(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7583233号
(P7583233)

(45)発行日　令和6年11月14日(2024.11.14)

(24)登録日　令和6年11月6日(2024.11.6)

(51)国際特許分類
Ｇ０６Ｑ　20/38　(2012.01)

ＦＩ
Ｇ０６Ｑ　20/38　３１０

請求項の数　7　（全29頁）

(21)出願番号　特願2020-81638(P2020-81638)
(22)出願日　令和2年5月5日(2020.5.5)
(65)公開番号　特開2021-177267(P2021-177267A)
(43)公開日　令和3年11月11日(2021.11.11)
審査請求日　令和4年2月3日(2022.2.3)
審判番号　不服2023-20323(P2023-20323/J1)
審判請求日　令和5年11月30日(2023.11.30)

(73)特許権者　518205368
仲宗根 豊
神奈川県横浜市泉区中田南３－２４－１５
(74)代理人　100187377
弁理士　芳野 理之
(72)発明者　仲宗根 豊
神奈川県横浜市泉区中田南３－２４－１５
合議体
審判長　佐藤 智康
審判官　相崎 裕恒
審判官　月野 洋一郎

最終頁に続く

(54)【発明の名称】　取引システム、取引システムの制御方法及び取引システムの制御プログラム

(57)【特許請求の範囲】
【請求項１】
複数のノードによって取引記録が保持され、これらによって構築されたネットワークで仮想通貨が管理されるブロックチェーンと、
前記ブロックチェーンの側鎖であるサイドチェーンと、を有し、
前記仮想通貨を取引する取引端末、取引を検証する検証サーバ、第三者機関である取引決済サーバを有する取引システムであって、
前記サイドチェーンでは、前記ブロックチェーンで管理される仮想通貨を管理できると共に、少なくとも、前記仮想通貨と法定通貨との交換を含む取引が可能な構成となっていると共に、前記サイドチェーンで実行された取引の結果情報は、前記ブロックチェーンに反映され、
前記サイドチェーンにおける取引情報は、監査端末及び前記検証サーバが検証し、
前記監査端末は、前記仮想通貨の取引の当事者として実際に機能していない前記取引端末から選択された複数の前記取引端末であり、
複数の前記取引端末が、前記サイドチェーンにおける取引に当事者として複数回、関与し、複数回の前記取引の結果情報が発生するときに、途中の前記取引の結果情報を省略し、最終の前記取引の結果情報のみを記憶するネッティング処理を行うと共に、前記ネッティング処理の前記最終の結果情報に基づき、当事者である各前記取引端末と前記取引決済サーバとの間のみの契約である取引情報を生成し、前記取引端末と前記取引決済サーバとの間の前記取引情報に基づいて、前記サイドチェーンで取引が実行される構成となってい

ることを特徴とする取引システム。
【請求項２】
前記サイドチェーンにおける当事者である端末間の前記取引情報には、交換する取引対象を相互に条件付けて、当事者の一方の端末が取引内容を実行しない場合、他方の端末の取引内容も実行されない構成を含んでいることを特徴とする請求項１に記載の取引システム。
【請求項３】
前記サイドチェーンにおける前記取引情報は、その内容を秘匿化するための秘匿化処理が施されていることを特徴とする請求項１又は請求項２に記載の取引システム。
【請求項４】
前記仮想通貨及び前記法定通貨は、それぞれ、前記サイドチェーン上では、サイドチェーン上で使用可能なサイドチェーン用トークンに変換されて取引され、
前記サイドチェーン用トークンは、前記検証サーバが、その発行を許可する構成となっており、
前記検証サーバは、前記サイドチェーンにおける前記取引情報の取引対象の交換価値の妥当性を判断することを特徴とする請求項１乃至請求項３のいずれか１項に記載の取引システム。
【請求項５】
前記取引決済サーバは、前記仮想通貨を使用不可となるように、前記ブロックチェーンにロックし、
複数の前記監査端末が、当該仮想通貨がロックされているか否かを検証し、前記監査端末が検証に成功すると、前記ブロックチェーンにロックされた当該仮想通貨と等価なサイドチェーン用トークンを前記サイドチェーンにアンロック又は新規発行することを特徴とする請求項４に記載の取引システム。
【請求項６】
複数のノードによって取引記録が保持され、これらによって構築されたネットワークで仮想通貨が管理されるブロックチェーンと、
前記ブロックチェーンの側鎖であるサイドチェーンと、を有し、
前記仮想通貨を取引する取引端末、取引を検証する検証サーバ、第三者機関である取引決済サーバを有する取引システムの制御方法であって、
前記サイドチェーンでは、前記ブロックチェーンで管理される仮想通貨を管理できると共に、少なくとも、前記仮想通貨と法定通貨との交換を含む取引が可能な構成となっていると共に、前記サイドチェーンで実行された取引の結果情報は、前記ブロックチェーンに反映され、
前記サイドチェーンにおける取引情報は、監査端末及び前記検証サーバが検証し、
前記監査端末は、前記仮想通貨の取引の当事者として実際に機能していない前記取引端末から選択され、
複数の前記取引端末が、前記サイドチェーンにおける取引に当事者として複数回、関与し、複数回の前記取引の結果情報が発生するときに、途中の前記取引の結果情報を省略し、最終の前記取引の結果情報のみを記憶するネッティング処理を行うと共に、前記ネッティング処理の前記最終の結果情報に基づき、当事者である各前記取引端末と第三者機関である取引決済サーバとの間のみの契約である取引情報を生成し、前記取引端末と前記取引決済サーバとの間の前記取引情報に基づいて、前記サイドチェーンで取引が実行される構成となっていることを特徴とする取引システムの制御方法。
【請求項７】
複数のノードによって取引記録が保持され、これらによって構築されたネットワークで仮想通貨が管理されるブロックチェーンと、前記ブロックチェーンの側鎖であるサイドチェーンと、前記仮想通貨を取引する取引端末、取引を検証する検証サーバ、第三者機関である取引決済サーバを有する取引システムに、
前記サイドチェーンでは、前記ブロックチェーンで管理される仮想通貨を管理できると

共に、少なくとも、前記仮想通貨と法定通貨との交換を含む取引が可能な構成となっていると共に、前記サイドチェーンで実行された取引の結果情報は、前記ブロックチェーンに反映される機能、
前記サイドチェーンにおける取引情報は、監査端末及び前記検証サーバが検証する機能、
複数の前記取引端末が、前記サイドチェーンにおける取引に当事者として複数回、関与し、複数回の前記取引の結果情報が発生するときに、途中の前記取引の結果情報を省略し、最終の前記取引の結果情報のみを記憶するネッティング処理を行う機能、
前記ネッティング処理の前記最終の結果情報に基づき、当事者である各前記取引端末と第三者機関である取引決済サーバとの間のみの契約である取引情報を生成し、前記取引端末と前記取引決済サーバとの間の前記取引情報に基づいて、前記サイドチェーンで取引が実行される機能、を実現させるための取引システムの制御プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、例えば、ブロックチェーン等の分散型台帳技術に関する取引システム、取引システムの制御方法及び取引システムの制御プログラムに関するものである。
【背景技術】
【０００２】
従来から、ブロックチェーン等の分散型台帳技術を用いて実現される仮想通貨が利用されている。
また、これら仮想通貨を円等の法定通貨と交換する需要があり、例えば、仮想通貨と法定通貨を固定価格で交換する等の提案もなされている（例えば、特許文献１等）。
【先行技術文献】
【特許文献】
【０００３】
【文献】特開２０１７－２９７０６号
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかし、ブロックチェーン等の分散型台帳技術を用いて信用が担保されている「仮想通貨」を円等の法定通貨と交換するには、ブロックチェーン等で、例えば、ＰＯＷ（Ｐｒｏｏｆ　ｏｆ　Ｗｏｒｋ）等の手法でマイナーの合意が形成される必要があり、例えば、約１０分間程度かかり、このため、仮想通貨と法定通貨と取引結果が、実際にブロックチェーン等に反映されるまで、時間がかかりすぎるという問題があった。
また、ブロックチェーン等で管理されている「仮想通貨」を法定通貨と交換して、その取引結果をブロックチェーン等に反映させるには、マイナーの合意が必要で、そのマイナーの手数料が高騰しているため、取引のコストが上昇しているという問題もあった。
【０００５】
そこで、本発明は、仮想通貨と法定通貨との交換、又は仮想通貨を媒介通貨としての法定通貨間の交換を迅速且つ低コストで行うことができると共に、セキュリテイの安全性や効率性も確保できる取引システム、取引システムの制御方法及び取引システムの制御プログラムを提供することを目的とする。
【０００６】
前記目的は、本発明によれば、複数のノードによって取引記録が保持され、これらによって構築されたネットワークで仮想通貨が管理されるブロックチェーンと、前記ブロックチェーンの側鎖であるサイドチェーンと、を有し、前記仮想通貨を取引する取引端末、取引を検証する検証サーバ、第三者機関である取引決済サーバを有する取引システムであって、前記サイドチェーンでは、前記ブロックチェーンで管理される仮想通貨を管理できると共に、少なくとも、前記仮想通貨と法定通貨との交換を含む取引が可能な構成となっていると共に、前記サイドチェーンで実行された取引の結果情報は、前記ブロックチェーン

に反映され、前記サイドチェーンにおける取引情報は、監査端末及び前記検証サーバが検証し、前記監査端末は、前記仮想通貨の取引の当事者として実際に機能していない前記取引端末から選択された複数の前記取引端末であり、複数の前記取引端末が、前記サイドチェーンにおける取引に当事者として複数回、関与し、複数回の前記取引の結果情報が発生するときに、途中の前記取引の結果情報を省略し、最終の前記取引の結果情報のみを記憶するネッティング処理を行うと共に、前記ネッティング処理の前記最終の結果情報に基づき、当事者である各前記取引端末と前記取引決済サーバとの間のみの契約である取引情報を生成し、前記取引端末と前記取引決済サーバとの間の前記取引情報に基づいて、前記サイドチェーンで取引が実行される構成となっていることを特徴とする取引システムにより達成される。

【０００７】

前記構成によれば、サイドチェーンでは、ブロックチェーンで管理される仮想通貨を管理できると共に、少なくとも、仮想通貨と法定通貨との交換を含む取引が可能な構成となっていると共に、サイドチェーンで実行された取引の結果情報は、ブロックメインチェーンに反映される構成となっている。

ブロックチェーンでは、ＰＯＷ（Ｐｒｏｏｆ　ｏｆ　Ｗｏｒｋ）により「マイナー」の合意が形成されるまでの時間が１ブロック当たり、約１０分間と長いが、本発明では、実際の取引（例えば、仮想通貨と法定通貨の交換等）が、サイドチェーンで行われる。

このため、サイドチェーンでは、ＰＯＷでの合意形成を待つ必要がないので、取引の時間を短縮することができ、これがため、迅速な取引が可能となる。

また、サイドチェーンを用いることで、ブロックチェーンのような「マイナー」の合意は不要なので、コストも低下させることもできる。

さらに、サイドチェーンでは、ブロックチェーンの「マイナー」とは異なる複数の監視部（例えば、検証サーバ、監査端末等）で、その取引を監視するため、取引の安全も確保することが可能となっている。

前記構成によれば、端末が、サイドチェーンおける取引に、当事者として複数回、関与するときに、当該取引情報の取引内容について、ネッティング処理を行う構成となっている。

当事者が複数回、取引に関与するときは、原則として、その都度、取引内容を実行しなければならない。例えば、Ａ端末がＢ端末に仮想通貨を１００万円と交換し、その後、仮想通貨を得たＢ端末が、Ｃ端末に同仮想通貨を１１０万円と交換する場合で、取引ごとに取引内容を実行する。このとき、Ｂ端末に所持金がないと、Ｂ端末は、１００万円を借り入れて、Ａ端末から仮想通貨を取得し、その後、Ｃ端末と仮想通貨を１１０万円と交換した後、１００万円を返済することになる。これでは、取引の迅速化を図ることができない。一方、上述の例で、Ａ端末からＣ端末に仮想通貨を渡し、Ｃ端末からＡ端末に１００万円、Ｃ端末からＢ端末に１０万円渡すという取引内容の「ネッティング処理」を行えば、Ｂ端末は、Ａ端末との取引のために、わざわざ借り入れをする必要がなく、迅速な取引が可能となる。

また、この「ネッティング処理」では、Ｃ端末に１万円でも資金不足等が生じると、Ａ端末、Ｂ端末、Ｃ端末の全体の取引が債務不履行となるおそれがある。

そこで、本発明では、さらに、ネッティング処理の結果情報に基づき、当事者である各端末と第三者機関（例えば、取引決済サーバ等）との間のみの前記取引情報を、端末毎に生成し、第三者機関との取引情報に基づいて、サイドチェーンで取引が実行される構成としている。

すなわち、上述の例では、例えば、それぞれ、取引決済サーバ等の第三者機関と端末Ａ、端末Ｂ、端末Ｃとの間の取引情報を生成する。

具体的には、第三者機関がＡ端末に１００万円支払う取引情報、第三者機関がＢ端末に１０万円支払う取引情報、そして、第三者機関が１１０万円と交換にＣ端末に仮想通貨を引き渡す取引情報等を生成する。

