(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7559111号
(P7559111)

(45)発行日　令和6年10月1日(2024.10.1)

(24)登録日　令和6年9月20日(2024.9.20)

(51)国際特許分類

		FI		
G06F	*9/50*	*(2006.01)*	G06F	9/50	150Z
H04L	*45/16*	*(2022.01)*	H04L	45/16	

請求項の数　18　外国語出願　（全21頁）

(21)出願番号　特願2023-28186(P2023-28186)
(22)出願日　令和5年2月27日(2023.2.27)
(62)分割の表示　特願2022-159994(P2022-159994)の分割
原出願日　平成30年6月19日(2018.6.19)
(65)公開番号　特開2023-71805(P2023-71805A)
(43)公開日　令和5年5月23日(2023.5.23)
審査請求日　令和5年2月27日(2023.2.27)
(31)優先権主張番号　1709848.4
(32)優先日　平成29年6月20日(2017.6.20)
(33)優先権主張国・地域又は機関
英国(GB)

(73)特許権者　318001991
エヌチェーン ライセンシング アーゲー
スイス・６３００・ツーク・グラーフェナウヴェーク・６
(74)代理人　100107766
弁理士　伊東 忠重
(74)代理人　100070150
弁理士　伊東 忠彦
(74)代理人　100135079
弁理士　宮崎 修
(72)発明者　デステファニス，ジュゼッペ
イギリス国 シーエフ１０　２エイチエイチ カーディフ チャーチル ウェイ チャーチル ハウス ７ス フロア アーカート－ダイクス アンド ロード エルエルピー

最終頁に続く

(54)【発明の名称】　ブロックチェーン・ネットワークにおける高速伝搬のための方法及び特殊ネットワーク・ノード

(57)【特許請求の範囲】

【請求項１】

ブロックチェーン・ノードのネットワークにおいてブロックチェーン・トランザクションの高速伝搬を促進するように配置及び構成された特殊ネットワーク・ノードであって、

ｉ）前記特殊ネットワーク・ノードは、特殊ネットワーク・ノードのオーバーレイ・ネットワークであって前記ブロックチェーン・ノードのネットワークに対するオーバーレイ・ネットワークのノードであり；

ii）前記特殊ネットワーク・ノードは：

少なくとも１つのプロセッサ；

ネットワーク・インターフェース；

メモリ；及び

プロセッサ実行可能な命令を含むブロックチェーン特殊ネットワーク・ノード・アプリケーション；

を含み、前記命令は、前記プロセッサにより実行されると、前記特殊ネットワーク・ノードに、ブロックチェーン・トランザクションを伝搬させる又は伝搬を開始させる、特殊ネットワーク・ノード。

【請求項２】

請求項１に記載の特殊ネットワーク・ノードにおいて、前記特殊ネットワーク・ノードのオーバーレイ・ネットワークは：

ｉ）前記ブロックチェーン・ノードのネットワーク内に分散されたサブ・ネットワークを

形成しているか、又は
ii）前記ブロックチェーン・ノードのネットワークとは物理的に別個のものである、特殊ネットワーク・ノード。
【請求項３】
請求項２に記載の特殊ネットワーク・ノードにおいて、前記特殊ネットワーク・ノードのオーバーレイ・ネットワークは、非セントラル化されたＩＰマルチキャスト・タイプのネットワークとして実装されている、特殊ネットワーク・ノード。
【請求項４】
請求項１－３のうちの何れか１項に記載の特殊ネットワーク・ノードにおいて、前記特殊ネットワーク・ノードは、未承認ブロックチェーン・トランザクションを受信するように構成されている、特殊ネットワーク・ノード。
【請求項５】
請求項１－４のうちの何れか１項に記載の特殊ネットワーク・ノードにおいて、前記命令が前記特殊ネットワーク・ノードに伝搬させる又は伝搬を開始させる前記ブロックチェーン・トランザクションは、未承認ブロックチェーン・トランザクションである、特殊ネットワーク・ノード。
【請求項６】
請求項１－５のうちの何れか１項に記載の特殊ネットワーク・ノードにおいて、前記命令は、前記特殊ネットワーク・ノードが、前記ブロックチェーン・トランザクションの真正を確認する検証動作を実行することを引き起こすように構成されている、特殊ネットワーク・ノード。
【請求項７】
請求項１－６のうちの何れか１項に記載の特殊ネットワーク・ノードにおいて、前記特殊ネットワーク・ノードは、前記ブロックチェーン・トランザクションを、少なくとも１つの他の特殊ネットワーク・ノードへ伝搬させる又は伝搬を開始させるように構成されている、特殊ネットワーク・ノード。
【請求項８】
請求項１－７のうちの何れか１項に記載の特殊ネットワーク・ノードにおいて、前記特殊ネットワーク・ノードは、前記ブロックチェーン・トランザクションを、前記ブロックチェーン・ノードのネットワークにおける少なくとも１つのブロックチェーン・ノードへ伝搬させる又は伝搬を開始させるように構成されている、特殊ネットワーク・ノード。
【請求項９】
請求項１－８のうちの何れか１項に記載の特殊ネットワーク・ノードおいて、前記特殊ネットワーク・ノードは、前記ブロックチェーン・トランザクションを、マルチキャストを用いて、前記オーバーレイ・ネットワークにおける少なくとも１つの他の特殊ネットワーク・ノードへ伝搬させる又は伝搬を開始させることにより、前記ブロックチェーン・トランザクションの高速伝搬を促進するように構成されている、特殊ネットワーク・ノード。
【請求項１０】
請求項１－９のうちの何れか１項に記載の特殊ネットワーク・ノードにおいて、前記特殊ネットワーク・ノードは、前記ブロックチェーン・トランザクションを、前記オーバーレイ・ネットワークにおける複数の又は全ての特殊ネットワーク・ノードへ、前記オーバーレイ・ネットワークにおける前記複数の又は全ての特殊ネットワーク・ノードのマルチキャスト・アドレスを用いて伝搬させる又は伝搬を開始させるように構成されている、特殊ネットワーク・ノード。
【請求項１１】
請求項１０に記載の特殊ネットワーク・ノードにおいて、前記特殊ネットワーク・ノードは、前記トランザクションを、前記特殊ネットワーク・ノードのオーバーレイ・ネットワークの全ての特殊ネットワーク・ノードへ伝搬させるために、少なくとも１つの他のマルチキャスト・アドレスへの前記ブロックチェーン・トランザクションの他の伝搬が必要とされるか否かを評価するように構成されている、特殊ネットワーク・ノード。

【請求項１２】
請求項１１に記載の特殊ネットワーク・ノードにおいて、他のブロードキャストが必要とされる旨の決定に基づいて、前記ブロックチェーン・トランザクションを、少なくとも１つの他のマルチキャスト・アドレスへ伝搬させるように構成されている、特殊ネットワーク・ノード。
【請求項１３】
請求項１－１２のうちの何れか１項に記載の特殊ネットワーク・ノードにおいて、前記特殊ネットワーク・ノードは、ブロックチェーンの完全なコピーを保存していない、特殊ネットワーク・ノード。
【請求項１４】
請求項１－１３のうちの何れか１項に記載の特殊ネットワーク・ノードにおいて、前記特殊ネットワーク・ノードは、マイニング機能を実行しない、特殊ネットワーク・ノード。
【請求項１５】
請求項１－１４のうちの何れか１項に記載の特殊ネットワーク・ノードにおいて、前記特殊ネットワーク・ノードは、前記ブロックチェーン・ノードのネットワーク内の非特殊ネットワーク・ノードに対して、より多い数の進入及び進出コネクションが許容され、それにより、前記特殊ネットワーク・ノードは、前記ブロックチェーン・ノードより速やかにトランザクションを伝搬させることができるようになる、特殊ネットワーク・ノード。
【請求項１６】
複数の特殊ネットワーク・ノードを含むオーバーレイ・ネットワークであって、各々の特殊ネットワーク・ノードは、請求項１に記載されているように配置及び構成されている、オーバーレイ・ネットワーク。
【請求項１７】
１つ以上の非特殊ネットワーク・ノード、及び請求項１に記載されているように配置及び構成されている複数の特殊ネットワーク・ノードを含むオーバーレイ・ネットワークを有するブロックチェーン・ネットワークであって、前記非特殊ネットワーク・ノードのうちの少なくとも１つはマイニング機能を実行する、ブロックチェーン・ネットワーク。
【請求項１８】
ブロックチェーンを実現するために使用される相互接続された複数のノードのネットワークを介してブロックチェーン・トランザクションの高速伝搬を促進するコンピュータで実現される方法であって、前記複数のノードの部分集合は、相互接続されたノードのネットワークに対するオーバーレイ・ネットワークにより相互接続された特殊ネットワーク・ノードであり、前記方法は：
特殊ネットワーク・ノードにおいて、未承認ブロックチェーン・トランザクションを受信するステップ；
前記特殊ネットワーク・ノードが、前記未承認ブロックチェーン・トランザクションを検証するステップ；及び
前記特殊ネットワーク・ノードが、その未承認ブロックチェーン・トランザクションを、少なくとも１つの他の特殊ネットワーク・ノードへブロードキャストするステップ；
を含み、前記高速伝搬は、（i）前記未承認ブロックチェーン・トランザクションを前記少なくとも１つの他の特殊ネットワーク・ノードへブロードキャストするマルチキャスト及び（ii）非特殊ネットワーク・ノードに対して許容されているものより多い数の進入及び進出コネクションを有する前記特殊ネットワーク・ノード、のうちの少なくとも１つを用いた結果として達成される、方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は一般に分散された台帳（ブロックチェーン）ネットワークに関連する。特に、本発明はブロックチェーン・ネットワークのパフォーマンスを改善し、及び／又はネットワーク上で転送が実行され得る速度を増大させる暗号強制方法及びシステムに関連し得る。

