(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7221546号
(P7221546)

(45)発行日　令和5年2月14日(2023.2.14)

(24)登録日　令和5年2月6日(2023.2.6)

(51)国際特許分類

Ｇ０６Ｆ　21/62　(2013.01)		Ｇ０６Ｆ	21/62	３４５
Ｇ０６Ｑ　40/02　(2023.01)		Ｇ０６Ｑ	40/02	

ＦＩ

請求項の数　15　（全25頁）

(21)出願番号　特願2020-518690(P2020-518690)
(86)(22)出願日　平成30年9月27日(2018.9.27)
(65)公表番号　特表2020-536322(P2020-536322A)
(43)公表日　令和2年12月10日(2020.12.10)
(86)国際出願番号　PCT/US2018/053242
(87)国際公開番号　WO2019/067800
(87)国際公開日　平成31年4月4日(2019.4.4)
審査請求日　令和3年9月22日(2021.9.22)
(31)優先権主張番号　62/585,943
(32)優先日　平成29年11月14日(2017.11.14)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　62/571,556
(32)優先日　平成29年10月12日(2017.10.12)
最終頁に続く

(73)特許権者　520106736
レヴァレジ ロック リミテッド ライアビリティ カンパニー
ＬＥＶＥＲＡＧＥ ＲＯＣＫ ＬＬＣ
アメリカ合衆国 ニューメキシコ州 ８７１１４ アルバカーキ，ブライアン ノースウェスト ４１０９
(74)代理人　110001302
特許業務法人北青山インターナショナル
(72)発明者　アンダーソン，トーマス，ジー．
アメリカ合衆国 ニューメキシコ州 ８７１１４ アルバカーキ，ブライアン ノースウェスト ４１０９
審査官　宮司 卓佳
最終頁に続く

(54)【発明の名称】　公開分散台帳システムにおける取引プライバシー

(57)【特許請求の範囲】

【請求項１】

分散台帳を実装する複数のコンピュータの分散ネットワークを用いて、第三者機関を介して資産譲渡人から受取人への資産の移転を実行する匿名であるが追跡可能な一次取引を実行する方法であって、

（ａ）前記資産譲渡人の属性を判定可能にする、前記資産譲渡人に関する情報を前記第三者機関のコンピュータによって記録するステップと、

（ｂ）前記コンピュータの分散ネットワークによって、前記資産譲渡人からの前記第三者機関への前記資産の移転を前記分散台帳に記録し、前記移転が前記分散台帳に記録されていることを確認するステップと、

（ｃ）前記第三者機関のコンピュータによって、前記資産譲渡人から前記第三者機関へ前記受取人の識別情報を取り次ぎ、前記取り次ぎが前記分散台帳に記録されないようにするステップと、

（ｄ）前記第三者機関のコンピュータによって、各々が前記受取人及び二次資産譲渡機関並びに資産部分を含む複数の二次取引を設定し、資産部分の組み合わせが前記資産に対応し、且つ前記二次資産譲渡機関の少なくとも一部が前記資産譲渡人以外の関係者を示しているステップと、

（ｅ）前記コンピュータの分散ネットワークによって、前記複数の二次取引を分散台帳に記録するステップを含み、

前記複数の二次取引の二次資産譲渡機関が、前記分散台帳に記録されて、前記分散台帳の

ウォレットにより特定されるものであることを特徴とする方法。
【請求項２】
請求項１に記載の方法において、前記複数の二次取引の個数が所定の方法により判定され、少なくとも所定の下限に等しいことを特徴とする方法。
【請求項３】
請求項２に記載の方法において、前記複数の二次取引の個数が所定の上限を超えない乱数であることを特徴とする方法。
【請求項４】
請求項１に記載の方法において、前記第三者機関が前記分散台帳の複数のウォレットを制御し、複数の前記二次資産譲渡機関の少なくとも１つが、複数の前記二次資産譲渡機関の少なくとも他の１つとは異なるウォレットに紐付けられていることを特徴とする方法。
【請求項５】
請求項１に記載の方法において、前記複数の二次取引を記録するステップが、複数の時点で前記複数の二次取引を記録するステップを含んでいることを特徴とする方法。
【請求項６】
請求項５に記載の方法において、前記複数の時点のうち少なくとも二つの時点が、所定の方法により決定され且つ所定の下限を下回らない時間間隔を空けられていることを特徴とする方法。
【請求項７】
請求項５に記載の方法において、前記複数の時点のうち少なくとも二つの時点が、所定の方法により決定され且つ所定の上限を超えない時間間隔を空けられていることを特徴とする方法。
【請求項８】
請求項１に記載の方法において、前記第三者機関が複数の一次取引を指定する通知を受信し、前記複数の一次取引の少なくとも１個が前記資産譲渡人からであり、少なくとも１個が前記資産譲渡人以外の関係者からであり、及び全部が前記受取人宛であり、前記第三者機関が前記複数の一次取引を前記受取人に紐付けて、前記紐付けられた取引が本方法の残りにおいて前記一次取引として扱われることを特徴とする方法。
【請求項９】
請求項８に記載の方法において、前記複数の二次取引の個数が所定の方法により判定され、且つ少なくとも所定の下限に等しいことを特徴とする方法。
【請求項１０】
請求項９に記載の方法において、前記複数の二次取引の個数が所定の方法により判定され、且つ所定の上限を超えないことを特徴とする方法。
【請求項１１】
請求項１に記載の方法において、前記第三者機関が前記分散台帳の複数のウォレットを制御し、複数の前記二次資産譲渡機関の少なくとも１つが複数の前記二次資産譲渡機関の少なくとも他の１つとは異なるウォレットに紐付けられていることを特徴とする方法。
【請求項１２】
請求項１に記載の方法において、前記複数の二次取引を記録するステップが、複数の時点で前記複数の二次取引を記録するステップを含んでいることを特徴とする方法。
【請求項１３】
請求項１２に記載の方法において、前記複数の時点のうち少なくとも二つの時点が、所定の方法により決定され且つ所定の下限を下回らない時間間隔を空けられていることを特徴とする方法。
【請求項１４】
請求項１２に記載の方法において、前記複数の時点のうち少なくとも二つの時点が、所定の方法により決定され且つ所定の上限を超えない時間間隔を空けられていることを特徴とする方法。
【請求項１５】

請求項１に記載の方法において、前記資産譲渡人と前記受取人が同一の主体であることを特徴とする方法。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
本出願は、２０１８年９月２７日出願のＰＣＴ出願第ＰＣＴ／ＵＳ２０１８／０５３２４２号の米国特許法第３７１条に基づく国内段階出願であり、以下の米国仮特許出願、すなわち２０１７年９月２９日出願の第６２／５６５，０９９号、２０１７年１０月１２日出願の第６２／５７１，５５６号、２０１７年１１月１４日出願の第６２／５８５，９４３号、及び２０１８年３月１９日出願の第６２／６４４，８４１号の優先権を主張するものであり、各々を本明細書に引用している。
【０００２】
本出願は、分散台帳システムの分野に関し、より具体的には公開されてアクセス可能な分散台帳における取引プライバシーの保護に関する。
【背景技術】
【０００３】
暗号通貨及び他の類似概念の実装に利用可能な各種の信用できないブロックチェーンが存在する。このようなブロックチェーンの背後にある仮定、特に信用できる主体が存在しないという仮定により、そのようなブロックチェーンが即時取引、プライバシー保護、安定した暗号通貨、及び詐欺、盗難、及び紛失の防止の実行が制約される。本発明は、このような望ましい特徴を促進すべく既存のブロックチェーンで使用できる機構を提供する。
【発明の概要】
【０００４】
本発明のいくつかの実施形態は、分散台帳（「分散台帳」はハッシュグラフ、ブロックチェーン等を含む）を実装する複数のコンピュータの分散ネットワークを用いて、第三者機関を介して資産譲渡人から受取人への資産の移転を実行する匿名であるが追跡可能な一次取引を実行する方法を提供するものであり、本方法は（ａ）資産譲渡人の属性（「属性」は、名前、住所、政府識別番号等の直接識別情報、又は特定のユーザーに紐付け可能なウォレットの識別情報、或いは後で識別が可能なゼロ知識証明等の機構であってよい）を判定可能にする、資産譲渡人に関する情報を第三者機関側で記録（「第三者機関側での記録」は、後で必要に応じてＲＯＭ、フラッシュメモリ、光ディスク、磁気ディスクその他の読み出し可能な持続的メモリへの保存を意味する）するステップと、（ｂ）資産譲渡人からの第三者機関への資産の移転を分散台帳に記録し（「分散台帳への記録」は、使用する特定の実装方式に応じて様々な機構を含んでいてよく、一般に取引の暗号認証と合わせて分散台帳を実装する複数のコンピュータのネットワークへの取引の送付を含み、当該取引が、不変であることが分かっているブロックに達するまで分散台帳を観察し、「資産の移転」が一次取引に必要な資産だけであっても、又は当該資産及び他の資産、例えば一部を一次取引に使用し、残りは他の取引要求を満たすべく第三者機関に残されている高額の資金を含んでいてよい）、前記送金が分散台帳に記録されていることを確認するステップと、（ｃ）資産譲渡人から第三者機関へ受取人の識別情報を取り次ぎ（第三者機関が資産譲渡人の単一の、分割不可能な資産だけを保持している場合、資産譲渡人からの要求は受取人を指定するだけでよいが、受取人が複数の資産、又は通貨等の分割可能な資産を保持する場合、資産譲渡人からの要求は送金される資産の特定の一部の資産を指定することもできる）、前記取り次ぎが分散台帳に記録されないようにするステップと、（ｄ）各々が受取人及び二次資産譲渡人並びに資産部分を含む複数の二次取引を設定し、資産部分の組み合わせは当該資産に対応し、（「資産に対応する」は資産部分の組み合わせが資産の移転要件を満たすことを意味しており、簡単な通貨送金の場合、単に当該部分の合計が要求金額に等しい対応であってよく、ある状況では単純合計以外に対応していてよい、例えば取引手数料、記録手数料、交換手数料、割引、保留等を賄うものであってよい）、且つ当

該二次資産譲渡人の少なくとも一部が資産譲渡人以外の関係者を示しているステップと、（ｅ）複数の二次取引を分散台帳に記録するステップとを含んでいる。

【０００５】

いくつかの実施形態においては、複数の二次取引の個数は、少なくとも所定の下限に等しい所定の方法（「所定の方法」は無作為に数を選択するステップ、例えば資産価値の大きさ、資産譲渡人の属性又は居所、受取人の属性又は居所、第三者機関の属性、送金時刻、受取人の取引履歴、資産譲渡人の取引履歴等の要因に応答するアルゴリズム的な方法により数を選択するステップを含んでいてよい）により決定される。一般に、二次取引が多いほど一次取引の再構築が困難になり、例えば、一次取引を２個の二次取引に分割すれば一次取引が不明瞭になり、５個に分割すればより不明瞭に、１０又は１００個に分割すればまたさらに不明瞭になる。しかし、二次取引が多いということは、取引の送付及び記録により多くのオーバーヘッドが生じることを意味する。