このように、当事者である各端末と第三者機関との間のみの取引情報を、端末毎に生成

することで、例えば、Ｃ端末に資金不足があっても、Ｃ端末と第三者機関との取引のみが不履行となり、他の２つの取引は有効に成立することになる。
　したがって、取引の安全と効率性の双方を達成することができる。
【０００８】
　好ましくは、取引システムの前記サイドチェーンにおける当事者である端末間の前記取引情報には、交換する取引対象を相互に条件付けて、当事者の一方の端末が取引内容を実行しない場合、他方の端末の取引内容も実行されない構成を含んでいることを特徴とする。
【０００９】
　前記構成によれば、前記サイドチェーンにおける当事者である端末間の取引情報には、交換する取引対象（例えば、ビットコイントークン、円トークン等）を相互に条件付けて、当事者の一方の端末が取引内容を実行しない場合、他方の端末の取引内容も実行されない構成、例えば、デリバリー・バーサス・ペイメント・スワップ（Ｄｅｌｉｖｅｒｙ　Ｖｅｒｓｕｓ　Ｐａｙｍｅｎｔ　Ｓｗａｐ）等を含んでいる。
　このため、サイドチェーン上で取引を行う端末である当事者同士について、互いに信頼関係がなくても、第３者である仲介者等を介することなく、相対取引を安心して行うことができる。
【００１０】
　好ましくは、取引システムの前記サイドチェーンにおける前記取引情報は、その内容を秘匿化するための秘匿化処理が施されていることを特徴とする。
【００１１】
　前記構成によれば、サイドチェーンにおける前記取引情報は、その内容（例えば、取引量、トークンの種類等）を秘匿化するための秘匿化処理、例えば、コンフィデンシャル・トランザクション、コンフィデンシャル・アセット等が施されているので、サイドチェーン上の取引内容が外部等に漏れることがなく、取引の安全が図られている。
【００１２】
　好ましくは、取引システムの前記仮想通貨及び前記法定通貨は、それぞれ、前記サイドチェーン上では、サイドチェーン上で使用可能なサイドチェーン用トークンに変換されて取引され、前記サイドチェーン用トークンは、前記検証サーバが、その発行を許可する構成となっており、前記サイドチェーン用トークンは、前記検証サーバが、その発行を許可する構成となっており、前記検証サーバは、前記サイドチェーンにおける前記取引情報の取引対象の交換価値の妥当性を判断することを特徴とする。
【００１３】
　前記構成によれば、仮想通貨及び法定通貨は、それぞれ、サイドチェーン上では、サイドチェーン上で使用可能なサイドチェーン用トークン（例えば、ビットコイントークン、円トークン等）に変換されて取引され、サイドチェーン用トークンは、監視部（例えば、監査端末、検証サーバ等）が、その発行を許可する構成となっている。
　したがって、サイドチェーンでは、監視部の許可なく取引ができず、取引の安全（セキュリテイ）が確保されている。
また、前記構成によれば、監視部（例えば、検証サーバ等）は、サイドチェーンにおける取引情報の取引対象の交換価値（例えば、ビットコイントークンと円トークンの交換価値等）の妥当性を判断する。
　したがって、例えば、ビットコイントークンと円トークンの交換価値が、市場における時価情報と著しく相違する場合は、不適切な取引として、取引を承認しない。
　このように。本発明では、サイドチェーンにおける不適切な内容の取引の成立も未然に防ぐことができる。
【００１４】
　好ましくは、取引システムの前記取引決済サーバは、前記仮想通貨を使用不可となるように、前記ブロックチェーンにロックし、複数の前記監査端末が、当該仮想通貨がロックされているか否かを検証し、前記監査端末が検証に成功すると、前記ブロックチェーンにロックされた当該仮想通貨と等価なサイドチェーン用トークンを前記サイドチェーンにア

ンロック又は新規発行することを特徴とする。
【００２２】
前記目的は、本発明によれば、複数のノードによって取引記録が保持され、これらによって構築されたネットワークで仮想通貨が管理されるブロックチェーンと、前記ブロックチェーンの側鎖であるサイドチェーンと、を有し、前記仮想通貨を取引する取引端末、取引を検証する検証サーバ、第三者機関である取引決済サーバを有する取引システムの制御方法であって、前記サイドチェーンでは、前記ブロックチェーンで管理される仮想通貨を管理できると共に、少なくとも、前記仮想通貨と法定通貨との交換を含む取引が可能な構成となっていると共に、前記サイドチェーンで実行された取引の結果情報は、前記ブロックチェーンに反映され、前記サイドチェーンにおける取引情報は、監査端末及び前記検証サーバが検証し、前記監査端末は、前記仮想通貨の取引の当事者として実際に機能していない前記取引端末から選択され、複数の前記取引端末が、前記サイドチェーンにおける取引に当事者として複数回、関与し、複数回の前記取引の結果情報が発生するときに、途中の前記取引の結果情報を省略し、最終の前記取引の結果情報のみを記憶するネッティング処理を行うと共に、前記ネッティング処理の前記最終の結果情報に基づき、当事者である各前記取引端末と第三者機関である取引決済サーバとの間のみの契約である取引情報を生成し、前記取引端末と前記取引決済サーバとの間の前記取引情報に基づいて、前記サイドチェーンで取引が実行される構成となっていることを特徴とする取引システムの制御方法により達成される。
【００２３】
前記目的は、本発明によれば、複数のノードによって取引記録が保持され、これらによって構築されたネットワークで仮想通貨が管理されるブロックチェーンと、前記ブロックチェーンの側鎖であるサイドチェーンと、前記仮想通貨を取引する取引端末、取引を検証する検証サーバ、第三者機関である取引決済サーバを有する取引システムに、前記サイドチェーンでは、前記ブロックチェーンで管理される仮想通貨を管理できると共に、少なくとも、前記仮想通貨と法定通貨との交換を含む取引が可能な構成となっていると共に、前記サイドチェーンで実行された取引の結果情報は、前記ブロックチェーンに反映される機能、前記サイドチェーンにおける取引情報は、監査端末及び前記検証サーバが検証する機能、複数の前記取引端末が、前記サイドチェーンにおける取引に当事者として複数回、関与し、複数回の前記取引の結果情報が発生するときに、途中の前記取引の結果情報を省略し、最終の前記取引の結果情報のみを記憶するネッティング処理を行う機能、前記ネッティング処理の前記最終の結果情報に基づき、当事者である各前記取引端末と第三者機関である取引決済サーバとの間のみの契約である取引情報を生成し、前記取引端末と前記取引決済サーバとの間の前記取引情報に基づいて、前記サイドチェーンで取引が実行される機能、を実現させるための取引システムの制御プログラムにより達成される。
【発明の効果】
【００２４】
以上説明したように、本発明は、仮想通貨と法定通貨との交換、又は仮想通貨を媒介通貨としての法定通貨間の交換を迅速且つ低コストで行うことができると共に、セキュリティの安全性や効率性も確保できる取引システム、取引システムの制御方法及び取引システムの制御プログラムを提供できるという利点がある。
【図面の簡単な説明】
【００２５】
【図１】本発明の「取引システム」の実施の形態である「ビットコイン（登録商標）取引システム１」を示す概略説明図である。
【図２】図１のインターネット網２等により提供されるプラットフォームにおける「ビットコイン」の「ブロックチェーン（メインチェーン）」と、その側鎖である「サイドチェーン」の概略説明図である。
【図３】図１の「取引決済サーバ２００」の主な構成を示す概略ブロック図である。
【図４】図３の「取引決済サーバ側第１の各種情報記憶部２１０」の主な構成を示す概略

ブロック図である。
【図５】図３の「取引決済サーバ側第２の各種情報記憶部２２０」の主な構成を示す概略ブロック図である。
【図６】図３の「取引決済サーバ側第２の各種情報記憶部２３０」の主な構成を示す概略ブロック図である。
【図７】図１の「検証サーバ１００」の主な構成を示す概略ブロック図である。
【図８】図７の「検証サーバ側第１の各種情報記憶部１１０」の主な構成を示す概略ブロック図である。
【図９】図７の「検証サーバ側第２の各種情報記憶部１２０」の主な構成を示す概略ブロック図である。
【図１０】図１の取引端末１０Ａ、１０Ｂ、１０Ｃ等の主な構成を示す概略図である
【図１１】図１の「取引端末」のうち、本実施の形態で「監査端末」として機能する図１の「取引端末１０Ｄ（Ｅ，Ｆ、Ｇ）」を示す概略ブロック図である。
【図１２】取引端末１０Ａ乃至１０Ｃが、それぞれ、「ビットコイン」の取引希望の情報を発信した場合に、図１の「取引決済サーバ２００」が「マッチング処理」や「ネッティング処理」等を行う工程を示す概略フローチャートである。
【図１３】取引端末１０Ａ乃至１０Ｃが、それぞれ、「ビットコイン」の取引希望の情報を発信した場合に、図１の「取引決済サーバ２００」が「マッチング処理」や「ネッティング処理」等を行う工程を示す他の概略フローチャートである。
【図１４】確定した「取引決済サーバ２００」と各「取引端末１０Ａ」等との個々の契約（取引）を、本システム１のプラットフォームを利用して実行する工程を示す概略フローチャートである。
【図１５】確定した「取引決済サーバ２００」と各「取引端末１０Ａ」等との個々の契約（取引）を、本システム１のプラットフォームを利用して実行する工程を示す他の概略フローチャートである。
【図１６】確定した「取引決済サーバ２００」と各「取引端末１０Ａ」等との個々の契約（取引）を、本システム１のプラットフォームを利用して実行する工程を示す他の概略フローチャートである。
【図１７】確定した「取引決済サーバ２００」と各「取引端末１０Ａ」等との個々の契約（取引）を、本システム１のプラットフォームを利用して実行する工程を示す他の概略フローチャートである。
【図１８】確定した「取引決済サーバ２００」と各「取引端末１０Ａ」等との個々の契約（取引）を、本システム１のプラットフォームを利用して実行する工程を示す他の概略フローチャートである。
【図１９】確定した「取引決済サーバ２００」と各「取引端末１０Ａ」等との個々の契約（取引）を、本システム１のプラットフォームを利用して実行する工程を示す他の概略フローチャートである。
【発明を実施するための形態】
【００２６】
以下、この発明の好適な実施の形態を添付図面等を参照しながら、詳細に説明する。
尚、以下に述べる実施の形態は、本発明の好適な具体例であるから、技術的に好ましい種々の限定が付されているが、本発明の範囲は、以下の説明において特に本発明を限定する旨の記載がない限り、これらの態様に限られるものではない。
【００２７】
図１は、本発明の「取引システム」の実施の形態である「ビットコイン（登録商標）取引システム１」を示す概略説明図である。
図１に示すように、本システム１は、取引対象であり仮想通貨である例えば、「ビットコイン」の取引所１０Ａ乃至取引所１０Ｇ等が有する取引端末１０Ａ乃至取引端末１０Ｇを有している。
これら、取引端末１０Ａ等は、それぞれ地理的に離間して配置され、例えば、取引端末

１０Ａは東京、取引端末１０Ｂは、大阪、取引端末１０Ｇはロンドン等に配置されている。
【００２８】
そして、これら取引端末１０Ａ等は、図１に示すようにインターネット網２により、相互に通信可能な構成となっている。
また、インターネット網２には、図１に示すように、監視部である例えば、「検証サーバ１００」と、第三者機関である例えば、「取引決済サーバ２００」も通信可能となっている。
【００２９】
また、図１に示すように、取引端末Ａ等は、「ビットコイン」の取引の当事者として機能する場合の他、後述する「監査端末１０Ａ等」としても機能する構成となっている。
【００３０】
図２は、図１のインターネット網２等により提供されるプラットフォームにおける「ビットコイン」の「ブロックチェーン（メインチェーン）」と、その側鎖である「サイドチェーン」の概略説明図である。
現在、ビットコインの取引価格や流通量は、取引所等によってばらつきがあり、均衡がとれておらず、ビットコインの取引の共通取引基盤や共通決済基盤がない。
このため、本実施の形態の本システム１は、ビットコインの取引の共通基盤を提供するものである。
【００３１】
また、図１の「ブロックチェーン（メインチェーン）」は、仮想通貨であるビットコインの取引履歴を管理する分散型台帳の一種である。
ブロックチェーンのネットワークは、マイナーと呼ばれる不特定多数のノードにより形成され、各ノードがトランザクションを検証して検証結果の合意を形成し、ブロックチェーン上の取引履歴を更新する。
なお、本発明において、仮想通貨は、ビットコインに限定されず、イーサリアム（登録商標）等のアルトコインであっても構わない。
【００３２】
図２に示すように、本実施の形態では、メインチェーンは、その側鎖となるブロックチェーンである「サイドチェーン」を有している。
この「サイドチェーン」は、後述するように、「メインチェーン」とは異なる「アルゴリズム」で動作するネットワークであるが、「メインチェーン」と「サイドチェーン」との間では、後述するように、「双方向ペグ（Ｔｗｏ－ｗａｙ　Ｐｅｇ）」が可能な構成となってなっている。
すなわち、「メインチェーン」上で管理されている「ビットコイン」と「サイドチェーン」上で管理されている「サイドチェーン用トークン」とを相互に交換することができる。
【００３３】
サイドチェーンの動作のアルゴリズムは、特に限定しないが、本実施の形態に係るサイドチェーンは、「ストロング・フェデレーションズ（Ｓｔｒｏｎｇ　Ｆｅｄｅｒａｔｉｏｎｓ）と呼ばれるアルゴリズムで動作する。
「ストロング・フェデレーションズ」は、ネットワーク上に地理的及び管轄的に分散して配置された複数の監査端末が、サイドチェーン上のトランザクションの検証動作を実行すると共に、「メインチェーン」との間の「ビットコイン」の双方ペグの検証動作を実行する。
【００３４】
本実施の形態では、図１の取引端末１０Ａ等が、監査端末としても機能する構成となっている。
この検証は、「ｋ－ｏｆ－ｎ」の「マルチシグネチャースキーム」（複数の秘密鍵が必要とされ、そのうち一定数の秘密鍵が要求される）のアルゴリズムで実行される。
「メインチェーン」では「Ｐｏｗ（Ｐｒｏｏｆ　ＯＦ　Ｗｏｒｋ）」により「マイナー」の合意形成を行うが、「サイドチェー」ンでは「マルチシグネチャ」に置き換えることで

