(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7571997号
(P7571997)

(45)発行日　令和6年10月23日(2024.10.23)

(24)登録日　令和6年10月15日(2024.10.15)

(51)国際特許分類

		FI		
Ｇ０６Ｆ　16/182 (2019.01)		Ｇ０６Ｆ	16/182	
Ｈ０４Ｌ　9/32 (2006.01)		Ｈ０４Ｌ	9/32	２００Ｚ

請求項の数　6　（全29頁）

(21)出願番号　特願2020-199236(P2020-199236)
(22)出願日　令和2年11月30日(2020.11.30)
(65)公開番号　特開2022-86931(P2022-86931A)
(43)公開日　令和4年6月9日(2022.6.9)
審査請求日　令和5年11月27日(2023.11.27)

(73)特許権者　518156727
有限会社プラン・アンド・ドウ
東京都港区新橋二丁目２０番１５－３１
７号
(74)代理人　100177127
弁理士　▲高▼橋 一哉
(72)発明者　高橋 一哉
東京都港区新橋二丁目２０番１５－３１
７号 有限会社プラン・アンド・ドウ内
審査官　原 秀人

最終頁に続く

(54)【発明の名称】　分散台帳ネットワークシステムのコンセンサス形成方法およびコンセンサス形成用プログラム

(57)【特許請求の範囲】

【請求項１】

１６台以上のコンピュータがそれぞれノードコンピュータとしてピア・トゥー・ピアで情報を共有するネットワークシステムを構成し、

ある口座の資産の一部を別の口座に振り込んだりするといった一連のトランザクション処理を、前記ノードコンピュータの内の第一のノードコンピュータに託すことによって、該第一のノードコンピュータはリーダーノードと称されることとなり、

１６台以上の前記ノードコンピュータの中から前記リーダーノードが選定した、又は前記第一のノードコンピュータ以外に予め選定されていた１５台のノードコンピュータはバックアップノードと称されることとなり、

前記リーダーノードは託された前記一連のトランザクションの内容を１５個の前記バックアップノードに配信して、

前記リーダーノードと前記バックアップノードで成る１６個のノードそれぞれは独立に前記一連のトランザクション処理をして処理値を得る構成にして、

前記１６個のノードは、４個ずつ、第１基本単位及び第２基本単位、第３基本単位、第４基本単位として４つの基本単位にグループ分けされていて、

該４つの基本単位それぞれにおいて、該基本単位に属する４個のノードが前記処理値を互いに照合して３個以上のノードによる前記処理値が一致する場合には、該基本単位ではプレコンセンサスが成立したとして該一致する処理値を該基本単位が出力するプレコンセンサス値と定めるプレコンセンサス形成工程を経た後に、

前記プレコンセンサスが成立した前記基本単位が１又は２以上存在する場合は、前記プレコンセンサス値の一致する前記基本単位同士でプレコンセンサスグループを形成して各プレコンセンサスグループに属する前記基本単位の数を前記プレコンセンサスグループのメンバー数と定義し、
前記メンバー数において唯一最大数のプレコンセンサスグループが存在するときはコンセンサスが成立したこととし、該唯一最大数のプレコンセンサスグループで一致するプレコンセンサス値に基づいて前記一連のトランザクション処理の結果を確定し、確定した前記一連のトランザクション処理の結果を改ざん困難にするためのブロック化をする、ブロックチェーンとも称される分散台帳ネットワークシステム。
ム。
【請求項２】
ピア・トゥー・ピアで情報を共有するネットワークシステムを構成し、請求項１に記載の分散台帳ネットワークシステムにおける前記リーダーノードとしての動作をするコンピュータ。
【請求項３】
ピア・トゥー・ピアで情報を共有するネットワークシステムを構成し、請求項１に記載の分散台帳ネットワークシステムにおける前記バックアップノードとしての動作をするコンピュータ。
【請求項４】
前記１６個のノードから送信される定型書式データを受信して動作するコンセンサス成否判定器を備え、
前記第１基本単位及び第２基本単位、第３基本単位、第４基本単位として４つの基本単位にグループ分けされた１６個の前記ノードは、該４つの基本単位それぞれについて、該基本単位に属する４個のノードが前記処理値を互いに照合した結果に基づいて前記定型書式データを作成して前記コンセンサス成否判定器に送信する構成にして、
前記定型書式データには、前記ノードそれぞれが自己と一致する前記処理値を出力した他のノードに対するポイントを投票する欄である信用度ポイント投票領域と、前記自己が得た前記処理値を格納する処理値格納領域と、前記基本単位それぞれを構成するノードメンバが記録されている単位化テーブルとが含まれており、
前記コンセンサス成否判定器は受信した前記定型書式データに基づいてコンセンサス成否を判定するものであり、
前記信用度ポイント投票領域に投票された前記ポイントを集計して予め定められた所定のポイント数に達したものを信頼できるノードとみなしたうえで、前記単位化テーブルの記録に基づいて該信頼できるノードが属する前記基本単位を確定し、
該信頼できるノードが属する前記基本単位についてはプレコンセンサスが成立したものとし、
該信頼できるノードが得たものとして前記処理値格納領域に格納されている処理値を当該基本単位のプレコンセンサス値と定めたうえで、
前記定型書式データを通じて定められた前記プレコンセンサス値毎の出現頻度において唯一の最大頻度値を有するプレコンセンサス値があるときは該唯一の最大頻度値を有するプレコンセンサス値に従って前記一連のトランザクション処理値を確定し、確定した前記一連のトランザクション処理値を改ざん困難にするためのブロック化をする、
請求項１に記載の分散台帳ネットワークシステム。
【請求項５】
１６台以上のコンピュータがそれぞれノードコンピュータとしてピア・トゥー・ピアで情報を共有するネットワークシステムにおいて、
ある口座の資産の一部を別の口座に振り込んだりするといった一連のトランザクション処理を確定するために、前記一連のトランザクション処理をして自己処理値を得るトランザクション処理ステップと、
前記ノードコンピュータであって、自己ノードコンピュータと同一グループに属してい

る他の３台がそれぞれ独立に行った、同一の前記一連のトランザクション処理をして得られた３つの他人処理値を受信して、該他人処理値と前記自己処理値で成る４つの処理値の内で３つ以上一致する処理値があるときは該３つ以上一致する処理値を前記同一グループにおけるグループプレコンセンサス値と定めて該同一グループにおいてプレコンセンサス成立と判定すると共に、該同一グループにおけるグループプレコンセンサス値を前記ネットワークシステムにおいて共有するプレコンセンサス形成ステップと、
前記ノードコンピュータであって、前記同一グループに属しないものにより前記ネットワークシステムを使って共有されている、他グループでの他人グループプレコンセンサス値と前記同一グループにおけるグループプレコンセンサス値とを比較して一致する前記同一グループにおけるグループプレコンセンサス値又は前記他グループでの他人グループプレコンセンサス値に基づいてプレコンセンサスグループを形成し、
形成された前記プレコンセンサスグループに含まれる前記同一グループ及び前記他グループの数を前記プレコンセンサスグループのメンバー数と定義し、
前記メンバー数において唯一最大数の前記プレコンセンサスグループが存在するときはコンセンサスが成立したと判定して、該唯一最大数の前記プレコンセンサスグループに含まれる前記同一グループにおけるグループプレコンセンサス値又は前記他グループでの他人グループプレコンセンサス値を、確定すべき前記一連のトランザクション処理の処理結果とするコンセンサス判定ステップと、を有する処理を、
前記自己ノードコンピュータにさせるプログラム。
【請求項６】
１６台以上のコンピュータがそれぞれノードコンピュータとしてピア・トゥー・ピアで情報を共有するネットワークシステムにおいて、
ある口座の資産の一部を別の口座に振り込んだりするといった一連のトランザクション処理を確定するために、前記一連のトランザクション処理をして自己処理値を得るトランザクション処理ステップと、
前記ノードコンピュータであって、自己ノードコンピュータと同一グループに属している他の３台がそれぞれ独立に行った、同一の前記一連のトランザクション処理をして得られた３つの他人処理値を受信して、該他人処理値と前記自己処理値で成る４つの処理値の内で３つ以上一致する処理値があるときは該３つ以上一致する処理値を前記同一グループにおけるグループプレコンセンサス値と定めて該同一グループにおいてプレコンセンサス成立と判定すると共に、該同一グループにおけるグループプレコンセンサス値を前記ネットワークシステムにおいて共有するプレコンセンサス形成ステップと、
前記ノードコンピュータであって、前記同一グループに属しないものにより前記ネットワークシステムを使って共有されている、他グループでの他人グループプレコンセンサス値と前記同一グループにおけるグループプレコンセンサス値とを比較して一致する前記同一グループにおけるグループプレコンセンサス値又は前記他グループでの他人グループプレコンセンサス値に基づいてプレコンセンサスグループを形成し、
形成された前記プレコンセンサスグループに含まれる前記同一グループ及び前記他グループの数を前記プレコンセンサスグループのメンバー数と定義し、
前記メンバー数において唯一最大数の前記プレコンセンサスグループが存在するときはコンセンサスが成立したと判定して、該唯一最大数の前記プレコンセンサスグループに含まれる前記同一グループにおけるグループプレコンセンサス値又は前記他グループでの他人グループプレコンセンサス値を、確定すべき前記一連のトランザクション処理の処理結果とするコンセンサス判定ステップと、を有する、
ブロックチェーンとも称される分散台帳ネットワークシステムにおけるコンセンサス形成方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ブロックチェーンとも称される分散台帳ネットワークシステムを構成する２

台以上のノードコンピュータ間のコンセンサス形成方法およびコンセンサス形成装置、コンセンサス形成用プログラムに関するものである。

【背景技術】

【０００２】

非特許文献１によれば、ブロックチェーンとも称される分散台帳ネットワークシステムは、互いにＰ２Ｐ（ピア・トゥー・ピア）で直接通信できる２台以上のコンピュータで構成されている。これらのコンピュータはノードと呼ばれ、該ネットワークシステムに託された取引処理（以後、トランザクションともいう。）を履行する。これら複数のノードが協調的に動作することによって分散台帳ネットワークシステムは全体として１つの仮想コンピュータのように振る舞って利用者に託された取引を処理してその結果を保存する。

【０００３】

分散台帳ネットワークシステムにおいて、ノード同士は互いに補い合うというよりも、多くの場合、並行して同一の処理をして同一の結果を保存する。そして各ノードは１つの場所に存在するとは限らず世界中に分散していてもよい。このような冗長な構成により、分散台帳ネットワークシステムは故障に強く稼働率が高いといわれる。

【０００４】

また、ノードであるコンピュータの操作権限を含めた管理状態により、分散台帳ネットワークシステムはパブリックチェーンと、プライベートチェーンとコンソーシアムチェーンとに分類される。パブリックチェーンは一般の者に公開された分散台帳ネットワークシステムであって誰でも自由にノードとして参加することができるし撤退することもできる。そして権限ある特定の管理者は存在しないにもかかわらず健全に動作し続けるように設計されている。これは該ネットワークシステムの主催者を信用することで成り立っている従来のシステムとは異なり、信頼できる主催者不要のトラストレスシステムと言われる。パブリックチェーンは特定の者に恣意的に操作されることが無いという点で最も公平な分散台帳ネットワークシステムである。

【０００５】

一方、プライベートチェーンは主催者がノードに対して操作権限を有している。システムのバージョンアップをすることが比較的容易で処理効率を高めるための施策を講じやすい。このような利点を有しながらもその一方で、複数のノードに並行して同一処理をさせ、同一結果を保存させることによって故障耐性を高めて稼働率を上げることができる。コンソーシアムチェーンは２以上の主催者が共同でプライベートチェーンを営むものである。

【０００６】

分散台帳ネットワークシステムの利用者は該ネットワークシステムに自己の口座を有している必要がある。利用者が該ネットワークに託すトランザクションには、自己の口座の資産（以後、トークンということもある。）の一部を他者の口座に振り込むという単純なものもあるし、ある条件が充足した場合に自己の口座のトークンの一部を他者の口座に移すというものもある。

【０００７】

分散台帳ネットワークシステムを構成する各ノードは、例えば、トランザクション処理前の各口座の資産を把握し、所定の条件を充足したか否かの判断をし、処理した後の各口座の資産額を算出する。１つの取引について複数のノードが同一の演算処理を行う。

【０００８】

一般的な分散台帳ネットワークシステムでは、いずれかのノードが利用者からのトランザクションを託される。トランザクションを託されたノードはリーダーノードとしてそのトランザクションをその他のノードに配信する。ここではその他のノードをバックアップノードと呼ぶこととする。リーダーノードとバックアップノードとはそれぞれ同一のトランザクションの履行結果を算出する。算出された履行結果は各ノード内で比較検証されて誤りのないことが確認される。誤りのないトランザクション処理結果はその後ブロック化されてチェーンとして連結される。

【０００９】

チェーンに連結されたブロックは膨大な時間のかかる処理をしない限り改ざんすることは不可能な状態になっている。分散台帳ネットワークシステムにおいて、トランザクション履行後の各口座の資産高は、トランザクションの処理結果はブロック化を通じて強固に守られる。このブロックは過去に作成されたブロックとの整合性が要求されるため、改ざんは極めて困難である。一方、ブロックに組み込まれる前の段階での不正は別の方法で防がれる必要がある。

【００１０】

トランザクションを処理するうえでの不備はノードの障害に起因する。ノード障害には少なくとも二つの類型がある。機能障害と、意図的な不正を行う障害とである。機能障害として例えば、他のノードと通信できない通信障害と、演算を正しく行えない演算障害と、記録した情報に正しくアクセスできないストレージ障害などが挙げられる。これらの障害は各ノードに対する動作テストを行えば比較的たやすく検出できて対処することもできる。

【００１１】

一方、意図的な不正を行うノードの検出とその対策には困難が伴う。これらのノードは上記の動作テストは難なく合格する。そして、通常は他の正常なノードと同様にトランザクションを正しく処理する。しかし、ある時に突然不正な処理をする。例えば、所定の振込先とは別に、勝手に特定の口座に一部資産を移すということがあり得る。通常は他の正常なノードに紛れて目立たないが時として不正な動作をするノードを「ビザンチン障害を有するノード」又は単に「障害ノード」と呼ぶこととする。

