

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2021-517686

(P2021-517686A)

(43) 公表日 令和3年7月26日(2021.7.26)

(51) Int.Cl.
G06Q 10/08 (2012.01)

F I
G06Q 10/08

テーマコード(参考)
5 L049

審査請求 未請求 予備審査請求 未請求 (全 52 頁)

(21) 出願番号 特願2020-548681 (P2020-548681)
 (86) (22) 出願日 平成31年3月14日 (2019. 3. 14)
 (85) 翻訳文提出日 令和2年10月22日 (2020. 10. 22)
 (86) 国際出願番号 PCT/IL2019/050283
 (87) 国際公開番号 W02019/175878
 (87) 国際公開日 令和1年9月19日 (2019. 9. 19)
 (31) 優先権主張番号 62/642, 858
 (32) 優先日 平成30年3月14日 (2018. 3. 14)
 (33) 優先権主張国・地域又は機関 米国 (US)

(71) 出願人 517344619
 セキュリティ マターズ リミテッド
 イスラエル国、ディー、エヌ、シェヴェル
 エイロット 8884000、キブツ
 ケツラ
 (74) 代理人 110003007
 特許業務法人謝国際特許商標事務所
 (72) 発明者 アロン、ハガイ
 イスラエル国 7682900 キブツ
 ナアーン
 (72) 発明者 ヨラン、ナダヴ
 イスラエル国 6998250 テル ア
 ビブ、レフィジム ストリート 24

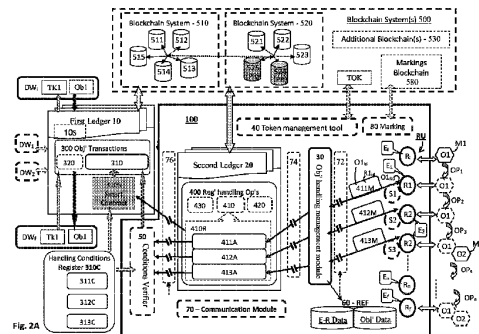
最終頁に続く

(54) 【発明の名称】 ブロックチェーンを介したサプライチェーンの管理、及び、整合性検証のためのシステム、及び、方法

(57) 【要約】

【課題】 ブロックチェーンを介したサプライチェーン管理、及び、完全性検証のためのシステム、及び、方法の提供。

【解決手段】 物理的な対象物の取引を管理するためのシステム、及び、方法が開示される。システムは、当事者間の、又は、複数の物理的な対象物の取引に関連する対象物取引を記録するように適合された第1の分散台帳に接続可能である。システムは、1つ以上の物理的な対象物に関して実行された対象物処理動作を示すデータを記録するように適合された第2の分散台帳と、1つ以上の物理的な対象物に関して実行される処理操作を認証するように構成された対象物処理管理モジュールを含む。対象物処理管理モジュールは、処理動作の実行パラメータを取得し、処理動作の実行パラメータを認証し、認証された処理動作を第2の分散台帳に記録するように構成され、及び、動作可能である。これにより、システムは、1つ以上の物理的な対象物に関して実行される処理動作の実行パラメータが、1つ以上のそれぞれの予め定められた条件を満たすことを認証する際に、1



【特許請求の範囲】**【請求項 1】**

物理的な対象物の取引を管理するためのシステムであって、
前記システムは、
当事者間の 1 以上の物理的な対象物の取引に関連する対象物取引を記録するように適合された第 1 の分散台帳に接続でき、
前記システムは、
1 つ以上の前記物理的な対象物に関して実行された対象物処理操作を示すデータを記録するように適合された第 2 の分散台帳、及び、
前記処理操作の実行パラメータを取得し、前記処理操作の実行パラメータを認証し、及び、前記第 2 の分散台帳に、前記認証された処理操作を記録することを実行することによって、1 つ以上の前記物理的な対象物に関して実行される処理操作を認証するように適合された対象物処理管理モジュール、
を有し、
これにより、1 つ以上の前記物理的な対象物に関して実行される前記処理操作の実行パラメータが、1 つ以上のそれぞれの予め定められた条件を満たすことを認証する際に、1 つ以上の前記物理的な対象物に関連する対象物取引を記録できる、
システム。

10

【請求項 2】

請求項 1 に係るシステムにおいて、
前記第 1 の台帳は、
(i) 前記 1 つ以上の対象物の所有権の取引；及び、
(i i) 前記 1 つ以上の対象物の所有権の変更に関連したトークンの取引。
の少なくとも 1 つを記録するように構成され、動作可能であるシステム。

20

【請求項 3】

請求項 1、又は、請求項 2 に係るシステムにおいて、
前記第 1 の分散台帳は、
前記第 2 の分散台帳へのアクセスを有し、及び、ある物理的な対象物に関して実行される少なくとも 1 つの処理操作を示す前記データを得るように適合されており、及び、前記少なくとも 1 つの処理操作が、前記少なくとも 1 つの取引のための前記スマートコントラクト台帳にスマートコントラクトによって示される少なくとも 1 つの予め定められた条件に依拠していることを判定する際に、前記第 1 の台帳に前記少なくとも 1 つの対象物の取引を記録する、スマートコントラクト台帳である、
システム。

30

【請求項 4】

請求項 1、又は、請求項 2 に係るシステムにおいて、
前記第 2 の分散台帳へのアクセスを有し、また、ある物理的な対象物に関して実行される少なくとも 1 つの処理操作を示すデータを得るように構成され、及び、動作可能であり、及び、前記少なくとも 1 つの処理操作が、少なくとも 1 つの予め定められた条件に依拠していることを判定する際に、前記第 1 の台帳 10 に、前記少なくとも 1 つの対象物の取引を記録する条件検証モジュール、
を有するシステム。

40

【請求項 5】

請求項 1 ~ 請求項 4 のいずれかに係るシステムにおいて、
前記第 1 の分散台帳を実行するように構成され、また、動作可能なブロックチェーンシステムに接続できる、
システム。

【請求項 6】

請求項 1 ~ 請求項 5 のいずれかに係るシステムにおいて、
前記第 2 の分散台帳を実行するように構成され、また、動作可能なブロックチェーンシ

50

システムに接続できる、
システム。

【請求項 7】

請求項 1 ~ 請求項 6 のいずれかに係るシステムにおいて、
前記第 1、及び、第 2 の分散台帳の両方を実行するように構成され、また、動作可能な
ブロックチェーンシステムに接続できる、
システム。

【請求項 8】

請求項 6、又は、請求項 7 に係るシステムにおいて、
前記対象処理管理モジュールは、
記第 2 の分散台帳において、処理操作の実行のパラメータを記録するように動作できる
前記ブロックチェーンシステムの特権ノードを有する、
システム。

10

【請求項 9】

請求項 8 に係るシステムにおいて、
前記ブロックチェーンシステムの非特権ノードは、
前記ブロックチェーンにおける前記第 2 の分散台帳のデータレコードの書き込みを開始
することを許可されない、
システム。

【請求項 10】

20

請求項 1 ~ 請求項 9 のいずれかに係るシステムにおいて、
前記対象物処理管理モジュール、又は、前記システムの通信モジュールに接続可能であ
り、及び、特定のブロックチェーンシステムにおける少なくとも 1 つの予め定められたト
ークンの取引を示すデータを受信すると、前記対象物処理管理モジュールによって前記処
理操作を認証 / 妥当性確認できるように構成され、また、動作可能であるトークン管理モ
ジュール、
を有するシステム。

【請求項 11】

請求項 10 に係るシステムにおいて、
前記第 1 の、及び、第 2 の台帳の少なくとも 1 つは、
前記特定のブロックチェーンシステムで実行される、
システム。

30

【請求項 12】

請求項 1 ~ 請求項 11 のいずれかに係るシステムにおいて、
前記対象物処理管理モジュールは、
前記 1 つ以上の物理的な対象物に関して実行される前記処理操作を認証するように構成
され、それによって、前記 1 つ以上の物理的な対象物は、1 つ以上の読取ユニットによっ
て読み取りできる 1 つ以上のマーキングによって、マークされ、
前記対象物処理管理モジュールは、
少なくとも 1 つの読取ユニットから、前記処理操作に関連して前記読取ユニットによっ
て読み取られる前記対象物の特定のマーキングを示すデータを取得することによって、物
理的な対象物の処理操作を認証するように適合されている、
システム。

40

【請求項 13】

請求項 12 に係るシステムにおいて、
前記対象処理管理モジュールは、
前記読取ユニットを識別するデータを取得し、前記対象物の前記特定のマーキングを用
いることによって、前記対象物の前記処理操作を認証して、前記対象物の同一性を認証し
、前記読取ユニットを識別するデータを用いて、前記読取ユニットの所有権を有し、前記
処理操作を実行する実体の同一性を認証し、及び、それによって、処理操作が、識別され

50

た対象物上に、前記実体によって、実行されたことを検証するように適合されている、システム。

【請求項 14】

請求項 13 に係るシステムにおいて、

i . 前記読取ユニットから取得された前記対象物の前記特定のマーキングのデータと、前記対象物によって前記特定のマーキングを示す予め記憶された参照データとの間の一致を判定することによって、前記対象物の同一性を認証すること、

ii . 前記読取ユニットを識別するデータと、前記 1 つ以上の読取ユニットを所有しているそれぞれの主体に関連付けられている前記 1 つ以上の読取ユニットの同一性を列挙する参照データとの間の一致を判定することによって、前記読取ユニットを所有する主体の同一性を認証すること、

の少なくとも 1 つを有するシステム。

【請求項 15】

請求項 13、又は、請求項 14 に係るシステムにおいて、

記処理操作の前記認証は、

前記対象物上に実行される前記処理操作が、前記実体に対して認証されることの検証を有する、

システム。

【請求項 16】

請求項 15 に係るシステムにおいて、

前記第 1 の分散台帳は、

前記物理的な対象物の取引のためのスマートコントラクトを含むスマートコントラクト台帳であって、それによって、前記スマートコントラクトは、前記物理的な対象物の前記対象物取引のために実行される特定の 1 つ以上のそれぞれの処理操作の予め定められた実行条件を示し、及び、

前記処理操作の妥当性確認は、

前記処理操作が、実行条件によって示されるそれぞれの実体によって、実行されること、及び、実行条件を予め定めた条件に沿っていることの判定を有する、

システム。

【請求項 17】

請求項 12 ~ 請求項 16 のいずれかに係るシステムにおいて、

前記対象処理管理モジュールは、

前記委読取ユニットを認証し、前記対象物の特定のマーキングを読み取るように適合される、

システム。

【請求項 18】

請求項 17 に係るシステムにおいて、

前記対象物処理管理モジュールは、

前記特定のマーキングを読み取るための読取パラメータを示すデータを用いて、前記読取ユニットと通信することによって、前記読取ユニットを認証し、前記特定のマーキングを読み取る、

システム。

【請求項 19】

請求項 18 に係るシステムにおいて、

前記読取ユニットは、

前記読み取りパラメータに対応する特定の読み取りスキームを処理し、及び、それによって、前記対象物の特定のマーキングを示すデータを、判定し、及び、前記対象処理管理モジュールに送信するように適合される、

システム。

【請求項 20】

10	
20	
30	
40	
50	

請求項 12 ~ 請求項 19 のいずれかに係るシステムにおいて、
前記物理的な対象物は、
物理的な対象物を示し、及び、前記物理的な対象物に適用され、又は、その中に埋め込まれる物理的なマーキングによってマークされる、
システム。

【請求項 21】

請求項 20 に係るシステムにおいて、
それぞれの物理的な対象物の前記物理的なマーキングは、
前記それぞれの物理的な対象物を識別する、
システム。

10

【請求項 22】

請求項 20、又は、請求項 21 に係るシステムにおいて、
それぞれの物理的な対象物の前記物理的なマーキングは、
前記物理的な対象物のそれぞれのタイプ、又は、バッチを識別する、
システム。

【請求項 23】

請求項 20 ~ 請求項 22 のいずれかに係るシステムにおいて、
前記物理的なマーキングは、
前記それぞれの物理的な対象物の XRF 分析装置を介して識別可能な X 線蛍光 (XRF
) 署名であり、及び、
前記読取ユニットは、
XRF 測定を実行し、前記 XRF 署名を読み取るように構成され、また、動作可能である、
システム。

20

【請求項 24】

請求項 23 に係るシステムにおいて、
前記読取ユニットは、
前記対象物の少なくとも一部を X 線、又は、
線で照射し、及び、前記物理的な対象物の前記 XRF 署名を示す X 線蛍光応答を検出するように構成され、また、動作可能である、
システム。

