(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6856772号
(P6856772)
(45)発行日　令和3年4月14日(2021.4.14)　(24)登録日　令和3年3月22日(2021.3.22)

(51)Int.Cl.　　F I
G06F 21/12 (2013.01)　G06F 21/12　３１０
G06F 21/62 (2013.01)　G06F 21/62
H04L 9/32 (2006.01)　H04L 9/00　６７５Ｚ

請求項の数 17　(全 22 頁)

(21)出願番号　特願2019-559278 (P2019-559278)
(86)(22)出願日　平成31年4月3日(2019.4.3)
(65)公表番号　特表2020-525875 (P2020-525875A)
(43)公表日　令和2年8月27日(2020.8.27)
(86)国際出願番号　PCT/CN2019/081180
(87)国際公開番号　WO2019/120327
(87)国際公開日　令和1年6月27日(2019.6.27)
審査請求日　令和1年12月24日(2019.12.24)

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】信頼できる実行環境において実行されるスマートコントラクト動作に基づくブロックチェーンデータの処理

(57)【特許請求の範囲】
【請求項１】
ブロックチェーンデータを信頼できる実行環境(TEE)下で処理するためのコンピュータが実行する方法であって、
ブロックチェーンノードにより、前記ブロックチェーンノード上で実行するTEEにおいて1つまたは複数のソフトウェア命令を実行する要求を受信するステップと、
前記TEEにおける仮想マシンにより、前記1つまたは複数のソフトウェア命令の実行に関する1つまたは複数のブロックチェーンアカウントに関連するデータを前記要求に基づいて識別するステップと、
前記1つまたは複数のブロックチェーンアカウントに関連するデータの識別に応じて、前記仮想マシンにより、前記TEEに保存されているブロックチェーンのグローバルステートを走査して、前記1つまたは複数のブロックチェーンアカウントに関連するデータを見つけるステップと、
前記仮想マシンにより、前記データに基づいて前記1つまたは複数のソフトウェア命令を実行するステップであって、前記TEEに保存されているブロックチェーンのグローバルステートが、前記1つまたは複数のソフトウェア命令の実行中に更新されて、更新されたグローバルステートを生成する、ステップと、
前記1つまたは複数のソフトウェア命令の実行に応じて、前記ブロックチェーンノードにより、前記更新されたグローバルステートの暗号化表現を生成するステップと、
前記ブロックチェーンノードにより、前記TEEから分離している保存場所に前記更新さ

れたグローバルステートの暗号化表現を保存するステップと、
を含む、コンピュータが実行する方法。
【請求項２】
前記要求は、1つまたは複数の入力パラメータを含み、前記TEEのインターフェース関数に対して行われる、請求項1に記載のコンピュータが実行する方法。
【請求項３】
前記グローバルステートは、前記TEEにマークルパトリシアツリー(MPT)として保存されている、請求項1に記載のコンピュータが実行する方法。
【請求項４】
前記グローバルステートは、前記ブロックチェーンの複数のブロックチェーンアカウントのアドレスと状態との間のマッピングを含み、前記複数のブロックチェーンアカウントは、1つまたは複数の外部所有アカウントまたはコントラクトアカウントを含み、前記コントラクトアカウントのそれぞれがストレージルートを含む、請求項1に記載のコンピュータが実行する方法。
【請求項５】
前記ストレージルートはマークルパトリシアツリー(MPT)のルートノードのハッシュを含み、前記MPTは、対応するコントラクトアカウントのストレージ内容のハッシュをエンコードする、請求項4に記載のコンピュータが実行する方法。
【請求項６】
更新されたグローバルステートは、前記対応するコントラクトアカウントのストレージ内容のハッシュをエンコードする前記MPTを更新することによって生成される、請求項5に記載のコンピュータが実行する方法。
【請求項７】
前記TEEから分離している保存場所は、キャッシュまたはデータベースに関連している、請求項1に記載のコンピュータが実行する方法。
【請求項８】
前記要求は、前記TEEに関連するアプリケーションプログラミングインターフェースを介して受信される、請求項1に記載のコンピュータが実行する方法。
【請求項９】
請求項1から8のいずれか一項に記載の方法を1つまたは複数のコンピュータに実行させる1つまたは複数の命令を記憶した非一時的コンピュータ可読記憶媒体。
【請求項１０】
コンピュータが実装されたシステムであって、
1つまたは複数のコンピュータと、
前記1つまたは複数のコンピュータによって実行されるとき、ブロックチェーンデータを信頼できる実行環境(TEE)下で処理するための1つまたは複数の動作を実行する1つまたは複数の命令を記憶した有形の非一時的機械可読媒体を有し、前記1つまたは複数のコンピュータと相互作用可能に結合された1つまたは複数のコンピュータメモリデバイスと、
を含み、前記動作は、
ブロックチェーンノードにより、前記ブロックチェーンノード上で実行するTEEにおいて1つまたは複数のソフトウェア命令を実行する要求を受信するステップと、
前記TEEにおける仮想マシンにより、前記1つまたは複数のソフトウェア命令の実行に関する1つまたは複数のブロックチェーンアカウントに関連するデータを前記要求に基づいて識別するステップと、
前記1つまたは複数のブロックチェーンアカウントに関連するデータの識別に応じて、前記仮想マシンにより、前記TEEに保存されているブロックチェーンのグローバルステートを走査して、前記1つまたは複数のブロックチェーンアカウントに関連するデータを見つけるステップと、
前記仮想マシンにより、前記データに基づいて前記1つまたは複数のソフトウェア命令を実行するステップであって、前記TEEに保存されているブロックチェーンのグローバル

ステートが、前記1つまたは複数のソフトウェア命令の実行中に更新されて、更新されたグローバルステートを生成する、ステップと、
前記1つまたは複数のソフトウェア命令の実行に応じて、前記ブロックチェーンノードにより、前記更新されたグローバルステートの暗号化表現を生成するステップと、
前記ブロックチェーンノードにより、前記TEEから分離している保存場所に前記更新されたグローバルステートの暗号化表現を保存するステップと、
を含む、システム。
【請求項１１】
前記要求は、1つまたは複数の入力パラメータを含み、前記TEEのインターフェース関数に対して行われる、請求項10に記載のシステム。
【請求項１２】
前記グローバルステートは、前記TEEにマークルパトリシアツリー(MPT)として保存されている、請求項10に記載のシステム。
【請求項１３】
前記グローバルステートは、前記ブロックチェーンの複数のブロックチェーンアカウントのアドレスと状態との間のマッピングを含み、前記複数のブロックチェーンアカウントは、1つまたは複数の外部所有アカウントまたはコントラクトアカウントを含み、前記コントラクトアカウントのそれぞれがストレージルートを含む、請求項10に記載のシステム。
【請求項１４】
前記ストレージルートはマークルパトリシアツリー(MPT)のルートノードのハッシュを含み、前記MPTは、対応するコントラクトアカウントのストレージ内容のハッシュをエンコードする、請求項13に記載のシステム。
【請求項１５】
更新されたグローバルステートは、前記対応するコントラクトアカウントのストレージ内容のハッシュをエンコードする前記MPTを更新することによって生成される、請求項14に記載のシステム。
【請求項１６】
前記TEEから分離している保存場所は、キャッシュまたはデータベースに関連している、請求項10に記載のシステム。
【請求項１７】
前記要求は、前記TEEに関連するアプリケーションプログラミングインターフェースを介して受信される、請求項10に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本明細書は、信頼できる実行環境下でのブロックチェーンデータの処理に関する。
【背景技術】
【０００２】
分散型台帳システム(DLS)は、コンセンサスネットワーク、および/またはブロックチェーンネットワークとも呼ぶことができ、参加エンティティが安全に、かつ不変にデータを保存することを可能にしている。DLSは一般に、いずれの特定のユーザケースをも参照することなくブロックチェーンネットワークと呼ばれている。ブロックチェーンネットワークのタイプの例は、パブリックブロックチェーンネットワーク、プライベートブロックチェーンネットワーク、およびコンソーシアムブロックチェーンネットワークを含むことができる。コンソーシアムブロックチェーンネットワークは、コンセンサスプロセスを制御するエンティティの選択グループに提供され、アクセス制御層を含む。
【０００３】
スマートコントラクトは、ブロックチェーン上で実行されるプログラムである。スマートコントラクトは一連の事前定義された規則を含み、この規則の下でそのスマートコント

ラクトの当事者が互いに対話することに同意している。スマートコントラクトは、イーサリアムなどの分散型コンピューティングプラットフォームによって実行することができる。たとえば、イーサリアム仮想マシン(EVM)は、イーサリアムにおける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。イーサリアムブロックチェーンは、トランザクションベースの状態マシンとして見ることができる。イーサリアムは、ワールドステートと呼ばれるグローバルな共有状態を有することができる。ワールドステートは、イーサリアムアカウントアドレスとアカウント状態との間のマッピングを含む。このマッピングは、マークルパトリシアツリー(MPT)として知られているデータ構造に保存される。