【０００６】

いくつかの実施形態において、複数の二次取引の個数は、所定の上限を超えない乱数である。二次取引の個数の上限はオーバーヘッドを減少させることができ、例えば各二次取引に記録手数料が課される場合、二次取引の個数が一次取引の大きさに対して大き過ぎれば記録手数料が抑制的になる場合がある。

【０００７】

いくつかの実施形態において、第三者機関は分散台帳上で複数のウォレットを制御し、複数の二次資産譲渡人のうちの少なくとも１名が複数の二次資産譲渡人の少なくとも他の１名とは異なるウォレットに紐付けられている。

【０００８】

いくつかの実施形態において、複数の二次取引を記録するステップは、複数の時点で複数の二次取引を記録するステップを含んでいる。一次取引の特性とサイズ、及び取引を秘匿したい願望と至急に行いたい願望とのバランスに応じて二次取引の記録は数分、数日、又はより長い時間にわたる場合がある。

【０００９】

いくつかの実施形態において、複数の時点のうち少なくとも二つの時点が所定の方法により決定され且つ所定の下限を下回らない時間間隔を空けられている。間隔が長いほど一次取引の再構築が困難になるため、いくつかの状況において少なくとも１分、３０分、１日、又はより長い間隔が空けられていることが有用な場合がある。

【００１０】

いくつかの実施形態において、複数の時点のうち少なくとも二つの時点が所定の方法により決定され且つ所定の上限を超えない時間間隔を空けられている。上限は、全ての二次取引を記録することにより一次取引が終了する時点を関係者に知らせるのに役立ち、他の取引により二次取引同士の関係が不明瞭になるのに充分な時間を与える一方で、即時性に対するニーズが満たされることを保証すべく選択されていてよい。

【００１１】

いくつかの実施形態において、第三者機関は複数の一次取引を指定する通知を受信し、当該複数の一次取引の少なくとも１個が資産譲渡人からであり、少なくとも１個が資産譲渡人以外の関係者からであり、及び全部が受取人宛であり、第三者機関は複数の一次取引を受取人に紐付け、紐付けられた取引は本方法の残りの部分では一次取引として扱われる。

【００１２】

いくつかの実施形態において、複数の二次取引の個数が所定の方法により判定され、且つ少なくとも所定の下限に等しい。

【００１３】

いくつかの実施形態において、複数の二次取引の個数が所定の方法により判定され、所定の上限を超えない。

【００１４】

いくつかの実施形態において、第三者機関は分散台帳の複数のウォレットを制御し、複

数の二次資産譲渡人の少なくとも１名が当該複数の二次資産譲渡人の少なくとも他の１名とは異なるウォレットに紐付けられている。

【００１５】

いくつかの実施形態において、複数の二次取引を記録するステップは、複数の時点で複数の二次取引を記録するステップを含んでいる。

【００１６】

いくつかの実施形態において、複数の時点のうち少なくとも二つの時点は、所定の方法により決定され且つ所定の下限を下回らない時間間隔を空けられている。

【００１７】

いくつかの実施形態において、複数の時点のうち少なくとも二つの時点は、所定の方法により決定され且つ所定の上限を超えない時間間隔を空けられている。

【００１８】

いくつかの実施形態において、資産譲渡人と受取人は同一の主体である。これは一例として、ウォレットの所有者が識別された（例えばウォレットの所有者を識別可能にするパターンの取引のマイニングにより）た後で資産の所有権を不明瞭にするのに有用な場合がある。所有者は、露呈したウォレットから資産を同一人物が所有する別のウォレットに移転する一次取引を開始することができ、請求項に記載の方法は、所有された新規ウォレットが当該資産を有していることを他者が判定し難くすることができる。

【００１９】

本発明のいくつかの実施形態は、分散台帳を実装する複数のコンピュータの分散ネットワークを用いて、第三者機関を介して資産譲渡人から受取人への匿名であるが追跡可能な取引を実行する方法を提供するものであり、本方法は（ｂ）資産譲渡人による認証及び第三者機関による認証（例えば連署者又は保証人、子供の取引を承認する大人、政府又は規制による承認等）を要する資産の移転を分散台帳に記録するステップと、（ｃ）資産譲渡人の資産に対する制御を確認する確認情報を資産譲渡人から第三者機関へ取り次ぐステップと、（ｄ）第三者機関側で前記確認情報を確認するステップと、（ｅ）分散台帳に移転の承認を記録するステップとを含んでいる。

【００２０】

いくつかの実施形態において、承認が所定時間内に記録されなかった場合、分散台帳に記録された移転が無効になる。

【００２１】

いくつかの実施形態において、資産譲渡人は、分散台帳に承認が記録される前に、分散台帳に記録された移転を無効にすることができる。

【図面の簡単な説明】

【００２２】

【図１】図１は、本発明の実施形態による即時ノートネットワークの一例である。

【発明を実施するための形態】

【００２３】

産業上の利用可能性及び本発明を実施するモード

以下の説明において時折、複数の態様が「本質的である」又は「最も重要である」或いは「含まなければならない」などとしているが、これらの表現は読者の注意を喚起すべく態様を強調することを意図するものであって、本発明がこれらの態様を含む実施形態に限定されることを意味しない。以下の説明はまた、１個以上の例示的な実施形態を記述している。可変と記述されたパラメータを設定する、又は異なるイベント又は時点で変更することが可能な、及びいくつかの実施形態の例で固定されていると記述されたパラメータを変更することが可能な実施形態の例を含む、様々な代替的実施形態が考えられる。本発明の実施形態を、ブロックチェーンシステムの一例に紐付けて記述しており、本発明を他のブロックチェーンシステムを含む他の分散台帳で用いることができる。いくつかの実施形態は、信用できる第三者機関すなわちＴ３Ｐを考察する。基礎となる分散台帳の特定の実施形態及び特性に応じて、Ｔ３Ｐは分散台帳の所管当局又は組織からの特別な認可又はこ

れらとの関係、又は分散台帳により実行されるプロトコルに関する特別な権利を必要とする場合がある。当業者には、考慮する特定の分散台帳に対して当該実施形態を実行するために必要とされる特別な権利、認可、又は関係が理解されよう。

【００２４】

以下の記述でいくつかの商標を用いて、ＥＲＣ２０、イーサリアム、及びリップル等、他者から提供される製品及びサービスに言及する。このような商標の所有者はそのような商標の全ての権利を保持する。

【００２５】

本発明は、様々なブロックチェーンシステムに有用である。簡潔のため、以下の記述において、以下の米国仮特許出願、すなわち２０１７年９月２９日出願の第６２／５６５，０９９号、２０１７年１０月１２日出願の第６２／５７１，５５６号、２０１７年１１月１４日出願の第６２／５８５，９４３号、及び２０１７年３月１９日出願の第６２／６４４，８４１号に記述されているブロックチェーンシステムを仮定し、各々を本明細書に引用している。当業者には、実施に際しての変型及び以下に示す複数の例が他のブロックチェーンシステムを含むことが理解されよう。

【００２６】

本発明は、信用できる主体と信用できないブロックチェーンとの統合を通じて様々な能力を提供する。信用できないブロックチェーン自体は信用できる主体を信用する必要がなく、且つ信用できる主体が信用できないブロックチェーンの全てのユーザーに信用されなくてもよい点に注意されたい。むしろ、信用できる主体を信用することで満足する、又は信用せざるを得ないユーザーが、信用できる主体を利用することで、全く信用できないブロックチェーンでは不可能な特定の利益を享受できる。

【００２７】

本発明の特定の実施形態は、信用できる主体が運用する信用ベースのネットワークを利用する。当該ネットワークは、本明細書において即時ノードネットワーク、又はＩＮＮと称され、図１に示す。当該ネットワークは基礎となる分散台帳に構築されている。当該ネットワークは、１秒未満で確認可能な即時取引を可能にする。また、詐欺及び盗難防止、紛失防止、暗号通貨の安定したバージョン、及び匿名取引等の多くの追加的な機能を可能にする。ＩＮＮの利用に関する詳細、及び本発明の実施形態に本来紐付けられている機能について以下の様々な段落で述べる。ＩＮＮは、後述する保護通貨と呼ばれるブロックチェーンの暗号通貨の二次的形式を利用する。保護通貨ウォレット及び保護通貨取引は、自身に紐付けられ、且つＩＮＮの任意選択的特徴を可能にするＴ３Ｐにより匿名で保持された公知の属性を有している。

【００２８】

ウォレット

ウォレットは、秘密及び公開鍵のペアを含んでおり、主要通貨の所有権を示す。ウォレットは、主要通貨を用いるシステムのアカウントに自動的に追加することができる。個人が自身のウォレットを作成するためのコードも利用できる。

【００２９】

保護された後述の２種類のウォレット、すなわち標準主要通貨ウォレット及び保護通貨ウォレットがある。システムＡＰＩは他の暗号通貨用のラップ口座も含んでいる。これらのラップ口座は、システムと他のブロックチェーンとの相互運用のインターフェースを生成する。

【００３０】

バリデータのインセンティブ

バリデータは、コンセンサス維持に対する報酬である。バリデータの報酬は、サーバを運用する業務に相応しているが、新たな主要通貨発行の全てではないが大部分はシステムを取り巻くコミュニティへのインセンティブとして有用である。バリデータが主要通貨準備高から、又は法定通貨から支払われることが期待される。

【００３１】

バリデータの報酬は、コンセンサスの維持だけに基づいていて、主要通貨がインセンティブの一部である場合にブロックペア毎に授与される。ブロック報酬は、どのバリデータが実際にブロックを提案及び生成しているかには影響されない。報酬計算量は、以下でＧＯＶと称する所管当局又は組織により連続的に調整することができる。稼働中のバリデータは、誰がブロックを提案したかに依らずブロック報酬の分け前を得る。

【００３２】

スマート契約及びスマートコイン

スマート契約は、中核プロトコル自体の一部として、又は追加的な機能を提供するスマートコインの形式で実行することができる。ブロックチェーン全体の価値を生み出す中核機能はプロトコル自体に実装されている。例えば、利用可能なスマートコインの種類の定義、及びそれらの処理の仕方はプロトコルの一部である。保護通貨に紐付けられた機能（支払取消及び盗難又は紛失の回復等）、融資機能、及び即時性の実装（保護通貨割当量）もまたプロトコルの一部である。プロトコルはより一般的な機能のためにスマートコインを利用する。

