(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6936396号
(P6936396)
(45)発行日　令和3年9月15日(2021.9.15)　(24)登録日　令和3年8月30日(2021.8.30)

(51)Int.Cl.　　F I
G06Q 20/38 (2012.01)　G06Q 20/38
H04L 9/32 (2006.01)　H04L 9/00　675Z
G06F 9/46 (2006.01)　G06F 9/46　430

請求項の数 14　(全 31 頁)

(21)出願番号　特願2020-529460 (P2020-529460)
(86)(22)出願日　令和1年5月29日(2019.5.29)
(65)公表番号　特表2021-509189 (P2021-509189A)
(43)公表日　令和3年3月18日(2021.3.18)
(86)国際出願番号　PCT/US2019/034243
(87)国際公開番号　WO2019/231945
(87)国際公開日　令和1年12月5日(2019.12.5)
審査請求日　令和2年7月28日(2020.7.28)
(31)優先権主張番号　201810531740.6
(32)優先日　平成30年5月29日(2018.5.29)
(33)優先権主張国・地域又は機関
中国(CN)

早期審査対象出願

(73)特許権者　520015461
アドバンスド　ニュー　テクノロジーズ　カンパニー　リミテッド
英国領ケイマン諸島　グランド　ケイマン　ケーワイ１－９００８　ジョージ　タウン　ホスピタル　ロード　２７　ケイマン　コーポレート　センター
(74)代理人　100188558
弁理士　飯田　雅人
(74)代理人　100205785
弁理士　▲高▼橋　史生

最終頁に続く

(54)【発明の名称】ブロックチェーンベースのトランザクション処理方法および装置

(57)【特許請求の範囲】
【請求項１】
コンピュータで実行されるブロックチェーンベースのトランザクションを処理するための方法であって、
ブロックチェーン内のメンバーノードデバイスによって開始されたターゲットトランザクションを受信するステップであって、前記ターゲットトランザクションが、基準時間パラメータを含み、前記基準時間パラメータが前記ターゲットトランザクションが作成されるときに生成される基準タイムスタンプであり、トランザクション有効期間が第1の値と第2の値との間の数値間隔に対応し、前記第1の値が、候補ブロックの作成タイムスタンプから第1のしきい値を差し引いたものであり、前記第2の値が、前記候補ブロックの前記作成タイムスタンプと第2のしきい値の和であり、前記基準時間パラメータは前記ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるかどうかを決定するために使用される、ステップと、
前記基準時間パラメータに基づいて、前記ターゲットトランザクションが前記トランザクション有効期間内の有効トランザクションであるかどうかを決定するステップであって、前記ターゲットトランザクションが前記トランザクション有効期間内の有効トランザクションであるかどうかを決定するステップは、
前記基準タイムスタンプが前記第1の値より大きく、前記第2の値より小さいかどうかを決定するために、前記基準タイムスタンプを前記第1の値および前記第2の値の各々と比較するステップと、

前記基準タイムスタンプが前記第1の値より大きく、前記第2の値より小さいとの決定に応答して、前記ターゲットトランザクションが前記トランザクション有効期間内の有効トランザクションであると決定するステップと
を含む、ステップと、
前記ターゲットトランザクションが前記トランザクション有効期間内の有効トランザクションであるとの決定に応答して、前記ターゲットトランザクションを生成された候補ブロックに記録するステップとを含む、
方法。
【請求項２】
前記基準時間パラメータが、前記ターゲットトランザクションが作成されるときに生成される基準ブロック高さ値であり、
前記トランザクション有効期間が、第3の値と前記ブロックチェーン内の前記候補ブロックのブロック高さ値との間の数値間隔に対応し、
前記第3の値が、前記ブロックチェーン内の前記候補ブロックの前記ブロック高さ値と第3のしきい値との間の差であり、
前記基準時間パラメータに基づいて、前記ターゲットトランザクションが前記トランザクション有効期間内の前記有効トランザクションであるかどうかを決定するステップが、
前記基準ブロック高さ値が前記第3の値より大きく、前記ブロックチェーン内の前記候補ブロックの前記ブロック高さ値より小さいかどうかを決定するために、前記基準ブロック高さ値を前記ブロックチェーン内の前記候補ブロックの前記ブロック高さ値および前記第3の値の各々と比較するステップと、
前記基準ブロック高さ値が前記第3の値より大きく、前記ブロックチェーン内の前記候補ブロックの前記ブロック高さ値より小さいとの決定に応答して、前記ターゲットトランザクションが前記トランザクション有効期間内の有効トランザクションであると決定するステップとを含む、
請求項１に記載のコンピュータで実行される方法。
【請求項３】
前記基準ブロック高さ値を前記ブロックチェーン内の前記候補ブロックの前記ブロック高さ値および前記第3の値の各々と比較するステップの前に、前記方法が、
前記候補ブロックの候補ブロック数が前記ブロックチェーン内の最新ブロックの最新ブロック数より大きいかどうかを決定するステップと、
前記候補ブロックの前記候補ブロック数が前記ブロックチェーン内の最新ブロックの前記最新ブロック数より大きいとの決定に応答して、前記基準ブロック高さ値を前記ブロックチェーン内の前記候補ブロックの前記ブロック高さ値および前記第3の値の各々と比較するステップとをさらに含む、
請求項２に記載のコンピュータで実行される方法。
【請求項４】
前記ターゲットトランザクションが、前記ターゲットトランザクションの一意の識別子をさらに含み、
前記ターゲットトランザクションが前記トランザクション有効期間内の前記有効トランザクションであるとの決定に応答して、前記ターゲットトランザクションを前記候補ブロックに記録するステップが、
前記ターゲットトランザクションが前記トランザクション有効期間内の有効トランザクションであるとの決定に応答して、前記ターゲットトランザクションの前記一意の識別子に対応するトランザクション冪等レコードが所定のトランザクション冪等テーブルに記憶されているかどうかを問い合わせるステップであって、前記所定のトランザクション冪等テーブルが、前記トランザクション有効期間内の有効トランザクションに対応する前記トランザクション冪等レコードを記憶するために使用される、ステップと、
前記ターゲットトランザクションの前記一意の識別子に対応する前記トランザクション冪等レコードが前記所定のトランザクション冪等テーブルに記憶されていないとの決定

に応答して、前記ターゲットトランザクションを前記候補ブロックに記録するステップとを含む、
請求項３に記載のコンピュータで実行される方法。
【請求項５】
前記トランザクション冪等レコードが、前記トランザクション冪等レコードに対応するトランザクションが前記ブロックチェーンの分散データベースに正常に記録されたことを示し、
前記方法が、
前記ターゲットトランザクションが前記候補ブロックに記録されていると決定され、かつ前記候補ブロックに関するコンセンサスに達し、前記候補ブロックが前記ブロックチェーンの前記分散データベースに正常に記憶されているとの決定に応答して、前記ターゲットトランザクションの前記一意の識別子に対応する前記トランザクション冪等レコードを生成するステップと、
前記トランザクション冪等レコードを前記所定のトランザクション冪等テーブルに挿入するステップとをさらに含む、
請求項４に記載のコンピュータで実行される方法。
【請求項６】
動作を実行するためにコンピュータシステムにより実行可能な１つ以上の命令を含むコンピュータ可読記録媒体であって、
前記動作は、
ブロックチェーン内のメンバーノードデバイスによって開始されたターゲットトランザクションを受信することであって、前記ターゲットトランザクションが、基準時間パラメータを含み、前記基準時間パラメータが前記ターゲットトランザクションが作成されるときに生成される基準タイムスタンプであり、トランザクション有効期間が第1の値と第2の値との間の数値間隔に対応し、前記第1の値が、候補ブロックの作成タイムスタンプから第1のしきい値を差し引いたものであり、前記第2の値が、前記候補ブロックの前記作成タイムスタンプと第2のしきい値の和であり、前記基準時間パラメータは前記ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるかどうかを決定するために使用される、受信することと、
前記基準時間パラメータに基づいて、前記ターゲットトランザクションが前記トランザクション有効期間内の有効トランザクションであるかどうかを決定することであって、前記ターゲットトランザクションが前記トランザクション有効期間内の有効トランザクションであるかどうかを決定することは、
前記基準タイムスタンプが前記第1の値より大きく、前記第2の値より小さいかどうかを決定するために、前記基準タイムスタンプを前記第1の値および前記第2の値の各々と比較することと、
前記基準タイムスタンプが前記第1の値より大きく、前記第2の値より小さいとの決定に応答して、前記ターゲットトランザクションが前記トランザクション有効期間内の有効トランザクションであると決定することと
を含む、決定することと、
前記ターゲットトランザクションが前記トランザクション有効期間内の有効トランザクションであるとの決定に応答して、前記ターゲットトランザクションを生成された候補ブロックに記録することと
を含むコンピュータ可読記録媒体。
【請求項７】
前記基準時間パラメータが、前記ターゲットトランザクションが作成されるときに生成される基準ブロック高さ値であり、
前記トランザクション有効期間が、第3の値と前記ブロックチェーン内の前記候補ブロックのブロック高さ値との間の数値間隔に対応し、
前記第3の値が、前記ブロックチェーン内の前記候補ブロックの前記ブロック高さ値と

第3のしきい値との間の差であり、
前記基準時間パラメータに基づいて、前記ターゲットトランザクションが前記トランザクション有効期間内の前記有効トランザクションであるかどうかを決定することが、
前記基準ブロック高さ値が前記第3の値より大きく、前記ブロックチェーン内の前記候補ブロックの前記ブロック高さ値より小さいかどうかを決定するために、前記基準ブロック高さ値を前記ブロックチェーン内の前記候補ブロックの前記ブロック高さ値および前記第3の値の各々と比較することと、
前記基準ブロック高さ値が前記第3の値より大きく、前記ブロックチェーン内の前記候補ブロックの前記ブロック高さ値より小さいとの決定に応答して、前記ターゲットトランザクションが前記トランザクション有効期間内の有効トランザクションであると決定することとを含む、
請求項６に記載のコンピュータ可読記録媒体。
【請求項８】
前記基準ブロック高さ値を前記ブロックチェーン内の前記候補ブロックの前記ブロック高さ値および前記第3の値の各々と比較する前に、前記動作が、
前記候補ブロックの候補ブロック数が前記ブロックチェーン内の最新ブロックの最新ブロック数より大きいかどうかを決定することと、
前記候補ブロックの前記候補ブロック数が前記ブロックチェーン内の最新ブロックの前記最新ブロック数より大きいとの決定に応答して、前記基準ブロック高さ値を前記ブロックチェーン内の前記候補ブロックの前記ブロック高さ値および前記第3の値の各々と比較することとをさらに含む、
請求項７に記載のコンピュータ可読記録媒体。
【請求項９】
前記ターゲットトランザクションが、前記ターゲットトランザクションの一意の識別子をさらに含み、
前記ターゲットトランザクションが前記トランザクション有効期間内の前記有効トランザクションであるとの決定に応答して、前記ターゲットトランザクションを前記候補ブロックに記録することが、
前記ターゲットトランザクションが前記トランザクション有効期間内の有効トランザクションであるとの決定に応答して、前記ターゲットトランザクションの前記一意の識別子に対応するトランザクション冪等レコードが所定のトランザクション冪等テーブルに記憶されているかどうかを問い合わせることであって、前記所定のトランザクション冪等テーブルが、前記トランザクション有効期間内の有効トランザクションに対応するトランザクション冪等レコードを記憶するために使用される、問い合わせることと、
前記ターゲットトランザクションの前記一意の識別子に対応する前記トランザクション冪等レコードが前記所定のトランザクション冪等テーブルに記憶されていないとの決定に応答して、前記ターゲットトランザクションを前記候補ブロックに記録することとを含む、
請求項８に記載のコンピュータ可読記録媒体。
【請求項１０】
前記トランザクション冪等レコードが、前記トランザクション冪等レコードに対応するトランザクションが前記ブロックチェーンの分散データベースに正常に記録されたことを示し、
前記動作が、
前記ターゲットトランザクションが前記候補ブロックに記録されていると決定され、かつ前記候補ブロックに関するコンセンサスに達し、前記候補ブロックが前記ブロックチェーンの前記分散データベースに正常に記憶されているとの決定に応答して、前記ターゲットトランザクションの前記一意の識別子に対応する前記トランザクション冪等レコードを生成することと、
前記トランザクション冪等レコードを前記所定のトランザクション冪等テーブルに挿