【０００４】

イーサリアムアカウント状態は、アカウントプライバシーを保護するためによく暗号化されるが、用いられる暗号化キーはすべてのアカウントについて同じである。そのため、MPTのデータ構造を保持することができるので、マークルプルーフまたは状態更新のためにすべてのブロックチェーンノードによって同じ方法でマークルルートを計算することができる。しかしながら、すべてのアカウント間で同じ暗号化キーを用いることによって、ワールドステートのデータ構造を隠すことができず、アカウントの関係および挙動に関連するプライバシー情報が攻撃者によって分析されることがある。

【０００５】

したがって、信頼できる実行環境においてブロックチェーンのアカウント値を取得および更新し、対応するMPTを暗号化テキストで保存してそのデータ構造を隠すことが望ましいであろう。

【発明の概要】

【課題を解決するための手段】

【０００６】

本明細書は、信頼できる実行環境(TEE)において実行されるスマートコントラクト動作に基づいてブロックチェーンデータを処理するための技術を記載している。これらの技術は一般に、ブロックチェーンノード上で実行されるTEEにおいて1つまたは複数のソフトウェア命令を実行する要求を受信することと、要求に基づいて1つまたは複数のソフトウェア命令を実行するため、1つまたは複数のブロックチェーンアカウントに関連するデータを判定することと、TEEに保存されているブロックチェーンのグローバルステートを走査して、データを見つけることと、データに基づいて1つまたは複数のソフトウェア命令を実行することと、を伴う。

【０００７】

本明細書はまた、1つまたは複数のプロセッサに結合されるとともに、1つまたは複数のプロセッサによって実行されると、本明細書で提供される方法の実施形態による動作を1つまたは複数のプロセッサに実行させる命令を格納している1つまたは複数の非一時的コンピュータ可読記憶媒体を提供する。

【０００８】

本明細書は、本明細書で提供される方法を実装するためのシステムをさらに提供する。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よって実行されると、本明細書で提供される方法の実施形態による動作を1つまたは複数のプロセッサに実行させる命令を格納している1つまたは複数のプロセッサに結合されたコンピュータ可読記憶媒体と、を含む。

【０００９】

本明細書による方法は、本明細書に記載の態様および特徴の任意の組み合わせを含むことができることが理解される。すなわち、本明細書による方法は、本明細書で具体的に説明する態様および特徴の組み合わせに限定されず、提供される態様および特徴の任意の組み合わせも含む。

【００１０】

本明細書の1つまたは複数の実施形態の詳細は、添付の図面および以下の説明に記載されている。本明細書の他の特徴および利点が、説明および図面から、ならびに特許請求の

範囲から明らかになるであろう。
【図面の簡単な説明】
【００１１】
【図１】本明細書の実施形態を実行するために用いることができる環境の一例を示す図である。
【図２】本明細書の実施形態によるアーキテクチャの一例を示す図である。
【図３】本明細書の実施形態によるTEEの外部のデータベースと通信するTEEの構造の一例を示す図である。
【図４】本明細書の実施形態によるプロセスの一例のフローチャートである。
【図５】本明細書の実施形態による装置のモジュールの例を示す。
【発明を実施するための形態】
【００１２】
様々な図面における同様の参照番号および名称は同様の要素を示す。
【００１３】
本明細書は、信頼できる実行環境(TEE)において実行されるスマートコントラクト動作に基づいてブロックチェーンデータを処理するための技術を記載している。これらの技術は一般に、ブロックチェーンノード上で実行されるTEEにおいて1つまたは複数のソフトウェア命令を実行する要求を受信することと、要求に基づいて1つまたは複数のソフトウェア命令を実行するため、1つまたは複数のブロックチェーンアカウントに関連するデータを判定することと、TEEに保存されているブロックチェーンのグローバルステートを走査して、データを見つけることと、データに基づいて1つまたは複数のソフトウェア命令を実行することと、を伴う。
【００１４】
本明細書の実施形態にさらなる状況を提供するため、そして上で紹介したように、分散型台帳システム(DLS)は、コンセンサスネットワーク(たとえば、ピアツーピアのノードからなる)、およびブロックチェーンネットワークとも呼ぶことができ、参加エンティティが安全に、かつ不変にトランザクションを実行し、データを保存することを可能にしている。ブロックチェーンという用語は一般に特定のネットワーク、および/または使用ケースに関連付けられているが、本明細書ではブロックチェーンを用いていずれの任意の特定の使用ケースをも参照することなく一般的にDLSを指す。
【００１５】
ブロックチェーンは、トランザクションが不変である方法でトランザクションを保存するデータ構造である。したがって、ブロックチェーンに記録されたトランザクションは信頼でき、信用に値する。ブロックチェーンは1つまたは複数のブロックを含む。チェーンにおける各ブロックは、チェーンにおける直前のブロックの暗号化ハッシュを含めることによって前のブロックにリンクされている。各ブロックは、タイムスタンプ、独自の暗号化ハッシュ、および1つまたは複数のトランザクションも含む。ブロックチェーンネットワークのノードによってすでに検証されたトランザクションは、ハッシュされてマークルツリーにエンコードされる。マークルツリーは、ツリーのリーフノードでのデータがハッシュされ、ツリーの各ブランチにおけるすべてのハッシュがブランチのルートで連結されるデータ構造である。このプロセスはツリーを上ってツリー全体のルートまで続き、これはツリーにおけるすべてのデータを表すハッシュを保存する。ツリーに保存されているトランザクションのものであると見なされるハッシュは、それがツリーの構造と一致しているかどうかを判断することによって迅速に検証することができる。
【００１６】
ブロックチェーンは、トランザクションを保存するための分散型または少なくとも部分的に分散型のデータ構造であるが、ブロックチェーンネットワークは、トランザクションなどをブロードキャスト、検証および有効化することによって1つまたは複数のブロックチェーンを管理、更新、および維持するコンピューティングノードのネットワークである。上で紹介したように、ブロックチェーンネットワークは、パブリックブロックチェーン

ネットワーク、プライベートブロックチェーンネットワーク、またはコンソーシアムブロックチェーンネットワークとして提供することができる。コンソーシアムブロックチェーンネットワークを参照して本明細書の実施形態をここでさらに詳細に説明する。しかしながら、任意の適切なタイプのブロックチェーンネットワークにおいて本明細書の実施形態を実現することができると考えられる。

【００１７】

一般に、コンソーシアムブロックチェーンネットワークは、参加エンティティ間でプライベートである。コンソーシアムブロックチェーンネットワークにおいて、コンセンサスプロセスは、コンセンサスノードと呼ぶことができる承認されたノードのセットによって制御され、1つまたは複数のコンセンサスノードがそれぞれのエンティティ(たとえば、金融機関、保険会社)によって操作される。たとえば、10のエンティティ(たとえば、金融機関、保険会社)のコンソーシアムがコンソーシアムブロックチェーンネットワークを操作することができ、これらのそれぞれがコンソーシアムブロックチェーンネットワークにおける少なくとも1つのノードを操作する。

【００１８】

いくつかの例において、コンソーシアムブロックチェーンネットワーク内で、すべてのノードにわたって複製されるブロックチェーンとしてグローバルブロックチェーンが提供される。すなわち、すべてのコンセンサスノードが、グローバルブロックチェーンに対して完全状態のコンセンサスにある。コンセンサス(たとえば、ブロックチェーンへのブロックの追加に対する合意)を達成するため、コンソーシアムブロックチェーンネットワーク内にコンセンサスプロトコルが実装される。たとえば、コンソーシアムブロックチェーンネットワークは、以下でさらに詳細に説明する、実用的ビザンチン障害耐性(PBFT)コンセンサスを実装することができる。

【００１９】

図1は、本明細書の実施形態を実行するために用いることができる環境100の一例を示す図である。いくつかの例において、環境100は、エンティティがコンソーシアムブロックチェーンネットワーク102に参加することを可能にしている。環境100は、コンピューティングデバイス106、108、およびネットワーク110を含む。いくつかの例において、ネットワーク110は、ローカルエリアネットワーク(LAN)、ワイドエリアネットワーク(WAN)、インターネット、またはこれらの組み合わせを含み、ウェブサイト、ユーザデバイス(たとえば、コンピューティングデバイス)、およびバックエンドシステムを接続する。いくつかの例において、ネットワーク110は、有線および/または無線通信リンクを介してアクセスすることができる。いくつかの例において、ネットワーク110は、コンソーシアムブロックチェーンネットワーク102との、およびこのネットワーク内での通信を可能にしている。一般に、ネットワーク110は、1つまたは複数の通信ネットワークを表す。いくつかの場合において、コンピューティングデバイス106、108はクラウドコンピューティングシステム(図示せず)のノードであり得、または各コンピューティングデバイス106、108は、ネットワークによって相互接続されて分散型処理システムとして機能する複数のコンピュータを含む分離したクラウドコンピューティングシステムであり得る。