30

【請求項 25】

請求項 24 に係るシステムにおいて、
前記読取ユニットは、
前記対象物の前記 XRF 署名を処理し、前記マーキングを、それぞれに判定するように適合される、
システム。

【請求項 26】

請求項 25 に係るシステムにおいて、
前記マーキングは、
前記対象物の材料組成に関連付けられた前記物理的な対象物の根本的なマーキングであって、したがって、前記対象物から分離できない、
システム。

40

【請求項 27】

請求項 10 ~ 請求項 20 のいずれかに係るシステムにおいて、
前記処理動作は、
(i) 前記対象物の占有権の変更、
(ii) 前記対象物の輸送 / 保尊、
(iii) 他の対象物と前記対象物との組み立て品、
のいずれかを有する、

50

システム。

【請求項 28】

請求項 1 ~ 請求項 27 のいずれかに係るシステムにおいて、
前記システムは、
前記対象物の前記取引の前記処理操作を実行するための少なくとも 1 つの予め定められた条件を含む、スマートコントラクト、又は、処理条件レジストリに関連付けられる、
システム。

【請求項 29】

請求項 28 に係るシステムにおいて、
少なくとも 1 つの前記処理操作を実行するための前記予め定められた条件は、
前記それぞれの処理操作を実行するために前記対象物の占有を有していることを示した、
特定の実体を示すデータを有する、
システム。

10

【請求項 30】

請求項 28、又は、請求項 29 に係るシステムにおいて、
前記スマートコントラクトにおける前記処理操作に関連付けて指定される前記予め定められた条件は、
前記処理操作を実行するために必要とされる環境 / 周囲条件、
前記処理操作を実行するための位置条件、
前記処理操作のための必須条件としての前記他の対象物の識別性、
の 1 つ以上を有する、
システム。

20

【請求項 31】

請求項 30 に係るシステムにおいて、
前記対象処理管理モジュールは、
前記少なくとも 1 つの予め定められた条件の実行条件を、前記処理操作に関連付けて、
測定し、及び、したがって、前記対象物処理管理モジュールに、前記処理操作の前記実行
パラメータを伝達するように構成され、また、動作可能な 1 つ以上の知覚システムに接続
可能である、
システム。

30

【請求項 32】

請求項 31 に係るシステムにおいて、
前記対象処理管理モジュールは、
前記対象物の特定のマーキングを読み取ることによって、前記対象物の識別するように
適合された少なくとも 1 つの読取ユニットに接続可能であり、及び、
前記 1 つ以上の知覚システムは、
少なくとも 1 つの読取ユニットに関連付けられ、及び、前記それぞれの処理操作の前記
実行パラメータに関連付けられて、前記処理操作の前記実行条件を通信するように適合さ
れる、
システム。

40

【請求項 33】

請求項 31、又は、請求項 32 に係るシステムにおいて、
前記 1 つ以上の前記感知システムの感知システムは、
少なくとも 1 つのセンサ、及び、前記センサによって測定される実行データのパラメー
タを通信するための読出ユーティリティを有する、
システム。

【請求項 34】

請求項 31 ~ 請求項 33 のいずれかに係るシステムにおいて、
前記 1 つ以上の前記感知システムの感知システムは、
温度センサ、湿度センサ、光センサ、位置センサ（例えば、GPS）、及び、慣性セン

50

サの少なくとも1つを有する少なくとも1つのセンサを有する、システム。

【請求項35】

対象物に関して実行される予定の1つ以上の処理操作のそれぞれ処理操作ごとに、第1の分散台帳に、前記対象物に関する対象物取引を登録するために、

前記処理操作の測定された実行パラメータを判定し、それによって、前記測定された実行パラメータの判定は、前記処理操作を実行する実体に割り当てられた読取装置によって前記対象物のマーキング/署名を読み取り、

前記測定された実行パラメータを認証し、前記読取装置によって読み取られたマーキング/署名に基づいて、前記処理操作が実行された前記物理的な対象物を示すデータを判定し、及び、前記読取装置に関するデータに基づいて、前記処理操作を実行する前記実体を識別し、並びに、

前記認証された実行パラメータを利用して、第2の分散台帳における前記処理操作の登録を妥当性検証し、認証された処理操作の分散台帳を提示し、

これにより、前記第2の分散台帳に認証された処理操作として、前記1つ以上の処理操作のそれぞれを登録する際に、前記第1の分散台帳における前記対象物取引の登録を妥当性確認できること、を実行すること、

を有する物理的な対象物の取引を管理する方法。

【請求項36】

請求項35に係る方法において、さらに、

前記処理操作の前記認証された実行パラメータが、前記対象物取引に必要とされ、及び、前記処理操作の対象となるように指定される、前記処理操作を実行するための少なくとも1つの主体、及び、指定された前記対象物の同一性、又は、タイプを示す予め定められた条件を満たすことを検証し、

前記検証は、

前記処理操作上の実際の対象物である前記対象物と、指定された対象物との間の一致を判定し、及び、前記処理操作を実行する実際の実態と、指定された実態との間の一致を判定する、

方法。

【請求項37】

請求項36に係る方法において、

少なくとも1つの処理操作の前記測定された実行パラメータの判定は、さらに、

前記読取ユニットに関連付けられたセンサからの追加の知覚データの計測を有し、

前記検証は、さらに、

前記感覚データと、前記予め定められた条件に含まれる追加の実行条件との間の一致を判定することを有する、

方法。

【請求項38】

請求項36、又は、請求項37に係る方法において、

前記第2の台帳における前記処理操作の登録の妥当性検証は、

前記処理操作の前記測定された実行パラメータの検証を有する、

方法。

【請求項39】

請求項36～請求項38のいずれかに係る方法において、

前記第1の台帳への前記対象物取引の登録の妥当性検証は、

前記1つ以上の処理操作のそれぞれ毎の前記測定された実行パラメータの検証を有する、

方法。

【請求項40】

請求項36～請求項39のいずれかに係る方法において、

10

20

30

40

50

前記第 1 の台帳は、

前記対象物取引を実行するためのスマートコントラクトを含むスマートコントラクト台帳であり、

前記スマートコントラクトは、

サブ取引を含み、それによって、1つ以上の前記サブ取引は、前記1つ以上の処理操作に関連付けられ、及び、前記第2の台帳にアクセスするように適合され、及び、前記1つ以上の処理操作の前記認証された実行パラメータは、前記対象物取引に要求される前記予め定められた条件を満たす前記検証を実行する、

方法。

【請求項 4 1】

10

請求項 3 5 ~ 請求項 4 0 のいずれかに係る方法において、

前記第 1、及び、第 2 の台帳は、

1つ以上のブロックチェーンシステムで実行される、

方法。

【請求項 4 2】

請求項 3 5 ~ 請求項 4 1 のいずれかに係る方法において、

前記物理的な対象物は、

識別可能な X R F 署名 / マーキングを有し、及び、

前記読み取りは、

前記対象物の前記 X R F / 署名を検出し、それによって、前記対象物の I D、又は、タイプ、又は、バッチを判定できることを有する、

20

方法。

【請求項 4 3】

請求項 4 2 に係る方法において、

前記 X R F 署名 / マーキングは、

前記対象物の要素であり、及び、前記対象物の1つ以上のパーツの材料組成に関連付けられ、したがって、前記対象物から分離できない、

方法。

【請求項 4 4】

前記1つ以上のブロックチェーンシステムの第1の分散台帳における前記対象物取引の妥当性検証するために、1つ以上のブロックチェーンシステムとデータ通信する対象物署名読取装置であって、

30

前記対象物署名読取装置は、

前記物理的な対象物上のマーキング / 署名を読み取り、前記マーキング / 署名を示すデータを判定するように構成され、また、動作可能である署名 / マーキング読取モジュール、

前記対象物署名読取装置を一意に識別する読取装置 I D データを搬送する識別モジュール、

前記対象物署名読取装置とデータ通信でき、1つ以上の物理的な対象物のマーキング / 署名を示し、及び、前記読取装置 I D データに関連付けられた前記対象物署名読取装置を占有している実体を示す参照データにアクセスし、及び、前記1つ以上のブロックチェーンシステムと前記対象物署名読取装置との通信を可能にするネットワーク通信モジュール、

40

前記署名 / マーキング読取モジュールに、及び、前記通信モジュールに、接続可能であり、及び、

(i) 前記読取モジュールから得られた前記物理的な対象物の前記マーキング / 署名のデータと前記参照データ内の1つ以上の物理的な対象物の前記マーキング / 署名との間の一致を判断することによって、前記対象物の物理的な対象物の同一性、又は、タイプ、又は、バッチを認証し、

前記対象物署名読取装置を識別する前記読取装置 I D データと、前記参照データにリス

50

トされている前記実体の識別との間の一致を判断することによって、前記対象物署名読取装置を占有する実体の同一性を認証し、

それによって、前記処理操作を認証する、

ことによって、前記物理的な対象物に関して実行される少なくとも1つの処理操作の実行パラメータを認証し、

(i i) 前記ネットワーク通信モジュールを動作させ、前記1つ以上のブロックチェーンシステムにアクセスし、及び、前記1つ以上のブロックチェーンシステムで第2の分散台帳における前記認証された処理操作の登録を妥当性検証し、それによって、前記第2の台帳におけるその対象物取引に関連付けられた処理操作の認証の妥当性確認の際に、前記第1の台帳に前記物理的な対象物に関連付けられた対象物取引を記録できる、

ように構成され、及び、動作可能な対象物処理管理モジュール、

を有する対象物署名読取装置。

【請求項45】

請求項44に係る対象物署名読取装置において

前記対象物処理管理モジュールは、

前記マーキング/署名を読み取るための前記読取パラメータを示すデータを前記レンダリングモジュールユニットに提供することによって、前記読取モジュールを認証し、前記物理的な対象物のマーキング/署名を読み取り、及び、

前記読取モジュールは、

前記読取パラメータに対応するある読取読スキームを動作させ、それによって、前記マーキング/署名を示す前記データを判定するように適合される、

対象物署名読取装置。

【請求項46】

請求項44、又は、請求項45に係る対象物署名読取装置において、

前記処理操作の予め定められた条件を示すデータを取得するように適合され、及び、前記認証された処理操作の前記実行パラメータが前記予め定められた条件に適合することを検証すると、前記第2の分散台帳における前記認証された処理操作の登録を妥当性検証できるように適合された前記条件検証モジュール、

を有する対象物署名読取装置。

【請求項47】

請求項44～請求項46のいずれかに係る対象物署名読取装置において、

前記対象物処理管理モジュールに、又は、前記ネットワーク通信モジュールに、接続可能であり、及び、前記1つ以上のブロックチェーンシステムにおいて、少なくとも1つの予め定められたのトークン取引に対する前記処理操作を認証し/妥当性検証できるように構成され、また、動作可能であるトークン管理モジュール、

を有する対象物署名読取装置。

【請求項48】

請求項44～請求項47のいずれかに係る対象物署名読取装置において、

前記物理的な対象物の署名/マーキングは、

前記物理的な対象物に埋め込まれた要素XRF署名であり、

前記読み取りモジュールは、

前記XRF署名/マーキングを読み取るために前記物理的物体のXRF測定を実行するように構成され動作可能なXRF測定モジュール、

を有し、

前記読取モジュールは、

前記対象物の少なくとも一部を、X線、又は、線で照射し、及び、前記XRF署名/マーキングを示すX線-蛍光応答を検出することによって、XRF測定を実行するように構成おされ、また、動作可能である、

対象物署名読取装置。

【請求項49】

10

20

30

40

50

請求項 4 4 ~ 請求項 4 8 のいずれかに係る対象物署名読取装置において、
前記参照データの少なくとも一部は、
前記 1 つ以上のブロックチェーンシステムによって非集中の分散された方式で記憶される、
対象物署名読取装置。

【請求項 5 0】

請求項 4 4 ~ 請求項 4 9 のいずれかに係る対象物署名読取装置において、
少なくとも 1 つの処理が実行されたときに存在する 1 つ以上の実行条件を測定するように構成され、及び、動作可能であり、それによって、許容できる実行条件の下で前記処理動作が実行されることを検証できる 1 つ以上のセンサ、
を有する対象物署名読取装置。