、メインチェーンのセキュリテイを維持しつつ、時間的遅延を生じ難くする構成となっている。

【００３５】

また、「メインチェーン」でも実装されているマルチシグネチャ技術によって双方向ペグを行うことで、メインチェーンの仕様を変更せずとも、双方向ペグが可能となっている。

本実施の形態では、「サイドチェーン」上に、「監査端末１０Ａ等」に加え、検証者の「検証サーバ１００」及び「取引決済サーバ２００」が通過交換取引を検証するプラットフォームを構築する。

【００３６】

本プラットフォーム上では、検証サーバの承認を得ずに取引を行うことができないように構成されている。検証サーバは、取引者のＩＤ等の確認等を行うが、法規制の観点から取引内容のチェックを行い、法令等に違反する取引には承認を与えないとの機能も発揮する。

【００３７】

また、図１の取引端末１０Ａ等、検証サーバ１００及び取引決済サーバ２００等は、コンピュータを有し、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）やハードディスク等を有し、バスを介して接続されている。

【００３８】

図３は、図１の「取引決済サーバ２００」の主な構成を示す概略ブロック図である。

図３に示すように、取引決済サーバ２００は、取引決済サーバ側制御部２０１を有し、同制御部２０１は、他の装置等と通信する「取引決済サーバ側通信装置２０２」、各種情報を表示する「取引決済サーバ側ディスプレイ２０３」、そして各種情報を入力する「取引決済サーバ側各種情報入力装置２０４」を制御する。

また、同制御部２０１は、図３の「取引決済サーバ側第１の各種情報記憶部２１０」、「取引決済サーバ側第２の各種情報記憶部２２０」及び「取引決済サーバ側第２の各種情報記憶部２３０」を制御する。

【００３９】

図４乃至図６は、それぞれ、図３の「取引決済サーバ側第１の各種情報記憶部２１０」、「取引決済サーバ側第２の各種情報記憶部２２０」及び「取引決済サーバ側第２の各種情報記憶部２３０」の主な構成を示す概略ブロック図である。

これらの内容については、後述する。

【００４０】

図７は、図１の「検証サーバ１００」の主な構成を示す概略ブロック図である。

図７に示すように、検証サーバ１００は、検証サーバ側制御部１０１を有し、同制御部１０１は、他の装置等と通信する「検証サーバ側通信装置１０２」、各種情報を表示する「検証サーバ側ディスプレイ１０３」、そして各種情報を入力する「検証サーバ側各種情報入力装置１０４」を制御する。

また、同制御部１０１は、図７の「検証サーバ側第１の各種情報記憶部１１０」及び「検証サーバ側第２の各種情報記憶部１２０」を制御する。

【００４１】

図８及び図９は、それぞれ、図７の「検証サーバ側第１の各種情報記憶部１１０」及び「検証サーバ側第２の各種情報記憶部１２０」の主な構成を示す概略ブロック図である。

これらの内容については、後述する。

【００４２】

図１０は、図１の取引端末１０Ａ、１０Ｂ、１０Ｃ等の主な構成を示す概略図である。本実施の形態では、後述のように、取引端末１０Ａ乃至取引端末１０Ｃが、「ビットコイン」の取引の当事者として機能し、図１の取引端末１０Ｄ乃至取引所１０Ｇが、「監査端末」として機能する。

なお、本実施の形態では、説明の便宜上、４つの監査端末で説明するが、本発明におけ

る監査端末は、これに限らず適切な数の監査端末が求められる。
　また、監査端末は、その数が多いほど、セキュリテイは高くなり、その数が少なくなるほど、処理速度が速くなる。
　このため、両者のバラスをとるように、監視端末の数を適切に定める。
　「取引端末」として機能するのは、取引端末１０Ａ、１０Ｂ、１０Ｃであるが、これらは同一の構成のため、以下「取引端末１０Ｃ」についてのみ説明する。
【００４３】
　図１０は、図１の「取引端末１０Ｃ（Ａ、Ｂ）」の主な構成を示す概略ブロック図である。
　図１０に示すように、取引端末１０Ｃは、取引端末側制御部１１Ｃを有し、同制御部１１Ｃは、他の装置等と通信する「取引端末側通信装置１２Ｃ」、各種情報を表示する「取引端末側ディスプレイ１３Ｃ」、そして各種情報を入力する「取引端末側各種情報入力装置１４Ｃ」を制御する。
　また、同制御部１１Ｃは、図１０の「Ｃ取引端末側鍵情報記憶部１５Ｃ」及び「取引端末側各種情報記憶部１６Ｃ」も制御する。
　このうち、「Ｃ取引端末側鍵情報記憶部１５Ｃ」については、後述する。
【００４４】
　図１１は、図１の「取引端末」のうち、本実施の形態で「監査端末」として機能する図１の「取引端末１０Ｄ（Ｅ，Ｆ、Ｇ）」を示す概略ブロック図である。
　以下、監査端末１０Ｄ（Ｅ，Ｆ、Ｇ）」として説明する。
　「監査端末」として機能するのは、監査端末１０Ｄ乃至監査端末１０Ｇであるが、これらは同一の構成のため、以下「監査端末１０Ｄ」についてのみ説明する。
【００４５】
　図１１に示すように、監査端末１０Ｄは、「監査端末側制御部１１Ｄ」を有し、同制御部１１Ｄは、他の装置等と通信する「監査端末側通信装置１２Ｄ」、各種情報を表示する「監査端末側ディスプレイ１３Ｄ」、そして各種情報を入力する「監査端末側各種情報入力装置１４Ｄ」を制御する。
　また、同制御部１１Ｄは、図１１の「監査端末側鍵情報記憶部１５Ｄ」及び「監査端末検証部１７Ｄ」も制御する。
　これら「監査端末側鍵情報記憶部１５Ｄ」及び「監査端末検証部１７Ｄ」の内容については、後述する。
【００４６】
　図１２乃至図１９は、本システム１の主な動作例を示す概略フローチャートである。
　本実施の形態では、図１の「取引端末１０Ａ」「取引端末Ｂ」及び「取引端末Ｃ」が、それぞれ「ビットコイン」に関する取引を希望し、図１の「取引端末１０Ｄ」乃至「取引端末１０Ｇ」が「監査端末」として機能する例で、以下、説明する。
【００４７】
　図１２及び図１３は、取引端末１０Ａ乃至１０Ｃが、それぞれ、「ビットコイン」の取引希望の情報を発信した場合に、図１の「取引決済サーバ２００」が「マッチング処理」や「ネッティング処理」等を行う工程を示す概略フローチャートである。
【００４８】
　本システム１の利用を希望する取引端末１０Ａ等は、図１の「決済サーバ２００」からプログラムをインストールする。
　具体的には、各取引端末１０Ａ等が取引のマッチングやコミュニケーション、及びトランザクションの生成等を実行するツールとしての機能するプログラムである。
　これにより、取引端末１０Ａ等は、当該プログラムを用いて、本システム１のプラットフォームにおいて、「ビットコイン」の取引の相手方を検索し、取引情報である例えば、取引内容（取引価格、取引量等）の交渉を行い、相手方と合意した場合、取引端末１０Ａ等は、本システム１を利用してく「ビットコイン」の交換等を実行する。
【００４９】

また、本システム１の利用を希望する取引端末１０Ａ等は、取引上、資金不足等が生じた場合に備えて「担保金」等を「取引決済サーバ２００」を管理する「取引決済所」に預ける等の対策を講じる。
これにより、取引端末１０Ａ等は、「取引決済サーバ２００」を含む本システム１を利用することが可能となる。
【００５０】
以下、図１２乃至図１３のフローチャートに沿って以下、説明する。
先ず、図１２のステップ（以下「ＳＴ」という。）１へ進む。
ＳＴ１では、各取引端末１０Ａ等から「ビットコイン」と「円」との交換の具体的な条件情報が、「取引決済サーバ２００」に送信される。
【００５１】
次いで、ＳＴ２へ進む。ＳＴ２では、「取引決済サーバ２００」は、各取引端末１０Ａ等の条件情報を「取引決済サーバ２００」の図４の「条件情報記憶部２１１」に記憶する。
例えば、１）取引端末Ａの条件情報は「１ビットコイン」を「１００万円」で購入したいことと「１ビットコイン」を「１１０万円」で売却したいことである。
また、２）「取引端末１０Ｂ」の条件情報は、「２ビットコイン」を「１８０万円」で購入したいことと、「１ビットコイン」を「１００万円」で売却したいこと、である
さらに、３）「取引端末１０Ｃ」の条件情報は、「１ビットコイン」を「１１０万円」で購入したことと、「２ビットコイン」を「１８０万円」で売却したいことである。
【００５２】
次いで、ＳＴ３へ進む。ＳＴ３では、「取引決済サーバ２００」の図４の「マッチング処理部（プログラム）２１２」が動作し、所定の時間内（例えば、９時から１１時等）での実行を希望する「ビットコイン」と、法定通貨である例えば、「円」との交換取引条件が一致する取引端末１０Ａ等との組み合わせを探し、図４の「マッチング結果記憶部２１３」に記憶する。
【００５３】
例えば、取引端末１０Ａが「１ビットコイン」を取引端末Ｂに「１１０万円」で売却、取引端末１０Ａが取引端末１０Ｃから「１ビットコイン」を「１００万円」で購入、取引端末１０Ｂが、取引端末１０Ｃから「２ビットコイン」を「１８０万円」で購入する。
このように、「取引端末１０Ａと取引端末Ｂの契約」、「取引端末１０Ｂと取引端末１０Ｃの契約」及び「取引端末１０Ｃと取引端末１０Ａの契約」を候補として選択し、「マッチング結果記憶部２１３」に記憶する。
【００５４】
次いで、ＳＴ４へ進む。ＳＴ４では、「マッチング結果記憶部２１３」の契約内容について、各契約当事者である取引端末１０Ａ等に同意を求め、取得する。
【００５５】
このように、契約毎に、各取引所Ａ等が契約内容を実行するとき、各取引所Ａ等は、契約内容に合致した「ビットコイン」や「円」を、その契約毎に用意する必要がある。
例えば、上述の例では、取引端末１０Ａは、１０Ｃに「１１０万円」を提供する契約であるが、取引端末Ｂとの契約で、Ｂから「１００万円」取得することになる。
【００５６】
この場合、取引所Ａが、先に取引所Ｃとの契約を実行するときに、１１０万を所持せず、１０万円のみ所持している場合、短期の借入で「１００万円」を借り、取引所Ｂとの契約で「１００万円」取得した後、「１００万円」を返済することになる。
これでは、迅速な取引が困難となるという問題がある。
【００５７】
そこで、本実施の形態では、各契約を、それぞれ実行するのではなく、各取引所の最終的な「ビットコイン」や「円」の取得内容や提供内容を計算し途中の各取引を省略する「ネッティング」という処理を以下のように実行する。
【００５８】

ＳＴ５では、図４の「ネッティング契約処理部２１４」が動作し、「マッチング結果記憶部２１３」の取引端末１０Ａ、１０Ｂ及び１０Ｃ３つの契約をそれぞれ実行するのではなく、取引端末１０Ａ、１０Ｂ及び１０Ｃと「取引決済サーバ２００」がそれぞれ、契約することで、１回の契約で、取引端末１０Ａ、１０Ｂ及び１０Ｃが最終的に取得又は提供する「ビットコイン」及び／又は「円」を取得及び／又は提供することができる契約組み合わせ情報を生成する。

【００５９】

具体的には、上述の例で、取引端末１０Ａ、１０Ｂ及び１０Ｃ間では、最終的には、１）取引端末１０Ｃが１０Ｂに「１ビットコイン」を提供し、２）取引端末１０Ｂは、取引端末１０Ａに１００万円を提供すると共に取引端末Ｃには、７０万円提供することになる。

そして、この「ネッティング契約処理」が行われた結果情報を、図５の「ネッティング契約処理結果情報記憶部２２１」に記憶する。

【００６０】

しかし、図５の「ネッティング契約処理結果情報記憶部２２１」の契約内容では、例えば、取引端末１０Ｂの取引所１０Ｂが１７０万円、用意できないときは、すべて契約が不履行となり、実行することができないという問題が生じる。

そこで、本実施の形態では、「取引決済サーバ２００」の図６の「セントラルカウンターパーティ契約処理部（プログラム）２３４」が動作し、図５の「ネッティング契約処理結果情報記憶部２２１」に記憶されている「ネッティング契約処理結果情報」の契約当事者を、それぞれ「取引決済サーバ２００」との契約に変更し、図５の「セントラルカウンターパーティ契約処理結果情報記憶部２２２」に記憶させる。

