

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6839267号
(P6839267)

(45) 発行日 令和3年3月3日(2021.3.3)

(24) 登録日 令和3年2月16日(2021.2.16)

(51) Int. Cl.	F I
G06F 21/62 (2013.01)	G06F 21/62 318
H04L 9/32 (2006.01)	H04L 9/00 675Z
G06F 21/60 (2013.01)	G06F 21/60 340

請求項の数 20 (全 23 頁)

(21) 出願番号	特願2019-513386 (P2019-513386)	(73) 特許権者	314015767
(86) (22) 出願日	平成28年9月9日(2016.9.9)		マイクロソフト テクノロジー ライセンシング, エルエルシー
(65) 公表番号	特表2019-533229 (P2019-533229A)		アメリカ合衆国 ワシントン州 98052 レッドモンド ワン マイクロソフト ウェイ
(43) 公表日	令和1年11月14日(2019.11.14)	(74) 代理人	100140109
(86) 国際出願番号	PCT/CN2016/098610		弁理士 小野 新次郎
(87) 国際公開番号	W02018/045574	(74) 代理人	100118902
(87) 国際公開日	平成30年3月15日(2018.3.15)		弁理士 山本 修
審査請求日	令和1年9月9日(2019.9.9)	(74) 代理人	100106208
			弁理士 宮前 徹
		(74) 代理人	100120112
			弁理士 中西 基晴

最終頁に続く

(54) 【発明の名称】 異なるパーティーにまたがるオブジェクトのトレース

(57) 【特許請求の範囲】

【請求項1】

コンピュータが、複数のパーティーの中の第1のパーティーからオブジェクトに関連する操作についての要求を受信するステップと、

前記コンピュータが、要求された前記操作を前記複数のパーティーによって合意されたルールセットに基づいて検証するステップであって、前記ルールセットは前記オブジェクトに関連する1つまたは複数の操作に対する1つまたは複数の制約を定義する、検証するステップと、

要求された操作が有効であるとの前記コンピュータによる検証に応答して該コンピュータが実施するステップであって、

前記操作を実施させるステップと、

前記操作についてのレコードを作成するステップであって、該レコードは前記ルールセットに固有である、作成するステップと、

前記レコードを前記複数のパーティーにアクセス可能であるブロックチェーンデータベースに記憶するステップと

を含むステップと

を含む方法。

【請求項2】

請求項1に記載の方法であって、さらに、前記複数のパーティーについて前記ルールセットを、

前記コンピュータが、前記複数のパーティーの中の第2のパーティーから、前記ルールセットを設定するための要求を受信するステップと、

前記コンピュータが、前記複数のパーティーに前記ルールセットをブロードキャストするステップと、

前記コンピュータが、前記複数のパーティーのうちの少なくとも1つからの前記ルールセットに対する確認の受信に 응답して、前記ルールセットを有効化するステップとによって設定するステップを含む方法。

【請求項3】

請求項2に記載の方法であって、前記ルールセットを有効化する前記ステップは、

前記複数のパーティーの中の第3のパーティーからの前記ルールセットに対する確認の受信に 응답して、前記確認についてのレコードを作成するステップであって、該レコードは、前記第3のパーティーのシグネチャを含む、作成するステップと、

前記確認についての前記レコードを前記ブロックチェーンデータベースに記憶するステップと

を含む、方法。

【請求項4】

請求項1に記載の方法であって、さらに、

前記コンピュータが、前記複数のパーティーの中の第4のパーティーから、前記オブジェクトをトレースする要求を受信するステップと、

前記オブジェクトをトレースする前記要求の前記コンピュータによる受信に 응답して、該コンピュータが前記オブジェクトに関連する操作についての1つまたは複数のレコードを前記ブロックチェーンデータベースから検索するステップと、

前記コンピュータが、検索された前記レコードを前記第4のパーティーに提供するステップと

を含む方法。

【請求項5】

請求項1に記載の方法であって、要求された前記操作を検証する前記ステップは、さらに、

前記操作についての前記要求の受信に 응답して、前記操作に関連する通知を前記複数のパーティーにブロードキャストするステップ

を含む、方法。

【請求項6】

請求項1に記載の方法であって、要求された前記操作を検証する前記ステップは、

前記要求から前記ルールセットへの参照を抽出するステップと、

検証する前記ステップのために、前記参照に基づいて前記ルールセットをアドレス指定するステップと

を含む、方法。

【請求項7】

請求項1に記載の方法であって、前記ルールセットは実行可能コードを含み、要求された前記操作を検証する前記ステップは、

前記コードを実行させることによって、要求された前記操作を検証するステップ

を含む、方法。

【請求項8】

請求項1に記載の方法であって、前記レコードは、さらに、

前記ルールセットに固有のイベント識別情報（ID）と、

前記ルールセットへの参照と、

前記操作についてのIDと、

前記操作の記載と、

前記第1のパーティーのシグネチャと、

前記第1のパーティーの前記シグネチャを復号するための公開鍵と、

10

20

30

40

50

前記要求が送信された時間ポイントを示すタイムスタンプと
のうちの少なくとも1つを含む、方法。

【請求項9】

請求項1に記載の方法であって、さらに、

前記コンピュータが、前記操作の状態であって、前記操作が成功裏に実施されたかどうかを示す状態についての問い合わせを受信するステップと、

前記コンピュータが、前記問い合わせに回答して、前記ブロックチェーンデータベースにおける前記操作についての前記レコードに追加される後続のレコードの数を決定するステップと、

前記コンピュータが、後続のレコードの数に基づいて、前記操作の状態を決定するステップと
を含む方法。

10

【請求項10】

処理ユニットと、

前記処理ユニットに接続され、前記処理ユニットによる実行のための命令を記憶したメモリと

を含むデバイスであって、前記命令は、前記処理ユニットによって実行されると、前記デバイスに、

複数のパーティーの中の第1のパーティーからオブジェクトに関連する操作についての要求を受信するステップと、

20

要求された前記操作を前記複数のパーティーによって合意されたルールセットに基づいて検証するステップであって、前記ルールセットは前記オブジェクトに関連する1つまたは複数の操作に対する1つまたは複数の制約を定義する、検証するステップと、

要求された操作が有効であるとの検証に回答して

前記操作を実施させるステップと、

前記操作についてのレコードを作成するステップであって、前記レコードは前記ルールセットに固有である、作成するステップと、

前記レコードを前記複数のパーティーにアクセス可能であるブロックチェーンデータベースに記憶するステップと

を含む動作を実施させる、デバイス。

30

【請求項11】

請求項10に記載のデバイスであって、前記命令は、前記処理ユニットによって実行されると、前記デバイスに、さらに、前記複数のパーティーについて前記ルールセットを、

前記複数のパーティーの中の第2のパーティーから、前記ルールセットを設定する要求を受信するステップと、

前記複数のパーティーに前記ルールセットをブロードキャストするステップと、

前記複数のパーティーの少なくとも1つからの前記ルールセットに対する確認の受信に回答して、前記ルールセットを有効化するステップと

によって設定させる、デバイス。

40

【請求項12】

請求項11に記載のデバイスであって、前記ルールセットを有効化する前記ステップは、

前記複数のパーティーの中の第3のパーティーからの前記ルールセットに対する確認の受信に回答して、前記確認についてのレコードを作成するステップであって、該レコードは前記第3のパーティーのシグネチャを含む、作成するステップと、

前記確認についての前記レコードを前記ブロックチェーンデータベースに記憶するステップと

を含む、デバイス。

【請求項13】

請求項10に記載のデバイスであって、前記動作は、さらに、

前記複数のパーティーの中の第4のパーティーから前記オブジェクトをトレースする要

50

求を受信するステップと、

前記オブジェクトをトレースする前記要求の受信に応答して、前記オブジェクトに関連する操作についての1つまたは複数のレコードを前記ブロックチェーンデータベースから検索するステップと、