10

【請求項 5 1】

請求項 1 ~ 請求項 3 4 のいずれかに係るシステムを有する請求項 4 4 ~ 請求項 5 0 のいずれかに係る対象物署名読取装置。

【発明の詳細な説明】

【& # 8 2 0 3 ; 技術分野】

【0 0 0 1】

本発明は、サプライチェーンの管理の分野に関し、より具体的には、分散型台帳を介するサプライチェーンの管理に関する。

20

& # 8 2 0 3 ;

【背景技術】

【0 0 0 2】

対象物の X 線蛍光署名、及び / 又は、マーキング（ここでは、一般的に、マーキングと呼ぶ）は、様々な物理的な対象物、及び / 又は、そのような物理的な対象物のタイプ、又は、バッチ / ロットをマーキングし、及び、認証するための堅牢性、信頼性のある技術を容易にする一方、そのような物理的な対象物の偽造を、実際的な手段（例えば、物理的な対象物を破壊することなく）で、防止 / 排除する。対象物に付加され、及び / 又は、対象物に本質的に存在する X R F マーキング / 署名に基づいて様々なタイプ、又は、対象物をマーキングし、及び / 又は、認証するための技術は、汎用的な堅牢性を有し、様々なタイプの対象物、及び、材料の識別、及び、認証のために使用され得る。

30

【0 0 0 3】

例えば、本出願の譲受人に譲渡された P C T 特許出願国際公開 W O 2 0 1 6 / 1 5 7 1 8 5 は、X R F マーキングでマークされた対象物を認証する方法、及び、システムを開示する。この方法は、対象物に照射された X 線、又は、線に依りて、対象物から到来する X 線信号の検出された部分に関する波長スペクトルプロファイルを提供し、また、X 線信号の検出された部分に関する波長スペクトルプロファイルをフィルタリングし、波長スペクトルプロファイルから、X 線信号部分のノイズ、及び、クラッタのうちの少なくとも 1 つに関連するトレンド的、及び、周期的成分を、抑制し、それによって、改善された信号対雑音、及び / 又は、信号対クラッタ比を有するフィルタリングされたプロファイルを得て、そこから、前記対象物に含まれる材料の署名に関連するスペクトルピークを、改善された精度、及び、信頼性で識別でき得ることを有する。対象物は、フィルタリングされたプロファイルを処理し、所定の条件を満たす 1 つ以上のピークを、その中で、識別することによって認証され、それによって、識別されたピークの波長は、対象物に含まれる材料の署名を示す。

40

【0 0 0 4】

本出願の譲受人に譲渡された P C T 特許出願国際公開 W O 2 0 1 7 / 1 3 4 6 6 0 は、X 線蛍光（X R F）分析を用いて、金属物体のような物体の真正性を検証するための偽造

50

防止マーキング技術を開示する。

【0005】

本出願の譲受人に譲渡されたPCT特許出願国際公開WO2017/175219は、電子システムのコンポーネント（例えば、部品、又は、デバイス）の互換性を検証するための方法、及び、システムを開示する。特定の実施形態では、この方法は、電子システムに関連するであろう第1、及び、第2のコンポーネントを、XRF励起放射線で、照射し、また、照射に 응답して前記第1、及び、第2のコンポーネントから放出される、第1、及び、第2のXRF署名を示す1つ以上のXRF応答信号を検出すること、を含む。そして、第1、及び、第2のXRF署名が処理され、それらが、第1、及び、第2のコンポーネント上の第1、及び、第2のXRFマーキング組成物に、それぞれ、関連付けられているかどうか判定され、また、第1、及び、第2のXRF署名/マーキング間の対応関係に基づいて、電子システムに対する第1、及び、第2のコンポーネントの互換性が、判断/検証される。特定の実施形態は、また、コンポーネントの互換性の検証を可能にする第1、及び、第2のXRFマーキング組成物を、それぞれ、有する第1、及び、第2の電子コンポーネント/デバイスを、少なくとも、有する電子システムを開示する。特定の実施形態は、第1、及び、第2のXRF署名/マーキングの間の対応に基づいて、第1、及び、第2のコンポーネント（例えば、デバイス）をペアリングするための技術を開示する。特定の実施形態は、電子コンポーネントの異なる基板材料に適用されるXRFマーキングのXRF測定値を校正するための様々な校正技術を開示する。

10

【0006】

本出願の譲受人に譲渡されたPCT特許出願国際公開WO2018/055625は、食品の誤取扱、及び、誤使用を検出するための方法を開示し、また、XRF識別可能マーケを有するヒト用、又は、動物用の製品をマーキングする方法を提供する。本方法は、少なくとも製品のある領域に、XRFによって識別できる少なくとも1つのFDAグレード材料のパターンを形成することを含み、そのパターンは、少なくとも部分的には人間の裸眼に対して不可視であり、また、予め定義された識別可能な特性を有し、製品は、食品、治療薬、及び、化粧品から選択される。

20

【0007】

本出願の譲受人に譲渡されたPCT特許出願国際公開WO2018/042427は、予め定められた一次放射に対する石固有の特徴的な放射応答に基づく、石の中に創造されている石固有のID、及び/又は、予め定められたマーキングに従って、石を認証するための方法、及び、システムを開示する。

30

【0008】

本出願の譲受人に譲渡されたPCT特許出願国際公開WO2018/069917は、ポリマー、及び、少なくとも1つのXRF識別可能マーケを含む透明要素を、様々な工業的用途用に、製造するためのポリマー材料、及び、XRF識別可能マーケの配合組成物、及び、マスターバッチを開示する。

【0009】

物理的対象物のXRFマーキング（例えば、署名）の正確で信頼性のある読み取りを実現するための様々な技術は、例えば、上述のWO2016/157185に記載されている技術を含む。その目的のためのXRFリーダは、例えば、本出願の譲受人に譲渡された、異なる対象物上で励起ビームの強度を変調/変化させ、その二次放射を測定することにより、複数の物体のマーキング組成物を検出する新規のXRF解析装置を開示するPCT特許出願国際公開WO2017/221246に記載されているように実施することができる。XRF解析装置は、複数のオブジェクトを同時に照射するための空間強度分布を有する、少なくとも1つのX線、又は、線の励起放射線ビームを照射するように適合された放射線照射アセンブリ、X線、又は、線の放射線による対象物への照射に応じて、複数の対象物から到来する二次放射線X線信号を検出し、また、複数の対象物上で検出されたデータX線信号の空間強度分布を示すデータを提供する放射線検出装置、及び、検出された応答X線信号を受信、処理し、複数の対象物のそれぞれの少なくとも1つの表面に含

40

50

まれるマーキング組成物の存在を検証するように構成された、前記検出器と通信する信号読取プロセッサ、を有する。

【0010】

また、本出願の譲受人に譲渡されたPCT特許出願国際公開WO2018/051353は、試料によって搬送された少なくとも1つの物質、例えば、試料によって搬送される少なくとも1つのマーカ、を検出するためのX線蛍光(XRF)システムの動作を制御するための制御システム、及び、方法を開示する。制御システムは、少なくとも1つの前記材料/マーカに関する材料/マーカ関連データを有する入力データを受け取るためのデータ入力ユーティリティ、データプロセッサ、及び、解析ユーティリティを有する。データプロセッサ、及び、解析ユーティリティは、入力データを解析し、前記XRFシステムの動作状態を最適化して、試料の予め定められた領域に到達し、前記領域の体積によって吸収される一次X線放射量を最大化し、また、XRFシステムの検出器に到達する、前記領域から放射される二次放射の一部を最大化するように、XRFシステムの最適な幾何学的特性を判定し、また、XRFシステムの幾何学的特性を調整できるXRFシステムに対して動作データを生成するように、構成され、動作可能である。

10

【0011】

仮想ドメインでは、ブロックチェーン技術は、分散してデータレコードを記憶/登録するための堅牢で安全な方法を提供する一方で、データの偽造、又は、他の許可されないデータ変更の可能性を実質的に排除する。ブロックチェーン技術は、成長し続ける時間シーケンスされたブロック内に編成されたレコード台帳のコピーを、それぞれが維持するノードのネットワークに基づいている。典型的には、ブロックチェーンタイプのデータレコードは、分散コンピューティングシステムを利用し、また、ハッキング、及び、不要な変化からデータセキュリティを達成するように構成されているレジストリ(例えば、公開)を提供する。ブロックチェーンのアーキテクチャ、及び、デザインは、デジタルデータレコードが破損、又は、複製されず(即ち、1回以上使用できない)、したがって、仮想資産として使用できることを保証する。ブロックチェーンに記録されたデータは、暗号通貨、又は、トークン(仮想通貨とも呼ばれる)として知られる、そのような仮想資産の所有権の連鎖を参照する。

20

【0012】

例えば、PCT特許出願公開WO2018/064645は、設計者、製造業者(例えば、3Dプリンタ所有者、及び、他の従来の製造業者)、配送業者、及び、他の実体を繋げ、また、新しい、及び、既存の製品を製造、及び、供給するプロセスを簡素化する分散型製造プラットフォーム、及び、関連技術を開示している。分散型台帳、又は、ブロックチェーンは、トランザクションを記録し、スマートコントラクトを実行し、他の動作を実行して、サプライチェーンの透明性、及び、完全性を増加させることに利用され得る。パッケージング可能なブロックチェーンは、製造から、輸送を通じた、配送までの小包の移動や状況を追跡するために利用され得る。

30

【0013】

米国特許出願公開2019/012861は、少なくとも物品の所有権を管理するサーバを有するサプライチェーンシステムを開示する。物品は、実際の物体である。コンテナはロックとともに、提供される。ロックは、少なくとも電子プロセスを通じて開放するように構成される。前記コンテナは、物理的に、前記物品を格納できる。少なくとも1つのプロセッサ、又は、回路は、ロックを解放するための開放要求を受信すると、開放要求を発行したユーザと、物品の所有権を有するユーザとが一致するか否かを判定する。開放要求を発行したユーザと、物品の所有権を有するユーザとが一致すると、ロックが解放され、物品をコンテナから取り出せるようにする。サーバは、ロックが解放されたことを通知される。

40

​

【発明の概要】

【0014】

50

様々なタイプの対象物が、固有の、及び／又は、追加された／組み込まれたXRFマーキング／署名に基づいて、容易に、識別され、又は、特徴付けられ得る。これらの対象物は、例えば、金属物、ポリマー、食品、貴重な石、電子コンポーネント／システム、同様に、様々な他の対象物／材料を含んでもよい。前記技術から理解されるように、対象物に対する固有のXRFマーキング／署名の追加、又は、特徴付けは、容易に、簡単な処理、及び、コスト効果的な方法によって（例えば、対象物に対するXRF応答性材料の組み込み、及び／又は、特徴づけによって）、達成され得る。

【0015】

本発明は、仮想ドメインにおける取引を登録するためのブロックチェーン技術の堅牢性と安全性とを結びつける新規なアプローチに、様々なタイプの対象物のXRFマーキング／署名をマーキングし／特徴付け、及び、そのようなXRFマーキングに基づく様々な対象物、及び／又は、その型／ロットを特定するXRF技術の堅牢性、偽造防止安全性、及び、汎用性を提供する。

10

【0016】

実際、本発明の技術は、本質的には、物理的な対象物のXRFタイプのマーキング／署名に限定されない。しかしながら、当業者にはすぐに分かるように、処理操作の組み合わせ識別、追跡、及び、認証の新規な組み合わせが、このような対象物の汎用のXRFマーキング／署名を具体的に用いることによって、物理的な対象物に実行される一方、以下に示す本発明に係るブロックチェーン台帳上で処理するこのような認証を記録することは、偽造防止を防止しながら、物理的な対象物の仮想取引を管理するための堅牢で、安全な手法を提供する。

20

【0017】

この目的のために、本発明の技術は、また、物理的な対象物自身（それらに関連付けられたパッケージ／タグでなく）と物理的な対象物に行われた処理操作の実行条件とを、分散の方法で、即ち、介在型／集中型のサービス／サーバ、又は、モジュールを用いることなく、対象物の処理操作を追跡し、及び、登録することに用いられる非集中のブロックチェーンシステムを用いて、直接リンクする統合／独立型の対象物署名読取装置によって実現されるようにしてもよい。従って、前述の物理的な対象物に行われる処理操作の認証、及び、処理操作が前述の対象物に行われたことの検証は、関係する第三者の介在なく、安全に得られる。

30

【0018】

この目的のために、いくつかの実施形態において、本発明は、物理的な対象物、及び／又は、製品を含むピア・トゥ・ピア（例えば、ビジネス・トゥ・ビジネス）取引を促進するブロックチェーン、及び、トークンシステムを提供する。

