(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6838260号
(P6838260)

(45)発行日　令和3年3月3日(2021.3.3)　(24)登録日　令和3年2月16日(2021.2.16)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675Z
G06F 21/64	(2013.01)	H04L	9/00	675B
G06Q 20/40	(2012.01)	G06F	21/64	
		G06Q	20/40	300

請求項の数 8　(全 17 頁)

(21)出願番号　特願2018-213408(P2018-213408)
(22)出願日　平成30年11月14日(2018.11.14)
(65)公開番号　特開2020-80498(P2020-80498A)
(43)公開日　令和2年5月28日(2020.5.28)
審査請求日　平成31年1月11日(2019.1.11)
審判番号　不服2019-15553(P2019-15553/J1)
審判請求日　令和1年11月20日(2019.11.20)

早期審査対象出願

(73)特許権者　518405049
カウリー株式会社
東京都渋谷区代々木２丁目１５－１２　井上ビル１１号館２０１号
(74)代理人　110002273
特許業務法人インターブレイン
(72)発明者　石ヶ谷　勉
東京都文京区千石４丁目１番２２－２０３号　カウリー株式会社内
(72)発明者　笹田　亮
東京都文京区千石４丁目１番２２－２０３号　カウリー株式会社内
(72)発明者　飯塚　高秋
東京都文京区千石４丁目１番２２－２０３号　カウリー株式会社内

最終頁に続く

(54)【発明の名称】ブロックチェーン制御方法

(57)【特許請求の範囲】
【請求項１】
複数の通常ノードそれぞれが、仮想通貨による商取引の結果を示す取引データを取引ネットワークに送信するステップと、
トランザクションプールが、前記取引ネットワークに送信された取引データを蓄積するステップと、
特権ノードが、前記トランザクションプールから１以上の取引データを取得するステップと、
前記特権ノードが、前記ブロックに含まれる情報のうち、あらかじめ定められた位置にある所定のサイズのデータを対象として秘密鍵を用いて署名値を生成するステップと、
前記特権ノードが、前記トランザクションプールから取得した取引データおよび前記生成した署名値を含むブロックを生成するステップと、
前記特権ノードが、生成したブロックを前記取引ネットワークにブロードキャストするステップと、
前記複数の通常ノードそれぞれが、ブロードキャストされたブロックを取得するステップと、
前記複数の通常ノードそれぞれが、前記秘密鍵に対応する公開鍵によりブロックに含まれる署名値の真正性を確認するステップと、
前記複数の通常ノードそれぞれが、署名値の真正性を確認できたことを条件として、個別に保有しているブロックチェーンに新たに取得したブロックをつなげるステップと、を

実行することにより、複数の通常ノードそれぞれが同一内容の取引履歴を示すブロックチェーンを分散管理することを特徴とするブロックチェーン制御方法。
【請求項２】
前記特権ノードは、前記トランザクションプールに蓄積された取引データを定期的に読み出し、読み出した取引データのデータサイズに応じた可変サイズのブロックを生成することを特徴とする請求項１に記載のブロックチェーン制御方法。
【請求項３】
前記特権ノードは、ブロックの生成に用いる取引データのデータサイズに所定の閾値を設定し、前記トランザクションプールから読み出した取引データのデータサイズが前記所定の閾値以下のときにはブロックの生成をスキップすることを特徴とする請求項２に記載のブロックチェーン制御方法。
【請求項４】
前記特権ノードは、ブロック生成のタイミングを取引の活発度に応じて調整することを特徴とする請求項１に記載のブロックチェーン制御方法。
【請求項５】
前記秘密鍵は、暗号化された状態で不揮発性メモリに保存されており、
前記特権ノードは、前記不揮発性メモリから前記秘密鍵を揮発性メモリに読み出して復号した上で署名値を生成し、前記ブロックの生成後に前記秘密鍵を前記揮発性メモリから削除することを特徴とする請求項１から４のいずれかに記載のブロックチェーン制御方法。
【請求項６】
前記秘密鍵は、複数パーツに分割された状態で複数の不揮発性メモリに分けて保存されており、
前記特権ノードは、前記複数の不揮発性メモリそれぞれから前記秘密鍵のパーツを揮発性メモリに読み出して前記秘密鍵を合成した上で署名値を生成し、前記ブロックの生成後に前記秘密鍵を前記揮発性メモリから削除することを特徴とする請求項１から４のいずれかに記載のブロックチェーン制御方法。
【請求項７】
前記特権ノードが、所定の変更条件が成立したとき、前記秘密鍵を変更するステップと、
前記特権ノードが、変更後の秘密鍵に対応する公開鍵を前記取引ネットワークにブロードキャストするステップと、を更に備えることを特徴とする請求項１から６のいずれかに記載のブロックチェーン制御方法。
【請求項８】
前記秘密鍵は、不揮発性メモリに保存されており、
前記特権ノードは、前記不揮発性メモリに対する前記特権ノード以外の通信端末からのアクセスを検出したとき、前記秘密鍵を変更することを特徴とする請求項７に記載のブロックチェーン制御方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ブロックチェーン、特に、ブロックチェーンに基づく電子取引の真正性を確認するための技術、に関する。
【背景技術】
【０００２】
ビットコイン（Bitcoin）やイーサリアム（Ethereum）などのさまざまな仮想通貨を支える仕組みがブロックチェーンである（特許文献１参照）。ブロックチェーンは、複数の通信ノードがピア・ツー・ピア技術にて共有する取引台帳である。
【０００３】
取引者となるユーザは、取引データを通信ネットワークにブロードキャストする。採掘

者（マイナー）とよばれるユーザは、取引データと任意のナンス（nonce）をハッシュ関数の変数として投入し、所定の条件を満たすハッシュ値（以下、「適正ハッシュ値」とよぶ）を探す。複数の採掘者は、適正ハッシュ値を一刻も早く発見すべく競争する。適正ハッシュ値が見つかったとき、取引データはブロックチェーンに登録される。適正ハッシュ値を作ることができるナンスを見つけるのは難しいが、いったん見つけられたナンスに基づいてハッシュ値が適正か否かを確認するのは容易である。適正ハッシュ値の見つけにくさと確認しやすさがブロックチェーンの改ざんを難しくしている。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特開２０１８－１６０８２８号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

ブロックチェーンは中央（サーバ）の管理に服さない分散型のシステムであるため、取引者は自分の素性（氏名など）を明かすことなく取引できる。その一方、ブロックチェーンは「中央」を持たないがゆえに、「分岐（フォーク）」とよばれる事象が発生することがある。具体的には、あるブロックについて採掘者Ａと採掘者Ｂが２種類の適正ハッシュ値を見つけたときには、２つのブロックができてしまい、ブロックチェーンは２系統に分岐する。ブロックチェーンは一本道であることを前提とする。フォークは、通常、長いチェーンを生き残らせ、短いチェーンを無効化することで解決される。短いチェーンの無効化は一部の取引データの無効化を意味するため、フォークの発生可能性は取引の安定性を損ないかねない。