【背景技術】
【０００２】
本書では電子的なコンピュータ・ベースの分散型の全ての形態の台帳を含むように用語「ブロックチェーン」を使用する。これらは、ブロックチェーン及びトランザクション・チェーン技術、許可された及び許可されていない台帳、共有台帳、並びにそれらの変形を含むが、これらに限定されない。ブロックチェーン技術の最も広く知られている応用はビットコイン台帳であるが、他のブロックチェーン実装が提案され開発されている。本願では、便宜上及び説明の目的でビットコインが参照されるかもしれないが、本発明は、ビットコイン・ブロックチェーンで使用することに限定されず、代替的なブロックチェーンの実装及びプロトコルが、本発明の範囲内に属することに留意すべきである。
【０００３】
ブロックチェーンはコンセンサス・ベースの電子台帳であり、これはトランザクションにより構成されるブロックにより構成される、コンピュータ・ベースの非セントラル化された分散システムとして実装される。各々のトランザクション（Ｔｘ）は、ブロックチェーン・システム内の参加者間でディジタル資産の支配権の移転をエンコードし、少なくとも１つのインプットと少なくとも１つのアウトプットとを含む。各ブロックは先行するブロックのハッシュを含み、その結果、ブロックは、開始以来ブロックチェーンに書き込まれてきた全てのトランザクションについての永続的で変更不可能な記録を作成するように一緒に鎖で繋がれる。トランザクションは、トランザクションのインプット及びアウトプットに組み込まれるスクリプトとして知られる小さなプログラムを含み、スクリプトは、トランザクションのアウトプットがどのように誰によってアクセスされ得るかを指定する。ビットコイン・プラットフォームでは、これらのスクリプトはスタック・ベースのスクリプト言語を使用して書かれる。
【０００４】
新たなトランザクションを受信したネットワーク・ノードは、ネットワーク内の他のノードへ、そのトランザクションを速やかにプッシュしようとするであろう。新たなトランザクションを他のノードへ送信する前にそれは「検証され（ｖａｌｉｄａｔｅｄ）」、検証は、トランザクションが、適用可能なブロックチェーン・プロトコルに従って適切なトランザクションの基本要件を満足していることを保証するために、一組の基準に対して検査されることを意味する。
【０００５】
トランザクションがブロックチェーンに書き込まれるために、トランザクションはノード（「マイナー」）によりブロック内に組み込まれ、そのノードはトランザクションを収集してそれらをブロックに形成するように設計されている。次いで、マイナーはノードに関する「プルーフ・オブ・ワーク」を完了しようとする。ブロックチェーン・ネットワーク中のマイナー達は、トランザクションのブロックを組み立て、ブロックに関する作業についての関連する証明を完了するために、１番になろうと競争する。成功したマイナーは、確認されたブロックをブロックチェーンに追加し、そのブロックはネットワークに伝搬され、その結果、ブロックチェーンのコピーを保持する他のノードは、各自の記録を更新することができる。ブロックを受信したこれらのノードもまたブロック及びその中の全てのトランザクションを「検証」し、それがプロトコルの正式な要件に従っていることを保証する。
【０００６】
ブロックチェーンの実装に関連するボトルネックの１つは、プルーフ・オブ・ワークを完了するまでマイナーを待機することに関連する遅延であり、プルーフ・オブ・ワークは、トランザクションのブロックを確認し、トランザクションのそのブロックをブロックチェーンに追加する結果をもたらす。一例としてビットコイン・システムを用いると、設計により、システムはブロックが確認されてブロックチェーンに追加されるまで約１０分を要する。一方、未承認のトランザクションはメモリ・プール（本願では「メンプール」（ｍｅｍｐｏｏｌ）と言及される）に溜まり、その完全なコピーがネットワーク内の各ノー

ドで維持される。ビットコイン・アーキテクチャの分析は、１０分のブロック承認スループットの場合、典型的なトランザクション及びブロックのサイズに基づいて、及び蓄積されたそれらの未承認トランザクションが新たなブロックに組み込まれ得る速度に基づいて、システムは、毎秒約３つの新たな未承認トランザクションというトランザクション・スループットを処理することが可能である。

【０００７】

ビットコインのようなブロックチェーンに基づくネットワークを利用して、広く行き渡った暗号的に保護される交換の利用を可能にする又は促進することは有益であろう。そのような交換は、例えば、クレジット・カード・トランザクション等に関する支払処理に関連し得る。しかしながら毎秒約３つというトランザクション・スループットは、毎秒約５０，０００というトランザクション量で現在動作しているそのような電子決済を処理するには不十分である。従って、大量のトランザクションを処理するために、ブロックチェーンの能力を現在制限しているスピード及びスケーラビリティの制約に対するソリューションを見出すことが望ましい。

【発明の概要】

【０００８】

今やそのようなソリューションが発明されている。

【０００９】

即ち、本発明によれば、添付の特許請求の範囲に記載されているような方法及びデバイスが提供される。

【００１０】

本願は、トランザクション処理の高速化／スピード改善のためにブロックチェーンを実装するように設計される専用マーチャント・ノード（ｄｅｄｉｃａｔｅｄ　ｍｅｒｃｈａｎｔ　ｎｏｄｅｓ）のネットワークによりブロックチェーン・トランザクション（ＴＸｓ）の高速伝搬を可能にする方法及びデバイスを説明及び開示する。用語「トランザクション」は金融の意味における取引以外の「ブロックチェーン・トランザクション」（即ち，Ｔｘ）を意味するものとして解釈され得る。ネットワーク・トラフィックを最小化し、記憶容量制限を緩和するために、ブロックへの組み込みを待機しているペンディング・トランザクションのメモリ・プール（「メンプール」）は、分散ハッシュ・テーブル（ＤＨＴ）により実現される分散メモリ・プールとして、特殊（マーチャント）ノード（ｔｈｅ　ｓｐｅｃｉａｌｉｓｅｄ（ｍｅｒｃｈａｎｔ）ｎｏｄｅｓ）内に格納されることが可能である。マーチャント・ノードにより受信された新たなトランザクションはハッシュされたその識別子を有することが可能であり、マーチャント・ノードは、それが分散されたメンプールに既に格納されているか否かを評価することができる。格納されていない場合、適用可能なＤＨＴプロトコルを利用して適切な１つ以上のマーチャント・ノードにおける分散されたメンプールにそれが格納され得る。マーチャント・ノードは次いで通常のピア・ツー・ピア・コネクションを利用してトランザクションＴｘを通常の非マーチャント・ノードへ送信してもよいが；トランザクションを全ての他のマーチャント・ノードへ送信する必要はない。

【００１１】

追加的又は代替的な態様において、本願は、ブロックチェーンを実現するために使用される相互接続されたノードのネットワーク上でブロックチェーン・トランザクションの（高速）分散を促す特殊ネットワーク・ノードを説明しており、相互接続されたノードの部分集合はオーバーレイ・ネットワークで相互接続された特殊ネットワーク・ノードである。以後、用語「特殊ネットワーク」は、便宜上の目的に限り用語「ＳＮ」又は「マーチャント・ノード」と可換に使用され得る。

【００１２】

幾つかの実装において、ＤＨＴの形式でメンプールを実現及び管理するために特殊ネットワーク・ノードのオーバーレイ・ネットワークを利用することは、全てのネットワーク・ノードでメンプールを実装することに勝る、演算速度及び伝搬速度の恩恵を提供するこ

とができる。更に、ブロックチェーン・ノードの正規のネットワークに対してオーバーレイ・ネットワークで特殊ネットワーク・ノードを利用することは、ブロックチェーン・ノードの全ネットワークにわたってＤＨＴメンプールを実現することについての予想されるスピード及び信頼性の複雑化した事態を回避し、各ノードはＤＨＴの非常に小さな部分を格納及び保持する。この構造は、非特殊ノードが特殊ノードのうちの１つを介してメンプールに速やかに問い合わせることを許容できる。マイニング・ノード等のオーバーレイ・ネットワーク以外のノードが、必要に応じて部分的な又は完全なメンプールを維持できることを保証するためにＤＨＴを更新した後に、特殊ネットワーク・ノードがピア・ツー・ピア通信を利用してオーバーレイ・ネットワーク以外の非特殊ネットワークへの伝搬を開始することは、更に有益であろう。他のスピード及びストレージの恩恵は、例示的な実装の説明から明らかになるように、本願の様々な態様により実現され得る。