【００６１】

具体的には、上述の例では、１）取引決済サーバ２００が取引端末１０Ａに「１０万円」提供する契約、２）取引決済サーバ２００が取引端末１０Ｂに「１ビットコイン」を」提供する契約、３）取引決済サーバ２００が取引端末１０Ｃに「１ビットコイン」を提供すると共に、取引端末１０Ｃは、取引決済サーバ２００に「７０万円」提供する契約とする。

【００６２】

このように、契約主体に「取引決済サーバ２００」を組み込むことで、契約当事者のいずれかが契約内容を履行できない場合でも、すべての契約が不履行となるのではなく、当該不履行が生じた「取引決済サーバ」との契約のみが不履行となり、他の「取引決済サーバ２００」との契約は履行されることなる。

また、これら「セントラルカウンターパーティ契約処理結果情報記憶部２２２」の契約は、ネッティング契約処理されているため、各当事者が、上述のネッティング前の契約で履行に必要な法定通貨（円）の全額等を履行時に用意する必要がないので、取引を迅速に行うことができる。

【００６３】

なお、本実施の形態では、図４の「ネッティング契約処理部２１４」が動作し、さらに図６の「セントラルカウンターパーティ契約処理部２３４」が動作する例で説明したが、これらを分けることなく、一括処理しても構わない。

また、取引を急ぐときは、図１乃至図７の処理を省略しても構わない。

【００６４】

次いで、ＳＴ７へ進む。ＳＴ７では、「取引決済サーバ２００」は、契約の相手方となる取引端末１０Ａ等の支払い能力や担保金等を確認し、かかる「セントラルカウンターパーティ契約」について、契約の相手方である取引端末１０Ａ等の「同意」を取得する。

【００６５】

以上で、図１のメインチェーンとサイドチェーンを利用して、実行すべき具体的な取引（契約）が確定する。

また、上述のように、「取引決済サーバ２００」と、各取引端末１０Ａ、１０ＢＣ及び１０Ｃとの契約（取引）としたことで、迅速且つ安全な取引を保証することができる。

【００６６】
なお、これらの取引内容には、例えば取引対象である仮想通貨（ビットコイン）、法定通貨の種類（円）、法定通貨（円）に対する仮想通貨（ビットコイン）の価格に相当する取引価格、通貨の取引量（交換量）の他、取引を行う日時、取引を行う取引端末ＩＤ等の情報が含まれる。
【００６７】
図１４乃至図１９は、上述の工程で、確定した「取引決済サーバ２００」と各「取引端末１０Ａ」等との個々の契約（取引）を、本システム１のプラットフォームを利用して実行する工程を示す概略フローチャートである。
【００６８】
取引内容について合意した場合、取引決済サーバ２００、取引端末１０Ａ、１０Ｂ及び１０Ｃは、それぞれ合意した取引内容に従って処理を行う。
具体的には、上述の例では、１）取引決済サーバ２００が取引端末１０Ａに「１０万円」提供する契約、２）取引決済サーバ２００が取引端末１０Ｂに「１ビットコイン」を」提供する契約、３）取引決済サーバ２００が取引端末１０Ｃに「１ビットコイン」を提供すると共に、取引端末１０Ｃは、取引決済サーバ２００に「７０万円」提供する契約となる。
【００６９】
以下、図１４乃至図１９のフローチャートに沿って説明するが、先ず、「取引決済サーバ２００」が「取引端末１０Ｃ」に「１ビットコイン」を提供すると共に、「取引端末１０Ｃ」が、「取引決済サーバ２００」に「７０万円」を提供する契約の工程について、説明する。
【００７０】
図１４のＳＴ１１では、取引決済サーバ２００は、所有する仮想通貨である例えば、「１ビットコイン」を「メインチェーン」から「サイドチェーン」に移動させるための動作を実行する。
すなわち、取引決済サーバ２００は、取引決済サーバ２００の特定の「１ビットコイン」を、使用不可となるように「ロック（凍結）」するため以下の動作を行う。
【００７１】
具体的には、図５の「ロック用マルチシグアドレス生成部（プログラム）２２３」が動作し、取引決済サーバ２００は、複数の監査端末Ｄ等（例えば、取引端末Ｄ等）の図１１の「監査端末側鍵情報記憶部１５Ｄ」の公開鍵と、取引決済サーバ２００の「取引決済サーバ側鍵情報記憶部２２４」（図５）の公開鍵とを用いて、メインチェーン上で、「１ビットコイン」をロックするための「ロック用マルチシグアドレス」を生成し、「ロック用マルチシグアドレス記憶部」に記憶する。
【００７２】
ここで「マルチシグアドレス」は、トランザクションの署名に複数の鍵を必要とする技術をいう。
また、このとき、取引決済サーバ２００は、楕円曲線の準同型性を利用して、各監査端末の公開鍵から新たな公開鍵を生成し、生成した公開鍵を用いて「マルチシグアドレス」を生成する。
【００７３】
次いで、ＳＴ１２へ進む。ＳＴ１２では、取引決済サーバ２００の「ロッキングトランザクション生成部（プログラム）２３１」（図６）が動作し、図５の「ロック用マルチシグアドレス記憶部２２５」の「ロック用マルチシグアドレス」に「１ビットコイン」をデポジットした「ロッキングトランザクション」を生成し、図６の「ロッキングトランザクション記憶部２３２」に記憶する。
【００７４】
次いで、ＳＴ１３へ進む。ＳＴ１３では、取引決済サーバ２００は、図６の「ロッキングトランザクション記憶部２３２」のロッキングトランザクションをメインチェーンのネ

ットワークに送信する。
　これにより、メインチェーンに当該１ビットコインがロックされる。
【００７５】
　また、メインチェーンの「ビットコイン」は、監査端末１０Ｄ等が電子署名を入力しなければ「アンロック」することができず、使用不可の状態となる。
【００７６】
　次いで、ＳＴ１４へ進む。ＳＴ１４では、取引決済サーバ２００の「ビットコイントークン要求部（プログラム）２３３」（図６）が動作し、取引決済サーバ２００は、図６の「ロッキングトランザクション記憶部２３２」の「ロッキングトランザクション」情報と、図５の「ロック用マルチシグアドレス記憶部２２５」の「ロック用マルチシグアドレス」生成時に使用した取引決済サーバ２００の公開鍵等の情報を「監査端末１０Ｄ等」に送信し、取引決済サーバ２００のサイドチェーンのアドレス宛に、取引対象であり、サイドチェーン用トークンである例えば、「ビットコイントークン」の送信を求める。
【００７７】
　次いで、ＳＴ１５へ進む。ＳＴ１５では、監査端末１０Ｄ等は、図１１の「監査端末側鍵情報記憶部１５Ｄ」の監査端末１０Ｄ等の秘密鍵と、図５の「取引決済サーバ側鍵情報記憶部２２４」の公開鍵等の情報を用いて、メインチェーンに当該「ビットコイン」がロックされているか否かを検証する。
【００７８】
　次いで、ＳＴ１６へ進む。ＳＴ１６では、サイドチェーンで用いられているアルゴリズムである「ストロング・フェデレーションズ」では、複数の監査端末１０Ｄ等のうち、適切な数の監査端末１０Ｄ等が検証に成功したか否かを判断する。
【００７９】
　そして、ＳＴ１７へ進む。ＳＴ１７では、適切な数の監査端末１０Ｄ等が、検証に成功すると、「ペグイン」が承認され、メインチェーンにロックされた「１ビットコイン」と等価な「１ビットコイントークン」をサイドチェーンでアンロック又は新規発行され、取引決済サーバ２００のアドレスへ当該情報を送信する。
【００８０】
　次いで、ＳＴ１８へ進む。ＳＴ１８では、「取引決済サーバ２００」は、上記で取得した「１ビットコイントークン」を保持する「ＵＴＸＯ」の情報を「検証サーバ１００」に送信し、図８の「取引データベース１１１」に、対応する「１ビットコイン」と対応付けて登録する。
【００８１】
　したがって、「ＵＴＸＯ」に登録された「１ビットコイントークン」を「取引決済サーバ２００」が、「検証サーバ１００」に無断で、使用した場合、「検証サーバ１００」は、トランザクションの検証時に取引を承認せず、そのトランザクションを無効とすることができる。
【００８２】
　次いで、ＳＴ１９へ進む。ＳＴ１９では、「取引端末１０Ｃ」は、金融振込等の手段で法定通貨（７０万円）を検証サーバ１００を管理する検証人又は円トークン発行人に送金し、サイドチェーンで取引履歴が管理される「サイドチェーン用トークン」である例えば、「７０万円トークン」を発行するように検証サーバに要求する。
【００８３】
　なお、本実施の形態では、「検証サーバ１００」が、取引の検証及び円トークンの発行の両方を行うものとして説明したが、本発明では、円トークンの発行主体が、「検証サーバ２００」と異なっても構わない。
【００８４】
　次いで、ＳＴ２０へ進む。ＳＴ２０では、図８の「検証サーバ側マルチシグアドレス生成部（プログラム）１１２」が動作し、図１０の「Ｃ取引端末側鍵情報記憶部１５Ｄ」の取引端末１０Ｃの公開鍵と、図８の「検証サーバ側鍵情報記憶部１１３」の検証サーバの

公開鍵を用いて、取引端末１０Ｃと検証サーバ２００の電子署名の入力を解除条件としたマルチシグアドレスを生成し、図８の「検証サーバ側マルチシグアドレス記憶部１１４」に記憶する。

【００８５】

次いで、ＳＴ２１へ進む。ＳＴ２１では、図８の「検証サーバ側トランザクション生成部（プログラム）１１５」が動作し、図８の「検証サーバ側マルチシグアドレス記憶部１１４」のマルチシグアドレスに「７０万円トークン」をデポジットしたトランザクションを生成し、サイドチェーンのネットワークにブロードキャストする。

【００８６】

これにより、本プラットフォーム上で、「７０万円トークン」は「検証サーバ１００」の承認（署名）を得なければ使用することができない状態となる。

【００８７】

次いで、ＳＴ２２へ進む。ＳＴ２２では、「検証サーバ１００」は、「取引端末１０Ｃ」が「７０万円トークン」を保持する旨の「ＵＴＸＯ」の情報を、図９の「取引データベース１２１」に登録する。

【００８８】

この後、「取引決済サーバ２００」は、取得した「１ビットコイントークン」と「取引端末１０Ｃ」の「７０万円トークン」とを交換するトランザクションを生成し、サイドチェーンのネットワークにブロードキャストすることとなる。

しかし、この場合、「取引決済サーバ２００」は、トランザクションを生成して、取引端末Ｃにトークンを送るだけでは、「取引端末１０Ｃ」の不正行為によって交換が成立しないおそれがある。

【００８９】

そこで、本実施の形態では、このような事態に備えて、取引決済サーバと取引端末Ｃは、「デリバリー・バーサス・ペイメント・スワップ（Ｄｅｌｉｖｅｒｙ Ｖｅｒｓｕｓ Ｐａｙｍｅｎｔ Ｓｗａｐ）（ビットコイントークンと円トークンを相互に条件付けて、一方が行なわれない場合、他方も行われないようにすること）によるトークンの交換を行う。（以下、「ＤＶＰスワップ」という。）

【００９０】

「ＤＶＰスワップ」は、互いの信頼関係を不要としながらも、第３者（仲介者）を介さず相対取引でビットコイ等の仮想通貨と「円トークン」の交換を可能とする手法である。

したがって、サイドチェーン上で取引を行う端末の当事者同士について、互いに信頼関係がなくても、第３者である仲介者等を介することなく、相対取引を安心して行うことができる。

【００９１】

以下、「ＤＶＰスワップ」について説明する

本実施の形態では、「取引決済サーバ２００」が、「取引決済サーバ２００」と「取引端末１０Ｃ」のそれぞれの公開鍵を用いて「マルチシグアドレス」を生成し、当該マルチシグアドレスを使用して「１ビットコイントークン」及び「７０万円トークン」をデポジットしたトランザクションを生成する。

【００９２】

そして、「取引決済サーバ２００」と「取引端末１０Ｃ」は、それぞれ、当該トランザクションに「取引決済サーバ２００」と「取引端末１０Ｃ」のそれぞれの電子署名を入力（付加）して、ブロードキャストする。

具体的には、以下のとおりである。

【００９３】

ＳＴ２４では、「取引決済サーバ１００」は、図５の「取引決済サーバ側鍵情報記憶部２２４」と図１０の「Ｃ取引端末側鍵情報記憶部１３Ｃ」の取引決済サーバ２００及び取引端末１０Ｃの公開鍵を用いて、取引決済サーバ２００及び取引端末１０Ｃの電子署名の入力を解除条件とし、出力先を「取引端末１０Ｃ」のアドレスとした「１ビットコイント

