

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2020-522778

(P2020-522778A)

(43) 公表日 令和2年7月30日(2020.7.30)

(51) Int.Cl.	F I	テーマコード (参考)
G06F 11/07 (2006.01)	G06F 11/07 193	5B042
G06F 15/00 (2006.01)	G06F 11/07 140A	5B089
G06F 16/182 (2019.01)	G06F 15/00 430	5B175
G06F 16/28 (2019.01)	G06F 16/182	
G06F 13/00 (2006.01)	G06F 16/28	
審査請求 有 予備審査請求 未請求 (全 32 頁) 最終頁に続く		

(21) 出願番号 特願2019-563220 (P2019-563220)
 (86) (22) 出願日 平成31年3月18日 (2019.3.18)
 (85) 翻訳文提出日 令和1年11月14日 (2019.11.14)
 (86) 国際出願番号 PCT/CN2019/078487
 (87) 国際公開番号 WO2019/101241
 (87) 国際公開日 令和1年5月31日 (2019.5.31)

(71) 出願人 510330264
 アリババ・グループ・ホールディング・リミテッド
 ALIBABA GROUP HOLDING LIMITED
 英国領、ケイマン諸島、グランド・ケイマン、ジョージ・タウン、ワン・キャピタル・プレイス、フォース・フロア、ピー・オー・ボックス 847
 (74) 代理人 100099759
 弁理士 青木 篤
 (74) 代理人 100123582
 弁理士 三橋 真二
 (74) 代理人 100114018
 弁理士 南山 知広

最終頁に続く

(54) 【発明の名称】 ビュー変更プロトコルを終了するためのシステムおよび方法

(57) 【要約】

ビュー変更を実行するための、コンピュータ記憶媒体上に符号化されたコンピュータ・プログラムを含む、方法、システム、および装置。これらの方法のうちの1つは、いくつか (N個) のノードによって維持されるブロックチェーン上で実施され、ビュー変更プロトコル中の、N個のノードのうちの第1のノードによって実行される。この方法は、N個のノードのうちの少なくともQ個の第2のノードからそれぞれ、少なくともQ個の第1のメッセージを取得することであって、各第1のメッセージは、(1) N個のノードの間で指定されるプライマリ・ノードを示す第2のノードに認識されている整合する現在のビューと、(2) 第2のノードに認識されている整合する現在の順序番号とを含み、現在の順序番号は、最新のトランザクションまたは最新のブロックに関連し、現在の順序番号は、第1のノードに認識されている第1の順序番号よりも大きい、取得することと、少なくともQ個の第1のメッセージを取得したこととを応答して、ビュー変更プロトコルを終了することを含む。

【選択図】 図1

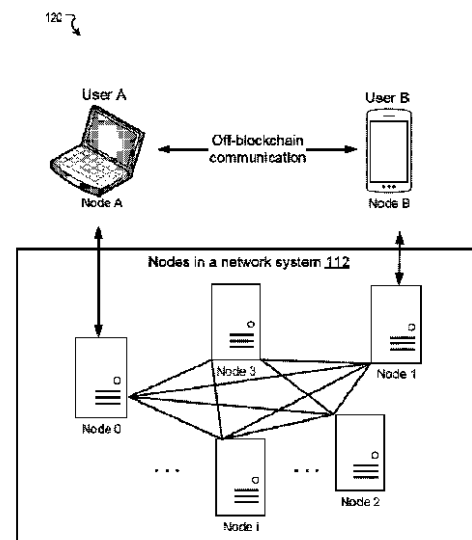


FIG. 1

【特許請求の範囲】

【請求項 1】

いくつか（N 個）のノードによって維持されるブロックチェーン上で実施されるコンピュータ実施ビュー変更方法であって、前記方法は、ビュー変更プロトコル中の、前記 N 個のノードのうちの第 1 のノードによって実行され、前記方法は、

前記 N 個のノードのうちの少なくとも Q 個の第 2 のノードからそれぞれ、少なくとも Q 個の第 1 のメッセージを取得することであって、各第 1 のメッセージは、（1）前記 N 個のノードの間で指定されるプライマリ・ノードを示す前記第 2 のノードに認識されている整合する現在のビューと、（2）前記第 2 のノードに認識されている整合する現在の順序番号とを含み、前記現在の順序番号は、前記第 2 のノードによってコミットされた最新のブロックまたは最新のトランザクションに関連し、前記現在の順序番号は、前記第 1 のノードに認識されている第 1 の順序番号よりも大きく、 Q （定足数）は $(N + F + 1) / 2$ を最も近い整数に切り上げた値であり、 F は $(N - 1) / 3$ を最も近い整数に切り捨てた値である、取得することと、

前記少なくとも Q 個の第 1 のメッセージを取得したことに応答して、前記ビュー変更プロトコルを終了することとを含む、方法。

【請求項 2】

前記少なくとも Q 個の第 1 のメッセージを取得することは、

前記少なくとも Q 個の第 2 のノードからそれぞれ、前記少なくとも Q 個の第 2 のノードが前記ブロックチェーンに追加する次のブロックに同意することを示す少なくとも Q 個のコミット・メッセージを取得することであって、前記 Q 個のコミット・メッセージは、前記 Q 個の第 1 のメッセージをそれぞれ含む、取得することを含む、請求項 1 に記載の方法。

【請求項 3】

前記少なくとも Q 個の第 1 のメッセージを取得することは、

前記少なくとも Q 個の第 2 のノードからそれぞれ、前記少なくとも Q 個の第 2 のノードが前記ブロックチェーンに追加する次のブロックに同意することを示す少なくとも Q 個のコミット・メッセージを取得することであって、前記 Q 個の第 1 のメッセージは、前記 Q 個のコミット・メッセージにそれぞれ付加される、取得することを含む、請求項 1 に記載の方法。

【請求項 4】

前記現在の順序番号は、前記第 2 のノードによって維持される前記ブロックチェーンの第 2 のコピーの高さを含み、

前記第 1 の順序番号は、前記第 1 のノードによって維持される前記ブロックチェーンの第 1 のコピーの高さを含む、

請求項 1～3 のいずれかに記載の方法。

【請求項 5】

前記現在の順序番号は、前記第 2 のノードによってコミットされた前記最新のトランザクションの順序番号を含み、

前記第 1 の順序番号は、前記第 1 のノードによってコミットされた最新のトランザクションの順序番号を含む、

請求項 1～3 のいずれかに記載の方法。

【請求項 6】

前記第 1 のメッセージは、両方とも前記第 2 のノードに認識されている前記現在のビューおよび前記現在の順序番号を保証するデジタル署名を含む、

請求項 1～5 のいずれかに記載の方法。

【請求項 7】

前記第 1 のメッセージは、前記最新のブロックまたは前記最新のトランザクションのダイジェストをさらに含む、

請求項 1～6 のいずれかに記載の方法。

【請求項 8】

前記ダイジェストは、前記最新のブロックまたは前記最新のトランザクションのハッシュ値を含む、

請求項 7 に記載の方法。

【請求項 9】

前記ダイジェストは、前記第 2 のノードには認識されているが、前記第 1 のノードには認識されていない前記最新のブロックのマークル・ルートを含む、

請求項 7 または 8 に記載の方法。

【請求項 10】

前記ビュー変更プロトコルを終了することは、

前記第 1 のノードによって維持される前記ブロックチェーンの第 1 のコピーを、前記第 2 のノードによって維持される前記ブロックチェーンの第 2 のコピーと同期させることと、

前記第 1 のノードに対して前記整合する現在のビューを使用することによって、前記ビュー変更プロトコルから退出して、通常動作プロトコルに入ることと

を含む、請求項 1～9 のいずれかに記載の方法。

【請求項 11】

前記少なくとも Q 個の第 2 のノードに認識されている前記現在の順序番号は $(n+1)$ であり、

前記第 1 のノードに認識されている前記第 1 の順序番号は n である、

請求項 1～10 のいずれかに記載の方法。

【請求項 12】

前記少なくとも Q 個の第 2 のノードの前記現在のビューは v であり、

前記第 1 のノードは、前記ビュー変更プロトコル中の場合、 v より大きい第 1 のビューを有する、

請求項 1～11 のいずれかに記載の方法。

【請求項 13】

前記 N 個のノードは、前記 N 個のノードのうちの 1 つが前記プライマリ・ノードとして機能し、その他の $(N-1)$ 個のノードがバックアップ・ノードとして機能する、実用的ビザンチン障害耐性 (PBFT) ネットワークを形成する、

請求項 1～12 のいずれかに記載の方法。

【請求項 14】

1 つまたは複数のプロセッサと、

前記 1 つまたは複数のプロセッサに結合され、請求項 1～13 のいずれかに記載の方法を実行するための、前記 1 つまたは複数のプロセッサによって実行可能な命令が記憶される、1 つまたは複数のコンピュータ可読メモリとを備える、ビュー変更システム。

【請求項 15】

請求項 1～13 のいずれかに記載の方法を実行するための複数のモジュールを備える、ビュー変更装置。

【発明の詳細な説明】

【技術分野】

【0001】

本出願は一般には、ビュー変更を実行するための方法およびデバイスに関し、より詳細には、実用的ビザンチン障害耐性 (PBFT: Practical Byzantine Fault Tolerance) システムにおいてビュー (View) の変更を終了するための方法およびデバイスに関する。

【背景技術】

【0002】

10

20

30

40

50

実用的ビザンチン障害耐性 (P B F T) は、ブロックチェーン・システムなどの分散システムにおいて実装することができる一種のコンセンサス・メカニズムである。P B F T コンセンサス・メカニズムによって、分散システムは、システムの特定のノードが故障する (たとえば、不十分なネットワーク接続が原因で、もしくは他の原因で障害が生じる) 可能性があろうと、他のピアに誤った情報を伝播する (たとえば、悪意を持って行動する) 可能性があろうと、安全性および生存性 (l i v e n e s s) を持って、十分なコンセンサスに到達することが可能になる。そのようなメカニズムの目的は、機能していないノードによる、システムの正しい機能への影響と、システム内の機能しているノード (たとえば、障害のない善意のノード) が到達するコンセンサスへの影響とを軽減することにより、壊滅的なシステム故障を防ぐことである。

10

【0003】

P B F T コンセンサス・メカニズムは、独立したノード故障と、特定の独立したノードによって伝播される改ざんされたメッセージとがあるという仮定を通じて、ビザンチン障害 (たとえば、機能していないノード) を許容する実用的ビザンチン・ステート・マシンの複製を提供することに焦点を当てている。この P B F T コンセンサス・メカニズムでは、たとえば、ブロックチェーン・システム内の全てのノードはある順序に順序付けられ、あるノードはプライマリ・ノード (別名、リーダーまたはマスター・ノード) となり、その他はバックアップ・ノード (別名、フォロワー・ノード) と呼ばれる。システム内の全てのノードは互いに通信し、目標は、全ての善意のノードがシステムの状態に関する合意 / コンセンサスに至ることである。

20

【0004】

たとえば、P B F T コンセンサス・メカニズムが機能するには、その前提は、ブロックチェーン・システム内の機能していないノードの量が、所与の脆弱性の窓において一斉にシステム内のノード全体の3分の1以上になってはならないというものである。この方法は、たかだかF個のノードが同時に機能していないノードである限り、生存性および安全性の両方を効果的に提供する。換言すれば、いくつかの実装形態では、P B F T コンセンサス・メカニズムが許容できる機能していないノードの数Fは、 $(N - 1) / 3$ を最も近い整数に切り捨てた値に等しく、ここでNはシステム内のノードの総数を表す。一部の实装形態では、P B F T コンセンサス・メカニズムを実装しているブロックチェーン・システムは、全部で少なくとも $3F + 1$ 個のノードが存在する場合に、最大F個のビザンチン障害に対処することができる。コンセンサス検証を実行するために、各ノードはプライマリ・ノードのリーダーシップの下で通常動作プロトコルを実行する。プライマリ・ノードが機能していないとあるノードが考えた場合、そのノードはビュー変更プロトコルに入っ

30

【0005】

現在の技術では、ノードは従来の手順に従って、すなわち、大多数のノードが同様にビュー変更プロトコルに入り、プライマリ・ノードが機能していないことに合意するまで待機して、ビュー変更プロトコルから退出する。従来のビュー変更プロトコルでは、この条件は、少なくとも $2F + 1$ 個のノードがビュー変更プロトコルに入り、それぞれビュー変更メッセージをマルチキャストする場合、少なくとも $2F + 1$ 個のビュー変更メッセージを取得した新たなプライマリ・ノードが新ビュー・メッセージをマルチキャストして、それらのノードが通常動作に戻るのを支援することである。しかしながら、場合によっては、ネットワーク通信の途絶により、ノードが、プライマリ・ノードが機能していないと誤解し、その他のノードがまだ通常動作中である間にビュー変更プロトコルに入る場合がある。結果として、そのノードはビュー変更プロトコルで立ち往生し、コンセンサス・プロセスから実質的に遮断される。立ち往生しているノードが通常動作に戻るまでの遅延は、いつ本当のプライマリ・ノードの機能停止または誤動作が発生するかによる場合があるので、予測不可能である。そのため、立ち往生しているノードの計算能力は、他のノードが

40

50

ビュー変更に参加するのを待っている間、無駄になる。したがって、ノードがビュー変更プロトコルから退出するのを支援することができる代替メカニズムを提供することが望ましい。