【００１３】

ＳＮノードは、プロセッサ；分散ハッシュ・テーブルとして構造化された分散されたメンプールのうちの指定された部分を格納するメモリであって、分散されたメンプールはコンファメーション（承認）を待機しているペンディング・トランザクションを含む、メモリ；ネットワーク・インターフェース；及びプロセッサ実行可能な命令を含むブロックチェーンＳＮノード・アプリケーションを含むことが可能である。命令は、実行されると、プロセッサに：トランザクション識別子を含むトランザクションを受信すること；（暗号）キーを得るためにトランザクション識別子をハッシュすること；分散されたメンプールにトランザクションが格納されているか否かをキーを利用して確認し、格納されていない場合、トランザクションをペンディング・トランザクションとして分散されたメンプールに格納すること；及びトランザクションをＳＮノード以外のノード群へピア・ツー・ピア・コネクションを利用して送信することを行わせることができる。

【００１４】

幾つかの実装において、メモリは、トランザクションを含むブロックであってブロックチェーンに含まれるブロックの承認数に関するデータを更に格納してもよく、命令は、承認数が最小数に到達した場合に、分散されたメンプールからトランザクションを取り除くことをプロセッサに行わせる。幾つかの例において、承認数に関するデータは、ブロックチェーンに追加される新たなブロック各々に関して更新される承認数のカウント、又はトランザクションが含まれるブロックのブロック番号の何れかであってもよい。

【００１５】

幾つかの実装において、メモリはＳＮノード評判テーブルを更に格納することが可能であり、ＳＮノード評判テーブルは、何らかの検出された新たな近隣のＳＮノードに関する識別子と、新たな近隣のマーチャント・ノードの検出された活動（又はアクティビティ）に基づく新たな近隣のマーチャント・ノードの関連するスコアとを含む。幾つかの例において、命令は、新たな近隣のＳＮノードのスコアを更新すること、新たな近隣のＳＮノードのスコアが閾値より下に落ち込んだことを判定し、その結果、新たな近隣のＳＮノードを悪意のノードとして指定し、新たな近隣のＳＮノードを孤立させることをプロセッサに行わせる。

【００１６】

幾つかの実装において、分散されたメンプールのうちの指定された部分は、別のＳＮノードに格納された分散されたメンプールの第２部分と部分的にオーバーラップしている。

【００１７】

幾つかの実装において、各々のＳＮノードは、分散されたメンプールの各自指定された部分を格納し、各自指定された部分は、各々のペンディング・トランザクションが少なくとも２つのＳＮノードに格納されるが、全てのＳＮノードには格納されないように部分的にオーバーラップしていてもよい。選択的に、各々のペンディング・トランザクションは、分散されたメンプールの各自指定された２つに過ぎない部分に含まれる。

【００１８】

追加的又は代替的に、本願はブロックチェーンを実現するために使用されるネットワー

クに結合される複数のノードに関わるブロックチェーン転送（例えば、トランザクション）を促進するコンピュータ実現方法を提供することが可能であり、複数のノードのうちの部分集合はＳＮノードであり、ＳＮノードは、承認を待機するペンディング・トランザクションを含む分散されたメンプールを格納し、分散されたメンプールはＳＮノード群の中で分散されたハッシュ・テーブルとして実現される。本方法（ＳＮノードのうちの１つで実現され得る）は、トランザクション識別子を含むトランザクションを受信するステップ；キーを得るためにトランザクション識別子をハッシュするステップ；分散されたメンプールにトランザクションが格納されているか否かをキーを利用して確認し、格納されていない場合、トランザクションをペンディング・トランザクションとして分散されたメンプールに格納するステップ；及びトランザクションをＳＮノード以外のノード群へピア・ツー・ピア・コネクションを利用して送信するステップを含むことができる。

【００１９】

追加的又は代替的に、本願は複数の参加ノードの中でブロックチェーン・トランザクションに参加するためのプロセッサ実行可能命令を格納する非一時的なプロセッサ読み取り可能な媒体を提供することが可能であり、プロセッサ実行可能な命令は、参加ノードのうちの１つでプロセッサにより実行されると、本願で説明される１つ以上の方法をプロセッサに実行させる。

【図面の簡単な説明】

【００２０】

本発明のこれら及び他の態様は、本願で説明される実施形態から明らかになり且つ実施形態に関連して説明される。本発明の実施形態は、単なる例示に過ぎないものとして添付図面に関連して説明される。

【００２１】

【図１】図１はマーチャント（ＳＮ）ノードのオーバーレイ・ネットワークとともにノードのネットワーク例を示す。

【００２２】

【図２】図２は新たなトランザクションを分散されたメンプールに格納するプロセスを示すシーケンス図を示す。

【００２３】

【図３】図３はブロックチェーン・ネットワークでトランザクションを伝搬させる方法の一例をフローチャート形式で示す。

【００２４】

【図４】図４は簡略化された例示的なＭノードをブロック図形式で示す。

【００２５】

【図５】図５はＭネットに参加する新たなノード例を示すシーケンス図を示す。

【００２６】

【図６】図６はＭノード登録テーブル例を概略的に示す。

【００２７】

【図７】図７は例示的なメンプール・データ・エントリを示す。

【発明を実施するための形態】

【００２８】

本願において、用語「及び／又は」は、列挙された要素の全ての可能なコンビネーション及びサブ・コンビネーションをカバーするように意図され、列挙された任意の１つの要素単独、任意のサブ・コンビネーション、又は全ての要素を含み、必ずしも追加的な要素を排除することを要しない。

【００２９】

本願において、「・・・又は・・・の少なくとも１つ」という言い回しは、列挙された要素のうちの任意の１つ以上をカバーするように意図され、列挙された任意の１つの要素単独、任意のサブ・コンビネーション、又は全ての要素を含み、必ずしも何らかの追加的な要素を排除することを必要とせず、必ずしも全ての要素を必須としない。

【００３０】
先ず図１を参照すると、図１はブロックチェーンに関連するネットワーク例をブロック図形式で示しており、そのネットワークは本願でブロックチェーン・ネットワーク１００と言及され得る。ブロックチェーン・ネットワーク１００は、招待無しに又は他のメンバーからの同意無しに誰でも参加し得るピア・ツー・ピア・オープン・メンバーシップ・ネットワークである。ブロックチェーン・ネットワーク１００はブロックチェーン・プロトコルの下で動作し、そのブロックチェーン・プロトコルのインスタンスを実行する分散された電子デバイスは、ブロックチェーン・ネットワーク１００に参加することができる。そのような分散された電子デバイスはノード１０２と言及され得る。ブロックチェーン・プロトコルは、例えばビットコイン・プロトコル、又は他の暗号通貨であってもよい。
【００３１】
ブロックチェーン・プロトコルを実行し且つブロックチェーン・ネットワーク１００のノード１０２を形成する電子デバイスは様々なタイプのものであるとすることが可能であり、例えば、デスクトップ・コンピュータ、ラップトップ・コンピュータ、タブレット・コンピュータ、サーバー等のコンピュータ、スマートフォン等のモバイル・デバイス、スマート・ウォッチ等のウェアラブル・コンピュータ、又は他の電子デバイスを含む。
【００３２】
ブロックチェーン・ネットワーク１００のノード１０２は、有線及び無線通信技術を含み得る適切な通信技術を利用して互いに結合されている。多くのケースにおいて、ブロックチェーン・ネットワーク１００は少なくとも部分的にインターネット上で実現され、幾つかのノード１０２は地理的に分散した場所に位置していてもよい。
【００３３】
ノード１０２はブロックチェーンにおける全てのトランザクションのグローバル台帳を維持し、ブロックチェーンはブロックにグループ化され、各ブロックは、チェーンの中で先行するブロックのハッシュを含む。グローバル台帳は分散された台帳であり、各ノード１０２はグローバル台帳の完全なコピー又は部分的なコピーを格納することが可能である。グローバル台帳に影響を及ぼすノード１０２によるトランザクションは、他のノード１０２により検証され、その結果、グローバル台帳の有効性が維持される。ビットコイン・プロトコルを使用するもの等のブロックチェーン・ネットワークの実現及び動作の詳細は、当業者により理解されるであろう。
【００３４】
各々のトランザクションは典型的には１つ以上のインプットと１つ以上のアウトプットとを有する。インプット及びアウトプットに埋め込まれるスクリプトは、トランザクションのアウトプットがどのように誰によりアクセスされ得るかを指定する。トランザクションのアウトプットは、トランザクションの結果として、価値（ａ　ｖａｌｕｅ）が移転される先のアドレスであってもよい。そしてその価値は、未使用トランザクション・アウトプット（ＵＴＸＯ）としてその出力アドレスに関連付けられる。そして、以後のトランザクションは、その価値を使用又は消却するために、そのアドレスを入力として参照することができる。
【００３５】
ノード１０２は各自の機能に応じて様々なタイプ又はカテゴリのものであってよい。ノード１０２に関連する４つの基本機能が存在することが示唆されており、ウォレット、マイニング、フル・ブロックチェーン・メンテナンス、及びネットワーク・ルーティングである。これらの機能の変形が存在してもよい。ノード１０２は１つより多い機能を有することが可能である。例えば、「フル・ノード」は４つ全ての機能を提供する。ライトウェイト・ノードは例えばディジタル・ウォレットで実装されてもよく、ウォレット及びネットワーク・ルーティング機能のみを発揮してもよい。完全なブロックチェーンを格納するのではなく、ディジタル・ウォレットはブロック・ヘッダを追跡することが可能であり、ブロック・ヘッダは、ブロックを問い合わせる場合にインデックスとして役立つ。ノード１０２は、ＴＣＰ／ＩＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ

