(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7410060号
(P7410060)

(45)発行日　令和6年1月9日(2024.1.9)

(24)登録日　令和5年12月25日(2023.12.25)

(51)国際特許分類			FI		
H04L	*9/32*	*(2006.01)*	H04L	9/32	200Z
G06F	*21/62*	*(2013.01)*	G06F	21/62	318
G06F	*21/60*	*(2013.01)*	G06F	21/60	320

請求項の数　2　（全9頁）

(21)出願番号　特願2020-571719(P2020-571719)
(86)(22)出願日　令和1年7月18日(2019.7.18)
(65)公表番号　特表2022-548185(P2022-548185A)
(43)公表日　令和4年11月17日(2022.11.17)
(86)国際出願番号　PCT/ES2019/070503
(87)国際公開番号　WO2021/009390
(87)国際公開日　令和3年1月21日(2021.1.21)
審査請求日　令和4年7月15日(2022.7.15)

(73)特許権者　520498206
オールファウンズ バンク エスエイユー
ＡＬＬＦＵＮＤＳ ＢＡＮＫ， Ｓ．Ａ．Ｕ．
スペイン国 ２８０５０ マドリード カレー デ ロス パドレス ドミニコス ニュメロ ７
(74)代理人　100147485
弁理士　杉村 憲司
(74)代理人　230118913
弁護士　杉村 光嗣
(74)代理人　100221899
弁理士　高倉 みゆき
(72)発明者　アルベルト ミゲル ヘルナンデス アコスタ

最終頁に続く

(54)【発明の名称】　制限トランザクションを有するブロックチェーンシステム

(57)【特許請求の範囲】

【請求項１】

少なくとも１つのパブリックトランザクション及び制限トランザクションを同時に分散させるように構成されるブロックチェーンシステムであって、

電気通信ネットワーク（１４）によって接続される複数の宛先参加者ノード（１２）と複数の検証ノード（１３）とを含み、

前記複数の宛先参加者ノード（１２）のうち、提案参加者ノード（１２）は、情報トランザクションレコードt_xのコンテンツを、特定の事前構成されたプライバシーグループの識別子と共に、前記複数の検証ノード（１３）の全てに送信するように構成され、

前記複数の検証ノード（１３）のうち、受信検証ノード（１３）が、前記提案参加者ノード（１２）からの制限トランザクション実行要求メッセージを受信するように構成され、

前記受信検証ノード（１３）は、特定の事前構成されたプライバシーグループに入力されるメンバに基づいて前記複数の宛先参加者ノード（１２）を決定する、ブロックチェーンシステム。

【請求項２】

前記受信検証ノード（１３）によって受信される前記制限トランザクション実行要求メッセージが、前記提案参加者ノード（１２）によって提案されたトランザクションデータに加えて、前記制限トランザクションが実行されるプライバシーコンテキストに関するメタデータを含む、請求項１に記載のブロックチェーンシステム。