【００２０】

図示の例において、コンピューティングシステム106、108は、コンソーシアムブロックチェーンネットワーク102におけるノードとしての参加を可能にする任意の適切なコンピューティングシステムをそれぞれ含むことができる。コンピューティングデバイスの例は、サーバ、デスクトップコンピュータ、ラップトップコンピュータ、タブレットコンピューティングデバイス、およびスマートフォンを含むが、これらに限定されない。いくつかの例において、コンピューティングシステム106、108は、コンソーシアムブロックチェーンネットワーク102と対話するための1つまたは複数のコンピュータ実装サービスをホストする。たとえば、コンピューティングシステム106は、第1のエンティティ(たとえば、ユーザA)のコンピュータ実装サービス、たとえば第1のエンティティがその1つまたは複数の他のエンティティ(たとえば、他のユーザ)とのトランザクションを管理するために用いる

トランザクション管理システムをホストすることができる。コンピューティングシステム108は、第2のエンティティ(たとえば、ユーザB)のコンピュータ実装サービス、たとえば第2のエンティティがその1つまたは複数の他のエンティティ(たとえば、他のユーザ)とのトランザクションを管理するために用いるトランザクション管理システムをホストすることができる。図1の例において、コンソーシアムブロックチェーンネットワーク102はノードのピアツーピアネットワークとして表され、コンピューティングシステム106、108はそれぞれ第1のエンティティ、および第2のエンティティのノードを提供し、これらがコンソーシアムブロックチェーンネットワーク102に参加している。

【００２１】

図2は、本明細書の実施形態によるアーキテクチャ200の一例を示している。アーキテクチャ200は、エンティティ層202、ホステッドサービス層204、およびブロックチェーンネットワーク層206を含む。図示の例において、エンティティ層202は、参加者A、参加者B、および参加者Cの3人の参加者を含み、各参加者はそれぞれのトランザクション管理システム208を有する。

【００２２】

図示の例において、ホステッドサービス層204は、各トランザクション管理システム208のためのインターフェース210を含む。いくつかの例において、それぞれのトランザクション管理システム208は、プロトコル(たとえば、ハイパーテキストトランスファープロトコルセキュア(HTTPS))を用いて、ネットワーク(たとえば、図1のネットワーク110)を介してそれぞれのインターフェース210と通信する。いくつかの例において、各インターフェース210は、それぞれのトランザクション管理システム208と、ブロックチェーンネットワーク層206との間で通信接続を提供する。より詳細には、インターフェース210は、ブロックチェーンネットワーク層206のブロックチェーンネットワーク212と通信する。いくつかの例において、インターフェース210と、ブロックチェーンネットワーク層206との間の通信は、リモートプロシージャコール(RPC)を用いて行われる。いくつかの例において、インターフェース210は、それぞれのトランザクション管理システム208のためにブロックチェーンネットワークノードを「ホスト」する。たとえば、インターフェース210は、ブロックチェーンネットワーク212へのアクセスのためのアプリケーションプログラミングインターフェース(API)を提供する。

【００２３】

本明細書で説明したように、ブロックチェーンネットワーク212は、ブロックチェーン216に情報を不変に記録する複数のノード214を含むピアツーピアネットワークとして提供される。単一のブロックチェーン216が概略的に示されているが、ブロックチェーン216の複数のコピーが提供され、ブロックチェーンネットワーク212にわたって維持される。たとえば、各ノード214がブロックチェーンのコピーを保存する。いくつかの実施形態において、ブロックチェーン216は、コンソーシアムブロックチェーンネットワークに参加している2つ以上のエンティティ間で実行されるトランザクションに関連する情報を保存する。

【００２４】

ブロックチェーン(たとえば、図2のブロックチェーン216)はブロックのチェーンからなり、各ブロックがデータを保存する。データの例は、2人以上の参加者間のトランザクションを表すトランザクションデータを含む。本明細書では非限定的な例としてトランザクションを用いるが、任意の適切なデータをブロックチェーンに保存することができることが企図される(たとえば、文書、画像、ビデオ、オーディオ)。トランザクションの例は、価値のある何か(たとえば、資産、製品、サービス、通貨)の交換を含むが、これらに限定されない。トランザクションデータは、ブロックチェーン内に不変に保存される。すなわち、トランザクションデータは変更することができない。

【００２５】

ブロックに保存する前に、トランザクションデータはハッシュされる。ハッシュは、トランザクションデータ(文字列データとして提供される)を固定長のハッシュ値(これも文

字列データとして提供される)に変換するプロセスである。ハッシュ値をハッシュ解除してトランザクションデータを取得することは不可能である。ハッシュにより確実に、トランザクションデータのわずかな変更でも、まったく異なるハッシュ値が得られる。さらに、そして上記のように、ハッシュ値は固定長である。すなわち、トランザクションデータのサイズに関係なく、ハッシュ値の長さは固定されている。ハッシュは、ハッシュ関数を通じてトランザクションデータを処理してハッシュ値を生成することを含む。ハッシュ関数の一例は、256ビットのハッシュ値を出力するセキュアハッシュアルゴリズム(SHA)-256を含むが、これに限定されない。

【００２６】

複数のトランザクションのトランザクションデータがハッシュされてブロックに保存される。たとえば、2つのトランザクションのハッシュ値が提供され、これら自体がハッシュされて別のハッシュを提供する。このプロセスは、ブロックに保存されるべきすべてのトランザクションについて、単一のハッシュ値が提供されるまで繰り返される。このハッシュ値はマークルルートハッシュと呼ばれ、ブロックのヘッダに保存される。トランザクションのいずれが変更されてもそのハッシュ値が変更され、最終的に、マークルルートハッシュが変更されることになる。

【００２７】

ブロックは、コンセンサスプロトコルを介してブロックチェーンに追加される。ブロックチェーンネットワーク内の複数のノードがコンセンサスプロトコルに参加し、ブロックチェーンにブロックを追加する作業を実行する。このようなノードはコンセンサスノードと呼ばれる。PBFTは、上で紹介したが、コンセンサスプロトコルの非限定的な例として用いる。コンセンサスノードは、コンセンサスプロトコルを実行してトランザクションをブロックチェーンに追加し、ブロックチェーンネットワークの全体的な状態を更新する。

【００２８】

さらに詳細には、コンセンサスノードは、ブロックヘッダを生成し、ブロックにおけるトランザクションのすべてをハッシュし、ハッシュ値を対に組み合わせて、ブロックにおけるすべてのトランザクションに単一のハッシュ値が提供されるまでさらなるハッシュ値を生成する(マークルルートハッシュ)。このハッシュはブロックヘッダに追加される。コンセンサスノードは、ブロックチェーンにおける最新のブロック(すなわち、ブロックチェーンに追加された最後のブロック)のハッシュ値も決定する。コンセンサスノードはまた、ナンス値、およびタイムスタンプをブロックヘッダに追加する。

【００２９】

一般に、PBFTは、ビザンチン障害(たとえば、誤動作しているノード、悪意のあるノード)を許容する実用的なビザンチン状態マシンの複製を提供する。これは、PBFTにおいて障害が発生するであろうと仮定すること(たとえば、独立したノード障害、および/またはコンセンサスノードによって送信された操作されたメッセージの存在を仮定すること)によって達成される。PBFTにおいて、コンセンサスノードは、プライマリコンセンサスノード、およびバックアップコンセンサスノードを含むシーケンスで提供される。プライマリコンセンサスノードは定期的に変更される。トランザクションは、ブロックチェーンネットワーク内のすべてのコンセンサスノードがブロックチェーンネットワークのワールドステートについて合意に達することによってブロックチェーンに追加される。このプロセスにおいて、コンセンサスノード間でメッセージが送信され、各コンセンサスノードは、特定のピアノードからメッセージが受信されたことを証明し、送信中にメッセージが変更されなかったことを検証する。

【００３０】

PBFTにおいて、コンセンサスプロトコルは複数のフェーズにおいて提供され、すべてのコンセンサスノードが同じ状態で始まる。まず、クライアントがプライマリコンセンサスノードにリクエストを送信して、サービス動作を呼び出す(たとえば、ブロックチェーンネットワーク内でトランザクションを実行する)。リクエストの受信に応じて、プライマリコンセンサスノードはリクエストをバックアップコンセンサスノードにマルチキャスト

する。バックアップコンセンサスノードはリクエストを実行し、それぞれがクライアントに応答を送信する。クライアントは、閾値数の応答が受信されるまで待機する。いくつかの例において、クライアントはf+1の応答の受信を待機し、ここでfは、ブロックチェーンネットワーク内で許容することができる障害のあるコンセンサスノードの最大数である。最終結果は、十分な数のコンセンサスノードが、ブロックチェーンに追加されるべき記録について合意に達し、記録が受け入れられるか、拒否されるかである。

【００３１】

いくつかのブロックチェーンネットワークにおいて、トランザクションのプライバシーを維持するために暗号化が実装されている。たとえば、ブロックチェーンネットワークにおける他のノードがトランザクションの詳細を識別することができないように、2つのノードがトランザクションをプライベートに保ちたければ、両ノードはトランザクションデータを暗号化することができる。暗号化の一例は、対称暗号化、および非対称暗号化を含むが、これらに限定されない。対称暗号化は、暗号化(プレーンテキストから暗号化テキストを生成)と、復号化(暗号化テキストからプレーンテキストを生成)との両方に単一の鍵を用いる暗号化プロセスを指す。対称暗号化において、同じ鍵が複数のノードに利用可能であるため、各ノードがトランザクションデータを暗号化/復号化することができる。