検索された前記レコードを前記第4のパーティーに提供するステップとを含む、デバイス。

【請求項14】

請求項10に記載のデバイスであって、要求された前記操作を検証する前記ステップは、さらに、

前記操作についての前記要求の受信に応答して、前記操作に関連する通知を前記複数のパーティーにブロードキャストするステップを含む、デバイス。

【請求項15】

請求項10に記載のデバイスであって、要求された前記操作を検証する前記ステップは、前記要求から前記ルールセットへの参照を抽出するステップと、

検証する前記ステップのために、前記参照に基づいて前記ルールセットをアドレス指定するステップとを含む、デバイス。

【請求項16】

請求項10に記載のデバイスであって、前記ルールセットは実行可能コードを含み、要求された前記操作を検証する前記ステップは、

前記コードを実行させることによって要求された前記操作を検証するステップを含む、デバイス。

【請求項17】

請求項10に記載のデバイスであって、前記レコードは、さらに、

前記ルールセットに固有のイベントIDと、

前記ルールセットへの参照と、

前記操作についてのIDと、

前記操作の記載と、

前記第1のパーティーのシグネチャと、

前記第1のパーティーの前記シグネチャを復号するための公開鍵と、

前記要求が送信された時間ポイントを示すタイムスタンプと

のうちの少なくとも1つを含む、デバイス。

【請求項18】

請求項10に記載のデバイスであって、前記動作は、さらに、

前記操作の状態であって、前記操作が成功裏に実施されたかどうかを示す状態についての問い合わせを受信するステップと、

前記問い合わせに回答して、前記ブロックチェーンデータベースにおける前記操作についての前記レコードに追加される後続のレコードの数を決定するステップと、

後続のレコードの数に基づいて、前記操作の状態を決定するステップとを含む、デバイス。

【請求項19】

非一時的な機械読み取り可能媒体に有形に記憶され、機械実行可能命令を含むコンピュータプログラムであって、前記命令は、デバイス上で実行されると、前記デバイスに、

複数のパーティーの中の第1のパーティーからオブジェクトに関連する操作についての要求を受信するステップと、

要求された前記操作を前記複数のパーティーによって合意されたルールセットに基づいて検証するステップであって、前記ルールセットは前記オブジェクトに関連する1つまたは複数の操作に対する1つまたは複数の制約を定義する、検証するステップと、

要求された操作が有効であるとの検証に回答して、

10

20

30

40

50

前記操作を実施させるステップと、
前記操作についてのレコードを作成するステップであって、前記レコードは前記ルールセットに固有である、作成するステップと、
前記レコードを前記複数のパーティーにアクセス可能であるブロックチェーンデータベースに記憶するステップと
をさせる、コンピュータプログラム。

【請求項 20】

請求項 19 に記載のコンピュータプログラムであって、前記命令は、前記デバイス上で実行されると、前記デバイスに、さらに、前記複数のパーティーについて前記ルールセットを、

10

前記複数のパーティーの中の第 2 のパーティーから、前記ルールセットを設定する要求を受信するステップと、

前記複数のパーティーに前記ルールセットをブロードキャストするステップと、

前記複数のパーティーの少なくとも 1 つからの前記ルールセットに対する確認の受信に
応答して、前記ルールセットを有効化するステップと
によって設定させる、コンピュータプログラム。

【発明の詳細な説明】

【背景技術】

【0001】

[0001]個人、会社、組織または他のエンティティなどの異なるパーティーは、例えば資産、文書、品物などの対象のオブジェクトを記録するために、パーティーの中でたいてい自身のデータベースを有する。各パーティーは自身のレコードを保持し、レコードに互いに一貫性があるかどうかを定期的に互いにチェックする。異なるデータフォーマット、スキーマ、同期の頻度さらにはエラーのため、常に一致に到達することは全てのパーティーにとって、厳しい要求である。組織横断的なアクティビティを系統立てる別のやり方は、全てのレコードを保持するために複数のパーティーの中の 1 つのパーティーを選択すること、または全てのレコードを記憶するために独立したサードパーティーを探すことを必要とする。しかし、これらの集中型のソリューションでは、中央管理的なパーティーとして活動するパーティーが攻撃に曝されやすい。したがって、異なるパーティーにまたがってオブジェクトの流れまたは分散を確実に制御およびトレースすることは難しいものである

20

30

【発明の概要】

【0002】

[0002]本明細書で記載される主題の実装形態にしたがって、異なるパーティーにまたがってオブジェクトを制御およびトレースするための新しい手法が提案される。これらのパーティーの 1 つまたは複数が、これらの異なるパーティーにまたがってオブジェクトの流れを制御およびトレースできるように、ルールセットが複数のパーティーに有効化される。ルールセットは、オブジェクトに関連する 1 つまたは複数の操作に対する制約を定義する。パーティーからオブジェクトに関連する操作についての要求を受信すると、ルールセットに基づいて要求された操作は検証され得る。要求された操作が有効である場合、操作が実施され、ルールセットに固有の操作についてのレコードが作成される。次いで、レコードは複数のパーティーにアクセス可能であるブロックチェーンデータベースに記憶される。ブロックチェーン台帳またはブロックチェーン分散データベースとも称され得るブロックチェーンデータベースは、絶え間なく増加するデータレコードの一覧を改竄および改訂からセキュリティ保護するよう維持する分散データベースである。このように、オブジェクトの分散および流れは異なるパーティー間で効果的および効率的に制御されおよびトレースされることができる。

40

【0003】

[0003]発明の概要は、本明細書で記載される主題の実装形態の主要なまたは本質的な特徴を特定することを意図されておらず、本明細書で記載される主題の範囲を限定するため

50

に使用されることも意図されていないことを理解されたい。本明細書で記載される主題の他の特徴は以下の記載を通して容易に理解できるであろう。

【0004】

[0004]本明細書で記載される主題の1つまたは複数の実装形態の詳細が、添付の図面および以下の記載において説明される。本開示の他の特徴、態様、および利点は発明の詳細な説明、図面、および特許請求の範囲より明らかになるであろう。

【図面の簡単な説明】

【0005】

【図1】[0005]本明細書で記載される主題の実装形態にしたがってシステムを説明する概略図である。

10

【図2】[0006]本明細書で記載される主題の例示の実装形態にしたがってルールセットを設定するための方法を説明するフローチャートである。

【図3】[0007]本明細書で記載される主題の例示の実装形態にしたがってオブジェクトに関連する操作を実施する方法を説明するフローチャートである。

【図4】[0008]本明細書で記載される主題の例示の実装形態にしたがってオブジェクトに関連する操作を検証する方法を説明するフローチャートである。

【図5】[0009]本明細書で記載される主題の例示の実装形態にしたがってオブジェクトをトレースする方法を説明するフローチャートである。

【図6】[0010]本明細書で記載される主題の例示の実装形態にしたがって操作の状態を問い合わせる方法を説明するフローチャートである。

20

【図7】[0011]本明細書で記載される主題の1つまたは複数の実装形態を実装するために適切なデバイスのブロック図である。

【図8】[0012]本明細書で記載される主題の例示の実装形態にしたがって、オブジェクトをトレースすることの例示の視覚化を説明する概略図である。

【発明を実施するための形態】

【0006】

[0013]図面を通して、同一または類似の参照符号は常に同一または類似の要素を指す。

[0014]次に、本明細書で記載される主題の原理がいくつかの例示の実装形態を参照して記載される。これらの実装形態は、本開示の範囲に関していかなる限定も示唆することなく、当業者が本明細書で記載される主題を理解して実装することを助ける説明のためだけに記載されることを理解されたい。本明細書で記載される本開示は以下に記載されるもの以外の様々なやり方で実装され得る。

30

【0007】

[0015]本明細書で使用されるように、用語「含む(include)」およびその変形は「それに限定はされないが、含む」を意味する広い意味の用語として読み取られる。用語「基づいて(based on)」は「少なくとも一部基づいて」として読み取られる。用語「1つの(a)」は、そうでないと特定されない限り「1つまたは複数の」として読み取られる。用語「1つの実装形態(one implementation)および(an implementation)」は「少なくとも1つの実装形態」として読み取られる。用語「別の実装形態(another implementation)」は

40

【0008】

[0016]さらに、本明細書で記載される主題の文脈においては、用語「第1の」、「第2の」、「第3の」などは、要素の順番に関していかなる限定も示唆することなく、これらの個々の要素または構成要素を指すために使用されることを理解されたい。さらに、そうでないと指定されない限り、第1の要素は第2の要素と同一であってもよく、同一でなくてもよい。他の明示的および暗示的な定義が、以下に含まれてよい。

【0009】

[0017]上で言及したように、従来、組織、会社、個人などのパーティーはオブジェクトを別のパーティーに転送した後、そのパーティーのオブジェクトを他のパーティーの間で

50

、どのように転送するかを、確実に制御およびトレースすることができないことがある。本明細書で使用されるように、オブジェクトは、文書、品物、資産などを表現する任意のデジタル情報を指してよい。言い換えると、オブジェクトがパーティーの境界を離れた後、それは制御から外れ得る。例えば、慈善組織への寄贈者が、慈善組織に寄付を寄贈した後、自身の寄付の流れを制御およびトレースしたいと思う。このように寄贈者は寄付が意図されたように実際に使用されることを保証したいと思う。別の例として、自身の写真をソーシャルネットワーク上で共有するユーザーはまた、プライバシー目的でその写真の流れを制御およびトレースしたいと思う。しかし、従前のデータベース管理システムでは、各パーティーはそれ自身のデータベースシステムを維持および制御するので、一般にパーティーは自身のオブジェクトの流れを確実におよび容易に制御およびトレースできるようになっていない。