【発明の概要】

【0006】

本明細書の様々な実施形態は、ビュー変更を実行するためのシステム、方法、および非一時的コンピュータ可読媒体を含むが、これらに限定されない。

【0007】

一実施形態によれば、いくつか（ N 個）のノードによって維持されるブロックチェーン上で実施されるコンピュータ実施ビュー変更方法は、ビュー変更プロトコル中の、 N 個のノードのうちの第1のノードによって実行される。この方法は、 N 個のノードのうちの少なくとも Q 個の第2のノードからそれぞれ、少なくとも Q 個の第1のメッセージを取得することであって、各第1のメッセージは、（1） N 個のノードの間で指定されるプライマリ・ノードを示す第2のノードに認識されている整合する現在のビューと、（2）第2のノードに認識されている整合する現在の順序番号とを含み、現在の順序番号は、第2のノードによってコミットされた最新のブロックまたは最新のトランザクションに関連し、現在の順序番号は、第1のノードに認識されている第1の順序番号よりも大きく、 Q （定足数（ $quorum$ ））は $(N + F + 1) / 2$ を最も近い整数に切り上げた値であり、 F は $(N - 1) / 3$ を最も近い整数に切り捨てた値である、取得することと、少なくとも Q 個の第1のメッセージを取得したことに応答して、ビュー変更プロトコルを終了することとを含む。

【0008】

いくつかの実施形態では、少なくとも Q 個の第1のメッセージを取得することは、少なくとも Q 個の第2のノードからそれぞれ、少なくとも Q 個の第2のノードがブロックチェーンに追加する次のブロックに同意することを示す少なくとも Q 個のコミット・メッセージを取得することであって、 Q 個のコミット・メッセージは、 Q 個の第1のメッセージをそれぞれ含む、取得することを含む。

【0009】

他の実施形態では、少なくとも Q 個の第1のメッセージを取得することは、少なくとも Q 個の第2のノードからそれぞれ、少なくとも Q 個の第2のノードがブロックチェーンに追加する次のブロックに同意することを示す少なくとも Q 個のコミット・メッセージを取得することであって、 Q 個の第1のメッセージは、 Q 個のコミット・メッセージにそれぞれ付加される、取得することを含む。

【0010】

さらに他の実施形態では、現在の順序番号は、第2のノードによって維持されるブロックチェーンの第2のコピーの高さを含み、第1の順序番号は、第1のノードによって維持されるブロックチェーンの第1のコピーの高さを含む。

【0011】

さらに他の実施形態では、現在の順序番号は、第2のノードによってコミットされた最新のトランザクションの順序番号を含み、第1の順序番号は、第1のノードによってコミットされた最新のトランザクションの順序番号を含む。

【0012】

いくつかの実施形態では、第1のメッセージは、両方とも第2のノードに認識されている現在のビューおよび現在の順序番号を保証するデジタル署名を含む。

【0013】

他の実施形態では、第1のメッセージは、最新のブロックまたは最新のトランザクションのダイジェストをさらに含む。

【0014】

さらに他の実施形態では、ダイジェストは、最新のブロックまたは最新のトランザクションのハッシュ値を含む。

【0015】

さらに他の実施形態では、ダイジェストは、第2のノードには認識されているが、第1のノードには認識されていない最新のブロックのマークル・ルートを含む。

【0016】

いくつかの実施形態では、ビュー変更プロトコルを終了することは、第1のノードによって維持されるブロックチェーンの第1のコピーを、第2のノードによって維持されるブロックチェーンの第2のコピーと同期させることと、第1のノードに対して整合する現在のビューを使用することによって、ビュー変更プロトコルから退出して、通常動作プロトコルに入ることを含む。

【0017】

他の実施形態では、少なくともQ個の第2のノードに認識されている現在の順序番号は $(n+1)$ であり、第1のノードに認識されている第1の順序番号は n である。

【0018】

さらに他の実施形態では、少なくともQ個の第2のノードの現在のビューは v であり、第1のノードは、ビュー変更プロトコル中の場合、 v より大きい第1のビューを有する。

【0019】

さらに他の実施形態では、N個のノードは、N個のノードのうちの1つがプライマリ・ノードとして機能し、その他の $(N-1)$ 個のノードがバックアップ・ノードとして機能する、実用的ビザンチン障害耐性(PBFT)ネットワークを形成する。

【0020】

いくつかの実施形態では、ビュー変更システムは、1つまたは複数のプロセッサと、1つまたは複数のプロセッサに結合され、前述の実施形態のいずれか1つの方法を実行するための、1つまたは複数のプロセッサによって実行可能な命令が記憶される、1つまたは複数のコンピュータ可読メモリとを備える。

【0021】

他の実施形態では、ビュー変更装置は、前述の実施形態のいずれか1つの方法を実行するための複数のモジュールを備える。

【0022】

他の実施形態によれば、ビュー変更システムはブロックチェーンを維持するためのものであり、いくつか(N個)のノードはブロックチェーンを維持し、このシステムは、ビュー変更プロトコル中の、N個のノードのうちの第1のノードとして機能する。このシステムは、1つまたは複数のプロセッサと、1つまたは複数のプロセッサに結合され、このシステムに動作を実行させるための、1つまたは複数のプロセッサにより実行可能な命令によって構成される、1つまたは複数の非一時的コンピュータ可読メモリとを備え、これらの動作は、N個のノードのうちの少なくともQ個の第2のノードからそれぞれ、少なくともQ個の第1のメッセージを取得することであって、各第1のメッセージは、(1) N個のノードの間で指定されるプライマリ・ノードを示す第2のノードに認識されている整合する現在のビューと、(2) 第2のノードに認識されている整合する現在の順序番号とを含み、現在の順序番号は、第2のノードによってコミットされた最新のブロックまたは最新のトランザクションに関連し、現在の順序番号は、第1のノードに認識されている第1の順序番号よりも大きく、 Q (定足数)は $(N+F+1)/2$ を最も近い整数に切り上げた値であり、 F は $(N-1)/3$ を最も近い整数に切り捨てた値である、取得することと、少なくともQ個の第1のメッセージを取得したことに応答して、ビュー変更プロトコルを終了することを含む。

【0023】

さらに他の実施形態によれば、非一時的コンピュータ可読記憶媒体は、ブロックチェーンを維持するためのものであり、いくつか(N個)のノードはブロックチェーンを維持し、この記憶媒体は、ビュー変更プロトコル中の、N個のノードのうちの第1のノードに関連付けられる。この記憶媒体は、1つまたは複数のプロセッサに動作を実行させるための、1つまたは複数のプロセッサにより実行可能な命令によって構成され、これらの動作は

10

20

30

40

50

、N個のノードのうちの少なくともQ個の第2のノードからそれぞれ、少なくともQ個の第1のメッセージを取得することであって、各第1のメッセージは、(1) N個のノードの間で指定されるプライマリ・ノードを示す第2のノードに認識されている整合する現在のビューと、(2) 第2のノードに認識されている整合する現在の順序番号とを含み、現在の順序番号は、第2のノードによってコミットされた最新のブロックまたは最新のトランザクションに関連し、現在の順序番号は、第1のノードに認識されている第1の順序番号よりも大きく、 Q (定足数) は $(N + F + 1) / 2$ を最も近い整数に切り上げた値であり、 F は $(N - 1) / 3$ を最も近い整数に切り捨てた値である、取得することと、少なくともQ個の第1のメッセージを取得したことに応答して、ビュー変更プロトコルを終了することを含む。

10

【0024】

さらに他の実施形態によれば、ビュー変更装置はブロックチェーンを維持するためのものであり、いくつか(N個)のノードはブロックチェーンを維持し、この装置は、ビュー変更プロトコル中の、N個のノードのうちの第1のノードとして機能する。この装置は、N個のノードのうちの少なくともQ個の第2のノードからそれぞれ、少なくともQ個の第1のメッセージを取得するための取得モジュールであって、各第1のメッセージは、(1) N個のノードの間で指定されるプライマリ・ノードを示す第2のノードに認識されている整合する現在のビューと、(2) 第2のノードに認識されている整合する現在の順序番号とを含み、現在の順序番号は、第2のノードによってコミットされた最新のブロックまたは最新のトランザクションに関連し、現在の順序番号は、第1のノードに認識されている第1の順序番号よりも大きく、 Q (定足数) は $(N + F + 1) / 2$ を最も近い整数に切り上げた値であり、 F は $(N - 1) / 3$ を最も近い整数に切り捨てた値である、取得モジュールと、少なくともQ個の第1のメッセージを取得したことに応答して、ビュー変更プロトコルを終了するための終了モジュールとを備える。

20

【0025】

本明細書で開示した実施形態は、1つまたは複数の技術的效果を有する。いくつかの実施形態では、これらの方法およびシステムは、ビュー変更プロトコルに入ったPBF Tコンセンサス・システムのノード(たとえば、第1のノード)が、効率的にビュー変更プロトコルから退出し、通常動作プロトコルを再開できるようにすることができる。他の実施形態では、通常動作プロトコル中の第2のノードは、コミット・メッセージをマルチキャストするときに、第1のメッセージをコミット・メッセージに追加または付加することができ、第1のメッセージは、第2のノードに認識されている現在のビューおよび現在の順序番号を含む。現在のビューは、プライマリ・ノードの第2のノードのビューを示し、現在の順序番号は、第2のノードがコミットした最新のトランザクションを示し、または第2のノードによって維持されるブロックチェーンの最新のブロックに関連するブロックチェーンの高さ(ブロックの高さとも呼ばれる)を示す。さらに他の実施形態では、ビュー変更プロトコルで立ち往生している第1のノードは、第1のメッセージから現在のビューおよび現在の順序番号を取得することができる。定足数 Q の整合する第1のメッセージを受信すると、第1のノードは、それらを自身のビューおよび順序番号と比較して、ノードの大多数がまだ通常動作中であるか否かを判定することができる。他のノードの大多数がまだ通常動作中である場合、第2のノードは、ビュー変更プロトコルを終了し、通常動作プロトコルを再開することができる。さらに他の実施形態では、第1のメッセージ内の順序番号によって示されるように、大多数のノードが、コンセンサス検証順序における次のトランザクションまたは次のブロックに同意しており、次のトランザクションまたは次のブロックは、まだ第1のノードに認識されていない場合がある。大多数のノードがビュー変更に入らなかったと気付くことにより、第1のノードはスムーズにビュー変更プロトコルを終了することができる。いくつかの実施形態では、大多数のノードが同様にビュー変更に入り、新たなビューに同意してビュー変更プロトコルを終了しなくても、第1のノードはビュー変更を終了することができる。このようにして、通常動作中のノードの数、およびそれらの計算能力の提供を最適化することができる。

30

40

50

【0026】

本明細書で開示したシステム、方法、および非一時的コンピュータ可読媒体のこれらおよび他の特徴のみならず、関連する構造要素の動作方法および機能、ならびに部品の組み合わせおよび製造の経済性は、添付図面を参照して以下の説明および添付の特許請求の範囲を考察するとより明らかになり、添付図面は全て本明細書の一部を形成し、同様の参照番号は様々な図における対応する部分を示す。しかしながら、図面は例示および説明のみを目的とするものであり、限定を意図したものではないことは明確に理解されたい。

【図面の簡単な説明】

【0027】

【図1】 様々な実施形態によるネットワークを示す図である。

10

【図2A】 P B F Tの通常動作プロトコルを示す図である。

【図2B】 1つのレプリカが機能していない場合のP B F Tの通常動作プロトコルを示す図である。

【図2C】 P B F Tの通常動作プロトコルおよびビュー変更プロトコルを示す図である。

【図3A】 通常動作プロトコルとビュー変更プロトコルとの間での経路の切り替えのフローチャートである。

【図3B】 様々な実施形態による、通常動作プロトコルとビュー変更プロトコルとの間での経路の切り替えのフローチャートである。

【図4】 様々な実施形態によるビュー変更退出ステップのフローチャートである。

【図5A】 様々な実施形態によるビュー変更方法のフローチャートである。

20

【図5B】 様々な実施形態によるビュー変更方法のフローチャートである。

【図6】 様々な実施形態によるビュー変更システムのブロック図である。

【図7】 本明細書に記載の実施形態のいずれかを実装することができるコンピュータ・システムのブロック図である。

【発明を実施するための形態】

【0028】

本明細書で開示した実施形態は、限定はしないが、P B F Tシステムにおいて実装することができるビュー変更システム、方法、および非一時的コンピュータ可読媒体を含む。様々な実施形態において、ビュー変更プロトコルから退出し、通常動作プロトコルを再開する経路が提供される。ビュー変更に入ったノードは、少なくともQ個のノードがビュー変更に入る必要がある従来のビュー変更プロトコルを経由せずに、通常動作に戻るることができる。Q（定足数）は $(N + F + 1) / 2$ を最も近い整数に切り上げた値であり、Nはノードの総数を表し、4以上の整数であり、Fは $(N - 1) / 3$ を最も近い整数に切り捨てた値である。P B F Tと同様に、開示したシステム、方法、および非一時的コンピュータ可読媒体は、他のコンセンサス・プロトコル、たとえば、Secure Ring、Byzantine Paxos、Q/U、HQ、Zyzzyva、ABSTRACTs、RBFT、Adapt、Tangaroa、CheapBFT、MinBFT、FastBFTなどに適用することができる。P B F Tの様々な態様については、M. Castro、B. Liskov、「Practical Byzantine Fault Tolerance」、Proceedings of the Third Symposium on Operating Systems Design and Implementation、(1999年2月)を参照することができ、その全体が本明細書に引用により組み込まれている。