【００３２】

非対称暗号化は、それぞれが秘密鍵、および公開鍵を含む鍵の対を用い、秘密鍵はそれぞれのノードのみに知られ、公開鍵はブロックチェーンネットワークにおける任意またはすべての他のノードに知られている。あるノードが別のノードの公開鍵を用いてデータを暗号化することができ、暗号化されたデータは他のノードの秘密鍵を用いて復号化することができる。たとえば、そして再び図2を参照すると、参加者Aは参加者Bの公開鍵を用いてデータを暗号化し、暗号化されたデータを参加者Bに送信することができる。参加者Bはその秘密鍵を用いて暗号化されたデータ(暗号化テキスト)を復号化し、元のデータ(プレーンテキスト)を抽出することができる。あるノードの公開鍵で暗号化されたメッセージは、そのノードの秘密鍵を用いてのみ復号化することができる。

【００３３】

非対称暗号化はデジタル署名を提供するために用いられ、これにより、トランザクションの参加者が、そのトランザクションの他の参加者、ならびにそのトランザクションの有効性を確認することが可能になる。たとえば、あるノードがメッセージにデジタル署名することができ、別のノードが、参加者Aのデジタル署名に基づいて、メッセージがそのノードによって送信されたことを確認することができる。デジタル署名を用いて、送信中にメッセージが改ざんされないことを確実にすることもできる。たとえば、そして再び図2を参照すると、参加者Aは参加者Bにメッセージを送信しようとしている。参加者Aはメッセージのハッシュを生成し、次いで、その秘密鍵を用いて、ハッシュを暗号化して暗号化されたハッシュとしてデジタル署名を提供する。参加者Aはデジタル署名をメッセージに追加し、デジタル署名付きメッセージを参加者Bに送信する。参加者Bは、参加者Aの公開鍵を用いてデジタル署名を復号化し、ハッシュを抽出する。参加者Bはメッセージをハッシュし、両ハッシュを比較する。両ハッシュが同じであれば、参加者Bは、メッセージが実際に参加者Aからのものであり、改ざんされていないことを確認することができる。

【００３４】

いくつかの実施形態において、ブロックチェーンネットワークのノード、および/またはブロックチェーンネットワークと通信するノードは、TEEを用いて動作することができる。高レベルで、TEEはハードウェア(1つまたは複数のプロセッサ、メモリ)内の信頼できる環境であり、ハードウェアのオペレーティング環境(たとえば、オペレーティングシステム(OS)、基本入出力システム(BIOS))から隔離されている。さらに詳細には、TEEは、実行中のコード、およびメインプロセッサ内にロードされたデータの機密性、および整合性を保証する、プロセッサの分離した、安全な領域である。プロセッサ内で、TEEはOSと並行して動く。いわゆるトラステッドアプリケーション(TA)の少なくとも一部がTEE内で実行され、プロセッサおよびメモリにアクセスを有する。TEEを通じて、TAは、メインOSに

おいて動いている他のアプリケーションから保護される。さらに、TEEは、TEE内部でTAを互いに暗号で隔離している。

【００３５】

TEEの一例は、Santa Clara、California、United StatesのIntel Corporationによって提供されているSoftware Guard Extensions(SGX)を含む。本明細書ではSGXを例として議論するが、任意の適切なTEEを用いて本明細書の実施形態を実現することができることが企図される。

【００３６】

SGXはハードウェアベースのTEEを提供する。SGXにおいて、信頼できるハードウェアは中央処理装置(CPU)のダイであり、物理メモリの一部が、セレクトコードおよびデータを保護するために隔離されている。メモリのこの隔離された部分はエンクレーブと呼ばれる。より具体的には、エンクレーブは、メモリにおけるエンクレーブページキャッシュ(EPC)として提供され、アプリケーションアドレス空間にマップされる。メモリ(たとえば、DRAM)は、SGX用のプリザーブドランダムメモリ(PRM)を含む。PRMは、最も低いBIOSレベルにおける連続したメモリ空間であり、いずれのソフトウェアによってもアクセスすることができない。各EPCは、OSによって割り当てられてPRMにアプリケーションデータおよびコードをロードするメモリセット(たとえば、4KB)である。EPCメタデータ(EPCM)は、それぞれのEPCについてのエントリアドレスであり、各EPCは1つのエンクレーブによってのみ共有することができることを保証している。すなわち、単一のエンクレーブが複数のEPCを用いることができる一方、EPCは単一のエンクレーブ専用である。

【００３７】

TAの実行中、プロセッサは、エンクレーブに保存されているデータにアクセスするとき、いわゆるエンクレーブモードで動作する。エンクレーブモードでの動作により、各メモリアクセスに対して追加のハードウェアチェックが強制される。SGXにおいて、TAは、信頼できる部分、および信頼できない部分にコンパイルされる。信頼できる部分は、たとえば、OS、BIOS、特権システムコード、仮想マシンマネージャ(VMM)、システム管理モード(SMM)、などによってアクセス不能である。動作中、TAが実行されてメモリのPRM内にエンクレーブを作成する。エンクレーブ内の信頼できる部分によって実行される信頼できる関数が信頼できない部分によって呼び出され、エンクレーブ内で実行されるコードは、データをプレーンテキストデータ(暗号化されていない)として見、データへの外部アクセスは拒否される。

【００３８】

いくつかの実施形態において、TEEの内部で動作する仮想マシンが、アプリケーションがスマートコントラクトを安全に実行するための信頼できるランタイム環境を提供することができる。仮想マシンは、TEEの外部のアプリケーションからコールを受信することができる。コールは、TEEインターフェース関数を呼び出してスマートコントラクトの実行を開始することができる。スマートコントラクトの実行中、仮想マシンは、コールの入力パラメータまたはスマートコントラクトの内容に基づいて、ブロックチェーンアカウントからデータを取得することができる。ブロックチェーンのアカウントアドレスおよび対応するアカウント状態は、MPTとして知られているデータ構造にキーバリューペアとして保存されている。MPTは、ブロックチェーンのワールドステートに対応し、プレーンテキストでTEEに保存されている。スマートコントラクトの実行後、1つまたは複数のアカウント状態が変わることがあり、新たなアカウントが追加または削除されることがある。したがって、ブロックチェーンのワールドステートは、ハッシュエンコーディングに基づいてTEE内部で更新され、アカウント状態の変更を反映することができる。ワールドステートが更新された後、TEEからコールを行って、更新されたMPTをTEEの外部のデータベースへ保存することができる。TEEから出力された更新されたMPTを暗号化して、その構造および保存されているデータを隠すことができる。MPTはTEE内部で処理および更新され、そしてTEEの外部に暗号化された形式で保存されるため、ブロックチェーンアカウントの状態、挙動、および関係は、このような情報へのアクセスを許可されていないブロックチェーンノ

ード(たとえば、情報を復号化する適切なキーがないもの)から隠すことができる。

【００３９】

図3は、本明細書の実施形態によるTEEの外部のデータベースと通信するTEEの構造300の一例を示す図である。高レベルで、構造300は、仮想マシンおよびMPTのワールドステート308を格納するTEE302と、TEE302と通信するデータベース332と、を含む。

【００４０】

上で論じたように、SGX対応アプリケーションなどのTAは、信頼できるコンポーネント(またはエンクレーブコンポーネント)および信頼できないコンポーネント(アプリケーションコンポーネント)を含むことができる。アプリケーションコンポーネントは、TEE302の外部にあり、エンクレーブインターフェース関数を介してTEE302にアクセスすることができる。いくつかの実施形態において、これらのエンクレーブインターフェース関数は、アプリケーションコンポーネントによって用いられるアプリケーションプログラミングインターフェース(API)である。アプリケーションコンポーネントは、APIを用いて、TEEにおける仮想マシン304を呼び出してスマートコントラクトを実行するため、「eコール」306を行うことができる。仮想マシンは、特定のプログラミング言語で、またはビットストリームなどのバイナリ形式でエンコードされたプログラム命令を実行するソフトウェアプログラムであり得る。いくつかの場合において、仮想マシンは、プログラム命令と、仮想マシンを実行するコンピューティングデバイスの基盤となるハードウェアとの間に抽象化層を提供することができる。このような構成により、異なるハードウェアを有する異なるコンピューティングデバイスにわたって同じ方法で同じプログラム命令を実行することが可能になり得る。

【００４１】

いくつかの実装形態において、仮想マシンは、イーサリアムブロックチェーンの状況下でイーサリアム仮想マシン(EVM)であり得る。他のブロックチェーンネットワークが他のタイプの仮想マシンを用いることができることが理解されるべきである。eコール306を受信した後、仮想マシン304は、eコール306によって指定されたスマートコントラクトの実行に関する1つまたは複数のブロックチェーンアカウントを識別することができる。この識別は、eコール306の1つまたは複数の入力パラメータに基づくことができる。たとえば、アプリケーションコンポーネントによってeコール306を行って、2つのブロックチェーンアカウント間の新たなトランザクションをブロックチェーンに追加するためのスマートコントラクトを実行することができる。仮想マシン304は、キー(すなわち、アカウントアドレス)を識別して、対応するアカウント状態からアカウントバランスを取得することができる。仮想マシン304は次いで、新たなトランザクションのトランザクション量に基づいてアカウントバランスを計算し、これに応じてハッシュエンコーディングに基づいてワールドステート308を更新することができる。TEE302におけるデータはプレーンテキストの形式であるため、ワールドステート308を更新するために仮想マシン304によって復号化または暗号化を実行する必要はない。