10

【 0 0 1 0 】

[0018]本明細書で記載される主題の実装形態にしたがって上記および他の潜在的な問題を少なくとも一部解決するために、異なるパーティーにまたがってオブジェクトを制御およびトレースするための新しい手法が提案される。

例示のシステム

[0019]まず、本明細書で記載される主題の例示の実装形態が実装され得る環境 1 0 0 を説明する概略図を示す図 1 を参照する。

【 0 0 1 1 】

[0020]示されるように、個人、組織、または任意の他のエンティティなどの複数のパーティー 1 0 1 から 1 0 5 がある。5つのパーティー 1 0 1 ~ 1 0 5 が示されているが、システム 1 0 0 は任意の適切な数のパーティーを含むことができることを理解されたい。各パーティーは、例えばラップトップコンピュータ、デスクトップコンピュータ、タブレットコンピュータ、サーバー、モバイルデバイス、ウェアラブルデバイスなどのデバイスを有することができる。パーティー 1 0 1 ~ 1 0 5 はネットワークを介して互いに通信可能に接続されていてよい。ネットワークの例としては、限定はされないが、ローカルエリアネットワーク(「LAN」)、メトロポリタンエリアネットワーク(「MAN」)、ワイドエリアネットワーク(「WAN」)、などの有線または無線ネットワークまたはインターネット、通信ネットワーク、近接場通信接続またはその任意の組み合わせが挙げられる。

20

30

【 0 0 1 2 】

[0021]環境 1 0 0 はまた、ブロックチェーンデータベース 1 1 0 および管理モジュール 1 2 0 を含む。管理モジュール 1 2 0 はパーティー 1 0 1 から 1 0 5 と通信しており、ブロックチェーンデータベース 1 1 0 を制御する。すなわち、管理モジュール 1 2 0 はデータベース管理システム(DBMS)として考えられてよい。別個の構成要素として示されているが、ブロックチェーンデータベース 1 1 0 および管理モジュール 1 2 0 は互いに一体化され得ることを理解されたい。具体的には、いくつかの実装形態では、管理モジュール 1 2 0 は分散モジュールであってもよい。

【 0 0 1 3 】

[0022]ブロックチェーンデータベース 1 1 0 はパーティー 1 0 1 から 1 0 5 にアクセス可能である。ブロックチェーンデータベース 1 1 0 はデータレコードの一覧を改竄および改版からセキュリティ保護するよう維持する分散データベースであってもよい。レコードはデータブロックに編成されており、各ブロックは個々のレコードのまとまりを保有する。例えば、示されるように、レコード 1 ~ 6 はブロック 1 3 0₁、1 3 0₂ および 1 3 0_N に記憶される。いくつかの実装形態では、ブロックは1つずつ、暗号法によって接続されていてよい。ブロックはシグネチャを含んでもよく、あるブロックのシグネチャは先行ブロックのシグネチャおよびレコードに依存する。例えば、あるブロックのシグネチャは、先行ブロックのシグネチャおよびレコードのハッシュ値から計算され得る。以下の記載を通して、このデータベース管理システムにおいてオブジェクトの全ての操作は不変であり、制御可能およびトレース可能であることを諒解されたい。

40

50

【 0 0 1 4 】

[0023] 上述のように、1つまたは複数のオブジェクトは転送され、共有されてよく、またはそうでなければ、パーティー101から105の間を流れてもよい。オブジェクトの例としては、限定はされないが、電子文書、写真、動画、音声、資産などが挙げられる。各パーティーはオブジェクトに対する操作、例えば、転送すること、共有すること、消費すること、削除することなどを実施することができる。

【 0 0 1 5 】

[0024] 本明細書で記載される主題の実装形態にしたがって、パーティーは対象のオブジェクトに関連する1つまたは複数の操作に関する1つまたは複数の制約を記載するためにルールセット150を定義することができる。議論を容易にするために、以下の記載では用語「ルール」と「ルールセット」は互換的に使用され得る。

10

【 0 0 1 6 】

[0025] 一般的に言うと、ルールセット150はオブジェクトの1つまたは複数の操作に関する任意の態様および/または属性に関連していてもよい。例示のルールセット150は以下の段落でさらに記載される。いくつかの実装形態では、ルールセット150は例えばオブジェクトの所有者によって開始されてよい。もちろん、任意の他の関連性のあるパーティーが同様にルールセット150を提案してもよい。議論を容易にするために、以下の議論ではパーティー101がルールセット150を開始すると仮定する。

【 0 0 1 7 】

[0026] ルールセット150は任意の適切なフォーマットで実装されてもよい。例えば、いくつかの実装形態では、ルールセット150は任意の適切なプログラミング言語および/またはスクリプト言語で書かれた実行可能なコードを含むことができる。代替としてまたは追加で、ルールセット150は拡張マークアップ言語(XML)テキスト、またはプレーンテキストなどのフォーマットされたテキストで記載されてもよい。ルールセット150は管理モジュール120によってブロックチェーンデータベース110に、または任意の他の適切な記憶装置に記憶されてもよい。

20

【 0 0 1 8 】

[0027] パーティー101からルールセット150を設定する要求を受信した後(160)、管理モジュール120はルールセット150をパーティー102から105にブロードキャストする。パーティーがルールセット150を受け入れる場合、パーティーは確認メッセージを管理モジュール120に送信し返すことができる。いくつかの実装形態では、システム内の所定の数のパーティーがルールセット150を確認する場合、次いで、ルールセット150が有効化される。いくつかの実装形態では、管理モジュール120は直接または問い合わせがあった時、提案されたルールセット150が他のパーティーによって受け入れられたかどうか、したがって有効化されたかどうかに関してパーティー101に通知を送信することができる(165)。この態様における例示の処理が図2を参照して以下に記載される。

30

【 0 0 1 9 】

[0028] 次いで、パーティーはオブジェクトの操作を開始するための要求を送信することができる。例えば、図1に示される例において、管理モジュール120はパーティー102からパーティー104にオブジェクトを転送する要求を受信する(170)。管理モジュール120は前もって記憶されていたルールセット150に基づいて要求された操作を検証する(172)。

40

【 0 0 2 0 】

[0029] 要求された操作が有効であると判断される場合、管理モジュール120は操作を実施させる。このイベントでは、管理モジュール120は操作についてのレコードを作成し、そのレコードをブロックチェーン110に記憶する(174)。とりわけこのレコードはルールセット150に固有のイベント識別情報(ID)を含むことができる。すなわち、ルールセット150の下でパーティー101から105によってオブジェクトに対して実施される全ての操作またはアクションは同一のイベントに属し、このイベントに属す

50

る全ての操作またはアクションは同一のイベントIDでブロックチェーンに記録されることができ。

【0021】

[0030]分散ブロックチェーンデータベース110は複数の記憶装置を含む。1つの記憶装置デバイスに記憶されるレコードは他の記憶装置と同期される。例えば、記憶装置は、それ自身に記憶されるレコードが所定の数の隣接する記憶装置に記憶されるレコードと同一かどうか、チェックする。レコードが同一でない場合、この記憶装置は隣接する記憶装置に記憶されるレコードにしたがって自身に記憶されるレコードを改版する。このように、オブジェクトの流れはトレース可能および不変であり、そのことを以下に議論する。

【0022】

[0031]いくつかの実装形態では、管理モジュール120のインスタンスは、パーティーが任意のインスタンスまたは管理モジュール120の全てのインスタンスと対話できるように、分散ブロックチェーンデータベース110に実装されてよい。代替として管理モジュール120のインスタンスは、個々のパーティーが管理モジュール120のそれぞれのインスタンスと対話できるようにそのパーティーに実装されてよい。したがって、ブロックチェーンデータベース110の複数の記憶装置に記憶されるレコードは、オブジェクトの流れが制御されおよびトレースされ得るように同期される。

【0023】

[0032]いくつかの実装形態では、異なるパーティーはそのオブジェクトに関連する1つまたは複数の操作に対する同一の制約を設定することができる。この場合、例えば、異なるパーティーを差別化するために、グローバルに制御されランダムに生成される数がそれぞれのイベントIDの生成に考慮されることができる。

【0024】

[0033]一方、要求された操作が無効である場合、管理モジュール120は要求を拒否してもよい。例えば、管理モジュール120は直接または問い合わせがあった時、操作が実施されたかどうかを知らせるためノード102に通知を送信することができる(175)。例示の実装形態が、図3を参照して記載され、およびデジタルコンテンツ分散における例示の実装形態が以下の段落で議論される。