【００１２】

ビザンチン障害を有するノードは、例えば重要な組織の中枢に侵入した厄介なスパイのようである。普段は普通に動作して目立たぬ存在である。しかし、特定のトランザクションを処理するときに、突如不正処理をする。このようなノードは通常の動作テストでは排除できない。

【００１３】

不正の利益を得る目的を持つ者がこのビザンチン障害を意図的に発生させている可能性がある。例えば、パブリックチェーンを構成するノードとして誰でも自身のコンピュータを自由に参加させることができる。したがって比較的容易にビザンチン障害を有するノードの複数個を分散台帳ネットワークシステムに組み込み得る。一方、プライベートチェーンやコンソーシアムチェーンでは主催者若しくは主催グループがノードコンピュータを整備するので比較的安全である。しかし外部からのハッキングにより、これらのノードもビザンチン障害を有するに至る可能性もある。このようなビザンチン障害を有するノードがネットワーク内に混入している可能性のあることを踏まえて不正防止対策を講じる必要がある。

【００１４】

ここで、利用者からトランザクション処理を託されて最終的にブロック化されるまでの過程を確認する。第１過程では、リーダーノードは履行前トランザクション情報をバックアップノードに配信する。第２過程では、処理を担当するノードがそのトランザクション履行後の口座資産高を算出する。第３過程では、トランザクション履行後の資産高をブロック化して改ざんを困難にする。このように３つの過程が存在し得る。

【００１５】

第１過程における不正はリーダーノードによるトランザクション内容の改ざんである。例えばトークンの振込先を変えたり、履行条件を変えたりすることがあり得る。しかし、この不正は一般的には秘密鍵を用いたデジタル署名で防止できる。デジタル署名を伴う情報列への改ざんの有無は秘密鍵と対の公開鍵を使うことで簡単に確認できる。したがって、バックアップノードは公開鍵を使って容易にリーダーノードによるトランザクション内容の改ざんを検出することができる。

【００１６】

第２過程であり得る不正はトランザクション処理の改変である。トランザクションの処

理結果が妥当であるか否かは一義的には判断できない。そこで、複数のノードに同一のトランザクションを処理させてその結果を比較し、一定数以上のノードで同一の結果であればその結果は正しいものとみなされる。しかし、ビザンチン障害を有する複数のノードが結託して同一の不正結果を生じさせることもあり得るので、これへの対処も必要である。

【００１７】

特許文献１には、複数のノードに同一のトランザクションの処理をさせてこれらの結果を比較して、結果が一致するノードの数が所定のしきい値を超えれば、これらのノードが出力した結果を正しいとみなすことが記載されている。

【００１８】

非特許文献２および特許文献２には、ｆを自然数としたときに、３ｆ＋１個のコンセンサスノードに同一のトランザクションの処理をさせてこれらの結果を比較してその正しさを確認することが記載されている。このとき、２ｆ＋１個のコンセンサスノードによる結果が一致した場合にその結果は正しいとみなすこととしている。このばあい、ビザンチン障害を有するコンセンサスノードがｆ個含まれていたとしても、その２倍を超える正常なコンセンサスノードによって正しい結果が得られるという考え方である。

【００１９】

更に特許文献２では更にトランザクション処理に時間制限が設けられており、通信障害やその他の障害によってこれを超える処理時間を要するコンセンサスノードはコンセンサス形成の処理から除外され代わりのコンセンサスノードがこの処理に充てられると記載されている。また、２ｆ＋１個のコンセンサスノードによる結果が一致した時点でコンセンサス形成の処理の結果を確定させることでコンセンサス形成の処理にかかる時間を短縮することが記載されている。

【００２０】

コンセンサス形成の処理に関わるノードの数が小さいと、不正を目論む者にとっては懐柔するノードが少ないので不正をし易いといえる。特許文献３にも、ブロックチェーンは規模が小さいほど少数の攻撃者による結託攻撃を受けるリスクが高まることが記載されている。同文献では、コンセンサス形成の処理への参加ノードを他のブロックチェーンからランダムに追加してノード数を増すことで結託攻撃を受けるリスクを減じようとしている。

【００２１】

第３過程における不正も防ぐ必要がある。非特許文献１によれば、ここでもやはりデジタル署名やハッシュ関数を活用することが挙げられているが詳細は割愛する。

【００２２】

コンセンサス形成の処理は以後、単にコンセンサス処理ということもある。コンセンサス処理は、これに参加するノード間でＰ２Ｐ通信を通じてトランザクションおよびその処理結果をやり取りして各ノードの結果を比較して正当性ある結果を決定するものである。この処理へ参加するノード数が多いと、１つのトランザクションを処理するために要する演算資源が多くなり、必要となるＰ２Ｐ通信の量も多くなる。しかし、該処理への参加ノードの数を少なくすると障害ノードによる結託攻撃にたいして脆弱になる。

【先行技術文献】

【特許文献】

【００２３】

【文献】特表２０２０－５１５９３９号公報
【文献】特表２０２０－５０４３５１号公報
【文献】特開２０２０－０６１６９６号公報

【非特許文献】

【００２４】

【文献】コンセンサス・ベイス株式会社著　「ブロックチェーンの仕組みと開発がしっかりわかる教科書」　技術評論社２０１９年.
【文献】LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE, "The Byzantine Generals Problem", ACM Transactions on Programming Languages and

Systems, Vol. 4, No. 3, July 1982.

【発明の概要】

【発明が解決しようとする課題】

【００２５】

そこで本発明の目的は、コンセンサス処理に参加するノードの数を減らすことなく、これらのノード間に要求される通信量を減じることができる分散台帳ネットワークシステムのコンセンサス形成方法およびコンセンサス形成用プログラムを提供することにある。

【課題を解決するための手段】

【００２６】

上記課題は、分散台帳ネットワークシステムを構成するノードコンピュータの中の１６台のノードコンピュータがコンセンサスを形成する場合において、上記１６台のノードコンピュータを、４台ずつ４つの基本単位に分割する単位化ステップと、これらの基本単位それぞれについて、該基本単位に属する４つの前記ノードコンピュータがそれぞれ処理した４つの前記処理値を互いに照合し合った上で、３つ以上の前記ノードコンピュータによる前記処理値が一致する場合にはそれをその基本単位が出力するプレコンセンサス値とするプレコンセンサス形成ステップとを有し、これに続くコンセンサス成否判定ステップにて、一致して唯一最高の頻度を有するプレコンセンサス値が有るときはコンセンサス成立と判定して、該プレコンセンサス値をそのトランザクションの処理結果とするコンセンサス形成方法により解決する。

【発明の効果】

【００２７】

本発明のコンセンサス形成方法およびコンセンサス形成用プログラムにより、コンセンサス処理に参加するノードの数を減らすことなく、これらのノード間に要求される通信量を減じることができるという効果がある。

【図面の簡単な説明】

【００２８】

【図１】図１は分散台帳ネットワークシステムのトランザクション処理過程を示す図である。

【図２】図２はビザンチン障害回避コンセンサス形成アルゴリズムの処理フローの図である。

【図３】図３はビザンチン障害回避コンセンサス形成アルゴリズムの具体的な例を示す図である。

【図４】図４はビザンチン障害回避コンセンサス形成アルゴリズムの実施に必要な通信量を見積もる図である。

【図５】図５はコンセンサス処理参加ノード数と必要な通信回数をまとめた図である。

【図６】図６は障害ノードの数に対する耐性評価を表す図である。

【図７】図７はＳ‐ＢＦＴＣにおいて、コンセンサスが成立又は不成立になる確率の算出方法を示す図である。

【図８】図８は本発明に係る第１実施形態を表す図である。

【図９】図９はＳ‐ＢＦＴＣによるプレコンセンサス形成の具体例を説明する図である。

【図１０】図１０はコンセンサス成否判定ステップの処理フローの図である。

【図１１】図１１は本発明の第１実施形態の通信量を見積もる図である。

【図１２】図１２は本発明の第１実施形態において、コンセンサスが成立又は不成立になる確率の算出方法を示す図である。

【図１３】図１３は各基本単位を構成する正常ノード数と障害ノード数が特定されたときの「場合の数」の具体的な計算方法を示す図である。

【図１４】図１４は第１実施形態の障害ノードに対する耐性の評価を表す図である。

【図１５】図１５は本発明に係る第２実施形態の分散台帳ネットワークシステムのトランザクション処理過程を示す図である。

【図１６】図１６はノードからコンセンサス成否判定器へ送信されるデータ書式を説明す

る図である。
【図１７】図１７はコンセンサス成否判定器の構成を説明する図である。
【発明を実施するための形態】
【００２９】
＜分散台帳ネットワークシステムのトランザクション処理過程＞
図１は分散台帳ネットワークシステムのトランザクション処理過程を示す図である。ここでは分散台帳ネットワークシステムを構成するノードの中の１６個のノードが、ビザンチン障害の影響を排除するためのコンセンサス処理を通じてトランザクション処理をする過程を説明する。このコンセンサス処理を「ビザンチン障害回避コンセンサス形成」又はＢＦＴＣと表すこともある。
【００３０】
図１では紙面水平方向に空間を表して、垂直方向矢印の向きに時間経過を表している。そして、分散台帳ネットワークシステムのトランザクション処理はｓｔｐｐ１～ｓｔｐｐ５の５段階を経る。まず、リーダーノードｎｘ０が利用者ＣＸ１からトランザクションＴＸの履行を託される（ｓｔｐｐ１）。トランザクションＴＸの履行とは、例えば、ある口座の資産の一部を別の口座に振り込んだりすることである。具体的には振込元の口座の資産の一部を減じて振込先口座の資産を増すことである。また、振込元口座から減じた資産の一部は振込手数料としてノード管理者の口座に振り込まれる場合もある。
【００３１】
利用者ＣＸ１からトランザクションＴＸの履行を託されたリーダーノードｎｘ０はそのトランザクションＴＸをバックアップノードｎｘ１～ｎｘ１５に配信する（ｓｔｐｐ２）。その結果、コンセンサス処理に参加する１６個のノードは同一のトランザクション情報を保持していることとなる。コンセンサス処理に参加する１６個のノードにはリーダーノードｎｘ０が含まれていてもよいし、含まれていなくてもよい。ここで示す例ではリーダーノードｎｘ０を含めてコンセンサス処理に参加するノードが１６個である。
【００３２】
コンセンサス処理に参加する各ノードは、保持しているトランザクションに添付されているデジタル署名を利用してそのトランザクションの正当性を確認する。その後トランザクション処理をして結果を算出する（ｓｔｐｐ３）。トランザクション処理の結果とは、例えば取引によって変化した当事者の口座残高である。
【００３３】
次いで、コンセンサス処理に参加しているノードはＰ２Ｐ通信を通じて、他のノードによるトランザクションＴＸの処理結果を相互に送信し合って収集する（ｓｔｐｐ４）。その後、各ノード内でこれらの処理結果を比較検証するコンセンサス処理が行われる（ｓｔｐｐ５）。
【００３４】
このステップ（ｓｔｐｐ５）完了後に、各ノードのメモリ領域には、同一のコンセンサス処理の結果が保持されている。コンセンサス処理の結果には、各ノードのトランザクションの一致又は不一致の記録、最終的に決定されたトランザクション処理の結果、最終結果とは異なる処理結果を出力したことによりビザンチン障害の疑いのあるノードに関する情報が含まれ得る。図示していないが、その後のトランザクションＴＸの処理結果をブロック化するにあたっては、ノードｎｘ０～ｎｘ１５のいずれかを参照すればよい。
【００３５】
＜ビザンチン障害回避コンセンサス形成アルゴリズム＞
コンセンサス処理の一例として、ビザンチン障害回避コンセンサス形成アルゴリズム（以下ＢＦＴＣアルゴリズムと言うこともある。）を説明する。ＢＦＴＣアルゴリズムを簡略に述べれば次のようになる。コンセンサス処理に参加したノードによる同一トランザクションの結果が全て一致したときはコンセンサス成立で、その一致した処理値は正当なトランザクション処理結果とみなされる。そして、これをコンセンサス値と称することとする。トランザクションの処理結果の全てが一致しなくても、一致する結果を出力したノー

ドが多数を占め、一致しなかった結果を出力したノード数の２倍を超える場合もコンセンサス成立とする。一方、トランザクション処理結果が何通りか出現し、最大多数の結果を出力したノード数が、その他の結果を出力したノード数の２倍を超えない場合はコンセンサス形成失敗で、コンセンサス値は不定、若しくは存在しないものとされる。この場合、トランザクションＴＸは履行されない。

【００３６】

図２はビザンチン障害回避コンセンサス形成（ＢＦＴＣ）アルゴリズムの処理フローの図である。図２において、コンセンサス参加ノードｎｘ０～ｎｘ１５にトランザクションＴＸを処理させて、その処理値の全てを各ノードｎｘ０～ｎｘ１５に集める（ｓｔｐｘ１）。これに続く処理はノードｎｘ０～ｎｘ１５でそれぞれ別個に行われる。次いで、一致する処理値同士をグループ化し、各グループに含まれる処理値の数をメンバー数とする（ｓｔｐｘ２）。メンバー数とは、その処理値を出力したノードの個数に他ならない。そして、メンバー数で唯一つの最大値を持つグループが存在するか否かを判定する（ｓｔｐｘ３）。唯一つの最大値を持つグループが存在しない場合は‘偽’としてステップｓｔｐｐ６へ分岐する。この場合はコンセンサス不成立であって、トランザクションTX処理結果不定との結論を出してコンセンサス処理を完了する（ｓｔｐｐ６）。そして、この分散台帳ネットワークシステムにおいてトランザクションＴＸは履行されない。