【0019】

本発明の技術は、仮想通貨と物理的な対象物／製品との間の交換のための、分散された、オープンな、そして、安全な電子商取引プラットフォームを提供するために、実行される。本発明のシステムによって使用／導入されるブロックチェーン、又は、それらのいくつかは、コンセンサスを達成するための操作の証明、又は、利害関係の証明のようなメカニズムを用いる、非集中の、許可を必要としないネットワーク、又は、認証された当事者のみがネットワーク内のノードとして参加することを許可された許可済システム（permissioned system）を形成できる。さらに別のオプションでは、非認証当事者／実体がノードとしてブロックチェーンに参加できる一方、1以上の当事者は、特権を与えられ、また、ブロックチェーンの他のメンバよりも多くの権限を有してもよい。例えば、特権を与えられた当事者は、取引を妥当性確認する権利、又は、新たなノードをブロックチェーンに追加する権限を有してもよい。以下の説明から容易に理解されるように、ある場合には好都合に、本発明のシステムは、ブロックチェーンの特権を与えられた当事者として実行できる。本発明のシステムは、とりわけ、様々なタイプの商品、製品、及び／又は、パッケージを物理的にマークし、それに、安全で、また、実際的に偽造不可能な物理的な署名を提供する能力に基づいている。本発明のシステムの全体的なアーキテクチャは、複数の仮想

40

50

通貨アカウントと物理的な対象物／製品との間での取引、及び、スマートコントラクト（すなわち、それらの目的がセットされると、自動的に実行し、又は、実施されるプロトコル）を実行できる。

【0020】

ブロックチェーンシステムは、（サーバのネットワーク上で動作している）ノードのネットワーク上で実行される。ブロックチェーンシステムは、マークされた有形の／物理的な対象物の所有権、及び／又は、占有に関する情報の保存、及び、管理に用いられる／を促進する（対象物の所有権者は、対象物を保持し、又は、占有している当事者とは異なってもよい）。ノードを操作しないブロックチェーンシステムのメンバは、デジタルウォレット、又は、ブロックチェーンアプリケーションを介して、ブロックチェーンシステムと情報交換し、それを介して、ブロックチェーン内のデータを読み出し、また、ブロックチェーンに記録されている資産を用いて取引（例えば、所有権の移転）を実行できる。ブロックチェーンシステムは、非集中で、オープンな、許可不要なシステムであってもよいし、認証された当事者のみがブロックチェーンネットワークのメンバになることができるシステムであってもよい。ブロックチェーンシステムは、ネイティブ暗号通貨、又は、トークンを有してもよい。すなわち、取引される仮想通貨、及び、その所有権履歴が、ブロックチェーンシステムに記録される。

10

【0021】

本発明の技術は、その所有権がブロックチェーンシステム上に記録された仮想資産、及び、マークされた有形の対象物（以下、マークされた対象物）を含む取引、及び、スマートコントラクトの実行を提供する。マークされた対象物の所有権の記録、又は、所有権の移転の操作は、（対象物を認証する）読取ユニットによるマークされた対象物上のマーキングの読み取りを必要としてもよい。マーキングを読み取るために、読取ユニットは、本発明のシステムによって実行され得る参照データストレージ、又は、1以上のブロックチェーンシステムにおける分散型ストレージを必要としてもよい。いくつかの実施形態では、物理的な対象物、又は、実体を認証するための本発明の技術によって用いられる読み取りユニットへの、及び／又は、関連付けられた参照データへのアクセスの態様では、認証／取引に関する1つ以上の当事者から予め選択されたデジタルウォレットへのブロックチェーンシステム上での予め選択されたトークンの取引（例えば、認証、又は、支払い）を介することが要求されてもよい。

20

30

【0022】

本発明のさらなる態様では、ブロックチェーンシステムは、マークされた対象物の所有権（例えば、第1の台帳における）、及び、マークされた対象物の占有当事者（例えば、別の台帳における）の両方を記録してもよい。異なる台帳が、同じブロックチェーンシステムによって、例えば、同じブロックのチェーンによって、又は、異なるブロックチェーンシステムによって、登録されてもよいことが容易に理解される。システムは、所有権の移転を伴っても、伴わなくても、対象物の占有の変更を有する取引を促進してもよい。対象物を占有する当事者から別の当事者に転送される取引は、所有権の移転を含む取引とは異なる量のトークンの転送、又は、両方を含む転送を必要としてもよい。加えて、読取ユニットの使用に関する要件は、異なる取引に対して異なってもよい。例えば、1つのタイプの取引（例えば、所有権の移転を伴う取引）は、対象物上のマーキングの読み取りを必要とし、一方、異なるタイプの取引（例えば、占有のみの移転）は、それを必要としなくてもよい。

40

【0023】

この目的のために、本発明の広範な態様によれば、物理的な対象物の取引を管理するためのシステムが提供される。システムは、当事者間の1以上の物理的な対象物の取引に関連する対象物取引を記録するように適合された第1の分散台帳に接続できる。システムは、1つ以上の前記物理的な対象物に関して実行された対象物処理操作を示すデータを記録するように適合された第2の分散台帳；及び、1つ以上の前記物理的な対象物に関して実行される処理操作を認証するように適合された対象物処理管理モジュールを有する。前記対

50

象処理管理モジュールは、前記処理操作の実行パラメータを取得し、前記処理操作の実行パラメータを認証し、及び、前記第2の分散台帳に、前記認証された処理操作（例えば、それらの前記認証された実行パラメータ）を記録するように構成され、動作可能である。これにより、システムは、1つ以上の前記物理的な対象物に関して実行される前記処理操作の実行パラメータが、1つ以上のそれぞれの予め定められた条件を満たすことを認証する際に、1つ以上の前記物理的な対象物に関連する対象物取引を記録できる。

【0024】

いくつかの実施形態では、第1の台帳は、以下の取引の少なくとも1つを記録するように構成され、動作可能である。（i）前記1つ以上の対象物の所有権の取引；及び、（ii）前記1つ以上の対象物の所有権の変更に関連したトークンの取引。

10

【0025】

いくつかの実施形態では、第1の分散台帳は、第2の分散台帳へのアクセスを有し、及び、ある物理的な対象物に関して実行される少なくとも1つの処理操作を示す前記データを得るように適合されており、及び、前記少なくとも1つの処理操作が、前記少なくとも1つの取引のための前記スマートコントラクト台帳にスマートコントラクトによって示される少なくとも1つの予め定められた条件に応じていることを判定する際に、前記第1の台帳に前記少なくとも1つの対象物の取引を記録するスマートコントラクト台帳である。

【0026】

いくつかの実施形態では、前記システムは、第2の分散台帳へのアクセスを有し、また、ある物理的な対象物に関して実行される少なくとも1つの処理操作を示すデータを得るように構成され、また、動作可能であり、さらに、前記少なくとも1つの処理操作が、少なくとも1つの予め定められた条件に応じていることを判定する際に、前記第1の台帳10に、前記少なくとも1つの対象物の取引を記録する条件検証モジュールを有する。

20

【0027】

いくつかの実施形態では、システムは、前記第1の分散台帳を実行するように構成され、また、動作可能なブロックチェーンシステムに接続できる。代替的に、又は、追加的に、いくつかの実施形態では、システムは、前記第2の分散台帳を実行するように構成され、また、動作可能なブロックチェーンシステムに接続できる。いくつかの実施形態では、ブロックチェーンシステムは、前記第1、及び、第2の分散台帳の両方を実行するように構成され、また、動作可能である。一部の実施形態では、前記対象処理管理モジュールは、前記ブロックチェーンシステムの特権ノードを含み、また、前記第2の分散台帳において、処理操作の実行のパラメータを記録するように動作できる。この点で、前記ブロックチェーンシステムの特権ノードは、前記ブロックチェーンにおける前記第2の分散台帳のデータレコードの書き込みを開始することを許可されないようにしてもよい。

30

【0028】

いくつかの実施形態では、前記システムは、前記対象物処理管理モジュール、又は、前記システムの通信モジュールに接続可能であり、及び、特定のブロックチェーンシステムにおける少なくとも1つの予め定められたトークンの取引を示すデータを受信すると、前記対象物処理管理モジュールによって前記処理操作を認証/妥当性確認できるように構成され、また、動作可能であるトークン管理モジュール（ここでは、ツールとしても参照される）を有する。

40

【0029】

いくつかの実施形態では、前記対象処理管理モジュールは、前記1つ以上の物理的な対象物に関して実行される前記処理操作を認証するように構成され、それによって、前記1つ以上の物理的なオブジェクトは、1つ以上の読取ユニット（以降、対象物署名読取装置としても、互換的に、参照される）によって読み取りできる1つ以上のマーキングによって、マークされる。前記対象処理管理モジュールは、少なくとも1つの読取ユニットから、前記処理操作に関連して前記読取ユニットによって読み取られる前記対象物の特定のマーキングを示すデータを取得することによって、物理的な対象物の処理操作を認証するように構成されている。いくつかの実施形態では、前記対象処理管理モジュールは、前記読

50

取ユニットを識別するデータを取得し、前記対象物の前記特定のマーキングを用いることによって、前記対象物の前記処理操作を認証して、前記対象物の同一性を認証し、前記読取ユニットを識別するデータを用いて、前記読取ユニットの所有権を有し、前記処理操作を実行する実体の同一性を認証し、及び、それによって、処理操作が、識別された対象物上に、前記実体によって、実行されたことを検証するように適合されている。この目的のために、対象処理管理モジュールは、以下を実行するように構成され、また、動作可能であってもよい：

i . 前記読取ユニットから取得された前記対象物の前記特定のマーキングのデータと、前記対象物によって前記特定のマーキングを示す予め記憶された参照データとの間の一致を判定することによって、前記対象物の同一性を認証すること、

i i . 前記読取ユニットを識別するデータと、前記1つ以上の読取ユニットを所有しているそれぞれの主体に関連付けられている前記1つ以上の読取ユニットの同一性を列挙する参照データとの間の一致を判定することによって、前記読取ユニットを所有する主体の同一性を認証すること。

【0030】

いくつかの実施形態によれば、前記処理操作の前記認証は、さらに、前記対象物上に実行される前記処理操作が、前記実体に対して認証されていることの検証を含む。

【0031】

いくつかの実施形態では、前記第1の分散台帳は、前記物理的な対象物の取引のためのスマートコントラクトを含むスマートコントラクト台帳である。スマートコントラクトは、前記物理的な対象物の前記対象物取引のために実行される特定の1つ以上のそれぞれの処理操作の予め定められた実行条件を示すようにしてもよい。前記処理操作の妥当性確認は、前記処理操作が、実行条件によって示されるそれぞれの実体（以降、指定された実体としても参照される）によって、実行されること、及び、実行条件を予め定めた条件に沿っていることの判定を含んでもよい。

【0032】

いくつかの実施形態によれば、前記対象処理管理モジュールは、また、前記委読取ユニット（例えば、及び/又は、そのマーキング/署名読取モジュール）を認証し、前記対象物の特定のマーキングを読み取るように適合される。この目的のために、前記対象処理管理モジュールは、読取パラメータを示すデータを提供し、それによって前記特定のマーキングを読み取るために、前記読取ユニットと（例えば、そのマーキング/署名読取モジュールと）通信することによって、前記読取ユニットを認証し、前記特定のマーキングを読み取るようにしてもよい。次に、前記読取ユニット（例えば、前記マーキング/署名読取モジュール）は、前記読み取りパラメータに対応する特定の読み取りスキームを処理し、それによって、前記対象物の特定のマーキングを示すデータを、判定し、及び、前記対象処理管理モジュールに送信するように適合される。

【0033】

いくつかの実施形態では、前記物理的な対象物は、物理的な対象物を示し、及び、前記物理的な対象物に適用され、又は、その中に埋め込まれる物理的なマーキングによってマークされる。それぞれの物理的な対象物の前記物理的なマーキングは、前記それぞれの物理的な対象物を識別し、及び/又は、前記物理的な対象物のそれぞれのタイプ、又は、バッチを識別してもよい。

【0034】

いくつかの実施形態では、前記物理的なマーキングは、前記それぞれの物理的な対象物のXRF分析装置を介して識別可能なX線蛍光（XRF）署名である。前記読取ユニット（例えば、そのマーキング/署名読取モジュール）は、XRF測定を実行し、前記XRF署名を読み取るように構成され、また、動作可能である。例えば、前記読取ユニットは、前記対象物の少なくとも一部をX線、又は、γ線で照射し、及び、前記物理的な対象物の前記XRF署名を示すX線蛍光応答を検出するように構成され、また、動作可能であってもよい。いくつかの実装形態では、前記読取ユニット（例えば、そのマーキング/署名読

