

【００５７】

を含み、これはアカウントB404が利用可能な第2の通貨での価値の残高である。

【００５８】

資産間トランザクション例では、アカウントB404からアカウントA402にプライベート為替レート(β)が送信される(408)。プライベート為替レートを伝達するメッセージはネットワークを通じて送信されてよい。一部の例では、プライベート為替レートを伝達するメッセージはサブチェーンチャネル(例えば、図3のサブチェーンチャネル308)を通じて送信される。

【００５９】

アカウントA402が2つの乱数(r_1、r_2)を生成する(410)。アカウントA402が交換額(t_2)および暗号文の集合(X_1、Y_1、Z_1)および(X_2、Y_2、Z_2)を計算する(412)。一部の実装例では、交換額(t_2)は、以下に示されるように、移転されることになる額(t_1)およびプライベート為替レート(β)の積に等しい:

$$t_2=\beta t_1$$

一部の実装例では、暗号文の集合(X_1、Y_1、Z_1)および(X_2、Y_2、Z_2)はコミットメント方式および暗号化方式に基づいて決定される。コミットメント方式例には、限定することなく、ペダーセンコミットメント(PC)を含む。暗号化方式例には、限定することなく、BGN暗号化を含む。BGN暗号化のために、各参加者はBGN公開鍵(PK)、秘密鍵(SK)ペアを含む。例えば、アカウントA402にBGN PK-SKペア(例えば、PK_{BGN_A}、SK_{BGN_A})が割り当てられ、アカウントB404にBGN PK-SKペア(例えば、PK_{BGN_B}、SK_{BGN_B})が割り当てられ、そしてアカウントC(図4に描かれない)にBGN PK-SKペア(例えば、PK_{BGN_C}、SK_{BGN_C})が割り当てられる。

【００６０】

一部の実装例では、暗号文の集合(X_1、Y_1、Z_1)および(X_2、Y_2、Z_2)は:

$$(X_1、Y_1、Z_1)=(PC(t_1、r_1)、BGN_A(t_1、r_1)、BGN_B(t_1、r_1))$$

$$(X_2、Y_2、Z_2)=(PC(t_2、r_2)、BGN_B(t_2、r_2)、BGN_C(t_2、r_2))$$

としてそれぞれ決定される。表記PC(t、r)は、ブラインド因子(blind factor)としての乱数rを持つtのペダーセンコミットメントを示す。表記BGN_Aは、アカウントA402の公開鍵を使用するBGN暗号化を示し、表記BGN_Bは、アカウントB404の公開鍵を使用するBGN暗号化を示し、そして表記BGN_Cは、アカウントCの公開鍵を使用するBGN暗号化を示す。一部の例では、アカウントA402は残高暗号文を:

【００６１】

【数３】

$$\left(PC(s_A,\bar{r}_A),BGN_A(s_A,\bar{r}_A)\right)$$

.

【００６２】

として提供し、ここで、

【００６３】

【数４】

$$\bar{r}_A$$

【００６４】

はアカウントA402によって生成される乱数である。

【００６５】

アカウントA402からアカウントB404に暗号文の部分集合(X_1、Z_1)および(X_2、Y_2)、乱数(r_1、r_2)ならびに額(t_1)が送られる(414)。一部の実装例では、アカウントA402からアカウントB404へのメッセージは暗号化メッセージ(例えば、上記した非対称暗号化を使用する)である。一部の例では、メッセージはサブチェーンチャネル(例えば、図3のサブチェーンチャネル308)を通じて送信される。一部の例では、(暗号化)メッセージはデータ集合$[t_1,r_1,r_2,X_1,Z_1,X_2,Y_2]$を含む。

【００６６】

アカウントBがメッセージを復号化してデータ(例えば、$[t_1,r_1,r_2,X_1,Z_1,X_2,Y_2]$)を明かす。暗号文データがアカウントB404によって検証される(416)。一部の例では、アカウントB404は、アカウントA402によって提供されるt_1、r_1、r_2に基づいて暗号文X_1、Z_1、X_2、Y_2が正しいかどうかを調べることによって暗号文データを検証する。すなわち、アカウ

ントBは、X_1、Z_1、X_2、Y_2を再計算し、そしてそれらがアカウントA402から受信されたものに等しいかどうかを判定する。暗号文が等しくなければ、アカウントAにエラーを送ることができ、そしてトランザクションは終了する。

【００６７】

暗号文が検証されれば、アカウントB404が範囲証明(RP_B)を生成する(418)。一部の実装例では、範囲証明(RP_B)は、アカウントB404が交換トランザクションを行うのに十分な資金を有するかどうかを確認するために使用できるゼロ知識証明(ZKP)である。例えば、範囲証明(RP_B)は以下を証明するために生成できる:

【００６８】

【数５】

$$s_{B_2} - t_2 \geq 0$$

【００６９】

一部の例では、アカウントB404は第1の残高暗号文および第2の残高暗号文をそれぞれ:

【００７０】

【数６】

$$\left(PC\left(s_{B_1}, \bar{r}_{B_1}\right), BGN_B\left(s_{B_1}, \bar{r}_{B_1}\right)\right)$$

$$\left(PC\left(s_{B_2}, \bar{r}_{B_2}\right), BGN_B\left(s_{B_2}, \bar{r}_{B_2}\right)\right)$$

【００７１】

として提供し、式中、

【００７２】

【数７】

$$\bar{r}_{B_1}$$

【００７３】

および

【００７４】

【数８】

$$\bar{r}_{B_2}$$

【００７５】

はアカウントB404によって提供される乱数である。一部の例では、アカウントB404は交換暗号文を:

(E'、E")=(PC(β、γ)、BGN_B(β、γ))