【００３７】

一方、唯一つの最大値を持つグループが存在する場合は‘真’としてｓｔｐｘ４へ分岐する。ここで、最大値グループのメンバー数が、その他の処理値の数の２倍を超えるか否かが判定される（ｓｔｐｘ４）。最大値グループのメンバー数が、その他の処理値の数の２倍を超えない場合は‘偽’としてステップｓｔｐｐ７へ分岐する。この場合はコンセンサス不成立であって、トランザクションTX処理結果不定との結論を出してコンセンサス処理を完了する。このときも、この分散台帳ネットワークシステムにおいてトランザクションＴＸは履行されない。

【００３８】

一方、最大値グループのメンバー数が、その他の処理値の数の２倍を超える場合は‘真’としてステップｓｔｐｐ５へ分岐する。この場合、コンセンサスは成立してトランザクションTXの処理結果は確定する。その最大値グループ内で一致する処理値がコンセンサス値であって、これをトランザクションＴＸの処理結果となる。この処理結果はやがてブロック化されて改ざん困難な状態で保管される。以上がビザンチン障害回避コンセンサス形成（ＢＦＴＣ）アルゴリズムの処理フローである。

【００３９】

図３はＢＦＴＣアルゴリズムの具体的な例を示す図である。図３（Ａ）は、コンセンサス処理に参加した１６個のノード全ての処理値がＷであった場合である。一致する処理値Ｗ同士をグループ化し、そのグループに含まれる処理値の数である１６をメンバー数とする。これは図２を参照して説明したステップｓｔｐｘ２の処理である。メンバー数１６のグループは唯一つの最大値を持つグループであるからステップｓｔｐｘ３では‘真’としてステップｓｔｐｘ４へ分岐する。そして、このグループ以外の処理値の数はゼロである。したがって、最大値グループのメンバー数はその他の処理値の数の２倍を超えるので、ｓｔｐｘ４にて‘真’であり、コンセンサスは成立しトランザクションTXの処理結果は確定する。その最大値グループ内で一致する処理値Ｗがコンセンサス値であって、これをトランザクションTXの処理結果とする。

【００４０】

図３（Ｂ）は、コンセンサス処理に参加した１６個のノードの処理値がＷとＭ、Ｐの３通りの場合である。一致する処理値Ｗ同士と、Ｍ同士と、Ｐ同士をそれぞれグループ化して３つのグループになる。これらグループに含まれる処理値の数である８、６、２を、それぞれのグループのメンバー数とする。そして処理値Ｗのグループは唯一つの最大値８を持つグループとなる。処理値Ｗのグループは唯一つの最大値８を持つグループであるからステップｓｔｐｘ３で‘真’としてステップｓｔｐｘ４へ分岐する。処理値Ｗのグループ以

外の処理値の数はＭが６個でＰが２個であるから合計８である。最大値グループのメンバー数８はその他の処理値の数８の２倍を超えないから‘偽’としてステップｓｔｐｘ７へ分岐する。すなわちコンセンサス不成立である。そしてコンセンサス値は不定であり、トランザクションTXは処理されない。

【００４１】

図３（Ｃ）は、コンセンサス処理に参加した１６個のノードの処理値がＷとＭの２通りの場合である。一致する処理値に基づいて、これらの処理値若しくはこれらの処理値を出力したノードをグループ分けすると２つのグループが生じる。各グループに属する処理値の数すなわちメンバー数は、処理値Ｗのグループは１１、処理値Ｍのグループは５である。ここで、メンバー数が唯一最大であるグループは処理値Ｗのグループで、そのメンバー数は１１である。処理値Ｗ以外のグループのメンバー数は５である。そうすると、メンバー数が唯一最大であるグループのメンバー数１１は、その他のメンバー数５の２倍を超えている。これは図２のステップｓｔｐｘ４の分岐である。ここでは‘真’としてステップｓｔｐｘ５へ進み、コンセンサス成立でコンセンサス値はＷとなる。

【００４２】

以上、コンセンサス処理に参加するノード数１６を例として、ＢＦＴＣアルゴリズムを説明した。この例で示したように、ノード数１６でＢＦＴＣアルゴリズムを適用すると最大で５個のノードが不正な処理値を出力してもコンセンサスは成立してコンセンサス値が定まる。ｆを自然数として、これを一般化すると、３×ｆ＋１個のノードでＢＦＴＣコンセンサス処理を行うならば、最大でｆ個までのノードの不正出力に耐性を有して、正当なトランザクション処理結果を確定することができる。

【００４３】

＜(3f+1)個のノードによるＢＦＴＣで必要な通信量＞

次に、自然数ｆについて（３ｆ＋１）個のノードによるＢＦＴＣに必要な通信量を見積もる。図４はＢＦＴＣアルゴリズムの実施に必要な通信量を見積もる図である。図４を参照して、コンセンサス処理に参加するノードの数が（３ｆ＋１）個である場合のＢＦＴＣ処理の流れと必要な通信量について説明する。図４では紙面水平方向に空間を表して、垂直方向矢印の向きに時間経過を表している。まず、利用者ＣＸ１が処理したいトランザクションＴＸを、分散台帳ネットワークシステムを構成するノードのいずれかに転送する。図４の例ではノードｎｘ０にトランザクションＴＸが転送されている。ここで１回の通信が発生する。利用者ＣＸ１から最初にトランザクションの転送を受けたノードをリーダーノードと称することとする。

【００４４】

リーダーノードｎｘ０はトランザクションＴＸに付されているデジタル署名を検証して、そのトランザクションＴＸが正当なものであることを確認する。正当なトランザクションであることが確認されたなら、リーダーノードｎｘ０は、コンセンサス処理に参加するノードｎｘ１～ｎｘ（３ｆ）にトランザクションＴＸをＰ２Ｐで配信する。ここで３ｆ回の通信が発生する。コンセンサス処理に参加するノードをバックアップ（ＢＫＵＰ）ノードと称することとする。この例では、リーダーノードｎｘ０に、（３ｆ）個のバックアップノードｎｘ１～ｎｘ（３ｆ）を加えて、全部で（３ｆ＋１）個のノードでコンセンサス処理をする。トランザクションＴＸの配信を受けたバックアップノードはそれぞれ、これに付されているデジタル署名を検証してトランザクションＴＸの正当性を確認する。リーダーノードｎｘ０がビザンチン障害を有していて、これらのバックアップノードに不正なトランザクションを送りつけてくる可能性があるからである。

【００４５】

トランザクションＴＸの正当性が確認された後に、リーダーノードｎｘ０とバックアップノードｎｘ１～ｎｘ（３ｆ）とは、それぞれ独立にトランザクションＴＸを処理して処理値を算出する。各処理値には処理したノードのデジタル署名が付されている。コンセンサス処理に参加するノードにビザンチン障害を有しているノードが無ければ、同一であるトランザクションＴＸの処理値は当然一致する。各ノードが算出した処理値はＰ２Ｐ通信

によって、コンセンサス処理に参加している全てのノードに配信される。この処理値を配信するのに３ｆ×（３ｆ＋１）回の通信が必要である。結局（３ｆ＋１）個のノードによるＢＦＴＣで必要な通信回数は３ｆ＋１＋３ｆ×（３ｆ＋１）＝（３ｆ＋１）（３ｆ＋１）である。

【００４６】

図５はコンセンサス処理参加ノード数と必要な通信回数をまとめた図である。上式のｆに具体的な自然数を入れ、図５に、コンセンサス処理に参加するノード数と必要な通信数を示す。図５に示すように、ｆを１、２、・・・、５と増加させると、コンセンサス処理に参加するノード数は線形で、４、７、・・・、１６と増加する。これに対して、必要な通信回数は１６、４９、・・・、２５６と、放物線として急速に増加する。

【００４７】

以上説明したＢＦＴＣアルゴリズムによれば、ビザンチン障害を有するノードの数がｆ以内であれば、それらの影響を受けることなくトランザクション処理を遂行することができる。しかし、ビザンチン障害を有するノードが２ｆを超えると、障害ノードによる不正な処理結果が正当な結果とみなされてしまうので注意が必要である。したがって、ビザンチン障害を有するノードの数がｆを超えないように継続的に保守をする必要がある。例えば、各ノードに保持されているコンセンサス成立とコンセンサス値から、不正処理をしたノードが明かになっている。この情報を参照して該当するノードを同ネットワークシステムから除外したり、該当するノードコンピュータのソフトウェアを再インストールしてノードの刷新をしたりすることが必要である。ここで、ｆの値が小さいほど必要とされる通信回数を減じることができる。その一方で、不正なノードの増加に対する耐性が弱くなるという課題がある。

【００４８】

＜障害ノードの数に対する分散台帳ネットワークシステムの耐性の評価＞

次に、ビザンチン障害を有して不正処理をし得るノードの数に対する、ＢＦＴＣアルゴリズムを適用した分散台帳ネットワークシステムの耐性について評価する。１６個のノードでコンセンサス処理をする場合を例とする。障害ノードが０個から徐々に増えて１６個になる過程において、正常なノードによるコンセンサスが成立して正当なトランザクションの処理値を得られる確率を評価する。図６は障害ノードの数に対する耐性評価を表す図であって、同図（Ａ）はＢＦＴＣアルゴリズムを適用した１６個ノードによるコンセンサス処理において、障害ノードが０個から１６個まで増えた場合のコンセンサス成立確率の推移を表している。図６（Ｂ）は後記するので説明は省略する。

【００４９】

同図（Ａ）は次の考えのもとに作成された。コンセンサス処理に参加する１６個のノードが１６個の正常なノードである場合、この中に正常なノードが１６個含まれる確率は勿論１００％である。また、コンセンサス処理に参加する１６個のノードが１５個の正常なノードと１個の障害ノードである場合、この中に正常なノードが１５個含まれる確率は当然１００％である。同様に、徐々に障害ノードの数を増していく。コンセンサス処理に参加するノードが正常な１２個と不正な４個である場合、この中に正常なノードが１２個含まれる確率は、これも当然１００％である。更に、コンセンサス処理に参加するノードが正常な１１個と不正な５個である場合、この中に正常なノードが１１個含まれる確率は１００％である。そして、正常なノードが１１個以上含まれているときは、ＢＦＴＣアルゴリズムの適用で正常なノードによるコンセンサスが成立してコンセンサス値が決まる。つまり、障害ノードの数が０個から５個まで増加しても、１００％の確率で正常ノードによるコンセンサスが成立する。これが図６（Ａ）に示されている。

【００５０】

図６（Ａ）の縦軸は発生確率で横軸は障害ノードの数である。この図において、左側の障害ノードの数が０～５個の場合は、１００％の確率で正常ノードによるコンセンサスが成立することを示している。図６（Ａ）において、白い棒グラフは正常なノードによる正当コンセンサスが成立する確率を表す。斜線の棒グラフはコンセンサスが成立しない確率

を表す。黒の棒グラフはビザンチン障害によって不正処理をする障害ノードによる不正コンセンサスが成立する確率を表す。

【００５１】

同様に、コンセンサス処理に参加するノードが正常な１０個と不正な６個である場合、この中に不正なノードが６個含まれる確率は１００％である。そして、１００％の確率でコンセンサスは不成立である。１００％の確率で不正なノードが１０個含まれる場合も、１００％の確率でコンセンサス不成立である。これを表しているのが、同図における、障害ノード数６～１０個の場合である。

【００５２】

更に障害ノードが増えて、１００％の確率で１１個になった場合であって、かつこれらの障害ノードが結託して同一の不正処理値を出力するならば、１００％の確率で障害ノードによるコンセンサスが成立し、不正な処理値が正当とみなされてしまう虞が生じる。これは同図における、障害ノード数１１～１６個の場合である。この図から、障害ノードの数をせいぜい５個以下にしておかねばならないことが分かる。

【００５３】

＜Ｓ‐ＢＦＴＣ＞

上述したように、コンセンサス処理への参加ノードは多い方がビザンチン障害ノードに対する耐性が高い。一方で、コンセンサス処理への参加ノードは少ない方が必要な通信量が少なくて済む。両方の利点を併せ持つコンセンサス処理方法を得るためにＳ‐ＢＦＴＣアルゴリズムを提案する。このアルゴリズムはコンセンサス処理に参加する１６個のノードから無作為に採取した４個のノードでＢＦＴＣアルゴリズムを行うものである。これは図５を使って上述したｆ＝１の時の通信量を必要とする。この時の通信回数は１６であり、ｆ＝５に該当する１６個ノードで必要な通信量２５６の１６分の１である。４個ノードＢＦＴＣは、ＢＦＴＣアルゴリズム実施可能な最小単位であることから、１６個ノードから採取した４個ノードによるＢＦＴＣをスモールＢＦＴＣ又はＳ‐ＢＦＴＣと称することとする。１６個のノードから４個を採取する方法は無作為に採取することができる。また、トランザクション処理ごとにローテーションしてもよい。

【００５４】

＜Ｓ‐ＢＦＴＣのビザンチン障害ノード数に対する耐性の評価＞

次に、Ｓ‐ＢＦＴＣのビザンチン障害ノード数に対する耐性を評価する。Ｓ‐ＢＦＴＣにおいて、正常ノードによってコンセンサスが成立するのは、採取された４個のノードが、４個の正常ノードで成る場合と、３個の正常ノードと１個の障害ノードで成る場合とである。障害ノード１個が存在しても正常ノードが３個以上あれば正常ノードの数が障害ノードの数の２倍を超えるからである。

【００５５】

また、コンセンサスが不成立になるのは、コンセンサス処理のために採取された４個のノードが、２個の正常ノードと２個の障害ノードで成る場合である。更に、障害ノードによるコンセンサスが成立するのは、コンセンサス処理のために採取された４個のノードが、４個の障害ノードで成っていてこれらの３個以上が結託して同じ不正値を出力する場合と、３個の障害ノードと１個の正常ノードで成っていてこれらの障害ノード３個が結託して同じ不正値を出力する場合である。

【００５６】

したがって、コンセンサス処理に参加する４個のノードの組み合わせが上記になる場合についての確率を求めれば、Ｓ‐ＢＦＴＣアルゴリズムによるコンセンサス処理のビザンチン障害耐性を評価できる。正常ノードは常に正しい処理値を出力する一方で、障害ノードは正しい処理値を出力したり不正な処理値を出力したりし得る。しかし説明を単純化するために、障害ノードは結託して必ず同一の不正処理値を出力するものとする。この仮定は当該分散台帳ネットワークシステムに最も深刻な障害を与える場合の仮定である。