【００３３】

スマートコインは、プロトコルの重要な側面である。スマートコインはチェーン内処理及び動作の実装方式であると共に、主要通貨自体以外の他の種類の所有権及び属性を表す。

【００３４】

スマートコインと共に維持される多くの所有権及び運用形態があり、これらの形態又は運用のいずれもがウォレットに紐付けられている。これらのスマートコインは、主要通貨がウォレットに保持されているのと同様の仕方でウォレットに保持し、主要通貨がブロックチェーン上で送金されるのと同様の仕方で送金することができる。スマートコインは、ＩＮＮにより（例えば、新たなバリデータが追加されたときに）、又はブロックチェーンによりアルゴリズム的に（例えば、新規ウォレットに対して所有権がマルチティアブロックチェーン方式で生成されたときに）により、又はシステムのユーザーから発行することができる。スマートコインは、スマートコイン要素のグループを組み合わせて、より洗練された振る舞いを生じさせるコンポジションベースのプログラム原則を利用する。スマートコインの複数の例を以下に挙げる。

【００３５】

スマートコインは自身の送金ルールを有していてよい。例えば、ＩＮＮはあるアカウントから別のアカウントへバリデータスマートコインを送金することができる。ＩＮＮはまた、ステータススマートコイン、ＩＤスマートコイン、又は投票スマートコインをウォレットに送金できるが、それらをウォレットから送金することはできない。ウォレットスマートコインは、Ｔ１ブロックチェーンによってのみ送金することができる。スマートコインはまた、スペースを節約すべくブロックチェーン状態から除外（自身のハッシュ表現だけをマークル木に残して）される際に準拠するルール、スマートコインが保護通貨ウォレットから送金された際に戻入に適しているか等の特別な特性、又は特化した機能に求められる他の特性を有していてもよい。スマートコインは、代替可能又は代替不可能なデジタル資産を表していても、又は単に送金又は所有権機構の一部として用いられてよい。

【００３６】

暗号通貨クラス

ネットワークへのスマートコインの追加と同様に、主要通貨自体とは別に他の代替可能な価値の表現があり得る。暗号通貨の別々のクラスは、ブロックチェーン内で維持することができる。一例として、単にネットワーク上で維持されているが、別の種類の価値又は所有権を表す別の暗号通貨がある。これは、ＥＲＣ２０コインをイーサリアムネットワークで用いるのと同様の仕方で貴重であり得る。当該例示的システムは、他のシステムと組み合わせて、ブロックチェーンに含まれていてその技術を用いて確認される他の種類の暗号通貨を持たせることができる。

【００３７】

保護通貨

例示的システムは、送金を保護を強めることができる保護通貨と呼ばれる特定の、第２の種類の暗号通貨を利用することができる。保護通貨はシステムの完全に任意選択的な特徴であるため、ユーザーは保護通貨の形式で取引の送信を要求されることは決してない。しかし、保護通貨を用いることで、１個以上の信用できる第三者機関（以下Ｔ３Ｐと称する）の信用に基づいて（人々がオンライン購入を行う際にクレジットカード会社が自身の利益を保護してくれるものと信用するのと同様に）有益な保護を提供することができる。保護通貨を用いる場合、保護が確認できるようにＴ３Ｐ用のアカウントが必要である。

【００３８】

支払取消

保護通貨を用いて、支払取消又は戻入取引を行える能力が望まれる状況を扱うことができる。保護通貨は主要通貨とは異なる特別のルールの下で運用されるが、全ての保護通貨取引は主要通貨と同じ方法論を用いてブロックチェーン上で確認される。保護通貨は、主要通貨を表す一時的なツールとして機能するが、保護通貨を用いた取引はＴ３Ｐにより差し戻すことができる。保護通貨は本質的に特定の種類のスマート契約と同様であるが、その目的と使用が規定されていてプロトコルの中核に組み込まれている。

【００３９】

保護通貨を用いて取引、例えば購入を行うことが望まれた場合、送金側は単に主要通貨の代わり保護通貨を送金すべきであることを示す。保護通貨は送金側のウォレットの主要通貨を置換し、次いで保護通貨が受取人に送金される。保護通貨はまた、送金された時点を示すタイムスタンプ及び標準主要通貨に戻せる期限を含んでいる。システム既定値はＳｄ秒（例えば１５日間と同等の秒数）である。この交換はノードにより計算及び確認される自動取引である。保護通貨が主要通貨となる前のＳｄ秒間において、Ｔ３Ｐは保護通貨取引を（戻入取引を追加することにより）差し戻す権限を有している。保護通貨は、受け取り後も依然として保護通貨の形式である間は受取人により送金することができない。保護通貨を所有している間の任意の時点で、受取人は保護通貨を拒否するメッセージを送信することができ、まるで取引が生じなかったかのように送金側のウォレット内の主要通貨となる（これは取引として実行される）。送金側はまた、（例えば、製品が良好な状態で受け取られた場合に）保護通貨を直ちに受取人に渡す主要通貨に交換するメッセージを送信することができる。

【００４０】

このように、保護通貨は、より安全な送金方法を表すことができる。顧客（送金側）は、売り手（受取人）が不正な行為を行った場合に備えて安全策が設定されていることを承知した上で支払いを送金することができる。紛争はクレジットカードにおける紛争と同様にＴ３Ｐにより調停される紛争解決処理により扱われる。紛争解決は、法律的原則、例えば売り手側の要件及び売却を行うプラットフォームにおける主張に基づいている。

【００４１】

保護通貨期限は、ユーザーが詐欺の疑惑を提示して紛争を開始したならば自動的に延長される。ＧＯＶ又はＴ３Ｐは、紛争解決により多くの時間が必要とされる場合、Ｓｄのシステム既定値を増分するか又は更に保護通貨の期限を延長することができる。

【００４２】

盗難保護

特別な保護通貨ウォレットは、取引の送金に主要通貨ではなく保護通貨を用いた場合のみ可能であるように作成することができる。保護通貨ウォレットは、属性が確認できるようにＴ３Ｐの承認の下で作成されなければならない。ユーザーがＴ３Ｐの確認済みアカウントを得たならば、必要に応じて新たな保護通貨ウォレットを作成することができる。保護通貨ウォレットを用いることで、ユーザーの秘密鍵が盗まれ、且つ資金が不法に送金された場合に取引を差し戻すことができる。ウォレットの盗まれた秘密鍵は証明可能であり、次いで取引を差し戻して、新たに作成された保護通貨ウォレットに送信することができる。これにより、保護通貨ウォレットの使用を選択する人々にとって盗難のリスクが著しく低下する。保護通貨ウォレットは、送金が行われた際のＳｄのシステム価値を用いて、

このケースで保護通貨に直接紐付けられた寿命ではなく、Ｓｄに対するタイムスタンプを確認する。保護通貨ウォレットは、保護通貨を主要通貨に即時交換するメッセージを送信することができない。ＳｄはＧＯＶ又はＴ３Ｐにより任意の時点で変更可能である。

【００４３】

紛失秘密鍵

ユーザーが秘密鍵を紛失した場合、当該ユーザーは、保護通貨ウォレットから同一ユーザーが所有する新たに作成された別の保護通貨ウォレットへの送金をＴ３Ｐが開始することを要求できる。同様に、保持者の死亡に伴い承継者に主要通貨を送金することができる。Ｔ３Ｐが保護通貨を不適切に送金する（決して起きてはならないが、予防措置としてユーザーが制御する安全策を認める）防止策として、ユーザーは、新たな主要通貨ウォレット（このケースでは実際には紛失していない秘密鍵を用いて）に保護通貨を主要通貨の形式で送金することにより、ＩＮＮが行った送金を効果的に差し戻すことができる。

【００４４】

特徴

主要通貨ウォレットから引き出すいかなる取引も送金側（買い手）がＴ３Ｐアカウントを有していれば保護通貨で行うことができる。保護通貨取引はいつものようにウォレットから主要通貨を引き出し、受取人は主要通貨ではなく保護通貨を受け取る。保護通貨は、作成時のタイムスタンプと、これに関連して主要通貨に交換できる期限とを含んでいる。購入された商品が届かなった等、受取人（売り手）が不正な行為を行った場合、送金側はＴ３Ｐに連絡し、支払いが依然として保護通貨の形式である間はＴ３Ｐが取引を差し戻すことができる。

【００４５】

保護通貨は、（主要通貨からの初期交換のケース以外は）ウォレットから送金することができない。保護通貨は、寿命の終了時点で自動的に主要通貨へ逆交換される。その時点で当該通貨はＴ３Ｐにより変更することができない。送金側は、保護通貨が生成されたか又はシステム既定値を用いる際に交換期限を設定することができる。受取人は取引を拒否することができ、その場合主要通貨を送金側のウォレットに戻す。送金側は、保護通貨を直ちに主要通貨に交換する取引メッセージ（購入した製品が良好な状態で到着した等）を送信することができる。

【００４６】

ユーザーは、自身の主要通貨を主要通貨ウォレットではなく保護通貨ウォレットに保持する方を選ぶことができる。保護通貨ウォレットは、盗難及び紛失に対して強化された保護策を含んでいる。保護通貨ウォレットはユーザーの主要通貨を通常のウォレットとして保持するが、保護通貨ウォレットから出て行くあらゆる送金が保護通貨の形式でなければならない。

【００４７】

保護通貨ウォレット送金の期限はシステムの既定時間であってよい。ユーザーの保護通貨ウォレット秘密鍵が盗まれ、且つ資金が不正に送金された場合、ユーザーはＴ３Ｐに連絡し、Ｔ３Ｐは取引を差し戻して、新たな秘密鍵を有する新たに作成された保護通貨ウォレットに資金を送金することができる。ユーザーがウォレットの秘密鍵を紛失した場合、Ｔ３Ｐは保護通貨を新たな保護通貨ウォレットに送金することができる。Ｔ３Ｐが保護通貨を不適切に送金する（決して起きてはならないが、予防措置としてユーザーが制御する安全策を認める）防止策として、ユーザーは、新たな主要通貨ウォレット（このケースでは実際には紛失していない秘密鍵を用いて）に保護通貨を主要通貨の形式で送金することにより、ＩＮＮが行った送金を効果的に差し戻す。

【００４８】

保護通貨ウォレットを用いて、即時取引、匿名取引、識別情報確認、及び与信／融資等の他の特徴を実装することができる。

【００４９】

即時取引

本システムは、例えばクレジットカードレール又はクレジットカードネットワーク上で取引を実行したい場合、又は移動取引を介して取引を直ちに承認したい場合等、即時ノードネットワーク（ＩＮＮ）上の即時ノードを介した取引を実行することができる。通常、取引は標準ノードにより受理され、ブロックペアの取引要素に入れられ、次いでブロックペアの確認要素が当該ブロック、従って取引を確認する。ブロックが深いほど安全であるが、確認の証明があれば、優先度がブロックチェーンの最上部にある確認済みブロックであっても比較的安全であり、特にＶｐ値が５０％を超える。これが意味するところは、取引が確認されるまでブロック時間すなわちＳｖ秒、Ｔ２においても１ブロック深くなるまで約２＊Ｓｖ秒かかる。この時間量は、直ちに確認を必要とする取引の場合、遅過ぎる。