）等のコネクション指向プロトコルを利用して互いに通信する。
【００３６】
本願はマーチャント・ノード１０４（時折「Ｍ－ノード」１０４のように言及される）という追加的なタイプ又はカテゴリのノードを提案及び説明している。Ｍ－ノード１０４はトランザクションの高速伝搬に焦点を当てて設計されている。それらは完全なブロックチェーンを保存せず、マイニング機能を実行しない。その意味において、それらはライトウェイト・ノード又はウォレットに類似している；しかしながら、それらはトランザクションの高速伝搬を可能にする追加的な機能を含む。Ｍ－ノード１０４の動作議論の中心は、迅速な検証及び特に他のＭ－ノード１０４に対する未承認トランザクションの伝搬であり、該他のＭ－ノード１０４から、未承認トランザクションが、ブロックチェーン・ネットワーク１００における他のノード１０２へ速やかにプッシュされる。この機能を促進するため、Ｍ－ノード１０４は非常に多数の入って来る及び特に出て行くコネクションを許容されており、それらのコネクションは管理プロトコルのもとでは別の方法でノード１０２に許容されるかもしれない。
【００３７】
Ｍ－ノード１０４はまとめてマーチャント・ネットワーク１０６（又は「Ｍ－ネット」１０６）と言及されてもよい。用語「マーチャント」は「特殊化された（ｓｐｅｃｉａｌｉｓｅｄ）を意味するものとして解釈され得る。図示の簡明化のため、図１では物理的に別個のネットワークとして示されているが、Ｍ－ノード１０４はブロックチェーン・ネットワーク１００に統合されてもよい。各々のＭ－ノード１０４は、ブロックチェーン・ネットワーク１００における特殊ノードであり、Ｍ－ノード１０４の機能を実行し得ることを保証する所定のハードウェア及びパフォーマンス能力を満たす。即ち、Ｍ－ネット１０６は、ブロックチェーン・ネットワーク１００の中にあり且つブロックチェーン・ネットワーク１００を通じて分散されているサブ・ネットワークと考えられてよい。Ｍ－ノードは１つ以上の専用の機能又はサービスを実行するように配置及び構成され得る。
【００３８】
Ｍ－ネット１０６が確実に動作し且つ所定のセキュリティ・レベルでサービスを提供するために、Ｍ－ノード１０４はＭ－ネット１０６全体についての良い外観を維持する必要があり、従って効率的なルーティング・プロトコルが配備される必要がある。Ｍ－ノード１０４が開始トランザクションを受信する度に、Ｍ－ノード１０４はそれを他のノード１０２に加えて幾つかの他のＭ－ノード１０４へブロードキャストする必要がある。Ｍ－ネット１０６の側面では、これは複数巡回セールスマン問題（ＭＴＳＰ）に対するソリューションを発見することに等しい。この問題に対処する非常に多くのソリューションが存在し、それらのうちの任意の１つがＭ－ネット１０５で使用され得る。Ｍ－ノード１０４の各々は何らかの最新の形式でルーティング最適化を行う。
【００３９】
幾つかの実装において、Ｍ－ネット１０６は非セントラル化ＩＰマルチキャスト・タイプのネットワークとして実現される。即ち、到来するトランザクションのブロックチェーン・ネットワーク１００への速やかな拡散を可能にするために、マルチキャストが使用されてトランザクションがＭ－ネット１０６を通じて速やかにブロードキャストされることを保証し、全てのＭ－ノード１０４が、ブロックチェーン・ネットワーク１００内の他のノード１０２へトランザクションを転送することに集中できるようにする。
【００４０】
マルチキャスト・ネットワーク・アーキテクチャは、情報を受信することに関心のある各ノードに対してデータ重複なしに、宛先ノードのグループへ向けたデータの同時配布の可能性を許容する。ノードがマルチキャスト送信を受信することを希望する場合、ノードはマルチキャスト・グループに参加し（登録段階）、以後、マルチキャスト・グループへ送信された全てのデータを受信できることになる。ＩＰマルチキャストは、どの程度多くの受信者が存在するかについての事前知識を必要とすることなく、より多くの受信者集団へスケーリングすることが可能であり、一度だけパケットを送信することをソースに要求

することにより、ネットワーク・インフラストラクチャは効率的に使用される。マルチキャスト・ネットワークの性質のために、コネクション指向プロトコル（ＴＣＰ等）を利用することは、多数の他ノードとの同時通信に起因して非実用的である。従ってコネクションレス・プロトコルが使用される。

【００４１】

ビットコイン等の幾つかのブロックチェーン・ネットワークは、ノード・ツー・ノードのＴＣＰを使用する。ＴＣＰを利用して送信されるデータ・パケットは、順序付けの目的で使用される関連シーケンス番号を有する。これに加えて、ＴＣＰプロトコルは、コネクションの設定及びその終了の双方の場合に、三段階ハンドシェーク手順を含む。ＴＣＰを介して送信されるパケットは関連するオーバーヘッドとともに到来し、それらは関連するシーケンス番号を有し、三段階ハンドシェーク・プロトコルが存在する。コネクションを設定する際に、１２８－１３６バイトが送信されているが、コネクションの閉鎖は１６０バイトのコストを要する。従ってパケット伝送におけるハンドシェークは２９６バイトに達するほどコストがかかる。更に、ノードが新しいトランザクションを受信すると、トランザクションのハッシュを含むインベントリ（ＩＮＶ）メッセージを他ノードに通知する。ＩＮＶメッセージを受信したノードは、そのトランザクションのハッシュが以前に見られたか否かを検査し；見られていない場合、ノードは、ＧＥＴＤＡＴＡメッセージを送信することにより、トランザクションを要求するであろう。ノードＡからノードＢへトランザクションを送信するのに要する時間は、

Ｔ１＝ｖｅｒｉｆｉｃａｔｉｏｎ＋ＴＣＰ（ｉｎｖ＋ｇｅｔｄａｔａ＋ｔｘ）

であり、ここでＴＣＰ（）はＴＣＰハンドシェーク手順で導入されるオーバーヘッドを示す。

【００４２】

Ｍ－ノード１０４は他ノード１０２との通信のためにＴＣＰを利用するように設定されているかもしれず、それは既存のプロトコルでは必須である。しかしながら、ノードは、Ｍ－ノード１０４からＭ－ノード１０４への通信に関して、又はより適切にはマルチキャストの状況でＭ－ノード１０４から複数のＭ－ノードへの通信に関してでさえ、ユーザー・データグラム・プロトコル（ＵＤＰ）等のコネクションレス・プロトコルを利用することができる。ＴＣＰとは異なり、ＵＤＰはハンドシェーク・プロトコルを含まず、従ってＭ－ノード１０４はより迅速にトランザクションを伝搬することが可能である。このことはまた、実際のトランザクションをそれまで送信することなく、反復されたＩＮＶメッセージを送信することにより、悪意のノードが他ノードと結びついてしまうことを回避することもできる。

【００４３】

ＵＤＰのライトウェイトの性質は所定のトレード・オフに関連する。誤り検査は少なく、誤り回復もない。幾つかの実装では、ＵＤＰのこれらの制限は、誤り回復、順序付け、再送をアプリケーション・レイヤの機能として実装することにより、アプリケーション・レベルで克服され得る。誤り検査をアプリケーション・レベルに配置することは、ネットワークからオーバーヘッドを取り除く。

【００４４】

ある例示的な状況において、ブロックチェーン・ネットワーク１００における正規のノード１０２が、マーチャント・ベース決済のようにＭ－ネット１０６により処理してもらうことを希望するトランザクションを生成する。ノードはそのトランザクションをＭ－ノード１０４へ送信してもよく、Ｍ－ノード１０４はマルチキャストを利用してそれを他のＭ－ノード１０４へブロードキャストする、あるいはノードがＭ－ノード１０４のＩＰマルチキャスト・アドレスを知っている場合には複数のＭ－ノード１０４へ直接的にトランザクションを送信してもよい。幾つかの例では、Ｍ－ネット１０６の全てのＭ－ノード１０４は単一のマルチキャスト・アドレスのメンバーであり、従ってそのアドレスへ送信された全てのトランザクションは全てのＭ－ノード１０４により受信される；しかしながら、幾つかのケースでは、Ｍ－ネット１０６に関連する１つより多いマルチキャスト・アド