【０００６】

一般的なブロックチェーンにおいては、フォークの発生を抑制するため、適正ハッシュ値を見つける作業の難易度（以下、「採掘難易度」とよぶ）を高くしている。しかし、採掘難易度を高めるほど取引の円滑さが損なわれてしまう。

【０００７】

本発明は、上記課題認識に基づいて完成された発明であり、その主たる目的は、ブロックチェーンにおける取引の安定化と円滑化を両立させるための技術、を提供することにある。

なお、本発明の趣旨をより明確にするため、一般的なブロックチェーンの仕組みとその問題点については後に詳述する。

【課題を解決するための手段】

【０００８】

本発明のある態様におけるブロックチェーンシステムは、複数の通常ノードを含む取引ネットワークと、取引ネットワークに接続される特権ノードを含む。

特権ノードは、秘密鍵を保有する。また、通常ノードは、秘密鍵に対応する公開鍵をあらかじめ保有している。

通常ノードは、仮想通貨による商取引の結果を示す取引データの入力を受け付ける取引入力部と、取引データを取引ネットワークに送信する取引送信部と、取引履歴をブロックチェーンとして管理する取引管理部と、特権ノードからブロックを受信するブロック受信部と、を備える。

特権ノードは、通常ノードから取引データを受信する取引受信部と、秘密鍵に基づいて署名値を生成し、取引データと署名値を含むデータセットとしてブロックを生成するブロック生成部と、ブロックを取引ネットワークに送信するブロック送信部と、を備える。

通常ノードの取引管理部は、特権ノードから受信したブロックの署名値の真正性を公開鍵により確認できたことを条件として、ブロックチェーンに受信したブロックを連結する。

【０００９】

本発明のある態様におけるサーバ（特権ノード）は、複数の通常ノードを含む取引ネットワークと接続される。
通常ノードは、サーバの秘密鍵に対応する公開鍵をあらかじめ保有しており、かつ、仮想通貨による商取引の履歴をブロックチェーンとして管理する通信端末である。
このサーバは、通常ノードから、仮想通貨による商取引の結果を示す取引データを受信する取引受信部と、秘密鍵に基づいて署名値を生成し、取引データと署名値を含むデータセットとしてブロックを生成するブロック生成部と、ブロックを取引ネットワークに送信するブロック送信部と、を備える。

【発明の効果】

【００１０】

本発明によれば、ブロックチェーンにおける取引の安定化と円滑化を両立させやすくなる。

【図面の簡単な説明】

【００１１】

【図１】一般的なブロックチェーンシステムの概要図である。
【図２】一般的なブロックチェーンシステムにおける採掘（ブロック生成）の方法を説明するための模式図である。
【図３】ブロックチェーンシステムにおいてフォークが発生する仕組みを説明するための模式図である。
【図４】本実施形態におけるブロックチェーンシステムの概要図である。
【図５】本実施形態におけるブロックのデータ構造図である。
【図６】ブロックチェーンシステムの機能ブロック図である。
【図７】取引データの入力過程を示すフローチャートである。
【図８】ブロック生成の処理過程を示すフローチャートである。
【図９】通常ノードがブロックを受信したときの処理過程を示すフローチャートである。
【図１０】特権ノードにおける秘密鍵の使用方法を説明するための模式図である。

【発明を実施するための形態】

【００１２】

一般的なブロックチェーンは、その運用を統括管理すべき中央集権的な特権ノード（サーバ）をもたない。不特定多数の採掘者が競争しながら適正ハッシュ値を探すことで、ブロックチェーンは延長されていく。適正ハッシュ値を探す作業は「採掘」とよばれる。以下、「採掘」のように新たなブロックを生成することを「ブロック生成」とよぶことにする。一般的なブロックチェーンでは、採掘競争に勝利した採掘者がブロック生成する。

【００１３】

本実施形態に示すブロックチェーンでは、その運用において中心的な役割を果たす特権ノード（サーバ）を設置する。不特定多数の採掘者ではなく、単一の特権ノードがブロック生成を実行する。
以下においては、図１，図２に関連して一般的なブロックチェーンの概要を説明する。図３に関連して、一般的なブロックチェーンにおいて「分岐（フォーク）」が生じるメカニズムとそれにともなって生じる弊害について指摘する。図４以降に関連して、本実施形態における新しいブロックチェーンシステムについて詳述する。

【００１４】

図１は、一般的なブロックチェーンシステム１００の概要図である。
ブロックチェーンシステム１００においては、多数の通常ノード１１０ａ、１１０ｂ・・・１１０ｎ（以下、「通常ノード１１０」とよぶ）と多数の採掘ノード１０８ａ、１０８ｂ・・・１０８ｎ（以下、「採掘ノード１０８」とよぶ）が取引ネットワーク１０２を介してピア・ツー・ピアにて接続される。取引ネットワーク１０２は、インターネットなどの公開型の通信ネットワークにおいて形成される。

【００１５】

通常ノード１１０は、取引の主体となるノードであり、個人ウォレットや仮想通貨の取

引所などが想定される。採掘ノード１０８は、ブロック生成（採掘）を行うために採掘者により使用される通信端末である。通常ノード１１０は、採掘ノード１０８の機能を備えてもよい。

【００１６】

取引ネットワーク１０２にはブロックチェーン１０４が形成される。ブロックチェーン１０４のデータ実体は、通常ノード１１０および採掘ノード１０８それぞれにおいてローカルに保存されている。ブロックチェーン１０４が更新されるとき、更新情報が取引ネットワーク１０２にブロードキャストされる。通常ノード１１０および採掘ノード１０８は更新情報にしたがって各自が保存するブロックチェーン１０４を更新することにより、全体として同一のブロックチェーン１０４が同期共有される仕組みとなっている。

【００１７】

ブロックチェーン１０４は、多数のブロック１０６が一本の鎖として連なるデータ構造を有する。ブロック１０６は、１以上の取引データが記録されたデータ単位である。通常ノード１１０は、仮想通貨による取引（送金）を実行するごとに、取引内容を示すデータ（以下、「取引データ」とよぶ）を取引ネットワーク１０２にブロードキャストする。複数の採掘ノード１０８は、新規の取引データの集合体を対象として採掘（ブロック生成）を行う。採掘後、新規のブロック１０６は既存のブロックチェーン１０４に繋げられる（詳細後述）。すなわち、ブロックチェーン１０４とは、過去からの膨大な取引履歴が記録された長大な取引台帳であるといえる。ブロックチェーン１０４を参照することにより、いつでも過去の取引内容を確認できる。また、通常ノード１１０は、一時的なアカウントで取引を行うことができるため、取引の匿名性が保たれる。

ビットコインの場合、１つのブロック１０６に書き込むことができる取引データの総量には上限が設けられている（理由は後述）。

【００１８】

図２は、一般的なブロックチェーンシステム１００における採掘（ブロック生成）の方法を説明するための模式図である。

ここでは、（ｎ＋１）番目のブロック１０６（以下、「ブロック１０６（ｎ＋１）」のように表記する）のブロック生成（採掘）の方法について説明する。ブロック１０６（ｎ＋１）の生成に際しては、１つ前に生成されたブロック１０６（ｎ）に基づく適正ハッシュ値（ｎ）が使用される。ブロック１０６（ｎ＋１）は、多数の通常ノード１１０からブロードキャストされた取引データを含む。以下、ブロック１０６に書き込まれる多種多様な取引データの集合体のことを「取引データセット」とよぶ。