【0025】

[0034]パーティー101などのパーティーが異なるパーティーにまたがってオブジェクトの流れをトレースしたい時、パーティーはトレース要求を送信することができる。要求を受信すると(180)、管理モジュール120はオブジェクトに関連する操作についての1つまたは複数のレコードをブロックチェーンデータベース110から検索する(182)。いくつかの実装形態では、トレース要求はイベントIDを含むことができ、オブジェクトに関連する操作についてのレコードはイベントIDに基づいて検索されることができる。次いで、管理モジュール120はパーティー101に検索されたレコードを返す(185)。したがって、パーティー101はそのイベントにおけるオブジェクトの流れまたは分散を通知されることができる。レコードをチェックすることによっていかなる違反も発見されない場合、パーティー101はそれにしたがった反応をしてもよい。例示の実装形態が図5を参照して記載される。

例示の処理

[0035]次に、上記の処理のいくつかの例示の実装形態を詳細に議論する。図2は本明細書で記載される主題の例示の実装形態にしたがってルールセット150を設定するための方法200を説明するフローチャートである。210において、管理モジュール120はルールセット150を設定する要求をパーティー101から受信する。ルールセット150は前もって、例えば、ブロックチェーン110に記憶されてもよい。

【0026】

[0036]上で言及したように、ルールセット150はオブジェクトの操作に関する任意の態様および/または属性に関連していてもよい。例えば、ルールセット150はパーティーがオブジェクトまたはオブジェクトが転送もしくは共有され得るターゲットを転送し得

10

20

30

40

50

る最大の回数を特定することができる。別の例として、ルールセット150はパーティーがオブジェクトを消費することができる条件を特定することができる。代替としてまたは追加で、ルールセット150は異なるパーティーに、オブジェクトのトレースを制御する許可のそれぞれのレベルを特定することができる。例えば、ルールセット150はパーティー102がパーティー101のオブジェクトをトレースすることを妨げることができる。さらになお他の実装形態では、ルールセット150はオブジェクトの1つまたは複数の操作に関連して時間制限を設定するためのタイマーを特定することができる。

【0027】

[0037]例えば、パーティー101がオブジェクトをパーティー102に転送すること、およびルールセット150がそのオブジェクトに関連して時間制限を設定するタイマーを特定することを仮定する。例えば、オブジェクトがパーティーに転送されるまたは提供される場合、タイマーは受信側のパーティーがそのオブジェクトを使用または消費することができる時間期間を特定することができる。受信側のパーティーがこの時間期間内にオブジェクトを消費しない場合、オブジェクトは回収されるか除去されることができる。この場合、まずオブジェクトはパーティー102に転送され、その転送に関するレコードが作成されて記憶される。管理モジュール120が、パーティー102がオブジェクトをルールセット150によって設定された所定の時間内にパーティー104に転送しないことを検出する場合、管理モジュール120はオブジェクトをパーティー101に返す操作をトリガーする。

【0028】

[0038]220において、管理モジュール120は、他のパーティー102から105がそれぞれパーティー101によって提案されるルールセット150を受け入れるかどうかについて決定できるように、ルールセット150を複数のパーティーにブロードキャストする。

【0029】

[0039]230において、ルールセット150についての確認がパーティー102から105のうちの少なくとも1つから受信される場合、管理モジュール120はルールセット150を有効化することができる。さらに、受信された確認のそれぞれについてレコードが作成されて記憶されることができる。例えば、パーティー102、103および105が、それらの確認を管理モジュール120に送信することを仮定する。確認はそれぞれパーティー102、103および105のシグネチャを含んでもよい。それぞれの確認について、管理モジュール120は例えば、次のうちの少なくとも1つを含むレコードを作成する：ルールセット150に固有のイベントID、確認についての記載、および確認が送信された時間ポイントを示すタイムスタンプ。

【0030】

[0040]いくつかの実装形態では、確認レコードはルールセット150への参照を含んでもよい。参照はポインターまたはuniform resource indicator (URI)として実装されてもよい。代替としてまたは追加で、確認はそれぞれのパーティーのシグネチャおよびシグネチャを復号するための公開鍵を含むことができる。シグネチャは、例えば、イベントID、公開鍵の暗号化によって、および/または秘密鍵を使用したルールセット150への参照によって計算されることができる。

【0031】

[0041]上述のように、パーティー101などの元々のパーティーはそのオブジェクトに関するルールセット150を開始することができ、したがってオブジェクトが別のパーティーに転送された後、他のパーティーの間でどのようにオブジェクトが転送されるかを制御することができる。例えば、自身の写真をソーシャルネットワーク上で共有するユーザーは、オブジェクトがある特定されたネットワークのみに転送されることができることを特定するルールセット150を開始することができる。そうでない場合、共有する操作は拒否される。このように、写真の分散が制御されることができる。

【0032】

10

20

30

40

50

[0042] 図 3 は本明細書で記載される主題の例示の実装形態にしたがってオブジェクトに対する操作を実施する方法 300 を説明するフローチャートである。310 において、管理モジュール 120 はパーティー 102 などのパーティーからオブジェクトに関連する操作について要求を受信する。例えば、要求された操作は、オブジェクトの少なくとも一部をパーティー 104 などの別のパーティーに転送することか、またはパーティー 104 などの別のパーティーと共有することである。

【0033】

[0043] 要求は、要求された操作の記載または ID、およびオブジェクトを含むことができる。追加で、いくつかの実装形態では、要求はさらに次のうちの少なくとも 1 つを含むことができる：パーティー 101 から 105 によって合意されたルールセット 150 に固有のイベント ID、ルールセット 150 への参照、パーティーのシグネチャ、開始する側のパーティー（この例では、パーティー 102）のシグネチャを復号するための公開鍵、および要求が送信された時間ポイントを示すタイムスタンプ。いくつかの実装形態では、操作についての ID はイベント ID、操作の記載、公開鍵およびルールセット 150 への参照のハッシュ値として計算され得る。

【0034】

[0044] 320 において、管理モジュール 120 は複数のパーティーによって合意されたルールセット 150 に基づいて要求された操作を検証する。この点に関する例示の実装形態が図 4 に示される。まず、管理モジュール 120 はブロックチェーンデータベース 110 をチェックして、確認するレコードが存在するか、レコードがパーティー 102 のシグネチャを含むかどうかを判断する。次いで 410 において、管理モジュール 120 は要求からルールセット 150 への参照を抽出することができる。420 において、管理モジュール 120 はその参照に基づいてルールセット 150 をアドレス指定して検索する。430 において、管理モジュール 120 は、要求された操作の記載がルールセット 150 に従っているかどうかをチェックすることによって、要求された操作を検証する。例えば、ルールセット 150 が実行可能なコードを含んでいる場合、管理モジュール 120 は、何らかの違反があるかどうかをチェックすることをコードに実行させることができる。

【0035】

[0045] 任意選択で、いくつかの実装形態では、440 において、管理モジュール 120 は操作に関連する通知を複数のパーティーにブロードキャストすることができる。例えば、管理モジュール 120 は、操作が検証または実施されることを通知するためのルールセット 150 に合意したパーティー 101 から 105 の全てに通知をブロードキャストすることができる。代替として管理モジュール 120 はルールセット 150 において特定されるようなある 1 つまたは複数のパーティーに通知を送信するだけでもよい。

【0036】

[0046] なお図 3 を参照すると、320 において要求された操作が有効であると判断される場合、管理モジュール 120 は 330 において操作を実行させ、340 において操作についてのレコードを作成する。レコードは少なくとも使用されたルールセット 150 に固有のイベント ID を含む。追加で、いくつかの実装形態では、操作レコードはさらに次のうちの 1 つまたは複数を含むことができる：ルールセット 150 への参照、操作についての ID、操作の記載、関連するパーティーのシグネチャ、シグネチャの復号のための公開鍵、および要求が送信された時間ポイントを示すタイムスタンプ。いくつかの実装形態では、レコードに含まれることになる情報のいくつかまたは全ては、例えば操作要求から得られることができる。

【0037】

[0047] 次いで 350 において、作成されたレコードはブロックチェーンデータベース 110 に記憶される。このように、オブジェクトの全ての操作は一意的イベント ID とともに記録される。以下で議論するように、後に、パーティーはそのオブジェクトの流れを、ブロックチェーン 110 でそれぞれのイベント ID を有するレコードを探すことによってトレースすることができる。

10

20

30

40

50

【 0 0 3 8 】

[0048]一方、320においてルールセット150が違反されていると判断された場合、管理モジュール120は360において要求を拒否することができる。このイベントにおいて、操作についてのレコードは作成されない。代替として、他の実装形態において、管理モジュール120はなお操作についてのレコードを作成し記憶することができ、このレコードに操作が拒絶されたというインジケータを割り当てる。