レスが存在してもよく、受信するＭ－ノード１０４は、トランザクションを完全なＭ－ネット１０６へ伝搬させるために、トランザクションの他のマルチキャスト・アドレスへの更なるブロードキャストが必要とされるか否かを、ルーティング情報から評価することができる。

【００４５】

マルチキャストは、全てのＭ－ノード１０４に対する新たなトランザクションの速やかな初期伝搬を保証することを支援する；しかしながら、マルチキャストのソリューションは、増加したトランザクション・スループットに由来するブロックチェーン・ネットワーク１００のスケーラビリティ問題には必ずしも対処していない。ネットワーク１００内の各ノード１０２は、典型的には、ノードが発見した未承認トランザクションを含むメンプールを維持し、未承認トランザクションは、プルーフ・オブ・ワークを完了したマイナーによりブロックチェーンへ未だ組み込まれていないものである。支払処理で使用することから生じるトランザクション数の著しい増加は、各々のメンプールで保存するトランザクション量の増加となるであろう。従って、Ｍ－ネット１０６のノードはほぼ同時に新たなトランザクションを受信することが可能であるが、大規模で迅速に変化するメンプールに関してストレージ能力の限界を有するかもしれない。

【００４６】

この問題に対処するため、本願は、マルチキャストを利用することに対する代替として、Ｍ－ノード１０４が、分散されたハッシュ・テーブル（ａ Ｄｉｓｔｒｉｂｕｔｅｄ Ｈａｓｈ Ｔａｂｌｅ：ＤＨＴ）により実現される共有されるメンプールを利用することを提案する。

【００４７】

５００バイトというトランザクション（ＴＸ）の平均サイズ、及び～10^4ＴＸ／ｓというトランザクション・レートを仮定すると、Ｍ－ネット１０６は～４００ＧＢという日々の到来データを受信し得る。このデータの全てが、未承認トランザクションのメンプールの中で、変動する期間にわたって保存されることを要する。従って、Ｍ－ネット１０６はデータを高速に記憶するためにかなりのストレージ及び能力を必要とする。各自それぞれのＭ－ノード１０４に過剰に多くの条件を課さないために、Ｍ－ノード１０４はＤＨＴを当てにする共有メンプールを実現する。各Ｍ－ノード１０４に、全ての到来するＴＸｓを各自自身のメンプールに維持させる代わりに、各Ｍ－ノード１０４は、全体の内の一部分と、残りの部分のハッシュ及び関連するキー値とを格納するだけである。

【００４８】

ＤＨＴは非セントラル化分散システムのクラスであり、そのシステムはノード間でキー・セットのメンバーシップ分割を許容し、且つ所与のキーの所有者だけに、効率的で最適化された方法でメッセージを送信することができる。ネットワークの各ノードは、ハッシュ・テーブルのアレイのセルとして理解され得る。ＤＨＴは、非常に多数のノードを管理するように、また、新たなノードがネットワークに参加し、古いノードが離脱及びクラッシュすることを、共有データの完全性を損なうことなく行うように設計されている。ＤＨＴは、非セントラル化（中央機関は存在せず、中央のコーディネータも存在しない）、スケーラビリティ（システムは何百万ものノードに対して効率的な行動をとる）、及び障害耐性（システムは信頼性があり、ネットワークに参加及び離脱する又はクラッシュするノードを管理することができる）を保証する。ネットワークの各ノードは、小数の他ノードだけと通じたままであってもよく、従って変動や新たなデータ部分が存在しても、ネットワークはオーバーロードにならない。

【００４９】

同じ概念がＵＴＸＯデータベースに適用されてもよく、そのデータベースはブロックチェーンにおける全ての未使用アウトプットの集合を含む。ＵＴＸＯデータベースは、一群のノードの中でコンテンツを共有するためにＤＨＴを利用して構築され得る。

【００５０】

Ｍ－ネット１０６のために共有メンプールを実現するために使用され得る多数の可能な

ＤＨＴアーキテクチャ及びプロトコルが存在する。一例はＰａｓｔｒｙ（商標）であるが、他にも多数存在する。Ｐａｓｔｒｙ（商標）は、オーバーレイ・ネットワークが分散システムで情報を格納及び転送することができることを維持するように設計されたプロトコルである。Ｐａｓｔｒｙ（商標）ネットワークにおける各ノードは１２８ビットの識別子を割り当てられ、識別子は循環ノードＩＤ空間（０から$2^{128}-1$までの範囲）内でのノードの位置を指定するために使用される。ＩＤはノードがネットワークに入るとランダムに指定される。各ノードは、ルーティング・テーブル、近隣セット及びリーフ・セットを維持する。

【００５１】

ロバストなＤＨＴの寸法決定において考察する一要因は、ネットワーク全体の堅牢性及び信頼性を保証するために必要なレプリカの数である。既に言及されているように、ノードはネットワークに参加して離脱することが可能であり、この事実はデータの利用可能性に影響すべきではない。トランザクションＡを格納しているノードがネットワークを離れる場合、ネットワークの他の部分でトランザクションＡを発見する必要がある。例えばビットコインのような既存のブロックチェーン・ネットワークでは、ネットワークは、ネットワークにおける全ノード数に等しい数のブロックチェーン・レプリカ（平均５０００レプリカ）を有するが、このことはスケーラビリティに影響を及ぼす。

【００５２】

目下提案しているＭ－ネット１０６では、メンプールは、全てのＭ－ノード１０４で完全には複製されておらず、そうではなくＤＨＴにより実現されている。信頼性をもたらすため、ＤＨＴは幾らかのオーバーラップを有するように実現されることが可能であり；即ち、各々のトランザクション・データ・アイテムは１つより多いＭ－ノード１０４（但し、全てのＭ－ノード１０４ではない）において複製される。一例として、ＤＨＴは２レプリカという最小数を指定するように実現されてもよい。これは、ノード間の完全な独立性を仮定した場合に、任意の所与の時間に２つのノードが一度に落ちてしまう確率が次のようになる結果をもたらす。

【数１】

$$\left(\frac{1}{(24*365)}\right)^2 = 1.30 * 10^{-8}$$

【００５３】

ここで図２を参照すると、図２は分散されたメンプール２０４に新たなトランザクションを格納するプロセス２００を示すシーケンス図を示す。分散されたメンプール２０４はＤＨＴを利用して実現される。プロセス２００はノード１０２がトランザクションをＭ－ノード１０４へ送信することを含む。Ｍ－ノード１０４は、キー値を得るために、実装に応じて、トランザクション又はトランザクションＩＤをハッシュする。キー値は、トランザクションが格納されるべきＭ－ノード１０４又は複数のＭ－ノード１０４（複製データの場合）を示す。Ｍ－ノード１０４はトランザクションを分散されたメンプール２０４に格納し、これは、Ｍ－ネット１０６におけるＭ－ノード１０４の割り当てられたＩＤ及びキー値に基づいて、トランザクションが格納されるべき適切なＭ－ノード１０４へトランザクションをルーティングすることを含み得る。Ｍ－ノード１０４は、関連するＤＨＴプロトコルに依存してアクノリッジメントを受信してもよい。

【００５４】

ここで図３も参照すると、図３はブロックチェーン・ネットワークでトランザクションを伝搬させる方法の一例３００をフローチャート形式で示す。方法３００はＭ－ノード１０４（図１）によって実現される。Ｍ－ノード１０４はオペレーション３０２において正規のノードから新しいトランザクションを受信する。Ｍ－ノード１０４はトランザクションの真正を確認するために、所定の検証オペレーションを実行することができる。

【００５５】

オペレーション３０４により示されるように、トランザクションは、トランザクションのキーを生成するためにハッシュされ得る。キーは、ＤＨＴの中でトランザクションが格納されるべき場所を示すことが可能であり、その場所は現在のＭ－ノード１０４以外のノードにおけるものであってもよい。次いでオペレーション３０６においてＭノード１０４はトランザクションがＤＨＴに既に存在するか否かを評価する。各Ｍ－ノード１０４は、Ｍ－ネット１０６（図１）を構築するＭ－ノード１０４の中でキー空間（ｔｈｅ　ｋｅｙ　ｓｐａｃｅ）の区分に基づいて、格納されたトランザクションの一部分を有する。幾つかの実装において、キー空間は、参加しているＭ－ノード１０４の中で分けられる。区分けは，ネットワークの回復力の複製（ｒｅｐｌｉｃａｔｉｏｎ　ｆｏｒ　ｒｅｓｉｌｉｅｎｃｙ　ｏｆ　ｔｈｅ　ｎｅｔｗｏｒｋ）を引き起こすようにオーバーラップを含んでもよい。Ｐａｓｔｒｙ（商標）を使用すること等のような幾つかの実装において、各Ｍ－ノード１０４は固有のキー又はＩＤ番号を割り当てられ、トランザクションは、トランザクションのキー値に対する近接性に基づいて、Ｍ－ノード１０４又は複数のＭ－ノード１０４（複製が望まれる場合）に格納され得る。Ｍ－ノード１０４は、トランザクションのローカルに格納された部分と、残りの部分のハッシュ又はキー値とを有し得る。従って、オペレーション３０６において、ノード１０４は、ローカル・データに基づいて新たなデータがＤＨＴにあるか否かを評価することが可能であり得る。