【発明の詳細な説明】

【技術分野】
【０００１】
本発明は、情報の転送又はトランザクション、より具体的には、ブロックチェーンソリューションの提供者に関する。提供者とはすなわち、暗号化され得る情報トランザクションレコードのブロックを検証及び分散させる分散ノードのネットワークであり、ブロックチェーンネットワークに接続される少なくとも１つの受信者メンバは、ブロックチェーンネットワーク内の検証ノード又はマイニングノードによって暗号化されたトランザクションレコードのブロックを、復号化、読み取り及び実行できる。
【背景技術】
【０００２】
どのような業界においても、特定のサービス及び／又はサービス資産を中心に多数のプライベートネットワークが構築されている。金融資産を中心に構築されるプライベートネットワークは、例えば銀行、清算機関等、金融資産の転送を要求する規制機関、顧客等のサービス提供者のような複数のネットワークメンバを含むことができる。
【０００３】
プライベートネットワーク及び一般的な任意のネットワークの主要な関心事の１つは、これらのシステムによって実行されるトランザクションのコンテンツが、トランザクション参加者にのみ開示されることを保証することである。
【０００４】
例えば、第１の顧客の金融資産からの情報の転送を処理するサービス提供者は、この情報の転送の内容を、転送に関与していない無許可の顧客に開示しないだろう。
【０００５】
サービス提供者は、他のアクターが対話する独自のシステムを開発するが、残りのネットワークメンバもまた独自のシステムを開発し、サービス提供者との統合を可能にする。このシナリオは本質的に、異なる技術で作成され、異なるプロトコルで相互接続される多くのシステムの共存を伴う。このようにシステムが多様であることは、解決が困難ないくつかの問題をもたらす。
【０００６】
第１に、各個々のシステムは、システムの開発に使用する技術及び各参加者の適応の両方によって、別の個々のシステムとは本質的に異なっている。各参加者による多額の個別投資を必要とすることに加えて、システム間の情報を適切な方法で統合して送信する必要がある。
【０００７】
第２に、各個々のシステムは、実装されるセキュリティのレベルが異なる場合がある。例えば、各ネットワークは、暗号化、認証、データマスキング等に対する異なるプロトコルを提供することができる。したがって、一部のシステムは侵害の影響を受けやすくなり、侵害されたシステムと他のシステムが共有しているデータの両方に影響を与える可能性がある。
【０００８】
第３に、各システムの性質が異なるということは、データが標準化されていない方法で格納されていることを意味する。これは、データ調整を繰り返し行い、異なるシステム間で共有されるデータのサブセットが同等であることを確認しなければならないことを意味する。
【０００９】
最後に、第４に、参加者の１人からの情報が失われる可能性がある場合、情報の回復には非常に費用がかかり、影響を受けるシステムが利用できないかなりの時間を必要とする。
【発明の概要】
【発明が解決しようとする課題】
【００１０】
本発明は、特許請求の範囲に定義されるように、少なくとも１つの制限トランザクショ

ンを有するブロックチェーン装置によって、上記の欠点の１つ以上を解決しようとするものである。

【課題を解決するための手段】

【００１１】

提案されたブロックチェーンシステムは、他のブロックチェーンシステムでは現在利用できない匿名性及びプライバシーの機能を提供する。これら２つの新機能は、単鎖内の差別化要素として開発され、ブロックチェーンネットワークの全ての統合ノードで共有される。

【００１２】

ブロックチェーンネットワークは、複数の参加ノードと、権限の証拠の合意形成機構を有する検証ノード又はマイニングノードとを含む。

【００１３】

この方法は、複数の検証ノードに対して、提案参加ノードからの制限トランザクションに対する提案された情報トランザクションレコードブロックを、ブロックチェーンネットワークの複数の宛先参加ノード又はブロックチェーンノードに送信される制限匿名情報トランザクションレコードブロックに変換する能力を提供する。

【００１４】

受信検証ノードは、暗号化された情報トランザクションレコードを有するブロックをブロックチェーンネットワーク内の宛先参加ノードに送信するように構成される。

【００１５】

受信検証ノード、すなわちマイニングノードによって検証されたトランザクションは、パブリック情報トランザクションレコードがすなわちブロックチェーン内のブロック内部で行われるのと同様の方法で、受信検証ノードからブロックチェーンネットワーク内の全ての宛先参加ノードに送信される。

【００１６】

検証されたトランザクションは、受信検証ノードによって暗号化され、トランザクションの参加ノードだけが読み取り及び実行できる。

【００１７】

したがって、ブロックチェーンは、無差別にパブリック及び／又は制限付き、すなわちプライベートな情報トランザクションレコードを含むブロックからなる。

【００１８】

このソリューションでは、少なくとも２種類の情報トランザクションレコードが共存する単鎖のみを使用し、これらはパブリック情報トランザクションレコード及び／又は制限情報トランザクションレコード（プライベート及び匿名）であることに留意することが重要である。

【００１９】

検証ノードは、提案参加ノードからの提案された情報トランザクションレコードを暗号化するように構成され、検証ノードは暗号化段階の最後に制限情報トランザクションレコードを提供する。

【００２０】

暗号化された情報トランザクションレコードは、提案された制限トランザクションが行われるプライバシーグループに対応する暗号化秘密鍵（privacy key）を保持するブロックチェーンネットワーク内の参加ノードによってのみ復号化及び実行できる。

【００２１】

プライバシーグループは、少なくとも１つの暗号化秘密鍵を共有するブロックチェーンネットワーク内のノードのサブセットであり、プライバシーグループ内のノード間で送信される制限トランザクションを読み取る。