10

20

30

40

50

取モジュール)は、前記物理な対象物の前記XRF署名を処理し、それらのマーキング/署名を、それぞれに判定するように構成され、また、動作可能である。この目的のために、マーキング/署名は、前記対象物の材料組成に関連付けられた前記物理的な対象物の根本的なマーキング(elemental markings)であってもよく、したがって、前記対象物から分離できなくてもよい。

【0035】

本発明のいくつかの実施形態によれば、物理的な対象物の対象物取引に含まれる処理操作は、以下のいずれかを含んでもよい：

- (i) 前記対象物の占有権の変更
- (ii) 前記対象物の輸送/保尊
- (iii) 他の対象物と前記対象物との組み立て品

10

【0036】

この目的のために、いくつかの実施形態では、前記システムは、前記対象物の前記取引の前記処理操作を実行するための少なくとも1つの予め定められた条件を含む、前記第1の台帳におけるスマートコントラクト、又は、処理条件レジストリに関連付けられてもよい。前記処理操作のための前記予め定められた条件は、例えば、前記それぞれの処理操作を実行するために前記対象物の占有を有していることを示した、特定の实体を示すデータ、及び/又は、前記処理操作の対象である前記対象物、及び/又は、そのタイプ/バッチの同一性を示すデータを含んでもよい。さらに、いくつかの場合では、前記予め定められた条件は、以下の1つ以上を含んでもよい。

20

- 前記処理操作を実行するために必要とされる環境/周囲条件
- 前記処理操作を実行するための位置条件
- 前記処理操作のための必須条件としての前記他の対象物の識別性

【0037】

いくつかの実施形態では、前記対象物処理管理モジュールは、少なくとも1つの予め定められた条件の実行条件を、前記処理操作に関連付けて、測定し、及び、したがって、前記対象物処理管理モジュールに、前記処理操作の前記実行パラメータを伝達するように構成され、また、動作可能な1つ以上の知覚システムに接続可能である。例えば、前記対象物処理管理モジュールは、前記対象物の特定のマーキングを読み取ることによって、前記対象物の識別するように適合された少なくとも1つの読取ユニットに接続可能であってもよい。前記1つ以上の知覚システムは、少なくとも1つの読取ユニットに関連付けられ(例えば、含まれ)ていてもよく、また、前記それぞれの処理操作の前記実行パラメータに関連付けられて、前記処理操作の前記実行条件を通信するように適合されてもよい。感知システムは、例えば、少なくとも1つのセンサ、及び、前記センサによって測定される実行データのパラメータを通信するための読出ユーティリティを含んでもよい。前記少なくとも1つのセンサは、例えば、温度センサ、湿度センサ、光センサ、位置センサ(例えば、GPS)、慣性センサ、及び、タイマ/タイミングセンサであってもよい。

30

【0038】

本発明のさらに別の広範な態様によれば、物理的な対象物の取引を管理する方法が提供される。前記方法は、物理的な対象物に関して実行される予定の1つ以上の処理操作のそれぞれ処理操作ごとに、第1の分散台帳に、その物理的な対象物に関する対象物取引を登録するために、以下のことを実行することを含む。

40

- 前記処理操作の測定された実行パラメータを判定し、それによって、前記測定された実行パラメータの判定は、前記処理操作を実行する实体に割り当てられた読取装置によって前記対象物のマーキング/署名を読み取り、
- 前記測定された実行パラメータを認証し、前記読取装置によって読み取られたマーキング/署名に基づいて、前記処理操作が実行された前記物理的な対象物を示すデータを判定し、及び、前記読取装置に関するデータに基づいて、前記処理操作を実行する前記实体を識別し、並びに、
- 前記認証された実行パラメータを利用して、第2の分散台帳における前記処理操作の登

50

録を妥当性検証し、それによって、認証された処理操作の分散台帳を提示すること。

【0039】

これにより、前記方法は、前記第2の分散台帳に認証された処理操作として、前記1つ以上の処理操作のそれぞれを登録する際に、前記第1の分散台帳における前記対象物取引の登録を妥当性確認できる。

【0040】

いくつかの実施形態では、前記方法は、さらに、前記処理操作の前記認証された実行パラメータが、前記対象物取引に必要とされ、及び、前記処理操作の対象となるように指定される、前記処理操作を実行するための少なくとも1つの主体、及び、指定された前記対象物の同一性、又は、タイプを示す予め定められた条件を満たすことを検証し、；前記検証は、；前記処理操作上の実際の対象物である前記対象物と、指定された対象物との間の一致を判定し、；及び、前記処理操作を実行する実際の実態と、指定された実態との間の一致を判定すること、を有している。

10

【0041】

いくつかの実施形態によれば、少なくとも1つの処理操作の前記測定された実行パラメータの判定は、さらに、前記読取ユニットに関連付けられたセンサからの追加の知覚データの計測を含む。；及び、前記検証は、さらに、前記感覚データと、前記予め定められた条件に含まれる追加の実行条件との間の一致を判定することを含む。

【0042】

いくつかの実施形態では、前記第2の台帳における前記処理操作の登録の妥当性検証は、前記処理操作の前記測定された実行パラメータが、前記予め定められた条件を満たすことの検証を含む。

20

【0043】

この目的のために、いくつかの実施形態では、前記第1の台帳への前記対象物取引の登録の妥当性検証は、前記対象物取引に関連付けられた前記1つ以上の処理操作のそれぞれ毎の前記測定された実行パラメータの検証を含んでもよい。

【0044】

上述したように、前記第1の台帳は、前記対象物取引を実行するためのスマートコントラクトを含むスマートコントラクト台帳であってもよい。いくつかの実施形態では、前記スマートコントラクトは、サブ取引を含み、それによって、1つ以上の前記サブ取引（例えば、選択的に、コンピュータ実行可能な、前記第1の台帳によって実行可能な、コード/スクリプトの形態であってもよい）は、前記1つ以上の処理操作に関連付けられ、及び、前記第2の台帳にアクセスするように適合され、及び、前記1つ以上の処理操作の前記認証された実行パラメータは、前記対象物取引に要求される前記予め定められた条件を満たす前記上述の検証を実行する。

30

【0045】

上述のように、いくつかの実施形態では、前記物理的な対象物は、識別可能なXRF署名/マーキングを有し、及び、前記マーキング/署名の読み取りは、前記対象物の前記XRF/署名を検出し、それによって、前記対象物のID、又は、タイプ、又は、バッチを判定できることを含む。前記XRF署名/マーキングは、前記対象物の要素であってもよく、また、前記対象物の1つ以上のパーツの材料組成に関連付けられていてもよく、したがって、前記対象物から分離できなくともよい。

40

【0046】

本発明のさらに別の広範な態様によれば、対象物の処理操作を監視し/測定するために独立して動作し、；前記処理操作を認証し、及び、前記認証された処理操作が予め定められた条件に一致することを、できる限り検証し、及び、前記認証され、及び、できる限りの検証もされた処理操作を、第2の台帳に登録する、ように構成され、動作可能である対象物署名読取装置（例えば、上記においても、読取装置、又は、読取ユニットとして参照されている）が提供される。前記対象物署名読取装置は、1つ以上のブロックチェーンシステムとデータ通信してもよく、及び、それによって、前記1つ以上のブロックチェーン

50

システムによって実行される第1の分散台帳における前記対象物取引の妥当性検証を可能にしてもよい。前記対象物署名読取装置は、：(a)前記物理的な対象物上のマーキング/署名を読み取り、前記マーキング/署名を示すデータを判定するように構成され、また、動作可能である署名/マーキング読取モジュール、(b)前記対象物署名読取装置を一意に識別する読取装置IDデータを搬送する識別モジュール、(c)前記対象物署名読取装置とデータ通信でき、1つ以上の物理的な対象物のマーキング/署名を示し、及び、前記読取装置IDデータに関連付けられた前記対象物署名読取装置を占有している実体を示す参照データにアクセスし、及び、前記1つ以上のブロックチェーンシステムと前記対象物署名読取装置との通信を可能にするネットワーク通信モジュール、及び、(d)前記署名/マーキング読取モジュールに、及び、前記通信モジュールに、接続可能な対象処理管理モジュール、を有する。前記対象処理管理モジュールは、以下を実行することによって、前記物理的な対象物に関して実行される少なくとも1つの処理操作の実行パラメータを認証するように構成され、また、動作可能であってもよい。

- 前記読取モジュールから得られた前記物理的な対象物の前記マーキング/署名のデータと前記参照データ内の1つ以上の物理的な対象物の前記マーキング/署名との間の一致を判断することによって、前記対象の物理的な対象物の同一性、又は、タイプ、又は、バッチを認証し、

- 前記対象物署名読取装置を識別する前記読取装置IDデータと、前記参照データにリストされている前記実体の識別との間の一致を判断することによって、前記対象物署名読取装置を占有する実体の同一性を認証し、

及び、それによって、前記処理操作を認証する。前記対象処理管理モジュールは、また、前記ネットワーク通信モジュールを動作させ、前記1つ以上のブロックチェーンシステムにアクセスし、及び、第2の分散台帳における前記認証された処理操作の登録を妥当性確認するように構成し、また、動作可能としてもよい。前記対象物署名読取装置は、前記第2の台帳におけるその対象物取引に関連付けられた処理操作の認証の妥当性確認の際に、前記第1の台帳に前記物理的な対象物に関連付けられた対象物取引を記録できる。

【0047】

いくつかの実施形態では、前記対象物署名読取装置の前記対象処理管理モジュールは、前記読取パラメータを示すデータを前記レンダリングモジュールに提供し、それによって、前記対象物のマーキング/署名を読み取ることによって、前記読取モジュールを認証し、前記物理的な対象物のマーキング/署名を読み取るように構成され、また、動作可能にしてもよい。前記読取モジュールは、前記読取パラメータに対応するある読取読スキームを動作させ、それによって、前記マーキング/署名を示す前記データを判定するように適合される。

【0048】

いくつかの実施形態では、前記対象物署名読取装置は、さらに、前記処理操作の予め定められた条件を示すデータを取得するように適合され、及び、前記認証された処理操作の前記実行パラメータが前記予め定められた条件に適合することを検証すると、前記第2の分散台帳における前記認証された処理操作の登録を妥当性検証できるように適合された前記条件検証モジュールを有する。

【0049】

いくつかの実施形態では、前記対象物署名読取装置は、さらに、前記対象処理管理モジュールに、又は、前記ネットワーク通信モジュールに、接続可能であり、及び、前記1つ以上のブロックチェーンシステムにおいて、少なくとも1つの予め定められたのトークン取引に対する前記処理操作を認証し/妥当性検証できるように構成され、また、動作可能であるトークン管理モジュールを有している。

【0050】

いくつかの実施形態では、前記物理的な対象物の署名/マーキングは、前記物理的な対象物に埋め込まれた要素XRF署名である。前記読取モジュールは、前記物理的な対象物のXRF測定を実行し、前記XRF署名/マーキングを読み取るように構成され、また、

10

20

30

40

50

動作可能な X R F 測定モジュールを有してもよい。例えば、前記読取モジュールは、前記対象物の少なくとも一部を、X線、又は、線で照射し、及び、前記 X R F 署名 / マーキングを示す X線 - 蛍光応答を検出することによって、X R F 測定を実行するように構成され、及び、動作可能であってもよい。

【 0 0 5 1 】

いくつかの実施形態では、前記参照データの少なくとも一部は、前記 1 つ以上のブロックチェーンシステムによって非集中の分散された方式で記憶され、及び、前記対象物署名読取装置の前記対象処理管理モジュールは、前記参照データの少なくとも一部を検索するための前記 1 つ以上のブロックチェーンシステムにアクセスするように構成される。

10

​

【 図面の簡単な説明 】

【 0 0 5 2 】

発明を実施するための最良の形態本明細書に開示され、実際に実施され得る方法を例示するために、本明細書に開示される主題をより良く理解するために、実施形態は、添付の図面を参照しながら、非限定的な例としてのみ説明される