30

40

【0029】

図1に、様々な実施形態によるネットワーク120を示す。以下に提示する構成要素は、例示的なものとする。図示のように、ネットワーク120は、ネットワーク・システム112を含むことができる。ネットワーク・システム112は、サーバ、コンピュータ、携帯電話などの1つまたは複数のコンピューティング・デバイスに実装された1つまたは複数のノード（たとえば、ノード0、ノード1、ノード2、ノード3、ノード4、ノードiなど）を含むことができる。ネットワーク・システム112には、ネットワーク120

50

の他のデバイスまたはさらなるシステムにアクセスするための適切なソフトウェア（たとえば、コンセンサス・プログラム）および／またはハードウェア（たとえば、有線、無線接続）をインストールすることができる。ノードは、1つまたは複数のプロセッサと、1つまたは複数のプロセッサに結合された1つまたは複数のメモリとを含むことができる。メモリは、非一時的かつコンピュータ可読にすることができ、1つまたは複数のプロセッサに本明細書に記載の動作を実行させるための、1つまたは複数のプロセッサによって実行可能な命令によって構成することができる。この図では、ノードは単一の構成要素として示しているが、これらのノードが単一のデバイスまたは互いに結合された複数のデバイスとして実装できることは理解されよう。一般に、ノードは互いに通信し、ネットワーク・システム 112 の外部の他のデバイスと通信することができてもよい。たとえば、1つまたは複数の有線または無線ネットワーク（たとえば、インターネット）を介して、データを通信することができる。

10

【0030】

様々な実施形態において、ネットワーク・システム 112 は、様々なブロックチェーン・ノードを含むブロックチェーン・ネットワーク・システムとして実装することができる。図示のように、ブロックチェーン・ネットワーク・システムは、複数のブロックチェーン・ノード（たとえば、ノード 0、ノード 1、ノード 2、ノード 3、ノード 4、ノード i など）を含むことができる。ブロックチェーン・ノードは、あるブロックチェーン・ノードが他のブロックチェーン・ノードと通信するネットワーク（たとえば、ピア・ツー・ピア・ネットワーク）を形成することができる。図示したブロックチェーン・ノードの順序および数は、単なる例であって、説明を簡単にするためのものである。ブロックチェーン・ノードは、サーバ、コンピュータなどに実装することができる。各ブロックチェーン・ノードは、TCP/IP などの様々なタイプの通信方法によって互いに結合された1つまたは複数の物理的なハードウェア・デバイスまたは仮想デバイスに対応することができる。分類に応じて、ブロックチェーン・ノードは、フル・ノード、Get h ノード、コンセンサス・ノードなどを含むことができる。

20

【0031】

様々な実施形態において、ブロックチェーン・ネットワーク・システムは、ノード A およびノード B（たとえば、軽量ノード）などの他のシステムおよびデバイスとインタラクト（interact）することができる。インタラクションは、たとえば、要求を受信し、要求の実行結果を返すなどの目的の、データの送受信を含むことができる。一例では、ユーザ A はブロックチェーン・ネットワークを介してユーザ B と取引したい場合がある。トランザクションは、ユーザ A の口座の一部の資産をユーザ B の口座に送金することを含む場合がある。ユーザ A およびユーザ B は、トランザクションのために適切なブロックチェーン・ソフトウェア（たとえば、暗号通貨ウォレットなど）がインストールされたノード A およびノード B のそれぞれのデバイスを使用することができる。ノード A はノード 0 との通信を通じてブロックチェーンにアクセスすることができ、ノード B はノード 1 との通信を通じてブロックチェーンにアクセスすることができる。たとえば、ノード A はノード 0 を介してブロックチェーンにトランザクション要求を提出することができ、ノード B はノード 1 を介してブロックチェーンにスマート・コントラクト実行要求を提出することができる。ブロックチェーンから外れて、ノード A およびノード B は、他の通信チャネル（たとえば、ノード 0 および 1 を経由しない通常のインターネット通信）を有することができる。

30

40

【0032】

ブロックチェーン・ノードはそれぞれ、メモリを備えるか、またはメモリに結合することができる。いくつかの実施形態では、メモリは、プール・データベースを記憶することができる。プール・データベースは、分散方式で複数のブロックチェーン・ノードがアクセスできるようにすることができる。たとえば、プール・データベースは、ブロックチェーン・ノードのメモリにそれぞれ記憶することができる。プール・データベースは、ユーザによって操作されるノード A および B などの 1つまたは複数のユーザデバイスによって

50

提出される複数のトランザクションを記憶することができる。

【0033】

ブロックチェーン・ノードは、コンセンサスを通じて、ブロックチェーンと呼ばれる分散型台帳にトランザクションを記録するネットワーク（たとえば、P2Pネットワーク）を形成する。P2Pネットワークの参加者はノードと呼ばれる場合があり、ノードはブロックチェーンを維持するものである。ブロックチェーンP2Pネットワークでは、各ノードはコンセンサス検証に参加し、ブロックチェーンの完全な台帳のコピーを記憶する。全てのノードは、ブロックチェーン・コンセンサス方法によりトランザクションのバッチを確認することによって、全てのノードが整合する確認結果を有し、ひいてはブロックチェーンの整合するコピーを有するようにする。

10

【0034】

ブロックチェーン・コンセンサス方法の1つは、実用的ビザンチン障害耐性（PBFT）である。ビザンチン障害耐性は、ビザンチン将軍問題が起源である。P2Pネットワーク・システムでは、そのような機能していないノードの数が特定の限度内である限り、システムは適切に機能し続けることができる。そのようなシステムは、ビザンチン障害耐性システムと呼ばれる。PBFTは、ビザンチン障害耐性ネットワーク機能の最適化の一例である。PBFTは、サーバをコピーし、クライアントのインタラクションをサーバのコピーと同期させることにより、ネットワークにビザンチン・ステート・マシンを提供する。

【0035】

PBFT動作の中心となるのは、ブロックチェーンに記録された情報の整合するグローバルなビューの維持であり、これにより、分散方式でユーザが互いにインタラクトできるようにするためのバックボーンが形成される。PBFTコンセンサス・モデルのセキュリティは、ブロックチェーン・プラットフォームにとって重要である。コンセンサス・モデルの2つの主要な特性は：1）安全性または整合性：全ての善意のノードが同じ有効な出力を生成すること、および、2）生存性：コンセンサスを得た全ての善意のノードは、中間段階で止まることなく最終的に値を生成すること、である。安全で堅牢なPBFTコンセンサス・プロトコルは、ネットワーク・ノードの故障、ネットワークの分割、メッセージ遅延、順不同のメッセージ配信、メッセージ破損などを含む多種多様なビザンチン行動を許容し、システム内の機能していないノードの数が限られている限り、ノード間でコンセンサスに到達する必要がある。その目的で、PBFTモデルは、2つの相互に排他的なプロトコル：通常動作／整合性プロトコルおよびビュー変更プロトコルのいずれか一方の下で動作し、これらは以下でさらに説明する。本明細書では、機能していないということは、障害があるおよび／または悪意があることを意味し、機能しているということは、障害がなく善意であることを意味する。可能性のある障害または悪意がある行為は、メッセージの配信の失敗、メッセージの配信の遅延、順不同のメッセージ配信、ビザンチン障害（プロトコルに違反する恣意的なメッセージを様々なノードに配信する）などを含むことができる。

20

30

【0036】

いくつかの実施形態では、実用的ビザンチン障害耐性（PBFT）システムはN個のノードを含むことができ、N個のノードのうちの1つはプライマリ・ノードとして機能し、N個のノードのうちのその他はバックアップ・ノードとして機能する。プライマリ・ノードの指定は特定のノードに固定されなくてもよく、その理由は、ビュー変更プロトコルを通じて他のノードが新たなプライマリ・ノードになるように選出することができるためである。たとえば、プライマリ・ノードは剰余演算によって選出することができ、最小のシリアル番号（ビュー番号の剰余）を有する機能しているノードが新たなプライマリ・ノードになる。現在のビューと、ノードの総数Nとによって、プライマリ・ノードid = $(view + 1) \bmod N$ を決定することができる。PBFTでは、新たなプライマリ・ノードが選出されるたびにビューが変更される。たとえば、ビュー変更のたびに、ビューはゼロから単調に増加する。すなわち、プライマリ・ノードの変更に伴い、ビューを変更す

40

50

ることができる。

【0037】

いくつかの実施形態では、プライマリ・ノードはビューVで機能しており、通常動作プロトコルが実行される。通常動作では、プライマリ・ノードおよび／またはバックアップ・ノードは、1つまたは複数のクライアントから未検証のトランザクションに関連する要求を受信する場合がある。たとえば、クライアントとしてのノードAは、プライマリ・ノードおよび／またはバックアップ・ノードに要求を送信する場合がある。要求は、未検証のトランザクション（たとえば、ブロックチェーンの新たなブロックに追加されるトランザクション）を含むことができる。未検証のトランザクションは、たとえば、ブロックチェーン・ベースの金融取引、スマート・コントラクト展開または実行トランザクションなどを含むことができる。プライマリ・ノードおよびバックアップ・ノードは、トランザクションの何らかの予備検証を実行してもよく、しなくてもよい。要求を受信したバックアップ・ノードは、受信した要求をプライマリ・ノードに転送することができる。プライマリ・ノードにおけるトランザクションが特定のレベルに達するかまたは他の方法でトリガー条件を満たす場合、プライマリ・ノードは1ラウンドのコンセンサス検証を開始し、未検証のトランザクションの検証結果を提案することができる。バックアップ・ノードはコンセンサスに対処し、コンセンサスに到達するための提案を確認することができる。ノードの要件は、それらが決定性であって、同じ状態で開始することである。最終的な結果は、全ての善意のノードがレコードの順序に関するコンセンサスに至り、それを受諾または拒否することである。コンセンサス検証されると、トランザクションは、ブロックチェーンの新たなブロック内にバックされ、ノードによって維持されるローカルのブロックチェーンのコピーに追加することができる。また、要求を元々送信したクライアント（たとえば、ノードA）に通知される。

【0038】

安全性を持続するために、主なPBF T方法は、通常動作プロトコルに関する3つのフェーズ：事前準備、準備、およびコミット・フェーズを含む。図2Aから図2Cを参照すると、PBF Tシステムの一例は、4つのレプリカ（レプリカとはノードの別名である）：レプリカ0、レプリカ1、レプリカ2、およびレプリカ3を含む。0～3の番号は、新たなプライマリ・ノードを決定するために使用できるレプリカのシリアル番号である。レプリカ0はプライマリ・ノード0に対応することができ、レプリカ1、2、および3はバックアップ・ノード1、2、および3に対応することができる。レプリカは、たとえば、上記のネットワーク・システム112の様々なブロックチェーン・ノードに実装することができる。機能していないノードが存在しない場合の通常動作プロトコルを図2Aに示し、レプリカ3が機能していないノードである場合の他の通常動作プロトコルを図2Bに示す。どちらの状況でも、通常動作プロトコルは、要求フェーズ、事前準備フェーズ、準備フェーズ、コミット・フェーズ、および返答フェーズに分けることができる。

【0039】

図2Aおよび図2Bを参照すると、通常動作は、クライアントが要求（メッセージ）をプライマリ・ノード（レプリカ0）に提出したときに、要求フェーズにおいて開始し、プライマリ・ノードはその要求の主唱（advocating）を担当するものである。要求は、クライアント、要求動作（たとえば、コンセンサス検証されるトランザクション要求）、および要求タイムスタンプの情報を含むことができる。クライアント（クライアント・ノードとも呼ばれる）は、たとえば、上記のノードAに実装することができる。ノードAは、軽量ノード（たとえば、携帯電話に実装されたもの）とすることができる。それに加えてまたはその代わりに、クライアントは要求をバックアップ・ノードに送信することができ、バックアップ・ノードは事前準備フェーズの前に要求をプライマリ・ノードに転送する。プライマリ・ノードまたはバックアップ・ノードのいずれが要求を受信するかに関係なく、対応するノードは受信した要求をネットワーク内の他のノードにマルチキャストすることができる。このようにして、プライマリ・ノードが、クライアントによってコンセンサス・ネットワークに提出された保留中の要求を最終的に何らかの方法で取得す

ることができる。

【0040】

したがって、プライマリ・ノードはリーダーのように機能し、バックアップ・ノードをリードして、要求に関連するトランザクションを検証する。プライマリ・ノードは、そのビュー内での要求の実行の順序付けを担当する。事前準備フェーズにおいて、プライマリ・ノードは取得した要求を検証し、各要求に順序番号を提案することができる。このようにして、各要求に増加する順序番号を割り当てて、並べることができる。加えて、事前準備メッセージは、ブロックの高さを含むことができる。ブロックの高さは、ブロックチェーンの現在の高さに基づくことができる。たとえば、ブロックチェーンが現在1000個のブロックを有する場合、ブロックの高さは1000とすることができ、これは1000個のブロックがブロックチェーンに既に存在していることを示し、または1001とすることができ、これは要求に関連するトランザクションが、他のノードによってまだ検証されていないブロックチェーンの1001番目のブロック内にバックされるように提案されることを示す。プライマリ・ノードは、要求を順序番号および／またはブロックの高さと共に転送することができる。たとえば、要求を取得した後、プライマリ・ノードは、順序番号を割り当てることにより、対応するトランザクションを実行する順序に要求を配列し、リストに記憶することができる。プライマリ・ノードは、PBF Tネットワーク・システム内の全てのバックアップ・ノード（レプリカ1からレプリカ3）に事前準備メッセージを送信することができる。図2Aに示すように、プライマリ・ノードは、リストを事前準備メッセージ内で、またはそれと共にバックアップ・ノードにマルチキャストすることができる。図2Bに示すように、バックアップ・ノード（レプリカ3）が機能しておらず、プライマリ・ノードがそれに気付いていない場合であっても、プライマリ・ノードはなお事前準備メッセージを送信することができる。各バックアップ・ノードは事前準備メッセージを、それが有効である限り受諾する。事前準備メッセージは、ビュー番号、順序番号、署名、ダイジェスト（d）、その他のメタ・データなどを含むことができ、これによりメッセージの有効性を判定することが可能になる。