【００２２】

ブロックチェーンネットワークのメンバは、少なくとも１つのプライバシーグループの一部とすることができ、最大でもブロックチェーンネットワークを含む異なるメンバの組

み合わせと同じ数のプライバシーグループに属することができる。
【００２３】
ブロックチェーンネットワーク内の参加ノード又はブロックチェーンノードとは、ブロックチェーンの自身のローカルコピー、すなわちレコードブック又は台帳を保持、共有及び運用する自然人又は法人を指す。
【００２４】
更に、メンバとは、情報トランザクションを行い、ブロックチェーン内の特定の情報トランザクションレコードにアクセスする権限を与えられている自然人又は法人を指す。
【００２５】
参加ノードは、参加ノードが含まれるプライバシーグループ内の制限情報トランザクションを記録することを目的とする複数の暗号化秘密鍵を含むだろう。
【００２６】
検証ノードは、提案参加ノードからの提案された情報トランザクションレコードを特定のプライバシーグループの暗号化秘密鍵で暗号化し、更に、暗号化されたトランザクションレコードデータブロックを制限付きとしてマークし、その後、作成されたブロックは、暗号化された情報トランザクションレコードを含み、ブロックチェーンに組み立てられ、後に検証ノードからブロックチェーンネットワークのメンバである他のノードに分散する。
【００２７】
したがって、ブロックチェーンネットワークに接続されるプライバシーグループの任意のメンバは、新しく作成されたブロックに含まれる特定の情報トランザクションの詳細にアクセスできる。
【００２８】
参加受信者ノードは、各プライバシーグループに割り当てられる暗号化秘密鍵のセットの中から該当する暗号化秘密鍵を使用して、作成されたブロックの制限情報トランザクションレコードを復号化する。
【００２９】
したがってシステムは、最終的にブロックチェーン内で組み立てられて全てのネットワークメンバに一様に分散するブロックに含まれる、制限トランザクション又はプライベートトランザクション及びパブリックトランザクションのレコードを提供することで、暗号化によりトランザクションのプライバシーを提供するだけでなく、ブロックが検証ノードによってのみ分散するため、匿名性を提供する。
【００３０】
ブロックチェーン内の全てのネットワークメンバは単鎖又は台帳を使用するため、冗長な資源を排除して個々のシステムを管理する。
【００３１】
ブロックチェーンネットワークのメンバは、そのメンバ、つまりブロックチェーンネットワーク内のノード又はプライバシーグループの一部のメンバが資格を付与された情報トランザクションの詳細にしかアクセスできないため、プライバシーが暗号化によって達成される。
【００３２】
情報要約アルゴリズムの使用はまた、トランザクションレコードの不変性を確立し、起こり得る悪意のある行為から保護する。暗号化されたトランザクションレコードはメンバによってローカルに格納されるため、データの信頼性が向上する。
【図面の簡単な説明】
【００３３】
【図１】電気通信ネットワークを介して接続され、ブロックチェーンからのパブリック及びプライベート情報トランザクションレコードを同時にブロードキャスト又は伝播する複数のノードを含む、ブロックチェーンネットワークのブロック図である。
【発明を実施するための形態】
【００３４】

以下では、添付の図面に基づいて、より詳細な説明を行う。

【００３５】

ブロックチェーンネットワーク１１の環境が表示されている図１に関連して、複数のノード、参加者１２、及び検証者又は採掘者（miner）１３が電気通信ネットワーク１４を介して接続され、ブロックのチェーン又はブロックチェーンに追加されるデータブロック内に分散するトランザクションを共有及び実行する。

【００３６】

ブロックチェーンは、電気通信ネットワーク１４を介して、ブロックチェーンネットワーク１１の１つの検証ノード１３から残りのノード１２、１３に分散する。

【００３７】

電気通信ネットワーク１４は、有線又は無線のＬＡＮ（ローカルエリアネットワーク）、イントラネット、エクストラネット又はインターネットなどのワイドエリアネットワーク（ＷＡＮ）とすることができる。電気通信ネットワーク１４は、ブロックチェーンネットワーク１１のノード１２及びノード１３間の通信を容易にする。