【００５７】

図７はＳ‐ＢＦＴＣにおいて、コンセンサスが成立又は不成立になる確率の算出方法を

示す図である。ここで、コンセンサス処理のために採取された４個のノードが、正常なノードｍ個と不正なノード（４－ｍ）個である場合を、Ｓ‐ＢＦＴＣ（ｍ，４－ｍ）と表すこととする。起こり得る場合を列挙すると、Ｓ‐ＢＦＴＣ（４，０）、Ｓ‐ＢＦＴＣ（３，１）、Ｓ‐ＢＦＴＣ（２，２）、Ｓ‐ＢＦＴＣ（１，３）、Ｓ‐ＢＦＴＣ（０，４）の５通りである。以下、図７を参照しながら、Ｓ‐ＢＦＴＣアルゴリズムによるコンセンサス成立又は不成立になる確率を説明する。

【００５８】

１６個のノードから４個のノードを採取する場合の数ＣＮＡＬＬは、１６のノードから４個取り出す組み合わせの数であるから図７（Ａ）に示す式で算出できて、１，８２０である。

【００５９】

まず、１６個のノードが、１６個の正常なノードと０個の不正なノードとで成っている場合を示す。この場合のＳ‐ＢＦＴＣ（４，０）およびＳ‐ＢＦＴＣ（３，０）、Ｓ‐ＢＦＴＣ（２，２）、Ｓ‐ＢＦＴＣ（１，３）、Ｓ‐ＢＦＴＣ（０，４）の場合の数は図７（Ｂ）に示されている。例えば、同図の行１は、Ｓ‐ＢＦＴＣ（４，０）すなわち正常なノードが４個採取される場合の数（Ｂ欄）が示されている。つまり正常ノード１６個から４個を採取する組み合わせ数は１，８２０で、障害ノード０個から０個を採取する組み合わせは１である。これらの積１，８２０がＳ‐ＢＦＴＣ（４，０）の場合の数である。これを上記ＣＮＡＬＬで除して確率（Ｃ欄）が１００．０％と算出される。

【００６０】

同図の行２は、Ｓ‐ＢＦＴＣ（３，１）すなわち正常なノードが３個採取される場合の数（Ｂ欄）が示されている。つまり正常ノード１６個から３個を採取する組み合わせ数は５６０で、障害ノード０個から１個を採取することは不可能であるからゼロである。これらの積ゼロがＳ‐ＢＦＴＣ（３，１）の場合の数である。これを上記ＣＮＡＬＬで除して確率（Ｃ欄）が０．０％と算出される。同図の行３、行４、行５についても、障害ノードを採取することはできないのでＢ欄の場合の数はゼロであり、Ｃ欄の確率も０．０％と算出される。結局、障害ノードが全く含まれていない場合は、１００．０％の確率で４個のノード全てが正常ノードであり、正常ノードによるコンセンサスが成立する。

【００６１】

同様にして、障害ノードが含まれる数を１から１６まで増して場合の数を計算する。ここでは、障害ノードが５個含まれる場合について具体的に説明して、その他は割愛する。図７（Ｃ）は１６個のノードが正常ノード１１個と障害ノード５個で成る場合を示している。同図の行１はＳ‐ＢＦＴＣ（４，０）の場合の数で、１１個の正常ノードから４個を採取する場合の数と５個の障害ノードから０個を採取する場合の数の積として、３３０が算出される（Ｂ欄）。同図の行２はＳ‐ＢＦＴＣ（３，１）の場合の数で、１１個の正常ノードから３個を採取する場合の数と５個の障害ノードから１個を採取する場合の数の積として、８２５が算出される（Ｂ欄）。その他の場合も同様に算出されて、これらを上記ＣＮＡＬＬで除してＣ欄の確率が計算される。Ｓ‐ＢＦＴＣ（４，０）とＳ‐ＢＦＴＣ（３，０）、Ｓ‐ＢＦＴＣ（２，２）、Ｓ‐ＢＦＴＣ（１，３）、Ｓ‐ＢＦＴＣ（０，４）の発生確率はそれぞれ、１８．１％と４５．３％、３０．３％、６．０％、０．３％である（Ｃ欄）。

【００６２】

Ｓ‐ＢＦＴＣアルゴリズムによれば、コンセンサス処理に正常ノードが４個又は３個含まれていれば正常ノードによるコンセンサスが成立する。そして、障害ノードが２個だけ含まれているとコンセンサス不成立である。また、障害ノードが３個又は４個含まれていて、これらのノードが結託して同一の不正な処理値を出力するならば障害ノードによるコンセンサスが成立する。したがって、１６個のノードが１１個の正常ノードと５個の障害ノードで成る場合、正常ノードによるコンセンサスが成立する確率は図７（Ｃ）の行１と行２の確率の和すなわち、１８．１＋４５．３＝６３．４％である。そして、同図の行３から、３０．３％の確率でコンセンサス不成立である。また、同図の行４と行５の確率の

和として、６．０＋０．３＝６．３％の確率で障害ノードによるコンセンサスが成立する。
【００６３】
再び図６に戻る。図６は障害ノードの数に対する耐性評価を表す図であって、同図（Ａ）は１６個ノードによるＢＦＴＣアルゴリズムによるコンセンサス処理において、障害ノードが０から１６個まで増えた場合のコンセンサスの成立確率の推移を表している。そして同図（Ｂ）は、１６個ノードによるＳ‐ＢＦＴＣアルゴリズムによるコンセンサス処理におけるコンセンサスの成立確率の推移を表している。
【００６４】
縦軸は発生確率で横軸は障害ノードの数である。白い棒グラフは正常なノードによる正当コンセンサスが成立する確率を表す。斜線の棒グラフはコンセンサスが成立しない確率を表す。黒の棒グラフはビザンチン障害によって不正処理をする障害ノードによる不正コンセンサスが成立する確率を表す。同図（Ｂ）から、左側の障害ノードの数が０又は１個の場合は、１００％の確率で正常ノードによるコンセンサスが成立することが分かる。しかし、障害ノードが２個の場合は５％の確率でコンセンサスが不成立になる。障害ノードが３個の場合は、１２．９％の確率でコンセンサス不成立になり、０．７％の確率で障害ノードによるコンセンサスが成立してしまう。
【００６５】
障害ノードが５個含まれる場合、正常なノードによってコンセンサスが成立する確率は６３．４％である。３０．３％の確率でコンセンサス不成立になり、６．３％の確率で障害ノードによるコンセンサスが成立する。コンセンサス処理をする分散台帳ネットワークシステムは、コンセンサス処理によってコンセンサスの成立又は失敗については判別可能である。この場合は３０．３％の確率でコンセンサス形成に失敗し、残りの６９．７％は成功する。しかし、成功したコンセンサスの中に９．０％（＝６．３×１００．０／６９．７）の確率で障害ノードによる不正な処理値について成立したコンセンサスが含まれている。これは深刻な問題である。障害ノード数５に対して１００％の耐性である「１６個ノードＢＦＴＣ」と比べて、Ｓ‐ＢＦＴＣは障害ノードに対する耐性が弱いことが分かる。
【００６６】
＜第１実施形態　複数Ｓ‐ＢＦＴＣ＞
そこで、１６個ノードＢＦＴＣよりも通信量を低減させながらも障害ノードに対する耐性を低下させないコンセンサスアルゴリズムを提案する。図８は本発明に係る第１実施形態を表す図である。同図（Ａ）は同実施形態の概要を示している。コンセンサス処理に参加するノードは１６個である。これらのノードｎ０，ｎ１，ｎ２，・・・，ｎ１５には同一のトランザクションＴＸを配信した後に処理をさせてそれぞれの処理値を出力させる〔トランザクション配信処理ステップ（ｓｔｐ０）〕。そして、これらのノードを４個ずつ４つの基本単位ｕ０およびｕ１，ｕ２，ｕ３に分割する〔単位化ステップ（ｓｔｐ１）〕。次いで、各基本単位にて、Ｓ‐ＢＦＴＣすなわち４個ノードによるＢＦＴＣを実施する〔プレコンセンサス形成ステップ（ｓｔｐ２）〕。そして、プレコンセンサスの成否とプレコンセンサス値とに基づいてトランザクションＴＸに対する最終的なコンセンサスの成否を判定する〔コンセンサス判定ステップ（ｓｔｐ３）〕。ここで、基本単位ｕ０およびｕ１，ｕ２，ｕ３における処理にプレコンセンサスおよびプレコンセンサス値と称するのは、トランザクションＴＸについての最終的なコンセンサスおよびコンセンサス値と区別するためである。また、同実施形態を、複数のＳ‐ＢＦＴＣを統合するアルゴリズムと言う意味で、「複数Ｓ‐ＢＦＴＣ」と称することもある。
【００６７】
＜プレコンセンサス形成ステップ（ｓｔｐ２）＞
４つの基本単位ｕ０およびｕ１，ｕ２，ｕ３において、プレコンセンサスが成立した場合にはプレコンセンサス値が定まる。各基本単位において、３個以上のノードで処理値が一致すればプレコンセンサスが成立し、この値がプレコンセンサス値となる。３個以上のノードで処理値が一致しなければプレコンセンサスは不成立で、プレコンセンサス値も不定である。

【００６８】
＜コンセンサス判定ステップ（ｓｔｐ３）＞
コンセンサス判定ステップ（ｓｔｐ３）において、プレコンセンサス形成ステップ（ｓｔｐ２）で得られたプレコンセンサス値を、一致するもの同士でグループ化する。各グループに属するプレコンセンサス値の数をそのグループのメンバー数とする。メンバー数とは、そのプレコンセンサス値を出力した基本単位の数に他ならない。いわゆる多数決でコンセンサス値が決定され、コンセンサス値が決定されるならばコンセンサスが成立したこととなる。したがって、プレコンセンサス形成ステップ（ｓｔｐ２）で得られるプレコンセンサス値が皆無であれば最終的なコンセンサス値は不定であってコンセンサス不成立である。また、２通りのプレコンセンサス値が１対１、又は２対２のように同数の時も、最終的なコンセンサス値は不定であってコンセンサス不成立である。
【００６９】
上述の一致するプレコンセンサス値がつくるグループのメンバー数において唯一最大数のグループが存在するときはそのグループで一致するプレコンセンサス値が最終的なコンセンサス値となってコンセンサスは成立する。したがって、プレコンセンサス形成ステップ（ｓｔｐ２）で得られるプレコンセンサス値が唯１つである場合は、そのプレコンセンサス値が作るグループのメンバー数１が唯一最大値であるから、そのプレコンセンサス値が最終的なコンセンサス値となってコンセンサスは成立する。また、得られたプレコンセンサス値がすべて一致する場合も、それらのプレコンセンサス値が作るグループがメンバー数において唯一最大であるからコンセンサス値が決定し、コンセンサスは成立する。また、得られた２以上のプレコンセンサス値がすべて一致しない場合は、それぞれが作るグループのメンバー数は１であって、唯一最大のグループが存在しないからコンセンサス値は不定であってコンセンサス不成立である。
【００７０】
また、上記グループのメンバー数は発生するプレコンセンサス値の頻度としてとらえてもよい。つまり、基本単位ｕ０～ｕ３の全て若しくは幾つかが一つずつ出力するプレコンセンサス値についてコンセンサス判定ステップ（ｓｔｐ３）の中では、一致するプレコンセンサス値同士の発生頻度を計数するプレコンセンサス値発生頻度計数ステップを設けてもよい。該プレコンセンサス値発生頻度計数ステップにて計数された頻度分布において唯一最大頻度である前記プレコンセンサス値が有るときは該プレコンセンサス値をトランザクションＴＸ処理結果と定めて、ブロック化前のコンセンサスは形成されたと判定するすることができる。一方で、前記プレコンセンサス値発生頻度計数ステップで計数された頻度分布において唯一最大頻度である前記プレコンセンサス値が無いときはブロック化前のコンセンサスは形成されなかったと判定することができる。
【００７１】
図８（Ｂ）は同実施形態の処理フローの図である。コンセンサス処理に参加する１６個のノードｎ０，ｎ１，ｎ２，・・・，ｎ１５に、履行を依頼されたトランザクションＴＸが配信される。そして各ノードのそれぞれがこれを処理して、その処理結果である処理値を得る〔トランザクション配信処理ステップ（ｓｔｐ０）〕。また、上記１６個のノードは４つの基本単位ｕ０およびｕ１，ｕ２，ｕ３に分割される〔単位化ステップ（ｓｔｐ１）〕。これらのノードはこのように４つの基本単位に分割されたからでもｓｔｐ０のトランザクション処理をすることができる。したがって、ｓｔｐ０とｓｔｐ１の履行順序を入れ替えることも可能な場合がある。次に、上記４つの基本単位内においてそれぞれＳ‐ＢＦＴＣを実施によりプレコンセンサスを形成してプレコンセンサス値を得る〔プレコンセンサス形成ステップ（ｓｔｐ２）〕。その後、プレコンセンサス値に基づいて、トランザクションＴＸの処理についての最終的なコンセンサスの成否を決定する〔コンセンサス判定ステップ（ｓｔｐ３）〕。
【００７２】
＜単位化ステップ（ｓｔｐ１）における基本単位への分割の仕方＞
単位化ステップ（ｓｔｐ１）において、コンセンサス処理に参加する１６個のノードｎ