【００５０】

即時ノードを用いて、従来の信用に基づくアカウントネットワークを実装する。しかし、即時ノードは、セキュリティ及びよりシームレスな統合用のためシステムプロトコルに直接組み込まれた動作プロシージャを用いる。主要通貨の所有者は保護通貨ウォレットを用いて、保護通貨割当又はＤａｌｌｏｃａｔｉｏｎと呼ばれる割当られた量を示すことができる。Ｄａｌｌｏｃａｔｉｏｎは、主要通貨、暗号法定通貨、又は他のトークンをＩＮＮにより即時確認されないよう除外する。Ｄａｌｌｏｃａｔｉｏｎは即時取引に利用でき、ＩＮＮがユーザーの行為（クレジットカードでの購入又は移動アプリでの購入等）に基づいて支払いチャネルを介して送金できる、ユーザーのウォレットに保持された主要通貨を表す。ユーザーは、保護通貨ウォレットのＤａｌｌｏｃａｔｉｏｎを作成すべく、暗号化された発行メッセージを、Ｄａｌｌｏｃａｔｉｏｎからの主要通貨送金をＩＮＮが許可した証拠と共に送信することができる。例えば、ＩＮＮ取引を所与の時間にわたる量に限定することができる。Ｄａｌｌｏｃａｔｉｏｎ内に留保された量は、ＩＮＮから生じた取引以外を介して保護通貨ウォレットから引き出して送金することができない。これらの取引は保護通貨ウォレットの秘密鍵を利用するのではなく、ＩＮＮ上のノードは自身の秘密鍵を用いて、Ｔ２のものと確認可能な取引を生じさせる。

【００５１】

従ってＴ３Ｐにより、支払いを直ちに保証する能力が得られ、標準的なクレジットカード機械を介して売却時点クレジットカード取引等の取引の処理が可能になる。ＰＯＳ購入は、Ｄａｌｌｏｃａｔｉｏｎからある金額を引き出す取引を起動することができる。ＩＮＮは、Ｄａｌｌｏｃａｔｉｏｎを有する各保護通貨ウォレットについてＤａｌｌｏｃａｔｉｏｎの残高の記録を維持する。ＩＮＮは、取引をＴ２に送り、ブロックチェーン自体でのアカウント残高を更新する。即時ノード支払いが望まれない場合、所有者は、保護通貨ウォレット内の標準主要通貨の金額にＤａｌｌｏｃａｔｉｏｎを放出する取引をネットワークに送信するようＩＮＮに指示することができる。Ｄａｌｌｏｃａｔｉｏｎが保護通貨ウォレットにあるため、ＩＮＮのハックから生じる盗難を防止できる。Ｄａｌｌｏｃａｔｉｏｎが保護通貨ウォレットに保持されているため、ＩＮＮからの不正な取引を差し戻すことができる。要するに、本方式によりＩＮＮは支払いを保証し、当該保証を即時に行うことができる。

【００５２】

ＩＮＮは、実際のブロックチェーンに取引を送付する前に、時間経過に伴い統合することができる。例えば、ウォレットＡが１００主要通貨をウォレットＢに送金し、ウォレットＢが１００主要通貨をウォレットＣに送金した場合、ＩＮＮはネットワークに対し、１００主要通貨の取引がウォレットＡからウォレットＣに送金された旨のメッセージを送信することができる。ＩＮＮは、ネットワークと同期する前に、自身のノードアカウント内で状態情報を要約することができる。

【００５３】

安定性

プロトコルは、法定通貨により１対１のレートで裏書きされた主要通貨の不揮発性表現である、暗号法定通貨と呼ばれる概念を介して安定性を保証する能力を有している。これはＤａｌｌｏｃａｔｉｏｎを用いることで実現される。ユーザーによりＤａｌｌｏｃａｔ

ｉｏｎに送金される金額は、交換機構を介して暗号法定通貨に交換することができる。暗号法定通貨は、例えば暗号ドル又は暗号化ユーロ等の多くの形式をなしていてよい。一例として、Ｔ３Ｐが発行する全ての暗号ドル毎に、１米ドルがＴ３Ｐにより管理されるエスクローアカウントに入れられる。エスクローアカウントは監査され、最初からその完全性に関して公に確認することができる。これらの暗号ドルは、Ｄａｌｌｏｃａｔｉｏｎ機構を介して、購入用ブロックチェーン内で送金することができる。将来の任意の時点で全ての暗号ドル保持者は、暗号ドル（次いで破棄される）と交換にエスクローから引き出された米ドルをＴ３Ｐから受け取ることができる。このように、存在する暗号ドルと厳密に同額の米ドルがエスクローに常に存在するため、暗号ドルの価値は棄損せず、米ドル（又は暗号化ユーロ対ユーロ等）の価値に極めて近接して追随するであろう。アカウントのＤａｌｌｏｃａｔｉｏｎ部分に含まれる暗号法定通貨はＴ３Ｐのみが送金でき、Ｔ３ＰはＤａｌｌｏｃａｔｉｏｎ送金の手数料を徴収する。しかし、ユーザーが暗号通貨を他のユーザーに無料で送金したい場合、暗号法定通貨を主要通貨と交換することにより可能であり、次いで受取人により元の暗号法定通貨へ交換することができる。基本的に、Ｄａｌｌｏｃａｔｉｏｎ及び主要通貨の暗号法定通貨による実装は、暗号通貨の安定した送金を可能にし、暗号通貨を単なる価値の保存以外の目的で用いる実用的な仕方をもたらす。暗号法定通貨は、詐欺、盗難及び紛失保護、又はプライバシーの実現等、プロトコルの他の特徴と共に用いられる。

【００５４】

暗号法定通貨はまた、他の資産の一括運用に用いることができる。Ｄａｌｌｏｃａｔｉｏｎは、暗号化ビットコイン、暗号化イーサ、又は暗号化金さえも含んでいてよい。Ｄａｌｌｏｃａｔｉｏｎはまた、法定通貨のグループ化を表す暗号化バスケット、及び米ドルよりも不安定でない他の金融ツールを含んでいてよい。

【００５５】

暗号法定通貨の効果は重要である。安定した暗号通貨により、これが無い場合には不可能であった多くの事柄が可能である。例えば、暗号通貨の価値が上がっている場合、購入し手はこれを購入目的では使用したくない。暗号通貨の価値が下がっている場合、売り手は売却目的では受け取りたくない。暗号通貨の価値が上昇している場合、融資又は与信の債務不履行レートは高く、貸し手はいずれの方向でも高い不安定性がある状況で貸したくない。不安定性が高いことで多くの実際的な状況において暗号通貨の使用が妨げられるが、主要通貨の安定したバージョンについては、実際にこれらの目的に用いることができる。オンライン支払い、小売購入、貸出、与信、及び外国為替は全て暗号法定通貨により可能になり、暗号通貨の他の全ての利点がはるかに強力になる。

【００５６】

デジタル与信及び融資

Ｔ３Ｐは、デジタル与信（すなわちデジタルクレジットカード又は融資に相当）に与信スマートコイン又は融資スマートコインを提供することができる。取引は、残高を清算すべく与信スマートコイン又は融資スマートコインを保持しているアカウントから自動的に処理される。これらのスマートコインは、融資／与信、例えば残高、金利、期限、支払い条件、コンプライアンス及び状況等に紐付けられた全てのパラメータを含んでいる。残高は、これらのパラメータに基づいて自動的に更新される（本質的には、残高は、計算が融資の状況に限定された特定のスマート契約のような役割を果たす）。与信スマートコイン及び融資スマートコインは無論、債権者以外が送金することはできない。与信スマートコインは、標準的クレジットカードのように利用可能な残高を含んでいる。融資スマートコインは清算された時点で消滅する。与信により受け取られた主要通貨は、即時支払いを可能にすべく上述のＤａｌｌｏｃａｔｉｏｎと共に用いることができる。この組み合わせにおいて、与信は従来のクレジットカードと同様に実装することができる。与信と貸出は、暗号法定通貨と組み合わされた場合に特に有益な概念である。

【００５７】

プライバシー

大多数のブロックチェーン方式の主要な短所の一つはプライバシーの不足であり、その理由はブロックチェーンが公に監査可能でない取引で必要な相互信用を不要にすべく（暗号化されているが）公に利用可能な全ての情報に依存するためである。例示的システムは、仮名によりプライバシーを提供する公に利用可能なブロックチェーンを有している。純粋に技術的な立場からは、何らの識別情報が紐付けられていなくてもアカウント／ウォレットを保持することができる。しかし、大多数のブロックチェーンと同様に誰でも資金の行方及び任意のウォレットの現在残高を追跡することができる。多くの正当且つ合法な状況において、より高レベルのプライバシーが必要である。例えば、ウォレット残高をウォレットに紐付けることが可能な場合、ウォレット残高を秘密にしておくことを望むかもしれない。人々が銀行口座の残高を公に発表したくないことは一般的である。属性とウォレットの紐付けは、例えば公知の購入タイミング又は公知の購入量を個人と相関させることにより、現実世界の情報をチェーン内イベントと組み合わせることにより時間経過に伴い行うことができる。例えば、抵当借り支払い、高額購入、又は自動車の給油又は地下鉄の切符等の少額購入でさえ、特定のウォレットを観察された個人と合致させるために利用できる。また、投票目的において、人は自身の投票と属性を切り離したい場合が多い。多くの場合、仮名で記名投票することも望ましくないであろう。人は自身の投票から後で自身に辿り着かれることを望まないであろう。

【００５８】

プライバシー問題を解決する方策の一つは、取引の可視性を防止して取引を真に匿名にする数学的解決策を用いることである。その一例として、取引は暗号化されているがブロックチェーンは依然として重複支出防止を保証するゼロ知識ＳＮＡＲＫＳを用いるＺＣａｓｈプロトコルである。しかし以下に記述する原則の場合、これは好適な解決策でない。第１に、システムの原則の大部分は透明性を旨として構築されている。バリデータが許可されているため、全てのユーザーの保護は、使用するコードの完全な透明性、統括機関のルール、及び、ここでの目的のためにブロックチェーン自体に依存する。最も透明な仕方で容易に監査可能なブロックチェーンは例示的システムの理念に合致する。第２に、別の所望の原則は、ルールが変化するに従い変化し得る現実的な解決策を構築することである。真のゼロ知識方式は、顧客確認（ＫＹＣ）及び資金洗浄対策（ＡＭＬ）ルールと整合させるのが困難である。政府により規制が変化するに従い、ＫＹＣ及びＡＭＬ的方式が最も普及及び成長しそうに思われる。