【００３８】

ブロックチェーンネットワーク１１内のノード１２及びノード１３は、オペレーティングシステムを実行するコンピュータと同様の電子機器である。

【００３９】

ブロックチェーンネットワーク１１を構成するノード１２及びノード１３は、コンピュータ可読記憶媒体に格納された命令を実行するように構成される。更に、全てのノード１２及びノード１３は、通信プロトコルを実行して、ブロックチェーンネットワーク１１によって提供されるサービス及び／又はコンテンツと対話する。

【００４０】

ブロックチェーンネットワーク１１内の全てのノード１２及びノード１３は、自身のローカルコピーのチェーンデータに対する読み取りアクセス権を持っている。検証ノード又はマイニングノード１３のみが、パブリック及び制限トランザクションレコードを持つ新しいブロックを発行又は作成できる。

【００４１】

あるパブリックトランザクション及び／又は制限トランザクションは、その検証及び合意形成のために、すなわち参加ノード１２から他の検証ノードに送信される。トランザクションが検証及び同意されると、検証ノードは、ブロックチェーンに追加するデータのブロックを生成する。各データブロックは直前のデータブロックに対するハッシュを含み、前の情報の変更を防止する。

【００４２】

しかし、参加ノード１２がプライベート又は制限トランザクションを提案する場合、提案されたトランザクションは、大多数の検証ノード又はマイニングノード１３によって検証されなければならない。このトランザクションは、電気通信ネットワーク１４を介して検証ノード又はマイニングノード１３に送信される。

【００４３】

制限トランザクション実行要求の受信検証ノード１３は、特定の事前構成されたプライバシーグループに入力されるメンバに従って、参加ノード１２を決定する。制限トランザクション実行要求メッセージは、提案されたトランザクションに特有のデータに加えて、制限トランザクションが実行されるプライバシーコンテキストに関連するメタデータも含む。

【００４４】

提案された制限トランザクションは、その検証及び合意形成のために、受信検証ノード１３から少なくとも１つ以上の検証ノード１３に送信可能である。各検証ノード１３は、トランザクションが有効で他の検証ノード１３と整合性があるかどうか、及びそれをチェーン内の次のブロックに統合すべきかどうかを判定する。

【００４５】

したがって、参加ノード１２及び検証ノード１３のネットワーク１１は、パブリック及び／又は制限トランザクションによって同時に構成されるデータブロックのチェーンを維持及び管理する。このように、特定のプライバシーグループ内の参加ノード１２のみが制限トランザクション及びパブリックトランザクションに対する同時アクセス権を持っているにもかかわらず、各ノード１２及びノード１３は、パブリック情報トランザクションレコードであるか制限情報トランザクションレコードであるかにかかわらず、全てのデータブロックに対するアクセス権を持っている。

【００４６】

ブロックチェーンネットワーク内の参加ノード１２によって提案されたトランザクションは、ＭＤ５、セキュアハッシュアルゴリズム、ＳＨＡ、ＢＬＡＫＥ又は他の類似のハッシュ関数のようなそのバイナリコンテンツに対する要約数学関数の実行に対応する固有識別子を有する。この固有識別子は、トランザクションハッシュと呼ばれる。

【００４７】

制限情報トランザクションを開始するために、提案者参加ノード１２は、プライバシーグループ識別子と共に、情報トランザクションレコードt_xのコンテンツを全ての検証ノード１３にプライベート送信する。

【００４８】

検証ノード１３は情報トランザクションを実行し、情報トランザクションが大多数の検証ノード１３によって検証及び同意されると、情報トランザクションレコードt_xは検証ノード１３の暗号化モジュールによって暗号化される。

【００４９】

暗号化された情報トランザクションt_xは新しい情報トランザクションt_x’によってカバーされるので、情報トランザクションt_x’は情報トランザクションtxと同じハッシュ識別子を強制的に維持する。このようにして、暗号化されたデータブロックは、暗号化された秘密鍵を有する参加ノード１２のみが制限情報トランザクションt_xを読み取り及び実行できる制限情報トランザクションt_xとしてマークされる。上記の処理は、検証ノード１３、暗号化モジュールによって実行される。