として提供し、式中、γはアカウントB404によって生成される乱数であり、かつ他のアカウントと共有される(例えば、為替レート(β)と共にアカウントA402に提供される)。

【００７６】

証拠集合(EX)が生成され(420)、これはプライベート為替レート(β)を検証するために使用できる。一部の実装例では、為替レートの証拠集合(EX)は:

【００７７】
【数９】

$$EX = (U, V, t'', \tilde{r}'', \hat{r}'')$$

【００７８】
として提供される。一部の例では、UおよびVはそれぞれ:
【００７９】
【数１０】

$$U = e(P_B, P_B)^{t'} e(P_B, Q_B)^{\tilde{r}'} \text{ and } V = e(P_B, P_B)^{t'} e(P_B, Q_B)^{\hat{r}'}$$

【００８０】
として計算され、式中、P_BおよびQ_BはPK_{BGN_A}に提供され、そしてt'、
【００８１】
【数１１】

$$\tilde{r}'$$

【００８２】
および
【００８３】
【数１２】

$$\hat{r}'$$

【００８４】
はアカウントB404によって生成される乱数である。一部の例では、t"、
【００８５】
【数１３】

$$\tilde{r}''$$

【００８６】
、
【００８７】
【数１４】

$$\hat{r}''$$

【００８８】
はそれぞれ:
【００８９】

【数１５】

$$t'' = t' + yt_2$$

$$\tilde{r}'' = \tilde{r}' + y\tilde{r}$$

$$\hat{r}'' = \hat{r}' + y\hat{r}$$

【００９０】
として計算され、式中、y=Hash(U、V)、ならびに
【００９１】
【数１６】

$$\tilde{r}$$

【００９２】
および
【００９３】
【数１７】

$$\hat{r}$$

【００９４】
はそれぞれ:
【００９５】
【数１８】

$$\tilde{r} = \beta t_1 + t_1\gamma + \gamma r_1 q_B \alpha_B$$

$$\hat{r} = 2t_2 + r_2 q_B \alpha_B$$

【００９６】
として計算される。一部の例では、Hashは、ブロックチェーンネットワークにおける、コンセンサスノードを含め、参加者にとって公知である任意の適切なハッシング関数(例えば、SHA-256)として提供できる。
【００９７】
一部の実装例では、アカウントB404がアカウントA402に暗号化メッセージを返信し(422)、これは以下のデータ集合例を含む:

$(X_1、Z_1、X_2、Y_2;RP_B、EX;Sig_B)$

ここで、Sig_BはアカウントB404のデジタル署名である。一部の例では、メッセージはサブチェーンチャネル(例えば、図3のサブチェーンチャネル308)を通じて送信される。
【００９８】
アカウントA402が、トランザクションが或る価値のためであり、かつアカウントA402がトランザクションを行うのに十分な資産を有するというZKPとして役立つ範囲証明(RP_A)を生成する(424)。言い換えれば、範囲証明(RP_A)は:

$t_1 \geqq 0$かつ$s_A - t_1 \geqq 0$

を証明するために使用できる。
【００９９】

アカウントA402が、額(t_1)のためのアカウントA402からアカウントB404への第1のサブトランザクションおよび額(t_2)のためのアカウントB404からアカウントCへの第2のサブトランザクションを含むサブトランザクションを生成する(426)。一部の例では、アカウントAは乱数(t'、r')を生成し、そして暗号文の集合を:

$(X', Y', Z')=(PC(t', r'), BGN_A(t', r'), BGN_B(t', r'))$

として提供する。アカウントAはデータ集合(PF)を:

$PF=(X', Y', Z'; t_1', r_1', t_2', r_2')$

として提供し、式中:

$t_1'=t'+xt_1$、$r_1'=r'+xr_2$、$t_2'=t'+xt_2$かつ$r_2'=r'+xr_2$

式中:

$x=Hash(X', Y', Z')$

【０１００】

アカウントA402は第1および第2のサブトランザクションをそれぞれ:

A、B:X_1、Y_1、Z_1

B、C:X_2、Y_2、Z_2

として提供し、ここで、Aはアカウント A402の識別子であり、Bはアカウント B404の識別子であり、そしてCはアカウントCの識別子である(例えば、識別子はブロックチェーンネットワーク内のそれぞれのアドレスとして提供される)。トランザクションが提供されるが、これは第1および第2のサブトランザクション、範囲証明および支持証拠集合を含む。例えば、トランザクションは:

A、B:X_1、Y_1、Z_1;B、C:X_2、Y_2、Z_2;RP_A、PF;RP_B、EX

として提供される。トランザクションはアカウントA402によってデジタル署名され(428)、かつアカウントA402の署名(Sig_A)もアカウントB404の署名(Sig_B)も含む。アカウントA402がコンセンサスノード406に署名済みトランザクションを提出する(430)。署名済みトランザクションは:

(A、B:X_1、Y_1、Z_1;B、C:X_2、Y_2、Z_2;RP_A、PF;RP_B、EX;Sig_A、Sig_B)

として提供される。

【０１０１】

コンセンサスノード406がアカウントA402のおよびアカウントB404の署名を検証する(432)。署名が検証されなければ、トランザクションは終了し、そしてアカウントA402にエラーメッセージを提供できる。署名が検証されれば、範囲証明(RP_A)および範囲証明(RP_B)がコンセンサスノード406によって検証される(434)。範囲証明がZKPであるので、各々が、基礎となる平文データを明かすことなく真として証明できる、または偽を返せる。範囲証明が検証されなければ、トランザクションは終了し、そしてアカウントA402にエラーメッセージを提供できる。範囲証明が検証されれば、トランザクション額がゼロより大きく、かつアカウントA402もアカウントB404もトランザクションを行うのに十分な資産をそれぞれの通貨で有すると判定される。