０～ｎ１５を基本単位ｕ０～ｕ３に分割する方法は様々な方法がある。たとえば、予め、基本単位ｕ０に属するノードをノードｎ０およびｎ１、ｎ２、ｎ３とし、基本単位ｕ１に属するノードをノードｎ４およびｎ５、ｎ６、ｎ７とし、基本単位ｕ２に属するノードをノードｎ８およびｎ９、ｎ１０、ｎ１１とし、基本単位ｕ３に属するノードをノードｎ１２およびｎ１３、ｎ１４、ｎ１５と決めておいてもよい。また、この分割状態を基本として、トランザクションを処理するたびに、ノードｎ０を基本単位ｕ３に、ノードｎ４を基本単位ｕ０に、ノードｎ８を基本単位ｕ１に、ノードｎ１２を基本単位ｕ２に組替えするというようにローテーションさせてもよい。又は、利用者から新たなトランザクション処理の依頼を受けるたびに、リーダーノードが分割状態を決めて、その情報を当該トランザクションに付加してバックアップノードに配信してもよい。例えば、図８（Ｃ）に示すように、ノード番号が記載された単位化テーブルＧＴＢのようなデータにリーダーノードのデジタル署名を付加したデータを送ってもよい。ただし、この場合はトランザクション配信処理ステップ（ｓｔｐ０）に続いて単位化ステップ（ｓｔｐ１）を行う必要がある。リーダーノードは無作為に基本単位ｕ０～ｕ３への分割状態を定義してもよいし、発生させた乱数に基づいてこの分割状態を定義してもよい。

【００７３】

＜プレコンセンサス形成ステップ（ｓｔｐ２）の具体例＞

Ｓ‐ＢＦＴＣによるプレコンセンサス形成の実態は４個ノードによるＢＦＴＣであるから、その処理フローは図２を参照しながら説明済みである。ここではプレコンセンサス形成の具体例を示す。図９はＳ‐ＢＦＴＣによるプレコンセンサス形成の具体例を説明する図である。同図（Ａ）は、同一基本単位に属していてプレコンセンサス処理に参加する４個のノードが全て同一の処理値Ｗを出力した場合である。一致する処理値Ｗのグループが１つだけ発生し、処理値Ｗの数すなわちメンバー数は４で、これはメンバー数において唯一最大値グループである。他のグループのメンバー数はゼロだから、この最大値は他のグループのメンバー数の２倍を超える。よってこの場合はプレコンセンサス成立で、プレコンセンサス値はＷである。

【００７４】

図９（Ｂ）は、３つの一致する処理値Ｗを含むグループと、一つの処理値Ｍを含むグループとで２つのグループが発生する場合である。勿論、各グループにおける処理値の数とは、これらの処理値を出力したノードコンピュータの台数でもある。ここで、処理値Ｗのグループはメンバー数において唯一最大である。そして、その他のグループに属するメンバー数１の２倍を超えている。よって、プレコンセンサス成立で、プレコンセンサス値はＷである。

【００７５】

一方、図９（Ｃ）と（Ｄ）はいずれもプレコンセンサス不成立でプレコンセンサス値不定の場合である。（Ｃ）では処理値Ｗのグループと処理値Ｍのグループがいずれもメンバー数２であって、唯一最大値を有するグループが無い。（Ｄ）では、メンバー数において唯一最大である処理値Ｗのグループは、その他のメンバー数の２倍を超えることができない。

【００７６】

以上をまとめると、４個のノードで行われるＳ‐ＢＦＴＣにおいては、３個以上のノードで処理値が一致すれば、図２を参照して説明したコンセンサス成立の条件が整う。すなわち、メンバー数において唯一最大であり、かつ、他のメンバー数の２倍を超えるという条件が整う。基本単位でＳ‐ＢＦＴＣによるプレコンセンサスが成立した場合、この基本単位を「プレコンセンサス成立基本単位」と称することもある。

【００７７】

また、処理値が一致するノードが２個以下の場合は上記コンセンサスの条件が整わず、基本単位でのプレコンセンサスは成立しないし、プレコンセンサス値も確定しない。そして、基本単位を「プレコンセンサス不成立基本単位」と称することもある。そして、コンセンサス値不定のことを「プレコンセンサス値不定」と称することもある。以上説明した

プレコンセンサス形成ステップ（ｓｔｐ２）によって、基本単位ｕ０～ｕ３はそれぞれ、プレコンセンサス成立基本単位又はプレコンセンサス不成立基本単位のいずれかに一方に定まる。

【００７８】

続いて、コンセンサス成否判定ステップ（ｓｔｐ３）が行われる。これは、４つの基本単位ｕ０およびｕ１、ｕ２、ｕ３によるプレコンセンサス値に基づいて、トランザクションＴＸ履行についてのコンセンサス成否を決定する処理である。図１０はコンセンサス成否判定ステップ（ｓｔｐ３）の処理フローの図である。図１０において、生成されたプレコンセンサス値の数がゼロの場合は‘真’としてｓｔｐｐ６へ分岐する。この場合は、コンセンサスは不成立であり、トランザクションTXの処理結果不定である（ｓｔｐｐ６）。そして場合のトランザクションＴＸは不履行であり、当該分散台帳ネットワークシステムの口座の残高状態は同トランザクションＴＸが依頼された時点と変化なしである。一方、生成されたプレコンセンサス値の数がゼロでない場合は‘偽’としてｓｔｐｐ２へ分岐する。

【００７９】

ここで、生成されたプレコンセンサス値の数が１の場合は‘真’としてｓｔｐｐ７へ分岐する。この場合は、コンセンサスは成立し、そのプレコンセンサス値をコンセンサス値とする。そしてこれをトランザクションＴＸの処理結果として同トランザクションは履行される（ｓｔｐｐ７）。一方、生成されたプレコンセンサス値の数が１ではない場合は‘偽’としてステップｓｔｐｐ３へ分岐する。

【００８０】

ｓｔｐｐ３において、２つ以上のプレコンセンサス値が存在する中で、一致するプレコンセンサス値同士をグループ化し、含まれるプレコンセンサス値の数をそのグループのメンバー数とする。続くｓｔｐｐ４にて、メンバー数で唯一つの最大値グループが存在する場合は‘真’としてｓｔｐｐ５へ分岐し、コンセンサス成立とし、その最大値グループ間で一致するプレコンセンサス値をトランザクションＴＸの処理結果として確定する（ｓｔｐｐ５）。一方メンバー数で唯一つの最大値グループが存在しない場合はｓｔｐｐ８へ分岐する。この場合はコンセンサス不成立でトランザクションＴＸ処理結果は不定である。以上がコンセンサス成否判定ステップ（ｓｔｐ３）の処理フローである。このコンセンサス成否判定ステップ（ｓｔｐ３）も各ノードｎ０～ｎ１５で行われて同一の結果が各ノードのメモリ領域に保持される。図示していないが、その後のトランザクションＴＸの処理結果をブロック化するにあたっては、ノードｎ０～ｎ１５のいずれかを参照すればよい。

【００８１】

＜第１実施形態における通信量の評価＞

図１１は本発明の第１実施形態の通信量を見積もる図である。図１１を参照して、本発明の第１実施形態の通信量を見積もる。まず、利用者ＣＸ１から、分散台帳ネットワークシステムを構成するノードの１つに履行を託されたトランザクションＴＸが通信される。ここで１回通信が発生する。最初にトランザクションＴＸを受付けたノードをリーダーノードｎ０とする。リーダーノードｎ０はその他のバックアップノードｎ１～ｎ１５にそのトランザクションＴＸを配信する。ここで１５回通信が発生する。図１１では、１６個のノードを４つの基本単位ｕ０およびｕ１、ｕ２、ｕ３にまとめて表している。基本単位ｕ０に属するノードｎ０は、同基本単位に属する他のノードへの配信で３回通信し、その他の基本単位に属するノード４個に対してそれぞれ通信するので上記の通信回数となる（１６回の通信）。

【００８２】

その後各基本単位にてＳ‐ＢＦＴＣが行われる。各基本単位にて３×４回の通信が発生し、４つ分の基本単位に対してこの４倍の通信量が必要となる。結局４８回〔＝（３×４）×４〕の通信が発生する。そして、最後に各ノードでコンセンサス成否判定するために、全ノードにＳ‐ＢＦＴＣによるプレコンセンサス値を配信する必要がある。各ノードには自身が属していない基本単位のプレコンセンサス値が必要である。各基本単位の中の１つのノードが他の基本単位にプレコンセンサス値を伝送するのに４８回〔＝（４×３）×

４〕の通信が必要である。

【００８３】

以上を合計すると、第１実施形態で必要な通信回数は１１２回（＝１６＋４８＋４８）である。これはＳ‐ＢＦＴＣ単独で必要な通信回数１６よりも大きくなっている。しかし、１６個ノードＢＦＴＣの通信回数２５６（図５参照。）よりも少ない。

【００８４】

＜第１実施形態のビザンチン障害ノードに対する耐性を評価＞

図１２は本発明の第１実施形態において、コンセンサスが成立又は不成立になる確率の算出方法を示す図である。１６個のノードｎ０、ｎ１、ｎ２、・・・、ｎ１５から、まず基本単位ｕ０に属するノードを選び、次いで基本単位ｕ１およびｕ２、ｕ３の順で属するノードを選ぶとすると、同図（Ａ）の式で場合の数を計算できる。選び方の場合の数はこの式より、ＣＮ２ＡＬＬ＝６３，０６３，０００である。

【００８５】

ここで、基本単位ｕ０およびｕ１、ｕ２、ｕ３において、４個ずつ採取されたノードにおいて、基本単位ｕ０およびｕ１、ｕ２、ｕ３に含まれる正常ノード数と障害ノード数の数とを、ＣＯＭＢ（ｕ０の正常ノード数，ｕ０の障害ノード数）（ｕ１の正常ノード数，ｕ１の障害ノード数）（ｕ２の正常ノード数，ｕ２の障害ノード数）（ｕ３の正常ノード数，ｕ３の障害ノード数）と表すこととする。このとき、それぞれの基本単位において、正常ノード数と異常ノード数との和は４である。そして、図１２（Ｂ）のように挙げると全部で６２５通りである。それは、各基本単位とも、正常ノード数と障害ノード数の組合せ数は（４，０）（３，１）（２，２）（１，３）（０，４）の５通りだから、４つの基本単位については、６２５（＝５×５×５×５）と算出されるからである〔同図（Ｃ）〕。

【００８６】

ビザンチン障害ノードに対する耐性を評価するのであるから、１６個のノードに含まれる障害ノードの数が０～１６の間で増加していく状況でコンセンサス成否の確率を求める必要がある。そこで、障害ノードの数のバリエーションが０、１、２、・・・、１６の１７通りについて上記６２５の組合せ数について計算する必要がある。つまり、１０，６２５（＝６２５×１７）通りについて「場合の数」を求める必要がある。そして、その「場合の数」をＣＮ２ＡＬＬで除すと、その「場合」が生じる確率が求まる。

【００８７】

図１３は各基本単位を構成する正常ノード数と障害ノード数が特定されたときの「場合の数」の具体的な計算方法を示す図である。同図（Ａ）は１６個のノードに正常ノード９個と障害ノード７個とが含まれる条件である。このとき、ＣＯＭＢ（３，１）（１，３）（３，１）（２，２）を発生する場合の数の算出方法を示している。基本単位ｕ０を構成する３個の正常ノードと１個の障害ノードとを採取する組合せ数は、正常ノード９個から３個採取する組合せ数と障害ノード７個から１個を採取する組合せ数との積である。そして、基本単位ｕ１を構成する１個の正常ノードと３個の障害ノードとを採取する組合せ数は、残る正常ノード６個から１個採取する組合せ数と、残る障害ノード６個から３個を採取する組合せ数との積である。基本単位ｕ２とｕ３についても同様の乗算で計算できる。これらを全て掛け合わせると、ＣＮ２＝２，１１６，８００である。これをＣＮ２ＡＬＬで除して発生確率３．３５６６４％を算出できる。尚、ＣＯＭＢ（３，１）（１，３）（３，１）（２，２）は、コンセンサス成否判定ステップ（ｓｔｐ３）によれば正常ノードによるコンセンサスが成立する。

【００８８】

図１３（Ｂ）は同じく１６個のノードに正常ノード９個と障害ノード７個とが含まれる条件下でＣＯＭＢ（３，１）（０，４）（４，０）（２，２）を発生する場合の数の算出方法である。上記と同様に計算すると。場合の数ＣＮ２＝１３２，３００が算出される。これをＣＮ２ＡＬＬで除して発生確率０．２０９７９％を算出できる。同組合せＣＯＭＢ（３，１）（０，４）（４，０）（２，２）もコンセンサス成否判定ステップ（ｓｔｐ３