【００５０】

ブロックチェーンの暗号化されマークされたデータブロック、つまり暗号化され制限付きとしてマークされたデータのブロックは、ブロックチェーンネットワークの検証ノード１３によって分散し、０～Ｎ個のトランザクション及び少なくとも１つの情報トランザクションt_x’を含む。$_x$tプライバシーグループ内の参加ノード１２は、t_x’がそのプライバシーグループ宛てのトランザクションであることを更に通知される。

【００５１】

検証ノード１３は、参加ノード１２から制約メタデータを受信すると、プライバシーグループに属する参加ノード１２に対して、全ての制限トランザクションを実行、検証、パッケージ化及び配信することが可能となる。

【００５２】

プライバシーグループ内で制限情報トランザクションを行うことを望む参加ノード１２は、トランザクションプライバシーグループに対応する該当暗号化秘密鍵を使用して、検証ノード１３から分散した暗号化ブロックを復号化するように構成される。

【００５３】

検証ノード１３は、暗号化秘密鍵のセットを分散させるようなプライバシーグループ管理タスクを行うように構成される。暗号化秘密鍵のセットの秘密鍵は検証ノード１３によって使用され、ブロック内で組み立てる前に暗号化されて制限データブロックとしてマークされなければならない提案された情報トランザクションを暗号化し、後にブロックチェーンネットワーク内の全てのノード１２、すなわちプライバシーグループ内のノード１２及びブロックチェーンネットワーク１１内の他の全てのノードに分散する。

【００５４】

ブロックチェーンネットワーク内の参加ノード１２がブロックチェーンネットワーク１

１内の少なくとも１つの特定の参加ノード１２との制限情報トランザクションを行えるように、ブロックチェーンネットワーク１１内の両方の参加ノード１２は、同じプライバシーグループに属していなければならない。

【００５５】

ブロックチェーンネットワーク１１内の全てのノード１２は、既存のブロックチェーン内のデータブロックの各々を受信し、その後連続的にブロックチェーンが進行する。

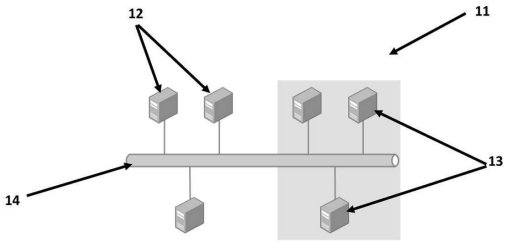
【００５６】

したがって、ブロックチェーンネットワーク内の全てのノード１２及びノード１３には、ブロックチェーンの同じバイナリコピーを格納している。すなわち不変の分散レコードブック、台帳であり、これにはパブリックトランザクションとプライベートトランザクションの両方が含まれる。ブロックチェーンネットワーク１１の参加ノード１２及び検証ノード１３は、ブロックチェーンネットワーク１１の異なるノード１２及びノード１３間の通信に対する少なくとも１つの入出力インターフェース、少なくとも１つの暗号解読モジュール、少なくとも１つの参加ノード１２及び少なくとも暗号化された秘密鍵のセットを含むプライバシーグループストア、及びブロックチェーンストアすなわち分散レコードブック、台帳を含む。

【００５７】

参加ノード１２上のプライバシーグループストアは、参加ノード１２がメンバであるプライバシーグループのみを格納する。対照的に、検証ノード１３上のプライバシーグループストアは、各ノードのプライバシーグループのスーパーセット、又はｎ－１個の参加ノード１２によってブロックチェーンネットワーク１１内に形成され得るプライバシーグループの結果となる。

【図面】
【図１】



フロントページの続き

スペイン国 ２８０５０ マドリード カレー デ ロス パドレス ドミニコス ニュメロ ７
(72)発明者 ルベン ニエト マルティン－バレス
スペイン国 ２８０５０ マドリード カレー デ ロス パドレス ドミニコス ニュメロ ７

審査官 金沢 史明

(56)参考文献 米国特許出願公開第２０１９／０１４９３２５（ＵＳ，Ａ１）
国際公開第２０１９／０７２２６２（WO，Ａ２）
国際公開第２０１９／１２０３２６（WO，Ａ２）
特開２０１８－１９６１５０（ＪＰ，Ａ）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０６Ｆ ２１／６２
Ｇ０６Ｆ ２１／６０