【0041】

準備フェーズにおいて、バックアップ・ノードは、事前準備メッセージを受諾した場合、それに続いて、プライマリ・ノードを含むPBF Tネットワーク・システム内の他のノードに準備メッセージをマルチキャストすることができる。準備メッセージをマルチキャストすることは、送信者ノードがその順序に同意することを示す。各準備メッセージは、有効である限り受信ノードによって受諾される。準備メッセージの有効性も同様に、ビュー番号、順序番号、署名、ダイジェスト（d）、その他のメタ・データなどに基づいて判定することができる。ノードは、プライマリ・ノードからオリジナルの要求を受信し、事前準備を行い（たとえば、事前準備メッセージをマルチキャストする）、事前準備メッセージに合致する少なくとも（ $Q-1$ ）個の別個の有効かつ整合する準備メッセージを取得した場合に、準備が整う。（ $Q-1$ ）個の準備メッセージは、マルチキャストした準備メッセージを含むことができる。 Q （定足数）は $(N+F+1)/2$ を最も近い整数に切り上げた値であり、 N はノードの総数を表し、4以上の整数であり、 F は $(N-1)/3$ を最も近い整数に切り捨てた値である。 Q 個のノードのPBF Tネットワーク・システムは、最大 F 個のビザンチン障害を許容することができる。いくつかの実施形態では、 N が少なくとも $(3F+1)$ である場合、 Q は $(2F+1)$ である。ここでは、 Q 個ではなく（ $Q-1$ ）個の準備メッセージが必要であり、その理由は、（プライマリ・ノード自体は準備メッセージを送信しなくてもよいが）事前準備メッセージをプライマリ・ノードの準備メッセージの同等物として扱うことができるためである。事前準備メッセージをもう1つの準備メッセージとしてカウントする場合、全てのノードのうちの少なくとも Q 個が事前準備メッセージを受諾したことを示す少なくとも Q 個の別個の有効な準備メッセージが存在することになり、そのうち最大 F 個の機能していないノードを許容することができる。このように、事前準備から準備までのフェーズによって、要求がビュー v において実行される場合に、その順序番号で実行されることに、少なくとも $(Q-F)$ 個の機能している

10

20

30

40

50

ノード（Q個の準備できたノードから最大F個の機能していないノードを除外したもの）が同意することが保証される。準備フェーズによって、ビュー内の各要求の障害耐性のある整合する順序付けが保証される。

【0042】

いくつかの実施形態では、バックアップ・ノードは、事前準備メッセージおよび（Q-1）個の準備メッセージを受信した後、順序を検証し、検証結果を、プライマリ・ノードによって事前準備メッセージ内に書き込まれた提案された検証結果と比較することができる。順序を検証するにはいくつかの方法があるであろう。たとえば、提案された検証結果は、ダイジェスト（d）に書き込まれた提案されたマークル・パトリシア・トライ（Merkle Patricia Trie）のルートを含むことができる。バックアップ・ノードは、要求に関連するトランザクションを順序に従って配列し、マークル・パトリシア・トライのルートを計算して、マークル・パトリシア・トライのルートと比較することができる。この計算は、ブロックチェーン内の既存ブロックのノード・ハッシュなどの特定の既存情報を必要とすることもできる。この比較により、バックアップ・ノードによって計算されるダイジェスト（D（m））が生成される。ダイジェスト（D（m））がダイジェスト（d）と整合する場合、検証は成功する。検証されると、バックアップ・ノードは、要求の順序付け（たとえば、要求に関連するトランザクションをブロックチェーンの新たなブロック内にバックする順序）に同意することができる。同様に、バックアップ・ノードは、受信したコミット・メッセージ（コミット・フェーズに関して後述する）が同じダイジェストD（m）を含むか否かを検証して、他のノードも要求の順序付けに同意するか否かを判定することができる。準備できたノードがQ個のコミット・メッセージを取得しており、より低い順序番号を有する要求が全て実行済みである場合、そのノードは要求を実行することができる。

【0043】

いくつかの実施形態では、事前準備メッセージは、新たなブロックのダイジェスト（d）、または要求の実行に他の方法に関連する情報（たとえば、要求に関連するトランザクション）を含むことができる。ダイジェスト（d）（たとえば、ハッシュ値）は、トランザクションなどのデータにハッシュ・アルゴリズムを適用した数値結果とすることができる。バックアップ・ノードは、トランザクションを実行してダイジェスト（d）を確認することができる。複数の要求の場合、バックアップ・ノードは、順序（すなわち、要求の順序番号）に従って要求を実行して、ダイジェストD（m）を取得することができる。D（m）およびdが整合する場合、バックアップ・ノードは、バックアップ・ノードがプライマリ・ノードの検証結果に同意することを示すコミット・メッセージ（コミット・フェーズに関して後述する）をマルチキャストする。いくつかの実施形態では、コミット・メッセージは、コミット・メッセージをマルチキャストしたバックアップ・ノードが事前準備メッセージに同意し、別個のノードから（Q-1）個以上の有効かつ整合する準備メッセージを取得したことを示す。特定の順序番号の保留中の要求に関して、準備できたノードがQ個のコミット・メッセージを取得しており、より低い順序番号を有する要求が全て実行済みである場合、そのノードは要求を実行することができる。

【0044】

コミット・フェーズでは、ノードが準備できている場合、コミット・メッセージを他のノードにマルチキャストすることができる。ノードは、他のノードからコミット・メッセージを受信することができる。各ノードはコミット・メッセージを有効である限り受諾する。コミット・メッセージは、ビュー番号、順序番号、署名、ダイジェスト、その他のメタ・データなどを含むことができ、これによりメッセージの有効性を判定することが可能になる。ノードが少なくともQ個の別個の有効かつ整合するコミット・メッセージを取得した場合、これは、定足数のノードがコミットしており（すなわち、少なくとも（Q-F）個の善意のノードが準備できている）、コンセンサスに到達したことを示す。少なくともQ個の有効なコミット・メッセージは、マルチキャストしたコミット・メッセージを含むことができる。したがって、準備からコミットまでのフェーズによって、要求が最終的

にビューvにおいてその順序番号で実行されることに、少なくとも $(Q - F)$ 個の機能しているノード(Q 個のコミット・メッセージから最大 F 個の機能していないノードを除外したもの)が同意することが保証される。ノードは異なるビューでコミットする場合があるので(たとえば、一部のノードが既に新たなビューに入っており、他の一部のノードが前のビューのままである場合)、受信されたコミット・メッセージは、異なるビューで実行されたコミットに対応する場合がある。機能しているノードが各要求の順序番号に同意するので、コミット・フェーズによって、ビュー全体にわたる各要求の障害耐性のある整合する順序付けが保証される。

【0045】

いくつかの実施形態では、ノードが少なくとも Q 個の別個の有効かつ整合するコミット・メッセージを取得した場合、そのノードは対応する要求を実行することができる。たとえば、 Q 個のコミット・メッセージが取得されると、これは新たなブロックがコンセンサス検証されることを意味する。したがって、ノードは、ローカルに保持しているブロックチェーンのコピー内に新たなブロックをバックすることができる。そうでなければ、バックアップ・ノードは、ビュー変更プロトコルを直接トリガーすることができる。

【0046】

返答フェーズでは、要求を実行した後、ノードは返答をクライアントに直接送信する。ブロックチェーン内にバックされたトランザクションについて、返答はブロックチェーン内のトランザクションのアドレスを含むことができる。最大 F 個の障害が許容されているので、クライアントは、異なるノードからの有効な署名と、同じ要求タイムスタンプおよび同じ実行結果を有する $(Q - F)$ 個の返答を待機した後、結果を受諾する。図2Aおよび図2Bに示すPBFTネットワーク・システムでは、合計4つのノードがあるので、最大で1つ($N = 4$ 、 $Q = 3$ 、および $F = 1$)の機能していないノードを許容することができる。したがって、図2Bにおいて、レプリカ3が機能していなくても、なおもコンセンサスに到達することができる。

【0047】

生存性を持続するために、プライマリ・ノードが要求をマルチキャストせずに特定の時間が経過した場合、ビュー変更プロトコルにおいてプライマリ・ノードを置き換えることができる。たとえば、バックアップ・ノードはタイマーを保持することができる。バックアップ・ノードは、要求を受信し、タイマーがまだ動作していないときにタイマーを開始する。バックアップ・ノードは、要求を実行するために待機しなくなった(すなわち、要求が実行された)ときにタイマーを停止するが、その時点で1つまたは複数の他の要求を実行するために待機している場合は、タイマーを再開する。タイマーが時間切れになった場合、バックアップ・ノードは、プライマリ・ノードが機能していないと判定することができる。したがって、バックアップ・ノードは、ビュー変更メッセージを他のノードにマルチキャストすることができる。他の例では、バックアップ・ノードは、プライマリ・ノードが機能していないと判定することができる。したがって、バックアップ・ノードは、ビュー変更メッセージをマルチキャストすることができる。他の例では、クライアントはタイマーを使用して、クライアントがプライマリ・ノードに要求を送信してから応答を受信することなく時間が経過しすぎているかを判定することができる。このタイマーが時間切れになった場合、クライアントはその要求を全てのノードに送信する。ノードが既に要求を認識している場合、再ブロードキャストは無視される。ノードが要求を認識していない場合、タイマーを開始する。ノードのタイマーがタイムアウトすると、ノードは、プライマリ・ノードが機能していないという疑いに基づいて、ビュー変更メッセージを他のバックアップ・ノードにマルチキャストすることにより、ビュー変更処理を開始する。ビュー変更メッセージは、(前の通常動作中の自身の準備メッセージを含むアーカイブ・メッセージの形式で)システム状態を含み、それによって他のノードは送信者ノードが故障していないことを知る。

【0048】

圧倒的多数の善意のノードは、プライマリ・ノードが機能していないか否かを判定し、

10

20

30

40

50

それを削除して、順番が次のプライマリ・ノードを代わりにすることができる。ビュー変更は、プライマリ・ノードが故障したと十分なノードが信じたときに行われる。図 2 Cの一部に、ビュー変更プロトコルを示す。図 2 Cを参照すると、ビュー変更フェーズの下で、現在のビューが v である場合、ノード $p = (v + 1) \bmod N$ は、新たなプライマリ・ノードになるために Q 個の有効なビュー変更メッセージの取得を待機し、ここで p はレプリカ／ノードのシリアル番号であり、 v はビュー番号であり、 N はレプリカ／ノードの総数である。 Q 個のビュー変更メッセージは、マルチキャストしたビュー変更メッセージを含むことができる。前のビューは v であるので、ビュー変更メッセージはそれぞれ新たなビュー $v + 1$ を含むことができる。新たなプライマリ・ノード p は、 Q 個のビュー変更メッセージを取得すると、新ビュー・メッセージをマルチキャストする。このメッセージは、受信した全ての有効なビュー変更メッセージに加え、プライマリ・ノードの故障のためにまだ完了していない場合がある全ての要求のセットも含む。新たなプライマリ・ノードは、最新のチェックポイントを決定し、とりわけ、機能しているノードが最新の状態に追いつくようにすることができ、これは、新たなビューにおける以前の要求（たとえば、準備済みかつコミット済みであるが未実行の要求）を再コミットすることを含むことができる。ビュー変更が行われている間、新たな要求は受諾されない。ノードは、 Q 個のビュー変更メッセージを含む有効な新ビュー・メッセージを受信した後、ビュー $v + 1$ に入り、未完了の要求のセットを処理する。その後、通常動作プロトコルが進行し、ノードは最新の安定したチェックポイントの順序番号と、準備メッセージ内の最大の番号との間の要求をやり直すが、要求を再実行しないようにする。通常動作プロトコルとビュー変更プロトコルとの間のノードのステータスの対応する切り替えを図 3 A に示す。図 3 A に示すように、たとえば、バックアップ・ノードのタイムアウトにより、通常動作プロトコルから（たとえば、通常動作プロトコルの任意のフェーズ中に）、ビュー変更プロトコルへの（たとえば、ビュー変更フェーズを開始する）切り替えをトリガーすることができる。ビュー変更プロトコルを実行した後、有効な新ビュー・メッセージを取得すると、バックアップ・ノードはビュー変更プロトコルから退出し、通常動作プロトコルを再開して保留中の要求を実行することができる。有効な新メッセージは、異なるノードからの Q 個のビュー変更メッセージを含むことができる。

【0049】

図 3 B に示すように、様々な実施形態によれば、ノードがビュー変更プロトコルから通常動作プロトコルに切り替えるための代替経路を提供することができる。いくつかの実施形態では、ビュー変更プロトコル中のノードは、 Q 個の第 1 のメッセージを取得して、ビュー変更プロトコルを終了することができる。第 1 のメッセージは、現在のビュー、現在の順序番号、および／またはダイジェストを含むことができる。第 1 のメッセージに基づいて、ビュー変更プロトコル中のノードは、他のノードの大多数が通常動作中であると判定して、ビュー変更から退出することができる。さらなる詳細については、図 4 から図 6 を参照して以下で説明する。