入することとをさらに含む、
請求項９に記載のコンピュータ可読記録媒体。
【請求項１１】
１つ以上のコンピュータと、
相互動作可能に前記１つ以上のコンピュータと結合し、前記１つ以上のコンピュータにより実行されると１つ以上の動作を実行する１つ以上の命令を含む有形な機械可読記録媒体を含む１つ以上のコンピュータメモリデバイス
を含むコンピュータで実行されるシステムであって、
前記動作は、
ブロックチェーン内のメンバーノードデバイスによって開始されたターゲットトランザクションを受信することであって、前記ターゲットトランザクションが、基準時間パラメータを含み、前記基準時間パラメータが前記ターゲットトランザクションが作成されるときに生成される基準タイムスタンプであり、トランザクション有効期間が第1の値と第2の値との間の数値間隔に対応し、前記第1の値が、候補ブロックの作成タイムスタンプから第1のしきい値を差し引いたものであり、前記第2の値が、前記候補ブロックの前記作成タイムスタンプと第2のしきい値の和であり、前記基準時間パラメータは前記ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるかどうかを決定するために使用される、受信することと、
前記基準時間パラメータに基づいて、前記ターゲットトランザクションが前記トランザクション有効期間内の有効トランザクションであるかどうかを決定することであって、前記ターゲットトランザクションが前記トランザクション有効期間内の有効トランザクションであるかどうかを決定することは、
前記基準タイムスタンプが前記第1の値より大きく、前記第2の値より小さいかどうかを決定するために、前記基準タイムスタンプを前記第1の値および前記第2の値の各々と比較することと、
前記基準タイムスタンプが前記第1の値より大きく、前記第2の値より小さいとの決定に応答して、前記ターゲットトランザクションが前記トランザクション有効期間内の有効トランザクションであると決定することと
を含む、決定することと、
前記ターゲットトランザクションが前記トランザクション有効期間内の有効トランザクションであるとの決定に応答して、前記ターゲットトランザクションを生成された候補ブロックに記録することと
を含むシステム。
【請求項１２】
前記基準時間パラメータが、前記ターゲットトランザクションが作成されるときに生成される基準ブロック高さ値であり、
前記トランザクション有効期間が、第3の値と前記ブロックチェーン内の前記候補ブロックのブロック高さ値との間の数値間隔に対応し、
前記第3の値が、前記ブロックチェーン内の前記候補ブロックの前記ブロック高さ値と第3のしきい値との間の差であり、
前記基準時間パラメータに基づいて、前記ターゲットトランザクションが前記トランザクション有効期間内の前記有効トランザクションであるかどうかを決定することが、
前記基準ブロック高さ値が前記第3の値より大きく、前記ブロックチェーン内の前記候補ブロックの前記ブロック高さ値より小さいかどうかを決定するために、前記基準ブロック高さ値を前記ブロックチェーン内の前記候補ブロックの前記ブロック高さ値および前記第3の値の各々と比較することと、
前記基準ブロック高さ値が前記第3の値より大きく、前記ブロックチェーン内の前記候補ブロックの前記ブロック高さ値より小さいとの決定に応答して、前記ターゲットトランザクションが前記トランザクション有効期間内の有効トランザクションであると決定することとを含む、

請求項１１に記載のコンピュータで実行されるシステム。
【請求項１３】
前記基準ブロック高さ値を前記ブロックチェーン内の前記候補ブロックの前記ブロック高さ値および前記第3の値の各々と比較する前に、前記動作が、
前記候補ブロックの候補ブロック数が前記ブロックチェーン内の最新ブロックの最新ブロック数より大きいかどうかを決定することと、
前記候補ブロックの前記候補ブロック数が前記ブロックチェーン内の最新ブロックの前記最新ブロック数より大きいとの決定に応答して、前記基準ブロック高さ値を前記ブロックチェーン内の前記候補ブロックの前記ブロック高さ値および前記第3の値の各々と比較することとをさらに含む、
請求項１２に記載のコンピュータで実行されるシステム。
【請求項１４】
前記ターゲットトランザクションが、前記ターゲットトランザクションの一意の識別子をさらに含み、
前記ターゲットトランザクションが前記トランザクション有効期間内の前記有効トランザクションであるとの決定に応答して、前記ターゲットトランザクションを前記候補ブロックに記録することが、
前記ターゲットトランザクションが前記トランザクション有効期間内の有効トランザクションであるとの決定に応答して、前記ターゲットトランザクションの前記一意の識別子に対応するトランザクション冪等レコードが所定のトランザクション冪等テーブルに記憶されているかどうかを問い合わせることであって、前記所定のトランザクション冪等テーブルが、前記トランザクション有効期間内の有効トランザクションに対応するトランザクション冪等レコードを記憶するために使用される、問い合わせることと、
前記ターゲットトランザクションの前記一意の識別子に対応する前記トランザクション冪等レコードが前記所定のトランザクション冪等テーブルに記憶されていないとの決定に応答して、前記ターゲットトランザクションを前記候補ブロックに記録することとを含む、
請求項１３に記載のコンピュータで実行されるシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
本出願は、その全体が参照により本明細書に組み込まれる、2018年5月29日に出願された中国特許出願第201810531740.6号の優先権を主張する。
【０００２】
本明細書の1つまたは複数の実装形態は、ブロックチェーン技術の分野に関し、より詳細には、ブロックチェーンベースのトランザクション処理方法および装置に関する。
【背景技術】
【０００３】
分散型台帳技術とも呼ばれるブロックチェーン技術は、コンピューティングデバイスが「アカウンティング」に共同で参加し、完全な分散データベースを共同で維持する、新しい技術である。ブロックチェーン技術は、分散化、ならびに公開性および透明性によって特徴付けられる。ブロックチェーン技術では、各コンピューティングデバイスはデータベース記録に参加することができ、データ同期はコンピューティングデバイス間で迅速に実装され得る。上記を考慮して、ブロックチェーン技術は分散システムを確立するために使用され、様々な実行プログラムが自動実行のためにブロックチェーン分散データベースにおいて収集される。ブロックチェーン技術は、様々な分野において広く適用されている。
【発明の概要】
【課題を解決するための手段】
【０００４】

本明細書は、ブロックチェーン内のメンバーノードデバイスによって開始されたターゲットトランザクションを受信するステップであって、ターゲットトランザクションが基準時間パラメータを含み、基準時間パラメータが、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるかどうかを決定するために使用される、ステップと、基準時間パラメータに基づいて、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるかどうかを決定するステップと、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであると決定された場合、ターゲットトランザクションを生成された候補ブロックに記録するステップとを含む、ブロックチェーンベースのトランザクション処理方法を提供する。

【０００５】

任意選択で、基準時間パラメータは、ターゲットトランザクションが作成されるときに生成される基準タイムスタンプであり、トランザクション有効期間は、第1の値と第2の値との間の数値間隔に対応し、第1の値は、候補ブロックの作成タイムスタンプと第1のしきい値との間の差であり、第2の値は、候補ブロックの作成タイムスタンプと第2のしきい値の和であり、基準時間パラメータに基づいて、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるかどうかを決定するステップは、基準タイムスタンプを第1の値および第2の値の各々と比較するステップと、基準タイムスタンプが第1の値より大きく、第2の値より小さい場合、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであると決定するステップとを含む。

【０００６】

任意選択で、基準タイムスタンプを第1の値および第2の値の各々と比較するステップの前に、本方法は、候補ブロックの作成タイムスタンプがブロックチェーン内の最新ブロックの作成タイムスタンプより大きいかどうかをチェックするステップと、そうである場合、基準タイムスタンプを第1の値および第2の値の各々とさらに比較するステップとをさらに含む。

【０００７】

任意選択で、基準タイムスタンプは、ターゲットトランザクションが作成されるときのシステムタイムスタンプ、またはトランザクション作成者によって指定される基準タイムスタンプである。

【０００８】

任意選択で、第1のしきい値は、第2のしきい値より大きい。

【０００９】

任意選択で、基準時間パラメータは、ターゲットトランザクションが作成されるときに生成される基準ブロック高さ値であり、トランザクション有効期間は、第3の値とブロックチェーン内の候補ブロックのブロック高さ値との間の数値間隔に対応し、第3の値は、ブロックチェーン内の候補ブロックのブロック高さ値と第3のしきい値との間の差であり、基準時間パラメータに基づいて、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるかどうかを決定するステップは、基準ブロック高さ値をブロックチェーン内の候補ブロックのブロック高さ値および第3の値の各々と比較するステップと、基準ブロック高さ値が第3の値より大きく、ブロックチェーン内の候補ブロックのブロック高さ値より小さい場合、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであると決定するステップとを含む。

【００１０】

任意選択で、基準ブロック高さ値をブロックチェーン内の候補ブロックのブロック高さ値および第3の値の各々と比較するステップの前に、本方法は、候補ブロックのブロック数がブロックチェーン内の最新ブロックのブロック数より大きいかどうかをチェックするステップと、そうである場合、基準ブロック高さ値をブロックチェーン内の候補ブロックのブロック高さ値および第3の値の各々とさらに比較するステップとをさらに含む。

【００１１】

任意選択で、基準ブロック高さ値は、ターゲットトランザクションが作成されるときの

ブロックチェーン内の最大ブロック高さ値、またはトランザクション作成者によって指定される基準ブロック高さ値である。

【００１２】

任意選択で、ターゲットトランザクションは、ターゲットトランザクションの一意の識別子をさらに含み、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであると決定された場合、ターゲットトランザクションを生成された候補ブロックに記録するステップは、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであると決定された場合、ターゲットトランザクションの一意の識別子に対応するトランザクション冪等レコードが所定のトランザクション冪等テーブルに記憶されているかどうかを問い合わせるステップであって、トランザクション冪等テーブルが、トランザクション有効期間内の有効トランザクションに対応するトランザクション冪等レコードを記憶するために使用される、ステップと、ターゲットトランザクションの一意の識別子に対応するトランザクション冪等レコードが所定のトランザクション冪等テーブルに記憶されていない場合、ターゲットトランザクションを候補ブロックに記録するステップとを含む。

【００１３】

任意選択で、トランザクション冪等レコードは、トランザクション冪等レコードに対応するトランザクションがブロックチェーンの分散データベースに正常に記録されたことを示し、本方法は、ターゲットトランザクションが候補ブロックに記録された場合、候補ブロックに関するコンセンサスに達し、候補ブロックがブロックチェーンの分散データベースに正常に記憶された後に、ターゲットトランザクションの一意の識別子に対応するトランザクション冪等レコードを生成するステップと、トランザクション冪等レコードをトランザクション冪等テーブルに挿入するステップとをさらに含む。

【００１４】

任意選択で、本方法は、トランザクション冪等テーブル内のトランザクション有効期間を過ぎたトランザクションのトランザクション冪等レコードを周期的に削除するステップをさらに含む。

【００１５】

本明細書は、ブロックチェーン内のメンバーノードデバイスによって開始されたターゲットトランザクションを受信するように構成された受信モジュールであって、ターゲットトランザクションが基準時間パラメータを含み、基準時間パラメータが、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるかどうかを決定するために使用される、受信モジュールと、基準時間パラメータに基づいて、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるかどうかを決定するように構成された決定モジュールと、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであると決定された場合、ターゲットトランザクションを生成された候補ブロックに記録するように構成された記録モジュールとを含む、ブロックチェーンベースのトランザクション処理装置をさらに提供する。

【００１６】

任意選択で、基準時間パラメータは、ターゲットトランザクションが作成されるときに生成される基準タイムスタンプであり、トランザクション有効期間は、第1の値と第2の値との間の数値間隔に対応し、第1の値は、候補ブロックの作成タイムスタンプと第1のしきい値との間の差であり、第2の値は、候補ブロックの作成タイムスタンプと第2のしきい値の和であり、決定モジュールは、基準タイムスタンプを第1の値および第2の値の各々と比較し、基準タイムスタンプが第1の値より大きく、第2の値より小さい場合、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであると決定するように構成される。

【００１７】

任意選択で、決定モジュールは、基準タイムスタンプを第1の値および第2の値の各々と比較する前に、候補ブロックの作成タイムスタンプがブロックチェーン内の最新ブロック

の作成タイムスタンプより大きいかどうかをチェックし、そうである場合、基準タイムスタンプを第1の値および第2の値の各々とさらに比較するようにさらに構成される。

【００１８】

任意選択で、基準タイムスタンプは、ターゲットトランザクションが作成されるときのシステムタイムスタンプ、またはトランザクション作成者によって指定される基準タイムスタンプである。