【００１９】

採掘ノード１０８は、取引データセット（ｎ＋１）、ハッシュ値（ｎ）およびナンス（ｎ＋１）を変数とする所定のハッシュ関数により、ハッシュ値（ｎ＋１）を計算する。実際には、ハッシュ関数にはこれ以外の変数も含まれるがここではブロック生成の原理の説明のため、上記３つの変数に基づくものとして説明する。

【００２０】

ナンス（ｎ＋１）は任意である。生成されたハッシュ値（ｎ＋１）が所定の条件を満たすとき、具体的には、所定の閾値Ｗ以下となるとき、そのハッシュ値（ｎ＋１）は適正ハッシュ値となる。適正ハッシュ値を見つけ出すために、採掘ノード１０８はさまざまなナンス（ｎ＋１）をハッシュ関数に投入しながら試行計算を繰り返す。適正ハッシュ値を見つけ出す採掘作業とは、適正なナンスを探す作業ともいえる。適正ハッシュ値を見つけた採掘ノード１０８は、ナンス（ｎ＋１）を含む変数群と計算結果としてのハッシュ値を取引ネットワーク１０２にブロードキャストする。他のノード（通常ノード１１０および採掘ノード１０８）は、計算結果が正しいことを確認できれば、適正なナンス（ｎ＋１）を含むブロック（ｎ＋１）をブロックチェーン１０４につなげる。適正ハッシュ値（ｎ＋１）は、次のブロック１０６（ｎ＋２）の一部となる。

【００２１】

ブロックチェーン１０４の取引データをあとから改ざんするとハッシュ値が変化してし

まう。適正ハッシュ値を計算するためにはそれなりの計算コストがかかるため、取引データとそれにもとづく適正ハッシュ値をすべて書き換えることは困難である。このような仕組みにより、ブロックチェーン１０４の改ざんは実質的に不可能となっている。

【００２２】

図３は、ブロックチェーンシステム１００においてフォークが発生する仕組みを説明するための模式図である。

上述したように、多数の採掘ノード１０８は、競争しながら適正ハッシュ値を探す。また、適正ハッシュ値は唯一無二ではないため、複数の採掘ノード１０８が複数の適正ハッシュ値を見つけ出すこともありうる。このとき、一本の鎖であるべきブロックチェーン１０４は、２系統に分岐することがある。

【００２３】

図３においては、ブロック１０６（２）に基づいて、２種類の適正ハッシュ値（Ｈ２Ａ、Ｈ２Ｂ）が見つかった場合を示す。適正ハッシュ値（Ｈ２Ａ）に基づいてブロック１０６（３Ａ）が生成されるとともに（以下、「Ａ系列」とよぶ）、適正ハッシュ値（Ｈ２Ｂ）に基づいてブロック１０６（３Ｂ）も生成されている（以下、「Ｂ系列」とよぶ）。

【００２４】

Ａ系列においてブロック１０６（３Ａ）がブロック生成され、続いてブロック１０６（４Ａ）が生成されたとする。一方、Ｂ系列においては、ある採掘ノード１０８ｘがブロック１０６（３Ｂ）のあとブロック１０６（４Ｂ）、ブロック１０６（５Ｂ）、ブロック１０６（６Ｂ）をＡ系列よりも早いペースで生成し、これら４つのブロック１０６をまとめてブロードキャストしたとする。この結果、Ａ系列とＢ系列が併存する。採掘ノード１０８ｘが圧倒的な計算能力を有しているときには、Ｂ系列のような「長いチェーン」が取引ネットワーク１０２に突然投げ込まれることがありうる。

【００２５】

ブロックチェーンシステム１００は、「分岐（フォーク）が発生したときには、長いチェーンを正式採用し、短いチェーンを破棄する」というルールにて運用される。図３の場合、Ａ系列にあるブロック１０６（３Ａ）、ブロック１０６（３Ｂ）に書き込まれた取引データは後発的に無効化されてしまう。たとえば、ある取引者が仮想通貨を使って食事をし、その取引データをブロック１０６（３Ａ）に書き込んだとする。ここでブロック１０６（３Ａ）が後発的に無効化されてしまうと、仮想通貨の支払いはなされなかったことになり、取引秩序に混乱をきたしてしまう。いいかえれば、圧倒的な計算力を有する１０８ｘであれば、密かに「長いチェーン」を作ることで、「短いチェーン」の取引を強引に無効化できてしまう。

【００２６】

ビットコインのような人気の高い仮想通貨であれば、多数の採掘者を一人の採掘者が圧倒するのは難しいため、このような「長いチェーン」を後発的に投入することは難しい。人気通貨ではフォークは生じにくいが、フォークが生じる可能性はゼロではない。一方、人気の薄い仮想通貨の場合にはフォークが発生するリスクが高くなる。

【００２７】

ビットコインでは、採掘におおよそ１０分程度を要するように採掘難易度を調整する仕組みが導入されている。たとえば、上述した閾値Ｗが小さいほど、適正ハッシュ値を見つけるのは難しくなる。この仕組みにより、１つの採掘ノード１０８だけが他の採掘ノード１０８を出し抜いて着々とブロック１０６を作り続けるのを難しくなっている。そのかわり、取引データを投入してから正式にブロックチェーンシステム１００に登録されるまでには１０分程度の待ち時間が発生することになる。

【００２８】

また、ビットコインでは、１つのブロック１０６に登録可能な取引データの総データ量（サイズ）に上限が設けられる。したがって、取引が活発なときには、取引データが今回のブロック１０６に登録してもらえず、次回以降のブロック生成まで待たされることもある。以下、１つのブロック１０６に登録可能な取引データ量の上限値を「取引上限値」と

よぶ。

【００２９】

ブロックチェーンシステム１００は中央集権型ではないため、設計上、取引上限値を変更するのが難しい。また、ハッシュ関数の性質上、取引上限値を大きくすると採掘難易度が高くなってしまう。採掘難易度が高くなりすぎると、通常の計算能力しか有しない一般的な採掘ノード１０８が採掘競争に勝てなくなってしまうというジレンマがある。

【００３０】

まとめると、フォークを発生させないためには、いいかえれば取引の安定性を確保するためにはある程度の採掘難易度を設定する必要がある。計算力に優れる一人の採掘者が他の採掘者を出し抜いてブロック生成しつづけるのを防ぐためである。しかし、採掘難易度を高くしすぎると取引の円滑性が損なわれてしまう。ビットコインのような人気のある仮想通貨の場合、取引（送金）を実行してもからブロックチェーンシステム１００に正式登録（以下、「取引承認」とよぶ）されるまでに長時間待たされるという弊害が目立ち始めている。