【００５６】

トランザクションがＤＨＴ内にある場合、オペレーション３０８において、Ｍ－ノード１０４はそのキー値に基づいてトランザクションをＤＨＴに格納する。一般的な意味において、これは、ｐｕｔ（ｋ，ｔｘ）オペレーションの形式をとることができ、ここでｋはキー値であり、ｔｘはトランザクションである。適用可能なＤＨＴルーティング・プロトコルは、トランザクションが適切なＭ－ノード１０４へ送信されてそこに格納されることを保証する。ＤＨＴは選択された実装に応じて分散ハッシュ・テーブルの様々なプロトコルに従って動作し得る。Ｍ－ネット１０６にトランザクションを格納するためにＤＨＴを利用することは、Ｍ－ネット１０６内でＩＮＶ／ＧＥＴＤＡＴＡメッセージを利用してトランザクションを全てのＭ－ノード１０４へルーティングすることを回避する。

【００５７】

オペレーション３１０において、Ｍ－ノード１０４は、この例では、ブロックチェーン・ネットワーク１００の通常のトランザクション転送プロトコルに従って、ブロックチェーン・ネットワーク１００の正規のノード１０２へトランザクションを送信する。例えば、通常のノードの通信は、ノード・ツー・ノード・コネクションのためにＴＣＰを利用することができる。

【００５８】

ここで図４を参照すると、図４はＭ－ノード４００の簡略化された一例をブロック図形式で示している。この例におけるＭ－ノード４００は、プロセッサ４０２と、ネットワーク・インターフェース４０４と、メモリ４０６とを含む。Ｍ－ノード４００は、本願で説明される機能を実行するためにネットワーク接続リソース、十分な処理リソース、及びメモリ・リソースを有する適切な任意のコンピューティング・ハードウェアを利用して実現され得る。Ｍ－ノード４００は本願で説明される機能を実現するプロセッサ実行可能命令を含み得る。幾つかのケースにおいて、プロセッサ実行可能命令は、ブロックチェーン・マーチャント・ノード・アプリケーション４２０として言及されてもよいが、命令は、ハードウェア及びオペレーティング・システムに依存して、１つ以上のモジュール、アプリケーション、スクリプト、又は他のプログラミング構造で実現され得ることが認められるであろう。プロセッサ４０２はマルチ・コア・プロセッサ、及び／又は複数のプロセッサを含み得る。

【００５９】

メモリ４０６は、ＤＨＴキー値（即ち、Ｍ－ノードＩＤ）に部分的に基づいて、ＤＨＴベース・メンプール４１０のうちの指定された部分を含むデータを格納する。この実装例では、メモリ４０６は、ルーティング・テーブル４１２と、近隣セット４１４と、リーフ

・セット４１６とを更に格納する。ルーティング・テーブル４１２はＭ－ネット内の特定のルーティング宛先のリストを含み、ノードがデータのパケットを受信すると、ノードはルーティング・テーブルを参照し、そのデータを送信する先を知る。ルーティング・テーブル４１２はまた、各宛先がＭ－ノード４００からどれだけ離れているかについての情報を含んでもよい。近隣セット４１４は、例えば近接性メトリック（ピン・レイテンシ）に基づく近接Ｍ－ノードに関する情報を含む。リーフ・セット４１６は数値的に近いＭ－ノードを含む。Ｍ－ノードは、それらのキー値（ノードＩＤ）が数値的に近い場合に、数値的に近い。メモリ４０６は、以下において更に説明されるように、Ｍ－ノード評判テーブル４１８を更に含む。

【００６０】

スケーラビリティを提供するために、ＤＨＴを利用してメンプールを実現することに加えて、Ｍ－ネットはノードがＭ－ネットに参加することを許容する。図５は、メンプールがＤＨＴ５０６として実装されているＭ－ネットに新たなノード５０４が参加する例を示すシーケンス図５００を示す。新たなノード５０４は既にＭ－ネットの一部である少なくとも１つのＭ－ノードのアドレスを有する必要があり、それにより、新たなノードは何れかのＭ－ノードへ参加リクエスト（ｊｏｉｎ　ｒｅｑｕｅｓｔ）を仕向けることができる。信号ダイアグラム５００は新たなノード５０４が「ｊｏｉｎＤＨＴ（ｍ－ｎｏｄｅ．ａｄｄｒｅｓｓ）リクエスト」をＭ－ノード５０２へ送信する例を示す。Ｍ－ノード５０２は、所定の検証アクションを実行し、検証アクションは新たなノード５０４を問い合わせることを含む。例えば、Ｍ－ネットは、Ｍ－ノード５０２を指定しているＭ－ネットに参加することに関連する一組の最低基準を有していてもよい。例示として、基準は、利用可能な最小処理リソース、利用可能な最小空きメモリ、接続条件を含んでもよい。

【００６１】

新たなノード５０４を検査するために検証オペレーションが実行されるものが何であれ、Ｍ－ノード５０２は完了したと仮定すると、Ｍ－ノードは、ＤＨＴプロトコルがＤＨＴ５０６の動作を管理するものが何であれそれに従ってＤＨＴ５０６へｊｏｉｎｒｅｑｕｅｓｔ（）を転送する。そしてＤＨＴ５０６は新たなノード５０４と通信し、ルーティング・テーブル、キー値（ノードＩＤ）、及び何らかの他のデータを提供し、新たなノード５０４がＭ－ネットにおける新たなＭ－ノードとして機能できるようにする。

【００６２】

ノードがＭ－ネットに参加し得る容易性は悪意のノードがネットワークに参加し得る点で脆弱性をもたらすことが認められるであろう。潜在的な悪意のノードを識別及び分離するために、本願はＭ－ノードがＭ－ノード評判テーブル４１８を格納することをもたらす。図６はノードの行動ランキングを追跡及び更新するために使用されるＭ－ノード評判テーブル４１８の一例を図式的に示す。

【００６３】

新たなノードがネットワークに参入すると、そのノードは、ノードＩＤフィールド６０２により示されるように、Ｍ－ノード評判テーブル４１８に追加され得る。テーブル４１８は幾つかの実装において参加時間６０４を更に含んでもよい。テーブル４１８はそのＭ－ノードに関するスコア６０６又は格付けを更に含む。

【００６４】

スコア６０６は所定の行動メトリックに基づいて上下に調整され得る。例えば、Ｍ－ノードがトランザクションを転送することに失敗した場合、ある期間にわたって沈黙したままである場合、取引でないと判断されるトラフィックでＭ－ネットをあふれさせる場合、あるいはその他の否定的な挙動に関わる場合、そのランキングは落とされる又は減らされることが可能である。ノードのスコアが所定の最小値より下に落ちた場合、ノードはＭ－ネットから排除されるかもしれない。

【００６５】

特定のＭ－ノードで保持されるＭ－ノード評判テーブル４１８は、全てのＭ－ネットではなく、近隣のスコアを追跡することに制限されてもよい。従って、新たなＭ－ノードが

時間ｔにネットワークに参加する場合、近隣のＭ－ネット評判テーブルは新たなノードに関する如何なる情報も含まないが、それらは、その時点ｔから、ノード・レジスタ・テーブルに情報を格納する新たなノードの評判を構築し始める。例えば、新たなノードがサイレント・ノードである場合、それは、そのノードはネットワークを介して受信した情報を転送しないことを意味し、全ての近隣は、各自それぞれのＭ－ノード評判テーブルでその挙動を記録し始め、例えば、新たなノードのＩＤに否定的な値を指定する。所定の時間の後（ｔ＋ｎ）、新たなノードに気付いている全てのノードのＭ－ノード評判テーブルが負の値を含む場合、それらのノードは、新たなノードを分離し、それをネットワークから禁止するように決定してもよい。

【００６６】

ここで図７を参照すると、図７は例示的なメンプール・データ・エントリ７００を示す。Ｍ－ネットの分散されたメンプール内のトランザクションは、承認される前に、即ちブロックチェーンに追加されて承認されるブロックに組み込まれる前に、かなりの期間にわたって待機するかもしれない。十分な数の後続ブロックがその上にブロックチェーンに追加されると、ブロックは「承認された」と考えられ、その結果、ブロックチェーンにおける成長を逆転させ、異なるブランチ又はフォークに変えるためにブロックを取り除くことは計算上不可能になる。

【００６７】

メンプールの大きさ及び柔軟性、並びにトランザクションの量に起因して、所与のトランザクションが、ビットコイン等の幾つかのブロックチェーンの実装におけるものより長期間にわたって承認されないかもしれないことがあり得る。従来のビットコイン実装では、トランザクションは、それがブロックに組み込まれると速やかにメンプールから除去される。これは、ブロックがオーファン（孤児）ブロックとなった場合、ブロック中の全てのトランザクションがネットワークで再送されることを意味する。これは非現実的であり得るし、高速トランザクション・ネットワークの場合に所定のトランザクションを承認するために長い遅延を招く結果となり得る。