【0050】

図 4 に、本明細書の様々な実施形態によるビュー変更退出ステップ 410 のフローチャートを示す。ステップ 410 は、図 1 のシステム 100 の 1 つまたは複数の構成要素（たとえば、上記のノード 0、ノード 1、ノード 2、...、もしくはノード i または同様のデバイス、あるいはそれらのノードのいずれかと、ノード A などの 1 つまたは複数のさらなるデバイスとの組み合わせ）によって実施することができる。ステップ 410 は、1 つまたは複数のブロックチェーン・ノード（たとえば、プライマリ・ノード、バックアップ・ノード）によって実施することができる。プライマリ・ノードおよびバックアップ・ノードは、PBF T モデルで定義されたものとしてすることができる。ステップ 410 は、様々なハードウェア・マシンおよび／またはソフトウェアを含むビュー変更システムまたはデバイス（たとえば、コンピュータ、サーバ）によって実施することができる。たとえば、ビュー変更退出システムまたはデバイスは、1 つまたは複数のプロセッサと、1 つまたは複数のプロセッサに結合され、そのシステムまたはデバイス（たとえば、プロセッサ）に

ステップ410を実行させるための、1つまたは複数のプロセッサにより実行可能な命令によって構成される、1つまたは複数の非一時的コンピュータ可読記憶媒体（たとえば、1つまたは複数のメモリ）とを備えることができる。以下に提示する動作は、例示的なものとする。実装形態に応じて、これらの動作は、様々な順序でまたは並行して実行される追加のステップ、より少ないステップ、または代替のステップを含むことができる。

【0051】

ステップ411において、第1のノード（たとえば、バックアップ・ノード）は、ビュー変更プロトコルに入ることができる。ステップ412において、第1のノードは、ビュー変更メッセージをマルチキャストすることができる。ビュー変更に入るために、第1のノードは通常動作プロトコルを終了し、上記のビュー変更プロトコルのビュー変更フェーズに入る。一実施形態では、第1のノードは、ビュー変更メッセージをマルチキャストすることにより、ビュー変更プロトコルに入ることができる。たとえば、第1のノードは、ビュー変更メッセージをプライマリ・ノードおよび他のバックアップ・ノードにマルチキャストすることができる。第1のノードは、プライマリ・ノードが障害があるかまたは他の原因で機能していないと判定し、ビュー変更プロトコルに従ってビュー変更メッセージのマルチキャストを開始することができる。

10

【0052】

プライマリ・ノードおよび $(N-1)$ 個のバックアップ・ノードは、PBFTコンセンサス・システムを形成することができる。ここで、プライマリ・ノードは、本当に機能していない場合と、そうでない場合とがある。プライマリ・ノードが本当に機能していない場合、大多数のバックアップ・ノード（たとえば、 Q 個のバックアップ・ノード）は、それぞれビュー変更プロトコルに入り、それぞれビュー変更メッセージをマルチキャストすることができる。第1のノードは、 Q 個のビュー変更メッセージを取得した場合、プライマリ・ノードが機能しておらず、新たなプライマリ・ノードが選出される必要があるというコンセンサスに大多数のノードが到達したと判定することができる。ビュー変更プロトコルの残りの部分を続けることができる。しかしながら、プライマリ・ノードがまだ機能している場合、第1のノードは以下のステップに従ってビュー変更プロトコルを終了することができる。そのような場合、第1のノードは、前述の事前準備メッセージ、準備メッセージ、またはコミット・メッセージの送信および／または受信の遅延を引き起こす、誤解、不安定な接続、および／またはその他の理由によって、ビュー変更に入った場合がある。

20

30

【0053】

ステップ413において、第2のノードは、それぞれ第1のメッセージをマルチキャストすることができる。いくつかの実施形態では、第2のノードは、まだ通常動作プロトコル中であり、上述の手順を実行している場合がある（たとえば、事前準備メッセージの受信、準備メッセージのマルチキャスト中、準備メッセージの受信、コミット・メッセージのマルチキャスト、コミット・メッセージの受信など）。通常動作プロトコルにおいて、第2のノードはそれぞれ、第1のメッセージを第1のノードに送信するか、または第1のメッセージをマルチキャストして、第1のノードが第1のメッセージを取得できるようすることができる。いくつかの実施形態では、第1のメッセージは、コミット・フェーズでマルチキャストするコミット・メッセージに含めることができる。他の実施形態では、第1のメッセージは、コミット・フェーズでマルチキャストするコミット・メッセージに付加することができる。さらに他の実施形態では、第1のメッセージは、たとえばコミット・メッセージをマルチキャストした後に、独立して送信またはマルチキャストすることができる。

40

【0054】

一実施形態では、第1のメッセージは、両方とも第2のノードに認識されている現在のビューおよび現在の順序番号を含むことができる。現在のビューは、いずれのノードが、第2のノードにプライマリ・ノードとして認識されているかを示すことができる。現在の順序番号は、（1）コミット・フェーズにおいて第2のノードによってコミットされた最

50

新の要求（たとえば、トランザクション要求）の順序番号、または（２）コミット・フェーズにおいて第２のノードによってコミットされた最新のブロックを示すブロックの高さ、を示すことができる。ブロックの高さは、ブロックチェーン内のブロックの数に基づくことができる。たとえば、あるブロックの高さは、そのブロックと創始（genesis）ブロックとの間のチェーン内のブロック数とすることができる。ブロックチェーンの最初のブロックは、ブロックの高さ０を有することができ、次のブロックはブロックの高さ１を有することができ、などとするすることができる。この例はブロックの高さを表す方法を限定することを意図したものではなく、ブロックの高さは、ブロックチェーンにおけるブロックのシリアル番号を示す限り、他のタイプの表現を有することができる。任意選択により、第１のメッセージは、最新の要求または最新のブロックのダイジェストを含むこともできる。

10

【００５５】

ステップ４１４において、第１のノードは、第２のノードからそれぞれ第１のメッセージを取得することができる。Ｑ個以上の整合する第１のメッセージを取得したことに応答して、第１のノードはビュー変更プロトコルを終了して、通常動作プロトコルに入ることができる。Ｑ個以上の第１のメッセージは、少なくともＱ個のノードが整合する「ビュー」および「順序番号」に同意したことを意味する。「ビュー」および「順序番号」が整合することは、ノードの大多数が、要求またはブロックに関する１つまたは複数のトランザクションのコンセンサス検証に成功したために、通常動作プロトコルで通常通りに機能していることを示す。第１のノードが、整合するビューおよび順序番号を有するＱ個の第１のメッセージを取得しなかった場合、第１のノードはビュー変更プロトコルのままでいることができる。

20

【００５６】

いくつかの実施形態では、Ｑ個以上の第２のノードに認識されている現在の順序番号は、第１のノードに認識されている第１の順序番号よりも大きい（たとえば、１だけ大きい）。これは、ノードの大多数が、第１のノードによって見逃された、要求またはブロックの１ラウンドのコンセンサス検証を完了していることを示す。したがって、少なくともＱ個の第１のメッセージを受信した第１のノードは、整合する第１のメッセージを通じて、ノードの大多数がまだ通常動作中であることを知ることができる。

【００５７】

いくつかの実施形態では、第１のノードは、少なくとも現在のビューに基づいて通常動作に入ることができる。たとえば、ビュー変更から退出すると、第１のノードは、現在のビューを自身のビューとして使用して、通常動作プロトコルに入ることができる。第１のノードは、最新のブロックの情報（たとえば、ダイジェスト）を組み込むことにより、ブロックチェーンの自身のコピーをブロックチェーンの最新のコピーと同期させることもできる。したがって、第１のノードは、正しいビューと、ブロックチェーンの更新されたコピーとを使用して、通常動作プロトコルを再開することができる。さらに、第１のノードがビュー変更に入ってから通常動作を再開するのにかかる時間は予測することができる。新たなブロックが追加されるとブロックチェーンの高さが増加するので、第１のノードがビュー変更に入り、新たなブロックのコンセンサス検証を見逃してから、１つの新たなブロックがブロックチェーンに追加されるまでに、第１のノードは自身の誤解に気付くことができる。したがって、通常動作を再開するのにかかる時間は、１ラウンドのコンセンサス検証を完了するための時間よりも短くすることができる。

30

40

【００５８】

したがって、ビュー変更に入ったノードは、代替経路を介してビュー変更プロトコルを効率的に終了し、他の通常動作しているノードに再参加することができる。この経路は、たとえば、誤解、不安定な接続、および／またはその他の理由により、ビュー変更に入ったノードに役立つことができる。この経路は、プライマリ・ノードを変更して通常動作を再開するためにＱ個のノードがビュー変更に同意する必要がある従来のビュー変更プロトコルを迂回する。したがって、通常動作の最大数のノードを確保することにより、ネット

50

ワーク・リソース全体をより効率的に利用することができる。

【0059】

図5Aに、本明細書の様々な実施形態によるビュー変更方法510のフローチャートを示す。方法510は、図1のシステム100の1つまたは複数の構成要素（たとえば、上記のノード0、ノード1、ノード2、...、もしくはノード*i*または同様のデバイス、あるいはそれらのノードのいずれかと、ノードAなどの1つまたは複数のさらなるデバイスとの組み合わせ）によって実施することができる。方法510は、1つまたは複数のブロックチェーン・ノード（たとえば、PBFTシステムのバックアップ・ノード）によって実施することができる。プライマリ・ノードおよびバックアップ・ノードは、PBFTモデルで定義されたものとして行うことができる。方法510は、様々なハードウェア・マシンおよび／またはソフトウェアを含むビュー変更システムまたはデバイス（たとえば、コンピュータ、サーバ）によって実施することができる。たとえば、ビュー変更システムまたはデバイスは、1つまたは複数のプロセッサと、1つまたは複数のプロセッサに結合され、そのシステムまたはデバイス（たとえば、プロセッサ）に方法510を実行させるための、1つまたは複数のプロセッサにより実行可能な命令によって構成される、1つまたは複数の非一時的コンピュータ可読記憶媒体（たとえば、1つまたは複数のメモリ）とを備えることができる。以下に提示する方法510の動作は、例示的なものとする。実装形態に応じて、方法510は、様々な順序でまたは並行して実行される追加のステップ、より少ないステップ、または代替のステップを含むことができる。方法510のさらなる詳細については、図1から図4および上記の関連する説明を参照することができる。方法510は、第1のノードによって実行することができる。

【0060】

様々な実施形態において、方法510は、いくつか（*N*個）のノード（たとえば、PBFTコンセンサス・システムのノード）によって維持されるブロックチェーン上で実施されるコンピュータ実施ビュー変更方法とすることができる。一実施形態では、*N*個のノードは、*N*個のノードのうちの1つがプライマリ・ノードとして機能し、その他の（*N*−1）個のノードがバックアップ・ノードとして機能する、実用的ビザンチン障害耐性（PBFT）ネットワークを形成する。方法510は、ビュー変更プロトコル中の、*N*個のノードのうちの第1のノード（たとえば、バックアップ・ノード）によって実行することができる。

【0061】

いくつかの実施形態では、ブロック511の前に、第1のノードはビュー変更に入っている場合がある。ビュー変更に入ると、第1のノードは、ビュー変更メッセージを他のノードにマルチキャストすることができる。たとえば、第1のノードはバックアップ・ノードとすることができる、ビュー変更メッセージをプライマリ・ノードおよび他のバックアップ・ノードにマルチキャストすることができる。プライマリ・ノードおよびバックアップ・ノードは、PBFTコンセンサス・システムを形成することができる。ビュー変更メッセージは、第1のノードが自身の通常動作プロトコルから退出し、ビュー変更プロトコルに入っていることを示す。第1のノードが他のノードから（*Q*−1）個の同様のビュー変更メッセージを受信しない場合（したがって、自身のビュー変更メッセージを含む合計*Q*個の整合するビュー変更メッセージを取得しない場合）、従来のビュー変更プロトコルの閾値は満たされない。それにもかかわらず、以下のステップにより、第1のノードはビュー変更プロトコルを終了し、通常動作プロトコルに入ることが可能になる。

【0062】

ブロック511は、*N*個のノードのうちの少なくとも*Q*個の第2のノードからそれぞれ、少なくとも*Q*個の第1のメッセージを取得することであって、各第1のメッセージは、（1）*N*個のノードの間で指定されるプライマリ・ノードを示す第2のノードに認識されている整合する現在のビューと、（2）第2のノードに認識されている整合する現在の順序番号とを含み、現在の順序番号は、第2のノードによってコミットされた最新のブロックまたは最新のトランザクションに関連し、現在の順序番号は、第1のノードに認識され

ている第1の順序番号よりも大きく（たとえば、1だけ大きく）、 Q （定足数）は $(N + F + 1) / 2$ を最も近い整数に切り上げた値であり、 F は $(N - 1) / 3$ を最も近い整数に切り捨てた値である、取得することを含む。 N は4以上の任意の整数とすることができる。いくつかの実施形態では、 N が少なくとも $(3F + 1)$ である場合、 Q は $(2F + 1)$ である。最新のトランザクションに関連する現在の順序番号は、たとえば、対応する第2のノードによってコミットされた1つまたは複数の最新のトランザクションの順序番号を含むことができる。最新のブロックに関連する現在の順序番号は、たとえば、対応する第2のノードによって維持されるブロックチェーンのコピーの高さを含むことができる。前述のように、ブロックチェーンの高さは、ブロックチェーン内のブロックの数に依存し、最新のブロックの追加に伴って増加することができる。一実施形態では、第1のノードがビュー変更を終了するために、少なくとも Q 個の第1のメッセージは、整合する現在のビューおよび整合する現在の順序番号を含むことができる。ブロック512は、少なくとも Q 個の第1のメッセージを取得したことに応答して、ビュー変更プロトコルを終了することを含む。