【００１９】

任意選択で、第1のしきい値は、第2のしきい値より大きい。

【００２０】

任意選択で、基準時間パラメータは、ターゲットトランザクションが作成されるときに生成される基準ブロック高さ値であり、トランザクション有効期間は、第3の値とブロックチェーン内の候補ブロックのブロック高さ値との間の数値間隔に対応し、第3の値は、ブロックチェーン内の候補ブロックのブロック高さ値と第3のしきい値との間の差であり、決定モジュールは、基準ブロック高さ値をブロックチェーン内の候補ブロックのブロック高さ値および第3の値の各々と比較し、基準ブロック高さ値が第3の値より大きく、ブロックチェーン内の候補ブロックのブロック高さ値より小さい場合、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであると決定するように構成される。

【００２１】

任意選択で、決定モジュールは、基準ブロック高さ値をブロックチェーン内の候補ブロックのブロック高さ値および第3の値の各々と比較する前に、候補ブロックのブロック数がブロックチェーン内の最新ブロックのブロック数より大きいかどうかをチェックし、そうである場合、基準ブロック高さ値をブロックチェーン内の候補ブロックのブロック高さ値および第3の値の各々とさらに比較するようにさらに構成される。

【００２２】

任意選択で、基準ブロック高さ値は、ターゲットトランザクションが作成されるときのブロックチェーン内の最大ブロック高さ値、またはトランザクション作成者によって指定される基準ブロック高さ値である。

【００２３】

任意選択で、ターゲットトランザクションは、ターゲットトランザクションの一意の識別子をさらに含み、記録モジュールは、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであると決定された場合、ターゲットトランザクションの一意の識別子に対応するトランザクション冪等レコードが所定のトランザクション冪等テーブルに記憶されているかどうかを問い合わせることであって、トランザクション冪等テーブルが、トランザクション有効期間内の有効トランザクションに対応するトランザクション冪等レコードを記憶するために使用される、ことと、ターゲットトランザクションの一意の識別子に対応するトランザクション冪等レコードが所定のトランザクション冪等テーブルに記憶されていない場合、ターゲットトランザクションを候補ブロックに記録することとを行うようにさらに構成される。

【００２４】

任意選択で、トランザクション冪等レコードは、トランザクション冪等レコードに対応するトランザクションがブロックチェーンの分散データベースに正常に記録されたことを示し、記録モジュールは、ターゲットトランザクションが候補ブロックに記録された場合、候補ブロックに関するコンセンサスに達し、候補ブロックがブロックチェーンの分散データベースに正常に記憶された後に、ターゲットトランザクションの一意の識別子に対応するトランザクション冪等レコードを生成し、トランザクション冪等レコードをトランザクション冪等テーブルに挿入するようにさらに構成される。

【００２５】

任意選択で、記録モジュールは、トランザクション冪等テーブル内のトランザクション有効期間を過ぎたトランザクションのトランザクション冪等レコードを周期的に削除する

ようにさらに構成される。

【００２６】

本明細書は、プロセッサと、メモリとを含み、機械実行可能命令を記憶するように構成された電子デバイスをさらに提供し、プロセッサは、ブロックチェーン内のメンバーノードデバイスによって開始されたターゲットトランザクションを受信することであって、ターゲットトランザクションが基準時間パラメータを含み、基準時間パラメータが、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるかどうかを決定するために使用される、ことと、基準時間パラメータに基づいて、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるかどうかを決定することと、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであると決定された場合、ターゲットトランザクションを生成された候補ブロックに記録することとを行うために、メモリに記憶され、ブロックチェーンベースのトランザクション処理制御論理に対応する機械実行可能命令を読み取り、実行する。

【図面の簡単な説明】

【００２７】

【図１】例示的な一実装形態による、ブロックチェーンベースのトランザクション処理方法を示すフローチャートである。

【図２】例示的な一実装形態による電子デバイスを示す概略構造図である。

【図３】例示的な一実装形態による、ブロックチェーンベースのトランザクション処理装置を示すブロック図である。

【図４】本開示の一実装形態による、ブロックチェーンベースのトランザクション処理のためのコンピュータで実行される方法の一例を示すフローチャートである。

【発明を実施するための形態】

【００２８】

本明細書は、ブロックチェーンに送信されるトランザクションに対するトランザクション有効期間を設定し、ブロックチェーン内のノードデバイスがトランザクション有効期間内のトランザクションのみを候補ブロックに記録することができることを保証するための、技術的解決策を提供するものである。

【００２９】

実装時に、ブロックチェーンのオペレータは、ブロックチェーンに送信されるトランザクションに対するトランザクション有効期間を一様に設定することができる。

【００３０】

たとえば、実際の適用例では、トランザクション有効期間は、ブロックチェーン内のノードデバイス(たとえば、「台帳ノード」として働くノードデバイス)が現在のアカウンティング期間内で候補ブロックを作成する作成時点の前の時間期間、または候補ブロックの作成時点の後の時間期間であり得る。

【００３１】

ユーザがクライアントを使用することによってトランザクションを作成するとき、トランザクションが以前のトランザクション有効期間内の有効トランザクションであるかどうかを決定するために使用される基準時間パラメータは、トランザクションに追加され得、次いで、トランザクションは、クライアントによってアクセスされるノードデバイスを使用することによってブロックチェーンに送信される。

【００３２】

トランザクションを受信した後、トランザクションを検証するプロセスにおいて、ブロックチェーン内の別のノードデバイスは、トランザクションにおいて搬送された基準時間パラメータに基づいて、トランザクションがトランザクション有効期間内の有効トランザクションであるかどうかを検証し、トランザクションがトランザクション有効期間内の有効トランザクションとして確認された場合、トランザクションを候補ブロックに記録することができる。

【００３３】

以前の技術的解決策に基づいて、トランザクション有効期間内の有効トランザクションのみが合法のトランザクションとして使用され、候補ブロックに記録され得る一方で、ブロックチェーン内の不法のノードデバイスは、かなり前に不法のノードデバイスによって傍受された期限切れのトランザクションを使用することによってブロックチェーンに対するリプレイ攻撃を開始することを妨げられ、それによって、ブロックチェーンのトランザクションセキュリティレベルを改善し得る。

【００３４】

以下では、適用例シナリオに関する実装形態を使用することによって、本明細書について説明する。

【００３５】

図1は、本明細書の一実装形態による、ブロックチェーンベースのトランザクション処理方法を示す。本方法は、ブロックチェーン内の任意のノードデバイスに適用され、以下のステップを含む。

【００３６】

ステップ102:ブロックチェーン内のメンバーノードデバイスによって開始されたターゲットトランザクションを受信し、ターゲットトランザクションは基準時間パラメータを含み、基準時間パラメータは、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるかどうかを決定するために使用される。

【００３７】

ステップ104:基準時間パラメータに基づいて、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるかどうかを決定する。

【００３８】

ステップ106:ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであると決定された場合、ターゲットトランザクションを生成された候補ブロックに記録する。

【００３９】

本明細書で説明されるブロックチェーンは、プライベートブロックチェーン、パブリックブロックチェーン、コンソーシアムブロックチェーンなどを含むことができる。これは、本明細書において特に限定されない。

【００４０】

たとえば、あるシナリオでは、ブロックチェーンは、サードパーティ支払プラットフォームサーバ、国内銀行サーバ、海外銀行サーバ、およびメンバーデバイスとして働くいくつかのユーザノードデバイスからなる、コンソーシアムブロックチェーンであり得る。コンソーシアムブロックチェーンのオペレータは、コンソーシアムブロックチェーンに基づいて越境移転および資産移転などのオンラインサービスをオンライン展開するために、コンソーシアムブロックチェーンに依拠することができる。

【００４１】

本明細書で説明されるトランザクション(たとえば、越境移転または資産移転など)は、ブロックチェーンのクライアントを使用することによってユーザによって作成され、最終的にブロックチェーンの分散データベースに送信される必要がある1つのデータを示す。

【００４２】

ブロックチェーン内のトランザクションは、狭い意味でのトランザクションおよび広い意味でのトランザクションに分類される。狭い意味でのトランザクションは、ユーザによってブロックチェーンにリリースされた価値移転を示す。たとえば、従来のビットコインブロックチェーンネットワークでは、トランザクションは、ブロックチェーン内のユーザによって開始された移転であり得る。広い意味でのトランザクションは、ユーザによってサービス目的でブロックチェーンにリリースされたサービスデータを示す。たとえば、オペレータは、実際のサービス要件に基づいてコンソーシアムブロックチェーンを作成し、コンソーシアムブロックチェーンに基づいて価値移転とは無関係の(賃貸住宅サービス、車両スケジューリングサービス、保険料決済サービス、クレジットサービス、および医療

サービスなどの)他のタイプのオンラインサービスを展開することができる。このタイプのコンソーシアムブロックチェーンでは、トランザクションは、コンソーシアムブロックチェーン内のユーザによってサービス目的でリリースされたサービスメッセージまたはサービス要求であり得る。

【００４３】

ターゲットトランザクションは、パックされ、候補ブロックに記録される必要がある候補トランザクションであって、他のメンバーノードデバイスによってリリースされた正常に検証された合法のトランザクションからブロックチェーン内の台帳ノードとして働くノードデバイスによって選択される候補トランザクションである。

【００４４】

トランザクション有効期間は、ブロックチェーンに送信されるトランザクションに対する、ブロックチェーンのオペレータによって一様に設定される有効期間である。有効期間内のトランザクションは、有効トランザクションとして使用され、候補ブロックに追加され得る合法のトランザクションと見なされ、さもなければ、有効期間を過ぎたトランザクションは、候補ブロックに追加され得ない無効トランザクションと見なされる。

【００４５】

トランザクション有効期間は、ブロックチェーン内の台帳ノードデバイスが現在のアカウンティング期間内で候補ブロックを作成する作成時点に基づいて設定される時間間隔であり得る。たとえば、トランザクション有効期間は、候補ブロックの作成時点の前の時間期間、または候補ブロックの作成時点の後の時間期間であり得る。ブロックチェーン内の他のノードデバイスによってリリースされた多数のトランザクションを取得するとき、台帳ノードは、トランザクション有効期間に基づいて、合法のトランザクションとして使用され、生成された候補ブロックに追加され得るトランザクションを決定することができる。

【００４６】

基準時間パラメータは、トランザクションに追加され、トランザクションがトランザクション有効期間内の有効トランザクションであるかどうかを決定するために使用される時間パラメータであり得る。収集されたトランザクションに対して検証を実行するとき、トランザクションにおいて搬送された基準時間パラメータによって示される時点を参照して、ブロックチェーン内の台帳ノードは、トランザクションがトランザクション有効期間内の有効トランザクションであるかどうかを決定することができる。

【００４７】

基準時間パラメータは、物理クロックであり得るか、または論理クロックであり得る。

【００４８】

物理クロックは、システムからまたはサードパーティクロックサーバから読み取られるシステムタイムスタンプである。論理クロックは、論理タイムスタンプである。分散システムでは、(トランザクションなどの)イベントの発生順を示すことができる任意の自動的に増加する値は、論理クロックとして使用され得る。

【００４９】

一実装形態では、基準時間パラメータが物理クロックである一例において、基準時間パラメータは、トランザクションに追加された基準タイムスタンプであり得る。これに対応して、この場合、トランザクション有効期間は、第1の値と第2の値との間の数値間隔であり得、第1の値は、候補ブロックの作成時点に対応する作成タイムスタンプと第1のしきい値との間の差であり得、第2の値は、候補ブロックの作成タイムスタンプと第2のしきい値の和であり得る。

【００５０】

たとえば、候補ブロックの作成タイムスタンプがB_{ts}として示され、第1のしきい値がK1として示され、第2のしきい値がK2として示されると想定される。そうすると、トランザクション有効期間は、数値間隔$[B_{ts}-K1,B_{ts}+K2]$を使用することによって示され得る。

【００５１】

第1のしきい値は、トランザクション有効期間が設定されるときに予約されるトランザクション有効性持続時間を示す。第2のしきい値は、トランザクションをリリースするノードデバイスのシステムタイムスタンプと候補ブロックを作成するノードデバイスのシステムタイムスタンプとの間のクロックオフセットを示す。通常、ブロックチェーンネットワークにおいて許容されるクロックオフセットは、実際の適用例では比較的小さい。これを考慮して、トランザクション有効期間が設定されるとき、第2のしきい値は、第1のしきい値より桁違いに小さいしきい値に設定され得る。

【００５２】

たとえば、第1のしきい値は5日に設定され得、第2のしきい値は5分に設定され得る。この場合、候補ブロックを作成する時点の前の5日以内にリリースされたトランザクションと、候補ブロックを作成する時点の後の5分以内にリリースされたトランザクションは両方とも、トランザクション有効期間内の有効トランザクションである。