【０１０２】

一部の実装例では、コンセンサスノード406が、データ集合(PF)および証拠集合(EX)における証拠を使用することによって、トランザクションを検証する(436)。一部の例では、コンセンサスノード406は、以下の関係が真であるかどうかを検証する:

$PC(t_1', r_1')=X'+xX_1$

$BGN_A(t_1', r_1')=Y'+xY_1$

$BGN_B(t_1', r_1')=Z'+xZ_1$

$PC(t_2', r_2')=X'+xX_2$

$BGN_B(t_2', r_2')=Y'+xY_2$

$BGN_C(t_2', r_2')=Z'+xZ_2$

式中、$x=Hash(X', Y', Z')$。上記の関係が真であれば、暗号文(BGN暗号文)が適切な公開鍵で暗号化されており、そしてトランザクションの額が正しいことが確認される。

【０１０３】

トランザクションが公開された(但し暗号化された)為替レートで行われることも検証される。例えば、コンセンサスノード406は、データ集合(EX)における証拠を使用することによって為替レートを検証する。一部の例では、コンセンサスノード406はy=Hash(U、V)を計算し、そしてyを使用して、以下の関係が真であるかどうかを検証する:

【０１０４】

【数１９】

$$e(P_B,P_B)^{t''}e(P_B,Q_B)^{\tilde{r}''}=U*e(E_2,Z_1)^{y}$$

$$e(P_B,P_B)^{t''}e(P_B,Q_B)^{\hat{r}''}=V*e(BGN_B(1,1),Y_2)^{y}$$

【０１０５】

関係が真でなければ、トランザクションおよび/または為替レートは検証されず、トランザクションは終了し、そしてアカウントA402にエラーメッセージを提供できる。関係が真であれば、コンセンサスノード406がコンソーシアムブロックチェーンネットワークにトランザクションを記録し(438)、そしてアカウントA402、アカウントB404およびアカウントCのアカウント残高が更新される。例えば、アカウントA402の残高(s_A)が額(t_1)だけ減少され、アカウントB404の残高

【０１０６】

【数２０】

$$(s_{B_1})$$

【０１０７】

が額(t_1)だけ増加され、アカウントB404の残高

【０１０８】

【数２１】

$$(s_{B_2})$$

【０１０９】

が額(t_2)だけ減少され、そしてアカウントCの残高が額(t_2)だけ増加される。

【０１１０】

図5は、本明細書の実装例に従って実行できるプロセス500の一例を描く。一部の実装例では、プロセス例500は、1つまたは複数のコンピューティングデバイスを使用して実行される1つまたは複数のコンピュータ実行可能プログラムを使用して行われてよい。一部の例では、プロセス例500は、コンソーシアムブロックチェーンネットワークのノードによって行われて、ブロックチェーンネットワーク内で資産間トランザクションを行える。

【０１１１】

為替レートが受信される(502)。例えば、ブロックチェーンネットワークの第1の参加者と関連する第1のノード(例えばブロックチェーンネットワークのノード)によって、ブロックチェーンネットワークの第2の参加者と関連する第2のノード(例えばブロックチェーンネットワークのノード)から、為替レートが受信される。一部の例では、為替レートはサブチェーンチャネルを通じて受信される。一部の例では、為替レートは第2の参加者のプライベート為替レートである。一部の実装例では、第2の参加者は金融機関である。一部の実装例では、為替レートは、第2の参加者が第1の種類の通貨を第2の種類の通貨と交

換するレートを指定する。例えば、為替レートは、第2の参加者がUSDをRMBと交換することになるレートを指定してよい。

【０１１２】

第1の乱数および第2の乱数が第1のノードによって生成される(504)。第1の額および第2の額が、それぞれ、第1の乱数および第2の乱数を使用して、それぞれ、第1の暗号文の集合および第2の暗号文の集合内に暗号化される(506)。一部の例では、第1の額は、第1の参加者によって交換のために参加者メンバーに移転されることになる第1の資産種類の額である。一部の例では、第2の額は、第1の額と交換されることになる第2の資産種類の額である。一部の例では、第2の額は、第2の参加者の為替レートが乗算された第1の額の積に等しい。

【０１１３】

一部の例では、第1の暗号文の集合は、第1の額および第1の乱数の乱数コミットメントならびに第1の額および第1の乱数の2つの準同型暗号を含む。一部の例では、第2の暗号文の集合は、第2の額および第2の乱数の乱数コミットメントならびに第2の額および第2の乱数の2つの準同型暗号を含む。一部の例では、第1の暗号文の集合は、第1の額および第1の乱数のPCならびに、それぞれ、第1の参加者のBGN公開鍵および第2の参加者のBGN公開鍵を使用する、第1の額および第1の乱数のBGN暗号を含む。一部の例では、第2の暗号文の集合は、第2の額および第2の乱数のPCならびに、それぞれ、第2の参加者のBGN公開鍵および第3の参加者のBGN公開鍵を使用する、第2の額および第2の乱数のBGN暗号を含む。

【０１１４】

第1の額、第1の乱数、第2の乱数、ならびに第1の暗号文の集合の少なくとも一部分(部分集合)および第2の暗号文の集合の少なくとも一部分(部分集合)が第1のノードから第2のノードに送信される(508)。一部の実装例では、第1の額、第1の乱数、第2の乱数、第1の暗号文の集合の少なくとも一部分および第2の暗号文の集合の少なくとも一部分がサブチェーンチャネルを通じて送信される。