【００４２】

ワールドステート308は、ブロックチェーンネットワークのグローバルステートと呼ぶこともできる。グローバルステートは、ブロックチェーンのアカウントアドレスとアカウント状態との間のマッピングを含むことができる。マッピングは、MPTとして知られているデータ構造に保存することができる。アカウントアドレスおよびアカウント状態は、キーバリューペア(KVP)としてMPTに保存することができる。

【００４３】

グローバルステートのMPTは、所与の時点でのグローバルステートのハッシュである。グローバルステートは、MPTについての安全で一意の識別子として用いられるルートノードを含むことができる。グローバルステートのMPTのルートノードは、アカウント状態を表すデータに暗号で依存することができる。

【００４４】

図3に示す構造300において、それぞれのアカウント状態0 310およびアカウント状態1 3

12を有する2つのアカウントが、ワールドステート308の下に示されている。図3において2つのアカウントのみが示されているが、いくつかの実装形態において、ブロックチェーンは多数のアカウント(すなわち、2つより多い)を含むことができる。アカウントは、外部所有アカウントおよびコントラクトアカウントであり得る。外部所有アカウントは秘密鍵によって制御することができ、いずれのコードにも関連付けられていない。コントラクトアカウントはそれらのコントラクトコードによって制御することができ、これらと関連付けられたコードを有する。

【００４５】

いくつかの実施形態において、アカウント状態は、状態1 312の下で図示のように4つの構成要素を含むことができる。4つの構成要素は、ナンス314、バランス316、コードハッシュ318、およびストレージルート320である。アカウントが外部所有アカウントであれば、ナンス314は、アカウントアドレスから送信されたトランザクションの数を表すことができる。バランス316は、アカウントによって所有されているデジタル資産を表すことができる。コードハッシュ318は空の文字列のハッシュである。ストレージルート320は空である。アカウントがコントラクトアカウントであれば、ナンス314は、アカウントによって作成されたコントラクトの数を表すことができる。バランス316は、アカウントによって所有されているデジタル資産を表すことができる。コードハッシュ318は、アカウントに関連付けられた仮想マシンコードのハッシュであり得る。ストレージルート320は、ストレージツリーと呼ばれるMPTのルートノードのハッシュを保存することができる。ストレージツリーは、アカウントのストレージ内容のハッシュをエンコードすることによってコントラクトデータを保存することができる。ストレージツリーは、MPTのデータ構造も有するため、コントラクトデータまたは変数を保存する1つまたは複数のブランチノードおよびリーフノードを含むことができる。図3に示す構造300において、ストレージツリーは、ブランチノード322と、値1 324、値2 326、および値3 328を格納している3つのリーフノードと、を含む。ストレージツリーは、追加のブランチノードおよびリーフノードを含むことができることが理解されるべきである。

【００４６】

eコール306の内容に基づいて、アカウント状態またはストレージルート320のストレージ内容を仮想マシン304によって取得して、スマートコントラクトを実行することができる。実行結果を用いて、ワールドステート308またはストレージルート320の下のストレージツリーを更新することができる。いくつかの実施形態において、ワールドステート308はMPTとして保存されている。このような場合、データを含むMPTのリーフノードと、これらのリーフノードに関連するブランチを上るノードのみを実行結果で更新する必要がある。その後、仮想マシン304は、TEE302内からコール(oコール330として知られている)を行って、データベース332にワールドステート308を保存することができる。いくつかの例において、データベース332は、RocksDBまたはLevelDBなど、KVP用のデータベースであり得る。いくつかの実施形態において、ワールドステート308は、KVP用のデータベースにキャッシュ同期する前にまず暗号化してキャッシュに保存することができる。いくつかの例において、キャッシュはオーバーレイDB329であり得る。オーバーレイDB329は、TEE302に含めることができ、またはダイレクトメモリアクセスを通じてTEE302から見に行くことができる。いくつかの実施形態において、ワールドステート308は、TEE302を出る前に暗号化される。したがって、TEE302の外部に保存されているワールドステート308は、対応する復号化キーを取得することなしに見られ得ない。

【００４７】

ワールドステート308をTEE302に含めることによって、データ取得および対応するMPTの内容更新を、TEE302内部の信頼できる環境において実行することができる。ワールドステート308は、更新された後、暗号化された形式でTEE302から出力される。そのため、ワールドステート308のデータ構造、アカウント関係、およびアカウント挙動は、適切な暗号キーなしではTEE302の外部から検出することができない。ブロックチェーンアカウントのデータプライバシーは強化することができる。

【００４８】
図4は、本明細書の実施形態によるプロセス400の一例のフローチャートである。便宜上、1つまたは複数の場所に配置され、本明細書に従って適切にプログラムされた、1つまたは複数のコンピュータのシステムによって実行されるものとしてプロセス400を説明する。たとえば、図1のコンピューティングシステム106、108が、適切にプログラムされ、プロセス400を実行することができる。
【００４９】
402で、ブロックチェーンノードが、ブロックチェーンノードのエンクレーブにおいて1つまたは複数のソフトウェア命令を実行する要求を受信する。エンクレーブは、ブロックチェーンノード上で実行されるTEEである。いくつかの例において、要求は、エンクレーブに関連するAPIを介して受信される。いくつかの実施形態において、エンクレーブの外部のアプリケーションは、エンクレーブへのeコール(すなわち、要求)を行って、信頼できるコンピューティング環境においてスマートコントラクトを実行することができる。APIは、アプリケーションが呼び出しを行うために用いることができる。いくつかの実施形態において、要求は、1つまたは複数の入力パラメータを含むことができ、エンクレーブのエンクレーブインターフェース関数に対して行われる。
【００５０】
404で、ブロックチェーンノードのエンクレーブのTCBにおける仮想マシンが、要求に基づいて1つまたは複数のソフトウェア命令を実行するため、1つまたは複数のブロックチェーンアカウントに関連するデータを判定する。いくつかの例において、TCBに保存されているブロックチェーンのグローバルステートが、1つまたは複数のソフトウェア命令の実行中に更新されて更新されたグローバルステートを生成する。いくつかの例において、グローバルステートはワールドステートと呼ばれる。グローバルステートは、TCBに保存することができ、ブロックチェーンの複数のブロックチェーンアカウントのアドレスと状態との間のマッピングを含むことができる。いくつかの実施形態において、グローバルステートはMPTとしてTCBに保存されている。いくつかの実施形態において、複数のブロックチェーンアカウントは、1つまたは複数の外部所有アカウントまたはコントラクトアカウントを含む。コントラクトアカウントのそれぞれはストレージルートを含む。いくつかの実施形態において、ストレージルートは、MPTのルートノードのハッシュを含む。ストレージルートに対応するMPTは、対応するコントラクトアカウントのストレージ内容のハッシュをエンコードする。
【００５１】
406で、仮想マシンは、TEEに保存されているブロックチェーンのグローバルステートを走査して、データを見つける。いくつかの実施形態において、更新されたグローバルステートは、対応するコントラクトアカウントのストレージ内容のハッシュをエンコードするMPTを更新することによって生成される。
【００５２】
408で、ブロックチェーンノードは、データに基づいて1つまたは複数のソフトウェア命令を実行する。いくつかの実施形態において、更新されたグローバルステートは、エンクレーブの外部のデータベースへ保存される前に暗号化される。いくつかの実施形態において、データベースは、RocksDBまたはLevelDBであり得る。
【００５３】
図5は、本明細書の実施形態による装置500のモジュールの一例の図である。装置500は、CPUの一部および物理メモリを含む信頼できるハードウェアの一実施形態の例であり得る。装置500は、上述の実施形態に対応することができ、装置500は以下を含む。すなわち、ブロックチェーンノード上で実行される信頼できる実行環境(TEE)において1つまたは複数のソフトウェア命令を実行する要求を受信するための受信モジュール502と、要求に基づいて1つまたは複数のソフトウェア命令を実行するため、1つまたは複数のブロックチェーンアカウントに関連するデータを判定するための判定モジュール504と、TEEに保存されているブロックチェーンのグローバルステートを走査して、データを見つけるための走査

モジュール506と、データに基づいて1つまたは複数のソフトウェア命令を実行するための実行モジュール508と、である。

【００５４】

任意選択で、要求は、1つまたは複数の入力パラメータを含み、エンクレーブのエンクレーブインターフェース関数に対して行われる。

【００５５】

任意選択で、グローバルステートはMPTとしてTCBに保存されている。

【００５６】

任意選択で、グローバルステートは、ブロックチェーンの複数のブロックチェーンアカウントのアドレスと状態との間のマッピングを含み、複数のブロックチェーンアカウントは、1つまたは複数の外部所有アカウントまたはコントラクトアカウントを含み、コントラクトアカウントのそれぞれがストレージルートを含む。