10

【0063】

いくつかの実施形態では、「トランザクション」という用語は、ブロックチェーン・システムによって実施され、ブロックチェーンに記録することができる。トランザクションは、たとえば、金融トランザクション、ブロックチェーン契約を展開するまたは呼び出すためのブロックチェーン契約トランザクション、ブロックチェーンの状態（たとえば、ワールド・ステート）を更新するトランザクションなどを含むことができる。トランザクションは金銭の交換を含む必要はない。

20

【0064】

いくつかの実施形態では、少なくとも Q 個の第1のメッセージを取得することは、少なくとも Q 個の第2のノードからそれぞれ、少なくとも Q 個の第2のノードがブロックチェーンに追加する次のブロックに同意することを示す少なくとも Q 個のコミット・メッセージを取得することであって、 Q 個のコミット・メッセージは、 Q 個の第1のメッセージをそれぞれ含む、取得することを含む。たとえば、コミット・メッセージは、現在のビューおよび現在の順序番号を含むことができる。

【0065】

他の実施形態では、少なくとも Q 個の第1のメッセージを取得することは、少なくとも Q 個の第2のノードからそれぞれ、少なくとも Q 個の第2のノードがブロックチェーンに追加する次のブロックに同意することを示す少なくとも Q 個のコミット・メッセージを取得することであって、 Q 個の第1のメッセージは、 Q 個のコミット・メッセージにそれぞれ付加される、取得することを含む。たとえば、第1のメッセージは、第2のノードによってコミット・メッセージと共に送信またはマルチキャストすることができる。

30

【0066】

様々な実施形態において、少なくとも Q 個の第2のノードの現在のビューは v であり、第1のノードは、ビュー変更プロトコル中の場合、 v より大きい第1のビューを有する。たとえば、第1のノードがビュー変更に入る前に、第1および第2のノードは全てビュー v を有する場合があります、しかしその後、第1のノードは、第1のノードが機能していないと疑い、ビュー $v + 1$ のビュー変更に入ったが、第2のノードはビュー v のままである。

40

【0067】

いくつかの実施形態では、現在の順序番号は、第2のノードによって維持されるブロックチェーンの第2のコピーの高さ（ブロックの高さとも呼ばれる）を含み、第1の順序番号は、第1のノードによって維持されるブロックチェーンの第1のコピーの高さを含む。一実施形態では、少なくとも Q 個の第2のノードに認識されている現在の順序番号は $(n + 1)$ であり、第1のノードに認識されている第1の順序番号は n である。たとえば、第1のノードがビュー変更に入る前に、第1および第2のノードは全て、ビュー v においてブロックの高さが99の（すなわち、ブロックチェーン内に100個のブロックがある）ブロックチェーンから開始している場合がある。第1のノードがコミット・フェーズ（た

50

たとえば、コミット・メッセージをマルチキャストするもの)に入る前にビュー変更プロトコルに入って、コンセンサス検証から抜けた後、第2のノードは、101番目のブロックに関するコンセンサスに到達して、ブロックの高さを100に増加させている。ビュー変更プロトコルで立ち往生している第1のノードに認識されていない101番目のブロックは、現在の順序番号(100)と第1の順序番号(99)との差を生じさせる場合がある。

【0068】

他の実施形態では、現在の順序番号は、第2のノードによってコミットされた最新のトランザクションの順序番号を含み、第1の順序番号は、第1のノードによってコミットされた最新のトランザクションの順序番号を含む。一実施形態では、少なくともQ個の第2のノードに認識されている現在の順序番号は $(n+1)$ であり、第1のノードに認識されている第1の順序番号は n である。たとえば、第1のノードがビュー変更に入る前に、第1および第2のノードは全て、コンセンサス検証される80個の要求(たとえば、トランザクション要求)から開始している場合がある。要求には、増加する順序番号を割り当てることができる。ビュー v において、第1および第2のノードは、50個の要求をコンセンサス検証している場合がある。第1のノードがコミット・フェーズ(たとえば、コミット・メッセージをマルチキャストするもの)に入る前にビュー変更プロトコルに入って、コンセンサス検証から抜けた後、第2のノードは、51番目の要求に関するコンセンサスに到達して、次の保留中の要求の順序番号を52に増加させている。コンセンサス検証された51番目の要求は、ビュー変更プロトコルで立ち往生している第1のノードには認識されておらず、現在の順序番号(51)と第1の順序番号(50)との差を生じさせる場合がある。

【0069】

いくつかの実施形態では、第1のメッセージは、最新のブロックまたは最新のトランザクションのダイジェストをさらに含む。ダイジェスト(たとえば、ハッシュ値)は、トランザクションなどのデータにハッシュ・アルゴリズムを適用した数値結果とすることができる。一実施形態では、ダイジェストは、最新のブロックまたは最新のトランザクションのハッシュ値を含む。一例では、ダイジェストは、第2のノードにはコミットされているが、第1のノードにはコミットされていない最新のトランザクションのトランザクション・ハッシュを含む。他の例では、ダイジェストは、第2のノードにはコミットされているが第1のノードにはコミットされていない複数の最新のトランザクションの複数のトランザクション・ハッシュを含む。他の例では、ダイジェストは、第2のノードには認識されているが第1のノードには認識されていない最新のブロックのマークル・ルートを含む。他の例では、ダイジェストは、第2のノードには認識されているが第1のノードには認識されていない複数の最新のブロックの複数のマークル・ルートを含む。

【0070】

いくつかの実施形態では、「ビュー」、「順序番号」、および/または「ダイジェスト」は、1つまたは複数のデジタル署名(または略して、署名)として第1のメッセージに含めることができる。第1のメッセージは、両方とも第2のノードに認識されている現在のビューおよび現在の順序番号を保証するデジタル署名を含む。「署名」は、対応するメッセージを送信したエンティティからの是認(endorsement)を示す。「署名」という用語は、あらゆる形態の承認を示すものとしてすることができる。一実施形態では、「ビュー」「順序番号」および/または「ダイジェスト」をまず一方向ハッシュ関数に入力し、その出力ハッシュ値を対応するノードの秘密鍵で暗号化して、デジタル署名を取得することができる。暗号化は様々な方法で、たとえば、公開-秘密鍵暗号化(非対称暗号とも呼ばれる)、デジタル署名アルゴリズム(DSA: Digital Signature Algorithm)、たとえば、楕円曲線デジタル署名アルゴリズム(ECDSA: Elliptic Curve Digital Signature Algorithm)などによって実現することができる。たとえば、RSAなどの公開鍵アルゴリズムを使用して、数学的にリンクされた2つの鍵:1つの秘密鍵および1つの公開鍵を生

成することができる。公開鍵暗号が、2つの相互に認証する暗号鍵に依存するので、デジタル署名は機能する。デジタル署名を生成したノードは、自身の秘密鍵を使用して、「ビュー」、「順序番号」、および／または「ダイジェスト」を暗号化することができ、そのデータを復号する唯一の方法は、署名者ノードの公開鍵を使用することである。したがって、デジタル署名は、対応するノードに認識されている「ビュー」、「順序番号」、および／または「ダイジェスト」を表すことができる。

【0071】

いくつかの実施形態では、ビュー変更プロトコルを終了することは、第1のノードによって維持されるブロックチェーンの第1のコピーを、第2のノードによって維持されるブロックチェーンの第2のコピーと同期させることと、第1のノードに対して整合する現在のビューを使用することによって、ビュー変更プロトコルから退出して、通常動作プロトコルに入ることを含む。したがって、第2のノードがビュー v にあり、第1のノードがビュー $(v+1)$ で立ち往生していた場合、第1のノードはビュー変更プロトコルを終了し、ビュー v で通常動作プロトコルに入ることができる。

【0072】

図5Bに、本明細書の様々な実施形態によるビュー変更方法520のフローチャートを示す。方法520は、図1のシステム100の1つまたは複数の構成要素（たとえば、上記のノード0、ノード1、ノード2、...、もしくはノード i または同様のデバイス、あるいはそれらのノードのいずれかと、ノードAなどの1つまたは複数のさらなるデバイスとの組み合わせ）によって実施することができる。方法520は、1つまたは複数のブロックチェーン・ノード（たとえば、PBFTシステムのプライマリ・ノードまたはバックアップ・ノード）によって実施することができる。プライマリ・ノードおよびバックアップ・ノードは、PBFTモデルで定義されたものとして行うことができる。方法520は、様々なハードウェア・マシンおよび／またはソフトウェアを含むビュー変更システムまたはデバイス（たとえば、コンピュータ、サーバ）によって実施することができる。たとえば、ビュー変更システムまたはデバイスは、1つまたは複数のプロセッサと、1つまたは複数のプロセッサに結合され、そのシステムまたはデバイス（たとえば、プロセッサ）に方法520を実行させるための、1つまたは複数のプロセッサにより実行可能な命令によって構成される、1つまたは複数の非一時的コンピュータ可読記憶媒体（たとえば、1つまたは複数のメモリ）とを備えることができる。以下に提示する方法520の動作は、例示的なものとする。実装形態に応じて、方法520は、様々な順序でまたは並行して実行される追加のステップ、より少ないステップ、または代替のステップを含むことができる。方法520のさらなる詳細については、図1から図4および上記の関連する説明を参照することができる。方法520は、第2のノードによって実行することができる。第2のノードがプライマリ・ノードである場合、第2のノードはステップ521a、522a、523、524、525、および526を実行することができる。第2のノードがバックアップ・ノードである場合、第2のノードはステップ521b、522b、523、524、525、および526を実行することができる。

【0073】

ブロック521aは、第2のノード（たとえば、プライマリ・ノード）により、1つまたは複数の要求（たとえば、トランザクション要求）を取得することを含む。要求は、コンセンサス検証されるブロックチェーン・トランザクション（スマート・コントラクトの有無によらない）を含むことができる。一例では、要求は、コンセンサス検証され、ブロックチェーンに追加されるトランザクションに対応することができる。コンセンサス検証は、1ラウンドの通常動作プロトコルの実行中に実行することができる。あるいは、要求は他の動作に対応することができる。いくつかの実施形態では、プライマリ・ノードは、クライアント（たとえば、軽量ノード）から、またはクライアントから要求を取得し、要求をプライマリ・ノードに転送したバックアップ・ノードから要求を取得することができる。

【0074】

ブロック522aは、事前準備メッセージおよび要求をバックアップ・ノードにマルチキャストすることを含む。いくつかの実施形態では、複数の要求を取得した後、第2のノードは、事前準備メッセージおよび要求を各バックアップ・ノードにマルチキャストすることができる。事前準備メッセージは、要求の順序（たとえば、要求に関連するトランザクションの順序）を含むことができる。順序は、各要求の順序番号、および／またはブロックチェーンに追加する次のブロックの順序番号を含むことができる。

【0075】

ブロック521bは、第2のノード（たとえば、バックアップ・ノード）により、事前準備メッセージおよび1つまたは複数の要求を取得することを含む。たとえば、事前準備メッセージおよび要求は、バックアップ・ノードによってプライマリ・ノードから取得することができる。同様に、バックアップ・ノードは、事前準備メッセージおよび要求を、それらの要求を実行する順序と共に取得することができる。

【0076】

ブロック522bは、第2のノードが事前準備メッセージを受諾した場合に、準備メッセージをマルチキャストすることを含む。マルチキャストはブロードキャストを意味する場合がある。たとえば、準備メッセージは、バックアップ・ノードによってプライマリ・ノードおよび他のバックアップ・ノードにマルチキャストすることができる。

【0077】

ブロック523は、 $(Q-1)$ 個以上の準備メッセージを取得することを含む。いくつかの実施形態では、 Q （定足数）は $(N+F+1)/2$ を最も近い整数に切り上げた値であり、 F は $(N-1)/3$ を最も近い整数に切り捨てた値であって、 N 個のノードのコンセンサス・システムを機能させ続けるために、 N 個のノード間で許容された機能していないノードの最大数を表す。 $(Q-1)$ 個以上の準備メッセージを取得することは、コミット・フェーズに入る前に満たすべき条件とすることができる。 $(Q-1)$ 個以上の準備メッセージは、対応するノード自身がマルチキャストした準備メッセージを含むことができる。

【0078】

ブロック524は、（1）第2のノードに認識されているプライマリ・ノードを示す現在のビューと、（2）第2のノードに認識されている現在の順序番号と、を含むコミット・メッセージを他のノードにマルチキャストすることを含む。いくつかの実施形態では、マルチキャストされるコミット・メッセージは、現在のビューおよび現在の順序番号を暗号化した1つまたは複数のデジタル署名を含む。

【0079】

いくつかの実施形態では、コミット・メッセージは、要求に関連する1つまたは複数のトランザクションのダイジェストをさらに含む。たとえば、ダイジェストは、最新のコミットされたトランザクションのトランザクション・ハッシュ、またはブロックチェーンの最新のブロックのマークル・トライ・ルートを含むことができる。

【0080】

いくつかの実施形態では、第2のノードはビュー変更に入っておらず、第2のノードに認識されている現在の順序番号は、ビュー変更に入った第1のノードに認識されている第1の順序番号よりも（たとえば、1だけ）大きい。

【0081】

いくつかの実施形態では、最大 F 個のノードが機能していなくてもよい。それにもかかわらず、PBFTシステムは最大 F 個の機能していないノードを許容するので、説明した方法およびコンセンサス検証は適切に実行することができる。