【０１１５】

第1の範囲証明、為替レートの証拠集合、および第1の署名が受信される(510)。一部の実装例では、第1の範囲証明、為替レートの証拠集合、および第1の署名は、第1のノードによってサブチェーンチャネルを通じて第2のノードから受信される。一部の例では、第1のデジタル署名は非対称暗号化方式に基づく第2の参加者のデジタル署名である。一部の例では、第1の範囲証明は、第2のメンバーと関連するアカウントが第1の額を第2の額と交換するのに十分な、第2の額と同じ資産種類の資産を有するという証拠を提供する。

【０１１６】

データ集合、第2の範囲証明および第2のデジタル署名が生成される(512)。一部の例では、データ集合は、資産間トランザクションの真正を少なくとも部分的に確認するためにブロックチェーンネットワーク内で使用される。一部の例では、第2のデジタル署名は非対称暗号化方式に基づく第1の参加者のデジタル署名である。一部の例では、第2の範囲証明は、第1の参加者と関連するアカウントが第2の参加者に第1の額を移転するのに十分な、第1の額と同じ資産種類の資産を有し、かつ第1の額が負でないという証拠を提供する。

【０１１７】

トランザクションが検証のためにブロックチェーンネットワークに提出される(514)。一部の実装例では、第1のノードによってブロックチェーンネットワークに提出されるトランザクションは、第1の暗号文の集合、第2の暗号文の集合、第1の範囲証明、データ集合、第2の範囲証明、為替レートの証拠集合、第1のデジタル署名および第2のデジタル署名を含む。一部の実装例では、ブロックチェーンネットワーク内の少なくとも1つのコンセンサスノードが署名および範囲証明を検証する。一部の実装例では、少なくとも1つのコンセンサスノードは、トランザクションデータ(例えば、第1の額、第2の額、為替レート)が明かされることなく、トランザクションを検証する。一部の実装例では、トランザクションの検証成功に応じて、トランザクションはブロックチェーンネットワーク内で実行される。一部の例では、第1の参加者および第2の参加者のアカウントはブロックチェー

ン上で更新されて交換資産を反映する。一部の例では、第3の参加者のアカウントが、第2の額の受領を反映するように更新される。

【０１１８】

図6は、本明細書の実装例に従う装置600のモジュールの一例の図である。装置600は、ブロックチェーンネットワークにおけるプライベート資産間取引に参加するように構成されるブロックチェーンノードの一実装例であることができ、ここではブロックチェーンネットワークはコンソーシアムブロックチェーンネットワークである。装置600は上記した実装例に対応でき、かつ装置600は以下を含む:

【０１１９】

生成ユニット602が、BGN暗号化を使用して、第1の値および第2の値に基づいて暗号文を生成し、第2の値が、第1の値およびブロックチェーンネットワークにおける第2のノードによって提供される為替レートに基づいて決定される。送信ユニット604が、第2のノードに第1の値および暗号文を送信する。受信ユニット606が、為替レートを明かすことなくZKPルーチンで為替レートを検証するために使用できるデータの集合を含む第1の証拠集合を受信する。生成ユニット602が、暗号文がBGN公開鍵によって暗号化されていることを、ZKPルーチンを使用して、検証するために使用できるデータの集合を含む第2の証拠集合を生成する。

【０１２０】

トランザクション定義ユニット608が、第1のノードから第2のノードへの第1の値の移転のための第1のノードと第2のノードとの間の第1のトランザクションおよび第2のノードから第3のノードへの第2の値の転送のための第2のノードと第3のノードとの間の第2のトランザクションを含むトランザクションを定義する。送信ユニット604が、トランザクションの検証および実行のためにブロックチェーンネットワークの少なくとも1つのコンセンサスノードにトランザクションを送信する。本明細書に記載されるように、トランザクションは第1の証拠集合および第2の証拠集合に基づいて検証できる。トランザクションの検証に応じて、コンセンサスノードは、第1のトランザクションおよび第2のトランザクションを実行して、第1のノードの残高を第1の値だけ減少させ、第2のノードの第1の残高を第1の値だけ増加させ、第2のノードの第2の残高を第2の値だけ減少させ、そして第3のノードの残高を第2の値だけ増加させる。

【０１２１】

任意選択の一実装例では、第1の証拠集合は、第1の値、第1のノードによって提供される一対の乱数、および暗号文に基づいて第2のノードによって提供される。

【０１２２】

任意選択の一実装例では、コンセンサスノードによってトランザクションを検証することは、第1のノードのデジタル署名および第2のノードのデジタル署名を検証することを含む。

【０１２３】

任意選択の一実装例では、コンセンサスノードによってトランザクションを検証することは、第1のノードによって提供される第1の範囲証明および第2のノードによって提供される第2の範囲証明を検証することを含む。

【０１２４】

任意選択の一実装例では、第1の範囲証明は、第1の値がゼロより大きいこと、および第1のノードの残高が第1の値以上であることを証明するZKPを含む。

【０１２５】

任意選択の一実装例では、第2の範囲証明は、第2のノードの第2の残高が第2の値以上であることを証明するZKPを含む。

【０１２６】

任意選択の一実装例では、トランザクションは、少なくとも部分的にBGN暗号化に基づいて生成される暗号文の集合を含むデータ集合をさらに含み、データ集合が、少なくとも1つのコンセンサスノードによってトランザクションを検証するために使用される。