【００５９】

要するに、プライバシーは多くのユーザーにとって重要である。本発明のプライバシー保証方式により、必要に応じて匿名取引を実行する任意選択的な方法論が可能になる。本発明の方式は、ＩＮＮを介して実行される信用に基づく方法論を用いる。匿名取引を送信すべく、ユーザーは最初に保護通貨ウォレットからＴ３Ｐが所有するプライバシーアカウントに保護通貨を送金する。ユーザーは次いで、送信自体と、取引の暗号化にウォレットの秘密鍵を用いることの両方の観点から暗号化されていて、取引の送信先を指示するチェーン外メッセージをＩＮＮに送信する。ＩＮＮは、ウォレットの公開鍵を用いて受け取った金額に対して送信を確認し、次いで取引を実行するネットワークに取引メッセージを送信する。ユーザーはこのように匿名で資金を送金することができる。しかし、ＫＹＣ及びＡＭＬの目的では、保護通貨ウォレット（ＩＤはＴ３Ｐに知られている）がこれらの匿名送信に用いられるため、Ｔ３Ｐが送金側の属性を知ることになる点に注意されたい。送金される金額は、ある期間にわたり１個以上のウォレットに１個以上の金額に分けて行うよう指示することで、金額に基づいて公に追跡し難くすることができる。ＩＮＮにより差し戻された、保護通貨の形式をなす取引は、保護通貨の公的送金側がブロックチェーン上のＩＮＮウォレットとなるため、ＩＮＮを介して差し戻す必要がある。ＩＮＮが受理した差し戻しは、主要通貨を本来のウォレットへ返送すべく内部の匿名の記録を参照する必要がある。ＩＮＮは、入金する保護通貨金額からの送金に基づいて出金する保護通貨又は主要通貨金額を送金できるブロックチェーン上の唯一の主体である。

【００６０】

上述の方式は多くの状況で用いることができる。１回の送金を匿名で行うことができ、送金する金額を宛先まで公に追跡することができない。主要通貨の所有者は、特にアカウントの識別子が判定された場合、自身が所有するアカウントのプライバシーを守るため、自身が所有する他のウォレットへ匿名で金額を送金することができる。これはまた、取引がリバースエンジニアリングされないように更に判り難くすることができる。例えば、匿名取引は受取人アドレスに送金された保護通貨を有していてよく、残った主要通貨のいずれをも送金側が所有する異なるウォレットに送金することができる。無記名投票を実施することができ、ＩＮＮへの匿名送金を介して投票スマートコインを匿名で送金（すなわち投票行為）することができ、ＩＮＮは次いでスマートコインを正しく重み付けられていて、投票が本来の保持者まで辿られないように他の投票と統合された正しい投票アカウントに送信する。投票は、投票が適切に行われたことを後で確認すべく送金側だけが復号できる暗号化メッセージを含んでいてよい。このように、ユーザーは投票すると共に、自身の投票が正しく処理されたことを確認することができるが、当該投票を行ったのが自分であることを知っているのは自分だけである。

【００６１】

プライバシーと即時性の両方が望まれる（すなわちクレジットカード取引と同様の取引）場合、ユーザーはＤａｌｌｏｃａｔｉｏｎ取引と示される各取引がウォレットの残り残高を新たな保護通貨ウォレットに移動させるよう指示することができる。新規ウォレット内のＤａｌｌｏｃａｔｉｏｎはＩＮＮにより調整することができ、取引の公的判定を困難にすべく金額を複数のウォレットに送金すること、又は金額を時間経過に伴い複数の取引に跨って送金することができる。ユーザーはＩＮＮアカウントを介して自身の残高及びウォレットを追跡することができる。代替的に、ＩＮＮアカウントはまた、プライバシー及び即時性の両方を以て送金可能でありながら、交換に際してよくあるようにブロックチェーン自体には決して反映されない主要通貨を受け取ることもできる。ＩＮＮによりアルゴリズム的に生成された保護通貨アカウントは、匿名の所有権に関する情報が維持されるように所有者に合致する所有権記録を維持することになる。

【００６２】

ＩＮＮは、多くの取引を統合して、ブロックチェーンに要約を間欠的に投稿することにより、プライバシー及び効率を更に向上させ得る。ブロックチェーンを同期させる間隔は取引の即時性に影響を及ぼさない。取引及び残高は、Ｔ３Ｐに紐付けられたウォレット内をＩＮＮにより内部追跡することで、完全にチェーン外で保持されてもよい。

【００６３】

取引カテゴリの要約例

以下のカテゴリは、送金側がどのように取引を実行できるかを示している。主要通貨以外の全ての取引のカテゴリは任意選択的であり、追加的な機能又は安全性が望まれる場合にのみ主要通貨の所有者により用いられる。ユーザーは、保護通貨又は保護通貨ウォレットを用いるか否か、及び所与の取引にＩＮＮが関与しているか否かを判定することができる。

【表１】

	信用無し	戻入可能	詐欺からの保護	窃盗/紛失からの保護	即時	匿名
・主要通貨	はい	いいえ	無し	無し	いいえ	いいえ
・保護通貨取引	はい	はい	有り	無し	いいえ	いいえ
・保護通貨ウォレット	はい	はい	有り	有り	いいえ	いいえ
・Dallocation付保護通貨/INN	いいえ	はい	有り	有り	はい	部分的
・チェーン外命令付INNに対する保護通貨	いいえ	はい	有り	有り	はい	はい

【００６４】
ユーザーインターフェースの観点から、任意選択を直接的に設定することができる。主要通貨を送金可能にする標準的ソフトウェア又は任意のアプリが、所与の任意の取引を送信する保護通貨任意選択を行うための直接的チェックボックス、及び保護通貨の使用に関する情報を提供する標準的「情報」アイコンを有していてよい。
【００６５】
同様に、主要通貨ソフトウェアによりウォレットが生成されたならば、保護通貨ウォレットを生成するＴ３Ｐページへのリンクを有する代替的な保護通貨ウォレットを記述することができる。保護通貨ウォレットを作成する場合、即時性及びプライバシー任意選択を任意選択として記述することができる。基礎となる実装方式をユーザーに詳述する必要はない。異なる種類のウォレットを設定して異なる種類の取引を実行する際の選択及び分岐を直接的に記述している。
【００６６】
信用できる主体及び即時ノードネットワークの動作
ＧＯＶは、コンセンサスを保証すべくネットワークの動作を監督する主体である。即時ノードネットワーク（ＩＮＮ）はＧＯＶにより制御され、コンセンサス動作を監督して、任意選択的な特徴を追加するために用いられる。ＧＯＶは、透明性のシステム、すなわち誰もが任意の時点でコンセンサスを利用できること、誰もが任意の時点でネットワークのアルゴリズム動作及び当該アルゴリズム動作（すなわちブロックチェーン自体）の全ての結果を利用できることを監督すべくＧＯＶが動作するルールに基づいている。
【００６７】
貸出システム
Ｔ３Ｐは、固定された供給量の、保護された、部分準備貸出を行う貸出機構を提供する。主要通貨の借入能力を有することは、コミュニティにとって極めて有益な機能であり得る。貸出、借入ことを可能にすべく、プロトコルは、貸出コイン、融資コイン及び当該コインに基づくチェーン内契約の機構を利用し、これらは共同で部分準備銀行業務の同じ特徴及び利点の一部を共有する貸出システムを構築する。しかし、例示的システムは対照的に、部分準備銀行業務の弱点に対処する。例示的システムのプロトコルは、発行可能な主要通貨の量に特定の制限を設けている。所与の任意の供託者に対して所与の任意の引き出し限度（８０％）を保証すべく、主要通貨融資準備金（ＤＬＲ）と呼ばれる、貸出能力の所定の部分がＴ３Ｐ用に取り置かれる。貸し手は、貸出コインにより制御された融資発行ルールを前提に、ＤＬＲに等しい合計金額の融資を行うことしかできない。ＤＬＲを超える合計金額の融資を行うことができないため、貸出システムは（資金供給に関する限り）ＤＬＲを超えてインフレを引き起こすことはなく、主要通貨の全体的な固定された供給量はＤＬＲを超える程度には設定できない。貸出機構を規定するアルゴリズムの全てがノードにより自動的に実行される。

【００６８】
貸出を実行すべく、貸出コインがＴ３Ｐにより発行される。貸出コインを含むウォレットが貸し手であると考えてよい。貸し手の活動の基礎とすべく、これらの貸出コインをＴ３Ｐが売り出すか、又はＴ３Ｐが供託を要求することができる。Ｔ３Ｐはまた、例えば法定通貨又は主要通貨を用いて、又は供託を返金することにより、貸出コインを購入し戻すことに同意することができる。詳細に関してＴ３Ｐと貸し手の間で交渉される。貸し手を生成すべく、Ｔ３Ｐは、他者に貸出し可能な金額と貸し手の義務の両方を示す貸し手のウォレットに貸出コインを送金する。２種類の貸出コイン、すなわち部分準備貸出コイン及び全準備貸出コインがある。貸出コインは貸出承認を記録し、部分準備貸出コインはＤＬＲに等しい合計金額までしか発行できない。全額準備貸出コインは当該合計金額に加算されない。Ｔ３ＰがＤＬＲよりも大きい部分準備貸出コインの合計金額の貸出を承認しようとする場合、当該発行額の送金はシステムのノード（例：コンピュータ）により無効であるとみなされる。
【００６９】
部分準備貸出コイン。
部分準備金の貸し手が部分準備貸出コインにより生成された後で、供託を受け取ることができる。Ｔ３Ｐは、貸し手のアカウントに主要通貨を供託することができない。貸し手が供託を受け取った場合、供託者が引き出しを要求したならば貸し手は供託を返金する義務を負う責任が生じる。貸し手が供託を受け取った後、他者に融資を行うことができる。貸し手は、自身の供託金の最大８０％しか融資を行うことができず、自身の未払い供託総額の２０％を主要通貨積立金として維持しなければならない。所与の任意の期限の終了時点で２０％の残高が維持されていない場合、貸し手は貸出コインにより設定されたレートでＴ３Ｐから資金を借り受けなければならない。これはブロックチェーン上で自動的に生じる。貸し手には、引き出しが要求された場合に供託金の８０％を直ちに返金する義務があり、貸し手は、引き出し要求の残り２０％を返金するまで更なる貸出を一切実行することができない。引き出し要求の最後の２０％を返金するには、貸し手は、他の供託者及びＴ３Ｐの場合と同じ２０％のリスクレベルを維持すべく、引き出された供託金に対し２０％のリスクを考慮するために（２０％の準備金を超える）追加的な準備金を維持しなければならない。貸し手が融資を行う場合、金利、期限、及び支払い義務等の標準的融資期限を規定する融資コインを発行する。貸し手はまた、借り手が使用可能な主要通貨を発行する。供託者が引き出しを行いたいが、貸し手が引き出しをカバーするのに充分な資金を当該準備金に有していなければ、貸し手は引き出しをカバーすべくＴ３Ｐから資金金を借り入れなければならない。Ｔ３Ｐにより全ての貸し手に対して部分準備金の８０％が引き出し用に保証されており、且つ供託者は自身の残高の８０％の引き出ししか要求できないため、全員が自身の全資金を同時に要求する（銀行業界で「取り付け騒ぎ」として知られる）場合であっても貸し手が自身の義務のために破綻するリスクはない。供託者は自身の供託金の２０％に対してリスクを負うため、貸し手を精査するインセンティブがある。また、貸出コインは供託者に融資を承認する際の投票権を与えることができる。
【００７０】
全額準備貸出コイン
Ｔ３Ｐにより、任意の貸出をカバーすべく主要通貨を含むウォレットに全予備貸出コインを発行することができる。貸出限度付きで全額準備貸出コインが発行された場合、ウォレット内の同金額の主要通貨が融資に固定され、融資を介する以外には送金できない。未払い融資が無い場合、貸し手は全額準備貸出コインを解除して、固定された主要通貨を解放することができる。固定された主要通貨は、全額準備貸出コインにより設定された要件内で他者に貸出すことができる。貸し手は、全額準備貸出コインによる融資における不良債権の全てのリスクを想定している。Ｔ３Ｐは、貸出コインにより規定された、全額準備融資の１パーセントの利子利益を受け取る。
【００７１】
貸出