）によれば正常ノードによるコンセンサスが成立する。
【００８９】
図１３（Ｃ）は（Ｂ）と同様の組合せＣＯＭＢ（３，１）（０，４）（４，０）（２，２）であるが、１６個のノードが正常ノード１１個と障害ノード5個とで成っている。上記と同じ方法でＣＮ２の計算式を作ると、最後の乗数は０個の障害ノードから２個を採取する組合せ数になっている。これは不可能であって実現し得ないのでゼロとして乗算する。そうすると、ＣＮ２＝０で、この発生確率は０．０％である。以上説明した方法で全ての組合せの発生確率を求めると、第１実施形態のビザンチン障害ノードに対する耐性を評価することができる。
【００９０】
図１４は第１実施形態の障害ノードに対する耐性の評価を表す図であって、障害ノードが０から１６個まで増えた場合のコンセンサスの成立確率の推移を表している。同図（Ａ）において、縦軸は発生確率で横軸は障害ノードの数である。白い棒グラフは正常なノードによる正当コンセンサスが成立する確率を表す。斜線の棒グラフはコンセンサスが成立しない確率を表す。黒の棒グラフはビザンチン障害によって不正処理をする障害ノードによる不正コンセンサスが成立する確率を表す。
【００９１】
同図（Ａ）によれば、障害ノードの個数が０～５までは、１００％の確率で正常ノードによるコンセンサスが成立する。また、障害ノードが６個、７個と増加するにつれてコンセンサス不成立の確率が１．２％、２２．２％と増加する。このコンセンサス方法を適用する分散台帳ネットワークシステムはコンセンサスの成否を検出できるので、コンセンサスが不成立になった場合は再度実施すると、次にはコンセンサスを成立させる確率が増加する。したがって、障害ノードが７個までならば、障害ノードの解消作業が済むまで暫定的にそのままシステムを稼働することができる。例えば、障害ノードの個数が６個の場合はコンセンサス処理で続けて２回ともコンセンサス不成立になる確率は０．０１４４％である。つまり、２回コンセンサス処理をすれば９９．９８５６％の確率で正常ノードによるコンセンサスが成立する。障害ノード数７の場合でも２回のコンセンサス処理で９５．０７１６％の確率で正常ノードによるコンセンサスが成立する。
【００９２】
図１４（Ｂ）は障害ノード数の増加に伴って変化するコンセンサスの成立確率を第１実施形態と１６個ノートＢＦＴＣで比較した図である。両者とも障害ノード数５以下の条件では１００％の確率で正常ノードによるコンセンサスが成立する。また、障害ノード数６～７では第１実施形態の方が正常ノードによるコンセンサス成立確率が高い。
【００９３】
＜第２実施形態＞
ｆを自然数としたときの、（３ｆ＋１）個ノードによるＢＦＴＣと、本発明に係る第１実施形態とは共に、コンセンサスの結果は各ノードに保存されている。そして、これをブロック化するためにいずれかのノードからコンセンサス値を読み取る必要がある。しかし、その情報を読み取ろうとしたノードがたまたま障害ノードである場合には正当な情報を提供する確証がないという課題がある。そこで、信頼度の高いノードから読み取った情報のみを利用する、本発明に係る第２実施形態を説明する。
【００９４】
図１５は本発明に係る第２実施形態の分散台帳ネットワークシステムのトランザクション処理過程を示す図である。第２実施形態は、図８を参照して説明した第１実施形態とは、トランザクション配信処理ステップ（ｓｔｐ０）と、単位化ステップ（ｓｔｐ１）と、プレコンセンサス形成ステップ（ｓｔｐ２）とにおいて共通する。しかし、コンセンサス判定ステップ（ｓｔｐ３）はコンセンサス成否判定器ｃｏｌ１で行う。プレコンセンサス形成ステップ（ｓｔｐ２）を完了した16個のノードｎ０およびｎ１、ｎ２、ｎ１５はプレコンセンサス形成ステップ（ｓｔｐ２）の結果を所定の書式データとしてコンセンサス成否判定器ｃｏｌ１に送る。

【００９５】
図１６はノードからコンセンサス成否判定器ｃｏｌ１へ送信されるデータ書式を説明する図である。同図（Ａ）はコンセンサス成否判定器ｃｏｌ１が受信するデータ書式の例である。ここには、各基本単位にて共にプレコンセンサス形成ステップ（ｓｔｐ２）に関わった４個のノードの信用度ポイントを投票する信用度ポイント投票領域ＴＰＶと、そのノード自身による処理値を格納する処理値格納領域ＴＥＶとを有する。更に、後記する、単位化テーブルＧＴＢを有する。
【００９６】
同図（Ｂ）は、各ノードが送信するデータの例である。これは、ある基本単位にてノードｎ０とｎ２と、ｎ３とは処理値Ｗを出力し、ノードｎ１は処理値Ｍを出力した例である。このときｎ０の送信データの信用度ポイント投票領域ＴＰＶには、自己同一処理値を出力するノードｎ２とｎ３と、自己ｎ０に該当する領域に1ポイントずつ投票されている。そして処理値格納領域ＴＥＶには自己の出力した処理値Ｗが格納されている。
【００９７】
また、ｎ１の送信データでは、信用度ポイント投票領域ＴＰＶには自己の領域のみに1ポイント投票されている。他のノードとは処理値が一致しないからである。そして処理値格納領域ＴＥＶには自己の出力した処理値Ｍが格納されている。
【００９８】
また、ｎ２とｎ３の送信データでは、信用度ポイント投票領域ＴＰＶには自己の領域と、自己の同一の処理値を出力した２個のノードにそれぞれ1ポイントずつ投票されている。そして処理値格納領域ＴＥＶには自己の出力した処理値Ｗが格納されている。この信用度ノードは各ノードとも自己の他に3個のノードに対して1ポイントずつ投票できる。
【００９９】
同図（Ｃ）は、コンセンサス成否判定器ｃｏｌ１における信用度ポイント集計結果である。この例では、ノードｎ０およびｎ２、ｎ３がそれぞれ信用度ポイント３点を獲得している。これは３ノード間の処理値が一致していることを示している。ノードｎ１は自己投票のポイント１点のみを獲得している。また、仮に基本単位内の４個のノードの処理値が全て一致した場合には各ノードとも信用度ポイント４点を獲得する。これを踏まえて、コンセンサス成否判定器ｃｏｌ１は、信用度ポイント３点以上を獲得しているノードを一時的に仮に信頼できるノードとして、そのノードが属する基本単位におけるプレコンセンサス形成ステップ（ｓｔｐ２）における結果として、プレコセンサス成立でプレコンセンサス値は当該ノードから送信された処理値をその基本単位におけるプレコンセンサス値とみなす。
【０１００】
図１７はコンセンサス成否判定器ｃｏｌ１の構成を説明する図である。図１７に示すように、コンセンサス成否判定器ｃｏｌ１はデータ受信部ｃ１と、受信データ格納部ｃ２と、信頼度ポイント集計部ｃ３と、プレコンセンサス成立基本単位の選別部ｃ４と、プレコンセンサス値頻度計数器ｃ５と、コンセンサス判定器ｃ６と、判定結果保持部ｃ７と、データ配信部ｃ８と、単位化テーブル検証部ｃ９とで構成されている。
【０１０１】
プレコンセンサス形成ステップ（ｓｔｐ２）を経た後に１６個のノードｎ０～ｎ１５から送信されるデータは、データ受信部ｃ１で受信されて受信データ格納部ｃ２に一時的に保存される。受信されたデータは、信用度ポイント投票領域ＴＰＶと、処理値格納領域ＴＥＶと、単位化テーブルＧＴＢとからなっている。
【０１０２】
単位化テーブル検証部ｃ９では、各ノードから送信された単位化テーブルＧＴＢ同士を比較検証する。単位化テーブルＧＴＢはリーダーノードｎ０が決めた該１６個のノードの基本単位ｕ０およびｕ１、ｕ２、ｕ３への分割の仕方が定義されている。各ノードから送信されたこのテーブルは一致するはずである。これらのテーブルにはリーダーノードｎ０のデジタル署名が付されており、各ノードによって痕跡を残さずに改ざんすることは不可

能である。それにもかかわらず、各ノードから受信した単位化テーブルＧＴＢが一致しない場合にはリーダーノードｎ０が不正を行って各ノードに異なる単位化テーブルＧＴＢを送信したことになる。この場合には、プレコンセンサス形成ステップ（ｓｔｐ２）の信頼性が確保されないとして、再度、単位化ステップ（ｓｔｐ１）とプレコンセンサス形成ステップ（ｓｔｐ２）とが実施される。これらが再実施される旨は、データ配信部ｃ８を通じて各ノードに送信される。

【０１０３】

再度実施されるにあたり、障害ノードの疑いのあるリーダーノードｎ０は除外される。再度実施されるコンセンサス処理のために、その他のノードから新たなリーダーノードが選択される。再実施に際してどのノードをリーダーノードにするのかは、予め決めておいてもよい。コンセンサス処理に参加する全ノードに連番を付しておいて、第１のリーダーノードに障害が認められた場合には、１つ番号の大きな、若しくは小さなノードを新たなリーダーノードとしてもよい。新たなリーダーノードが再度、単位化テーブルＧＴＢを定義してそのノードのデジタル署名を付して他のコンセンサス処理参加ノードに配信する。処理すべきトランザクションＴＸはデジタル署名により改ざん不可能に既に各ノードに配信されているので新たに配信しなくてもよい。

【０１０４】

また、コンセンサス処理に参加するノードを１６個にするために、新規なノードを１個参加させてもよい。このときは新たなリーダーノードよりトランザクションＴＸと単位化テーブルＧＴＢとをその新規なノードに送信してもよい。また、増やさず新たなリーダーノードを２個分のノードとして扱う運用もあり得る。すなわち、単位化テーブルＧＴＢを定義するに際しては、新たなリーダーノードが属する基本単位には、他に２個のノードを属することとして該基本単位は３個のノードで構成する。また、プレコンセンサス形成ステップ（ｓｔｐ２）では、その新たなリーダーノードの処理値は２つ分に数えることとする。また、どのノードがリーダーノードであるかは、単位化テーブルＧＴＢに付されたデジタル署名から明らかであるし、又は、単位化テーブルＧＴＢにリーダーノードとそれ以外のノード（バックアップノード）の別が判別できるようなマークが付されていてもよい。

【０１０５】

信頼度ポイント集計部ｃ３では信用度ポイント投票領域ＴＰＶで投票されたポイントを集計する。また、上記コンセンサス処理の再実施にあたり、上記新たなリーダーノードを２個分として扱う運用では、該新たなリーダーノードによる投票ポイントは２倍化して扱ってもよい。投票されたポイントを集計した結果、３点ト以上獲得しているノードは仮の信頼すべきノードである。プレコンセンサス成立基本単位の選別部ｃ４では、信用度ポイントを３点以上獲得しているノードが属している基本単位を「プレコンセンサス成立基本単位」として選別し、そのノードによる処理値をそのプレコンセンサス成立基本単位の「プレコンセンサス値」として抽出する。

【０１０６】

プレコンセンサス値頻度計数器ｃ５は、プレコンセンサス成立基本単位の選別部ｃ４で抽出されたプレコンセンサス値の一致するものについてその頻度を計数する。そもそも、プレコンセンサス値の数はプレコンセンサス成立基本単位の数でもあって０～４の間である。そしてプレコンセンサス値が一致するものの頻度を取るならばこれも０～４の間である。

【０１０７】

コンセンサス判定器ｃ６は、プレコンセンサス値頻度計数器ｃ５の出力する頻度分布に基づいてコンセンサスの成否を判定する。該頻度分布において、唯一の最大頻度値が存在する場合に、トランザクションＴＸに関するコンセンサス成立と判定する。そして、この唯一の最大頻度値を有するプレコンセンサス値をコンセンサス値と決定する。そして、受信データ格納部ｃ２に格納されている各ノードの処理値を参照し、このコンセンサス値と一致するノードを正常ノードと決定し、それ以外の処理値を出力したノードを障害ノードと決定する。また、このコンセンサス値はトランザクションＴＸの処理値としてやがてブ

ロック化される。

【０１０８】

一方で、プレコンセンサス値頻度計数器ｃ５の出力する頻度分布において、唯一の最大頻度値を有するプレコンセンサス値が無いときは、コンセンサス判定器ｃ６によってトランザクションＴＸに関するコンセンサスは形成されなかったと判定される。

【０１０９】

分散台帳ネットワークシステムにおけるコンセンサス処理は、一部のノードに専ら処理を任せることによって生じる不正行為を防止するために、多数のノードで処理データを交換し合って処理するものである。ＢＦＴＣアルゴリズムではコンセンサス処理にかかわる全ノードで処理データを交換し合う。しかし、本発明に係る第１実施形態および第２実施形態では、全プレコンセンサス処理にこれらの全ノードが関わっておらず、その不透明性に懸念を示される可能性もある。そこで、判定結果保持部ｃ７には、コンセンサス判定器ｃ６にて判定されたコンセンサス値と、プレコンセンサス成立基本単位の選別部ｃ４で判明した全プレコンセンサス値と、受信データ格納部ｃ２に保存されている受信データから抽出された各ノードによる処理値とが一定期間保持されていて、この分散台帳ネットワークシステムを構成する全ノードがその内容を、データ配信部ｃ８を通して判読検証することが可能である。また、一定期間経過後に当トランザクションＴＸをブロック化するにあたっては、ここからコンセンサス値を入手することができる。

【０１１０】

判定結果保持部ｃ７の内容には、絶対的な信頼性が要求されるところ、コンセンサス成否判定器ｃｏｌ１はビザンチン障害を起こさない構造若しくは起こし難い構造である方が好ましい。そこで、判定結果保持部ｃ７は演算器とメモリと該メモリに記憶されているプログラムとで、汎用的な機能を持つ構成ではなく、必要最小限の機能のみを実現する構成が望ましい。例えば、トランジスタ・トランジスタ・ロジック等の電子回路で構成され、ハッキングの原因となるソフトウェア処理を含まない構成が好ましい。

【０１１１】

それにはプレコンセンサス値頻度計数器ｃ５において、プレコンセンサス値の一致又は不一致の判定動作にも単純化が求められる。そのため、各ノードから送信される処理値は定型化されていることが好ましい。処理値の定型化とは、例えば、取引対象である振込元口座番号や、振込先口座番号や、振込額や、手数料などは、記載順序や桁数を固定化するなどがあり得る。振込条件も幾つかの類型に分類されていて、それを選択するなどの定型化されていることが好ましい。

【０１１２】

コンセンサス処理に参加するノードはソフトウェア処理が可能であるから、利用者からのトランザクションＴＸの記載は融通性を持たせることが可能である。しかし、コンセンサス成否判定器ｃｏｌ１に送信するデータに含まれる処理値は定型化されていることが好ましい。