【0082】

ブロック525は、少なくとも Q 個のコミット・メッセージを取得することを含む。 Q 個のコミット・メッセージは、対応するノード自身がマルチキャストしたコミット・メッセージを含むことができる。

【0083】

10

20

30

40

50

ブロック526は、1つまたは複数の要求を実行することを含む。たとえば、1つまたは複数の要求をコンセンサス検証し、それに対応してブロックチェーンのローカル・コピーに追加することができる。結果として、十分なノード（たとえば、Q個のノード）が対応するトランザクションを検証した場合、そのトランザクションはブロックチェーン内にバックされる。

【0084】

図6に、様々な実施形態によるビュー変更システム610のブロック図を示す。ビュー変更システム610（たとえば、コンピュータ・システム）は、上記のノード0、ノード1、ノード2、...、もしくはノードiまたは同様のデバイス、あるいはそれらのノードのいずれかと、さらなるデバイス（たとえば、ノードA）との組み合わせの実装形態の一例とすることができる。方法510は、ビュー変更システム610によって実施することができる。ビュー変更システム610は、1つまたは複数のプロセッサと、1つまたは複数のプロセッサに結合され、そのシステムまたはデバイス（たとえば、プロセッサ）に方法510を実行させるための、1つまたは複数のプロセッサにより実行可能な命令によって構成される、1つまたは複数の非一時的コンピュータ可読記憶媒体（たとえば、1つまたは複数のメモリ）とを備えることができる。ビュー変更システム610は、命令（たとえば、ソフトウェア命令）に対応する様々なユニット／モジュールを備えることができる。

【0085】

いくつかの実施形態では、ビュー変更システム610は、ビュー変更装置と呼ばれる場合がある。ビュー変更装置は、ブロックチェーンを維持するためのものとすることができる、いくつか（N個）のノードがブロックチェーンを維持し、N個のノードのうちの1つはプライマリ・ノードとして機能し、その他の（N-1）個のノードはバックアップ・ノードとして機能し、コンセンサス装置は、ビュー変更プロトコル中の、N個のノードのうちの第1のノードとして機能する。コンセンサス装置は、1つまたは複数のプロセッサと、1つまたは複数のプロセッサに結合され、その装置に動作を実行させるための、1つまたは複数のプロセッサにより実行可能な命令によって構成される、1つまたは複数の非一時的コンピュータ可読メモリとを備えることができる。コンセンサス装置は、命令（たとえば、ソフトウェア命令）に対応する様々なユニット／モジュールを備えることができる。コンセンサス装置は、N個のノードのうちの少なくともQ個の第2のノードからそれぞれ、少なくともQ個の第1のメッセージを取得するための取得モジュール611であって、各第1のメッセージは、（1）N個のノードの間で指定されるプライマリ・ノードを示す第2のノードに認識されている整合する現在のビューと、（2）第2のノードに認識されている整合する現在の順序番号とを含み、現在の順序番号は、第2のノードによってコミットされた最新のブロックまたは最新のトランザクションに関連し、現在の順序番号は、第1のノードに認識されている第1の順序番号よりも大きく、Q（定足数）は $(N + F + 1) / 2$ を最も近い整数に切り上げた値であり、Fは $(N - 1) / 3$ を最も近い整数に切り捨てた値である、取得モジュール611と、少なくともQ個の第1のメッセージを取得したことに応答して、ビュー変更プロトコルを終了するための終了モジュール612とを備えることができる。

【0086】

本明細書に記載の技術は、1つまたは複数の専用コンピューティング・デバイスによって実装される。専用コンピューティング・デバイスは、これらの技術を実装するためのハード・ワイヤードおよび／またはプログラム・ロジックを組み込んだ、デスクトップ・コンピュータ・システム、サーバ・コンピュータ・システム、ポータブル・コンピュータ・システム、ハンドヘルド・デバイス、ネットワークング・デバイス、または他の任意のデバイスもしくはデバイスの組み合わせとすることができる。専用コンピューティング・デバイスは、パーソナル・コンピュータ、ラップトップ、携帯電話、カメラ付き携帯電話、スマート・フォン、携帯情報端末、メディア・プレーヤー、ナビゲーション・デバイス、電子メール・デバイス、ゲーム・コンソール、タブレット・コンピュータ、ウェアラブル

10

20

30

40

50

・デバイス、またはそれらの組み合わせとして実装することができる。コンピューティング・デバイスは、通常、オペレーティング・システム・ソフトウェアによって制御および調整される。従来のオペレーティング・システムは、実行すべきコンピュータ・プロセスを管理およびスケジュールし、メモリ管理を実行し、ファイル・システム、ネットワーキング、I/Oサービスを提供し、とりわけグラフィカル・ユーザ・インターフェース（「GUI」）などのユーザ・インターフェース機能を提供する。本明細書に記載の様々なシステム、装置、記憶媒体、モジュール、およびユニットは、専用コンピューティング・デバイス、あるいは1つまたは複数の専用コンピューティング・デバイスの1つまたは複数のコンピューティング・チップに実装することができる。いくつかの実施形態では、本明細書に記載の命令は、専用コンピューティング・デバイス上の仮想マシンに実装することができる。命令は、実行されると、専用コンピューティング・デバイスに、本明細書に記載の様々な方法を実行させることができる。仮想マシンは、ソフトウェア、ハードウェア、またはそれらの組み合わせを含むことができる。たとえば、仮想マシンは、イーサリアムでのスマート・コントラクトのためのランタイム環境を提供するイーサリアム仮想マシン（EVM：Ethereum Virtual Machine）ソフトウェアを含むことができる。

10

【0087】

図7は、本明細書に記載の実施形態のいずれかを実装することができるコンピュータ・システム700を示すブロック図である。システム700は、本明細書に記載の方法のいずれか（たとえば、ビュー変更方法510、ビュー変更方法520）を実行することができる。システム700は、本明細書に記載のシステムのいずれか（たとえば、ビュー変更システム610）に実装することができる。システム700は、本明細書に記載のノードのいずれかに実装し、ブロックチェーン契約を実施するための対応するステップを実行するように構成することができる。コンピュータ・システム700は、情報を伝達するためのバス702または他の通信メカニズム、情報を処理するための、バス702で結合された1つまたは複数のハードウェア・プロセッサ704を含む。ハードウェア・プロセッサ704は、たとえば、1つまたは複数の汎用マイクロプロセッサとすることができる。

20

【0088】

コンピュータ・システム700は、情報と、プロセッサ704によって実行可能な命令とを記憶するための、バス702に結合されたメイン・メモリ706、たとえば、ランダム・アクセス・メモリ（RAM）、キャッシュ、および／または他の動的記憶デバイスなどをさらに含む。メイン・メモリ706は、プロセッサ704によって実行可能な命令の実行中に一時変数または他の中間情報を記憶するために使用することもできる。そのような命令は、プロセッサ704がアクセスできる記憶媒体に記憶されると、コンピュータ・システム700を、それらの命令で指定された動作を実行するようにカスタマイズされた専用マシンにする。コンピュータ・システム700は、プロセッサ704用の静的情報および命令を記憶するための、バス702に結合された読み取り専用メモリ（ROM）708または他の静的記憶デバイスをさらに含む。情報および命令を記憶するためのストレージ・デバイス710、たとえば、磁気ディスク、光ディスク、またはUSBサム・ドライブ（フラッシュ・ドライブ）などが設けられ、バス702に結合される。

30

40

【0089】

コンピュータ・システム700は、コンピュータ・システムと組んで、コンピュータ・システム700を専用マシンにするかまたはそうなるようにプログラムする、カスタマイズされたハード・ワイヤード・ロジック、1つまたは複数のASICまたはFPGA、ファームウェアならびに／あるいはプログラム・ロジックを使用して、本明細書に記載の技術を実装することができる。一実施形態によれば、本明細書に記載の動作、方法、および処理は、プロセッサ704が、メイン・メモリ706に含まれる1つまたは複数の命令の1つまたは複数のシーケンスを実行したことに応答して、コンピュータ・システム700によって実行される。そのような命令は、ストレージ・デバイス710などの他の記憶媒体からメイン・メモリ706に読み込むことができる。メイン・メモリ706に含まれる

50

命令のシーケンスを実行することにより、プロセッサ704は本明細書に記載の処理ステップを実行する。代替的实施形態では、ソフトウェア命令の代わりに、またはソフトウェア命令と組み合わせて、ハード・ワイヤード回路を使用することができる。

【0090】

メイン・メモリ706、ROM708、および／またはストレージ710は、非一時的記憶媒体を含むことができる。「非一時的媒体」という用語および類似の用語は、本明細書で使用する場合、マシンを特定の方法で動作させるデータおよび／または命令を記憶する媒体を指し、その媒体は一時的な信号を除外する。そのような非一時的媒体は、不揮発性媒体および／または揮発性媒体を含むことができる。不揮発性媒体には、たとえば、ストレージ・デバイス710などの光ディスクまたは磁気ディスクが含まれる。揮発性媒体には、メイン・メモリ706などの動的メモリが含まれる。非一時的媒体の一般的な形式には、たとえば、フロッピー（登録商標）・ディスク、フレキシブル・ディスク、ハード・ディスク、ソリッド・ステート・ドライブ、磁気テープ、またはその他の任意の磁気データ記憶媒体、CD-ROM、その他の任意の光学データ記憶媒体、穴のパターンを有する任意の物理媒体、RAM、PROM、およびEPROM、フラッシュEPROM、NVRAM、その他の任意のメモリチップまたはカートリッジ、ならびにそれらのネットワーク接続バージョンが含まれる。

10

【0091】

コンピュータ・システム700は、バス702に結合されたネットワーク・インターフェース718をさらに含む。ネットワーク・インターフェース718は、1つまたは複数のローカル・ネットワークに接続された1つまたは複数のネットワーク・リンクに結合する双方向データ通信を提供する。たとえば、ネットワーク・インターフェース718は、サービス総合デジタル網（ISDN：integrated services digital network）カード、ケーブル・モデム、衛星モデム、または対応するタイプの電話回線へのデータ通信接続を提供するモデムとすることができる。他の例として、ネットワーク・インターフェース718は、互換性のあるLANへのデータ通信接続を提供するローカル・エリア・ネットワーク（LAN）カード（またはWANと通信するためのWANコンポーネント）とすることができる。無線リンクを実装することもできる。任意のそのような実装形態では、ネットワーク・インターフェース718は、様々なタイプの情報を表すデジタル・データ・ストリームを運ぶ電気信号、電磁信号、または光信号を送受信する。

20

30

【0092】

コンピュータ・システム700は、ネットワーク、ネットワーク・リンク、およびネットワーク・インターフェース718を介して、メッセージを送信し、プログラム・コードを含むデータを受信することができる。インターネットの例では、サーバは、インターネット、ISP、ローカル・ネットワーク、およびネットワーク・インターフェース718を介して、アプリケーション・プログラムの要求されたコードを送信してもよい。

【0093】

受信されたコードは、受信されたときにプロセッサ704によって実行され、および／または後で実行するためにストレージ・デバイス710もしくはその他の不揮発性記憶装置に記憶することができる。

40

【0094】

前のセクションで説明した処理、方法、およびアルゴリズムのそれぞれは、1つまたは複数のコンピュータ・システム、あるいはコンピュータ・ハードウェアを備えるコンピュータ・プロセッサによって実行されるコード・モジュールに具現化し、それによって完全にまたは部分的に自動化することができる。処理およびアルゴリズムは、特定用途向け回路に部分的または全体的に実装することができる。

【0095】

上記の様々な特徴および処理は、互いに独立して使用することができ、または様々な方法で組み合わせることができる。可能な全ての組み合わせおよび部分的組み合わせは、本

50

明細書の範囲内に入るものとする。加えて、特定の手法または処理ブロックは、実装形態によっては省略される場合がある。本明細書に記載の方法および処理も、任意の特定の順序に限定されるものではなく、それに関連するブロックまたは状態は、適切な他の順序で実行することができる。たとえば、説明したブロックまたは状態は、具体的に開示した順序以外の順序で実行することができ、あるいは複数のブロックまたは状態を単一のブロックまたは状態に組み合わせることができる。ブロックまたは状態の例は、直列に、並列に、または他の何らかの態様で実行することができる。開示した実施形態に対して、ブロックまたは状態を追加または削除することができる。本明細書に記載のシステムおよび構成要素の例は、記載とは異なるように構成することができる。たとえば、開示した実施形態と比較して、要素を追加、削除、または再配置することができる。

10

【0096】

本明細書に記載の方法の様々な動作は、関連する動作を実行するように（たとえば、ソフトウェアで）一時的に構成されるまたは永続的に構成される1つまたは複数のプロセッサによって少なくとも部分的に実行することができる。一時的に構成されるか永続的に構成されるかにかかわらず、そのようなプロセッサは、本明細書に記載の1つまたは複数の動作または機能を実行するように動作するプロセッサ実装エンジンを構成することができる。

【0097】

同様に、本明細書に記載の方法は、ハードウェアの一例である1つまたは複数の特定のプロセッサを使用して、少なくとも部分的にプロセッサで実装することができる。たとえば、方法の動作の少なくとも一部は、1つまたは複数のプロセッサまたはプロセッサ実装エンジンによって実行することができる。そのうえ、1つまたは複数のプロセッサは、「クラウド・コンピューティング」環境で、または「ソフトウェア・アズ・ア・サービス」（SaaS）として、関連する動作の実行をサポートするように動作することもできる。たとえば、動作の少なくとも一部は、（プロセッサを含むマシンの例としての）コンピュータのグループによって実行することができ、これらの動作はネットワーク（たとえば、インターネット）と、1つまたは複数の適切なインターフェース（たとえば、アプリケーション・プログラム・インターフェース（API））とを介してアクセス可能である。