【 0 0 3 9 】

[0049]パーティー101などの元々のパーティーからのオブジェクトを受信するパーティー102などのパーティーは、ルールセット150に基づいて検証される操作を実施できるだけなので、元々のパーティーは、オブジェクトが別のパーティーに転送された後、他のパーティーの間でどのように転送されるかを制御することができる。例えば、ソーシャルネットワークにおいて、共有される写真はその後、その写真の元々の所有者によって特定された他のユーザーだけと共有され得る。別の例として、慈善組織への寄贈者は自身の寄付がある目的によってのみ使用され得ることを特定できる。

10

【 0 0 4 0 】

[0050]図5は本明細書で記載される主題の例示の実装形態にしたがってオブジェクトをトレースする方法500を説明するフローチャートである。510において、管理モジュール120は、複数のパーティー101から105の中の任意のパーティーからオブジェクトをトレースする要求を受信する。それに応じて、520において、管理モジュール120はオブジェクトに関連する操作についての1つまたは複数のレコードをブロックチェーンデータベース110から検索する。530において、管理モジュール120は検索されたレコードを問い合わせ側のパーティーに提供する。上述のように、ルールセット150に基づいて検証されたオブジェクトの操作は同一のイベントIDを共有することができる。すなわち、同一のイベントに属する操作についてのレコードはイベントIDによって検索されることができる。これらのレコードに基づいて、問い合わせ側のパーティーは、例えば、オブジェクトはまずパーティー101からパーティー102に転送され、次いで、パーティー102からパーティー104に転送されたということなどを知ることができる。いくつかの実装形態では、検索された操作はオブジェクトの流れまたは分散を明確に表すために視覚化されることができる。したがって、パーティーは確実におよび容易にそのオブジェクトの流れをトレースすることができる。図8を参照して視覚化の例を記載する。

20

30

【 0 0 4 1 】

[0051]図6は、本明細書で記載される主題の例示の実装形態にしたがって操作の状態を問い合わせる方法600を説明するフローチャートである。610において、管理モジュール120は操作の状態についての問い合わせを受信する。本明細書で使用されるように、用語「状態」は操作が成功裏に（正常に；*successfully*）実施されたかどうかを示す。

【 0 0 4 2 】

[0052]620において、問い合わせに回答して管理モジュール120はブロックチェーンデータベース110におけるターゲット操作についてのレコードに追加された後続のレコードの数を決定する。

40

【 0 0 4 3 】

[0053]630において、管理モジュール120は後続のレコードの数に基づいて操作の状態を決定（判断；*determines*）する。ブロックチェーンデータベース110のメカニズムから、後続の追加されたレコードの数が所定の数を超える場合、そのシステムに参与するパーティーの十分多数によって、操作についてのレコードが受け入れられたことを意味する、ことが知られ得る。この場合、操作は正常であると考えてよい。そうでなければ、追加されたレコードの比較的少数が、操作レコードが他のパーティーによって、例えば、通信遅延および/または他の要因に起因して、恐らく認識されないことを示すことがある。結果として、後続のレコードの数は操作の状態を判断するために使用され得

50

る。いくつかの実装形態では、管理モジュール120はそれ自身によって操作の状態を判断することができる。代替として管理モジュール120は、パーティー102が後続のレコードの数に基づいて操作の状態を判断することができるように、そのレコードに追加される後続のレコードのブロックを問い合わせ側のパーティー102に返すことができる。

【0044】

[0054]結果として、問い合わせ側のパーティーは操作の現在の状態を得ることができ、その状態に基づいてさらなる操作を行うかどうかを判断することができる。例えば、パーティー102がその要求された操作が拒否されたことを見つけた場合、パーティー102は再度操作に対する別の要求を送信することができる。

【0045】

[0055]図7は、本明細書で記載される主題の1つまたは複数の実装形態を実装するために適切なデバイス700のブロック図である。例えば、デバイス700は図2を参照して上記で議論したように管理モジュール120として機能してもよい。デバイス700は、様々な実装形態が多様な汎用または専用のコンピューティング環境において実装され得るように、本明細書で記載される主題の使用または機能性の範囲に限りかからない限定も示唆することを意図されていないことを理解されたい。

【0046】

[0056]示されるように、デバイス700は少なくとも1つの処理ユニット(またはプロセッサ)710およびメモリ720を含む。処理ユニット710はコンピュータ実行可能命令を実行し、現実のまたは仮想のプロセッサであってもよい。マルチプロセッシングシステムにおいては、複数の処理ユニットがコンピュータ実行可能命令を実行して処理能力を向上させる。メモリ720は、揮発性メモリ(例えば、レジスタ、キャッシュ、RAM)、非揮発性メモリ(例えば、ROM、EEPROM、フラッシュメモリ)、またはそのいくつかの組み合わせであってもよい。

【0047】

[0057]図7に示される例において、デバイス700はさらに記憶装置730、1つまたは複数の入力デバイス740、1つまたは複数の出力デバイス750、および1つまたは複数の通信接続760を含む。バス、コントローラ、またはネットワークなどの相互接続メカニズム(図示せず)はデバイス700の構成要素を相互接続する。典型的には、オペレーティングシステムソフトウェア(図示せず)はデバイス700で実行する他のソフトウェアに動作環境を提供し、デバイス700の構成要素のアクティビティを調和させる。

【0048】

[0058]記憶装置730はリムーバブルであってもよく、またはリムーバブルでなくてもよく、フラッシュドライブ、磁気ディスクまたは情報を記憶するために使用され得、かつデバイス700内でアクセスされ得る任意の他の媒体などの、コンピュータ読み取り可能記憶装置媒体を含むことができる。入力デバイス740は様々な異なる入力デバイスのうちの1つまたは複数であってもよい。例えば、入力デバイス740はマウス、キーボード、トラックボール等、などのユーザーデバイスを含んでもよい。入力デバイス740は、会話認識またはタッチおよびスタイラス認識などの1つまたは複数の自然なユーザーインターフェイス技法を実装することができる。他の例として、入力デバイス740はスキャンデバイス、ネットワークアダプター、またはデバイス700に入力を提供する別のデバイスを含んでもよい。出力デバイス750はディスプレイ、プリンター、スピーカー、ネットワークアダプター、またはデバイス700からの出力を提供する別のデバイスであってもよい。入力デバイス740および出力デバイス750はタッチスクリーンまたは仮想現実システムなどの単一のシステムまたはデバイスに組み込まれてもよい。

【0049】

[0059]通信接続760は通信媒体を介して別のコンピューティングエンティティへの通信を可能にする。追加で、デバイス700の構成要素の機能性は、単一のコンピューティングマシンまたは通信接続を介して通信することができる複数のコンピューティングマシンに実装されてもよい。したがって、デバイス700は1つまたは複数の他のサーバー、

10

20

30

40

50

ネットワークPC、または別の共通ネットワークノードへの論理接続を使用して、ネットワーク化された環境（例えば、環境100）において動作することができる。例として、また限定ではなく、通信媒体は、有線または無線ネットワーク技法を含む。

【0050】

[0060]本明細書で記載される主題の実装形態にしたがって、管理モジュール120はデバイス700で実行され、オブジェクトに関するイベントに関連する操作を制御およびトレースすることができる。処理ユニット760によって実行される時、管理モジュール120の少なくとも一部はメモリ720にロードされる。管理モジュール120の他の部分（もしあれば）は記憶装置730または任意の他の非揮発性記憶装置媒体に記憶されてもよい。操作において、管理モジュール120は上述のように1つまたは複数の方法/処理を実行することができる。

10

例示のシナリオ

[0061]次に、デジタル著作権管理（CRM）の文脈において本明細書で記載される主題の例示の実装形態を記載する。例えば、パーティー（例えば、パブリッシャー）は、容易におよび確実にそのデジタルコンテンツの流れを制御およびトレースしたいと思い、デジタルコンテンツが意図されたパーティー（例えば、視聴者）によって特定の時間制限内にまたは特定の回数、使用されることを保証したいと思う。デジタルコンテンツの例としては、限定はされないが、動画、音声、画像、レビュー、または任意の他の適切なデジタルコンテンツが挙げられる。

【0051】

20

[0062]この目的のため、パブリッシャーはデジタルコンテンツのためのルールセット150を規定することができ、管理モジュール120を介してルールセット150をブロックチェーン110に記憶することができる。例えば、ルールセット150はパブリッシャーからデジタルコンテンツを受信する任意の視聴者が、デジタルコンテンツを15日間以内だけ消費してよいことを特定することができる。デジタルコンテンツはこの期間の間だけ、視聴者によってアクセスされまたは消費されることができる。ルールセット150は視聴者がデジタルコンテンツを他の視聴者と10回以下共有することができることを特定することもできる。