ークン」のアウトプットをトランザクションとして格納する。
【００９４】
次いで、ＳＴ２５へ進む。ＳＴ２５では「取引決済サーバ２００」は、図５の「取引決済サーバ側鍵情報記憶部２２４」、図１０の「Ｃ取引端末側鍵情報記憶部１３Ｃ」及び図８の「検証サーバ側鍵情報記憶部１１３」の取引決済サーバ２００、取引端末１０Ｃ及び検証サーバ１００」、それぞれの公開鍵を用いて、三者の電子署名の入力を解除条件とし、出力先を「取引決済サーバ２００」のアドレス又は取引決済サーバ２００と検証サーバ１００の「マルチシグアドレス」とした「７０万円トークン」のアウトプットをトランザクションに格納する。
【００９５】
上述のトランザクションを生成する際に、「取引決済サーバ２００」は、当該トランザクションで交換される「１ビットコイントークン」と「７０万円トークン」の種類や数量、すなわち、取引内容を第三者から秘匿化するため、当事者以外では閲覧できないよう暗号化したトランザクションを生成する。
【００９６】
具体的には、取引決済サーバ２００」は、秘匿化処理である例えば、「コンフィデンシャル・トランザクション（Ｃｏｎｆｉｄｅｎｔｉａｌ　Ｔｒａｎｓａｃｔｉｏｎ）」、及び「コンフィデンシャル・アセット（Ｃｏｎｆｉｄｅｎｔｉａｌ　Ａｓｓｅｔｓ）」と呼ばれる手法を用いて、取引内容を暗号化したトランザクションを生成する。
【００９７】
したがって、サイドチェーン上の取引内容が漏れることなく、取引の安全を図ることができることになる。
【００９８】
以下、取引量の暗号化を行う「コンフィデンシャル・トランザクション」について説明する。
コンフィデンシャル・トランザクションは、ブロックチェーンにより公開される「ビットコイントークン」及び「円トークン」の取引量を秘匿化する手法であり、準同型暗号を利用して取引量を暗号化する手法である。
【００９９】
コンフィデンシャル・トランザクションでは「Ｐｅｄｅｒｓｅｎ　Ｃｏｍｍｉｔｍｅｎｔ」を用い、取引量（ａ）を以下の式（１）で示すコミットメントＣ（ａ）で表現する。
コミットメントＣ（ａ）＝ｘＧ＋ａＨ・・・（１）
ｘは、当事者が共有する秘密鍵（ｂｌｉｎｄｉｎｇ　ｆａｃｔｏｒ）、Ｇ及びＨは、楕円曲線上のベースポイント（離散対数点）である。
【０１００】
式（１）で示すように、通常の楕円曲線暗号において秘密鍵を公開鍵に変換するベースポイント（Ｇ）のほかに、取引量（ａ）を暗号化するためのベースポイント（Ｈ）を追加することで、コミットメントＣ（ａ）を生成する。
コンフィデンシャル・トランザクションでは、トランザクションに格納される各インプット及びアウトプットの数量をコミットメントＣ（ａ）で表し、数量の代わりにコミットメントＣ（ａ）を各インプット及びアウトプットのスクリプトに記述する。
【０１０１】
コミットメントＣ（ａ）は、加法特性を有し、複数のコミットメントＣ（ａ）の総和は、コミットされる取引量（ａ）の総和のコミットメントＣ（ａ）に等しくなる。
例えば、Ｃ（１）＋Ｃ（１）＝Ｃ（２）の関係が成り立つ。
したがって、各インプットのコミットメントＣ（ａ）の総和から各アウトプットのコミットメントＣ（ａ）の総和を差し引いて０になるかをチェックすることで、取引量（ａ）を検証することができる。
これにより、秘密鍵（ｘ）を知る当事者は、取引量（ａ）を知ることができる一方、第三者は、取引量（ａ）を知ることができない。

【０１０２】
なお、コンフィデンシャル・トランザクションでは、さらにコミットされる取引量（ａ）が０以上であることを証明するためにリング署名等レンジプルーフを用いる。
【０１０３】
次に、取引量に加えて取引する「トークン」等の種類（アセットタイプ）を秘匿化する「コンフィデンシャル・アセット」について説明する。
コンフィデンシャル・アセットは、コンフィデンシャル・トランザクションを応用した手法であり、取引量に加えて、取引する「ビットコイントークン」「円トークン」の種類（アセットタイプ）を秘匿化する手法である。
【０１０４】
コンフィデンシャル・アセットでは、「ビットコイントークン」等の種類ごとに異なるベースポイントを用いてコミットメントを計算する。
例えば、取引量（ａ）（ｂ）である２種類の「ビットコイントークン」「円トークン」を想定した場合、取引量（ａ）の「ビットコイントークン」等のコミットメントＣ（ａ）が、式（１）で計算すると共に、取引量（ｂ）の「ビットコイントークン」等のコミットメントＣ（ｂ）は、次の式（２）で計算する。
【０１０５】
Ｃ（ｂ）＝ｘＧ＋ｂＩ・・・（２）
「Ｉ」と「Ｈ」は、同様に楕円曲線上のベースポイントである。
式（１）、（２）を比較するとわかるように、コンフィデンシャル・アセットでは、「ビットコイントークン」等の種類に応じて異なるベースポイントＨ、Ｉを選択してコミットメントＣ（ａ）、Ｃ（ｂ）を計算する。
【０１０６】
そして、各インプット及びアウトプットの数量としてコミットメントＣ（ａ）、Ｃ（ｂ）を記述とすると共に、「ビットコイントークン」等の種類に応じたベースポイントＨ、Ｉを各コミットメントＣ（ａ）、Ｃ（ｂ）にラベル付けする。
【０１０７】
これにより、取引量（ａ）（ｂ）は秘匿化される。
ただし、ベースポイントＨを固定値としては、「ビットコイントークン」等の種類が分ってしまうため、コンフィデンシャル・アセットでは、次の式（３）のように、ベースポイントＨをＡに置き換える。
Ａ＝Ｈ＋ｒＧ・・・（３）
ｒは、当事者のみが知る秘密の欄数値である。ベースポイントＨをＡに置き換えた場合、式（１）は、次の式（４）で表される。
Ｃ（ａ）＝ｘＧ＋ａＡ＝ｘＧ＋ａ（Ｈ＋ｒＧ）＝（ｘ＋ｒａ）Ｇ＋ａＨ・・・（４）
式（１）、（４）を比較すると分かるように、秘密鍵ｘは（ｘ、ｒ）に置き換わる。
【０１０８】
乱数値ｒを知る当事者は、ベースポイントＡから「ビットコイントークン」等の種類を知ることができる一方、第三者は知ることができない。
なお、コンフィデンシャル・アセットでは、さらに、通貨の創造を防ぐためベースポイントＡをリング署名で構成する。
【０１０９】
なお、上記では所謂シングルチェーンでの「ＤＶＰスワップ」について説明したが、クロスチェーンでの「ＤＶＰスワップ」や「アトミックスワップ」のように、複数のトランザクションを生成して通貨交換を行うようにしても良い。
すなわち、「取引決済サーバ２００」と「取引端末１０Ｃ」が生成するトランザクションの数は単数に限定されない。
【０１１０】
このように、「取引決済サーバ２００」と「取引端末１０Ｃ」は、上述の如く「ＤＶＰスワップ」により信頼関係を不要として、「１ビットコイントークン」と「７０万円トー

クン」を交換するための取引内容等を暗号化したトランザクションを生成することができる。

【０１１１】

次いで、図１７のＳＴ２６へ進む。ＳＴ２６では、「取引決済サーバ２００」は図５の「取引決済サーバ側鍵情報記憶部２２４」の「取引決済サーバ２００」の秘密鍵を用いて、当該トランザクションに「取引決済サーバ２０」の電子署名を入力し、「取引端末１０Ｃ」に送信する。

【０１１２】

次いで、ＳＴ２７へ進む。ＳＴ２７では、「取引端末１０Ｃ」は、受信したトランザクションに「Ｃ取引端末側鍵情報記憶部１５Ｃ」の「取引端末１０Ｃ」の秘密鍵を用いて電子署名を入力する。

【０１１３】

この際に、「取引端末１０Ｃ」が不正行為を働き、「取引決済サーバ２００」に出力すべき「７０万円トークン」の出力先を改変した場合、「取引決済サーバ２００」が入力した電子署名の検証に失敗し、無効なトランザクションと判定される。

このように、上述の工程により、第三者を介さず、相手方と信頼関係なしに、安心して取引を行うことができる。

【０１１４】

次いで、ＳＴ２８へ進む。ＳＴ２８では、「取引決済サーバ２００」と「取引端末１０Ｃは」、生成したトランザクションを「検証サーバ１００」に送信し、トランザクションの検証を要求すると共に、「検証サーバ１００」がトランザクションを検証可能なように、「取引決済サーバ２００」と「取引端末１０Ｃ」は、トランザクションの秘匿化の際に用いた秘密鍵を併せて送信する。

【０１１５】

次いで、ＳＴ２９へ進む。ＳＴ２９では、図９の「復号部（プログラム）１２２」が動作し、「取引決済サーバ２００」と「取引端末１０Ｃ」から、送信された秘密鍵を用いて、「トークン」の交換量（取引量）、種類といった取引内容を表す情報を復号する。

【０１１６】

次いで、図９の「承認部（プログラム）１２３」が動作し、復号した取引内容が適正か否かを検証し、適正な場合は、当該トランザクションを承認し、適正でない場合は、当該トランザクションを承認しない。

【０１１７】

具体的には、例えば、「検証サーバ１００」の「承認部（プログラム）１２３」は、上記のトランザクションで交換される「ビットコイントークン」の数量と「円トークン」の数量とから、「取引決済サーバ２００」と「取引端末１０Ｃ」との間で行われる通貨交換取引の取引価格（交換レート）を算出する。

【０１１８】

「ビットコイントークン」は、仮想通貨に、「円トークン」は法定通貨に対応するため、算出した価格は、法定通貨に対する仮想通貨の売買価格に相当する。

また、「検証サーバ２００」は、法定通貨に対する仮想通貨の現在の時価情報を、所定の外部ＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｇｒａｍｍａｂｌｅ Ｉｎｔｅｒｆａｃｅ）から取得する。

【０１１９】

そして、「検証サーバ１００」は、上記で算出した取引価格と、一般に流通する仮想通貨の取引価格（流通ルート）との差分が所定の閾値以上であるか否かを判断する。

両者の差分が閾値以上であると判定した場合、「検証サーバ１００」は、当該トランザクションが不適切な取引に係るものと判定し、当該トランザクションを承認しない。

【０１２０】

金融取引では、一般的に、不適切な取引を取り締まるため、法令、自主規制等を含めて種々の規制が設けられている。

一方で、本システム１はブロックチェーンを用いた分散型の取引システムであり、取引を管理する中央集権的な管理者が存在しない。
しかし、取引を完全にユーザのみに委ねた場合、一般的な金融取引の規制に鑑みて、不適切な取引が行われるおそれがある。
【０１２１】
例えば、当事者同士が結託し、少額の日本円を多額の仮想通貨（ビットコイン）と交換することで、資金洗浄のような行為が発生するおそれがある。
そこで、本実施の形態では、「検証サーバ１００」が取引内容を検証することで、不適切な取引を防止する。
【０１２２】
例えば、検証サーバは、上述の如く、トランザクションにより交換される通貨の交換レートを検証し、不適切な取引であるか否かを判定する。
その他にも、「検証サーバ１００」は、各取引端末のＩＤ、ＵＴＸＯ等の取引に関わる情報を検証し、不適切な取引であるか否かを判定する。
【０１２３】
なお、本実施の形態では、上記では、通貨の交換レート、当事者のＩＤ、ＵＴＸＯ等を基準に検証を行っているが、本発明は、これに限定されるものではなく、例えば、通貨の取引量等を基準に検証を行っても構わない。
【０１２４】
すなわち、「検証サーバ１００」は、取引内容が適合する適正なトランザクションであるか否かを判定可能であれば良く、その判定条件は特に限定されない。
【０１２５】
次いで、図１８のＳＴ３１では、「検証サーバ１００」の「承認部（プログラム）１２３」が、適正な取引であると判定し、検証に成功した場合、「検証サーバ１００」は、図８の「検証サーバ側鍵情報記憶部１１３」の「検証サーバ１００」の秘密鍵を用いて、当該トランザクションに電子署名を付加し、サイドチェーンのネットワークにブロードキャストする。
【０１２６】
次いで、ＳＴ３２へ進む。ＳＴ３２では、「検証サーバ１００」からブロードキャストされたトランザクションは、「監査端末１０Ｄ等」で検証が実行される。
「監査端末１０Ｄ」等は、それらの図１１に示す「監査端末検証部（プログラム）１７Ｄ」が動作し、端末の計算力に依拠した「Ｐｏｗ」ではなく、サイドチェーンで採用される「ストロング・フェデレーション」のアルゴリズムによりトランザクションを検証し、サイドチェーンにブロックに追加することに同意する場合、各監査端末１０Ｄ等は、当該ブロックに「監査端末１０Ｄ」等の電子署名を入力する。
【０１２７】
「監査端末１０Ｄ」等は、端末の計算力に依拠した「Ｐｏｗ」ではなく、サイドチェーンで採用される「ストロング・フェデレーション」のアルゴリズムによりトランザクションを検証して合意を形成する。
ストロング・フェデレーションでは、ラウンドロビンで処理が行われ、複数の監査端末のうち、いずかの監査端末１０Ｄ等が順番にマスターに選出されて検証を行う。
マスターとなった監査端末１０Ｄ等は、サイドチェーンのネットワーク上にブロードキャストされた各トランザクションのスクリプトを検証し、サイドチェーンに追加するブロックの候補を生成する。
マスターである「監査端末１０Ｄ」等は、生成したブロックの候補を他の「監査端末に送信する。
【０１２８】
次いで、ＳＴ３３へ進む。ＳＴ３３では、「複数の監査端末１０Ｄ等のうち、所定数の監査端末から電子署名が入力された場合、当該ブロックはサイドチェーンに追加され、「取引決済サーバ２００」と「取引端末１０Ｃ」の間のトランザクションはサイドチェーン