【００３１】

図４は、本実施形態におけるブロックチェーンシステム２００の概要図である。

本実施形態におけるブロックチェーンシステム２００においては、多数の採掘ノード１０８ではなく、単一の特権ノード１２０がブロック生成を担当する。複数の通常ノード１１０は取引ネットワーク１０２を介してピア・ツー・ピアにて接続される。取引ネットワーク１０２は、インターネットなどの公開型の通信ネットワークにおいて形成される点は図１と同じである。

【００３２】

取引ネットワーク１０２にはブロックチェーン１０４が形成される。ブロックチェーン１０４のデータ実体は、通常ノード１１０および特権ノード１２０それぞれにおいてローカルに保存されている。

【００３３】

本実施形態においても、通常ノード１１０は、一時的なアカウントで取引を行うことができるため、取引の匿名性が保たれる。また、本実施形態においてもブロック１０６に取引上限値を設定してもよいが、取引上限値を設定することは必須ではない。以下、ブロック１０６に取引上限値は設定されないものとして説明する。

【００３４】

特権ノード１２０は、公開鍵と秘密鍵のペアを有する。公開鍵は取引ネットワーク１０２にブロードキャストされ、すべての通常ノード１１０が公開鍵を保有する。通常ノード１１０は、取引データを取引ネットワーク１０２にブロードキャストし、特権ノード１２０はローカルな記憶領域（以下、「トランザクションプール」とよぶ）に取引データを蓄積する。特権ノード１２０は、定期的に、たとえば、１秒に１回のペースでトランザクションプールから取引データを読み出し、これらの取引データを含むブロック１０６を生成する。ブロック生成に際し、特権ノード１２０はブロック１０６に含まれるデータの一部を秘密鍵により暗号化し、署名値を生成する（詳細後述）。

【００３５】

特権ノード１２０は、署名値を含むブロック１０６を取引ネットワーク１０２にブロードキャストする。通常ノード１１０は、ブロック１０６の署名値を公開鍵によって復号することにより、署名値（ブロック１０６）の真正性を確認する。真正性を確認できたとき、通常ノード１１０はブロックチェーン１０４に新たなブロック１０６を追加する（取引承認）。

【００３６】

本実施形態においては、複数の採掘ノード１０８が採掘競争（適正ハッシュ値探し）をするのではなく、中央集権的な特権ノード１２０のみがブロック生成を行う。特権ノード１２０が署名値を生成するだけなのでブロック生成にともなう処理コストが低く、１秒に１回程度の高頻度にてブロック１０６を生成できる。

【００３７】
図５は、本実施形態におけるブロック１０６のデータ構造図である。
ブロック１０６（ｎ）の署名値（ｎ）は、取引データセット（ｎ）の所定の一部、たとえば、１０１ビット目から１０５ビット目までの５ビット分のデータを秘密鍵で暗号化したデータである。特権ノード１２０と通常ノード１１０は、取引データのどの部分から署名値を生成するかについてあらかじめ情報共有（合意）しておく。以下、署名値生成のための対象となるデータを「原データ」とよぶ。通常ノード１１０は、ブロック１０６（ｎ）の取引データセット（ｎ）から原データを取得するとともに署名値（ｎ）も取得する。通常ノード１１０は、署名値（ｎ）を公開鍵により復号し、復号後の署名値（ｎ）が原データと一致したとき、ブロック１０６（ｎ）は特権ノード１２０によりブロック生成された真正のブロック１０６であると判定する。署名値の確認が取引承認となる。
【００３８】
図６は、ブロックチェーンシステム２００の機能ブロック図である。
上述したように、ブロックチェーンシステム２００は、複数の通常ノード１１０および特権ノード１２０を含む。
（通常ノード１１０）
通常ノード１１０の各構成要素は、ＣＰＵ（Central Processing Unit）および各種コプロセッサなどの演算器、メモリやストレージといった記憶装置、それらを連結する有線または無線の通信線を含むハードウェアと、記憶装置に格納され、演算器に処理命令を供給するソフトウェアによって実現される。コンピュータプログラムは、デバイスドライバ、オペレーティングシステム、それらの上位層に位置する各種アプリケーションプログラム、また、これらのプログラムに共通機能を提供するライブラリによって構成されてもよい。以下に説明する各ブロックは、ハードウェア単位の構成ではなく、機能単位のブロックを示している。
特権ノード１２０についても同様である。
【００３９】
通常ノード１１０は、ユーザインタフェース処理部１３０、データ処理部１３２、通信部１３４およびデータ格納部１３６を含む。
通信部１３４は、取引ネットワーク１０２を対象として通信処理を担当する。ユーザインタフェース処理部１３０は、ユーザ（取引者）からの操作を受け付けるほか、画像表示や音声出力など、ユーザインタフェースに関する処理を担当する。データ格納部１３６は各種データを格納する。データ処理部１３２は、通信部１３４、ユーザインタフェース処理部１３０により取得されたデータおよびデータ格納部１３６に格納されているデータに基づいて各種処理を実行する。データ処理部１３２は、ユーザインタフェース処理部１３０、通信部１３４およびデータ格納部１３６のインタフェースとしても機能する。
【００４０】
通信部１３４は、取引送信部１４６とブロック受信部１４８を含む。
取引送信部１４６は、取引データ（送金記録）を取引ネットワーク１０２にブロードキャストする。ブロック受信部１４８は、特権ノード１２０が生成するブロック１０６を受信する。
【００４１】
ユーザインタフェース処理部１３０は、入力部１３８と出力部１４０を含む。
入力部１３８は、ユーザからの各種入力を受け付ける。出力部１４０は、ユーザに対して各種情報を出力する。入力部１３８は、取引入力部１４２を含む。取引入力部１４２は、仮想通貨による取引が行われたとき、ユーザから取引内容の入力を受け付ける。
【００４２】
データ処理部１３２は、取引管理部１４４を含む。取引管理部１４４は、ブロック１０６の真正性を確認し、ブロックチェーン１０４を更新する。
【００４３】
データ格納部１３６は、ブロックチェーン１０４および公開鍵を格納する。