【0052】

[0063]1つの実装形態において、ルールセット150を設定および検証することは、実行可能コードとして実装され得る。例示のコードの抜粋を以下に示す：

30

【0053】

【数 1】

```

content AutoDelete{ // delete the digital content for 15 days
Unit_64 public start_time;
Unit public digital_content;
Int public lifetime;

function AutoDelete{ // constructor, called when the rule set 150
is created
    lifetime = 15 day;
    digital_content = 0;
    start_time = 0;
    transfer_times = 10;
}
function() { // main code, called per invocation
    if (msg.sender.type == 'delete' && digital_content && now
- start_time > lifetime){ // periodical system delete testing
transaction
        unit object = digital_content;
        digital_content = 0;
        delete (object);
    }
    else if (msg.sender.type == 'digital_content'){ // digital
content transferring
        start_time = now;
        digital_content = msg.sender.object;
    }
    else if (msg.sender.type == 'viewer' && digital_content
&& msg.sender.value <= transfer_times){ // processing the digital
content
        transfer_times -= msg.sender.value;
    }
}

```

10

20

30

【0054】

[0064]パブリッシャーはコードを設定するための要求を管理モジュール120に送信する。管理モジュール120は他のパーティーの確認についてのコードをブロードキャストする。次いで、パブリッシャーはデジタルコンテンツを第1の視聴者へ転送するための要求を送信することができる。管理モジュール120はブロックチェーンデータベース110をチェックして、第1の視聴者がルールセット150を受け入れるかどうかを判断する。受け入れる場合、管理モジュール120は要求からコードへの参照を抽出し、コードにアクセスし、コードを実行させて何らかの違反があるかどうかをチェックする。

【0055】

[0065]要求された操作が有効であると判断された場合、管理モジュール120はデジタルコンテンツを第1の視聴者に分散させることを許可する。この分散操作についてのレコードが作成され、ブロックチェーン110に記憶される。このレコードはルールセット150に固有である。上述のように、ルールセット150の下でデジタルコンテンツに対してパブリッシャーおよび第1の視聴者によって実施される全ての操作またはアクションは、同一のイベントに属する。結果として、ブロックチェーン120内のそれらのレコードは同一のイベントIDを有する。

40

【0056】

[0066]第1の視聴者がデジタルコンテンツを第2の視聴者と共有したいと仮定する。そのような要求を受信すると、管理モジュール120はルールセット150に基づいて要求された操作を検証する。より具体的には、この例において、コードを実行することによ

50

て管理モジュール120は第1の視聴者がすでにそのデジタルコンテンツを他の視聴者と共有した回数をチェックすることができる。回数が10と等しい場合、管理モジュール120はデジタルコンテンツを共有することに対する要求を拒否する。

【0057】

[0067]追加で、ルールセット150によって規定されるように、いかなる視聴者も15日間だけデジタルコンテンツを消費できる。したがって、デジタルコンテンツを第1の視聴者に分散すると、管理モジュール120は第1の視聴者がデジタルコンテンツを所有する時間の長さを監視するためのタイマーを設定することができる。15日間が過ぎると、管理モジュール120はデジタルコンテンツを第1の視聴者から除去する操作をトリガーする。

10

【0058】

[0068]さらに、パブリッシャーおよび/または視聴者は彼らが開始した操作の状態をチェックすることができる。例えば、パブリッシャーが異なるパーティーにまたがってデジタルコンテンツの流れをトレースしたい場合、イベントIDを含むトレース要求を送信することができる。それに応じて、管理モジュール120はそのイベントIDを含む1つまたは複数のレコードをブロックチェーンデータベース110から検索し、検索されたレコードをパブリッシャーに返す。いくつかの実装形態では、これらのレコードはデジタルコンテンツの流れを表すために視覚化されることができる。例えば、図8はデジタルコンテンツの流れを示すユーザーインターフェース(UI)800の概略図を示している。

【0059】

20

[0069]UI800の示される状態において、パブリッシャー810は、デジタルコンテンツがまず第1の視聴者802に転送されるデジタルコンテンツの分散経路を明確に見ることができる。そしてパーティー802はデジタルコンテンツを視聴者803および804と共有し、視聴者804はさらにそのコンテンツをさらなる視聴者805と共有する。UI800は本明細書で記載される主題の範囲に関していかなる限定も示唆することなく例示のためだけであることを理解されたい。任意の他の適切な形態のUIがエンドユーザーにデジタルコンテンツの流れを提示するために使用することができる。

【0060】

[0070]このように、パブリッシャーが、デジタルコンテンツが違法にいくつかのパーティー(例えば、競争相手)に分散されることを見つける場合、パブリッシャーはその著作権を保護するためのアクションを取ることができる。したがって、パブリッシャーはそのデジタルコンテンツの流れを効果的および効率的に制御およびトレースすることができる。

30

【0061】

[0071]本明細書で記載される主題の精神および原理を説明する目的のため、そのいくつかの具体的な実装形態を上で記載してきた。オブジェクトに関連する1つまたは複数の操作に対する1つまたは複数の制約を定義するルールセットを設定することによって、およびイベントIDに基づいてオブジェクトをトレースすることによって、あるパーティーは元々所有していたオブジェクトの流れまたは分散を他のパーティーを越えて、簡易で、確実にかつ信頼できるやり方で、制御およびトレースすることができるようになり得る。

40

【0062】

[0072]一般に、様々な例示の実装形態がハードウェアまたは特殊目的の回路、ソフトウェア、論理またはその任意の組み合わせにおいて実装され得る。いくつかの態様はハードウェアに実装されてもよく、一方で他の態様は、コントローラ、マイクロプロセッサまたは他のコンピューティングデバイスによって実行され得るファームウェアまたはソフトウェアに実装されてもよい。本明細書で記載される主題の例示の実装形態の様々な態様がブロック図、フローチャートまたはいくつかの他の図的表現を使用して説明され、記載されるが、本明細書で記載されるブロック、装置、システム、技法または方法は非限定的な例として、ハードウェア、ソフトウェア、ファームウェア、特殊目的の回路もしくは論理、汎用ハードウェアまたはコントローラまたは他のコンピューティングデバイス、またはそ

50

のいくつかの組み合わせにおいて実装されてもよいことを諒解されたい。

【0063】

[0073] 本明細書で記載される主題の文脈において、機械読み取り可能媒体は、命令実行システム、装置、またはデバイスによって、またはそれらと関連して使用するためのプログラムを含む、または記憶することができる任意の有形な媒体であってもよい。機械読み取り可能媒体は機械読み取り可能信号媒体または機械読み取り可能記憶装置媒体であってもよい。機械読み取り可能媒体は、限定はされないが、電子的、磁氣的、光学的、電磁的、赤外または半導体のシステム、装置、またはデバイス、または上記の任意の適切な組み合わせを含むことができる。機械読み取り可能記憶装置媒体のより具体的な例としては、1つまたは複数のワイヤを有する電氣的接続、ポータブルコンピュータディスク、ハードディスク、ランダムアクセスメモリ(RAM)、読み取り専用メモリ(ROM)、消去可能プログラム可能読み取り専用メモリ(EPROMまたはフラッシュメモリ)、光ファイバ、ポータブルコンパクトディスク読み取り専用メモリ(CD-ROM)、光学記憶装置デバイス、磁気記憶装置デバイス、または上記の任意の適切な組み合わせが挙げられる。

10

【0064】

[0074] 本明細書で記載される主題の方法を実行するコンピュータプログラムコードは1つまたは複数のプログラミング言語の任意の組み合わせで記述されることができる。これらのコンピュータプログラムコードは、プログラムコードがコンピュータまたは他のプログラム可能データ処理装置のプロセッサによって実行されると、フローチャートおよび/またはブロック図において特定される機能または操作を実装させるように、汎用コンピュータ、専用コンピュータ、または他のプログラム可能データ処理装置のプロセッサに提供されてよい。プログラムコードは、全体的にコンピュータ上で、部分的にコンピュータ上で、スタンドアロンのソフトウェアパッケージとして、部分的にコンピュータ上でおよび部分的にリモートコンピュータ上で、または全体的にリモートコンピュータ上もしくはサーバー上で実行することもできる。

20

【0065】

[0075] さらに、操作は特定の順序で描かれるが、これは、望ましい結果を達成するために、そのような操作が示される特定の順序でもしくは順次を実施されること、または全ての説明した操作が実施されること、を要求するものとして理解されるべきではない。ある状況において、マルチタスキングおよび並列処理は有利であり得る。同様に、いくつかの具体的な実装形態の詳細が上記の議論に含まれるが、これらはいかなる開示の範囲または特許請求され得ることに対する限定と解釈されるべきではなく、むしろ特定の開示の特定の実装形態に固有であり得る特徴の記載として解釈されるべきである。別個の実装形態の文脈において本明細書で記載されるある特徴はまた、単一の実装形態において組み合わせで実装されてもよい。逆に、単一の実装形態の文脈において記載される様々な特徴はまた、別個にまたは任意の適切な部分組み合わせとして複数の実装形態に実装されてもよい。