【００５３】

基準タイムスタンプは、ユーザがクライアントを使用することによってトランザクションを作成するときにユーザによって手動で指定され得るか、またはクライアントによって自動的に追加され得ることに留意する価値がある。

【００５４】

たとえば、ある場合、ユーザがクライアントを使用することによってトランザクションを作成するとき、クライアントは、システムからトランザクションの作成時点を読み取り、次いで、作成時点に対応するタイムスタンプを基準タイムスタンプとして使用し、作成されたトランザクションにタイムスタンプを自動的に追加することができる。別の場合、ユーザは、要件に基づいてトランザクション有効期間内の時点を指定し、次いで、その時点に対応するタイムスタンプを基準タイムスタンプとして使用し、作成されたトランザクションにタイムスタンプを手動で追加することができる。

【００５５】

確かに、実際の適用例では、トランザクションをリリースするノードデバイスのシステムタイムスタンプと候補ブロックを作成するノードデバイスのシステムタイムスタンプとの間のクロックオフセットは、トランザクション有効期間が設定されるときに考慮されないことがある。この場合、トランザクション有効期間は、候補ブロックの作成時点に対応する作成タイムスタンプと第1のしきい値との間の差を表す第1の値と、候補ブロックの作成タイムスタンプとの間の数値間隔であり得る。

【００５６】

たとえば、依然として、候補ブロックの作成タイムスタンプがB_{ts}として示され、第1のしきい値がK1として示されると想定される。そうすると、トランザクション有効期間は、数値間隔$[B_{ts}-K1,B_{ts}]$を使用することによって示され得る。

【００５７】

別の実装形態では、基準時間パラメータが論理クロックである一例において、ブロックチェーン内のブロックのブロック高さは、ブロックチェーンに対応するP2Pネットワークにおける論理クロックとして使用され得る。この場合、基準時間パラメータは、トランザクションに追加された基準ブロック高さ値であり得る。トランザクション有効期間は、ブロックチェーン内の候補ブロックのブロック高さ値と、ブロックチェーン内の候補ブロックのブロック高さ値と第3のしきい値との間の差(第3の値)との間の数値間隔であり得る。

【００５８】

たとえば、ブロックチェーン内の候補ブロックのブロック高さ値がB_hとして示され、第3のしきい値がK3として示されると想定される。そうすると、トランザクション有効期間は、数値間隔$[B_h-K3,B_h]$を使用することによって示され得る。

【００５９】

第3のしきい値は、第1のしきい値と同じ意味を有し、トランザクション有効期間が設定されるときに予約されるトランザクション有効性持続時間を示す。しかしながら、ブロック高さ値がトランザクション有効期間を示すための論理クロックとして使用されるシナリ

オでは、トランザクションをリリースするノードデバイスのシステムタイムスタンプと候補ブロックを作成するノードデバイスのシステムタイムスタンプとの間のクロックオフセットは、考慮されないことがある。したがって、クロックオフセットを示すしきい値は、上記の数値間隔の上限に追加されないことがある。

【００６０】

基準ブロック高さ値は、ユーザがクライアントを使用することによってトランザクションを作成するときにユーザによって手動で指定され得るか、またはクライアントによって自動的に追加され得ることに留意する価値がある。

【００６１】

たとえば、ある場合、ユーザがクライアントを使用することによってトランザクションを作成するとき、クライアントは、システムからトランザクションの作成時点を読み取り、次いで、作成時点でのブロックチェーンにおける最大ブロック高さ値をさらに問い合わせ、作成されたトランザクションに最大ブロック高さ値を自動的に追加することができる。別の場合、ユーザは、要件に基づいてトランザクション有効期間内のブロック高さを指定し、次いで、ブロック高さに対応する値を基準ブロック高さ値として使用し、作成されたトランザクションにその値を手動で追加することができる。

【００６２】

確かに、ブロックチェーン内のブロックのブロック高さを論理クロックとして使用する実装形態に加えて、実際の適用例では、トランザクションの発生順を記述するために使用され得る他のタイプの増加する値も、論理クロックとして使用され得る。これらの値は、本明細書では1つずつ列挙されない。

【００６３】

本明細書では、クライアントを使用することによってユーザによって作成されるトランザクションは、ユーザによって保持される秘密鍵に基づいて署名され得、次いで、トランザクションは、クライアントによってアクセスされるノードデバイスを使用することによって、ブロックチェーンのP2Pネットワークにおいてブロードキャストおよびリリースされる。台帳ノードとして働くノードデバイスは、別のノードデバイスによってブロードキャストおよびリリースされたトランザクションを収集し、収集されたトランザクションを確認なしの(unacknowledged)トランザクションとして使用し、収集されたトランザクションをローカルトランザクションプール(メモリプールとも呼ばれる)に記憶することができる。

【００６４】

さらに、台帳ノードとして働くノードデバイスは、現在のアカウンティング期間内で候補ブロックを作成し、トランザクションプール内のトランザクションに対して合法の検証を実行し、合法の検証に合格したトランザクションを候補トランザクションとして使用し、そのトランザクションを作成された候補ブロックに記録することができる。

【００６５】

実際の適用例では、トランザクションプール内のトランザクションに対して検証を実行することは、トランザクションの発行者に対するアイデンティティ認証およびトランザクションコンテンツに対するチェックを含むことができる。トランザクションコンテンツに対するチェックは、トランザクションコンテンツに対する整合性チェックをさらに含むことができる。

【００６６】

実装時に、トランザクションが署名されるとき、一般に、コンテンツ要約(たとえば、ハッシュ値)を取得するために、トランザクションに対して計算が実行され得、次いで、デジタル署名を取得するために、保持された秘密鍵に基づいてコンテンツ要約が暗号化され得る。署名されたトランザクションを受信した後、台帳ノードとして働くノードデバイスは、トランザクションが署名されたときに使用された秘密鍵に基づいてデジタル署名を解読することができる。ノードデバイスが解読に成功した場合、それは、トランザクションをリリースするユーザのアイデンティティ認証が成功し、トランザクションがユーザに

よってリリースされた合法のトランザクションであることを示す。

【００６７】

加えて、台帳ノードとして働くノードデバイスは、コンテンツ要約を取得するために、トランザクションに対して再計算をさらに実行し、次いで、再計算されたコンテンツ要約を、デジタル署名を解読することによって取得された元のコンテンツ要約と照合することができる。コンテンツ要約が元のコンテンツ要約と一致する場合、それは、トランザクションコンテンツに対する整合性チェックが成功し、トランザクションのトランザクションコンテンツがトランザクション送信プロセス中に不法に改ざんされていないことを示す。

【００６８】

本明細書では、トランザクションプール内のトランザクションの発行者に対するアイデンティティ認証およびトランザクションコンテンツに対する検証に加えて、トランザクションにおいて搬送された基準時間パラメータに基づいて、トランザクションプール内のトランザクションがトランザクション有効期間内の有効トランザクションであるかどうかがさらに検証される。発行者に対するアイデンティティ認証とトランザクションコンテンツに対する検証の両方に合格したトランザクションプール内のトランザクションについて、このタイプのトランザクションにおいて搬送された基準時間パラメータに基づいて、トランザクションプール内のトランザクションがトランザクション有効期間内の有効トランザクションであるかどうかがさらに検証され得る。

【００６９】

図示の実装形態では、基準時間パラメータが、トランザクションに追加された基準タイムスタンプであり、T_{ts}として示され、トランザクション有効期間が、候補ブロックの作成時点に対応する作成タイムスタンプB_{ts}と第1のしきい値K1との間の差と、候補ブロックの作成タイムスタンプB_{ts}と第2のしきい値K2の和との間の数値間隔$[B_{ts}-K1,B_{ts}+K2]$であると想定される。

【００７０】

この場合、台帳ノードとして働くノードデバイスは、作成された候補ブロックの作成タイムスタンプB_{ts}がブロックチェーン内の最新ブロックの作成タイムスタンプより大きいかどうかをチェックするために、作成された候補ブロックの作成タイムスタンプに対して単調増加チェックを最初に実行することができる。そうである場合、それは、候補ブロックが、ブロックチェーン内のブロックの作成タイムスタンプが単調増加するという特徴を満たし、候補ブロックが合法のブロックであることを示す。

【００７１】

候補ブロックが単調増加チェックに合格した後、台帳ノードとして働くノードデバイスは、トランザクションから基準タイムスタンプT_{ts}をさらに読み取り、読み取られた基準タイムスタンプT_{ts}を$B_{ts}-K1$および$B_{ts}+K2$の各々と比較することができる。T_{ts}が$B_{ts}-K1$より大きく、$B_{ts}+K2$より小さい場合、トランザクションは、トランザクション有効期間内の有効トランザクションとして決定され得る。

【００７２】

図示の実装形態では、基準時間パラメータが、トランザクションに追加された基準ブロック高さ値であり、T_hとして示され、トランザクション有効期間が、ブロックチェーン内の候補ブロックのブロック高さ値B_hと第3のしきい値K3との間の差と、ブロックチェーン内の候補ブロックのブロック高さ値B_hとの間の数値間隔$[B_h-K3,B_h]$であると想定される。

【００７３】

この場合、台帳ノードとして働くノードデバイスは、作成された候補ブロックのブロック数がブロックチェーン内の最新ブロックのブロック数より大きいかどうかをチェックするために、作成された候補ブロックのブロック数に対して単調増加チェックを最初に実行することができる。そうである場合、それは、候補ブロックが、ブロックチェーン内のブロックのブロック数が単調増加するという特徴を満たし、候補ブロックが合法のブロックであることを示す。

【００７４】

候補ブロックが単調増加チェックに合格した後、台帳ノードとして働くノードデバイスは、トランザクションから基準ブロック高さ値T_hをさらに読み取り、読み取られた基準ブロック高さ値T_hをB_h-K3およびB_hの各々と比較することができる。T_hがB_h-K3より大きく、B_hより小さい場合、トランザクションは、トランザクション有効期間内の有効トランザクションとして決定され得る。

【００７５】

本明細書では、発行者に対するアイデンティティ認証およびトランザクションプール内のトランザクションコンテンツに対する検証に合格したトランザクション、ならびにトランザクションに対する合法の検証に合格したトランザクションは、候補トランザクションとして使用され、次いで、パックされ、作成された候補ブロックに記録され得る。

【００７６】

たとえば、台帳ノードとして働くノードデバイスは、候補トランザクションとして、合法の検証に合格したすべてのトランザクションを使用し、これらのトランザクションを候補ブロックに記録するか、または、候補トランザクションとして、一定の原理に基づいて(たとえば、トランザクションの優先順位に基づいて)、合法の検証に合格したすべてのトランザクションからいくつかのトランザクションを選択し、これらのトランザクションを候補ブロックに記録することができる。

【００７７】

本方法では、トランザクション有効期間内の有効トランザクションのみが合法のトランザクションとして使用され、候補ブロックに記録され得る一方で、かなり前に期限切れになったトランザクションは、後続のトランザクション実行のために候補ブロックに記録されることが不可能であり、その結果、ブロックチェーン内の不法のノードデバイスは、かなり前に不法のノードデバイスによって傍受された期限切れのトランザクションを使用することによってブロックチェーンに対するリプレイ攻撃を開始することを妨げられ、それによって、ブロックチェーンのトランザクションセキュリティレベルを改善し得る。

【００７８】

本明細書では、台帳ノードとして働くノードデバイスのトランザクション実行環境は、マルチインスタンス実行環境であり得る(たとえば、同じトランザクションクライアントは、トランザクションを同時に開始することができる複数のスレッドを可能にする)。マルチインスタンス実行環境では、同じトランザクションは、同じノードデバイスの異なるインスタンスによって繰り返しサブミットされ得る。したがって、ブロックチェーンにおけるトランザクション実行中に「冪等」問題が存在し得る。「冪等」問題は、同じトランザクションが繰り返し実行された後でユーザに悪影響がもたらされることを意味する。

【００７９】

たとえば、ビットコインネットワークにおける「二重支払い」(double spending)問題は、典型的な「冪等」問題である。ユーザの秘密鍵を使用することによって署名された移転トランザクションは、不法のノードによって傍受される。トランザクションが実行された後、不法のノードは、傍受されたトランザクションに基づいてリプレイ攻撃を開始し、ブロックチェーンにおいてトランザクションを繰り返し実行することができる。結果として、同じ資金移転が複数回実行され、ユーザに資金損失をもたらす。