【００４４】
（特権ノード１２０）
特権ノード１２０は、通信部１５０、データ処理部１５２およびデータ格納部１５４を含む。
通信部１５０は、取引ネットワーク１０２を対象とした通信処理を担当する。データ格納部１５４は各種データを格納する。データ処理部１５２は、通信部１５０により取得されたデータおよびデータ格納部１５４に格納されているデータに基づいて各種処理を実行する。データ処理部１５２は、通信部１５０およびデータ格納部１５４のインタフェースとしても機能する。
【００４５】
データ処理部１５２は、ブロック生成部１６０を含む。ブロック生成部１６０は上述の方法により、ブロック生成を行う。
【００４６】
通信部１５０は、取引受信部１５６とブロック送信部１５８を含む。
取引受信部１５６は、取引ネットワーク１０２から取引データを受信し、データ格納部１５４の記憶領域であるトランザクションプールに取引データを蓄積する。ブロック送信部１５８は、生成されたブロック１０６を取引ネットワーク１０２にブロードキャストする。
【００４７】
データ格納部１５４は、ブロックチェーン１０４および秘密鍵を格納する。また、データ格納部１５４の一部にはトランザクションプールが形成され、トランザクションプールには取引データが蓄積される。
【００４８】
図７は、取引データの入力過程を示すフローチャートである。
図７に示す処理は、通常ノード１１０において、ユーザが仮想通貨による取引をしたときに実行される。取引入力部１４２は、まず、ユーザからの取引データの入力を受け付ける（Ｓ１０）。取引送信部１４６は、取引データを直ちに取引ネットワーク１０２にブロードキャストする（Ｓ１２）。
【００４９】
特権ノード１２０の取引受信部１５６は、多数の通常ノード１１０から取引データを取得し、トランザクションプールに蓄積する。一方、取引データをブロードキャストした通常ノード１１０は、取引データを含むブロック１０６の生成を待つ。
【００５０】
図８は、ブロック生成の処理過程を示すフローチャートである。
本実施形態においては、１秒に１回の頻度にて、特権ノード１２０のブロック生成部１６０はトランザクションプール（データ格納部１５４）から取引データを読み出す。図８に示す処理は、読み出しタイミング（ブロック生成のタイミング）ごとに実行される。
【００５１】
ブロック生成部１６０は、トランザクションプールに蓄積されている取引データの総データ量が所定の閾値Ｔ以上であれば（Ｓ２０のＹ）、取引データセットの一部から原データを抽出し、これを秘密鍵により暗号化することで署名値を生成する（Ｓ２２）。ブロック生成部１６０は、署名値および取引データセットを含むブロック１０６を生成する（Ｓ２４）。ブロック送信部１５８は、署名値を含むブロック１０６を取引ネットワーク１０２にブロードキャストする（Ｓ２６）。
【００５２】
取引データの総データ量が閾値Ｔ未満のときには（Ｓ２０のＮ）、Ｓ２２以降の処理はスキップされる。ブロック生成部１６０は、定期的にブロック１０６を生成するが、取引データがトランザクションプールにあまり溜まっていないときには次回の読み出しタイミングまで待ってからブロック１０６を生成する。このような処理方法により、取引が閑散としているときに中身の少ないブロック１０６（以下、「スモール・ブロック」とよぶ）

が生成されるのを防いでいる。

【００５３】

図９は、通常ノード１１０がブロックを受信したときの処理過程を示すフローチャートである。

通常ノード１１０のブロック受信部１４８は、特権ノード１２０がブロードキャストしたブロック１０６を受信する。取引管理部１４４は、ブロック１０６の署名値を公開鍵で復号し、ブロック１０６に含まれる原データと比較することにより、ブロック１０６が真正か否かを判定する（Ｓ３０）。真正であれば（Ｓ３０のＹ）、取引管理部１４４はブロックチェーン１０４にブロック１０６を追加することにより取引承認する（Ｓ３２）。真正でなければ（Ｓ３０のＮ）、Ｓ３２の処理はスキップされる。このときには、通常ノード１１０の通信部１３４は、不正なブロック１０６が検出されたことを特権ノード１２０に警告してもよい。

すべての通常ノード１１０は、受信したブロック１０６に基づいてブロックチェーン１０４を更新する。

【００５４】

図１０は、特権ノード１２０における秘密鍵１７２の使用方法を説明するための模式図である。

ブロックチェーンシステム２００の運用の前提は、特権ノード１２０のみが秘密鍵１７２を保持することである。秘密鍵１７２が他のノードに不正取得されると偽物のブロック１０６が生成されてしまう可能性がある。

【００５５】

秘密鍵の秘匿性を守るため、特権ノード１２０は、データベースＡ、Ｂ、Ｃとローカル接続される。秘密鍵１７２は、まず、暗号鍵１７４により暗号化される。暗号化された秘密鍵１７２は、更に、第１部分鍵１７２ａおよび第２部分鍵１７２ｂに分割される。データベースＡは第１部分鍵１７２ａを保存する。データベースＢは第２部分鍵１７２ｂを保存する。暗号鍵１７４はデータベースＣに保存される。通常時においては、特権ノード１２０は秘密鍵１７２も暗号鍵１７４も保存していない。このため、通常時においては、特権ノード１２０への不正アクセスが発生しても秘密鍵１７２も暗号鍵１７４も漏洩することはない。

【００５６】

トランザクションプールからの読み出しのタイミング、すなわち、ブロック生成のタイミングに至るとき、特権ノード１２０のブロック生成部１６０は、データベースＡから第１部分鍵１７２ａ、データベースＢから第２部分鍵１７２ｂを読み出し、内蔵の揮発性メモリ１７０にロードする。ブロック生成部１６０は、第１部分鍵１７２ａと第２部分鍵１７２ｂをつなげることにより、揮発性メモリ１７０上に秘密鍵１７２を生成する。この段階では、秘密鍵１７２はまだ暗号化されている。

【００５７】

続いて、ブロック生成部１６０は、データベースＣから暗号鍵１７４を読み出し、揮発性メモリ１７０に展開された秘密鍵１７２を暗号鍵１７４により復号する。ブロック生成部１６０は、復号された秘密鍵１７２に基づいて署名値を生成する。ブロック生成後、特権ノード１２０のブロック生成部１６０は揮発性メモリ１７０から秘密鍵１７２を削除する。ブロック生成のための一瞬のタイミングにおいてしか、特権ノード１２０は秘密鍵１７２を保有しない構成とすることにより、特権ノード１２０から秘密鍵１７２が漏洩するリスクを低減させている。

【００５８】

データベースＡ、Ｂ、Ｃはいずれも特権ノード１２０にローカル接続されており、インターネット等の公開型通信回線とは接続されていない。このため、これらのデータベースへの不正アクセスは生じにくくなっている。また、データベースＡ、Ｂは秘密鍵１７２の一部しか保存しないため、一方のデータベースに不正アクセスが発生しても秘密鍵１７２全体が漏洩することはない。更に、第１部分鍵１７２ａと第２部分鍵１７２ｂが漏洩した