【０１１３】

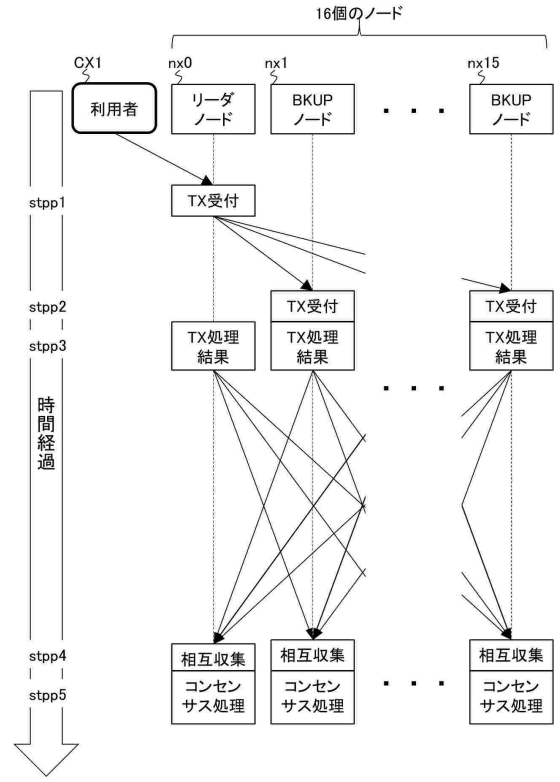
＜第２実施形態における通信量の評価＞

再び図１５に戻って、第２実施形態における通信量の評価をする。図１５は本発明に係る第２実施形態の分散台帳ネットワークシステムのトランザクション処理過程を示す図である。図１５において、利用者ＣＸ１からノードｎ０へのトランザクションＴＸの通信が１回発生する。ノードｎ０から他のノードｎ１～ｎ１５へのトランザクションＴＸの通信が１５回発生する。図１５では４個のノードずつまとめて基本単位ｕ０～ｕ３として記載されている。そして、Ｓ‐ＢＦＴＣによるプレコンセンサス処理で通信が４８〔＝（３×４）×４〕回発生する。最後に１６個のノードからそれぞれ、コンセンサス成否判定器ｃｏｌ１へデータを送るので、１６回の通信が発生する。以上を合計すると、８０（＝１＋１５＋４８＋１６）回の通信が必要になる。これは１６個ノードＢＦＴＣで必要な通信回数２５６の３０％余りであり、本発明に係る第２実施形態は通信量を減らす効果が高いといえる。

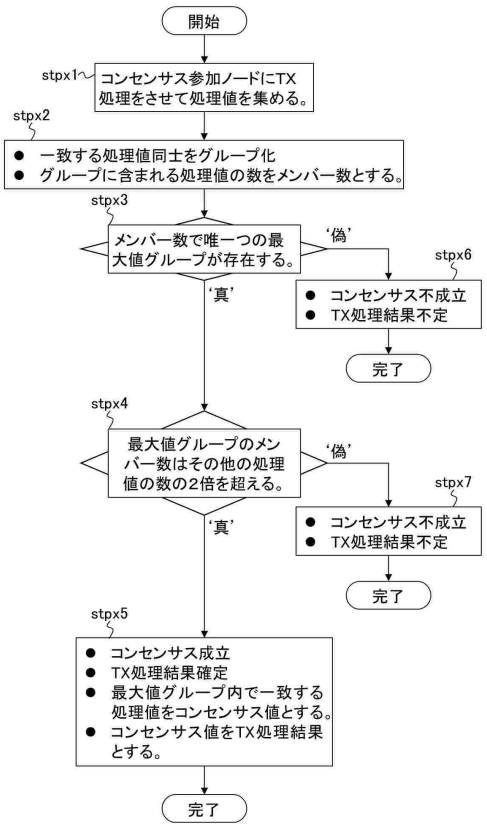
【産業上の利用可能性】
【０１１４】
本発明に係る実施形態は、分散台帳ネットワークシステムにおける通信量を削減しつつも障害ノードへの耐性に優れるコンセンサス形成方法およびコンセンサス形成用プログラムとして利用できる。
【符号の説明】
【０１１５】
ＣＸ１・・・利用者、ＴＸ・・・トランザクション、
ｎｘ０～ｎｘ１５、ｎ０～ｎ１５・・・コンセンサス処理に参加するノード、
ｃｏｌ１・・・コンセンサス成否判定器、ｕ０～ｕ３・・・基本単位、
ＴＰＶ・・・信用度ポイント投票領域、ＴＥＶ・・・処理値格納領域、
ＧＴＢ・・・単位化テーブル、ｃ１・・・データ受信部、ｃ２・・・受信データ格納部、
ｃ３・・・信頼度ポイント集計部、ｃ４・・・プレコンセンサス成立基本単位の選別部、
ｃ５・・・プレコンセンサス値頻度計数器、ｃ６・・・コンセンサス判定器、
ｃ７・・・判定結果保持部、ｃ８・・・データ配信部、ｃ９・・・単位化テーブル検証部

【図面】

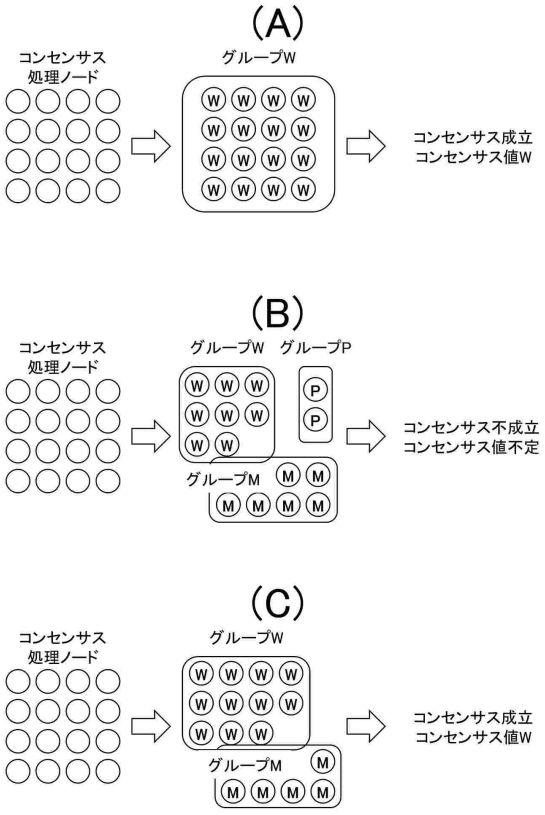
【図１】


16個のノード
CX1
nx0
nx1
nx15
利用者
リーダノード
BKUPノード
BKUPノード
TX受付
stpp1
stpp2
stpp3
stpp4
stpp5
時間経過
TX処理結果
TX受付
TX処理結果
TX受付
TX処理結果
相互収集
コンセンサス処理
相互収集
コンセンサス処理
相互収集
コンセンサス処理

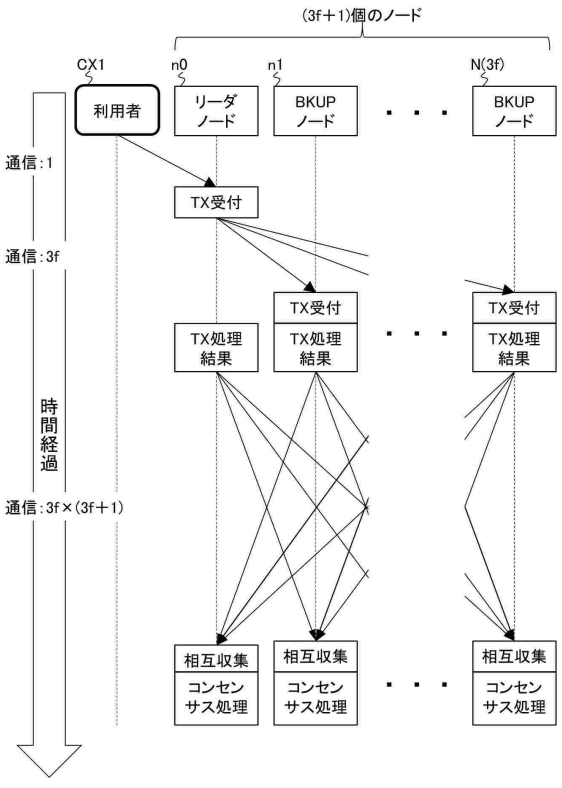
【図２】


開始
stpx1
コンセンサス参加ノードにTX処理をさせて処理値を集める。
stpx2
● 一致する処理値同士をグループ化
● グループに含まれる処理値の数をメンバー数とする。
stpx3
メンバー数で唯一つの最大値グループが存在する。
'偽'
'真'
stpx6
● コンセンサス不成立
● TX処理結果不定
完了
stpx4
最大値グループのメンバー数はその他の処理値の数の2倍を超える。
'偽'
'真'
stpx7
● コンセンサス不成立
● TX処理結果不定
完了
stpx5
● コンセンサス成立
● TX処理結果確定
● 最大値グループ内で一致する処理値をコンセンサス値とする。
● コンセンサス値をTX処理結果とする。
完了

【図３】


(A)
コンセンサス処理ノード
グループW
コンセンサス成立
コンセンサス値W
(B)
コンセンサス処理ノード
グループW
グループP
グループM
コンセンサス不成立
コンセンサス値不定
(C)
コンセンサス処理ノード
グループW
グループM
コンセンサス成立
コンセンサス値W

【図４】

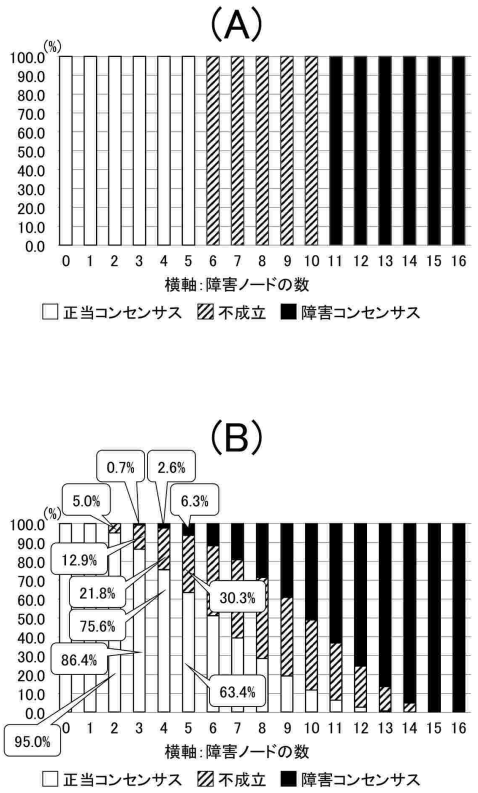

(3f+1)個のノード
CX1
n0
n1
N(3f)
利用者
リーダノード
BKUPノード
BKUPノード
通信:1
TX受付
通信:3f
TX受付
TX受付
TX処理結果
TX処理結果
TX処理結果
時間経過
通信:3f×(3f+1)
相互収集
コンセンサス処理
相互収集
コンセンサス処理
相互収集
コンセンサス処理

【図５】

f	コンセンサス処理参加ノード数	通信回数
1	4	16
2	7	49
3	10	100
4	13	169
5	16	256

コンセンサス処理参加ノード数計算式: 3f+1
通信回数計算式: (3f+1)(3f+1)

【図６】



【図７】

(A)

CNALL = $_{16}C_4$ =1,820

(B)

正常ノード16個、障害ノード0個

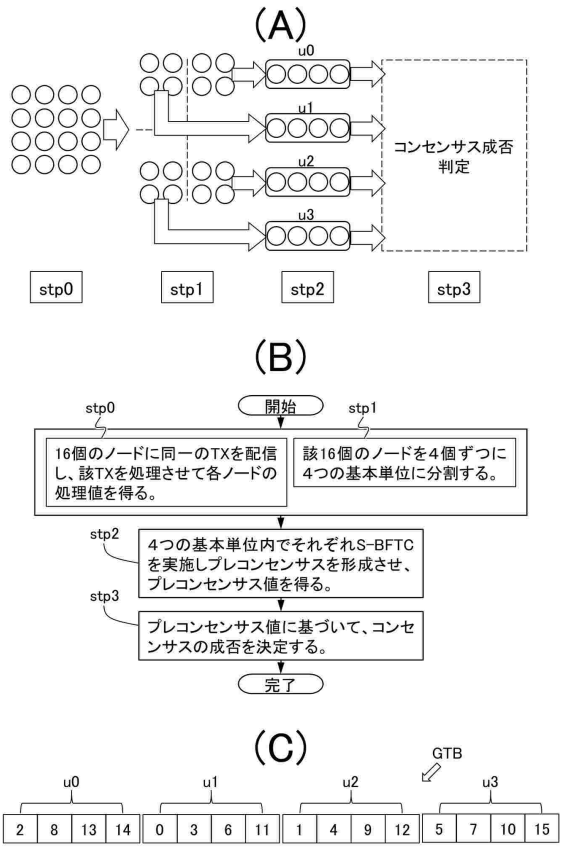
	A欄	B欄 場合の数	C欄 確率(%)
1	S-BFTC(4,0)	$_{16}C_4 \times {}_0C_0 = 1820 \times 1 = 1820$	100.0
2	S-BFTC(3,1)	$_{16}C_3 \times {}_0C_1 = 560 \times 0 = 0$	0.0
3	S-BFTC(2,2)	$_{16}C_2 \times {}_0C_2 = 120 \times 0 = 0$	0.0
4	S-BFTC(1,3)	$_{16}C_1 \times {}_0C_3 = 16 \times 0 = 0$	0.0
5	S-BFTC(0,4)	$_{16}C_0 \times {}_0C_4 = 1 \times 0 = 0$	0.0

(C)

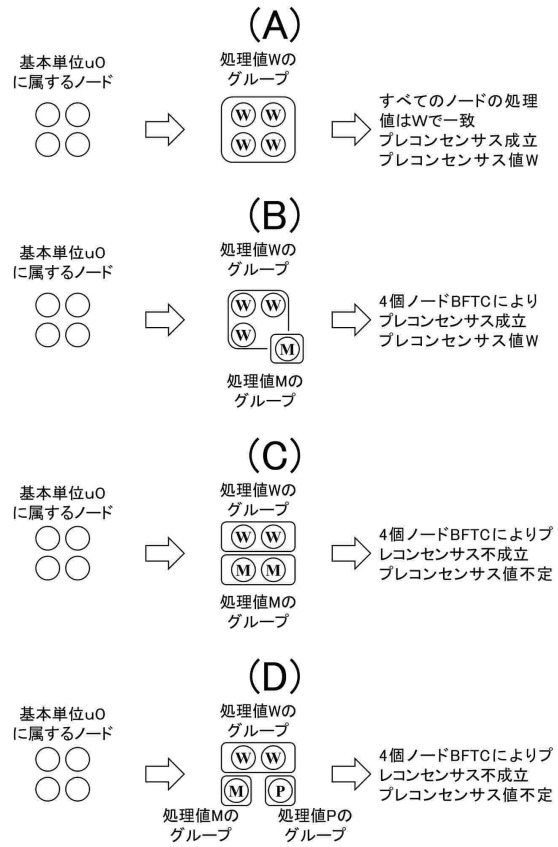
正常ノード11個、障害ノード5個

	A欄	B欄 場合の数	C欄 確率(%)
1	S-BFTC(4,0)	$_{11}C_4 \times {}_5C_0 = 330 \times 1 = 330$	18.1
2	S-BFTC(3,1)	$_{11}C_3 \times {}_5C_1 = 165 \times 5 = 825$	45.3
3	S-BFTC(2,2)	$_{11}C_2 \times {}_5C_2 = 55 \times 10 = 550$	30.3
4	S-BFTC(1,3)	$_{11}C_1 \times {}_5C_3 = 11 \times 10 = 110$	6.0
5	S-BFTC(0,4)	$_{11}C_0 \times {}_5C_4 = 1 \times 5 = 5$	0.3