【００８０】

これを考慮して、マルチインスタンス実行環境におけるトランザクションの繰り返される実行を低減するために、ブロックチェーン内の台帳ノードとして働くノードデバイスは、トランザクション冪等テーブルを共同で維持することができる。たとえば、台帳ノードとして働くノードデバイスは、ブロックチェーンの既存のコンセンサス機構を使用することによって、コンセンサス手順の後で取得されたトランザクション冪等テーブルを共同で維持することができる。

【００８１】

トランザクション冪等テーブルは、トランザクション有効期間内の有効トランザクションを記録するブロックチェーン内の分散データのストレージレコード(言い換えれば、ブ

ロックレコード)に基づいて作成されるインデックスレコードテーブルであり、ブロックチェーンの分散データベースに正常に記録されたすべての有効トランザクションに対応するトランザクション冪等レコードを記憶するために使用される。

【００８２】

言い換えれば、トランザクション冪等テーブルに記憶されたトランザクション冪等レコードは、トランザクション冪等レコードに対応するトランザクションが候補ブロックに正常にパックされたことを示すために使用され、候補ブロックに関するコンセンサスに達した後、候補ブロックは、最終的にブロックチェーン内の最新ブロックとして使用され、ブロックチェーン内の分散データベース(言い換えれば、分散型台帳)に正常に追加され得る。

【００８３】

有効トランザクションを候補ブロックに記録する前に、台帳ノードとして働くノードデバイスは、トランザクションがブロックチェーンの分散データベースに正常に記録された複製トランザクションであるかどうかを決定するために、トランザクション冪等テーブルに基づいてトランザクションに対して冪等チェックをさらに実行することができる。

【００８４】

図示の実装形態では、上記で説明された基準時間パラメータに加えて、クライアントを使用することによってユーザによって作成されたトランザクションは、トランザクションについてのクライアントによって作成された一意の識別子をさらに搬送することができる。

【００８５】

たとえば、実際の適用例では、ブロックチェーン内のノードデバイスは、複数のインスタンスで構成されたノードデバイスであり得、各インスタンスは、一意のインスタンスIDを有する。この場合、トランザクションシリアル番号は、インスタンスIDと生成された乱数とを含む一意のトランザクションシリアル番号であり得る。

【００８６】

別の例として、ブロックチェーン内のノードデバイスは、複数のデバイスを含む分散デバイスであり、各デバイスは、一意のデバイス識別子(たとえば、デバイスIDまたはデバイスのIPアドレス)を有する。この場合、トランザクションシリアル番号は、デバイス識別子と生成された乱数とを含む一意のトランザクションシリアル番号であり得る。

【００８７】

収集されたトランザクションがトランザクション有効期間内の有効トランザクションであると決定した後、台帳ノードとして働くノードデバイスは、トランザクションの一意の識別子に対応するトランザクション冪等レコードがトランザクション冪等テーブルに記憶されているかどうかをさらに問い合わせることができる。

【００８８】

トランザクションの一意の識別子に対応するトランザクション冪等レコードがトランザクション冪等テーブルに記憶されている場合、それは、トランザクションが以前にブロックチェーンの分散データベースに正常に記録されており、トランザクションが繰り返し開始されるトランザクションであることを示す。この場合、トランザクションは、直接破棄され得る。

【００８９】

しかしながら、トランザクションの一意の識別子に対応するトランザクション冪等レコードがトランザクション冪等テーブルに記憶されていない場合、それは、トランザクションが以前にブロックチェーンの分散データベースに正常に記録されていないことを示す。この場合、ノードデバイスは、トランザクションを候補ブロックに記録することができる。

【００９０】

本明細書では、候補ブロックが生成された後、台帳ノードとして働くノードデバイスは、ブロックチェーン内の生成された候補ブロックをさらにブロードキャストおよびリリー

スし、ブロックチェーンによってサポートされるコンセンサスアルゴリズムに基づいて、ブロックチェーン内の候補ブロックに記録されたトランザクションに対するコンセンサス処理を開始して、アカウンティング許可を求めて「競合する」ことができる。

【００９１】

ブロックチェーンにおいてサポートされるコンセンサスアルゴリズムのタイプは、本明細書では限定されない。実際の適用例では、コンセンサスアルゴリズムは、プルーフオブワーク(PoW:proof of work)およびPBFTアルゴリズムなどの標準のコンセンサスアルゴリズムであり得るか、または実際のサービス要件に基づいてブロックチェーンのオペレータによってカスタマイズされ得る。

【００９２】

候補ブロックに関するコンセンサスに達し、台帳ノードとして働くノードデバイスがアカウンティング許可を取得した後、候補ブロックは、ブロックチェーン内の最新ブロックとして使用され、ブロックチェーンの分散データベース(言い換えれば、分散型台帳)に追加され得る。この場合、候補ブロックは、ブロックチェーン内のブロックとして使用され、ブロックチェーンに恒久的に記憶される。

【００９３】

加えて、ノードデバイスのトランザクション実行環境では、ノードデバイスは、トランザクションにおいて搬送されたトランザクションコンテンツに基づいて、コンセンサスを取得し、候補ブロックに記録されたトランザクションの実行をトリガすることができる。たとえば、これらのトランザクションは、ブロックチェーンに送信されたスマートコントラクトへの入力として使用され得る。ノードデバイスのトランザクション実行環境におけるトランザクションの実行を完了するために、スマートコントラクトを請求するトランザクション実行プログラムコード(たとえば、トランザクションに関するいくつかの関数呼び出し)が実行される。

【００９４】

図示の実装形態では、ターゲットトランザクションは、候補ブロックに正常に記録され、候補ブロックに関するコンセンサスに達した後、候補ブロックは、最終的にブロックチェーン内の最新ブロックとして使用され、ブロックチェーンの分散データベースに正常に記憶される。この場合、ターゲットトランザクションは、ブロックチェーンの分散データベースに正常に記憶されている(言い換えれば、トランザクションは正常にチェイニングされる)。ターゲットトランザクションの一意の識別子に対応するトランザクション冪等レコードがさらに生成され得、トランザクション冪等レコードがトランザクション冪等テーブルに挿入される。

【００９５】

トランザクション冪等レコードのフォーマットは、本明細書では限定されない。たとえば、ある方法では、トランザクション冪等レコードは、トランザクションの一意の識別子を含むデータレコードであり得る。代替的に、別の方法では、トランザクションの一意の識別子は、トランザクション冪等レコードとして直接使用され、トランザクション冪等テーブルに挿入され得る。

【００９６】

本方法では、トランザクション冪等テーブル内のトランザクション冪等レコードは、トランザクション有効期間内のすべての「有効トランザクション」のトランザクション冪等レコードのみをカバーしており、トランザクション有効期間の前の履歴トランザクションのトランザクション冪等レコードをカバーすることを必要としない。したがって、トランザクション冪等テーブルは非常に大きい記憶空間を消費せず、トランザクション冪等テーブルによって消費される非常に大きい記憶空間によって引き起こされる問合せ性能問題は存在しない。

【００９７】

たとえば、台帳ノードとして使用され得る任意のノードデバイスについて、トランザクション冪等テーブルは比較的小さい記憶空間を占めるので、トランザクション冪等テーブ

ルは、サードパーティ記憶ディスクを使用することによって記憶される代わりに、デバイスのメモリに直接ロードされ、維持され得る。トランザクション冪等テーブルの問合せ動作は、メモリにおいて直接実行され、それによって、問合せ性能を大幅に改善し得る。

【００９８】

加えて、すべての有効トランザクションについて、トランザクション冪等テーブル内にトランザクション冪等レコードを有しないそれらのトランザクションのみが候補ブロックに正常に記録され得る。したがって、ブロックチェーン内のトランザクション実行中の「冪等」問題が緩和され得、トランザクション有効期間内の傍受された有効トランザクションを使用することによっていくつかの不法のノードによって開始されたプレイバック攻撃が効果的に妨げられ、それによって、同じ有効トランザクションの繰り返される実行を低減することができる。

【００９９】

加えて、複数のインスタンスがブロックチェーン内のノードデバイス用に構成されるか、またはノードデバイスが分散デバイスであるシナリオでは、同じトランザクションの繰り返される実行という以下の問題も、効果的に緩和され得る。すなわち、同じ有効トランザクションは、異なるインスタンスまたは分散デバイス内の異なるサブデバイスによって同時にリリースされる。

【０１００】

本明細書では、トランザクション冪等テーブルは、トランザクション有効期間内の「有効トランザクション」に対応するトランザクション冪等レコードを維持するために使用されるので、実際の適用例では、トランザクション冪等テーブルを共同で維持するメンバーノードデバイスは、削除処理を周期的に実行して、トランザクション有効期間を過ぎたトランザクションのトランザクション冪等レコードをトランザクション冪等テーブルから削除することができる。

【０１０１】

たとえば、トランザクション有効期間は、現在のアカウンティング期間におけるブロックチェーン内の台帳ノードデバイスによって作成された候補ブロックの作成時点に基づいて設定される時間間隔である。候補ブロックが周期的に作成されるので、トランザクション有効期間も、周期的で動的な時間期間である。この場合、次のアカウンティング期間において新しい候補ブロックを作成するとき、ノードデバイスは、トランザクション有効期間を再決定し、次いで、再決定されたトランザクション有効期間を過ぎたトランザクションのトランザクション冪等レコードを求めてトランザクション冪等テーブルをアクティブに検索することができる。たとえば、トランザクションが再決定されたトランザクション有効期間外にあるかどうかは、依然として、トランザクション内の基準時間パラメータに基づいて決定され得る。特定の実装プロセスは、ここでは省略される。

【０１０２】

さらに、これらの見つかったトランザクション冪等レコードは、トランザクション冪等テーブルにおいて維持されるトランザクション冪等レコードを動的に更新および維持するために削除され得る。これは、トランザクション冪等テーブル内のトランザクション冪等レコードがすべて、現在のトランザクション有効期間内の有効トランザクションに対応するトランザクション冪等レコードであることを保証する。

【０１０３】

本出願は、前述の方法の実装形態に対応するブロックチェーンベースのトランザクション処理装置の実装形態をさらに提供する。本明細書におけるブロックチェーンベースのトランザクション処理装置の実装形態は、電子デバイスに適用され得る。装置の実装形態は、ソフトウェア、ハードウェア、またはハードウェアとソフトウェアの組合せによって実装され得る。ソフトウェア実装形態が一例として使用される。論理装置として、本装置は、本装置が配置される電子デバイスのプロセッサによって不揮発性メモリ内の対応するコンピュータプログラム命令をメモリに読み出すことによって形成される。ハードウェアの観点では、図2は、本明細書による、ブロックチェーンベースのトランザクション処理装

置が配置される電子デバイスを示すハードウェア構造図である。図2に示されたプロセッサ、メモリ、ネットワークインターフェース、および不揮発性メモリに加えて、本実装形態における装置が配置される電子デバイスは、通常、電子デバイスの実際の機能に基づいて他のハードウェアを含むことができる。簡単にするために、詳細はここでは省略される。

【０１０４】

図3は、本明細書の例示的な一実装形態による、ブロックチェーンベースのトランザクション処理装置を示すブロック図である。

【０１０５】

図3を参照すると、ブロックチェーンベースのトランザクション処理装置30は、図2に示された電子デバイスに適用され得、受信モジュール301と、決定モジュール302と、記録モジュール303とを含む。

【０１０６】

受信モジュール301は、ブロックチェーン内のメンバーノードデバイスによって開始されたターゲットトランザクションを受信するように構成され、ターゲットトランザクションは基準時間パラメータを含み、基準時間パラメータは、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるかどうかを決定するために使用される。

【０１０７】

決定モジュール302は、基準時間パラメータに基づいて、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるかどうかを決定するように構成される。

【０１０８】

記録モジュール303は、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであると決定された場合、ターゲットトランザクションを生成された候補ブロックに記録するように構成される。

【０１０９】

本実装形態では、基準時間パラメータは、ターゲットトランザクションが作成されるときに生成される基準タイムスタンプであり、トランザクション有効期間は、第1の値と第2の値との間の数値間隔に対応し、第1の値は、候補ブロックの作成タイムスタンプと第1のしきい値との間の差であり、第2の値は、候補ブロックの作成タイムスタンプと第2のしきい値の和であり、決定モジュール302は、基準タイムスタンプを第1の値および第2の値の各々と比較し、基準タイムスタンプが第1の値より大きく、第2の値より小さい場合、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであると決定するように構成される。

【０１１０】

本実装形態では、決定モジュール302は、基準タイムスタンプを第1の値および第2の値の各々と比較する前に、候補ブロックの作成タイムスタンプがブロックチェーン内の最新ブロックの作成タイムスタンプより大きいかどうかをチェックし、そうである場合、基準タイムスタンプを第1の値および第2の値の各々とさらに比較するようにさらに構成される。