としても、暗号鍵１７４がなければ秘密鍵１７２を使用できない。
【００５９】
データベースＣは、複数の暗号鍵を保有してもよい。たとえば、第１部分鍵１７２ａを復号するための暗号鍵Ａと第２部分鍵１７２ｂを復号するための暗号鍵Ｂをそれぞれ用意してもよい。また、ブロック生成部１６０は複数の暗号鍵を定期的に変更してもよい。
【００６０】
特権ノード１２０は、取引ネットワーク１０２とは非公開型の通信回線により接続されてもよい。具体的には、ＶＰＮ（Virtual Private Network）等の秘匿回線により接続されてもよいし、専用の有線回線により接続されてもよいし、取引ネットワーク１０２側からの特権ノード１２０へのアクセスを制限するためのファイアウォールを設けてもよい。このような制御方法によれば、特権ノード１２０およびデータベースＡ、Ｂ、Ｃへの不正アクセスをいっそう確実に防止しやすくなる。
【００６１】
以上、実施形態に基づいてブロックチェーンシステム２００を説明した。
本実施形態によれば、ブロック１０６を生成するのは唯一の特権ノード１２０であるため、分岐（フォーク）が発生することはない。また、秘密鍵で署名値を作ることでブロック１０６を生成する方式であるためブロック生成にともなう計算コストが一般的なブロックチェーン１０４に比べると格段に小さい。ビットコインでは、通常、１つのブロック１０６を生成するのに１０分程度を要する。本実施形態におけるブロックチェーンシステム２００によれば、１秒に１回程度の高頻度にてブロック１０６を生成できるため、実質的な即時決済が実現される。また、高頻度にてブロック１０６を生成できるため、１つのブロック１０６に含まれる取引データの総データ量が肥大化するのを防ぎやすい。
【００６２】
一般的なブロックチェーン１０４においては、１つのブロック１０６を生成するための時間を約１０分とするため採掘難易度を適宜コントロールしている。統計的にブロック生成の頻度が決まるため、１０分以上待たされることもありうる。これに対して、本実施形態においては、特権ノード１２０により定期的にブロック生成するため、取引者は取引データの入力からブロック生成（取引の認証）までの時間をより確実に見積もることができる。また、取引上限値が設定されないため取引承認まで待たされることもない。
【００６３】
一般的なブロックチェーン１０４と同様、通常ノード１１０は一時的なアカウントにて仮想通貨取引を実行できる。取引者は、特権ノード１２０等に自身の素性を明かす必要はない。したがって、ブロックチェーン１０４本来の魅力である「匿名性」は、本実施形態におけるブロックチェーンシステム２００においても維持できる。
【００６４】
本実施形態におけるブロックチェーンシステム２００は、採掘難易度により取引安全性を高めるという考え方ではない。したがって、取引上限値を設けなくてもブロック生成のパフォーマンスが落ちることはない。取引が活発な時期（繁忙期）であっても、特権ノード１２０は通常時と同じペースでブロック１０６を生成できる。取引が不活発な時期（閑散期）には１つのブロック１０６に含まれる取引データの量が小さくなり、繁忙期には１つのブロック１０６に含まれる取引データの量が多くなる。短期間に大量の取引が発生したときには、１つのブロック１０６に多くの取引データをまとめて記録すればよい。ブロック１０６に登録可能な取引データの総量が可変であるため、取引の活発度によってブロック生成のペースが影響されることがない。
【００６５】
一般的なブロックチェーン１０４における採掘競争の場合、競争に負ける大多数の採掘ノード１０８の計算は無駄になる。採掘には電気代等の現実的なコストがかかっている。本実施形態においては、特権ノード１２０だけがブロック生成をするため、採掘競争にともなう無駄なコストをなくすことができる。
【００６６】

また、本実施形態においては、トランザクションプールに蓄積している取引データの総データ量が閾値Ｔ以下のときには、ブロック生成はスキップされる（図８参照）。このため、スモール・ブロックの生成を抑制できる。閾値Ｔは数メガバイトであってもよいし、ゼロであってもよい。閾値Ｔをゼロとすれば取引データをまったく含まない無駄なブロック１０６が生成されるのを防ぐことができる。一般的なブロックチェーン１０４にはスモール・ブロックの生成を抑止する仕組みがない。スモール・ブロックは無駄な送金遅延を引き起こすだけでなく、取引ネットワーク１０２に対しても不必要な負荷をかけてしまう。本実施形態によれば、取引円滑性と取引活発度の双方に鑑みてスモール・ブロックの生成を避けつつ、合理的なペースにてブロック１０６を生成できる。

【００６７】

ブロック１０６の生成だけでなく、各通常ノード１１０における署名値の確認（取引承認）にも若干のコストがかかる。したがって、すべての通常ノード１１０においてブロックチェーン１０４（ブロック１０６）を同期させるためにはある程度の時間がかかる。この点からも、生成側（特権ノード１２０）だけでなく、受け入れ側（通常ノード１１０）にとってもスモール・ブロックの生成を抑制することが好ましい。

【００６８】

特権ノード１２０は、図１０に関連して説明したように、秘密鍵１７２を分離と暗号化により不正アクセスから守る。特に、ブロック生成のときだけ秘密鍵１７２を揮発性メモリ１７０に展開し、ブロック生成を完了したあとに揮発性メモリ１７０から秘密鍵１７２を消去することで秘密鍵１７２の漏洩をいっそう防ぎやすくなる。

【００６９】

なお、本発明は上記実施形態や変形例に限定されるものではなく、要旨を逸脱しない範囲で構成要素を変形して具体化することができる。上記実施形態や変形例に開示されている複数の構成要素を適宜組み合わせることにより種々の発明を形成してもよい。また、上記実施形態や変形例に示される全構成要素からいくつかの構成要素を削除してもよい。

【００７０】

［変形例］

本実施形態においては、ブロック１０６に取引上限値を設定しないとして説明した。変形例として、数メガバイトから１ギガバイト程度の取引上限値を設定してもよい。ビットコインにおけるブロック生成（採掘）を１０分に１回、本実施形態におけるブロック生成を１秒に１回と想定するならば、ブロックチェーンシステム２００はビットコインの６００倍の速度にてブロック１０６を生成できることになる。このため、仮に、比較的小さな取引上限値を設定したとしても、ブロック生成と取引承認の待ち時間を大幅に短縮できる。

【００７１】

本実施形態においては、取引データを特権ノード１２０のトランザクションプールに蓄積し、特権ノード１２０は定期的にトランザクションプールから取引データを読み出してブロック生成するとして説明した。変形例として、特権ノード１２０はいずれかの通常ノード１１０から取引データを受信するごとにブロック１０６を生成してもよい。あるいは、特権ノード１２０はトランザクションプールに蓄積される取引データの総データ量が所定の閾値Ｋ以上となるときにブロック生成をするとしてもよい。このような制御方法によれば、取引の活発度に応じてブロック生成のタイミングを自動的に調整できる。繁忙期においては高頻度でブロック生成され、閑散期には低頻度でブロック生成されることになる。また、１つのブロック１０６に含まれる取引データの総データ量のばらつきを抑制しやすくなる。

【００７２】

本実施形態においては、特権ノード１２０は１つのブロック１０６に１つの署名値を付加するとして説明した。変形例として、特権ノード１２０は１つのブロック１０６に複数の署名値を付加してもよい。たとえば、特権ノード１２０のブロック生成部１６０は、１０１バイト目から１０５バイト目までの第１の原データに基づいて第１の署名値を生成し

、１００１バイト目から１００５バイト目までの第２の原データに基づいて第２の署名値を生成してもよい。このように、取引データの総データ量が多いときほど多くの署名値を含ませてもよい。通常ノード１１０は、複数の署名値すべてについて真正性が確認されたことを条件として取引承認する。このような制御方法によれば、ブロック１０６の真正性をいっそう確実に証明しやすくなる。