に正常に取り込まれる。
【０１２９】
サイドチェーン上では、ストロング・フェデレーションを採用するため、「監査端末１０Ｄ」等の計算力に依拠しないため、計算負荷が大きく削減され、合意形成に要する時間を短時間とし、迅速な取引を実行することができる。
一方で、所定数の「監査端末１０Ｄ」等の同意を必要とすることで、メインチェーンで担保されているセキュリティ（ビザンチン耐性）を維持することができる。
【０１３０】
次いで、ＳＴ３４へ進む。ＳＴ３４では、「取引決済サーバ１００」は、「監査端末１０Ｄ」等及び／又は検証サーバ１００に、メインチェーン上で「１ビットコイン」をロックしている「ロッキングトランザクション」の解除を要求する。
【０１３１】
次いで、ＳＴ３５では、「取引端末１０Ｃ」は、サイドチェーンの「ビットコイントークン」をメインチェーンの「ビットコイン」に変換するため、ペグアウトの要求を「監査端末１０Ｄ」等に送信、または、サイドチェーンに埋め込む。
【０１３２】
次いで、ＳＴ３６へ進む。ＳＴ３６では、「ペグアウト」の要求を受けた、各「監査端末１０Ｄ」等は、「取引端末１０Ｃ」が「ビットコイントークン」を保持するサイドチェーン上、すなわち、「検証サーバ１００」の「ＵＴＸＯ」を検証する。
【０１３３】
次いで、ＳＴ３７へ進む。ＳＴ３７では、所定数の監査端末１０Ｄ等が、検証に成功し、ペグアウトを承認した場合、ロッキングトランザクションに各「監査端末１０Ｄ」等が電子署名を入力し、「ビットコイン」のロックを解除する。
【０１３４】
「１ビットコイン」のロックが解除されることにより、「取引端末１０Ｃ」は、自らのウォレットアドレスに「ビットコイン」を送信可能となる。
なお、ロックが解除される「ビットコイン」は、今回の取引において「取引決済サーバ２００」が、ロックした「ビットコイン」とは限らず、他の取引でロックされた「ビットコイン」である場合で良い。
【０１３５】
なお、「取引決済サーバ２００」が、ペグイン時に「ビットコイン」をロックしておいたロッキングトランザクションと、取引の相手方である「取引端末１０Ｃ」がペグアウト時にアンロックするロッキングトランザクションは必ずしも一致せず、他の取引において他の「取引端末１０Ｃ」が生成したロッキングトランザクションである場合もあり得る。
【０１３６】
次いで、ＳＴ３８へ進む。ＳＴ３８では、「取引決済サーバ２００」は、上述のトランザクションにより取得した「円トークン」に基づく法定通貨（７０万円）の償還要求を送信サーバに送信する。
【０１３７】
次いで、ＳＴ３９へ進む。ＳＴ３９では、償還要求を受け付けた「検証サーバ１００」は、「取引決済サーバ２００」が「７０万円トークン」を保有しているか否かをチェックした後、「取引決済サーバ２００」が保有する「円トークン」と等価な法定通貨（７０万円）を、金融振込等の手段で取引決済サーバの口座に送金する。
【０１３８】
このように、本実施の形態では、「取引端末１０Ｃ」は「１ビットコイントークン」をサイドチェーンからメインチェーンに移動するペグアウト（Ｐｅｇ－ｏｕｔ）を行って「１ビットコイン」を取得すると共に、「取引決済サーバ２００」は「円トークン」に基づく法定通貨（７０万円）の償還要求を行い、金融振込等の手段で法定通貨（７０万円）を取得する。
そして、これにより、「取引決済サーバ２００」の「１ビットコイン」と、「取引端末

１０Ｃ」の法定通貨（７０万円）との交換が完了する。
【０１３９】
　また、本実施の形態では、サイドチェーンは、監査端末１０Ｄ等や検証サーバ１００により管理される「トークン」で取引が実行されるため、取引の安全が担保される構成となっている。
【０１４０】
　続いて、他の取引、すなわち、「取引決済サーバ２００」が「取引端末１０Ａ」に「１０万円」を提供する契約も本システム１を利用して実行する。
　この場合、上述の「取引端末１０Ｃ」が「取引決済サーバ２００」に「７０万円」を提供する工程と、同様の工程を経て実行される。
【０１４１】
　また、他の取引である「取引端末１０Ｃ」に「１ビットコイン」を提供する契約も本システム１を利用して実行される。
　その場合、上述の「取引端末１０Ｃ」が「取引決済サーバ２００」に「１ビットコイン」を提供する工程と、同様の工程を経て実行される。
【０１４２】
　以上のように、本システム１を利用することで、仮想通貨（１ビットコイン）及び法定通貨（７０万円）の交換を、所謂カウンターパーティのリスクなしに実現することができる。
　また、第三者を介さずに相対取引で交換可能であり、当事者は売買対象である通貨のコントロールを自らで行うことができる。
　さらに、「検証サーバ１００」が実行する処理を組み合わせることで、通貨交換取引に一定の規制を加えることもできる。
　また、複数の連続した契約について、個々の契約について、それぞれ処理すると不都合があるが、本実施の形態では、「取引決済サーバ２００」等を動作させることで解決される。
【０１４３】
　なお、「検証サーバ１００」は、トランザクションの検証だけでなく、各トランザクションにより行われる取引記録の出力、つまり、本プラットフォーム上で行われる通貨交換取引のレポートを出力可能とする構成としても良い。
　一般的な金融取引では、金融官庁からの要請に応じて取引記録を提出する必要がある。
　これに対応して、「検証サーバ１００」は、各トランザクションで暗号化されている取引内容を秘匿化用の秘密鍵を用いて復号し、取引記録を出力する。
　これにより一般ユーザからは本プラットフォーム上での取引記録が秘匿化される一方、必要に応じて取引記録を閲覧可能とすることができる。
【０１４４】
　本実施の形態では、ビットコイン等の仮想通貨と法定通貨である円の交換を例に説明したが、本実施の形態では、法定通貨は、円のみならず「ＵＳドル」や「ベトナムドン」等の他の国家の法定通貨としても構わない。
【０１４５】
　また、本実施の形態では、仮想通貨と法定通貨との間の交換を例に説明したが、仮想通貨を媒介通貨等として、例えば、円とＵＳ（アメリカ合衆国）ドルや円とベトナムドン等を交換する構成としても構わない。
　この場合、日本円監査端末、ＵＳドル監査端末、ベトナムドン監査端末、マレーシアリンギット監査端末等を本実施の形態の図１のシステム１に配置することで、日本円、ＵＳドル、ベトナムドン、マレーシアリンギットをビットコイン等の仮想通貨を介して相互に交換することが可能となる。
【０１４６】
　以上説明した実施形態においては、装置として実現される場合を例に挙げて説明したが、本発明は、これに限定されず、コンピュータに実行させることのできるプログラムとし

て、磁気ディスク（フロッピー（登録商標）ディスク、ハードディスクなど）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤなど）光磁気ディスク（ＭＯ）、半導体メモリなどの記憶媒体に格納され頒布されてもよい。

【０１４７】

また、記憶媒体は、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であればよい。記憶媒体の記憶形式は、特には限定されない。

【０１４８】

また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているＯＳ（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のＭＷ（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行してもよい。

【０１４９】

さらに、本発明における記憶媒体は、コンピュータと独立した媒体には限定されず、ＬＡＮやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【０１５０】

また、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づいて本実施形態における各処理を実行すればよく、１つのパソコン等からなる装置であってもよいし、複数の装置がネットワーク接続されたシステム等であってもよい。

【０１５１】

また、本発明におけるコンピュータとは、パソコンには限定されず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【０１５２】

以上、本発明の実施形態について説明した。しかし、本発明は、上記実施形態に限定されず、特許請求の範囲を逸脱しない範囲で種々の変更を行うことができる。上記実施形態の構成は、その一部を省略したり、上記とは異なるように任意に組み合わせたりすることができる。

【符号の説明】

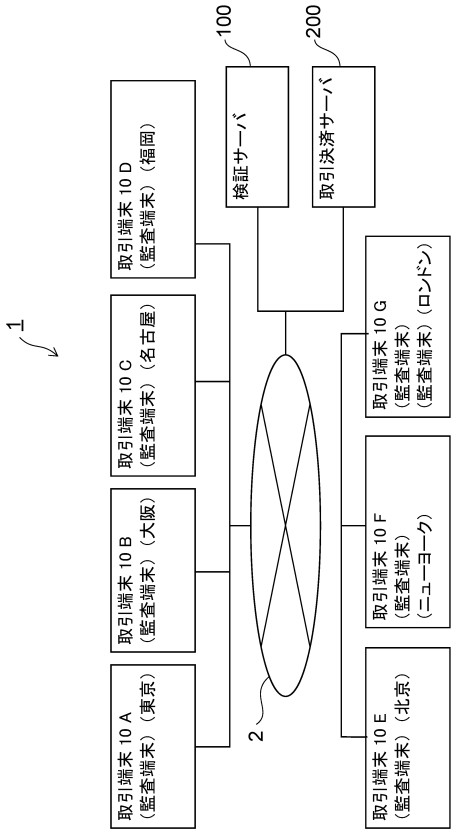
【０１５３】

１・・・ビットコイン取引システム、１０Ａ乃至１０Ｇ・・・取引端末、１１Ｃ・・・取引端末側制御部、１１Ｄ・・・監査端末側制御部、１２Ｃ・・・取引端末側通信装置、１２Ｄ・・・監査端末側通信装置、１３Ｃ・・・取引端末側ディスプレイ、１３Ｄ・・・監査端末側ディスプレイ、１４Ｃ・・・取引端末側各種情報入力装置、１４Ｄ・・・監査端末側各種情報入力装置、１５Ｃ・・・Ｃ取引端末側鍵情報記憶部、１５Ｄ・・・監査端末側鍵情報記憶部、１６Ｃ・・・取引端末側各種情報記憶部、１７Ｄ・・・監査端末検証部（プログラム）、１００・・・検証サーバ、１０１・・・検証サーバ側制御部、１０２・・・検証サーバ側通信装置、１０３・・・検証サーバ側ディスプレイ、１０４・・・検証サーバ側各種情報入力装置、１１０・・・検証サーバ側第１の各種情報記憶部、１１１、１２１・・・取引データベース、１１２・・・検証サーバ側マルチシグアドレス生成部（プログラム）、１１３・・・検証サーバ側鍵情報記憶部、１１４・・・検証サーバ側マルチシグアドレス記憶部、１１５・・・検証サーバ側トランザクション生成部（プログラム）、１２０・・・検証サーバ側第２の各種情報記憶部、１２２・・・復号部（プログラム）、１２３・・・承認部（プログラム）、２００・・・取引決済サーバ、２０１・・・取引決済サーバ側制御部、２０２・・・取引決済サーバ側通信装置、２０３・・・取引決済サーバ側ディスプレイ、２０４・・・取引決済サーバ側各種情報入力装置、２１０・・・取引決済サーバ側第１の各種情報記憶部、２１１・・・条件情報記憶部、２１２・・・マッチング処理部（プログラム）、２１３・・・マッチング結果記憶部、２１４・・・ネッティング契約処理部、２２０・・・取引決済サーバ側第２の各種情報記憶部、２２１・・・ネッティング契約処理結果情報記憶部、２２２・・・セントラルカウンターパーティ

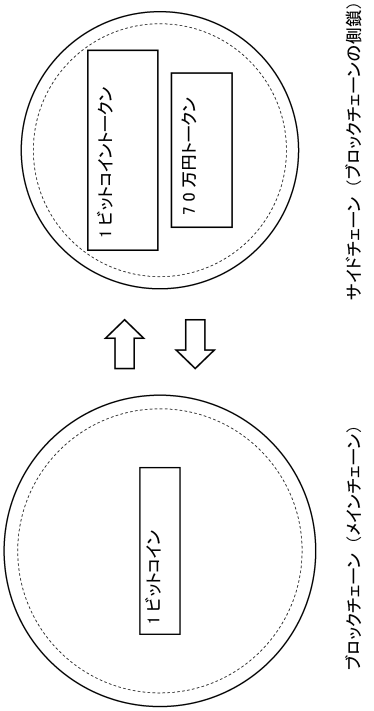
契約処理結果情報記憶部、２２３・・・ロック用マルチシグアドレス生成部（プログラム）、２２４・・・取引決済サーバ側鍵情報記憶部、２２５・・・ロック用マルチシグアドレス記憶部、２３０・・・取引決済サーバ側第２の各種情報記憶部、２３１・・・ロッキングトランザクション生成部（プログラム）、２３２・・・ロッキングトランザクション記憶部、２３３・・・ビットコイントークン要求部（プログラム）、２３４・・・セントラルカウンターパーティ契約処理部（プログラム）、