30

【0066】

[0076] 次に、説明の目的だけのために、いくつかの例示の実装形態を以下に列挙する。

[0077] いくつかの実装形態では、本明細書で記載される主題は方法として具体化されることができる。方法は、複数のパーティーの中の第1のパーティーからオブジェクトに関連する操作について要求を受信することと、要求された操作を複数のパーティーによって合意されたルールセットに基づいて検証することと、ルールセットはオブジェクトに関連する1つまたは複数の操作に対する1つまたは複数の制約を定義する、検証することと、要求された操作が有効であると検証することに応答して操作を実施させることと、操作についてのレコードを作成することと、レコードはルールセットに固有である、作成することと、レコードを複数のパーティーにアクセス可能であるブロックチェーンデータベースに記憶することと、を含む。

40

【0067】

[0078] いくつかの実装形態では、方法はさらに、複数のパーティーの中の第2のパーテ

50

イーからルールセットを設定するための要求を受信することによって、複数のパーティーにルールセットをブロードキャストすることによって、および複数のパーティーのうちの少なくとも1つからルールセットに対する確認を受信することによって、ルールセットを有効化することによって、複数のパーティーについてルールセットを設定することを含む。

【0068】

[0079]いくつかの実装形態では、ルールセットを有効化することは、複数のパーティーの中の第3のパーティーからルールセットに対する確認を受信することによって確認についてのレコードを作成することによって、レコードは、第3のパーティーのシグネチャを含む、作成することと、確認についてのレコードをブロックチェーンデータベースに記憶することと、を含む。

10

【0069】

[0080]いくつかの実装形態では、方法はさらに、複数のパーティーの中の第4のパーティーから、オブジェクトをトレースする要求を受信することと、オブジェクトをトレースする要求を受信することによって、オブジェクトに関連する操作についての1つまたは複数のレコードをブロックチェーンデータベースから検索することと、検索されたレコードを第4のパーティーに提供することと、を含む。

【0070】

[0081]いくつかの実装形態では、要求された操作を検証することはさらに、操作についての要求を受信することによって、操作に関連する通知を複数のパーティーにブロードキャストすることを含む。

20

【0071】

[0082]いくつかの実装形態では、要求された操作を検証することは、要求からルールセットへの参照を抽出することと、検証することについての参照に基づいてルールセットをアドレス指定することを含む。

【0072】

[0083]いくつかの実装形態では、ルールセットは実行可能コードを含み、要求された操作を検証することは、コードを実行させることによって、要求された操作を検証することを含む。

【0073】

30

[0084]いくつかの実装形態では、第1のレコードはさらに、次のうちの少なくとも1つを含む：ルールセットに固有のイベント識別情報(ID)、ルールセットへの参照、操作についてのID、操作の記載、第1のパーティーのシグネチャ、第1のパーティーのシグネチャを復号するための公開鍵、および第1の要求が送信された時間ポイントを示すタイムスタンプ。

【0074】

[0085]いくつかの実装形態では、方法はさらに、操作の状態、操作が成功裏に実施されたかどうかを示す状態についての問い合わせを受信することと、問い合わせによって、ブロックチェーンデータベースにおける操作についてのレコードに追加される後続のレコードの数を決定することと、後続のレコードの数に基づいて操作の状態を判断することと、を含む。

40

【0075】

[0086]いくつかの実装形態では、本明細書に記載される主題はデバイスとして具体化されることができる。デバイスは、処理ユニットおよびメモリを備える。メモリは処理ユニットに接続され、処理ユニットによる実行のための命令を記憶する。命令は、処理ユニットによって実行される時、デバイスに、複数のパーティーの中の第1のパーティーからオブジェクトに関連する操作についての要求を受信することと、複数のパーティーによって合意されたルールセットに基づいて要求された操作を検証することによって、ルールセットはオブジェクトに関連する1つまたは複数の操作に対する1つまたは複数の制約を定義する、検証することと、要求された操作が有効であると検証することによって操作を実

50

施させることと、操作についてのレコードを作成することであって、レコードはルールセットに固有である、作成することと、レコードを複数のパーティーにアクセス可能であるブロックチェーンデータベースに記憶することと、をさせる。

【 0 0 7 6 】

[0087]いくつかの実装形態では、命令は、処理ユニットによって実行される時、さらにデバイスに、複数のパーティーの中の第2のパーティーから、ルールセットを設定する要求を受信することによって、複数のパーティーにルールセットをブロードキャストすることによって、および複数のパーティーの少なくともいくつかからルールセットに対する確認を受信することによって、ルールセットを有効化することによって、複数のパーティーについてルールセットを設定すること、をさせる。

10

【 0 0 7 7 】

[0088]いくつかの実装形態では、ルールセットを有効化することは、複数のパーティーの中の第3のパーティーからルールセットに対する確認を受信することによって、確認についてのレコードを作成することであって、レコードは第3のパーティーのシグネチャを含む、作成することと、確認についてのレコードをブロックチェーンデータベースに記憶することと、を含む。

【 0 0 7 8 】

[0089]いくつかの実装形態では、命令は、処理ユニットによって実行される時、さらにデバイスに、複数のパーティーの中の第4のパーティーからオブジェクトをトレースする要求を受信することと、オブジェクトをトレースする要求を受信することによって、オブジェクトに関連する操作についての1つまたは複数のレコードをブロックチェーンデータベースから検索することと、検索されたレコードを第4のパーティーに提供することと、をさせる。

20

【 0 0 7 9 】

[0090]いくつかの実装形態では、要求された操作を検証することはさらに、操作についての要求を受信することによって、操作に関連する通知を複数のパーティーにブロードキャストすることを含む。

【 0 0 8 0 】

[0091]いくつかの実装形態では、要求された操作を検証することは、要求からルールセットへの参照を抽出することと、検証することについての参照に基づいてルールセットをアドレス指定することと、を含む。

30

【 0 0 8 1 】

[0092]いくつかの実装形態では、ルールセットは実行可能コードを含み、要求された操作を検証することは、コードを実行させることによって要求された操作を検証することを含む。

【 0 0 8 2 】

[0093]いくつかの実装形態では、レコードはさらに、次のうちの少なくとも1つを含む：ルールセットに固有のイベントID、ルールセットへの参照、操作についてのID、操作の記載、第1のパーティーのシグネチャ、第1のパーティーのシグネチャを復号するための公開鍵、および要求が送信された時間ポイントを示すタイムスタンプ。

40

【 0 0 8 3 】

[0094]いくつかの実装形態では、命令は、処理ユニットによって実行される時、さらにデバイスに：操作の状態、操作が成功裏に実施されたかどうかを示す状態についての問い合わせを受信することと、問い合わせに応じて、ブロックチェーンデータベースにおける操作についてのレコードに追加される後続のレコードの数を決定することと、後続のレコードの数に基づいて操作の状態を判断することと、をさせる。

【 0 0 8 4 】

[0095]いくつかの実装形態では、本明細書に記載される主題はコンピュータプログラム製品として具体化されることができる。コンピュータプログラム製品は有形に非一時的な機械読み取り可能媒体に記憶され、機械実行可能命令を含む。命令はデバイス上で実行さ

50

れる時、デバイスに複数のパーティーの中の第1のパーティーからオブジェクトに関連する操作についての要求を受信することと、複数のパーティーによって合意されたルールセットに基づいて要求された操作を検証することと、ルールセットはオブジェクトに関連する1つまたは複数の操作に対する1つまたは複数の制約を定義する、検証することと、要求された操作が有効であると検証することに応答して操作を実施させることと、操作についてのレコードを作成することと、レコードはルールセットに固有である、作成することと、レコードを複数のパーティーにアクセス可能であるブロックチェーンデータベースに記憶することと、をさせる。

【0085】

[0096]いくつかの実装形態では、命令はデバイス上で実行される時、さらにデバイスに、複数のパーティーの中の第2のパーティーから、ルールセットを設定する要求を受信することによって、複数のパーティーにルールセットをブロードキャストすることによって、および複数のパーティーの少なくともいくつかからルールセットに対する確認を受信することに応答して、ルールセットを有効化することによって、複数のパーティーについてルールセットを設定すること、をさせる。

10

【0086】

[0097]いくつかの実装形態では、ルールセットを有効化することは、複数のパーティーの中の第3のパーティーからルールセットに対する確認を受信することに応答して、確認についてのレコードを作成することと、レコードは第3のパーティーのシグネチャを含む、作成することと、確認についてのレコードをブロックチェーンデータベースに記憶することと、を含む。