【０１１１】

本実装形態では、基準タイムスタンプは、ターゲットトランザクションが作成されるときのシステムタイムスタンプ、またはトランザクション作成者によって指定される基準タイムスタンプである。

【０１１２】

本実装形態では、第1のしきい値は、第2のしきい値より大きい。

【０１１３】

本実装形態では、基準時間パラメータは、ターゲットトランザクションが作成されるときに生成される基準ブロック高さ値であり、トランザクション有効期間は、第3の値とブ

ロックチェーン内の候補ブロックのブロック高さ値との間の数値間隔に対応し、第3の値は、ブロックチェーン内の候補ブロックのブロック高さ値と第3のしきい値との間の差であり、決定モジュール302は、基準ブロック高さ値をブロックチェーン内の候補ブロックのブロック高さ値および第3の値の各々と比較し、基準ブロック高さ値が第3の値より大きく、ブロックチェーン内の候補ブロックのブロック高さ値より小さい場合、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであると決定するように構成される。

【０１１４】

本実装形態では、決定モジュール302は、基準ブロック高さ値をブロックチェーン内の候補ブロックのブロック高さ値および第3の値の各々と比較する前に、候補ブロックのブロック数がブロックチェーン内の最新ブロックのブロック数より大きいかどうかをチェックし、そうである場合、基準ブロック高さ値をブロックチェーン内の候補ブロックのブロック高さ値および第3の値の各々とさらに比較するようにさらに構成される。

【０１１５】

本実装形態では、基準ブロック高さ値は、ターゲットトランザクションが作成されるときのブロックチェーン内の最大ブロック高さ値、またはトランザクション作成者によって指定される基準ブロック高さ値である。

【０１１６】

本実装形態では、ターゲットトランザクションは、ターゲットトランザクションの一意の識別子をさらに含み、記録モジュール303は、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであると決定された場合、ターゲットトランザクションの一意の識別子に対応するトランザクション冪等レコードが所定のトランザクション冪等テーブルに記憶されているかどうかを問い合わせることであって、トランザクション冪等テーブルが、トランザクション有効期間内の有効トランザクションに対応するトランザクション冪等レコードを記憶するために使用される、ことと、ターゲットトランザクションの一意の識別子に対応するトランザクション冪等レコードが所定のトランザクション冪等テーブルに記憶されていない場合、ターゲットトランザクションを候補ブロックに記録するようにさらに構成される。

【０１１７】

本実装形態では、トランザクション冪等レコードは、トランザクション冪等レコードに対応するトランザクションがブロックチェーンの分散データベースに正常に記録されたことを示し、記録モジュール303は、ターゲットトランザクションが候補ブロックに記録された場合、候補ブロックに関するコンセンサスに達し、候補ブロックがブロックチェーンの分散データベースに正常に記憶された後に、ターゲットトランザクションの一意の識別子に対応するトランザクション冪等レコードを生成し、トランザクション冪等レコードをトランザクション冪等テーブルに挿入するようにさらに構成される。

【０１１８】

本実装形態では、記録モジュール303は、トランザクション冪等テーブル内のトランザクション有効期間を過ぎたトランザクションのトランザクション冪等レコードを周期的に削除するようにさらに構成される。

【０１１９】

装置におけるモジュールの機能および役割の実装プロセスについて、前述の方法における対応するステップの実装プロセスが参照され得る。簡単にするために、詳細はここでは省略される。

【０１２０】

装置の実装形態は、基本的に、方法の実装形態に対応する。関連する部分について、方法の実装形態における関連する説明が参照され得る。以前に説明された装置の実装形態は、一例にすぎない。別個のコンポーネントとして説明されるモジュールは、物理的に別個であってもよく、そうでなくてもよく、モジュールとして表示されるコンポーネントは、物理モジュールであってもよく、そうでなくてもよく、言い換えれば、コンポーネントは

、1つの位置に配置される場合があるか、または複数のネットワークモジュール上に分散される場合がある。モジュールのいくつかまたはすべては、本明細書の解決策の目的を達成するために、実際の要件に基づいて選択される場合がある。当業者は、創造的な努力なしに本明細書の解決策を理解し、実装することができる。

【０１２１】

前述の実装形態に例示されたシステム、装置、またはモジュールは、コンピュータチップもしくはエンティティを使用することによって実装され得るか、または一定の機能を有する製品を使用することによって実装され得る。典型的な実装デバイスは、コンピュータである。コンピュータは、パーソナルコンピュータ、ラップトップコンピュータ、セルラーフォン、カメラフォン、スマートフォン、携帯情報端末、メディアプレーヤ、ナビゲーションデバイス、電子メール送受信デバイス、ゲームコンソール、タブレットコンピュータ、ウェアラブルデバイス、またはこれらのデバイスの任意の組合せであり得る。

【０１２２】

本出願は、前述の方法の実装形態に対応する電子デバイスの実装形態をさらに提供する。電子デバイスは、プロセッサと、機械実行可能命令を記憶するように構成されたメモリとを含む。プロセッサおよびメモリは、一般に、内部バスを使用することによって互いに接続される。別の可能な実装形態では、デバイスは、別のデバイスまたはコンポーネントと通信するために、外部インターフェースをさらに含むことができる。

【０１２３】

本実装形態では、プロセッサは、ブロックチェーン内のメンバーノードデバイスによって開始されたターゲットトランザクションを受信することであって、ターゲットトランザクションが基準時間パラメータを含み、基準時間パラメータが、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるかどうかを決定するために使用される、ことと、基準時間パラメータに基づいて、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるかどうかを決定することと、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであると決定された場合、ターゲットトランザクションを生成された候補ブロックに記録することとを行うために、メモリに記憶され、ブロックチェーンベースのトランザクション処理制御論理に対応する機械実行可能命令を読み取り、実行する。

【０１２４】

本実装形態では、基準時間パラメータは、ターゲットトランザクションが作成されるときに生成される基準タイムスタンプであり、トランザクション有効期間は、第1の値と第2の値との間の数値間隔に対応し、第1の値は、候補ブロックの作成タイムスタンプと第1のしきい値との間の差であり、第2の値は、候補ブロックの作成タイムスタンプと第2のしきい値の和であり、プロセッサは、基準タイムスタンプを第1の値および第2の値の各々と比較し、基準タイムスタンプが第1の値より大きく、第2の値より小さい場合、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであると決定するために、メモリに記憶され、ブロックチェーンベースのトランザクション処理制御論理に対応する機械実行可能命令を読み取り、実行する。

【０１２５】

本実装形態では、プロセッサは、基準タイムスタンプを第1の値および第2の値の各々と比較する前に、候補ブロックの作成タイムスタンプがブロックチェーン内の最新ブロックの作成タイムスタンプより大きいかどうかをチェックし、そうである場合、基準タイムスタンプを第1の値および第2の値の各々とさらに比較するために、メモリに記憶され、ブロックチェーンベースのトランザクション処理制御論理に対応する機械実行可能命令を読み取り、実行する。

【０１２６】

本実装形態では、基準時間パラメータは、ターゲットトランザクションが作成されるときに生成される基準ブロック高さ値であり、トランザクション有効期間は、第3の値とブロックチェーン内の候補ブロックのブロック高さ値との間の数値間隔に対応し、第3の値

は、ブロックチェーン内の候補ブロックのブロック高さ値と第3のしきい値との間の差であり、プロセッサは、基準ブロック高さ値をブロックチェーン内の候補ブロックのブロック高さ値および第3の値の各々と比較し、基準ブロック高さ値が第3の値より大きく、ブロックチェーン内の候補ブロックのブロック高さ値より小さい場合、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであると決定するために、メモリに記憶され、ブロックチェーンベースのトランザクション処理制御論理に対応する機械実行可能命令を読み取り、実行する。

【０１２７】

本実装形態では、プロセッサは、基準ブロック高さ値をブロックチェーン内の候補ブロックのブロック高さ値および第3の値の各々と比較する前に、候補ブロックのブロック数がブロックチェーン内の最新ブロックのブロック数より大きいかどうかをチェックし、そうである場合、基準ブロック高さ値をブロックチェーン内の候補ブロックのブロック高さ値および第3の値の各々とさらに比較するために、メモリに記憶され、ブロックチェーンベースのトランザクション処理制御論理に対応する機械実行可能命令を読み取り、実行する。

【０１２８】

本実装形態では、ターゲットトランザクションは、ターゲットトランザクションの一意の識別子をさらに含み、プロセッサは、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであると決定された場合、ターゲットトランザクションの一意の識別子に対応するトランザクション冪等レコードが所定のトランザクション冪等テーブルに記憶されているかどうかを問い合わせることであって、トランザクション冪等テーブルが、トランザクション有効期間内の有効トランザクションに対応するトランザクション冪等レコードを記憶するために使用される、ことと、ターゲットトランザクションの一意の識別子に対応するトランザクション冪等レコードが所定のトランザクション冪等テーブルに記憶されていない場合、ターゲットトランザクションを候補ブロックに記録することとを行うために、メモリに記憶され、ブロックチェーンベースのトランザクション処理制御論理に対応する機械実行可能命令を読み取り、実行する。

【０１２９】

本実装形態では、トランザクション冪等レコードは、トランザクション冪等レコードに対応するトランザクションがブロックチェーンの分散データベースに正常に記録されたことを示し、プロセッサは、ターゲットトランザクションが候補ブロックに記録された場合、候補ブロックに関するコンセンサスに達し、候補ブロックがブロックチェーンの分散データベースに正常に記憶された後に、ターゲットトランザクションの一意の識別子に対応するトランザクション冪等レコードを生成し、トランザクション冪等レコードをトランザクション冪等テーブルに挿入するために、メモリに記憶され、ブロックチェーンベースのトランザクション処理制御論理に対応する機械実行可能命令を読み取り、実行する。

【０１３０】

本実装形態では、プロセッサは、トランザクション冪等テーブル内のトランザクション有効期間を過ぎたトランザクションのトランザクション冪等レコードを周期的に削除するために、メモリに記憶され、ブロックチェーンベースのトランザクション処理制御論理に対応する機械実行可能命令を読み取り、実行する。

【０１３１】

当業者は、本明細書について熟考し、ここで本開示を実践した後に、本明細書の別の実装形態を容易に見つけ出すことができる。本明細書は、本明細書の任意の変形形態、使用形態、または適応形態をカバーするものである。これらの変形形態、使用形態、または適応形態は、本明細書の一般原理に従い、本明細書の技術分野に開示されていない一般常識または従来の技法を含む。本明細書および実装形態は、例と見なされるにすぎない。本明細書の実際の範囲および趣旨は、以下の特許請求の範囲によって指摘される。

【０１３２】

本明細書は、上記で説明され、図面に示された厳密な構造に限定されず、本明細書の範

囲から逸脱することなく様々な修正および変更が加えられ得ることを理解されたい。本明細書の範囲は、添付の特許請求の範囲のみによって限定される。

【０１３３】

前述の説明は、本明細書の好ましい実装形態にすぎず、本明細書を限定するものではない。本明細書の趣旨および原理から逸脱することなく行われる任意の修正、同等の置換、または改善は、本明細書の保護範囲内に入るものとする。

【０１３４】

図4は、本開示の一実装形態による、ブロックチェーンベースのトランザクション処理のためのコンピュータで実行される方法400の一例を示すフローチャートである。提示を明確にするために、以下の説明では、概して、本明細書の他の図に照らして方法400について説明する。しかしながら、方法400は、必要に応じて、たとえば、任意のシステム、環境、ソフトウェア、およびハードウェア、またはシステム、環境、ソフトウェア、およびハードウェアの組合せによって実行され得ることを理解されたい。いくつかの実装形態では、方法400の様々なステップは、並行して、組み合わせて、ループで、または任意の順序で実行され得る。

【０１３５】

402において、ブロックチェーン内のメンバーノードデバイスによって開始されたターゲットトランザクションが受信され、ターゲットトランザクションは基準時間パラメータを含み、ターゲットトランザクションは、資産の移転と、候補ブロックへの移転のためにメンバーノードデバイスによってブロックチェーンにリリースされた関連するデータとを示す。

【０１３６】

いくつかの実装形態では、基準時間パラメータは、ターゲットトランザクションが作成されるときに生成される基準タイムスタンプであり、トランザクション有効期間は、第1の値と第2の値との間の数値間隔に対応し、第1の値は、候補ブロックの作成タイムスタンプと第1のしきい値との間の差であり、第2の値は、候補ブロックの作成タイムスタンプと第2のしきい値の和である。