【００７３】

特権ノード１２０のデータ処理部１５２は、鍵変更部（図示せず）と鍵送信部（図示せず）を備えてもよい。鍵変更部は、秘密鍵および公開鍵を定期的に変更してもよい。また、鍵変更部は、暗号鍵１７４を定期的に変更してもよい。鍵変更部は、不正アクセスまたは不正の疑いのあるアクセスが検出されたときに秘密鍵等を変更してもよい。通常ノード１１０は、署名値に基づいて真正性が確認できないブロック１０６が検出されたときには、特権ノード１２０に不正ブロックの存在を通知してもよい。このとき、特権ノード１２０の鍵変更部は、秘密鍵等を変更してもよい。また、特権ノード１２０の鍵変更部は、特権ノード１２０またはデータベースＡ、Ｂ、Ｃへの外部からのアクセスがあったときにも秘密鍵等を変更してもよい。特権ノード１２０は、あらかじめ複数種類の秘密鍵／公開鍵を用意しておき、これらの変更条件が成立したとき、秘密鍵／公開鍵のペアを変更してもよい。変更に際しては、特権ノード１２０の鍵送信部は、新規採用の公開鍵を取引ネットワーク１０２にブロードキャストすればよい。

【００７４】

図１０に示したデータベースＡ、Ｂ、Ｃの全部または一部は特権ノード１２０が内蔵するハードディスク等の不揮発性メモリであってもよい。また、各データベースは、特権ノード１２０の不揮発性メモリにおいてパーティションを分けることで形成されてもよい。

【００７５】

特権ノード１２０は、ブロック生成のタイミングにおいて、取引ネットワーク１０２との接続を遮断してもよい。特権ノード１２０は、取引ネットワーク１０２との接続を遮断後、図１０に関連して説明した処理過程により、トランザクションプールに溜まっている取引データからブロックを生成する。ブロック生成後、揮発性メモリ１７０から秘密鍵１７２等を消去する。秘密鍵１７２の消去後、取引ネットワーク１０２と再接続し、ブロック１０６をブロードキャストする。このような制御方法によれば、特権ノード１２０が秘密鍵１７２を使用するときには完全にオフラインにできるため、特権ノード１２０から秘密鍵１７２が漏洩するリスクをいっそう低減できる。

【００７６】

本実施形態においては、取引データセットの一部を原データとし、この原データから署名値を作るとして説明した。変形例として、特権ノード１２０は任意の原データを生成し、この原データから署名値を生成してもよい。ブロック１０６は、特権ノード１２０が指定する原データおよび署名値を含んでいればよい。

【００７７】

本実施形態においては、特権ノード１２０が生成したブロック１０６は、ブロックチェーン１０４につなげられるとして説明した。本実施形態の場合、必ずしも「チェーン」である必要はない。図２に示したような適正ハッシュ値によるつながりを作る必要がないためである。たとえば、特権ノード１２０は、ブロック１０６に生成日時（日時情報）を記録した上で取引ネットワーク１０２にブロック１０６をブロードキャストし、通常ノード１１０は署名値の真正性を確認した上で、このブロック１０６を正式に受け入れるか否かを判定してもよい。ブロック１０６には日時情報が含まれているため、複数のブロック１０６の日時情報を参照することにより、取引の順番を後から確認できる。

【００７８】

本実施形態においては、仮想通貨による取引を前提として説明した。ブロック１０６に登録される取引データは仮想通貨取引以外のものであってもよい。たとえば、取引者Ａが取引者Ｂにモノ（有体物または無体物）を渡したとき、その取引データをブロック１０６に登録してもよい。この場合には、ブロックチェーン１０４により、取引者Ａから取引者

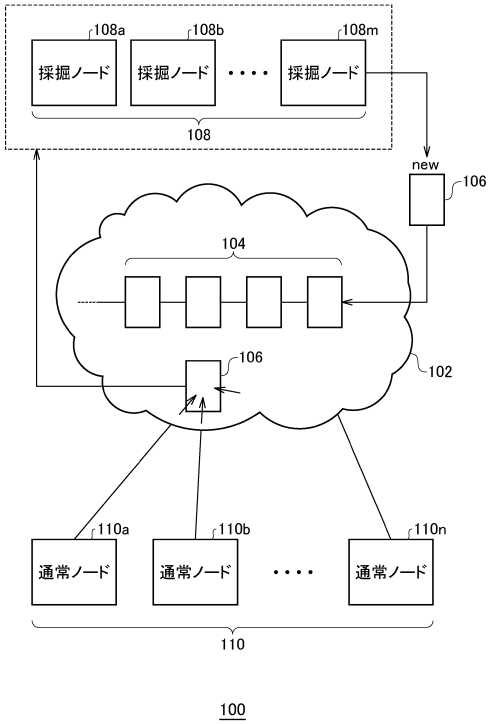
Ｂにモノの所有権が移転していることを確認できる。このように、ブロックチェーンシステム２００は、仮想通貨（金銭等価物）に限らず、モノや情報の所有権の管理に利用することもできる。

【符号の説明】

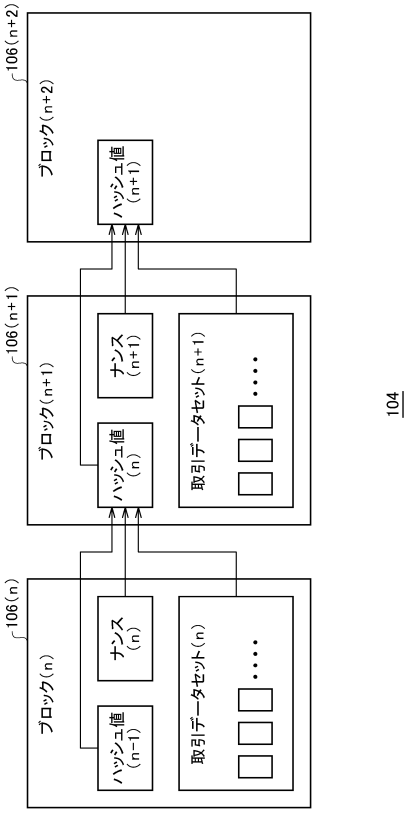
【００７９】

１００　ブロックチェーンシステム、１０２　取引ネットワーク、１０４　ブロックチェーン、１０６　ブロック、１０８　採掘ノード、１１０　通常ノード、１２０　特権ノード、１３０　ユーザインタフェース処理部、１３２　データ処理部、１３４　通信部、１３６　データ格納部、１３８　入力部、１４０　出力部、１４２　取引入力部、１４４　取引管理部、１４６　取引送信部、１４８　ブロック受信部、１５０　通信部、１５２　データ処理部、１５４　データ格納部、１５６　取引受信部、１５８　ブロック送信部、１６０　ブロック生成部、１７０　揮発性メモリ、１７２　秘密鍵、１７２ａ　第１部分鍵、１７２ｂ　第２部分鍵、１７４　暗号鍵、２００　ブロックチェーンシステム