【００５７】

任意選択で、ストレージルートはMPTのルートノードのハッシュを含み、MPTは、対応するコントラクトアカウントのストレージ内容のハッシュをエンコードする。

【００５８】

任意選択で、更新されたグローバルステートは、対応するコントラクトアカウントのストレージ内容のハッシュをエンコードするMPTを更新することによって生成される。

【００５９】

任意選択で、エンクレーブから分離している保存場所は、キャッシュまたはデータベースに関連している。

【００６０】

本明細書に記載の技法は、1つまたは複数の技術的効果を生み出している。たとえば、主題の実施形態により、信頼できる環境で動いているブロックチェーン仮想マシンが、TEEの外部のアプリケーションからのコールを受信してスマートコントラクトを実行することが可能になる。TEE内部にブロックチェーンのワールドステートを保存することによって、仮想マシンは、TEE内からブロックチェーンデータを取得して、信頼できるコンポーネントと信頼できないコンポーネントとの間のデータトラフィックを減らすことができる。信頼できるコンポーネントと信頼できないコンポーネントとの間を移動するデータは暗号化または復号化する必要があるため、エンクレーブを通過するデータトラフィックが少なくなる結果、計算リソースの消費が少なくなり、データセキュリティが高くなる。また、ワールドステートをTEE内に含めることによって、信頼できる環境においてプレーンテキストに基づいてワールドステートのデータ取得および内容更新を実行することができる。ワールドステートは、更新および暗号化された後にエンクレーブの外部のデータベースに出力されるため、ワールドステートのデータ構造、アカウント関係、およびアカウント挙動は、TEEの外部からは見ることができない。ブロックチェーンアカウントのデータプライバシーは強化することができる。

【００６１】

説明した方法により、様々なブロックチェーントランザクションおよびトランザクション/データセキュリティ全体の強化が可能になる。スマートコントラクトを実行するためのコールを開始するブロックチェーンユーザは、信頼できる環境で計算が実行され、計算結果は変更され得ないことを確信することができる。ブロックチェーンのワールドステートの暗号化テキストのみがTEEの外部に保存されている状態では、ブロックチェーンアカウントの挙動および関係を識別することは極めて困難または不可能になるので、更新されたワールドステートをバッチで暗号化してデータ構造を隠し、下にあるデータおよびトランザクションの高レベルのセキュリティを可能にすることができる。

【００６２】

ワールドステートからのブロックチェーンデータはプレーンテキストで保存され、TEEの内部で取得および更新されるため、前述の方法は、コンピュータリソース(たとえば、処理サイクル、ネットワーク帯域幅、およびメモリ使用)の効率的な使用を保証すること

ができる。少なくともこれらのアクションは、ブロックチェーンデータの暗号化および復号化に関して利用可能なコンピュータリソースの浪費を最小限に抑えるか、防ぐことができる。仮想マシンは、スマートコントラクト処理のためにデータを復号化する代わりに、エンクレーブの内部のプレーンテキスト上で直接動作することができる。

【００６３】

先の実施形態において示したシステム、装置、モジュール、またはユニットは、コンピュータチップまたはエンティティを用いることによって実装することができ、または特定の機能を有する製品を用いることによって実装することができる。典型的な実施形態のデバイスはコンピュータであり、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、携帯電話、カメラ付き電話、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み合わせであり得る。

【００６４】

装置における各モジュールの機能および役割の実施形態プロセスについて、先の方法における対応するステップの実施形態プロセスを参照することができる。簡略化のためここでは詳細を省略する。

【００６５】

装置の実施形態は基本的に方法の実施形態に対応するので、関連する部分について、方法の実施形態における関連する説明を参照することができる。前述の装置の実施形態は単なる一例である。分離した部分として説明したモジュールは、物理的に分離していることもしていないこともあり、モジュールとして表示された部分は、物理的モジュールであることもそうでないこともあり、1つの位置に配置することも、またはいくつかのネットワークモジュールに分散させることもできる。モジュールのいくつかまたはすべてを実際の要求に基づいて選択して、本明細書の解決策の目的を達成することができる。当業者は、創造的な努力なしに本願の実施形態を理解し実装することができる。

【００６６】

主題の記載の実施形態は、1つまたは複数の特徴を、単独でまたは組み合わせて含むことができる。

【００６７】

たとえば、第1の実施形態において、ブロックチェーンノードによって、ブロックチェーンノード上で実行される信頼できる実行環境(TEE)において1つまたは複数のソフトウェア命令を実行する要求を受信し、TEEにおける仮想マシンによって、要求に基づいて1つまたは複数のソフトウェア命令を実行するため、1つまたは複数のブロックチェーンアカウントに関連するデータを判定し、仮想マシンによって、TEEに保存されているブロックチェーンのグローバルステートを走査してデータを見つけ、そして仮想マシンによって、データに基づいて1つまたは複数のソフトウェア命令を実行する。

【００６８】

前述および他の記載の実施形態はそれぞれ、任意選択で、以下の特徴の1つまたは複数を含むことができる。

【００６９】

第1の特徴は、以下の特徴のいずれかと組み合わせ可能であり、要求は、1つまたは複数の入力パラメータを含み、TEEのインターフェース関数に対して行われることを特定している。

【００７０】

第2の特徴は、先のまたは以下の特徴のいずれかと組み合わせ可能であり、グローバルステートは、マークルパトリシアツリー(MPT)としてTEEに保存されていることを特定している。

【００７１】

第3の特徴は、先のまたは以下の特徴のいずれかと組み合わせ可能であり、グローバル

ステートは、ブロックチェーンの複数のブロックチェーンアカウントのアドレスと状態との間のマッピングを含み、複数のブロックチェーンアカウントは、1つまたは複数の外部所有アカウントまたはコントラクトアカウントを含み、コントラクトアカウントのそれぞれはストレージルートを含むことを特定している。

【００７２】

第4の特徴は、先のまたは以下の特徴のいずれかと組み合わせ可能であり、ストレージルートはMPTのルートノードのハッシュを含み、MPTは、対応するコントラクトアカウントのストレージ内容のハッシュをエンコードすることを特定している。

【００７３】

第5の特徴は、先のまたは以下の特徴のいずれかと組み合わせ可能であり、更新されたグローバルステートは、対応するコントラクトアカウントのストレージ内容のハッシュをエンコードするMPTを更新することによって生成されることを特定している。

【００７４】

第6の特徴は、先のまたは以下の特徴のいずれかと組み合わせ可能であり、TEEから分離している保存場所は、キャッシュまたはデータベースに関連していることを特定している。

【００７５】

第7の特徴は、先のまたは以下の特徴のいずれかと組み合わせ可能であり、要求は、TEEに関連するアプリケーションプログラミングインターフェースを介して受信されることを特定している。

【００７６】

第8の特徴は、先のまたは以下の特徴のいずれかと組み合わせ可能であり、TEEに保存されているブロックチェーンのグローバルステートは、1つまたは複数のソフトウェア命令の実行中に更新されて更新されたグローバルステートを生成し、このコンピュータで実施される方法は、1つまたは複数のソフトウェア命令の実行に応じて、ブロックチェーンノードによって、更新されたグローバルステートの暗号化表現を生成するステップと、ブロックチェーンノードによって、TEEから分離している保存場所に更新されたグローバルステートの暗号化表現を保存するステップと、をさらに含むことを特定している。

【００７７】

本明細書に記載の主題とアクションおよび動作との実施形態は、本明細書に開示された構造およびそれらの構造的等価物を含む、デジタル電子回路において、具体的に実現されたコンピュータソフトウェアまたはファームウェアにおいて、コンピュータハードウェアにおいて、またはこれらの1つまたは複数の組み合わせにおいて実装することができる。本明細書に記載の主題の実施形態は、1つまたは複数のコンピュータプログラム、たとえば、データ処理装置による、またはデータ処理装置の動作を制御するための実行のためにコンピュータプログラム担体上にエンコードされたコンピュータプログラム命令の1つまたは複数のモジュールとして実装することができる。たとえば、コンピュータプログラム担体は、命令がエンコードまたは格納されている1つまたは複数のコンピュータ可読記憶媒体を含むことができる。担体は、磁気ディスク、光磁気ディスク、光ディスク、ソリッドステートドライブ、ランダムアクセスメモリ(RAM)、リードオンリメモリ(ROM)、または他のタイプの媒体など、具体的な非一時的コンピュータ可読媒体であってよい。あるいは、または加えて、担体は、人工的に生成された伝播信号、たとえば、データ処理装置による実行のために適切な受信機装置に伝送するための情報をエンコードするために生成される、機械生成の電気、光、または電磁信号であってよい。コンピュータ記憶媒体は、機械可読ストレージデバイス、機械可読ストレージ基板、ランダムまたはシリアルアクセスメモリデバイス、またはこれらの1つまたは複数の組み合わせであってよい。コンピュータ記憶媒体は伝播信号ではない。