【０１３７】

いくつかの実装形態では、基準時間パラメータは、ターゲットトランザクションが作成されるときに生成される基準ブロック高さ値であり、トランザクション有効期間は、第3の値とブロックチェーン内の候補ブロックのブロック高さ値との間の数値間隔に対応し、第3の値は、ブロックチェーン内の候補ブロックのブロック高さ値と第3のしきい値との間の差であり、基準時間パラメータに基づいて、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるかどうかを決定することは、1)基準ブロック高さ値をブロックチェーン内の候補ブロックのブロック高さ値および第3の値の各々と比較して、基準ブロック高さ値が第3の値より大きく、ブロックチェーン内の候補ブロックのブロック高さ値より小さいかどうかを決定することと、2)基準ブロック高さ値が第3の値より大きく、ブロックチェーン内の候補ブロックのブロック高さ値より小さいとの決定に応答して、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであると決定することとを含む。

【０１３８】

いくつかの実装形態では、ターゲットトランザクションは、ターゲットトランザクションの一意の識別子をさらに含み、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるとの決定に応答して、ターゲットトランザクションを候補ブロックに記録することは、1)ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるとの決定に応答して、ターゲットトランザクションの一意の識別子に対応するトランザクション冪等レコードが所定のトランザクション冪等テーブルに記憶されているかどうかを問い合わせることであって、所定のトランザクション冪等テーブルが、トランザクション有効期間内の有効トランザクションに対応するトランザクション冪等レコードを記憶するために使用される、ことと、2)ターゲットトランザ

クションの一意の識別子に対応するトランザクション冪等レコードが所定のトランザクション冪等テーブルに記憶されていないとの決定に応答して、ターゲットトランザクションを候補ブロックに記録することとを含む。

【０１３９】

いくつかの実装形態では、トランザクション冪等レコードは、トランザクション冪等レコードに対応するトランザクションがブロックチェーンの分散データベースに正常に記録されたことを示し、本方法は、1)ターゲットトランザクションが候補ブロックに記録されており、候補ブロックに関するコンセンサスに達し、候補ブロックがブロックチェーンの分散データベースに正常に記憶されているとの決定に応答して、ターゲットトランザクションの一意の識別子に対応するトランザクション冪等レコードを生成することと、2)トランザクション冪等レコードを所定のトランザクション冪等テーブルに挿入することとをさらに含む。402から、方法400は404に進む。

【０１４０】

404において、基準時間パラメータに基づいて、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるかどうかが決定される。

【０１４１】

いくつかの実装形態では、基準時間パラメータに基づいて、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるかどうかを決定することは、1)基準タイムスタンプを第1の値および第2の値の各々と比較して、基準タイムスタンプが第1の値より大きく、第2の値より小さいかどうかを決定し、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであると決定することと、2)基準タイムスタンプが第1の値より大きく、第2の値より小さいとの決定に応答して、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであると決定することとを含む。

【０１４２】

いくつかの実装形態では、基準ブロック高さ値をブロックチェーン内の候補ブロックのブロック高さ値および第3の値の各々と比較する前に、方法400は、1)候補ブロックのブロック数がブロックチェーン内の最新ブロックのブロック数より大きいかどうかを決定することと、2)候補ブロックのブロック数がブロックチェーン内の最新ブロックのブロック数より大きいとの決定に応答して、基準ブロック高さ値をブロックチェーン内の候補ブロックのブロック高さ値および第3の値の各々と比較することとをさらに含む。404から、方法400は406に進む。

【０１４３】

406において、ターゲットトランザクションがトランザクション有効期間内の有効トランザクションであるとの決定に応答して、ターゲットトランザクションを候補ブロックに記録する。420の後、方法400は停止することができる。

【０１４４】

説明される主題は、様々な技術的利点および効果を提供する。たとえば、いくつかの実装形態では、トランザクション有効期間内の有効トランザクションのみが合法のトランザクションとして使用され、候補ブロックに記録され得る一方で、以前に期限切れになったトランザクションは、後続のトランザクション実行のために候補ブロックに記録されることが不可能であり、その結果、ブロックチェーン内の不法のノードデバイスは、以前に不法のノードデバイスによって傍受された期限切れのトランザクションを使用することによってブロックチェーンに対するリプレイ攻撃を開始することを妨げられ、それによって、ブロックチェーンのトランザクションセキュリティレベルを改善し得る。発行者に対するアイデンティティ認証およびトランザクションプール内のトランザクションコンテンツに対する検証に合格したトランザクション、ならびにトランザクションに対する合法の検証に合格したトランザクションは、候補トランザクションとして使用され、次いで、パックされ、作成された候補ブロックに記録され得る。ここで、台帳ノードとして働くノードデバイスは、候補トランザクションとして、合法の検証に合格したすべてのトランザクショ

ンを使用し、これらのトランザクションを候補ブロックに記録するか、または、候補トランザクションとして、一定の原理に基づいて(たとえば、トランザクションの優先順位に基づいて)、合法の検証に合格したすべてのトランザクションからいくつかのトランザクションを選択し、これらのトランザクションを候補ブロックに記録することができる。

【０１４５】

台帳ノードとして働くノードデバイスのトランザクション実行環境は、マルチインスタンス実行環境であり得る(たとえば、同じトランザクションクライアントは、トランザクションを同時に開始することができる複数のスレッドを可能にする)。マルチインスタンス実行環境では、同じトランザクションは、同じノードデバイスの異なるインスタンスによって繰り返しサブミットされ得る。したがって、ブロックチェーンにおけるトランザクション実行中に「冪等」問題が存在し得る。「冪等」問題は、同じトランザクションが繰り返し実行された後でユーザに悪影響がもたらされることを意味する。たとえば、ビットコインネットワークにおける「二重支払い」(double spending)問題は、典型的な「冪等」問題である。ここで、ユーザの秘密鍵を使用することによって署名された移転トランザクションは、不法のノードによって傍受される。トランザクションが実行された後、不法のノードは、傍受されたトランザクションに基づいてリプレイ攻撃を開始し、ブロックチェーンにおいてトランザクションを繰り返し実行することができる。結果として、同じ資金移転が複数回実行され、ユーザに資金損失をもたらす。これを考慮して、マルチインスタンス実行環境におけるトランザクションの繰り返される実行を低減するために、ブロックチェーン内の台帳ノードとして働くノードデバイスは、トランザクション冪等テーブルを共同で維持することができる。たとえば、台帳ノードとして働くノードデバイスは、ブロックチェーンの既存のコンセンサス機構を使用することによって、コンセンサス手順の後で取得されたトランザクション冪等テーブルを共同で維持することができる。トランザクション冪等テーブルは、トランザクション有効期間内の有効トランザクションを記録するブロックチェーン内の分散データのストレージレコード(言い換えれば、ブロックレコード)に基づいて作成されるインデックスレコードテーブルであり、ブロックチェーンの分散データベースに正常に記録されたすべての有効トランザクションに対応するトランザクション冪等レコードを記憶するために使用される。言い換えれば、トランザクション冪等テーブルに記憶されたトランザクション冪等レコードは、トランザクション冪等レコードに対応するトランザクションが候補ブロックに正常にパックされたことを示すために使用され、候補ブロックに関するコンセンサスに達した後、候補ブロックは、最終的にブロックチェーン内の最新ブロックとして使用され、ブロックチェーン内の分散データベース(言い換えれば、分散型台帳)に正常に追加され得る。いくつかの実装形態では、有効トランザクションを候補ブロックに記録する前に、台帳ノードとして働くノードデバイスは、トランザクションがブロックチェーンの分散データベースに正常に記録された複製トランザクションであるかどうかを決定するために、トランザクション冪等テーブルに基づいてトランザクションに対して冪等チェックをさらに実行することができる。

【０１４６】

いくつかの実装形態では、上記で説明された基準時間パラメータに加えて、クライアントを使用することによってユーザによって作成されたトランザクションは、トランザクションについてのクライアントによって作成された一意の識別子をさらに搬送することができる。たとえば、実際の適用例では、ブロックチェーン内のノードデバイスは、複数のインスタンスで構成されたノードデバイスであり得、各インスタンスは、一意のインスタンスIDを有する。この場合、トランザクションシリアル番号は、インスタンスIDと生成された乱数とを含む一意のトランザクションシリアル番号であり得る。別の例として、ブロックチェーン内のノードデバイスが複数のデバイスを含む分散デバイスである場合、各デバイスは、一意のデバイス識別子(たとえば、デバイスIDまたはデバイスのIPアドレス)を有することができる。この場合、トランザクションシリアル番号は、デバイス識別子と生成された乱数とを含む一意のトランザクションシリアル番号であり得る。収集されたトランザクションがトランザクション有効期間内の有効トランザクションであると決定した後、

台帳ノードとして働くノードデバイスは、トランザクションの一意の識別子に対応するトランザクション冪等レコードがトランザクション冪等テーブルに記憶されているかどうかをさらに問い合わせることができる。トランザクションの一意の識別子に対応するトランザクション冪等レコードがトランザクション冪等テーブルに記憶されている場合、それは、トランザクションが以前にブロックチェーンの分散データベースに正常に記録されており、トランザクションが繰り返し開始されるトランザクションであることを示す。この場合、トランザクションは、直接破棄され得る。しかしながら、トランザクションの一意の識別子に対応するトランザクション冪等レコードがトランザクション冪等テーブルに記憶されていない場合、それは、トランザクションが以前にブロックチェーンの分散データベースに正常に記録されていないことを示す。この場合、ノードデバイスは、トランザクションを候補ブロックに記録することができる。

【０１４７】

本明細書で説明される実施形態および動作は、デジタル電子回路において、または本明細書で開示される構造を含むコンピュータソフトウェア、ファームウェア、もしくはハードウェアにおいて、またはそれらのうちの1つまたは複数のそれらの組合せにおいて実装され得る。動作は、1つもしくは複数のコンピュータ可読記憶デバイス上に記憶されたまたは他のソースから受信されたデータに対してデータ処理装置によって実行される動作として実装され得る。データ処理装置、コンピュータ、またはコンピューティングデバイスは、例として、プログラマブルプロセッサ、コンピュータ、システムオンチップ、または上記の複数のもの、もしくは組合せを含む、データを処理するための装置、デバイス、および機械を包含し得る。装置は、専用論理回路、たとえば、中央処理ユニット(CPU)、フィールドプログラマブルゲートアレイ(FPGA)または特定用途向け集積回路(ASIC)を含むことができる。装置は、当該のコンピュータプログラムのための実行環境を作成するコード、たとえば、プロセッサファームウェア、プロトコルスタック、データベース管理システム、オペレーティングシステム(たとえば、1つのオペレーティングシステムまたはオペレーティングシステムの組合せ)、クロスプラットフォームランタイム環境、仮想マシン、またはそれらのうちの1つもしくは複数の組合せを構成するコードも含むことができる。装置および実行環境は、ウェブサービス、分散コンピューティングおよびグリッドコンピューティングインフラストラクチャなどの、様々な異なるコンピューティングモデルインフラストラクチャを実現することができる。

【０１４８】

コンピュータプログラム(たとえば、プログラム、ソフトウェア、ソフトウェアアプリケーション、ソフトウェアモジュール、ソフトウェアユニット、スクリプト、またはコードとしても知られている)は、コンパイル型言語またはインタプリタ型言語、宣言型言語または手続き型言語を含む任意の形態のプログラミング言語で書かれ得、スタンドアロンプログラムとして、またはモジュール、コンポーネント、サブルーチン、オブジェクト、もしくはコンピューティング環境で使用するのに適した他のユニットとしてを含む任意の形態で展開され得る。プログラムは、他のプログラムまたはデータ(たとえば、マークアップ言語文書に記憶された1つまたは複数のスクリプト)を保持するファイルの一部分に、当該のプログラム専用の単一のファイルに、または複数の協調ファイル(たとえば、1つもしくは複数のモジュール、サブプログラム、またはコードの部分を記憶するファイル)に記憶され得る。コンピュータプログラムは、1つのコンピュータ上で、または1つのサイトに配置されるかもしくは複数のサイトにわたって分散され、通信ネットワークによって相互接続された複数のコンピュータ上で実行され得る。

【０１４９】

コンピュータプログラムの実行のためのプロセッサは、例として、汎用マイクロプロセッサと専用マイクロプロセッサの両方、および任意の種類のデジタルコンピュータの任意の1つまたは複数のプロセッサを含む。一般に、プロセッサは、読取り専用メモリもしくはランダムアクセスメモリまたは両方から命令およびデータを受信する。コンピュータの必須要素は、命令に従ってアクションを実行するためのプロセッサ、ならびに命令および