【０１２７】
任意選択の一実装例では、受信ユニット606は、ブロックチェーンネットワークのサブチェーンチャネルを通じて第2のノードから為替レートを受信する。
【０１２８】
任意選択の一実装例では、暗号文のうちの少なくとも1つの暗号文が、PCを使用して提供される。
【０１２９】
任意選択の一実装例では、第1の証拠集合のデータの集合は第1のデータ値および第2のデータ値を含み、第1のデータ値および第2のデータ値の各々が、第2のノードのBGN公開鍵を生成するために使用されるパラメータに基づいて決定される。
【０１３０】
任意選択の一実装例では、第2の証拠集合のデータの集合は暗号文の集合および値の集合を含み、値の集合における各値が少なくとも部分的に暗号文の集合のハッシュに基づく。
【０１３１】
前述の実装例に例示されるシステム、装置、モジュールまたはユニットは、コンピュータチップもしくはエンティティを使用することによって実装できる、または或る機能を有する製品を使用することによって実装できる。典型的な実装例デバイスはコンピュータであり、コンピュータは、パーソナルコンピュータ、ラップトップコンピュータ、携帯電話、カメラ付き電話、スマートフォン、携帯情報端末、メディアプレーヤ、ナビゲーションデバイス、電子メール送受信デバイス、ゲーム機、タブレットコンピュータ、ウェアラブルデバイス、またはこれらのデバイスの任意の組合せであることができる。
【０１３２】
装置における各ユニットの機能および役割の実施プロセスについては、前述の方法における対応するステップの実施プロセスを参照できる。簡略化のために詳細はここでは省略される。
【０１３３】
装置実装例が基本的に方法実装例に対応するので、関連部分については、方法実装例における関連説明を参照できる。前述した装置実装例は単に一例である。別々の部分として記載されるユニットは物理的に別々であってもなくてもよく、そしてユニットとして表示される部分は、物理的ユニットであってもなくてもよく、1つの位置に設けられてもよく、またはいくつかのネットワークユニットに分散されてもよい。モジュールの一部または全部が、本明細書の解決策の目的を達成するように実需に基づいて選択できる。当業者は創意工夫なしに本出願の実装例を理解および実装できる。
【０１３４】
図6を再び参照すると、それは、プライベート資産間取引装置の内部機能モジュールおよび構造を例示すると解釈できる。プライベート資産間取引装置は、ブロックチェーンネットワーク内のプライベート資産間取引に参加するように構成されるブロックチェーンノードの一例であることができる。実行体は本質的に電子デバイスであることができ、そして電子デバイスは以下:1つまたは複数のプロセッサ、および1つまたは複数のプロセッサの実行可能命令を記憶するように構成されるメモリを含む。
【０１３５】
本明細書に記載される対象ならびに行為および動作の実装例は、デジタル電子回路網で、有形に具現化されたコンピュータソフトウェアもしくはファームウェアで、本明細書に開示される構造およびそれらの構造等価物を含め、コンピュータハードウェアで、またはそれらの1つもしくは複数の組合せで実装できる。本明細書に記載される対象の実装例は、1つまたは複数のコンピュータプログラム、例えば、データ処理装置による実行のために、またはその動作を制御するためにコンピュータプログラムキャリアに符号化されたコンピュータプログラム命令の1つまたは複数のモジュールとして実装できる。例えば、コンピュータプログラムキャリアには、命令が符号化または記憶された1つまたは複数のコ

ンピュータ可読記憶媒体を含むことができる。キャリアは、磁気、光磁気もしくは光ディスク、ソリッドステートドライブ、ランダムアクセスメモリ(RAM)、リードオンリメモリ(ROM)または他の種類の媒体などの有形の非一時的コンピュータ可読媒体でよい。代替的に、または加えて、キャリアは、データ処理装置による実行のために適切な受信器装置に伝送するための情報を符号化するために発生される人工発生伝搬信号、例えば、機械発生電気、光または電磁信号でよい。コンピュータ記憶媒体は、機械可読記憶デバイス、機械可読記憶基板、ランダムもしくはシリアルアクセスメモリデバイス、またはそれらの1つもしくは複数の組合せである、またはその一部であることができる。コンピュータ記憶媒体は伝搬信号でない。

【０１３６】

コンピュータプログラムは、プログラム、ソフトウェア、ソフトウェアアプリケーション、アプリ、モジュール、ソフトウェアモジュール、エンジン、スクリプトまたはコードとも称してまたは記載してよく、コンパイラ型もしくはインタープリタ型言語、または宣言型もしくは手続き型言語を含め、任意の形式のプログラミング言語で書くことができ、そしてそれは、スタンドアロンプログラムとして、あるいはモジュール、コンポーネント、エンジン、サブルーチン、または1つもしくは複数の場所にデータ通信ネットワークによって相互接続される1つもしくは複数のコンピュータを含んでよいコンピューティング環境での実行に適する他のユニットとしてを含め、任意の形式に展開できる。

【０１３７】

コンピュータプログラムは、ファイルシステムにおけるファイルに対応してよいが、しなくてもよい。コンピュータプログラムは、他のプログラムもしくはデータ、例えば、マークアップ言語文書に記憶される1つもしくは複数のスクリプトを保持するファイルの一部分に、当該プログラムに専用の単一のファイルに、または複数の連係ファイル、例えば、1つもしくは複数のモジュール、サブプログラムもしくはコードの一部分を記憶するファイルに記憶できる。

【０１３８】

コンピュータプログラムの実行のためのプロセッサには、例として、汎用および専用の両マイクロプロセッサ、ならびに任意の種類のデジタルコンピュータの任意の1つまたは複数のプロセッサを含む。一般に、プロセッサは、プロセッサに結合される非一時的コンピュータ可読媒体から実行するためのコンピュータプログラムの命令の他にデータを受けることになる。