借り手は、主要通貨及び自身の負債を表す融資コインを受け取る。融資は、ウォレット内の融資コインにより記述された設定済み分割払いで自動的に返済される。ウォレット内の主要通貨金額は融資支払いに自動的に適用される。融資支払い期限が到来したときにウォレットに充分な主要通貨が含まれていない場合、融資は直ちに債務不履行と見なされ、融資コインの規定に従い融資の残高にペナルティを課すことができる。融資コインにより規定されるように、融資の債務不履行が過度に長期間にわたる、又は過度に高額である場合、貸し手には融資を差し押さえる任意選択肢がある。融資コイン条件は、発行している貸し手の貸出コインにより規定された金利その他の債務に合致しなければならない。貸出コインは、ＴＳＰの細則により規定される全体的な貸出要件に合致しなければならない。ＴＳＰは、細則内で貸出コインを発行する場合、貸出に関する要件について交渉する。

【００７２】

融資を返済する場合、元本所有者は第１にＴＳＰからの任意の融資を与信し、第２に貸し手の準備金に加算する。融資の利子は当事者間で利益として分配される。利益の４０％が貸し手の供託者（支払い期間中の供託金の有効期間全体にわたり比例配分される）に、５０％が貸し手に、及び１０％がＴＳＰに支払われる。融資が返済されない場合、貸し手は担保（チェーン内又は外）を差し押さえることにより、又は他の融資における利益を用いて未払い債務を充当しなければならない。最終的に、貸し手自身が債務不履行に陥って破産した場合、ＴＳＰはＤＬＲから供託金の８０％を保証し、問題の貸出コインは凍結される。融資債務不履行の場合、供託者は自身の供託金の２０％を失う立場にあるため、信用できる貸し手を選択すべく動機付けられる。貸出コインが凍結された場合、依然としてＤＬＲに関して貸出し可能な合計金額に反映されるが、ＴＳＰが当該コインに紐付けられた不良債権を返済するまで、その貸出コインによる更なる貸出は起こり得ない。従って、凍結された貸出コインは、ＴＳＰが凍結貸出コインに紐付けられた不良債権を清算するまで融資に利用できる主要通貨の総額を下げる。

【００７３】

与信

ＴＳＰは、ＤＬＲの利用できる金額から、又は主要通貨所有権から、与信コインの形式でユーザーに直接与信を発行することができる。与信コインはクレジットカードと同様に機能する。融資が清算された際に融資コインが消滅する場合、継続的な与信を行うために与信コインを用いることができ、その使用に紐付けられた条件に従うものとする。

【００７４】

ＤＬＲ有効性

ＤＬＲは時間経過に伴い解除されて、貸出目的に利用可能になり得る。例えば、２０％は発行の１年後に解除され、その後追加的な２０％は全ＤＬＲが貸出に使用可能になるまで毎年解除される。

【００７５】

属性

属性は、例示的プロトコル内の強力な解決策である。スマートコインは、様々なユースケースにおいてユーザーが自身の属性を証明するためにＩＮＮにより発行することができる。ＴＳＰが保護通貨ウォレット所持者の属性を定義により知っているため、属性スマートコインは、保護通貨ウォレットだけに発行される。

【００７６】

属性スマートコインは、売り手が売却に際して属性を確認したい場合等、取引に属性が必要な任意の状況で用いることができる。この場合ＩＮＮは、取引用の主要通貨を有する保護通貨ウォレットに属性スマートコインを発行することができる。個人の属性が当人の主要通貨所有権に紐付けられている必要がない点に注意することが重要である。主要通貨所有者は、個別ケース毎に新たな保護通貨ウォレットを生成し、主要通貨を当該ウォレットに送金するか又は他の誰かから主要通貨を受け取り、次いでＩＮＮが新たなアカウント用の属性スマートコインを発行することを要求することができる。新たな保護通貨ウォレットへの主要通貨の送金は追加的に、属性スマートコインが公に他のアカウントと紐付け

られないように、後述する匿名取引を介して扱うことができる。
【００７７】
属性スマートコインは、意図された受取人が属性を確認及び使用できる唯一の主体であるように暗号化できる。例えば、第三者機関パートナーは、Ｔ３Ｐとの関係を利用して自身の属性確認技術を利用することができる。ＩＮＮは、提供された復号鍵を用いて第三者機関が後で復号する属性を暗号化することができる。代替的に、所有者は、当該所有者が保持するキーにより暗号化された属性スマートコインを要求することができる。ＩＮＮは、所有者から要求があれば属性スマートコインをウォレットに送金することができる。次いで、識別された保護通貨ウォレットから生じた取引は、主要通貨が関与しているか否かに依らず、ＩＮＮが送金した属性スマートコインを用いて、指定された識別から生じたものと確認することができる。属性はまた、所有者の事前承認を得てＴ３Ｐにより確認することができる。属性スマートコイン暗号化は、ＩＮＮにより送金された属性スマートコインは公的記録を用いて無関係なアカウントに紐付けできないように公開鍵等のウォレットの数値的側面を含んでいる。
【００７８】
属性スマートコインを用いる別の例として、Ｔ３Ｐは保護通貨ウォレットの所有者の市民権状況を確認することができる。これは最初にＴ３Ｐにより、パスポートのコピーを取得する等の標準的手段を介して行うことができる。所有者は次いで、特定の国の国民しか利用できないサービスで用いるべく、名前及び市民権情報を含む暗号化された属性スマートコインを自身のウォレットに送金するよう要求することができる。所有者は次いで、主要通貨支払いをサービスプロバイダに送金することができる。サービスプロバイダは属性（Ｔ３Ｐにより予め用意された場合）を復号するか、又は所有者の許可を（アカウント設定として、又は元の主要通貨送金の一部として）与えることができるＴ３ＰからのＩＤの確認を要求することができ、或いは所有者がチェーン外メッセージと共に属性を復号するために用いるキーを提供することができる。
【００７９】
属性確認には多くの有用な目的があり得る。属性確認を用いて第三者機関による投票を可能にすることができる。属性確認は、組織への加入、クレジットカード又は抵当の確保、購入を行う、特定のグループに制限された措置の実行、抽選への参加、又はオンライングループとの対話等、ある程度の識別を必要とする取引に用いることができる。
【００８０】
属性スマートコインは、名前、住所、電子メール、電話番号、性別、国籍、又は識別要求で必要とされる他の任意の情報等、個人の詳細事項を含んでいてよい。Ｔ３Ｐはまた、他の種類の属性入力、例えば銀行口座確認（少額送金を行って後で報告）、携帯電話テキスト送信の確認、政府発行ＩＤ又は参照番号の確認、物理的な顔又は指紋スキャン、或いはデジタル属性及び使用可能な他の任意の種類の識別情報を監視することにより属性確認を支援することができる。属性スマートコインは第三者機関のシステムにより、例えば要求の送付に用いることができる。属性スマートコインを用いて、メンバーシップを申請することができ、申請に必要とされる詳細事項の全てが属性スマートコインに含めることができ、属性スマートコインの送金はメンバーシップを申請する行為である。
【００８１】
以下は例示的なユースケースのリストである。これらは、Ｔ３Ｐとの関係を確立する第三者機関により実行できるか、又は所有者が別々に提供する暗号化キーを介して実行することができる。Ｔ３Ｐは、ユーザーの命令に基づいて様々な実装方式に対応することができる。
【００８２】
投票－ＩＮＮは、投票に適格であるアカウントに暗号化された属性スマートコインを発行することができ、これらのスマートコインは、投票選択（匿名又は公開送金のいずれか）を表す第三者機関のアドレスに送ることができる。このように、属性毎に１回の投票を保証できる。

【００８３】
メンバーシップ－ＩＮＮは、メンバーシップの申請に必要とされる全ての情報を有する適格メンバーに暗号化された属性スマートコインを発行することができる。ユーザーは第三者機関のアドレスに属性スマートコインを送金してメンバーシップを申請することができる。会費がある場合、当該会費は属性スマートコインを保持しているアカウントから主要通貨で支払うことができる。メンバーシップは、ジム又はクラブ等の物理的位置に紐付けられていても、又はビデオゲーム又はソーシャルサイト等のオンライン活動用であってもよい。属性スマートコインは、オンラインデートサイトでの性別確認、又はゲームその他のウェブサイトにおけるＣＯＰＡ（児童オンライン保護法）目的での年齢確認に用いることができる。

【００８４】
抽選－ＩＮＮは、抽選等のマーケティングイベントの適格な参加者に暗号化された属性スマーコインを発行することができる。ユーザーは、自身がマーケティングスマートコイン（マーケティングスマートコインはまた、例えば参加を動機付けるべく主要通貨を含んでいてよい）を受け取る意思があるか否かを自己識別することができる。属性スマートコインは参加の公平性を保証することができる。

【００８５】
クレジットカードの取得－ＩＮＮは、アカウント取得のための属性情報だけではなく与信スコアの確認に必要な情報をも含む暗号化された属性スマートコインを発行することができる。代替的に、ユーザーのアカウントで主要通貨資金を用いるためにプリペイドクレジットカードを申請することができる。属性スマートコインを資産譲渡人のアカウントに移転する送金がアプリケーションを表す。アプリケーションは無論、融資（融資スマートコインにより実装）のようにチェーン内で、又は抵当（一旦適用が承認されたならば外部契約を介して実装される）のようなチェーン外で実装された他の同様の機器に送付することができる。