【 0 0 5 3 】

【 図 1 】本発明の一実施形態によるシステム 1 0 0 を概略的に示すブロック図である。

【 図 2 A 】本発明の様々な実施形態に従って実行されてもよい様々なモジュールを有するシステム 1 0 0 の詳細を概略的に示すブロック図である。

20

【 図 2 B 】本発明の一実施形態による方法 2 0 0 のフローチャートである。

【 図 2 C 】統合対象物署名読取装置システムとして実行される本発明によるシステム 1 0 0 を概略的に示すブロック図である。

【 図 3 】本発明の追加の実施形態によるシステム 1 0 0 を概略的に示すブロック図である。

【 図 4 】本発明の追加の実施形態によるシステム 1 0 0 を概略的に示すブロック図である。

【 図 5 】本発明のさらに別の実施形態による方法 6 0 0 のフローチャートである。

【 図 6 】本発明のさらに別の実施形態によるシステム 1 0 0 を示すブロック図である。

30

【 発明の詳細な説明 】

【 0 0 5 4 】

【 実施例 1 】

【 0 0 5 5 】

本発明の取引、及び / 又は、スマートコントラクトを実施するシステム 1 0 0 の実施形態を図 1 に示す。図 1 は、ブロックチェーンシステム 5 0 0、管理モジュール 3 0、及び、オプションのトークン管理ツール 4 0 を有するシステムの一般的な構造の概略図である。

【 0 0 5 6 】

管理モジュール 3 0 (以下、管理システム / モジュール、及び / 又は、処理管理モジュールも、同じ意味で参照される) は、マークされた対象物上の物理的なマーキング (対象物の署名) を読み取ることができる、複数の読取ユニット R 1、R 2 から R n と通信する。選択的に、読取ユニットは、対象物のマーキングが読み取られ、及び、認証されたこと (例えば、追加的な安全層として) を検証するためのブロックチェーンシステム 5 0 0 と通信してもよい。

40

【 0 0 5 7 】

ブロックチェーンシステム 5 0 0 は、複数のデジタルウォレット D W 1、D W 2 から D W n に相互作用する。デジタルウォレットは、スマートフォン、P D A、P C、及び、サーバ等の任意のタイプのコンピューティングデバイス上で動作するソフトウェアとして実行されてもよい。デジタルウォレットは、また、ブロックチェーン 5 0 0 のノード上で動作してもよい。デジタルウォレット D W 1 から D W n は、また、管理システム 3 0、及び

50

、トークン管理ツール40と通信してもよい。

【0058】

管理システム30は、マークされた対象物上のマーキングを示す情報を記憶する参照データと関連付けられる。対象物上のマーキングは、マーキングが特定の対象物に関連付けられた署名として用いられてもよいように、対象物に対して一意（例えば、対象物の識別子を提示）であってもよい。或いは、マーキングは、複数の対象物に、例えば、同じバッチに属する対象物、又は、製品に、対応してもよい。

【0059】

加えて、管理システム30は、マークされた対象物のマーキングの測定（例えば、それらの特定の対象物、又は、タイプのマーキングを読み取るために用いられるスキームを読み取ること）を実行するために要求されるデータを保存してもよい。このタイプの情報は、選択的に、管理システム30からこのデータを受信した後にのみ、読取ユニットは、対象物のマーキングを読み取ることができるように、管理システム30によってのみ任意にアクセスされてもよい。管理システム30は、また、読取装置に関する付加的な情報を保存する参照データと関連付けられてもよい。例えば、読取装置が用いられた場所、及び、時刻、及び、日時、読取装置を識別するシリアル番号（読取装置のID）、及び、ID識別読取装置、及び/又は、読取装置を操作する人物/実態を保存する参照データであってもよい。

【0060】

本発明の様々な実施形態によれば、読取ユニット（以下、読取装置）によって読み取られる対象物のマーキングは、ホログラム、QRコード、UV、又は、IRタグ、RFIDタグ、及び、X線回折（XRD）、又は、X線蛍光（XRF）分析技術に基づくX線署名等の様々なマーキング方法のいずれかであってもよく、対象物に適用され、又は、埋め込まれ、及び、対象物に永久的、及び、物理的に関連付けられるように構成されてもよい。マーキングの用語は、対象物に適用され、結合され、取り付けられ、又は、印刷されるマーク/タグ、又は、対象物に埋め込まれた分離不可能なマーク/署名を指すように、ここでは広く理解されるべきである。また、ここで用いられるようなマーキングは、対象物を特徴付ける署名、又は、対象物を識別できるその材料、及び/又は、そのタイプ、及び/又は、その起源（例えば、元素的なマーキング/署名は、貴重な石、又は、ダイヤモンドを、しばしば、特徴づけるように）等のように、対象物に固有の/要素的なマーク、又は、対象物に追加/付加されたマークを参照してもよい。

【0061】

適切な対象物マーキングは、標準的に、又は、具体的に構成された読取ユニットを用いて読み取り可能であってもよく、及び、特定の走査/読取プロトコル、及び、パラメータを必要としてもよい。例えば、読取装置は、マークされた対象物から放射された電磁放射を検出し、識別できる分光計である。特に、読取装置は、一次電磁放射によるマークされた対象物の照射に応答して、マークされた対象物から放出された応答信号を識別してもよい。好適な例では、読取装置は、マークされた対象物に向けてX線、又は、γ線を放出し、結果としてマークされた対象物から到来する応答X線信号を検出するXRF分析器（特に、エネルギー分散型XRF分析器）である。XRF感受性マーキング（すなわち、XRF分析によって検出され得るマーキング）を読み取るために、読取装置は、所定の読み取りパラメータに従って調整されるべきである。これらのパラメータは、X線照射パラメータ（X線放出管の電流、及び、電圧）、入ってくる信号、又は、出力信号をフィルタリングするフィルタのタイプ、及び、読み取りの持続時間（すなわち、X線照射装置が対象物に向かって放射線を照射する時間の持続時間）を含む。設定され得る追加のパラメータは、本明細書に参考として援用される国際特許出願PCT/IL2017/051050に記載されているように、X線照射装置、検出装置、及び、マークされた対象物の間の距離、及び、角度を含む。対象物上のマーキングを読み取るために必要なパラメータは、管理システム104に保存され、及び、参照により本明細書に組み込まれる米国仮特許出願番号62/503,067に記載されているように、特定の対象物の読み取りを実行するこ

10

20

30

40

50

とを許可された特定の読取装置のみに提供されてもよい。

【0062】

本発明のシステム100の一態様では、対象物は、2つ以上のタイプのマーキングによってマークされてもよい。1つは、管理システム30からデータを受信した後に読み取られ、及び、1つ以上は、測定システムからの情報を必要とすることなく、適切な読取装置によって読み取られてもよい。例えば、対象物は、管理システムからデータを受信した後にのみ、マーキングを測定してもよい（及び、不可視であり、及び、適切な読取装置なしでは検出できない）XRF感受性マーキングとして、マークされてもよく、及び、可視であり、及び、任意のバーコード、又は、RQコードスキャナによって読み取られるバーコード、又は、QRコードによってマークされてもよい。

10

【0063】

本発明の一態様では、管理システム30は、それ自体のブロックチェーンシステム（以下、管理ブロックチェーンとしても参照される）として設計され、そこでは、対象物上のマーキングに関連するデータの多くのコピーが複数のノードに保存されてもよい。マーキングに関する保存されたデータ（例えば、以下に示される参照Obj'データ）は、署名、及び/又は、署名が読取ユニットによって読み取られる方法に関連するデータが保護されるように、暗号化されてもよい。一例では、マーキング管理システム30は、ブロックチェーンシステム500の一部を構成する管理ブロックチェーンとして実行されてもよい。この場合、管理システム30のノードは、残りのブロックチェーンシステムとは共有されない、保護されたデータ（例えば、対象物のマーキングに関するデータ）を保存し、管理するブロックチェーンシステム500の特権ノードとして機能してもよい。

20

【0064】

ブロックチェーンシステム500は、公共台帳として用いられてもよく、公共台帳は、所有権（及び/又は、占有権）、及び、当事者間の取引可能アイテム（ここでは、以降、互換的に、対象物、又は、資産としても言及される）のタイプ数の取引データを記録する。上述したように、当事者は、デジタルウォレットDW1からDWnを介してブロックチェーンシステム500に接続してもよい。このようなデジタルウォレットの各々は、取引可能な資産/対象物、又は、そのような資産の一部の所有権を証明するために使用できるデータ（例えば、公開鍵暗号化システムにおける秘密鍵）を有する。取引可能な資産は、1以上の(i)マークされた実体的な対象物、又は、そのような対象物の一部であってもよく、(ii)トークン管理ツール40によって管理された、ブロックチェーンシステム500に関連付けられたネイティブトークンであってもよいトークン、であってもよい。トークンは、サービス、又は、ユーティリティに関連する資産を表してもよい。例えば、トークンは、その所有者が、管理システム30の使用によって提供される、又は、管理システム30の使用を要求するサービスを使用できるようにしてもよい。特定の例では、トークンは、管理システム30のデータへのアクセスが許可されるデータ（例えば、デジタルウォレットに保存された1以上の秘密鍵のセット）であってもよい。他の例では、使用者は、トークンを用いて、読取装置を購入したり、借りたりしてもよく、又は、読取装置の使用を必要とするサービスのための支払いをしてもよい。

30

【0065】

トークン管理ツール40は、ブロックチェーンシステム500と管理システム30との間のインタフェースを制御し、及び、管理システム30によって記録されているデータ、又は、管理システム30によって取得され得るデータへのアクセスを提供し、又は、拒否する。加えて、読取ユニットの使用、及び、読取サービスが、管理システム30によって管理されている場合には、トークン管理ツール40は、読取ユニットへのアクセスを制御してもよい。例えば、トークン管理ツール40は、マーキング管理システム、及び/又は、読取ユニットを操作/に指示し、対象物が特定のコードによってマークされていることを検証する（すなわち、トークン所有者が検証のためにトークントークンを支払う）ために、トークン所有者（例えば、トークンを所有する実体）によって提供される要求に回答して動作するように適合されてもよい。他の例では、トークン管理ツール40は、そのよ

40

50

うなデータへの自由なアクセス、及び、取引のためのみのトークンの要求を許可し、そこでは、対象物の所有権は、1のユーザ（すなわち、デジタルウォレット）から転送される。各サービスのトークンの価格は、必要とされる特定のサービスに、並びに、追加の要因に、依存してもよい。

【0066】

本発明のいくつかの実施形態による、1つ以上の対象物{O1、O2}の対象物取引300を管理するための、本発明の実施形態に係るそれぞれのシステム、及び、方法のブロック図100、及び、フローチャート200である図2A、及び、図2Bを、同時に、参照する。ここでの開示から理解されるように、本発明に係るシステム100、及び、方法200は、実体/当事者間、例えば、E1からEF間、の物理的な対象物、例えば、O1、の取引管理に、特に、適しており、それによって、対象物取引は、例えば、ブロックチェーン500のような分散台帳プラットフォーム、例えば、10、上で、そのようなものとして、実行/登録されてもよい。例えば、対象物Oaの取引310は、実体EiのデジタルウォレットDWiから実体EfのデジタルウォレットDWfのObj1のレジストリの移転として、分散台帳10に示される。できる限り、トークンTK1（例えば、暗号通貨）の反対取引も、実体EfのデジタルウォレットDWfから実体EiのデジタルウォレットDWiへのトークンTK1の転送によって、図に示すように、分散台帳10に、（例えば、対象物取引310に関連付けて、）登録される。

10

【0067】

実際には、多くの場合、物理的な対象物の取引は、例えば、（例えば、当事者EiとEfとの間のサプライチェーンに沿った対象物O1の供給、及び/又は、製造/組み立て、及び/又は、梱包、及び/又は、アッセンブル、及び/又は、輸送、及び/又は、保存として提供する）人物/会社であってもよいE1からEnによって、実行される特定の処理操作、例えば、OP1からOPn、によって条件づけられる。したがって、物理的な対象物O1、及び、相手方トークン取引TK1の両方の分散台帳10におけるレジストリObj1、TK1は、対象物取引310の要求された処理操作OP1からOPnが、要求された処理条件310Cで満たされ/実行されるように（例えば、認証された実体によって、及び/又は、（十分な環境条件/位置等）予め定められた実行条件の下で、物理的な対象物O1に関するこれら操作を実行するように）、条件づけられてもよい。