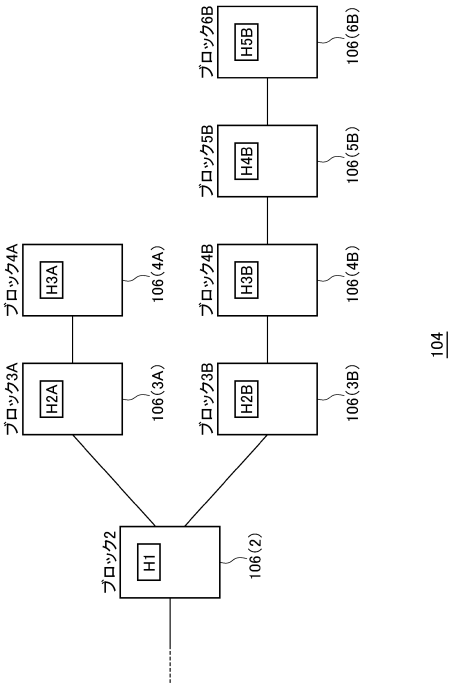
【図１】



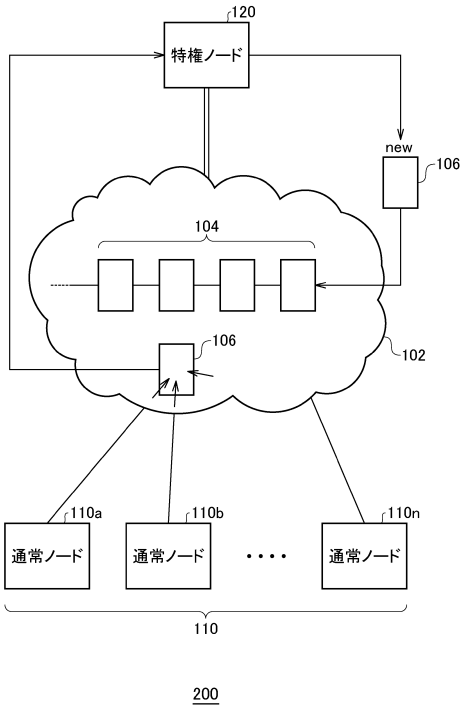
【図２】



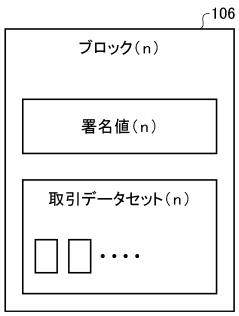
【図３】


ブロック6B
H5B
106(6B)
ブロック5B
H4B
106(5B)
ブロック4A
H3A
106(4A)
ブロック4B
H3B
106(4B)
ブロック3A
H2A
106(3A)
ブロック3B
H2B
106(3B)
ブロック2
H1
106(2)
104

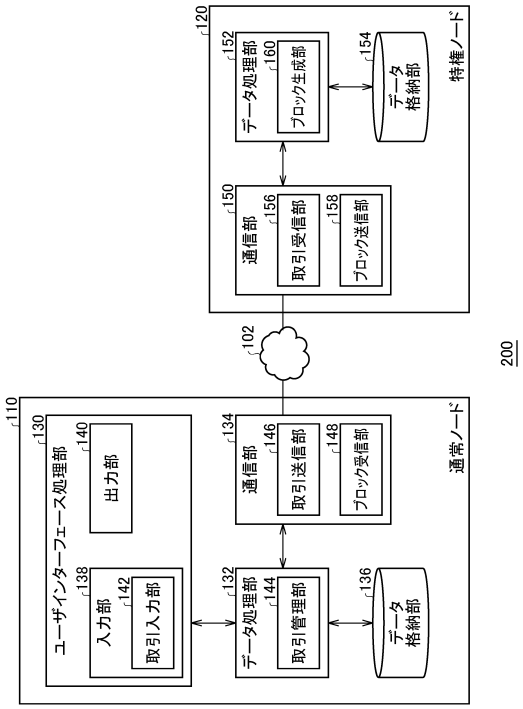
【図４】


120
特権ノード
new
106
104
106
102
110a
110b
110n
通常ノード
通常ノード
通常ノード
110
200

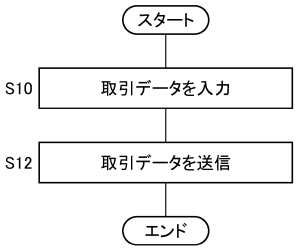
【図５】


106
ブロック(n)
署名値(n)
取引データセット(n)

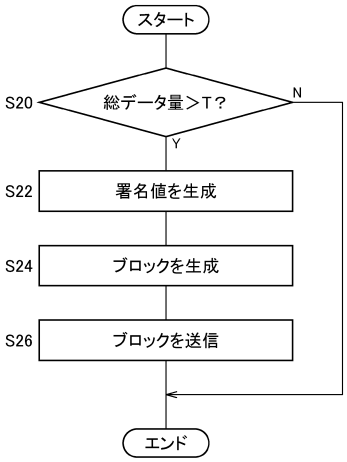
【図６】


120
特権ノード
データ処理部
152
ブロック生成部
160
データ格納部
154
通信部
150
取引受信部
156
ブロック送信部
158
102
200
110
通常ノード
ユーザインターフェース処理部
130
出力部
140
入力部
138
取引入力部
142
通信部
134
取引送信部
146
ブロック受信部
148
データ処理部
132
取引管理部
144
データ格納部
136

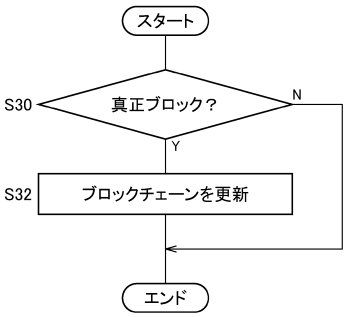
【図７】


スタート
S10
取引データを入力
S12
取引データを送信
エンド

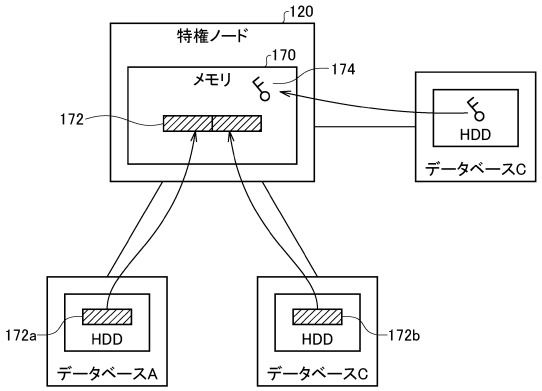
【図８】


スタート
S20
総データ量＞T？
N
Y
S22
署名値を生成
S24
ブロックを生成
S26
ブロックを送信
エンド

【図９】


スタート
S30
真正ブロック？
N
Y
S32
ブロックチェーンを更新
エンド

【図１０】


120
特権ノード
170
メモリ
174
172
HDD
データベースC
172a
HDD
データベースA
HDD
172b
データベースC

フロントページの続き

合議体
審判長　田中　秀人
審判官　石井　茂和
審判官　塚田　肇

(56)参考文献　特開２００３－２８０９７２（ＪＰ，Ａ）
特開２０１０－１８７４１９（ＪＰ，Ａ）
特開２０１７－２０４０７０（ＪＰ，Ａ）
特開２０１０－００４３７９（ＪＰ，Ａ）
国際公開第２００５／１０４４３０（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/32, G06F 21/64, G06Q 20/40