【０１３９】

用語「データ処理装置」は、例としてプログラマブルプロセッサ、コンピュータまたはマルチプロセッサもしくはコンピュータを含め、データを処理するための全ての種類の装置、デバイスおよび機械を包含する。データ処理装置は、専用論理回路網、例えば、FPGA(フィールドプログラマブルゲートアレイ)、ASIC(特定用途向け集積回路)またはGPU(グラフィック処理装置)を含むことができる。同装置は、ハードウェアに加えて、コンピュータプログラムのための実行環境を作成するコード、例えば、プロセッサファームウェア、プロトコルスタック、データベース管理システム、オペレーティングシステム、またはそれらの1つもしくは複数の組合せを構成するコードも含むことができる。

【０１４０】

本明細書に記載されるプロセスおよび論理フローは、1つまたは複数のコンピュータプログラムを実行して、入力データを演算して出力を生成することによって動作を行う1つまたは複数のコンピュータまたはプロセッサによって行える。プロセスおよび論理フローは、専用論理回路網、例えば、FPGA、ASICもしくはGPUによって、または専用論理回路網および1つもしくは複数のプログラムされたコンピュータの組合せによっても行える。

【０１４１】

コンピュータプログラムの実行に適するコンピュータは、汎用もしくは専用マイクロプロセッサもしくは両方、または任意の他の種類の中央処理装置に基づくことができる。一般に、中央処理装置は、リードオンリメモリまたはランダムアクセスメモリまたは両方か

ら命令およびデータを受けることになる。コンピュータの要素には、命令を実行するための中央処理装置ならびに命令およびデータを記憶するための1つまたは複数のメモリデバイスを含むことができる。中央処理装置およびメモリは、専用論理回路網によって補足、またはそれに統合できる。

【０１４２】

一般に、コンピュータは、1つまたは複数の記憶デバイスも含むか、または作動的に結合されてデータを受けるもしくはデータを転送することになる。記憶デバイスは、例えば、磁気、光磁気もしくは光ディスク、ソリッドステートドライブ、または任意の他の種類の非一時的、コンピュータ可読媒体であることができる。しかしながら、コンピュータは、そのようなデバイスを有する必要はない。したがって、コンピュータは、ローカルおよび/またはリモートである、1つまたは複数のメモリなどの、1つまたは複数の記憶デバイスに結合されてよい。例えば、コンピュータは、コンピュータの不可欠な部品である1つもしくは複数のローカルメモリを含むことができる、またはコンピュータは、クラウドネットワークにある1つもしくは複数のリモートメモリに結合できる。その上、コンピュータは、別のデバイス、例えば、いくつか挙げると、移動電話、携帯情報端末(PDA)、モバイルオーディオもしくはビデオプレーヤ、ゲーム機、全地球測位システム(GPS)受信器、またはポータブル記憶デバイス、例えば、ユニバーサルシリアルバス(USB)フラッシュドライブに組み込める。

【０１４３】

部品は、直接か1つまたは複数の中間部品を介してか、互いに電気的または光学的になど通信可能に接続されることによって互い「に結合」できる。部品の一方が他方へ統合されても、部品は互い「に結合」できる。例えば、プロセッサへ統合された記憶部品(例えば、L2キャッシュ部品)はプロセッサ「に結合」されている。

【０１４４】

ユーザとの対話を提供するために、本明細書に記載される対象の実装例は、ユーザに情報を表示するためのディスプレイデバイス、例えば、LCD(液晶ディスプレイ)モニタ、ならびにユーザがコンピュータに入力を提供できる入力デバイス、例えば、キーボードおよびポインティングデバイス、例えば、マウス、トラックボールまたはタッチパッドを有するコンピュータに実装できる、またはそれと通信するように構成できる。ユーザとの対話を提供するために他の種類のデバイスも使用でき、例えば、ユーザに提供されるフィードバックは任意の形態の感覚フィードバック、例えば、視覚フィードバック、聴覚フィードバックまたは触覚フィードバックであることができ、そしてユーザからの入力は、音響、音声または触覚入力を含め、任意の形態で受け取ることができる。加えて、コンピュータは、ユーザによって使用されるデバイスに文書を送信し、それから文書を受信することによって、例えば、ユーザのデバイス上のウェブブラウザから受信される要求に応じてウェブブラウザにウェブページを送信することによって、またはユーザデバイス、例えば、スマートフォンもしくは電子タブレット上で実行するアプリと対話することによって、ユーザと対話できる。また、コンピュータは、パーソナルデバイス、例えば、メッセージングアプリケーションを実行しているスマートフォンにテキストメッセージまたは他の形式のメッセージを送信し、そして折り返しユーザから応答メッセージを受信することによって、ユーザと対話できる。

【０１４５】

本明細書は、システム、装置およびコンピュータプログラム部品に関して用語「ように構成される」を使用する。1つまたは複数のコンピュータのシステムが特定の動作または行為を行うように構成されることは、システムが自らに、動作に際してシステムに同動作または行為を行わせるソフトウェア、ファームウェア、ハードウェア、またはそれらの組合せをインストールしたことを意味する。1つまたは複数のコンピュータプログラムが特定の動作または行為を行うように構成されることは、1つまたは複数のプログラムが、データ処理装置によって実行されると、装置に同動作または行為を行わせる命令を含むことを意味する。専用論理回路網が特定の動作または行為を行うように構成されることは、回

路網が同動作または行為を行う電子論理を有することを意味する。

【０１４６】

本明細書が多くの具体的な実施詳細を含むが、これらは、請求項自体によって定められる、特許請求されるものの範囲への限定としてではなく、むしろ特定の実装例に固有であり得る特徴の記述として解釈されるべきである。別々の実装例の状況で本明細書に記載される或る特徴が、組み合わせて単一の実装例でも実現できる。反対に、単一の実装例の状況で記載される様々な特徴が、別々に複数の実装例でも、または任意の適切な下位組合せでも実現できる。その上、特徴が或る組合せで作用すると上記され、しかも当初そのように特許請求され得るが、特許請求された組合せからの1つまたは複数の特徴が一部の場合に同組合せから削除でき、請求項は下位組合せまたは下位組合せの変形とされ得る。