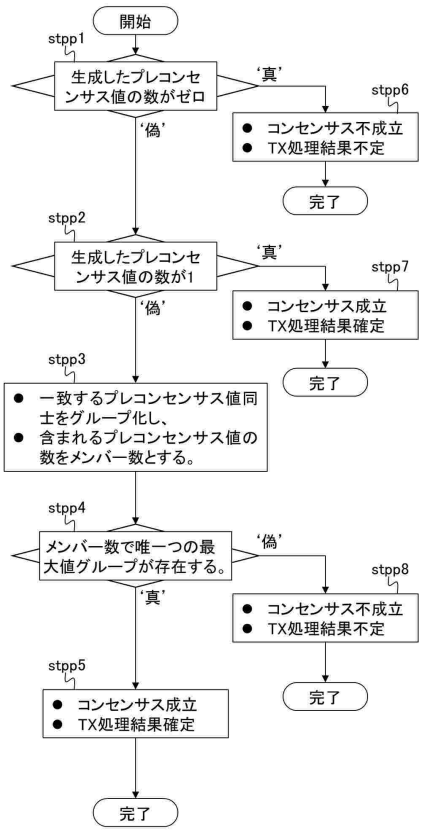
【図８】



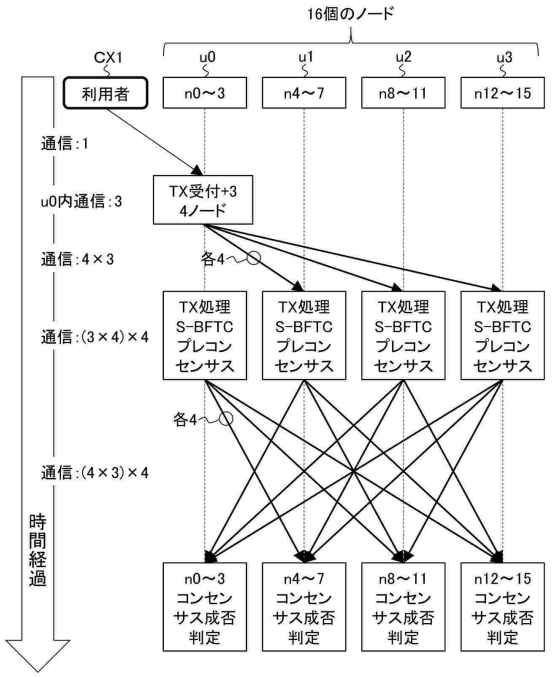
【図９】



【図１０】



【図１１】



【図１２】

(A)

$$CN2ALL = {}_{16}C_4 \times {}_{12}C_4 \times {}_{8}C_4 \times {}_{4}C_4 = 1{,}820 \times 495 \times 70 \times 1 = 63{,}063{,}000$$

基本単位u3のノードの選び方数
基本単位u2のノードの選び方数
基本単位u1のノードの選び方数
基本単位u0のノードの選び方数

(B)

基本単位u0およびu1, u2, u3に含まれる得る正常ノード数と
障害ノード数との組み合わせ一覧

基本単位 u3
基本単位 u2
基本単位 u1
基本単位 u0
正常ノード数
障害ノード数

COMB(4, 0)(4, 0)(4, 0)(4, 0)	COMB(3, 1)(4, 0)(4, 0)(4, 0)
COMB(2, 2)(4, 0)(4, 0)(4, 0)	COMB(1, 3)(4, 0)(4, 0)(4, 0)
COMB(0, 4)(4, 0)(4, 0)(4, 0)	COMB(4, 0)(3, 1)(4, 0)(4, 0)
COMB(4, 0)(2, 2)(4, 0)(4, 0)	COMB(4, 0)(1, 3)(4, 0)(4, 0)
・・・・・・・・・・・・・・・・・・・・・・・・・・・・	
COMB(0, 4)(0, 4)(3, 1)(0, 4)	COMB(0, 4)(0, 4)(2, 2)(0, 4)
COMB(0, 4)(0, 4)(1, 3)(0, 4)	COMB(0, 4)(0, 4)(0, 4)(4, 0)
COMB(0, 4)(0, 4)(0, 4)(3, 1)	COMB(0, 4)(0, 4)(0, 4)(2, 2)
COMB(0, 4)(0, 4)(0, 4)(1, 3)	COMB(0, 4)(0, 4)(0, 4)(0, 4)

625通り

(C)

各基本単位の正常ノード数と障害ノード数との組み合わせは
(4, 0) (3, 1) (2, 2) (1, 3) (0, 4)
の5通りであるから、
上記一覧の組み合わせの数は、
5×5×5×5＝ 625

【図１３】

(A)

正常ノード9個、障害ノード7個の場合

COMB(3,1)(1,3)(3,1)(2,2)の場合の数

$_9C_3 \times {}_7C_1$
$_6C_1 \times {}_6C_3$
$_5C_3 \times {}_3C_1$
$_2C_2 \times {}_2C_2$

$CN2 = {}_9C_3 \times {}_7C_1 \times {}_6C_1 \times {}_6C_3 \times {}_5C_3 \times {}_3C_1 \times {}_2C_2 \times {}_2C_2$

$= 84 \times 7 \times 6 \times 20 \times 10 \times 3 \times 1 \times 1 = 2{,}116{,}800 \Rightarrow 3.35664\%$

(B)

正常ノード9個、障害ノード7個の場合

COMB(3,1)(0,4)(4,0)(2,2)の場合の数

$_9C_3 \times {}_7C_1$
$_6C_0 \times {}_6C_4$
$_6C_4 \times {}_2C_0$
$_2C_2 \times {}_2C_2$

$CN2 = {}_9C_3 \times {}_7C_1 \times {}_6C_0 \times {}_6C_4 \times {}_6C_4 \times {}_2C_0 \times {}_2C_2 \times {}_2C_2$

$= 84 \times 7 \times 1 \times 15 \times 15 \times 1 \times 1 \times 1 = 132{,}300 \Rightarrow 0.20979\%$

(C)

正常ノード11個、障害ノード5個の場合

COMB(3,1)(0,4)(4,0)(2,2)の場合の数

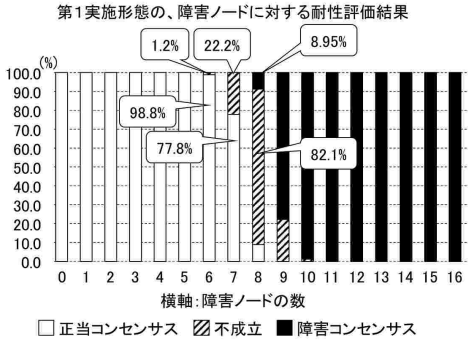
$_{11}C_3 \times {}_5C_1$
$_8C_0 \times {}_4C_4$
$_8C_4 \times {}_0C_0$
$_4C_2 \times {}_0C_2$

$CN2 = {}_{11}C_3 \times {}_5C_1 \times {}_8C_0 \times {}_4C_4 \times {}_8C_4 \times {}_0C_0 \times {}_4C_2 \times {}_0C_2$

$= 165 \times 5 \times 1 \times 1 \times 70 \times 1 \times 6 \times 0 = 0 \Rightarrow 0.0\%$

【図１４】

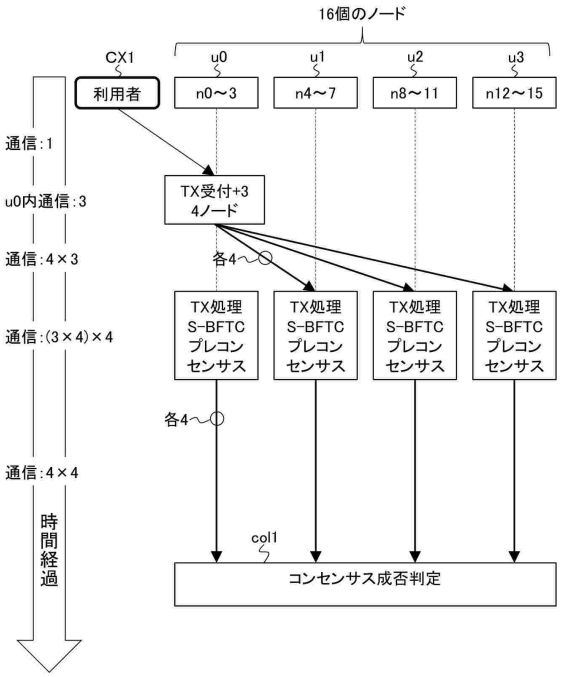
(A)



(B)

第1実施形態			障害ノード数	16個ノードのBFTC		
正常/成立	不成立	障害/成立		正常/成立	不成立	障害/成立
100.00%	0.00%	0.00%	0	100.00%	0.00%	0.00%
100.00%	0.00%	0.00%	1	100.00%	0.00%	0.00%
100.00%	0.00%	0.00%	2	100.00%	0.00%	0.00%
100.00%	0.00%	0.00%	3	100.00%	0.00%	0.00%
100.00%	0.00%	0.00%	4	100.00%	0.00%	0.00%
100.00%	0.00%	0.00%	5	100.00%	0.00%	0.00%
98.80%	1.20%	0.00%	6	0.00%	100.00%	0.00%
77.76%	22.24%	0.00%	7	0.00%	100.00%	0.00%
8.95%	82.10%	8.95%	8	0.00%	100.00%	0.00%
0.00%	22.24%	77.76%	9	0.00%	100.00%	0.00%
0.00%	1.20%	98.80%	10	0.00%	100.00%	0.00%
0.00%	0.00%	100.00%	11	0.00%	0.00%	100.00%
0.00%	0.00%	100.00%	12	0.00%	0.00%	100.00%
0.00%	0.00%	100.00%	13	0.00%	0.00%	100.00%
0.00%	0.00%	100.00%	14	0.00%	0.00%	100.00%
0.00%	0.00%	100.00%	15	0.00%	0.00%	100.00%
0.00%	0.00%	100.00%	16	0.00%	0.00%	100.00%

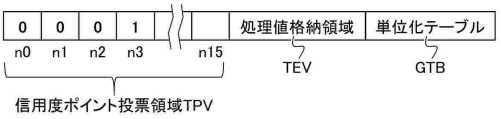
【図１５】



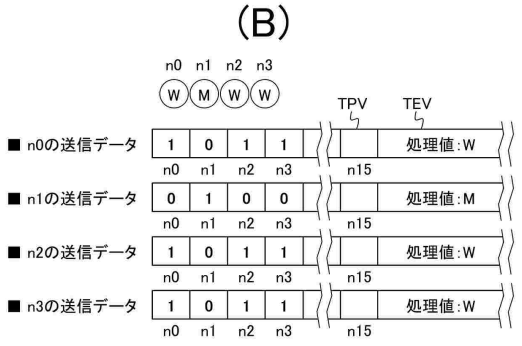
【図１６】

(A)

送信データ書式

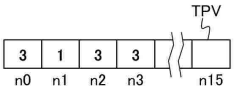


(B)

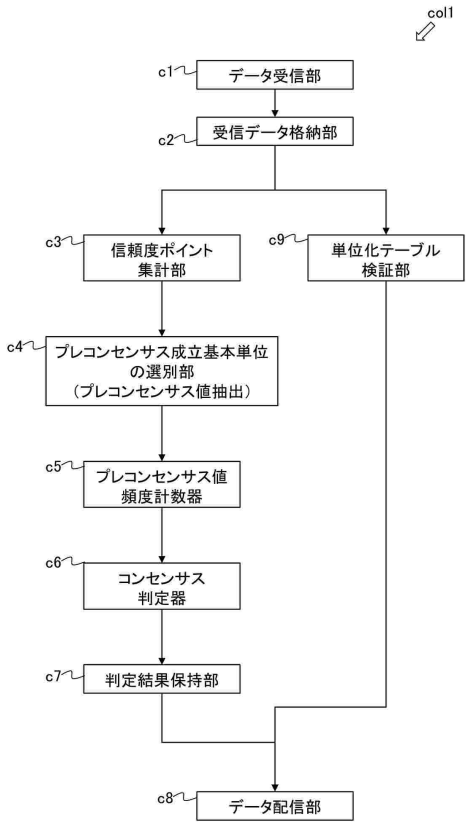


コンセンサス成否判定器col1における、信用度ポイント集計結果

(C)



【図１７】


col1
c1
データ受信部
c2
受信データ格納部
c3
信頼度ポイント
集計部
c9
単位化テーブル
検証部
c4
プレコンセンサス成立基本単位
の選別部
（プレコンセンサス値抽出）
c5
プレコンセンサス値
頻度計数器
c6
コンセンサス
判定器
c7
判定結果保持部
c8
データ配信部

フロントページの続き

(56)参考文献　　米国特許第１０８４８５４９（ＵＳ，Ｂ１）
中国特許出願公開第１０９１６５９４５（ＣＮ，Ａ）
中国特許出願公開第１１０９４１６７３（ＣＮ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１６／００－１６／９５８
Ｈ０４Ｌ　９／３２