【００７８】

コンピュータプログラムは、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、アプリ、モジュール、ソフトウェアモジュール、エンジン、スクリプト、またはコー

ドとも呼ばれ、または記載されることがあり、コンパイルもしくはインタプリタされた言語、または宣言型もしく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記述することができ、スタンドアロンプログラムとして、またはモジュールとして、コンポーネント、エンジン、サブルーチン、またはコンピューティング環境における実行に適した他のユニットを含む、任意の形態でデプロイすることができ、この環境は、1つまたは複数の場所にあるデータ通信ネットワークによって相互接続された1つまたは複数のコンピュータを含むことができる。

【００７９】

コンピュータプログラムは、ファイルシステムにおけるファイルに対応することがあるが、対応する必要はない。コンピュータプログラムは、他のプログラムもしくはデータ、たとえば、マークアップ言語ドキュメントに格納された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に、問題のプログラム専用の単一ファイルに、または複数の協調ファイル、たとえば、1つまたは複数のモジュール、サブプログラム、もしくはコードの一部を格納するファイルに格納することができる。

【００８０】

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、汎用および専用の両方のマイクロプロセッサ、およびあらゆる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、実行のためのコンピュータプログラムの命令、ならびにプロセッサに結合された非一時的コンピュータ可読媒体からのデータを受信する。

【００８１】

「データ処理装置」という用語は、例としてプログラマブルプロセッサ、コンピュータ、または複数のプロセッサまたはコンピュータを含む、データを処理するためのあらゆる種類の装置、デバイス、および機械を包含する。データ処理装置は、専用論理回路、たとえば、FPGA(フィールドプログラマブルゲートアレイ)、ASIC(特定用途向け集積回路)、またはGPU(グラフィックスプロセッシングユニット)を含むことができる。この装置はまた、ハードウェアに加えて、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、またはこれらの1つまたは複数の組み合わせを構成するコードを含むことができる。

【００８２】

本明細書に記載のプロセスおよび論理フローは、1つまたは複数のコンピュータプログラムを実行する1つまたは複数のコンピュータまたはプロセッサによって実行され、入力データに作用して出力を生成することによって動作を実行することができる。これらのプロセスおよび論理フローはまた、専用論理回路、たとえば、FPGA、ASIC、またはGPUによって、または専用論理回路と1つまたは複数のプログラムされたコンピュータとの組み合わせによって実行することができる。

【００８３】

コンピュータプログラムの実行に適したコンピュータは、汎用もしくは専用マイクロプロセッサまたはその両方、または任意の他の種類の中央処理装置に基づくことができる。一般に、中央処理装置は、リードオンリメモリまたはランダムアクセスメモリまたはその両方から命令およびデータを受信することになる。コンピュータの要素は、命令を実行するための中央処理装置と、命令およびデータを格納するための1つまたは複数のメモリデバイスと、を含むことができる。中央処理装置およびメモリは、専用論理回路によって補完する、またはこれに組み込むことができる。

【００８４】

一般に、コンピュータはまた、1つまたは複数のストレージデバイスを含むか、またはそこからデータを受信もしくはそこへデータを転送するように動作可能に結合されることになる。ストレージデバイスは、たとえば、磁気ディスク、光磁気ディスク、光ディスク、ソリッドステートドライブ、または任意の他のタイプの非一時的、コンピュータ可読媒

体であってよい。しかしながら、コンピュータはこのようなデバイスを有する必要はない。したがって、コンピュータは、ローカルおよび/またはリモートである、1つまたは複数のメモリなど、1つまたは複数のストレージデバイスに結合されてもよい。たとえば、コンピュータは、コンピュータの不可欠な構成要素である1つまたは複数のローカルメモリを含むことができ、またはコンピュータは、クラウドネットワークにある1つまたは複数のリモートメモリに結合することができる。また、コンピュータは、他のデバイス、ほんの数例を挙げると、たとえば、携帯電話、携帯情報端末(PDA)、モバイルオーディオまたはビデオプレーヤ、ゲームコンソール、全地球測位システム(GPS)受信機、またはポータブルストレージデバイス、たとえば、ユニバーサルシリアルバス(USB)フラッシュドライブに組み込むことができる。

【００８５】

コンポーネントは、直接または1つまたは複数の中間コンポーネントを介して、電気的または光学的になど通信可能に互いに接続されることによって、互いに「結合」することができる。コンポーネントはまた、コンポーネントの1つが他のコンポーネントに統合されていれば、互いに「結合」することができる。たとえば、プロセッサに統合されているストレージコンポーネント(たとえば、L2キャッシュコンポーネント)は、プロセッサに「結合」されている。

【００８６】

ユーザとの相互作用を提供するため、本明細書に記載の主題の実施形態は、ディスプレイデバイス、たとえば、ユーザに情報を表示するためのLCD(液晶ディスプレイ)モニタ、ユーザがコンピュータに入力を提供することができる入力デバイス、たとえば、キーボードおよびポインティングデバイス、たとえば、マウス、トラックボールまたはタッチパッドを有するコンピュータ上で実装、またはこれと通信するように構成することができる。他の種類のデバイスを用いて、ユーザとの相互作用を提供することもできる。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であってよく、ユーザからの入力は、音響、音声、または触覚の入力を含む任意の形態で受信することができる。加えて、コンピュータは、ユーザによって用いられるデバイスとの間で文書を送受信することによって、たとえば、ユーザのデバイス上のウェブブラウザに、そのウェブブラウザから受信された要求に応じてウェブページを送信することによって、またはユーザデバイス、たとえば、スマートフォンまたは電子タブレット上で動いているアプリと相互作用することによって、ユーザと相互作用することができる。また、コンピュータは、テキストメッセージまたは他の形態のメッセージを個人用デバイス、たとえば、メッセージングアプリケーションを動かしているスマートフォンに送信し、ユーザから返信として応答メッセージを受信することによって、ユーザと相互作用することができる。

【００８７】

本明細書では、システム、装置、およびコンピュータプログラムコンポーネントに関連して「ように構成され」という用語を用いている。特定の動作またはアクションを実行するように構成される1つまたは複数のコンピュータのシステムとは、動作中にシステムにその動作またはアクションを実行させるソフトウェア、ファームウェア、ハードウェア、またはこれらの組み合わせがシステムにインストールされていることを意味する。特定の動作またはアクションを実行するように構成される1つまたは複数のコンピュータプログラムとは、データ処理装置によって実行されると、その装置にその動作またはアクションを実行させる命令を1つまたは複数のプログラムが含むことを意味する。特定の動作またはアクションを実行するように構成される専用論理回路とは、その回路はその動作またはアクションを実行する電子論理を有することを意味する。

【００８８】

本明細書は多くの具体的な実施形態の詳細を含むが、これらは、請求項自体によって定義された、特許請求されている範囲に対する限定としてではなく、特定の実施形態に特有の特徴の説明として解釈されるべきである。別個の実施形態の文脈で本明細書に記載した

いくつかの特徴は、単一の実施形態において組み合わせて実現することもできる。逆に、単一の実施形態の文脈で説明した様々な特徴も、複数の実施形態において別個に、または任意の適切なサブコンビネーションで実現することができる。さらに、いくつかの組み合わせで動作するものとして特徴を上で説明し、最初はそのように特許請求さえしたが、特許請求された組み合わせからの1つまたは複数の特徴はいくつかの場合において組み合わせから削除することができ、特許請求の範囲はサブコンビネーションまたはサブコンビネーションの変形を対象とすることがある。

【００８９】

同様に、特定の順序で動作が図面において描かれ、特許請求の範囲に記載されているが、これは、所望の結果を達成するために、そのような動作を示した特定の順序でまたは連続した順序で実行すること、またはすべての説明した動作を実行することを要求するものとして理解されるべきではない。いくつかの状況において、マルチタスクおよび並列処理が有利なことがある。さらに、上述の実施形態における様々なシステムモジュールおよびコンポーネントの分離は、すべての実施形態においてそのような分離を必要とするものとして理解されるべきではなく、説明したプログラムコンポーネントおよびシステムは一般に単一のソフトウェア製品に統合することも複数のソフトウェア製品にパッケージ化することもできることが理解されるべきである。

【００９０】

本主題の特定の実施形態を説明してきた。以下の特許請求の範囲内には他の実施形態がある。たとえば、特許請求の範囲に記載されたアクションは、異なる順序で実行することができ、それでも望ましい結果を達成することができる。一例として、添付の図面に描かれたプロセスは、望ましい結果を達成するために、示した特定の順序、または連続的な順序を必ずしも必要としない。いくつかの場合において、マルチタスクおよび並列処理が有利なことがある。