データを記憶するための1つまたは複数のメモリデバイスである。一般に、コンピュータは、データを記憶するための1つまたは複数の大容量記憶デバイスも含むか、あるいは、大容量記憶デバイスからデータを受信するかもしくは大容量記憶デバイスにデータを転送するか、または両方を行うために、動作可能に結合される。コンピュータは、別のデバイス、たとえば、モバイルデバイス、携帯情報端末(PDA)、ゲームコンソール、全地球測位システム(GPS)受信機、またはポータブル記憶デバイスに埋め込まれ得る。コンピュータプログラム命令およびデータを記憶するのに適したデバイスは、例として、半導体メモリデバイス、磁気ディスク、および光磁気ディスクを含む、不揮発性メモリ、媒体およびメモリデバイスを含む。プロセッサおよびメモリは、専用論理回路によって補完されるか、または専用論理回路に組み込まれ得る。

【０１５０】

モバイルデバイスは、ハンドセット、ユーザ機器(UE)、モバイル電話(たとえば、スマートフォン)、タブレット、ウェアラブルデバイス(たとえば、スマートウォッチおよびスマート眼鏡)、人体内の埋め込みデバイス(たとえば、バイオセンサ、人工内耳)、または他のタイプのモバイルデバイスを含むことができる。モバイルデバイスは、(以下で説明される)様々な通信ネットワークと(たとえば、無線周波数(RF)信号を使用して)ワイヤレスに通信することができる。モバイルデバイスは、モバイルデバイスの現在の環境の特性を決定するためのセンサを含むことができる。センサは、カメラ、マイクロフォン、近接センサ、GPSセンサ、動きセンサ、加速度計、周囲光センサ、湿度センサ、ジャイロスコープ、コンパス、気圧計、指紋センサ、顔認識システム、RFセンサ(たとえば、Wi-Fi無線およびセルラー無線)、熱センサ、または他のタイプのセンサを含むことができる。たとえば、カメラは、可動レンズまたは固定レンズを備えたフロントカメラまたはリアカメラ、フラッシュ、画像センサ、および画像プロセッサを含むことができる。カメラは、顔認識および/または虹彩認識のための詳細をキャプチャすることが可能なメガピクセルカメラであり得る。データプロセッサと、メモリに記憶されたまたはリモートでアクセスされる認証情報とを伴ったカメラは、顔認識システムを形成することができる。顔認識システムまたは1つもしくは複数のセンサ、たとえば、マイクロフォン、動きセンサ、加速度計、GPSセンサ、もしくはRFセンサは、ユーザ認証に使用され得る。

【０１５１】

ユーザとの対話を提供するために、実施形態は、ディスプレイデバイスと入力デバイス、たとえば、情報をユーザに表示するための液晶ディスプレイ(LCD)または有機発光ダイオード(OLED)/仮想現実(VR)/拡張現実(AR)ディスプレイと、ユーザが入力をコンピュータに提供することができるタッチスクリーン、キーボード、およびポインティングデバイスとを有するコンピュータ上で実装され得る。他の種類のデバイスは、ユーザとの対話を提供するためにも使用され得、たとえば、ユーザに提供されるフィードバックは、任意の形態の感覚フィードバック、たとえば、視覚フィードバック、聴覚フィードバック、または触覚フィードバックとすることができ、ユーザからの入力は、音響入力、発話入力、または触覚入力を含む任意の形態で受信され得る。加えて、コンピュータは、ユーザによって使用されるデバイスに文書を送信し、そのデバイスから文書を受信することによって、たとえば、ユーザのクライアントデバイス上のウェブブラウザから受信された要求に応答して、そのウェブブラウザにウェブページを送信することによって、ユーザと対話することができる。

【０１５２】

実施形態は、任意の形態または媒体のワイヤラインまたはワイヤレスデジタルデータ通信(またはそれらの組合せ)、たとえば、通信ネットワークによって相互接続されたコンピューティングデバイスを使用して実装され得る。相互接続されたデバイスの例は、典型的には通信ネットワークを通じて対話する、一般的には互いから離れているクライアントおよびサーバである。クライアント、たとえば、モバイルデバイスは、サーバと、またはサーバを通じて、トランザクション自体を実施する、たとえば、購入、売却、支払、譲渡、送付、または貸付のトランザクションを実行するか、それを許可することができる。その

ようなトランザクションは、アクションおよびレスポンスが時間的に近接するようにリアルタイムであってもよく、たとえば、個人は、アクションおよびレスポンスがほぼ同時に発生していると知覚し、個人のアクションの後のレスポンスの時間差は、1ミリ秒(ms)より小さいかもしくは1秒(s)より小さく、または、システムのアカウント処理制限を考慮して、レスポンスには意図的な遅延がない。

【０１５３】

通信ネットワークの例は、ローカルエリアネットワーク(LAN)、無線アクセスネットワーク(RAN)、メトロポリタンエリアネットワーク(MAN)、およびワイドエリアネットワーク(WAN)を含む。通信ネットワークは、インターネット、別の通信ネットワーク、または通信ネットワークの組合せのすべてまたは一部分を含むことができる。情報は、ロングタームエボリューション(LTE)、5G、IEEE802、インターネットプロトコル(IP)、または他のプロトコルもしくはプロトコルの組合せを含む、様々なプロトコルおよび規格に従って、通信ネットワーク上で伝送され得る。通信ネットワークは、接続されたコンピューティングデバイスの間で、音声データ、ビデオデータ、生体データ、もしくは認証データ、または他の情報を伝送することができる。

【０１５４】

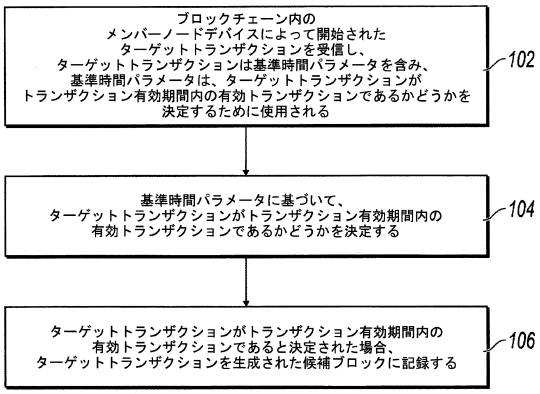
別個の実装形態として説明される特徴は、組み合わせて、単一の実装形態で実装され得るが、単一の実装形態として説明される特徴は、複数の実装形態で、別々に、または任意の適切な副組合せで実装され得る。特定の順序で説明され、特許請求される動作は、その特定の順序を必要とするものと理解されるべきではなく、すべての例示された動作が実行されなければならないと理解されるべきでもない(いくつかの動作は任意選択であり得る)。必要に応じて、マルチタスキングまたは並列処理(またはマルチタスキングと並列処理の組合せ)が実行され得る。

【符号の説明】

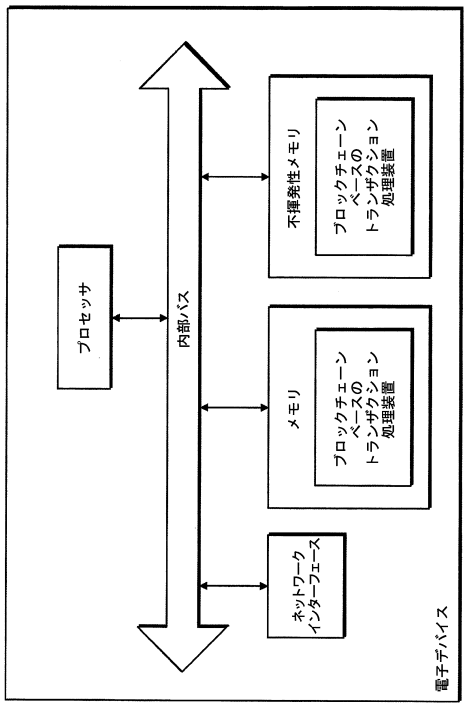
【０１５５】

30　ブロックチェーンベースのトランザクション処理装置
301　受信モジュール
302　決定モジュール
303　記録モジュール
400　方法

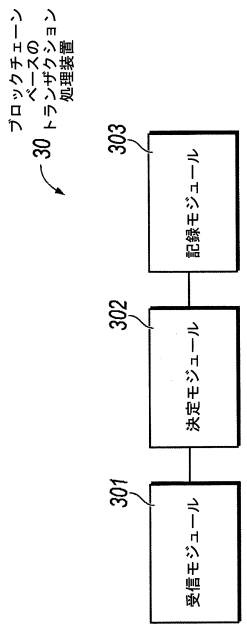
【図１】


ブロックチェーン内の
メンバーノードデバイスによって開始された
ターゲットトランザクションを受信し、
ターゲットトランザクションは基準時間パラメータを含み、
基準時間パラメータは、ターゲットトランザクションが
トランザクション有効期間内の有効トランザクションであるかどうかを
決定するために使用される
102
基準時間パラメータに基づいて、
ターゲットトランザクションがトランザクション有効期間内の
有効トランザクションであるかどうかを決定する
104
ターゲットトランザクションがトランザクション有効期間内の
有効トランザクションであると決定された場合、
ターゲットトランザクションを生成された候補ブロックに記録する
106

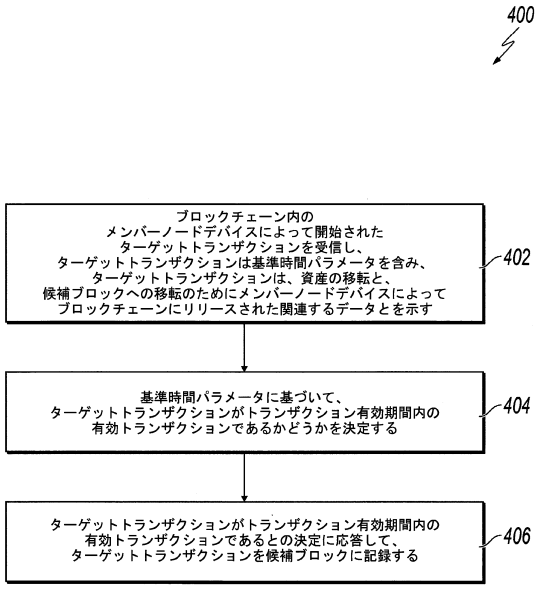
【図２】


電子デバイス
プロセッサ
内部バス
不揮発性メモリ
ブロックチェーンベースのトランザクション処理装置
メモリ
ブロックチェーンベースのトランザクション処理装置
ネットワークインターフェース

【図３】


ブロックチェーンベースのトランザクション処理装置
30
303
記録モジュール
302
決定モジュール
301
受信モジュール

【図４】


400
ブロックチェーン内の
メンバーノードデバイスによって開始された
ターゲットトランザクションを受信し、
ターゲットトランザクションは基準時間パラメータを含み、
ターゲットトランザクションは、資産の移転と、
候補ブロックへの移転のためにメンバーノードデバイスによって
ブロックチェーンにリリースされた関連するデータとを示す
402
基準時間パラメータに基づいて、
ターゲットトランザクションがトランザクション有効期間内の
有効トランザクションであるかどうかを決定する
404
ターゲットトランザクションがトランザクション有効期間内の
有効トランザクションであるとの決定に応答して、
ターゲットトランザクションを候補ブロックに記録する
406

フロントページの続き

(72)発明者　ジユアン・ワン
中華人民共和国・３１１１２１・ゼジャン・ハンジョウ・ユ・ハン・ディストリクト・ウェスト・ウェン・イ・ロード・ナンバー・９６９・ビルディング・３・５／エフ・アリババ・グループ・リーガル・デパートメント
(72)発明者　フアビン・ドゥ
中華人民共和国・３１１１２１・ゼジャン・ハンジョウ・ユ・ハン・ディストリクト・ウェスト・ウェン・イ・ロード・ナンバー・９６９・ビルディング・３・５／エフ・アリババ・グループ・リーガル・デパートメント
(72)発明者　シュエビン・ヤン
中華人民共和国・３１１１２１・ゼジャン・ハンジョウ・ユ・ハン・ディストリクト・ウェスト・ウェン・イ・ロード・ナンバー・９６９・ビルディング・３・５／エフ・アリババ・グループ・リーガル・デパートメント

審査官　上田　威

(56)参考文献　米国特許出願公開第２０１８／００７７１２２（ＵＳ，Ａ１）
国際公開第２０１７／１７８９５５（ＷＯ，Ａ１）
米国特許出願公開第２０１６／０２８３９３９（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　１０／００　－　９９／００
Ｇ０６Ｆ　９／４６
Ｈ０４Ｌ　９／３２