20

【0098】

特定の動作の実行は、単一のマシン内にあるプロセッサだけでなく、いくつかのマシンに配備されたプロセッサの間で分散させることができる。いくつかの実施形態では、プロセッサまたはプロセッサ実装エンジンは、単一の地理的位置（たとえば、家庭環境、オフィス環境、またはサーバ・ファーム内）に配置することができる。他の実施形態では、プロセッサまたはプロセッサ実装エンジンは、いくつかの地理的位置にわたって分散させることができる。

30

【0099】

本明細書全体を通して、複数のインスタンスが、単一のインスタンスとして記述した構成要素、動作、または構造を実装することができる。1つまたは複数の方法の個々の動作は別個の動作として図示および説明しているが、個々の動作のうちの1つまたは複数と同時に実行することができ、動作が図示した順序で実行される必要はない。構成において個別の構成要素として提示した構造および機能は、組み合わせられた構造または構成要素として実装することができる。同様に、単一の構成要素として提示した構造および機能は、個別の構成要素として実装することができる。これらおよび他の変形、修正、追加、および改良は、本明細書の主題の範囲内に入る。さらに、本明細書で使用する関連語（related terms）（「第1の」、「第2の」、「第3の」など）は、いかなる順序、高さ、または重要性を示すものではなく、ある要素と他の要素とを区別するために使用する。さらに、「1つの（a）」、「1つの（an）」、および「複数の（plural i t y）」という語は、本明細書において数量の限定を示すものではなく、言及した項目のうちの少なくとも1つの存在を示すものである。

40

【0100】

50

特定の実施形態を参照して本主題の概要を説明したが、本明細書の実施形態のより広い範囲から逸脱することなく、これらの実施形態に様々な修正および変更を加えることができる。詳細な説明は限定的な意味で解釈されるべきではなく、様々な実施形態の範囲は、添付の特許請求の範囲、ならびにそのような特許請求の範囲が権利を有する均等物の全範囲によってのみ定義される。

【図 1】

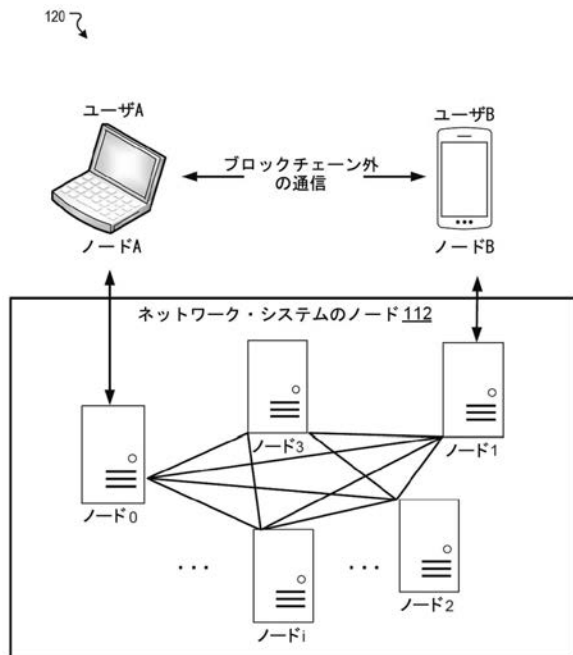


FIG. 1

【図 2 A】

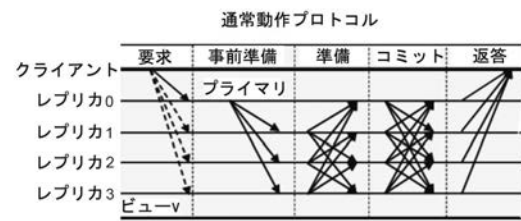


FIG. 2A

【図 2 B】

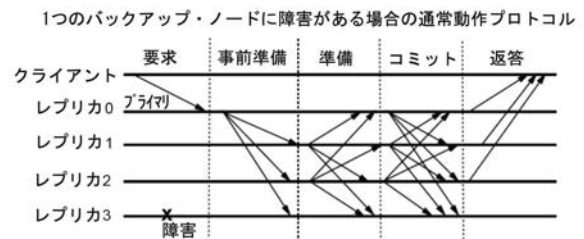


FIG. 2B

【図 2 C】

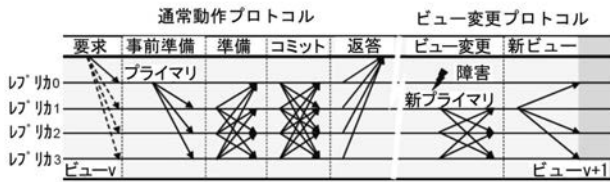


FIG. 2C

【図 3 A】

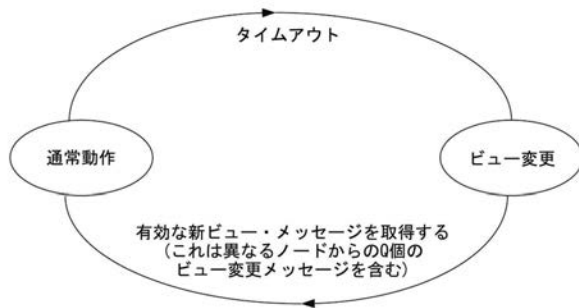


FIG. 3A

【図 3 B】

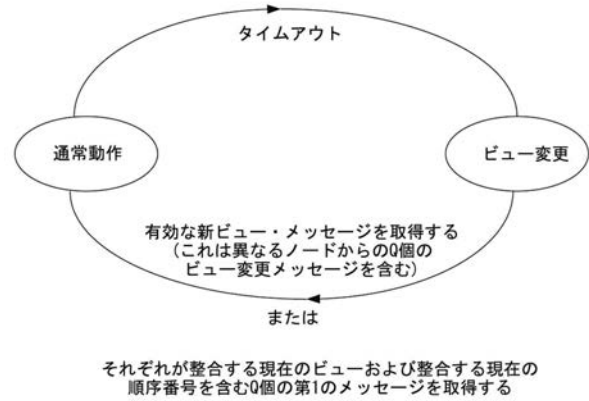


FIG. 3B

【図 4】

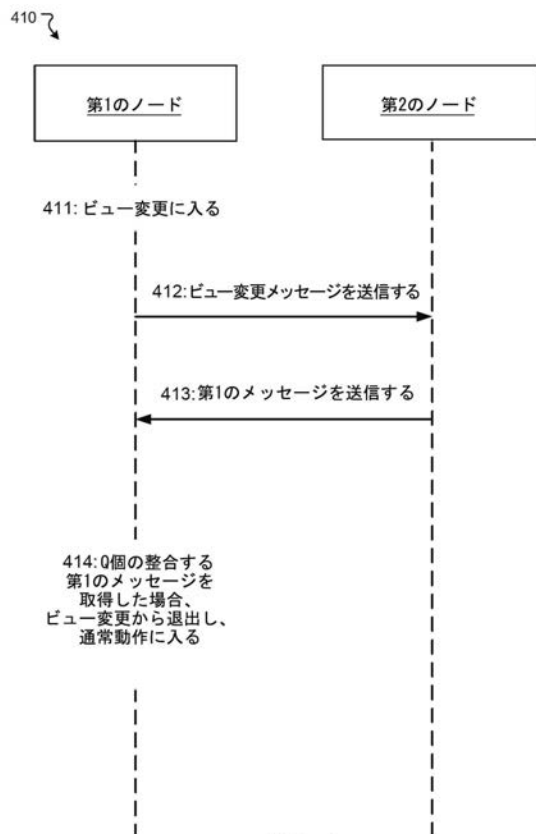


FIG. 4

【図 5 A】

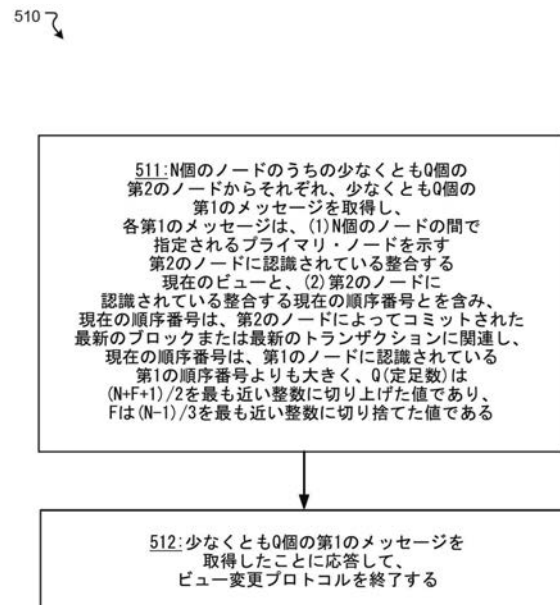


FIG. 5A

【図 5 B】

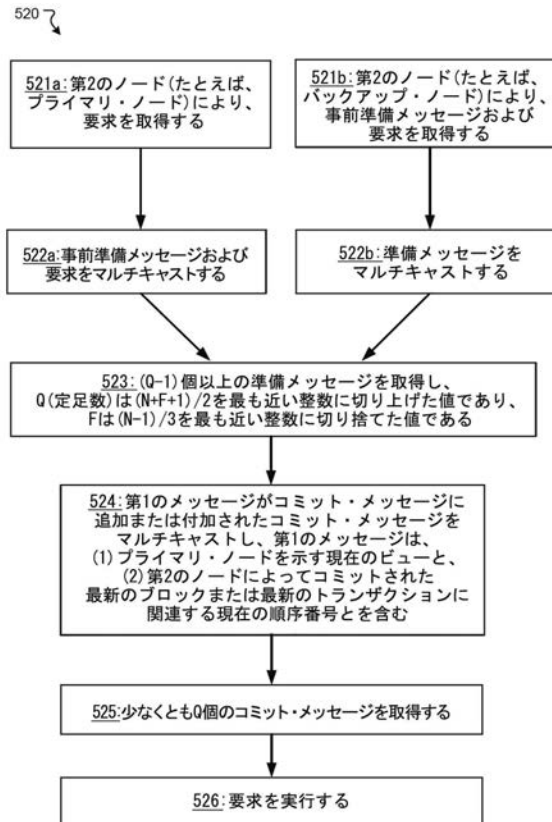


FIG. 5B

【図 6】



FIG. 6

【図 7】

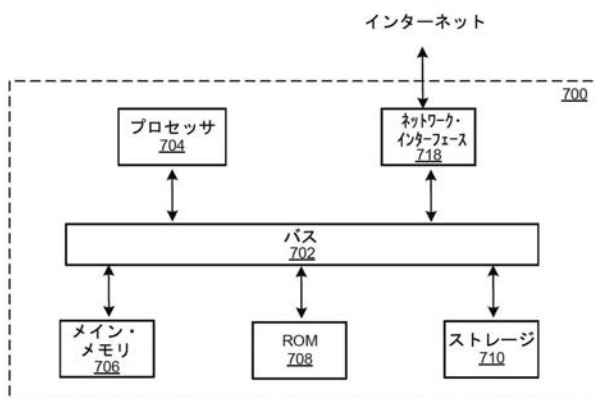


FIG. 7

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/078487

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/24(2006.01)i; G06Q 20/38(2012.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; G06Q; G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT,CNKI,WPI,EPODOC: protocol,change,view,PBFT,practical byzantine fault tolerance,node,number,sequence,message,consistent

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2012254412 A1 (SIEMENS CORPORATION) 04 October 2012 (2012-10-04) description, paragraphs [0037]-[0081]	1-15
A	CN 107579848 A (SHANGHAI INSURANCE EXCHANGE CO., LTD.) 12 January 2018 (2018-01-12) the whole document	1-15
A	CN 109039748 A (SHANGHAI STOCK EXCHANGE TECHNOLOGY CO. LTD. et al.) 18 December 2018 (2018-12-18) the whole document	1-15
A	CN 107040594 A (SHANDA DAREWAY SOFTWARE CO., LTD.) 11 August 2017 (2017-08-11) the whole document	1-15

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"D" document cited by the applicant in the international application

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

06 August 2019

Date of mailing of the international search report

17 December 2019

Name and mailing address of the ISA/CN

National Intellectual Property Administration, PRC
6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing
100088
China

Authorized officer

RAN, Jianguo

Facsimile No. (86-10)62019451

Telephone No. 86-(10)-53961729

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/078487

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US	2012254412	A1	04 October 2012	US 8549142 B2	01 October 2013
CN	107579848	A	12 January 2018	None	
CN	109039748	A	18 December 2018	None	
CN	107040594	A	11 August 2017	None	

フロントページの続き

(51)Int.Cl.

F I

テーマコード (参考)

G 0 6 F 13/00 3 5 1 M

(81)指定国・地域 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT

(74)代理人 100165191

弁理士 河合 章

(74)代理人 100133835

弁理士 河野 努

(72)発明者 ヤン ターイー

中華人民共和国, ジョージアーン 3 1 1 1 2 1, ハーンジョウ, ユイ ハーン ディストリクト, ウエスト ウエン イー ロード ナンバー 9 6 9, ビルディング 3, 5 / フロア, アリババ グループ リーガル ディパートメント

F ターム (参考) 5B042 GA12 KK17

5B089 GA11 GA25 HA03 HA06 HA10 JA11 KA12 ME01

5B175 AA01 KA09