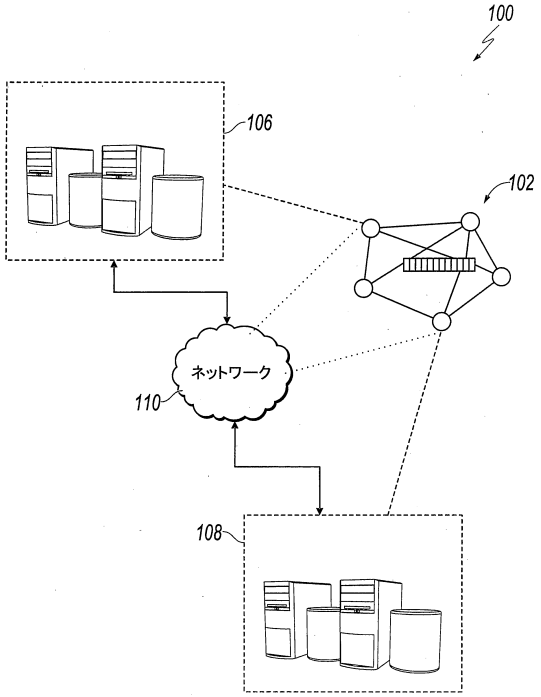
【符号の説明】

【００９１】

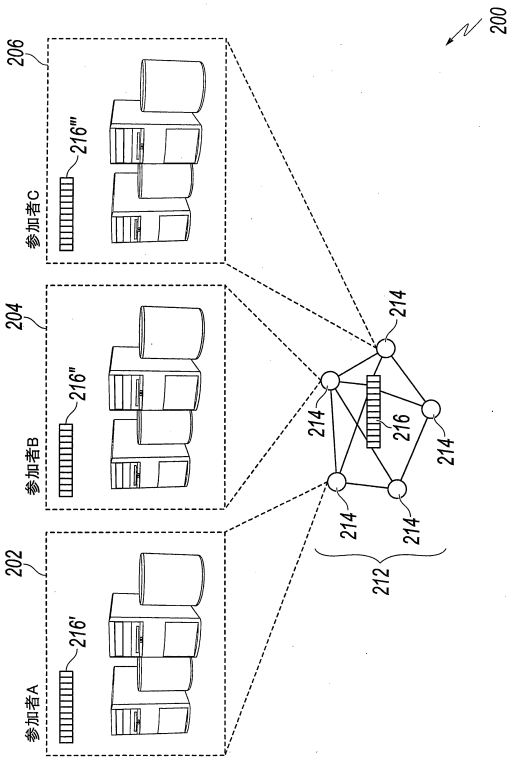
100 環境
102 コンソーシアムブロックチェーンネットワーク
106 コンピューティングデバイス
108 コンピューティングデバイス
110 ネットワーク
200 アーキテクチャ
202 エンティティ層
204 ホステッドサービス層
206 ブロックチェーンネットワーク層
212 ブロックチェーンネットワーク
214 ノード
216 ブロックチェーン
300 構造
302 TEE
304 仮想マシン
306 eコール
308 ワールドステート
310 状態0
312 状態1
314 ナンス
316 バランス
318 コードハッシュ
320 ストレージルート
322 ブランチノード

324　値1
326　値2
328　値3
329　オーバーレイDB
330　oコール
332　データベース
400　プロセス
500　装置
502　受信モジュール
504　判定モジュール
506　走査モジュール
508　実行モジュール

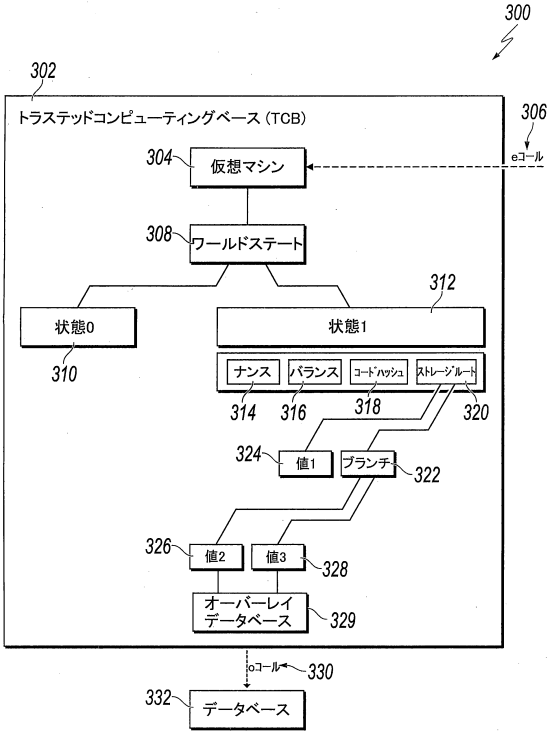
【図１】



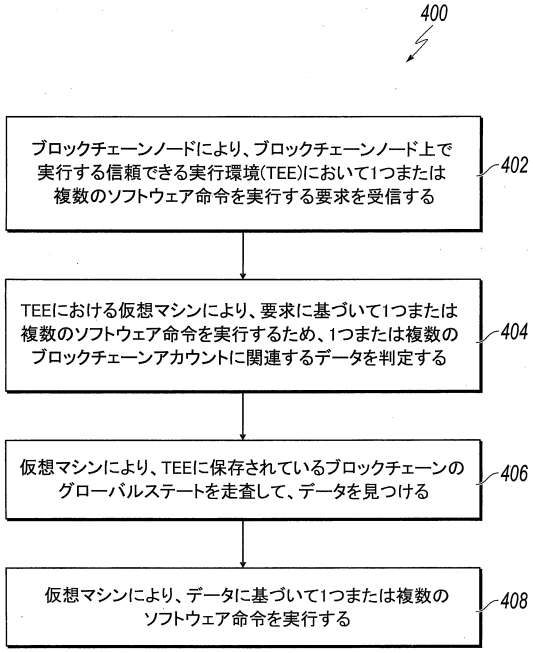
【図２】



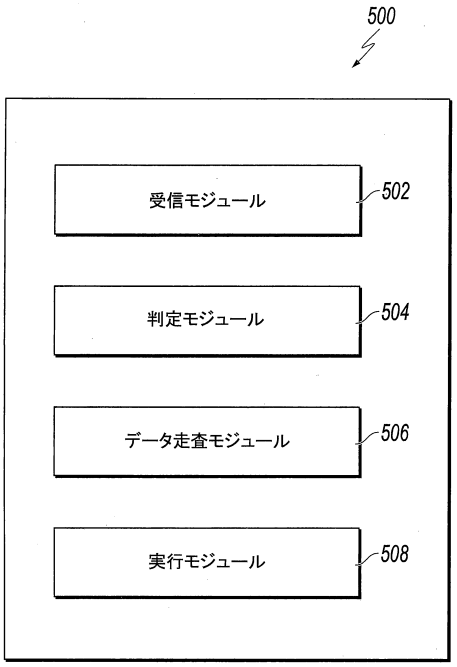
【図３】


300
302
トラステッドコンピューティングベース（TCB）
306
eコール
304
仮想マシン
308
ワールドステート
312
状態0
状態1
310
ナンス
バランス
コードハッシュ
ストレージルート
314
316
318
320
324
値1
ブランチ
322
326
値2
値3
328
オーバーレイデータベース
329
oコール
330
332
データベース

【図４】


400
ブロックチェーンノードにより、ブロックチェーンノード上で実行する信頼できる実行環境(TEE)において1つまたは複数のソフトウェア命令を実行する要求を受信する
402
TEEにおける仮想マシンにより、要求に基づいて1つまたは複数のソフトウェア命令を実行するため、1つまたは複数のブロックチェーンアカウントに関連するデータを判定する
404
仮想マシンにより、TEEに保存されているブロックチェーンのグローバルステートを走査して、データを見つける
406
仮想マシンにより、データに基づいて1つまたは複数のソフトウェア命令を実行する
408

【図５】


500
受信モジュール
502
判定モジュール
504
データ走査モジュール
506
実行モジュール
508

フロントページの続き

(72)発明者　チャンジェン・ウェイ
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　イン・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
(72)発明者　ボラン・ジャオ
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　シュヤン・ソン
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

審査官　岸野　徹

(56)参考文献　米国特許出願公開第２０１８／０３０９５６７（ＵＳ，Ａ１）
特開２００５－２２７９９５（ＪＰ，Ａ）
佐藤　雅史　MASASHI　SATOU，ブロックチェーンの技術の教科書　初版，株式会社シーアンドアール研究所　池田　武人，２０１８年　４月２３日，第1版，pp.140-161
加嵜　長門，ブロックチェーンアプリケーション開発の教科書　初版，株式会社マイナビ出版　滝口　直樹，２０１８年　１月３１日，第1版，pp.64-74
Ethreum，Ethreum白書，２０１９年　２月　３日，73 revisions，pp.1-50，ＵＲＬ，https://github.com/ethereum/wiki/wiki/[Japanese]-White-Paper
"An introduction creating a sample enclave using Intel Software Guard Extensions"，Intel，２０１６年　７月２１日，pp.1-18，ＵＲＬ，https://software.intel.com/en-us/articles/intel-software-guard-extensions-developing-a-sample-enclave-application
小松　昌平，プロセス内処理に対する遠隔認証手法の提案と実装，ＣＳＳ２０１８　コンピュータセキュリティシンポジウム２０１８論文集　［ＵＳＢ］，日本，一般社団法人情報処理学会，２０１８年１２月３１日，第2018巻，pp.1066-1072

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／１２
Ｇ０６Ｆ　２１／６２
Ｈ０４Ｌ　９／３２