【０１４７】

同様に、動作が特定の順に図面に描かれかつ請求項に列挙されるが、これは、望ましい結果を達成するために、そのような動作が図示される特定の順にもしくは順番に行われること、または全ての例示された動作が行われることを必要とすると理解されるべきでない。特定の状況では、マルチタスキングおよび並列処理が有利であり得る。その上、上記した実装例における様々なシステムモジュールおよび部品の分離は、全ての実装例においてそのような分離を必要とすると理解されるべきでなく、記載されたプログラム部品およびシステムが一般に単一のソフトウェア製品に共に統合できるまたは複数のソフトウェア製品へ実装できることが理解されるべきである。

【０１４８】

本対象の特定の実装例が記載された。他の実装例は以下の請求項の範囲内である。例えば、請求項に列挙される行為は異なる順に行うことができ、それでも望ましい結果を達成できる。一例として、添付図に描かれるプロセスは、望ましい結果を達成するために、必ずしも図示される特定の順または順番を必要とするわけではない。一部の場合には、マルチタスキングおよび並列処理が有利であり得る。

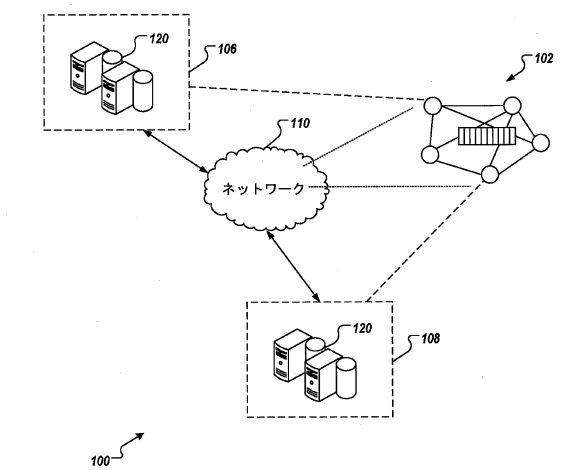
【符号の説明】

【０１４９】

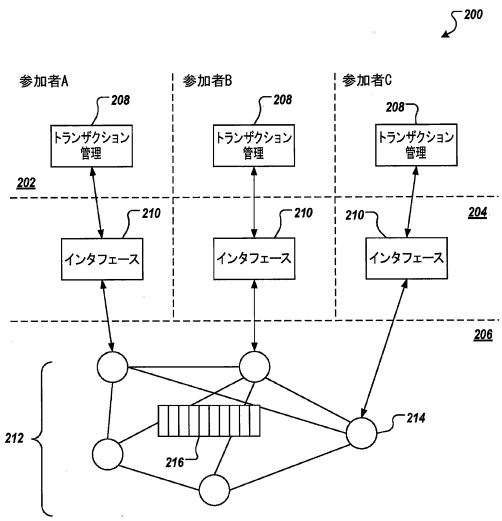
100 環境
102 コンソーシアムブロックチェーンネットワーク
106 コンピューティングデバイス
108 コンピューティングデバイス
110 ネットワーク
200 概念アーキテクチャ
202 エンティティ層
204 ホストサービス層
206 ブロックチェーンネットワーク層
208 トランザクション管理システム
210 インタフェース
212 ブロックチェーンネットワーク
214 ノード
216 ブロックチェーン
300 資産間取引プラットフォーム
302 デバイス
304 デバイス
306 デバイス
308 サブチェーンチャネル
310 ネットワーク
312 コンソーシアムブロックチェーンネットワーク
314 ノード
316 アカウントA

318　アカウントB
320　アカウントC
322　ブロックチェーン
402　アカウントA
404　アカウントB
406　コンセンサスノード
600　装置
602　生成ユニット
604　送信ユニット
606　受信ユニット
608　トランザクション定義ユニット