【００６８】

従って、幾つかの実装において、メンプールは，トランザクションが組み込まれたブロックの承認数、即ちトランザクションが組み込まれたブロックに続いてブロックチェーンに追加されたブロックの数を追跡することができる。所定数の承認が生じた後に限り、トランザクションはメンプールから削除される。所定数は４、５、６、７であってもよいし、あるいは所与の実装に関する適切な任意の数であってよい。図７に示されるように、メンプール・データ・エントリ７００は、トランザクションＩＤフィールド７０２、トランザクション・フィールド７０４、及び承認数（ＮｏＣ）フィールド７０６を含むように構成されてもよい。別の実装では、ＮｏＣを追跡するのではなく、メンプール・データ・エントリ７００は単にブロック番号を記録してもよい。ブロック番号から、ブロックチェーンの現在のブロック番号に基づいて、幾つの承認が生じたかを評価することが可能である。

【００６９】

必要な承認数が生じると、トランザクションはメンプールから安全に削除され得る。このように、オーファン・ブロックの場合にトランザクションのロスはなく、トランザクションは、必要承認数の後に永続的に削除される。

【００７０】

本発明の１つ以上の実施形態は、改善されたブロックチェーン実装方法及びシステムとして説明されてもよい。それはブロックチェーン・ネットワークによる書き込み動作、交換、移転などの処理の改善された速度を提供することができる。本発明の他の利点も提供され得る。

【００７１】

本願で説明されるデバイス及びプロセス、並びにビデオ特徴抽出器を構成する説明された方法／プロセスを実現する任意のモジュール、ルーチン、プロセス、スレッド、アプリケーション、又はその他のソフトウェア・コンポーネントは、標準的なコンピュータ・プ

ログラミング技術及び言語を利用して実現され得ることが、理解されるであろう。本願は特定のプロセッサ、コンピュータ言語、コンピュータ・プログラミング規則、データ構造、又は他のそのような実装の詳細に限定されない。

【００７２】

上記の実施形態は本発明を限定ではなく例示していること、及び当業者は添付の特許請求の範囲に規定されるような発明の範囲から逸脱することなく、多くの代替的な実施形態を設計し得ることに留意すべきである。特許請求の範囲において、括弧内の任意の参照符号は特許請求の範囲を限定するように解釈されてはならない。「有している」及び「有する」等の言葉は、任意の請求項又は明細書全体として列挙されているもの以外の要素又はステップの存在を排除していない。本明細書において、「～を有する」は「～を含む又は～から成る」を意味し、「～を有している」は「～を含んでいる又は～から構成されている」を意味している。要素の単独の参照は、そのような要素の複数の参照を排除しておらず、逆もまた同様である。発明は、幾つかの別個の要素を含むハードウェアによって、及び適切にプログラムされたコンピュータによって実現され得る。幾つかの手段を列挙する装置の請求項において、これらのうち幾つかの手段はハードウェアの１つの同じアイテムにより具現化されてもよい。所定の複数の事項が相互に異なる従属請求項で引用されているという単なるその事実は、これらの事項の組み合わせが有利に使用され得ないことを示すものではない。

【００７３】

（付記１）

ブロックチェーンを実現するために使用される相互接続されたノードのネットワーク上でブロックチェーン・トランザクションの分散を促すように構成される特殊ネットワーク・ノードであって、前記ノードの部分集合はオーバーレイ・ネットワークにより相互接続される特殊ネットワーク・ノードであり、前記特殊ネットワーク・ノードは：

プロセッサ；

分散ハッシュ・テーブルとして構造化された分散されたメンプールのうちの指定された部分を格納するメモリであって、前記分散されたメンプールは承認を待機しているペンディング・トランザクションを含む、メモリ；

ネットワーク・インターフェース；及び

プロセッサ実行可能な命令を含むブロックチェーン特殊ネットワーク・ノード・アプリケーション；

を含み、前記命令は、前記プロセッサにより実行されると、前記プロセッサに：

トランザクション識別子を含むトランザクションを受信すること；

キーを得るために前記トランザクション識別子をハッシュすること；

前記分散されたメンプールに前記トランザクションが格納されているか否かを前記キーを利用して確認し、格納されていない場合、前記トランザクションをペンディング・トランザクションとして前記分散されたメンプールに格納すること；及び

前記トランザクションを特殊ネットワーク・ノード以外のノード群へピア・ツー・ピア・コネクションを利用して送信すること；

を行わせる特殊ネットワーク・ノード。

（付記２）

前記メモリは、前記トランザクションを含み且つ前記ブロックチェーンに含まれるブロックの承認数に関するデータを更に格納し、前記命令は、前記承認数が最低数に到達した場合に、前記分散されたメンプールから前記トランザクションを削除することを前記プロセッサに行わせる、請求項１に記載の特殊ネットワーク・ノード。

（付記３）

前記承認数に関する前記データは、前記ブロックチェーンに追加される新たなブロック各々に関して更新される承認数のカウント、又は前記トランザクションが含まれる前記ブロックのブロック番号の何れかである、請求項２に記載の特殊ネットワーク・ノード。

（付記４）

前記メモリは、何らかの検出された新たな近隣の特殊マーチャント・ノードに関する識別子と、前記新たな近隣の特殊ネットワーク・ノードの検出されたアクティビティに基づく新たな近隣の特殊ネットワーク・ノードの関連するスコアとを含む特殊ネットワーク・ノード評判テーブルを更に格納する、請求項１－３のうち何れか一項に記載の特殊ネットワーク・ノード。

（付記５）

前記命令は、前記新たな近隣の特殊ネットワーク・ノードの前記スコアを更新すること、及び前記新たな近隣の特殊ネットワーク・ノードの前記スコアが閾値より下に落ちたことを判定し、その結果、前記新たな近隣の特殊ネットワーク・ノードを悪意のノードとして指定し、前記新たな近隣の特殊ネットワーク・ノードを孤立させることを前記プロセッサに行わせるように構成されている、請求項４に記載の特殊ネットワーク・ノード。

（付記６）

前記分散されたメンプールのうちの前記指定された部分は、前記特殊ネットワーク・ノードのうちの別のものに格納された前記分散されたメンプールの第２部分と部分的にオーバーラップしている、請求項１－５のうち何れか一項に記載の特殊ネットワーク・ノード。

（付記７）

前記特殊ネットワーク・ノードの各々は、前記分散されたメンプールの各自指定された部分を格納し、前記各自指定された部分は、前記ペンディング・トランザクションの各々が少なくとも２つの前記特殊ネットワーク・ノードに格納されるが、前記特殊ネットワーク・ノードの全てには格納されないように、部分的にオーバーラップし、選択的に、前記ペンディング・トランザクションの各々は、前記分散されたメンプールの各自指定された２つに過ぎない部分に含まれる、請求項１－５のうち何れか一項に記載の特殊ネットワーク・ノード。

（付記８）

ブロックチェーンを実現するために使用されるネットワークに結合される複数のノードに関わるブロックチェーン転送を促進するコンピュータで実現される方法であって、前記複数のノードの部分集合は特殊ネットワーク・ノードであり、前記特殊ネットワーク・ノードは、承認を待機するペンディング・トランザクションを含む分散されたメンプールを格納し、前記分散されたメンプールは前記特殊ネットワーク・ノードの中で分散ハッシュ・テーブルとして実現され、前記方法は：

トランザクション識別子を含むトランザクションを受信するステップ；

キーを得るために前記トランザクション識別子をハッシュするステップ；

前記分散されたメンプールに前記トランザクションが格納されているか否かを前記キーを利用して確認し、格納されていない場合、前記トランザクションをペンディング・トランザクションとして前記分散されたメンプールに格納するステップ；及び

前記トランザクションを特殊ネットワーク・ノード以外のノード群へピア・ツー・ピア・コネクションを利用して送信するステップ；

を含む方法。

（付記９）

前記トランザクションを含み且つ前記ブロックチェーンに含まれるブロックの承認数を判定し、前記承認数が最低数に到達した場合に、前記分散されたメンプールから前記トランザクションを削除するステップを更に含む請求項８に記載の方法。

（付記１０）

前記トランザクションを前記メンプールに格納するステップが、トランザクションが含まれるブロックの承認数に関連して前記トランザクションを格納するステップを含み、前記トランザクションに関して前記メンプールに格納される承認数は、新たなブロックが前記ブロックチェーンに追加されると更新される、請求項９に記載の方法。

（付記１１）

前記トランザクションを前記メンプールに格納するステップが、トランザクションが含まれるブロックの承認数に関連して前記トランザクションを格納するステップを含み、前

記承認数を決定することは、前記ブロックチェーンに関する現在のブロック番号を確認し、前記現在のブロック番号と、前記トランザクションが含まれている前記ブロックのブロック番号とを比較することを含む、請求項９に記載の方法。

（付記１２）

新たな近隣の特殊ネットワーク・ノードを検出するステップ；

前記新たな近隣の特殊ネットワーク・ノードの識別子を、特殊ネットワーク・ノード評判テーブルに格納するステップ；及び

前記新たな近隣の特殊ネットワーク・ノードの検出されたアクティビティに基づいて、前記特殊ネットワーク・ノード評判テーブルにおける前記新たな近隣の特殊マーチャント・ノードのスコアを更新するステップ；