【００８６】
限度付き購入－ＩＮＮは、ユーザーの要求を受けて、限度付き購入が行えるようにユーザーに属性スマートコインを発行することができる。購入自体は主要通貨で行うことができ、ＩＤスマートコインは、酒類購入時の年齢要件、高齢者割引の保証、デートイベントのチケット購入時の性別要件、軍用又は教育関連割引等のグループ要件、市民権等の位置要件、又は他の任意の種類の属性確認等の購入要件を確認することができる。

【００８７】
暗号法定通貨の例
以下に、暗号法定通貨、すなわちブロックチェーン内で保護通貨割当金額（Ｄａｌｌｏｃａｔｉｏｎ）として維持される主要通貨の１対１のレートで裏書されたバージョンの使用例を示す。これらの例は、暗号法定通貨がどのように使用できるかを概念的に示しているが、特定の実装方式は完全に発展するに従い将来的に変化しよう。ここに挙げた例に限らず、暗号法定通貨の他の多くの種類の使用法がある。

【００８８】
暗号ドルが欲しい主要通貨所有者：マイクは、主要通貨を受け取る場所で使えるように暗号ドルと交換したい主要通貨を有している。マイクの主要通貨は現在の為替相場で５００ドルの価値がある。ジョーはいくらかの主要通貨を購入したい。ジョーは、Ｔ３Ｐから主要通貨を５００ドルで購入する（簡潔のため、本例ではジョーしかいないが、このような取引は無論複数の購入し手と売り手の間で起こり得る）。Ｔ３Ｐは当該５００ドルをエスクローに入れ、マイクに対して５００暗号ドルを発行。現在Ｔ３Ｐはエスクローに５００ドルを有し、ジョーは主要通貨を有していて、マイクは５００暗号ドルを有している。マイクは主要通貨アプリ等、Ｔ３Ｐの支払いチャネルを介して自身の５００暗号ドルを使うことができる。

【００８９】
暗号ドルを受け取りたい企業：あるレストランチェーンは自身のレストランで暗号ドル

を受け取りたいと思っている。Ｔ３Ｐはチェーンとの合意を行い、例えば典型的にクレジットカード取引で請求される額より少額であるにもかかわらず、取引に少額の手数料を課す。Ｔ３Ｐは、自身のＤａｌｌｏｃａｔｉｏｎ支払いシステムへのアクセスを実行し易くする。購入がなされた場合、Ｔ３Ｐは直ちに当該購入を確認及び承認することができ、次いで全ての暗号ドル取引をＴ３Ｐによりブロックチェーンに送信する必要がある。エンドユーザー（レストランの客）にはクレジットカード支払いと同様に一切の追加的コストが生じない。チェーンが暗号ドル収益を有すると、後で暗号ドルをＴ３ＰのエスクローからのＵＳＤと交換することができる。月末時点でレストランチェーンはＴ３Ｐに対して手数料の支払い義務が生じる。これらの手数料は主要通貨で支払われてよく、主要通貨の流動性が増す。

【００９０】

暗号ドルが欲しい顧客：サリーは、暗号ドルの便利さと安全性を前提としてレストランチェーンで暗号ドルを使いたい。サリーは、ウォレットを生成して、Ｔ３Ｐのアカウントを生成し、次いで１００米ドルで１００暗号ドルを購入する。Ｔ３Ｐは次いで、Ｄａｌｌｏｃａｔｉｏｎに割り当てられたサリーのウォレットに１００暗号ドルを追加し、１００米ドルをエスクローアカウントに算入する。サリーは現在、例えばＴ３Ｐのアプリ又はデビットカードを用いて自身の暗号ドルを使うことができる。サリーはカウンタまで歩いて行き、食品を注文し、次いで１０．２２ドルの代金を暗号ドルで支払う。Ｔ３Ｐは直ちに取引を確認し、次いでレストランチェーンのＤａｌｌｏｃａｔｉｏｎアカウントへのブロックチェーンを介した送金を開始する。しばらく後で（保護通貨待機時間後）、レストランチェーンはＴ３Ｐにより１０．２２暗号ドルを１０．２２ドルに交換することができる

【００９１】

クレイグリストの何かを買うために主要通貨に無料で交換を望む暗号ドルの所有者：サリーは次いで、自身の暗号ドルを望み通りに送金すべく直接アクセスしたい、且つクレイグリストでの購入のためにより大きい金額を無料で送金できるように残りの９０暗号ドルを主要通貨に交換したいと決心する。サリーはＴ３Ｐの交換機に、自身の暗号ドルを主要通貨に交換したい旨を伝える。ロンは、交換機に、自身の主要通貨を売りたい旨を伝える。Ｔ３Ｐは、ロンの主要通貨をサリーに（現在の交換レートで決定される金額で）に送金し、サリーの暗号ドルを除外して、エスクローからロンに９０ドルを支払う。サリーは次いで、自身の主要通貨をクレイグリスト販売者の主要通貨ウォレットに直接送金することによりクレイグリストでの購入を行う。

【００９２】

他国にいる親類へ資金を送金する人：ボブは現在オランダに住んでいる姉妹のアリスに資金を送りたい。ボブはＴ３Ｐから５００暗号ドルを購入し、交換機で主要通貨に交換してアリスに送金し、アリスは当該主要通貨を交換機で暗号化ユーロに交換する。主要通貨から暗号化ユーロへの交換に少額の手数料がかかるが、当該手数料は電信送金手数料より大幅に安く、送金は即時且つ安全に行われ、簡単且つ便利に追跡することができる。

【００９３】

夕食を割り勘する友達のグループ：５人の友達が連れ出したい６人目の友達の誕生祝いにレストランへ夕食に出かける。レストランは主要通貨／暗号法定通貨を受け取る。夕食後、５人の友達は自身の主要通貨アプリを開き、ウェイタが持って来たＱＲコードをスキャンして、各々が自身の支払い分を支払い合計に簡単に算入する。

【００９４】

家賃を折半するルームメート：３人のルームメートが各自の家賃負担分を支払いたい。２人が手数料無しで主要通貨を３人目に送金する。３人目は、主要通貨を米ドルに交換して家賃を立て替える。翌月、アパートの経営者は暗号ドルを支払いとして受け取り始める。次いで３人全員が各自の家賃負担分を直接暗号ドルで支払う。

【００９５】

効率的な銀行：銀行は、調整された部分準備実施に際して暗号法定通貨を用いて銀行取引を実施するか、又は暗号法定通貨を用いて与信を行うことができる。暗号法定通貨は与

信又は貸出スマートコインと組み合わせることができる。これは特に、銀行サービスを受けられない、世界の６０％にとって魅力的である。

【００９６】

不安定な国で資金を有する人：ホセは、ハイパーインフレが起き始めた国に住んでいる。ホセ及び周辺の人々は単に自身の取引のために主要通貨を用いる。

【００９７】

インフレ、経済低下等を心配する人：ニコルは安定した国に住んでいるが、不況に突入しつつある。ニコルは暗号ドルを購入し、様々な国からの法定通貨、及び金（ゴールド）等の他の比較的安定した資産を含む金融ツールの集まりである主要通貨（時間経過に伴う安定性に応じて）、又は暗号ワールドコイン（仲介者としての主要通貨を介して）のいずれかに交換する。

【００９８】

法定通貨を安価に送金する方法を求める銀行：銀行は本システムを用いて銀行間支払いを安価に送金することができる。

【００９９】

主要通貨を売却したい人：主要通貨の流動性を望む者は誰でも、主要通貨の暗号通貨としての一般的な使用、暗号法定通貨にかかる手数料を支払う際の使用、及びデベロッパーストアを含むデジタル市場における使用により促進される流動性を前提として、主要通貨を売却及び交換することができる。

【０１００】

他の暗号通貨を送金するユーザー：Ｔ３Ｐは、暗号法定通貨の実施方法と同様に、他の暗号通貨を受け取って、１対１のレートで裏書きされたエスクローアカウントに算入することができる。例えば、大幅な遅延及び高い手数料無しにビットコインで取引を行いたいユーザーは、ＩＮＮにビットコインを送金して、代わりに暗号化ビットコインを受け取り、次いでネットワーク上で暗号化ビットコインを送金する。任意の時点で、暗号化ビットコインの所有者は、自身の暗号化ビットコインをエスクローから引き出したビットコインと交換することができる。

【０１０１】

実装。本発明による方法及び装置は、分散ネットワークに接続された複数のコンピュータを用いて実装することができる。従来、コンピュータプログラムは計算命令又はプログラム命令の有限個のシーケンスを含んでいる。プログラム可能装置（すなわちコンピュータ装置）がこのようなコンピュータプログラムを受信して、その計算命令を処理することにより更なる技術的効果を発揮できることが理解されよう。

【０１０２】

プログラム可能装置は、１個以上のマイクロプロセッサ、マイクロコントローラ、埋め込みマイクロコントローラ、プログラム可能デジタル信号プロセッサ、プログラム可能機器、プログラム可能ゲートアレイ、プログラム可能アレイ論理、メモリ装置、特定用途向け集積回路等を含んでいて、これらを適宜使用又は構成してコンピュータプログラム命令の処理、コンピュータ論理の実行、コンピュータデータの保存等を行うことができる。本開示及び他の箇所を通じて、コンピュータは、専用コンピュータ、プログラム可能データ処理装置、プロセッサ、プロセッサアーキテクチャ等のいずれをも、及びあらゆる適当な組み合わせを含んでいてよい。

【０１０３】

コンピュータがコンピュータ可読記憶媒体を含んでいてよく、当該媒体が内蔵されていても、又は外付け、着脱可能及び交換可能、或いは固定されていてもよいことが理解されよう。また、コンピュータが、本明細書に記述するソフトウェア及びハードウェアを含み、これらとのインターフェースを有し、又はサポートすることができる基本入出力システム（ＢＩＯＳ）、ファームウェア、オペレーティングシステム、データベース等を含んでいてよいことが理解されよう。

【０１０４】

本明細書に記述するシステムの実施形態は従来のコンピュータプログラムはこれらを動作させるプログラム可能装置が関わるアプリケーションに限定されない。例えば、以下の請求項に記述するように本発明の実施形態は光コンピュータ、量子コンピュータ、アナログコンピュータ等を含んでいてよいと考えられる。

【０１０５】

コンピュータプログラム又は関与するコンピュータの種類に依らず、コンピュータプログラムを、上述の機能のいずれか及び全部を実行可能な特定の機械を生成すべきコンピュータにロードすることができる。この特定の機械は上述の機能のいずれか及び全部を実行する手段を提供する。