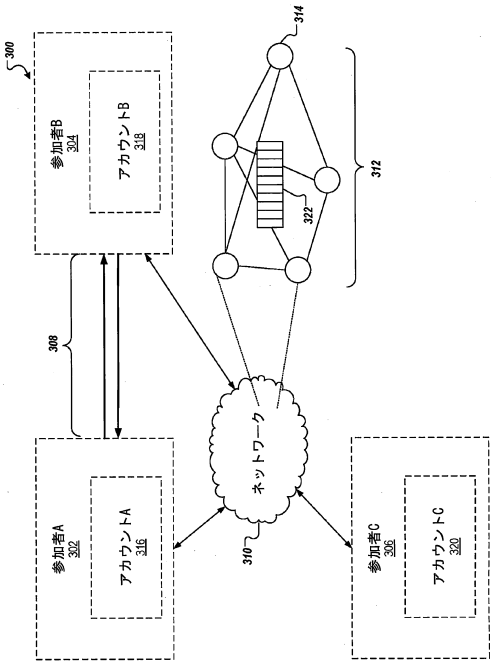
【図１】



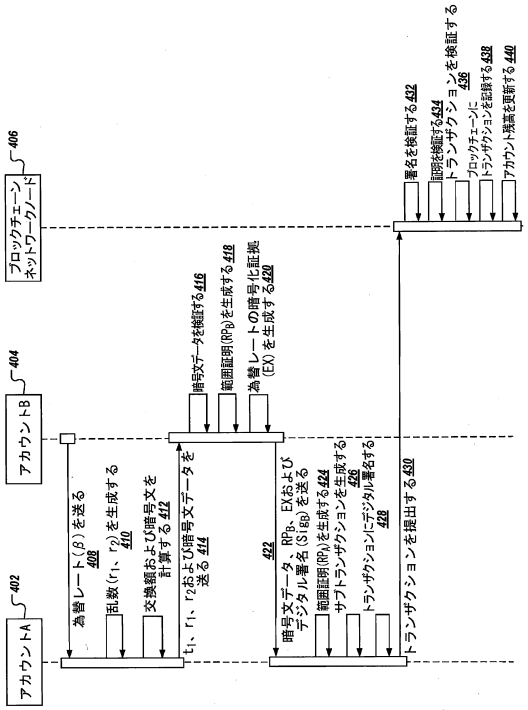
【図２】



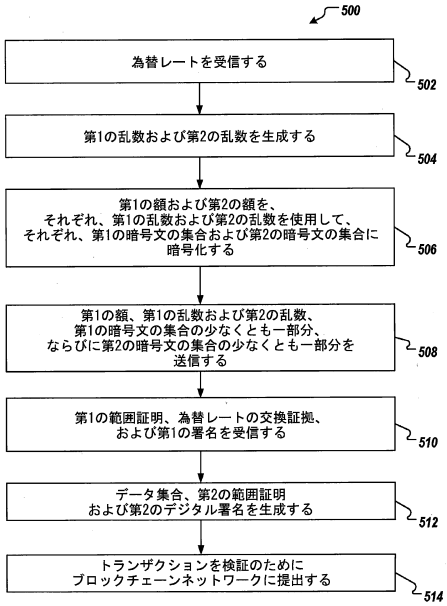
【図３】


300
参加者B
304
アカウントB
318
314
312
322
308
ネットワーク
310
参加者A
302
アカウントA
316
参加者C
306
アカウントC
320

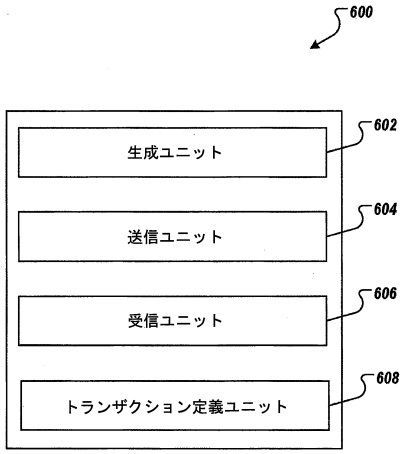
【図４】


406
ブロックチェーン
ネットワークノード
404
アカウントB
402
アカウントA
為替レート(β)を送る
408
乱数(r1、r2)を生成する
410
交換額および暗号文を
計算する412
t1、r1、r2および暗号文データを
送る414
暗号データを検証する416
範囲証明(RPB)を生成する418
為替レートの暗号化証拠
(EX)を生成する420
422
暗号文データ、RPB、EXおよび
デジタル署名(SIGB)を送る
範囲証明(RPA)を生成する424
サブトランザクションを生成する
426
トランザクションにデジタル署名する
428
トランザクションを提出する430
署名を検証する432
証明を検証する434
トランザクションを検証する
436
ブロックチェーンに
トランザクションを記録する438
アカウント残高を更新する440

【図５】


500
為替レートを受信する
502
第1の乱数および第2の乱数を生成する
504
第1の額および第2の額を、
それぞれ、第1の乱数および第2の乱数を使用して、
それぞれ、第1の暗号文の集合および第2の暗号文の集合に
暗号化する
506
第1の額、第1の乱数および第2の乱数、
第1の暗号文の集合の少なくとも一部分、
ならびに第2の暗号文の集合の少なくとも一部分を
送信する
508
第1の範囲証明、為替レートの交換証拠、
および第1の署名を受信する
510
データ集合、第2の範囲証明
および第2のデジタル署名を生成する
512
トランザクションを検証のために
ブロックチェーンネットワークに提出する
514

【図６】


600
生成ユニット
602
送信ユニット
604
受信ユニット
606
トランザクション定義ユニット
608

フロントページの続き

(72)発明者　ウェンビン・ジャン
中華人民共和国・３１１１２１・ゼジャン・ハンジョウ・ユ・ハン・ディストリクト・ウェスト・ウェン・イ・ロード・ナンバー・９６９・ビルディング・３・５／エフ・アリババ・グループ・リーガル・デパートメント
(72)発明者　ハオ・レイ
中華人民共和国・３１１１２１・ゼジャン・ハンジョウ・ユ・ハン・ディストリクト・ウェスト・ウェン・イ・ロード・ナンバー・９６９・ビルディング・３・５／エフ・アリババ・グループ・リーガル・デパートメント
(72)発明者　リチュン・リ
中華人民共和国・３１１１２１・ゼジャン・ハンジョウ・ユ・ハン・ディストリクト・ウェスト・ウェン・イ・ロード・ナンバー・９６９・ビルディング・３・５／エフ・アリババ・グループ・リーガル・デパートメント
(72)発明者　チャンジエ・フアン
中華人民共和国・３１１１２１・ゼジャン・ハンジョウ・ユ・ハン・ディストリクト・ウェスト・ウェン・イ・ロード・ナンバー・９６９・ビルディング・３・５／エフ・アリババ・グループ・リーガル・デパートメント

審査官　行田　悦資

(56)参考文献　中国特許出願公開第１０８３３５１０６（ＣＮ，Ａ）
特開２０１７－０７６８３９（ＪＰ，Ａ）
国際公開第２０１７／１７１７２６（ＷＯ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０６Ｑ　２０／３８