【図面】

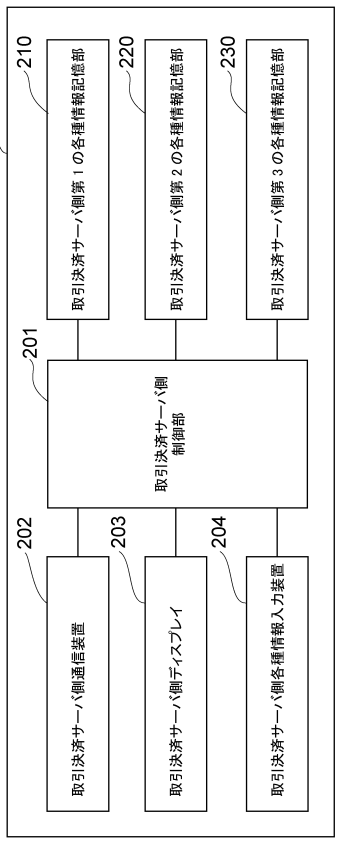
【図１】



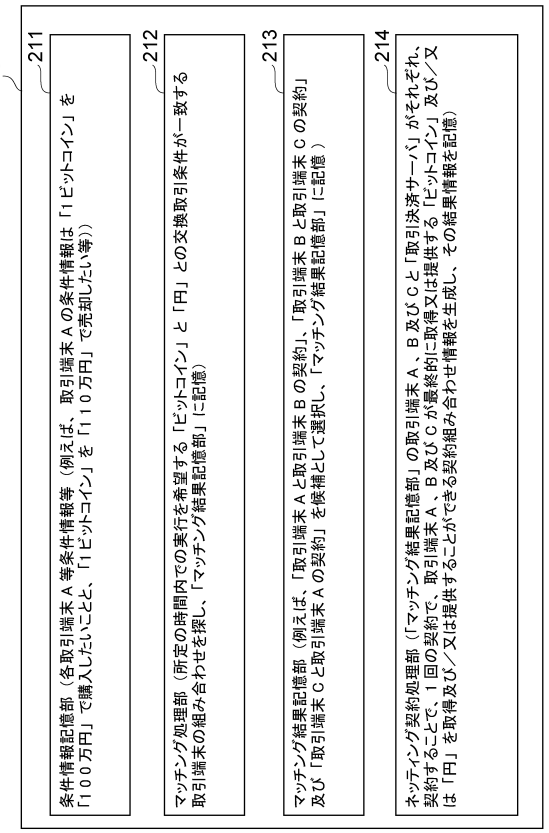
【図２】



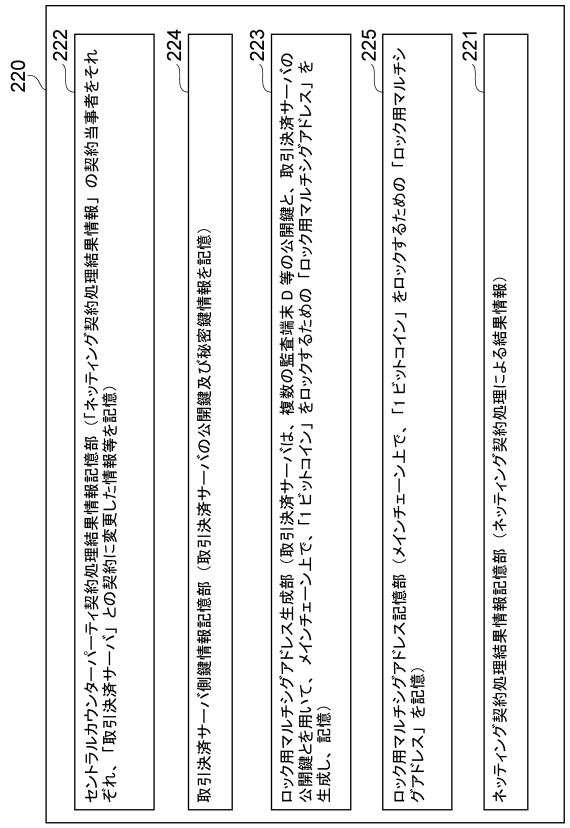
【図３】


200
210
取引決済サーバ側第１の各種情報記憶部
220
取引決済サーバ側第２の各種情報記憶部
230
取引決済サーバ側第３の各種情報記憶部
201
取引決済サーバ側制御部
202
取引決済サーバ側通信装置
203
取引決済サーバ側ディスプレイ
204
取引決済サーバ側各種情報入力装置

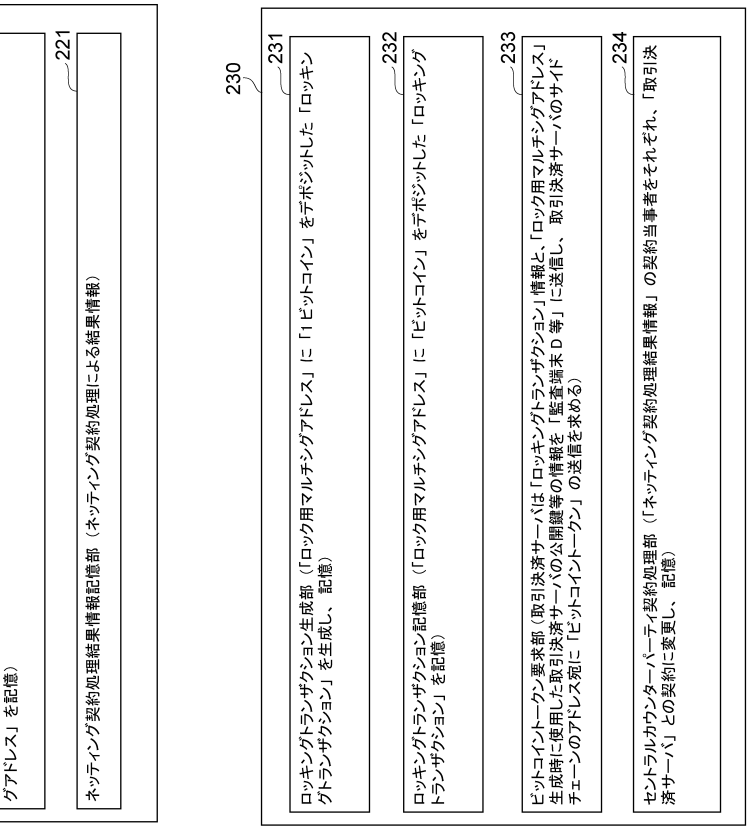
【図４】


210
211
条件情報記憶部（各取引端末Ａ等条件情報等（例えば、取引端末Ａの条件情報は「１ビットコイン」を「１００万円」で購入したいことと、「１ビットコイン」を「１１０万円」で売却したい等））
212
マッチング処理部（所定の時間内での実行を希望する「ビットコイン」と「円」との交換取引条件が一致する取引端末の組み合わせを探し、「マッチング結果記憶部」に記憶）
213
マッチング結果記憶部（例えば、「取引端末Ａと取引端末Ｂの契約」、「取引端末Ｂと取引端末Ｃの契約」及び「取引端末Ｃと取引端末Ａの契約」を候補として選択し、「マッチング結果記憶部」に記憶）
214
ネッティング契約処理部（「マッチング結果記憶部」の取引端末Ａ、Ｂ及びＣと「取引決済サーバ」がそれぞれ、契約することで、１回の契約で、取引端末Ａ、Ｂ及びＣが最終的に取得又は提供する「ビットコイン」及び／又は「円」を取得及び／又は提供することができる契約組み合わせ情報を生成し、その結果情報を記憶）

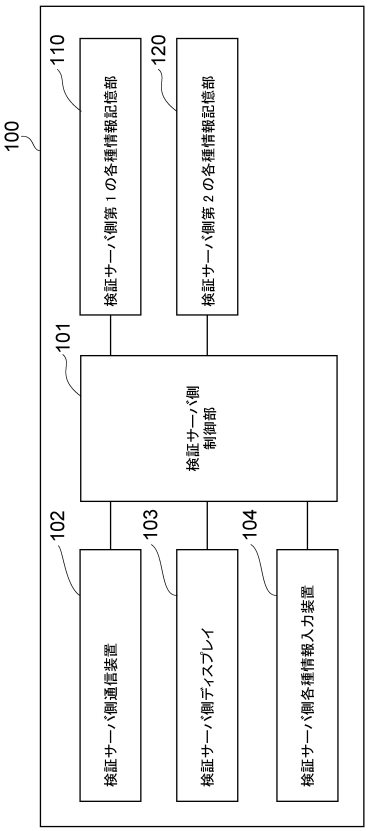
【図５】


220
222
セントラルカウンターパーティ契約処理結果情報記憶部（「ネッティング契約処理結果情報」の契約当事者をそれぞれ、「取引決済サーバ」との契約に変更した情報等を記憶）
224
取引決済サーバ側鍵情報記憶部（取引決済サーバの公開鍵及び秘密鍵情報を記憶）
223
ロック用マルチシグアドレス生成部（取引決済サーバは、複数の監査端末Ｄ等の公開鍵と、取引決済サーバの公開鍵とを用いて、メインチェーン上で、「１ビットコイン」をロックするための「ロック用マルチシグアドレス」を生成し、記憶）
225
ロック用マルチシグアドレス記憶部（メインチェーン上で、「１ビットコイン」をロックするための「ロック用マルチシグアドレス」を記憶）
221
ネッティング契約処理結果情報記憶部（ネッティング契約処理による結果情報）

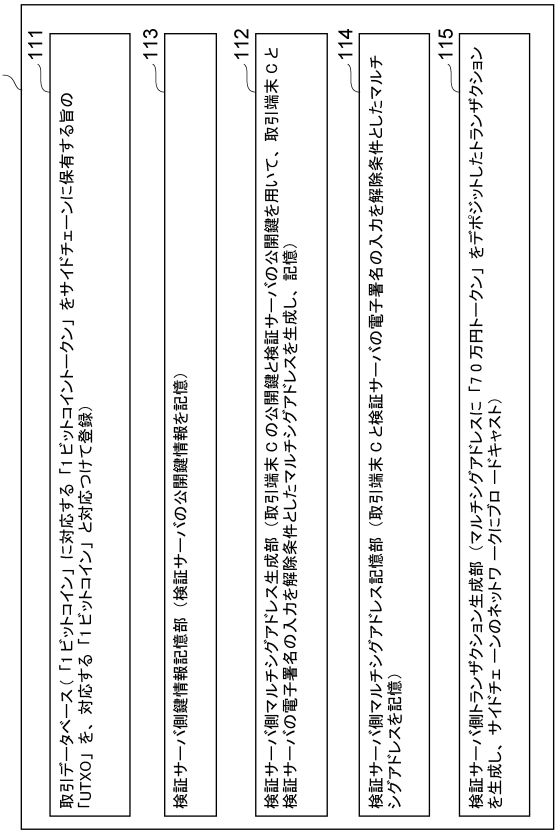
【図６】


230
231
ロッキングトランザクション生成部（「ロック用マルチシグアドレス」に「１ビットコイン」をデポジットした「ロッキングトランザクション」を生成し、記憶）
232
ロッキングトランザクション記憶部（「ロック用マルチシグアドレス」に「ビットコイン」をデポジットした「ロッキングトランザクション」を記憶）
233
ビットコイントークン要求部（取引決済サーバは「ロッキングトランザクション」情報と、「ロック用マルチシグアドレス」生成時に使用した取引決済サーバの公開鍵等の情報を「監査端末Ｄ等」に送信し、取引決済サーバのサイドチェーンのアドレス宛に「ビットコイントークン」の送信を求める）
234
セントラルカウンターパーティ契約処理部（「ネッティング契約処理結果情報」の契約当事者をそれぞれ、「取引決済サーバ」との契約に変更し、記憶）

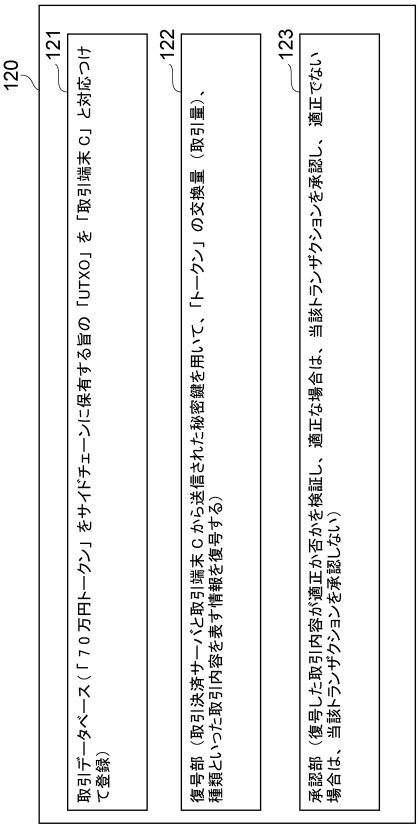
【図７】


100
101
検証サーバ側制御部
102
検証サーバ側通信装置
103
検証サーバ側ディスプレイ
104
検証サーバ側各種情報入力装置
110
検証サーバ側第１の各種情報記憶部
120
検証サーバ側第２の各種情報記憶部

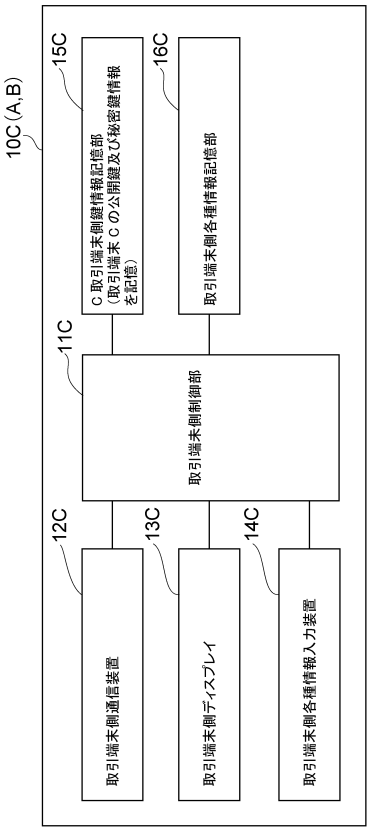
【図８】


110
111
取引データベース（「１ビットコイン」に対応する「１ビットコイントークン」をサイドチェーンに保有する旨の「UTXO」を、対応する「１ビットコイン」と対応つけて登録）
113
検証サーバ側鍵情報記憶部（検証サーバの公開鍵情報を記憶）
112
検証サーバ側マルチシグアドレス生成部（取引端末Ｃの公開鍵と検証サーバの公開鍵を用いて、取引端末Ｃと検証サーバの電子署名の入力を解除条件としたマルチシグアドレスを生成し、記憶）
114
検証サーバ側マルチシグアドレス記憶部（取引端末Ｃと検証サーバの電子署名の入力を解除条件としたマルチシグアドレスを記憶）
115
検証サーバ側トランザクション生成部（マルチシグアドレスに「７０万円トークン」をデポジットしたトランザクションを生成し、サイドチェーンのネットワークにブロードキャスト）