を更に含む請求項８－１１のうち何れか一項に記載の方法。

（付記１３）

前記新たな近隣の特殊ネットワーク・ノードの前記スコアが閾値より下に落ちたことを判定し、その結果、前記新たな近隣の特殊ネットワーク・ノードを悪意のノードとして指定し、前記新たな近隣の特殊ネットワーク・ノードを孤立させるステップを更に含む請求項１２に記載の方法。

（付記１４）

前記特殊ネットワーク・ノードのうちの１つが前記分散されたメンプールの一部分を格納し、前記特殊ネットワーク・ノードのうちの前記１つに格納された前記分散されたメンプールのうちの一部分は、前記特殊ネットワーク・ノードのうちの別のものに格納された前記分散されたメンプールの第２部分と部分的にオーバーラップしている、請求項８－１３のうち何れか一項に記載の方法。

（付記１５）

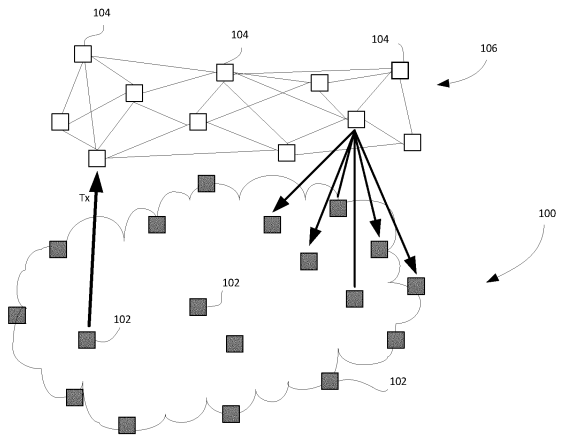
前記特殊ネットワーク・ノードの各々は、前記分散されたメンプールの各自の部分を格納し、前記各自の部分は、前記ペンディング・トランザクションの各々が少なくとも２つの前記特殊ネットワーク・ノードに格納されるが、前記特殊ネットワーク・ノードの全てには格納されないように、部分的にオーバーラップし、選択的に、前記ペンディング・トランザクションの各々は、前記分散されたメンプールの２つに過ぎない各自の部分に含まれる、請求項８－１３のうち何れか一項に記載の方法。

（付記１６）

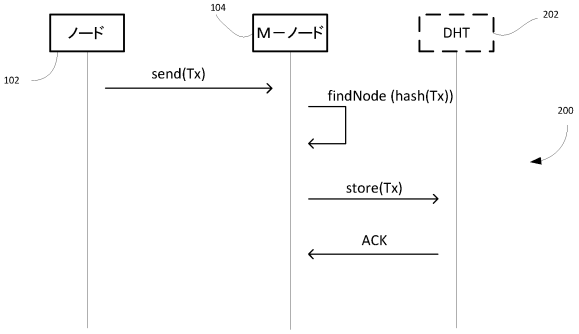
複数の参加ノードの中でブロックチェーン・トランザクションに参加するためのプロセッサ実行可能な命令を格納する非一時的なプロセッサ読み取り可能な媒体であって、前記プロセッサ実行可能な命令は、前記参加ノードのうちの１つにおけるプロセッサにより実行されると、請求項８－１５のうち何れか一項に記載の方法を前記プロセッサに実行させる、非一時的なプロセッサ読み取り可能な媒体。

【図面】

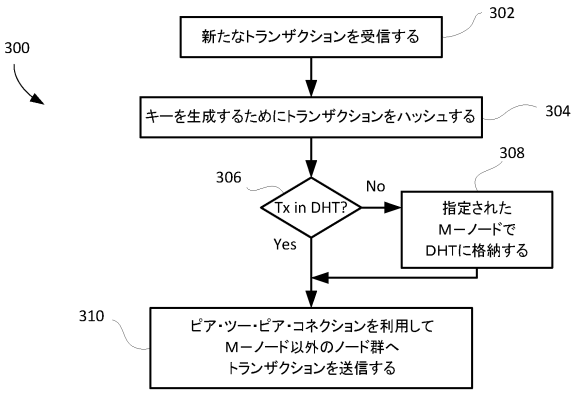
【図１】



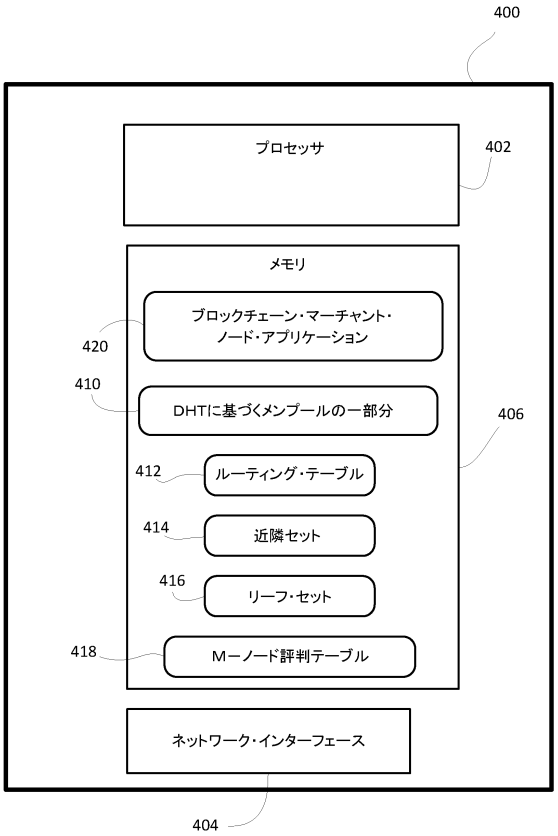
【図２】



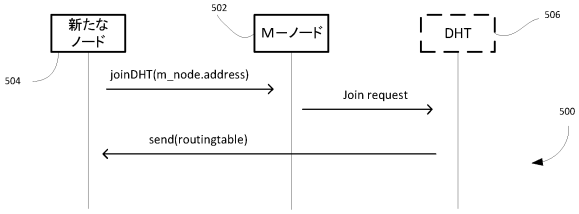
【図３】


300
新たなトランザクションを受信する
302
キーを生成するためにトランザクションをハッシュする
304
306
Tx in DHT?
No
Yes
308
指定された
Mーノードで
DHTに格納する
310
ピア・ツー・ピア・コネクションを利用して
Mーノード以外のノード群へ
トランザクションを送信する

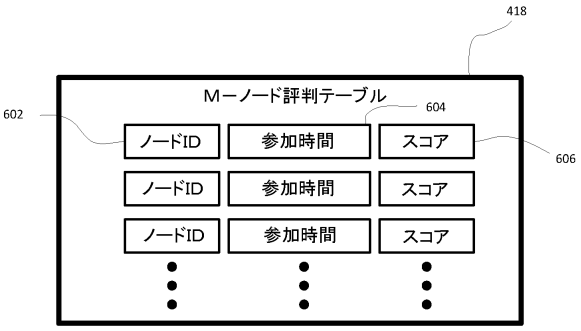
【図４】


400
プロセッサ
402
メモリ
ブロックチェーン・マーチャント・
ノード・アプリケーション
420
410
DHTに基づくメンプールの一部分
406
412
ルーティング・テーブル
414
近隣セット
416
リーフ・セット
418
Mーノード評判テーブル
ネットワーク・インターフェース
404

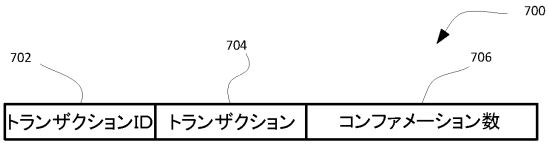
【図５】


新たな
ノード
504
502
Mーノード
506
DHT
joinDHT(m_node.address)
Join request
send(routingtable)
500

【図６】


418
Mーノード評判テーブル
602
604
ノードID
参加時間
スコア
606
ノードID
参加時間
スコア
ノードID
参加時間
スコア

【図７】



フロントページの続き

内
(72)発明者　モティリンスキ，パトリック
イギリス国 シーエフ１０ ２エイチエイチ カーディフ チャーチル ウェイ チャーチル ハウス ７ス フロア アーカート－ダイクス アンド ロード エルエルピー 内
(72)発明者　ヴィンセント，ステファヌ
イギリス国 シーエフ１０ ２エイチエイチ カーディフ チャーチル ウェイ チャーチル ハウス ７ス フロア アーカート－ダイクス アンド ロード エルエルピー 内
審査官　三坂 敏夫
(56)参考文献　国際公開第２０１６／１６４３１０（WO，Ａ１）
国際公開第２０１７／０６６７１５（WO，Ａ１）
特開２０１７－０９１１４９（ＪＰ，Ａ）
国際公開第２０１７／０１０４５５（WO，Ａ１）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　９／４５５－９／５４
Ｈ０４Ｌ　４５／１６