20

【0068】

本発明のシステム100、及び、方法200は、仮想環境ブロックチェーン500と台帳10とをリンクする新規の技術を提供し、それによって、対象物の取引300は、対象物{例えば、O1、及び、O2}が、そのような取引の間、実際に、取り扱われる現実の/物理的な環境で、記録され、及び、そのような対象物取引300のために、対象物{例えば、O1、及び、O2}を用いて/に関して行われる処理操作の実行条件の容易な証明を促進し、及び、処理操作が、対象物取引の必須の条件に沿って、適切に実行されたことを、できる限り自動的に、検証する。

30

【0069】

したがって、本発明は、例えば、対象物のサプライチェーンの監視に適した新規な解決策を提供する。

40

【0070】

この点について、ここでは、「認証」、及び、同様の用語は、処理操作に含まれる/を実行する実際の実体{E1からEn}と同様に、実際の対象物{O1、O2}、又は、処理操作に含まれる実際の対象物のタイプ/ロット/バッチの識別/認証を指すことに、及び、できる限り、いくつかの実施形態では、いくつかの実行条件（例えば、環境/慣性条件、及び/又は、位置）、その実行条件で/その実行条件下で、処理操作が事項される、を判定することにも、用いられる。一般的に、認証は、読取ユニットRU、及び、できる限り、それによって関連付けられる追加のセンサの操作に、関連付けられ、それによって、処理操作の実行条件が測定/判定される（含まれる対象物、及び、実体、並びに、センサによって検知され得る可能性のある追加的な条件の同一性）。これを達成するために、

50

(例えば、追加のセンサ 4 1 1 M から 4 1 3 M を伴っても伴わなくても) 読取ユニットによって計測された実行条件が、読取ユニット R U によって、又は、対象処理管理モジュール 3 0 によって、参照データと比較され、以下に示すように、それらの間の一致は、処理条件の信頼性を示し、信頼性のある処理条件 4 1 1 A から 4 1 3 A をもたらす。認証操作自体は、読取ユニットによってのみ実行されてもよい。

【 0 0 7 1 】

ここでは、「妥当性確認する」、又は、「妥当性確認」等の用語は、ブロックチェーンにおける取引(認証された取引)の保存/登録/記録のための必要条件である、ブロックチェーンシステム内で用いられる操作を指すことに用いられる。当業者には理解されるように、ブロックチェーンシステムにおいて取引の登録/保存を要求する際に、要求された取引は、妥当性確認されるまで、及び、それに関する非集中のコンセンサスが得られるまで、保留中である(この点で、正式な「保留中状態」が存在せず、要求された取引は、一般的に、その妥当性確認に関する非集中のコンセンサスが、ブロックチェーンノードによって達成されるまで、登録されないことに留意すべきである)。このような妥当性確認の際に、「保留中」の取引は、有効な/有効にされた取引になり、及び、ブロックチェーンに、登録され、及び、保存される。この目的のために、「保留中」取引、及び、取引「要求」の用語は、ここでは、事前検証された取引を参照してもよく、及び、文脈に従って解釈されるべきである。この点について、ここで記述される第 1 の台帳 1 0 は、その妥当性確認が、対象物、対象物取引の主題に対して実行される特定の処理操作の発生に依存する対象物取引 3 0 0 を登録することに用いられることに注意すべきである。この目的のために、これらの対象物取引 3 0 0 (ここでは、一般に、取引としても参照される)は、典型的には、これらの取引に関連するか、又は、要求される処理操作の妥当性確認/検証まで、保留中の取引(未登録)の状態に保持される。対象物取引、例えば、3 1 0、は、各取引に関連付けられた全ての処理操作 O P 1 から O P 3 の第 2 の台帳 2 0 での妥当性確認の際に、及び、有効な処理操作 O P 1 から O P 3 が、取引 3 0 0 の処理条件要件 3 1 1 C から 3 1 3 C を満たすことの検証の際に、妥当性確認される。同様に、特定の対象物取引 3 1 0 の処理操作 O P 1 から O P 3 は、第 2 の台帳 2 0 において、取引、例えば、4 1 1 A 4 1 3 A によって、一般的に、提起される。処理操作 O P 1 から O P 3 は、それらのそれぞれの測定された実行条件 4 1 1 M から 4 1 3 M が、それぞれの認証された実行条件 4 1 1 A から 4 1 3 A を生成するシステム 1 0 0 によって認証されるまで、第 2 の台帳 2 0 において、保留中の取引のままであり、及び、選択的に、一実施形態では、それらは、さらに、認証された実行条件 4 1 1 A から 4 1 3 A が、それぞれの処理操作 O P 1 から O P 3 の必須の処理条件 3 1 1 C から 3 1 3 C と一致しているとして検証されるまで、保留中のままであると、考えられてもよい。そして、少なくとも認証された、及び、おそらくは検証もされた処理操作 O P 1 から O P 3 は、システム 1 0 0 によって妥当性確認され、及び、例えば、第 2 の台帳 2 0 に、登録される(例えば、認証された実行条件 4 1 1 A から 4 1 3 A の登録によって、図中に、例示される)。

【 0 0 7 2 】

ここでは、「検証する」、又は、「検証」等の用語は、各対象物取引、例えば、3 1 0、の処理操作の要求(必須の処理条件 3 1 1 C から 3 1 3 C)を満たす処理操作 O P 1 から O P 3 に含まれる実際の/認証された対象物 { O 1、及び、O 2 }、実際の/認証された実体 { E 1 から E 2 }、及び/又は、実際の実行条件を指すことに用いられる。このために、認証された処理操作 4 1 1 A の検証は、台帳 2 0 に、認証された処理操作 4 1 1 A に登録される前に、システム 1 0 0 によって実行されてもよく、その場合、認証された処理操作 4 1 1 A は、実際に、検証済み認証された処理操作 4 1 1 A を提示する。代替的に、認証された処理操作の検証は、システム 1 0 0、又は、台帳 1 0 のスマートコントラクト、又は、その他の実体のいずれかによって、台帳 2 0 への認証された処理操作 4 1 1 A の登録の後に、実行されてもよく、この場合、台帳 2 0 は、認証されるが、必ずしも検証されていない処理操作を提示する。上述したように、対象物取引、例えば、3 1 0、は、すべてのその処理操作の検証、及び、認証の際に、妥当性確認される。

【0073】

これを達成するために、システム100は、第1の分散台帳10に接続可能であり、第1の分散台帳10は、当事者{E_i、E_f}の間での、1つ以上の物理的な対象物{O₁、O₂}の取引に関連付けられた対象物取引300の取引(例えば、所有権/トークンの変化)を記録するように適合されている。システム100は、第2の分散台帳20を有している。第2の分散台帳20は、1つ以上の物理的な対象物{O₁、O₂}の対象物取引、例えば、310、に関して実行される対象物処理操作{OP₁からOP_n}を示すデータ(例えば、所有権、及び/又は、輸送/取扱/組み立ての条件の変化)を記録するように適合されている。典型的には、処理操作の認証されたレコードのみが、第2の分散台帳20に保存され、その結果、第2の分散台帳20は、対象物の取引300に関連付けられた処理操作{OP₁からOP_n}の実行パラメータの認証されたレジストリとして働いてもよい。システム100は、また、対象物処理管理モジュールを有し、対象物処理管理モジュール30は、1つ以上の物理的な対象物{OP₁、OP₂}に関して実行される処理操作{OP_iからOP_n}を、以下の手順、(i)前記処理操作{OP₁からOP_n}の実行パラメータ{411Mから413M}を取得し(例えば、1つ以上の条件を判定し、その際に、処理操作{411Mから413M}が実行され)、(ii)前記実行パラメータ{411Mから413M}を認証し、及び、(iii)処理操作{OP₁からOP_n}の前記実行パラメータ{411Mから413M}(又は、対応する実行パラメータ{411Aから413A}のみ)を、第2の台帳20に、記録すること、を実行することによって、認証するように構成され、及び、動作可能であってもよい。したがって、システム100は、1つ以上の物理的な対象物{OP₁、OP₂}に関して実行される処理操作{OP_iからOP_n}の認証された実行パラメータが1つ以上の予め定められた条件{311Cから313C}を満足することを検証する際に、1つ以上の物理的な対象物{O₁、O₂}に関連付けられた対象物取引300(例えば、所有権の変更)の検証、及び、記録を容易にする。

10

20

【0074】

図2Bを参照すると、対象物取引の検証に関する本発明の実施形態に係る方法200は図2Aに示されるモジュールに関連して記述されている。

【0075】

210において、ある対象物O₁の保留中の対象物取引310が提供されている。対象物取引310は、第1の台帳10への登録が保留されており、及び、取引300の登録のために実行される必要がある、その各処理操作、例えばOP₁からOP₃、の予め定められた条件311Cから313Cの実行の際に、登録される。保留中の対象物取引310は、例えば、スマートコントラクト310Sの形態であってもよいし、又は、予め定められた条件311Cから313Cは、ある処理条件データレジストリ310Cに見つけ出されてもよい。

30

【0076】

オプション215では、保留中の対象物取引310の処理操作OP₁からOP₃が、第2の台帳20に登録されるであろう保留中の処理取引として設定/検討される。例えば、保留中の対象物取引310が、スマートコントラクト310Sである場合には、保留中の対象物取引310は、第2の台帳20における未処理の対象物取引310の操作OP₁からOP₃の検証、及び、登録によって調整されるスマートコントラクト310Sのサブ取引(例えば、条件311Cから313Cを有してもよい)。

40

【0077】

操作220は、一般的に、処理操作を実行している実体、例えば、E₁からE_n、によって、典型的には、操作される本発明の読取ユニットRUによって実行され、及び、実体には、各読取ユニットが割り当てられている。例えば、処理操作OP₁の実行の際に、操作220において、測定された実行パラメータ411Mが取得され、そのことは、処理操作OP₁の目的である対象物O₁のマーキングM₁の読み取りを示す。測定された実行パラメータ411Mは、処理操作OP₁を実行する実体E₁に割り当てられる読取ユニット

50

、例えば、R 1、によって、取得され/読み取られ、及び、できる限り、各読取ユニット R 1に関連付けられてもよい追加のセンサ S 1から取得される追加のセンサデータも有する。

【0078】

操作230は、典型的には、対象処理管理モジュール30によって実行され、及び、測定された実行パラメータ411Mを認証し、測定された実行パラメータ(411Mに基づいて、処理操作OP1の対象である対象物O1と処理操作OP1を実行する実体E1との同一性を判定し、それによって、認証された実行パラメータ411Aを取得することを含む。

【0079】

そして、操作250は、典型的には、対象処理管理モジュール40、又は、各リーダユニットR1によって実行され、第2の台帳20における処理操作OP1の認証された実行パラメータ411Aの登録を妥当性検証する。

【0080】

252に示すように、本発明のいくつかの実施形態によれば、第2の台帳20は、認証された処理操作(必須ではないが、検証されたもの)を登録する。

【0081】

代替的に、オプション254に示されるように、第2の台帳20における処理操作OP1の妥当性検証は、さらに、処理操作OP1の認証された実行パラメータ411Aが、各処理操作OP1の予め定められた条件311Cを満たし/実行することを検証することを有する。このことは、例えば、以下に記述されるようなシステム100の条件検証モジュール50によって実行されてもよい。この場合、第2の台帳20は、認証され、及び、検証された処理操作を登録する。

【0082】

最後に、対象物取引310のすべての処理操作{OP1からOPn}が認証され、及び、検証された場合、又は、検証され得る場合に、第1の台帳10への保留中の対象物取引310の登録を妥当性検証するために、操作260が実行されてもよい。この点で、第2の台帳20が、認証されたが、必ずしも検証されていない処理操作を登録する(例えば、上述の252で説明したような)場合(例えば、上述の252で説明したような場合)、操作262が実行されてもよい。このような場合、対象物取引310の登録を妥当性検証することは、認証された実行パラメータ411Aから413Aが、保留中の対象物取引310のすべての処理操作OP1からOP3に関して、第2の台帳20に登録されていることを検証することと、及び、これらの認証された実行パラメータ411Aから413A、すべてが、対象物取引310に関するその各予め定められた条件311Cから313Cを満たすこと、を検証することとを有する。操作262は、例えば、以下に説明するように、システム100の条件検証モジュール50によって実行されてもよい。代替的に、操作264は、第2の台帳20が、認証、及び、検証の両方をされた処理操作を登録する(例えば、上述の254で説明したような)場合に、実行されてもよい。このような場合には、264において、第2の台帳20に、検証され、及び、認証されたすべての処理操作OP1からOP3を登録する際に、保留中の対象物取引310は、妥当性検証され、第1の台帳10に登録される。これは、例えば、第1の台帳10のスマートコントラクトによって実行されてもよい