20

【0087】

[0098]いくつかの実装形態では、命令はデバイス上で実行される時、さらにデバイスに、複数のパーティーの中の第4のパーティーからオブジェクトをトレースする要求を受信することと、オブジェクトをトレースする要求を受信することに応答して、オブジェクトに関連する操作についての1つまたは複数のレコードをブロックチェーンデータベースから検索することと、検索されたレコードを第4のパーティーに提供することと、をさせる。

【0088】

[0099]いくつかの実装形態では、要求された操作を検証することはさらに、操作についての要求を受信することに応答して、操作に関連する通知を複数のパーティーにブロードキャストすることを含む。

30

【0089】

[0100]いくつかの実装形態では、要求された操作を検証することは、要求からルールセットへの参照を抽出することと、検証することについての参照に基づいてルールセットをアドレス指定することとを含む。

【0090】

[0101]いくつかの実装形態では、ルールセットは実行可能コードを含み、要求された操作を検証することは、コードを実行させることによって要求された操作を検証することを含む。

40

【0091】

[0102]いくつかの実装形態では、レコードはさらに、次のうちの少なくとも1つを含む：ルールセットに固有のイベントID、ルールセットへの参照、操作についてのID、操作の記載、第1のパーティーのシグネチャ、第1のパーティーのシグネチャを復号するための公開鍵、および要求が送信された時間ポイントを示すタイムスタンプ。

【0092】

[0103]いくつかの実装形態では、命令はデバイス上で実行される時、さらにデバイスに：操作の状態、操作が成功裏に実施されたかどうかを示す状態についての問い合わせを受信することと、問い合わせに応答して、ブロックチェーンデータベースにおける操作についてのレコードに追加される後続のレコードの数を決定することと、後続のレコードの

50

数に基づいて操作の状態を判断することと、をさせる。

【0093】

[00104]本開示の前述の例示の実装形態に対する様々な修正、適合が、添付の図面と併せて読む時、前述の記載に照らして関連分野の当業者にとって明らかになるであろう。任意のおよび全ての修正は、なお本開示の非限定的なおよび例示の実装形態の範囲内に入るであろう。さらに、本明細書において説明される本開示の他の実装形態は、本開示のこれらの実装形態の関連する分野の当業者にとって想到されるであろうことであり、前述の記載および図面において提示される教示の利益を有する。

【0094】

[00105]したがって、本開示の実装形態は開示される具体的な実装形態に限定されるものではないこと、および修正および他の実装形態は添付の特許請求の範囲に含まれることを意図されていることを諒解されたい。本明細書においては特定の用語が使用されているが、それらは一般のおよび説明的な意味において使用されるのみであって、限定の目的はない。

10

【図1】

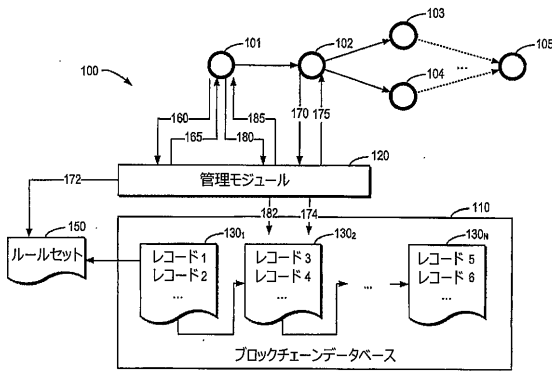


FIG. 1

【図2】

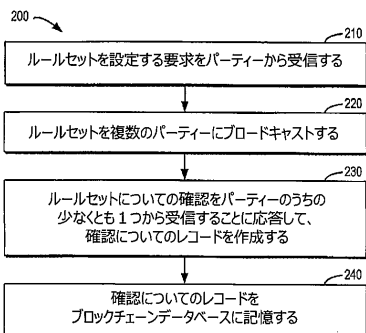


FIG. 2

【図3】

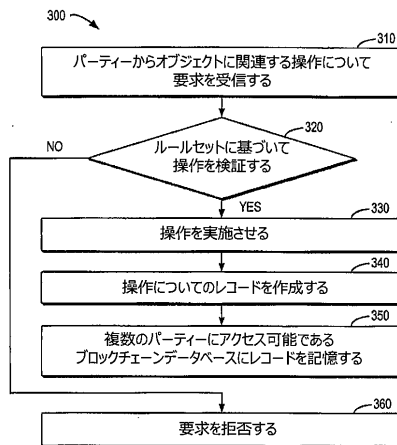


FIG. 3

【図4】

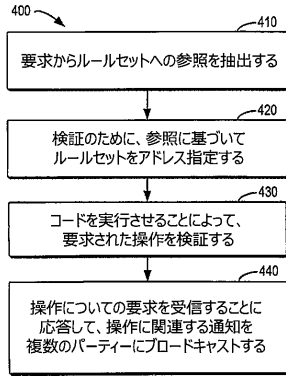


FIG. 4

【図5】

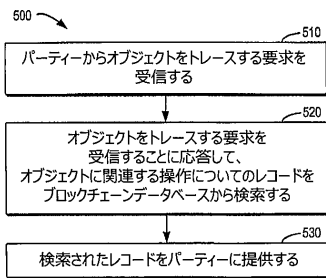


FIG. 5

【図6】

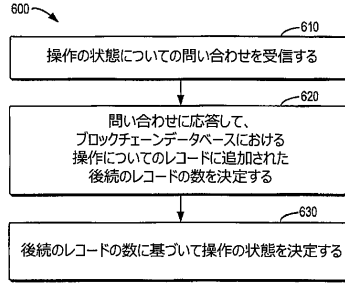


FIG. 6

【図7】

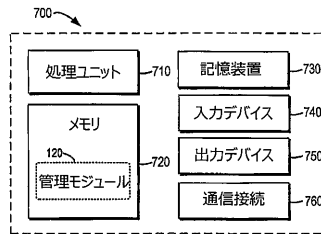


FIG. 7

【図8】

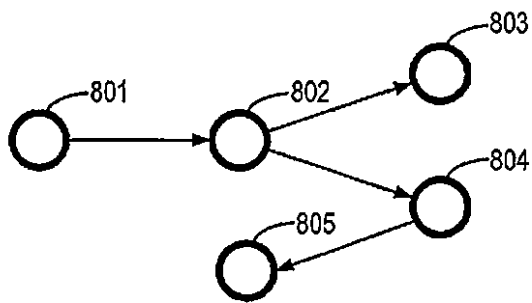


FIG. 8

フロントページの続き

(74)代理人 100153028

弁理士 上田 忠

(72)発明者 ヤン, イーン

中華人民共和国ペキン 100080, ハイディアンのディストリクト, ダンリーン・ストリート, ナンバー 5, ビルディング 2, ヘッドクォーターズ 14エフ, マイクロソフト・アジア・パシフィック・アールアンドディー

(72)発明者 チェン, ヤーン

中華人民共和国ペキン 100080, ハイディアンのディストリクト, ダンリーン・ストリート, ナンバー 5, ビルディング 2, ヘッドクォーターズ 14エフ, マイクロソフト・アジア・パシフィック・アールアンドディー

(72)発明者 モスキブローダ, トーマス

中華人民共和国ペキン 100080, ハイディアンのディストリクト, ダンリーン・ストリート, ナンバー 5, ビルディング 2, ヘッドクォーターズ 14エフ, マイクロソフト・アジア・パシフィック・アールアンドディー

(72)発明者 チャーン, エリック

中華人民共和国ペキン 100080, ハイディアンのディストリクト, ダンリーン・ストリート, ナンバー 5, ビルディング 2, ヘッドクォーターズ 14エフ, マイクロソフト・アジア・パシフィック・アールアンドディー

(72)発明者 レン, ジーンレイ

中華人民共和国ペキン 100080, ハイディアンのディストリクト, ダンリーン・ストリート, ナンバー 5, ビルディング 2, ヘッドクォーターズ 14エフ, マイクロソフト・アジア・パシフィック・アールアンドディー

(72)発明者 チェン, リヤーン

中華人民共和国ペキン 100080, ハイディアンのディストリクト, ダンリーン・ストリート, ナンバー 5, ビルディング 2, ヘッドクォーターズ 14エフ, マイクロソフト・アジア・パシフィック・アールアンドディー

(72)発明者 ガオ, ヤンジエ

中華人民共和国ペキン 100080, ハイディアンのディストリクト, ダンリーン・ストリート, ナンバー 5, ビルディング 2, ヘッドクォーターズ 14エフ, マイクロソフト・アジア・パシフィック・アールアンドディー

審査官 宮司 卓佳

(56)参考文献 米国特許第09300678 (US, B1)

国際公開第2016/063092 (WO, A1)

(58)調査した分野(Int.Cl., DB名)

G06F 21/62

G06F 21/60

H04L 9/32