【０１０６】

１個以上の計算機可読媒体（群）の任意の組み合わせを利用することができる。計算機可読媒体は、計算機可読信号媒体又は計算機可読記憶媒体であってよい。計算機可読記憶媒体は、例えば電子、磁気、光、電磁気、赤外線、又は半導体システム、装置、又は機器、或いは上記の任意の適当な組み合わせであってよいが、これらに限定されない。計算機可読記憶媒体のより具体的な（非網羅的リスト）は、１本以上の導線を有する電気接続、可搬コンピュータディスケット、ハードディスク、ランダムアクセスメモリ（ＲＡＭ）、読み出し専用メモリ（ＲＯＭ）、消去可能プログラム可能読み出し専用（ＥＰＲＯＭ又はフラッシュメモリ）、光ファイバ、可搬コンパクトディスク読出し専用メモリ（ＣＤ－ＲＯＭ）、光記憶装置、磁気記憶装置、又は上述の任意の適切な組み合わせを含んでいる。本明細書の文脈において、計算機可読記憶媒体は、命令実行システム、装置、又は機器により、又はこれらと組み合わせて用いられるプログラムを包含又は保存できる任意の有形媒体であってよい。

【０１０７】

本発明の一実施形態によれば、データ記憶装置は、データベース、ファイル記憶システム、リレーショナルデータ記憶システム又は好適にはリレーショナルにデータを保存すべく構成された他の任意のデータシステム又は構造の１個以上を含んでいてよい。本発明の一実施形態において、データ記憶装置は、データを受信、処理及び保存するリレーショナルデータベース管理システム（ＲＤＢＭＳ）と共同で動作するリレーショナルデータベースであってよい。一実施形態において、データ記憶装置は、移動情報及び推定情報の処理に関する情報を保存する１個以上のデータベース、並びに移動情報及び推定情報を記憶及び照会すべく構成された１個以上のデータベースを含んでいてよい。

【０１０８】

コンピュータプログラム命令は、コンピュータ又は他のプログラム可能データ処理装置に特定の仕方で機能するよう指示可能なコンピュータ可読メモリに保存されていてよい。コンピュータ可読メモリに保存された命令は、上述の機能の一部又は全部を実行するコンピュータ可読命令を含む製品を構成する。

【０１０９】

計算機可読信号媒体は、計算機可読プログラムコードが例えばベースバンド又は搬送波の一部として組み込まれた伝搬データ信号を含んでいてよい。このような伝搬信号は、電磁気、光、又はこれらの任意の適当な組み合わせを含むがこれらに限定されない様々な形式のいずれをなしていてよい。計算機可読信号媒体は、計算機可読記憶媒体ではないが、命令実行システム、装置、又は機器により、或いはこれらと組み合わせて使用されるプログラムの通信、伝搬、搬送が可能な任意の計算機可読媒体であってよい。

【０１１０】

計算機可読媒体に搭載されたプログラムコードは、無線、有線、光ファイバケーブル、ＲＦ等、又は上記の任意の適当な組み合わせを含むがこれらに限定されない任意の適当な媒体を用いて送信することができる。

【０１１１】

各図面を通じてフロー図表現及びブロック図に示す要素は、要素同士の論理的境界を示唆している。しかし、ソフトウェア又はハードウェア工学の実践によれば、図示する要素

及びそれらの機能は、単体ソフトウェア構造の複数部分として、スタンドアローンソフトウエアモジュールとして、又は外部ルーチン、コード、サービス等、或いはこれらの任意の組み合わせを用いるモジュールとして実装することができる。このような実装方式は全て本開示の範囲に含まれる。

【０１１２】

上の記述に鑑みて、ブロック図及びフロー図表現の要素が、指定された機能を実行する手段の組み合わせ、指定された機能を実行するステップの組み合わせ、指定された機能を実行するプログラム命令手段をサポートすることが理解されよう。

【０１１３】

コンピュータプログラム命令はコンピュータ実行コードを含んでいてよいことが理解されよう。Ｃ、Ｃ＋＋、Ｊａｖａ、ＪａｖａＳｃｒｉｐｔ、アセンブリ言語、Ｌｉｓｐ、ＨＴＭＬ、Ｐｅｒｌ等を含むがこれらに限定されないコンピュータプログラム命令を表す様々な言語が可能である。このような言語は、アセンブリ言語、ハードウェア記述言語、データベースプログラミング言語、関数型プログラミング言語、命令型プログラミング言語等を含んでいてよい。いくつかの実施形態において、コンピュータプログラム命令は、コンピュータ、プログラム可能データ処理装置、プロセッサ又はプロセッサアーキテクチャの異種組み合わせ等で動作すべく保存、コンパイル、又はインタープリットすることができる。非限定的に、本明細書に記述するシステムの実施形態は、クライアント／サーバソフトウェア、サービスとしてのソフトウェア、ピアツーピアソフトウェア等を含むウェブベースのコンピュータソフトウェアの形式をなしていてよい。

【０１１４】

いくつかの実施形態において、コンピュータは複数のプログラム又はスレッドを含むコンピュータプログラム命令の実行を可能にする。複数のプログラム又はスレッドは、プロセッサの利用度を向上させ、実質的に同時に機能を実行可能にすべく多少同時に処理することができる。実装を通じて、本明細書に記述するいかなるそしてすべての方法、プログラムコード、プログラム命令又は１個以上のスレッドで実行することができる。スレッドは他のスレッドを生起させることができ、当該他のスレッド自身にも自らに関する優先度が割り当てられいてよい。いくつかの実施形態において、コンピュータは、プログラムコードに記述された命令に基づく優先度又は他の任意の順序に基づいてこれらのスレッドを処理することができる。

【０１１５】

明示的に記述又は別途文脈から明らかでない限り、動詞「実行する」及び「処理する」は互いに代替可能に用いられて、実行する、処理する、インタープリットする、コンパイルする、アセンブルする、リンクする、ロードする、及びこれらのいずれか及び全部の組み合わせ等を示す。従って、コンピュータプログラム命令、コンピュータ実行可能コード等を実行又は処理する実施形態は、いま述べた仕方の一部又は全部に従い命令又はコードに適切に作用することができる。

【０１１６】

本明細書に示す機能及び動作は、特定のコンピュータその他の装置とは一切固有の関係を有していない。本明細書の教示に従いプログラムで用いられる汎用システムを変更又はカスタマイズすることが可能であり、又は必要な方法ステップを実行するより専用の装置を構築するのが便利であることが分かるかもしれない。これらの様々なシステムに求められる構造は、等価な変型例と共に当業者には明らかであろう。また、本発明の実施形態は、何らの特定のプログラミング言語に関連して記述していない。様々なプログラミング言語を用いて、本明細書に記述する教示内容を実現できることを理解されたい。特定の言語へのあらゆる言及は、本発明を実施可能にすること及び複数の実施形態のベストモードを開示すべく提供されている。本発明の実施形態は、多くのトポロジにわたる広範なコンピュータネットワークシステムに良く適している。当分野において、大規模ネットワークの構成及び管理は、インターネット等のネットワークを介して異種コンピュータ及び記憶装置に通信可能に結合された記憶装置及びコンピュータを含んでいる。

【０１１７】
本開示及び他の箇所を通じて、ブロック図及びフロー図表現は、方法、装置（すなわちシステム）、及びコンピュータプログラム製品を示す。ブロック図及びフロー図表現の各要素、並びにブロック図及びフロー図表現の要素の各々の組み合わせは、方法、装置、及びコンピュータプログラム製品の機能を示す。そのような機能のいずれか及び全部（「図示された機能」）は、コンピュータプログラム命令により、ハードウェアに基づく専用コンピュータシステムにより、専用ハードウェアとコンピュータ命令の組み合わせにより、コンピュータ命令を介して専用化された汎用ハードウェアの組み合わせ等により実装することができ、それらのいずれか及び全部を本明細書において「回路」、「モジュール」、又は「システム」と称してよい。

【０１１８】
上述の図面及び記述は開示するシステムの機能態様について述べているが、明示的に記述又は別途文脈から明らかでない限り、これらの機能態様を実装するソフトウェアのいかなる特定の構成もこれらの記述から推定すべきではない。

【０１１９】
フロー図表現の各要素は、コンピュータにより実行される方法の１ステップ、又は複数ステップのグループを示すことができる。更に、各ステップは、１個以上のサブステップを含んでいてよい。説明目的で、これらのステップを（上で識別及び記述した他のいずれか及び全部のステップも同様に）順次提示する。一実施形態が、本明細書に開示する技術の特定の用途に適合されたステップの代替的な順序を含んでいてよいことが理解されよう。このような変型及び変更は全て本開示の範囲内に含まれるものとする。特定の順序でのステップの描写及び記述は、特定の用途で必要とされない限り、明示的に記述されない限り、又は別途文脈から明らかでない限り、異なる順序のステップを有する実施形態を一切排除するものではない。

【０１２０】
本明細書に記述する機能、システム及び方法は複数の言語で利用及び提示することができる。個々のシステムを１個以上の言語で提示することができ、当該言語は上述の処理又は方法の任意の時点で容易に変更することができる。当業者には、システムを提供可能な複数の言語が存在し、本発明の複数の実施形態が任意の言語での使用を考慮していることが理解されよう。

【０１２１】
複数の実施形態を開示しているが、当業者には本発明の更に他の実施形態もこの詳細な記述から明らかになろう。本発明は、様々な明らかな態様において無数の変更を加えることが可能であり、全てが本発明の趣旨及び範囲から逸脱することない。従って、図面及び記述は本来例示的であって限定的ではないと考えるべきである。

【図面】
【図１】

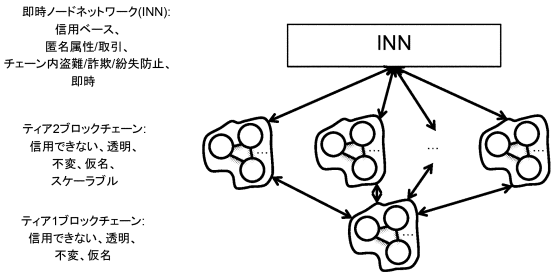
即時ノードネットワーク(INN):
信用ベース、
匿名属性/取引、
チェーン内盗難/詐欺/紛失防止、
即時
ティア2ブロックチェーン:
信用できない、透明、
不変、仮名、
スケーラブル
ティア1ブロックチェーン:
信用できない、透明、
不変、仮名
INN

図１

フロントページの続き

(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　62/644,841
(32)優先日　平成30年3月19日(2018.3.19)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　62/565,099
(32)優先日　平成29年9月29日(2017.9.29)
(33)優先権主張国・地域又は機関
米国(US)
(56)参考文献　米国特許出願公開第２０１７／０１３２６３０（ＵＳ，Ａ１）
米国特許出願公開第２０１７／０２００１４７（ＵＳ，Ａ１）
米国特許第０９２９８８０６（ＵＳ，Ｂ１）
アーヴィンド・ナラヤナン他，仮想通貨の教科書 －ビットコインなどの仮想通貨が機能する仕組み，第１版，日経ＢＰ社 村上 広樹，2016年12月09日，p.245-p.271,p.309-p.312
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６２
Ｇ０６Ｑ　４０／０２