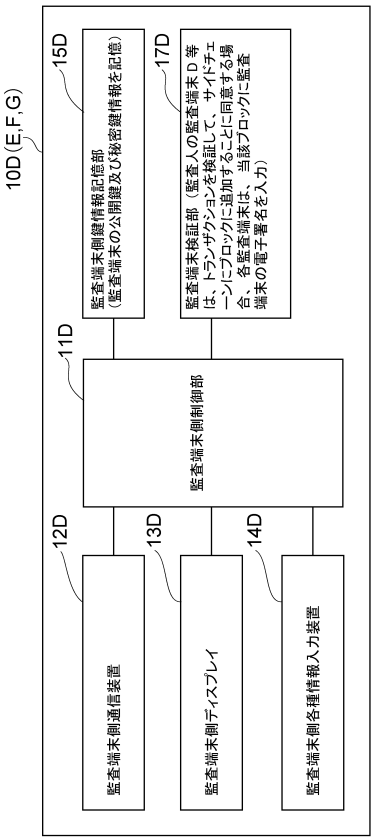
【図９】


120
121
取引データベース（「７０万円トークン」をサイドチェーンに保有する旨の「UTXO」を「取引端末Ｃ」と対応つけて登録）
122
復号部（取引決済サーバと取引端末Ｃから送信された秘密鍵を用いて、「トークン」の交換量（取引量）、種類といった取引内容を表す情報を復号する）
123
承認部（復号した取引内容が適正か否かを検証し、適正な場合は、当該トランザクションを承認し、適正でない場合は、当該トランザクションを承認しない）

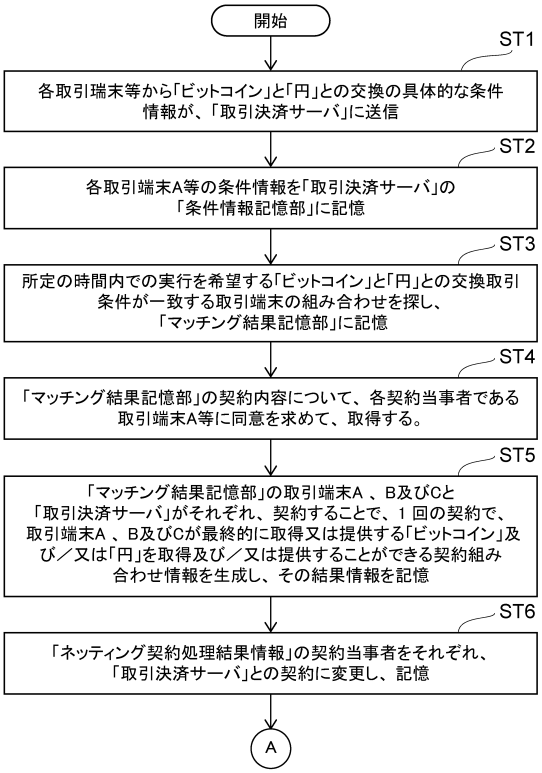
【図１０】


10C(A,B)
11C
取引端末側制御部
12C
取引端末側通信装置
13C
取引端末側ディスプレイ
14C
取引端末側各種情報入力装置
15C
Ｃ取引端末側鍵情報記憶部（取引端末Ｃの公開鍵及び秘密鍵情報を記憶）
16C
取引端末側各種情報記憶部

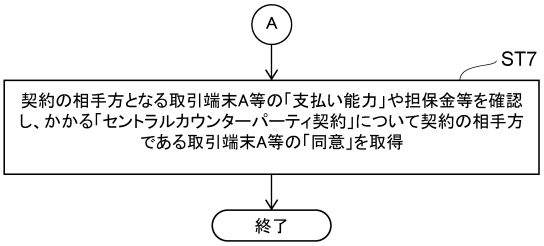
【図１１】



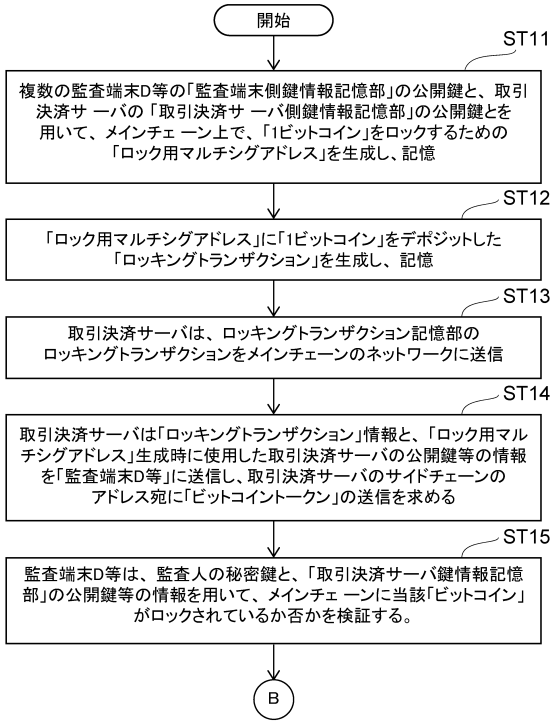
【図１２】



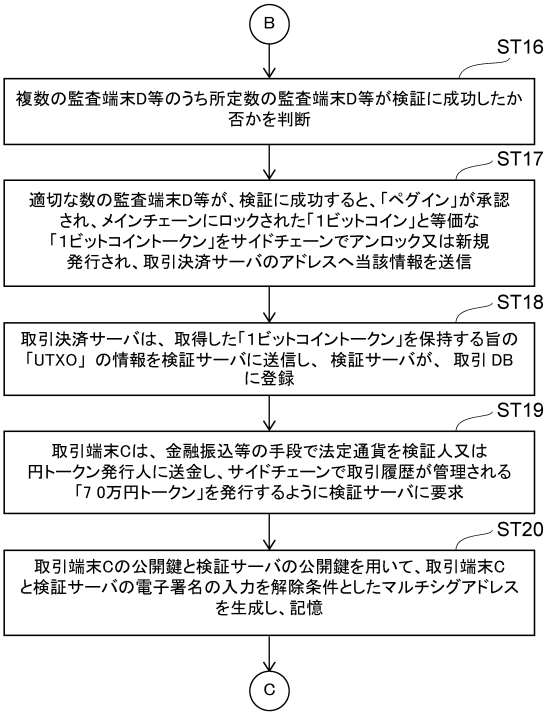
【図１３】



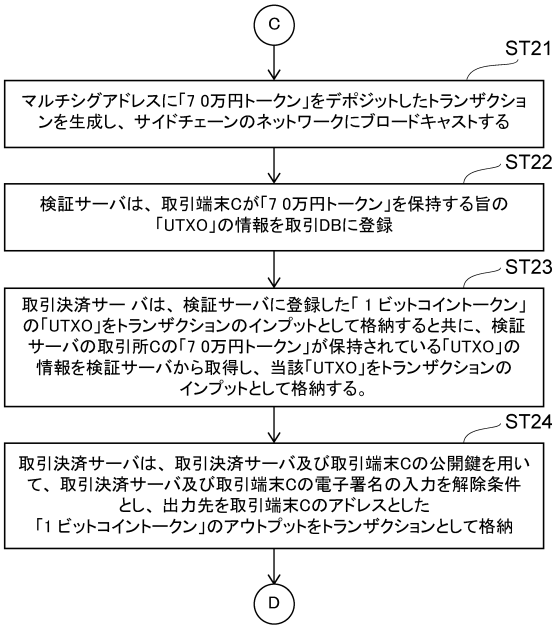
【図１４】



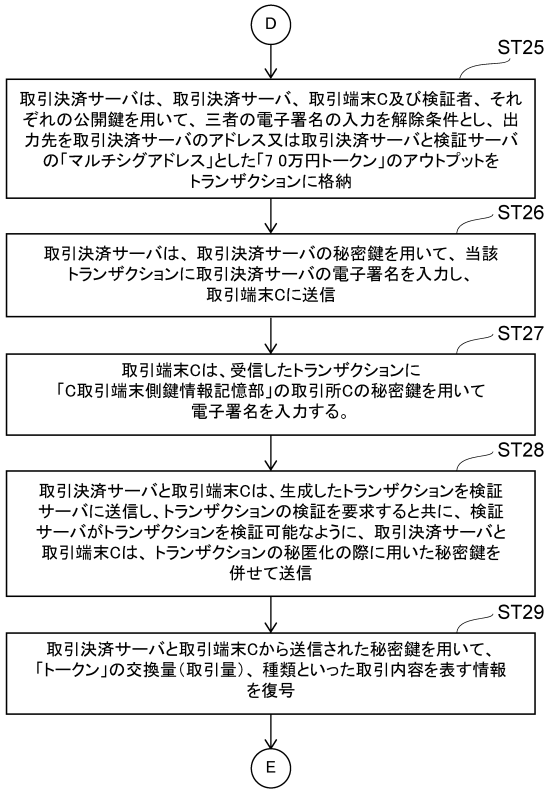
【図１５】



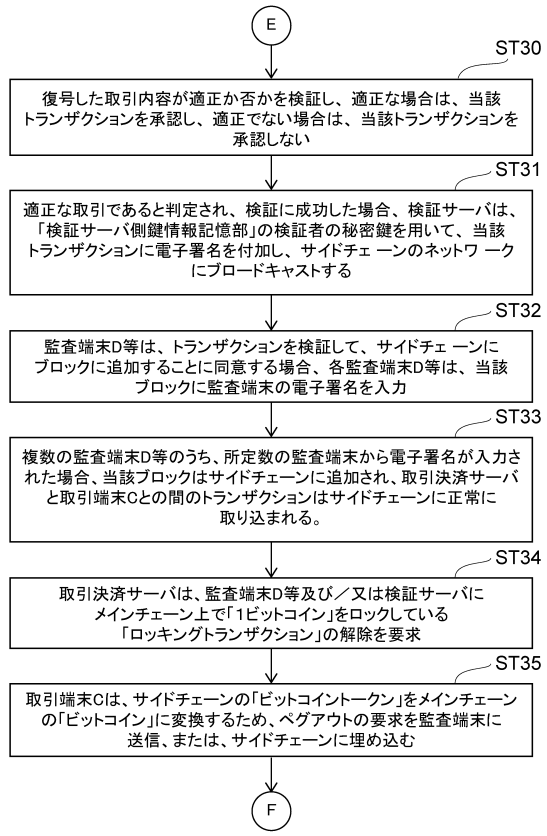
【図１６】



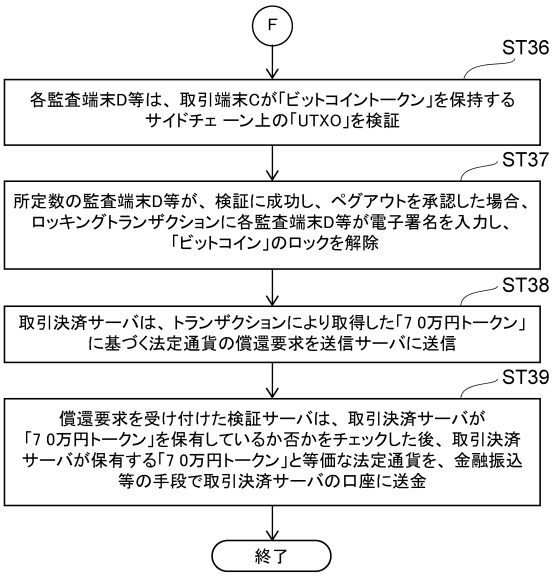
【図１７】



【図１８】



【図１９】


F
ST36
各監査端末D等は、取引端末Cが「ビットコイントークン」を保持するサイドチェーン上の「UTXO」を検証
ST37
所定数の監査端末D等が、検証に成功し、ペグアウトを承認した場合、ロッキングトランザクションに各監査端末D等が電子署名を入力し、「ビットコイン」のロックを解除
ST38
取引決済サーバは、トランザクションにより取得した「７０万円トークン」に基づく法定通貨の償還要求を送信サーバに送信
ST39
償還要求を受け付けた検証サーバは、取引決済サーバが「７０万円トークン」を保有しているか否かをチェックした後、取引決済サーバが保有する「７０万円トークン」と等価な法定通貨を、金融振込等の手段で取引決済サーバの口座に送金
終了

フロントページの続き

(56)参考文献　米国特許出願公開第２０１９／０２３８５２５（ＵＳ，Ａ１）
特開２０１９－１９１８７６（ＪＰ，Ａ）
国際公開第２０１９／０７２３１７（WO，Ａ２）
特許第６５００１５８号公報（ＪＰ，Ｂ１）
特開２０１９－１４４７８１（ＪＰ，Ａ）
特開２００２－３２９１５５（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
G06Q 10/00-99/00