【0083】

選択的に、操作240において、1つ以上の上記操作220、230、250(例えば、252、又は、254)、又は、260(例えば、262、又は、264)は、システム100を有する特定の1つ以上のブロックチェーンシステム500において(例えば、台帳10において)、予め定められたトークン取引が発生した際にのみ、実行されてもよい。このことは、システム100のトークン管理ツール40によって実行されてもよい。

【0084】

本発明の様々な実施形態による方法のさらなる詳細、及び、実行は、システム100を

10

20

30

40

50

参照しながら以下に説明される。当業者であれば、方法 200 における以下に説明される特徴をどのように実行するかを、容易に、理解するであろう。

【0085】

図 2A に戻って、第 1 の台帳 10 は、取引の条件 { 311C から 313C } が、認証された実行パラメータ { 411M から 413M } によって満たされていることの検証の際に、対象物取引、例えば、310、を、自動的に、記録するように構成され、及び、動作可能であってもよい。これに関連して、対象物取引 310 は、例えば、(i) 1 つ以上の対象物、例えば、O1、の所有権 Ob1 の取引、及び、(ii) 1 つ以上の対象物、例えば、O1、の所有権の変更に関連付けられたトークン Tk1 の取引、を有してもよい。

【0086】

例えば、第 1 の分散台帳 10 は、第 2 の分散台帳 20 へのアクセスを有するスマートコントラクト台帳 10S であってもよく、及び、物理的な対象物 O1 に関して実行される処理操作 OP1、OP2、OP3 の認証された実行パラメータ 411M、412M、又は、413M を取得するように適合され、及び、少なくとも 1 つの処理操作 (例えば、OP1、OP2、又は、OP3) が、その対象物の取引のための台帳 10S のスマートコントラクト 310S によって示される少なくとも 1 つの予め定められた条件 { 例えば、311C、312C、又は、313C } に準拠していることを判定する際に、第 1 の台帳 10 に、少なくとも 1 つの対象物 O1 の対象物取引 310 を記録してもよい。

【0087】

代替的に、又は、追加的に、システム 100 は、対象物 O1 に関して実行された処理操作 (例えば、OP1、OP2、OP3) の認証された実行パラメータ 411A、412A、又は、413A を取得し、認証された実行パラメータ 411A、412A、又は、413A を予め定められた条件 { 例えば、311C、312C、又は、313C } で検証 / 比較し、及び、この対象物取引 310 に関連付けられた全ての処理操作 (例えば、OP1 から OPn) のパラメータが、それぞれの予め定められた条件 { 例えば、311C、312C、又は、313C } に準拠していると判断する際に、第 1 の台帳 10 に、対象物 O1 の対象物取引 310 を記録 / 検証するように適合された条件検証モジュール 50 を有してもよい。

【0088】

分散台帳 10、及び、20 は、典型的には、1 つ以上のブロックチェーンシステム 500 で実行される。分散台帳 10、及び、20 を実行するブロックチェーンシステムは、接続されるノード / サーバ 511 から 515、及び、521 から 525 で例示される同じ (例えば、単一の) ブロックチェーンシステム 500 であってもよく、それによって、それぞれは、台帳 10、及び、20 の複製されたコピーを実行する。この点について、一部の実施形態では、分散台帳 10、及び、20 の両方のレコードは、同じブロックチェーン 500 のブロック内に、一緒に、書き込まれてもよい。

【0089】

代替的に、または追加的に、いくつかの実施形態では、分散台帳 10、及び、20 を実行するブロックチェーン 500 は、それぞれ、異なるブロックチェーン 519、及び、520 であり、そのことは、(第 1 の分散台帳 10 を実行している) ブロックチェーン 510 の接続されたノード / サーバ 511 から 515、及び、(第 2 の分散台帳 20 を実行している) ブロックチェーン 520 の接続されたノード / サーバ 521 から 525 によって、例示される。

【0090】

したがって、台帳 10、及び、20 が、ブロックチェーン (例えば、500、又は、510、及び、520) 上で実行されるように、台帳 10、及び、20 は、一般に、記録 / 取引の偽造に対する集中的な脆弱性を有しないか、又は、低減されている非集中の分散台帳である。これにより、システム 100 は、物理的な対象物の取引における使用に、特に、有利であり、その取引は、当然ながら、対象物の取引を取り扱う多数であるが、必ずしも信頼性が高くない実体を含んでおり (例えば、多くの場合、サプライチェーンを用いた

10

20

30

40

50

場合のように)、これは、単一の実体のみが、台帳へのデータの書き込み/記録に責任を有しているわけではないからである。この点に関し、ブロックチェーン、以降では、一般的に、500、のブロックへの書き込みに関連付けられた、いずれかの1つの台帳10、及び、20へのレコードの書き込みは、任意の適切なブロックチェーン技術に従って実施されてもよし、及び、適切なブロックチェーンプロトコル/技術(例えば、ブルーフ・オブ・ワーク+妥当性検証、又は、ブルーフ・オブ・ステーク)にしたがって、それぞれのブロックチェーンのノード間で「非集中の合意」を達成することを含むことを理解すべきである。システム100の特定の実行に応じて、台帳10、20、又は、両方を実行するブロックチェーン510、520、又は、500は、それぞれ、秘密、又は、公開のブロックチェーンであってもよく、及び、同じ、又は、異なるブロックチェーンプロトコル/技術で構成され、及び、動作可能であってもよい。

10

【0091】

本発明のいくつかの実施形態によれば、対象処理管理モジュール30は、ブロックチェーンシステム、500、又は、520、の特権PRノード(例えば、524、及び、525)を有してもよく、第2の分散台帳20内で処理操作(例えば、OP1、OP1、又は、OP3)の認証された実行パラメータ(411A、412A、又は、413A)を記録し/登録することを要求するように動作可能である。この目的を達成するために、前記ブロックチェーン500、又は、520そのような特権を有さないその他のノード(例えば、521から523)は、ブロックチェーン500、又は、520へのデータレコードの書き込みの開始/要求が許可されないようにしてもよい。

20

【0092】

本発明のいくつかの実施形態によれば、システム100は、また、トークン管理モジュール40を有し、トークン管理モジュール40は、第2の分散台帳20内の処理操作(例えば、OP1、OP1、又は、OP3)の認証された実行パラメータ(411A、412A、又は、413A)を、第2の分散台帳内に、書き込むこと(例えば、発行/登録)を、選択的に、許可したり、禁止したりし、又は、場合によっては、第2の分散台帳20への測定された実行パラメータ(例えば、411M、412M、又は、413M)の書き込みを、選択的に、許可したり、禁止したりするように、構成され、及び、動作可能である。この目的のために、トークン管理モジュール40は、システム100に関連付けられたブロックチェーンシステム500のうちの一つにおいて、トークンTOK予め定められた取引を示すデータTOKの受信にしたがって、任意の実行パラメータ、例えば、411M、又は、411A、の書き込み/発行/登録を、それぞれ、選択的に、可能にし/開始し、又は、禁止するように、構成され、及び、動作可能であってもよい。トークンTOKの必要とされる予め定められた取引は、特定の要求された実体(Ei、及び、Ef、又は、E1からEnの予め定められた実体)に関連付けられた取引であってもよく、及び、システム100を認証する信号として機能し、対応する処理操作、例えば、OP1の各測定/認証を実行してもよい。いくつかの実施形態では、処理操作OP1の測定/認証の許可/開始のために受信されるトークンTOKのプロパティ、又は、その実行パラメータ、例えば、411M、又は、411Aのいずれかのレジストリは、対応する対象物取引310に関連付けられたスマートコントラクト310S、又は、処理条件レジスタ310Cによって含められ/特定されてもよい。したがって、予め定められたトークンTOKを受け取る際に、トークン管理モジュール40は、対応する実行パラメータ、例えば、411M、又は、411A、の測定/認証、及び/又は、登録/記録を許可し/開始するようにしてもよい。

30

40

【0093】

この目的のために、システム100は、典型的には、ブロックチェーンシステム500(又は、少なくともその中で台帳20が実行されるもの、例えば、520)との通信を容易にするデータ/ネットワーク通信モジュール70を有している。トークン管理モジュール40は、データ/ネットワーク通信モジュール70に、例えば、その中の少なくとも一つのコンポーネント/スイッチ、例えば、70、72、74、又は、74に、接続されて

50

もよく、及び、データ/ネットワーク通信モジュール70を、特定のパラメータ、例えば、411M、又は、411Aの測定/認証、及び/又は、登録/記録を許可し/開始するために、又は、禁止するために、利用するように構成され、及び、動作可能である。代替的に又は、追加的に、対象処理管理モジュール30は、トークン管理モジュール40に接続されてもよく、及び、特定の実行パラメータ、例えば、411M、又は、411A、に関連して行われた測定/認証、及び/又は、登録/記録のいずれか1つの活動に優先して、トークン管理モジュール40から認証指示を要求し/受信するように適合されてもよい。

【0094】

この目的のために、対象処理管理モジュール30は、1つ以上の物理的な対象物O1、O2に関して実行される処理操作(例えば、OP1、OP1、又は、OP3)を認証するように適合されている。1つ以上の物理的な対象物O1、O2は、システム100に関連づけられた、又は、含まれる1つ以上の読取ユニットRUによって読み取りできる1つ以上のマーキングM1、M2によってマークされている。例えば、読取装置Ri、R1、R2、及び、Rfは、実体Ei、E1、E2、及び、Ef(例えば、ヒト/企業)に関連づけられるように、図2Aに示されている。対象処理管理モジュール30は、少なくとも1つの読取ユニット、例えばRiから、前記処理操作OP1に関連する読取ユニットR1によって読み取られる、対象物O1の特定のマーキングM1を示すデータを取得することによって、対象物、例えば、O1、の処理操作、例えば、OP1を認証するように適合されている。

【0095】

システム100は、(例えば、1つ以上のデータベース、クラウド・データ・ストレージを用いて、及び/又は、ブロックチェーン500の分散台帳において、実行されてもよい)参照データレジストリ60を有しても、又は、関連づけられてもよい。参照データは、一般に、以下を有している。

(a) システムの読取ユニットRi、R1、R2、R2、及び、Rfと、その読取装置を現在所有する実体Ei、E1、E2、及び、Efの識別子とを関連付けているデータを保存する実体-読取装置参照データERData。したがって、システム100、例えば、対象処理管理モジュール30、は、読取装置識別子R1id(即ち、各読取装置に割り当てられる特定の識別コード)と、各読取装置R1を有し/利用する実体E1(ヒト/企業/部門)のIDとを、テーブル1に示すように、容易に関連付けできる。

【0096】

【表1】

E-R-Data		
読取装置	実体	
R1id	E1のID	

【0097】

(b) システム100の読取ユニットRi、R1、R2、R2、及び、Rfによって容易に読み取りできる各マーキング、例えば、M1(例えば、好ましくは、要素XRFマーキング、又は、可能性のある他のマーキング/タグ)と関連づけられる各対象物、例えば、O1を示すIDデータ、例えば、O1idを保存する対象物参照データObj'Data。したがって、システム100、例えば、対象処理管理モジュール30、は、(例えば、いずれかの読取ユニットによって)対象物O1から読み取られるマーキング、例えば、M1と、対象物のID、例えば、O1idとを、容易に関連付けできる。実際に、いくつかの実施例では、象物参照データObj'Dataは、各/いくつかの対象物O1に関連して(例えば、各/いくつかの対象物マーキングであるマーキングM1に関連して)、適切に1つ以上の読取ユニットRi、R1、R2、及び、Rfを操作し、適切な読取スキ

10

20

30

40

50

ームを利用し、及び、対象物O1の各マーキングM1を正確に読み取るために要求される、特定の読取指示（読取スキーム/パラメータ）O1RDも保存する。このように、読取装置R1に読取スキームO1RDを提供することは、実際に、読取装置R1が、対象物のID O1idを読み取り/解読することを可能にし/認証する。この場合、対象物取引310の主題である対象物O1（又は、そのタイプ）を示すデータ（そのデータは、対象物取引300の処理条件レジスタ310Cから得ることができる）を与えられると、システム100、例えば、対象処理管理モジュール30、は、対象物参照データObj' Dataから、その対象物/対象物のタイプに関連付けられた適切な読取スキームO1RDを検索し、及び、同じものを、各読取装置、例えば、R1、に送信/通信し、読取装置R1によって対象物O1の特定を許可する。これは、例えば、テーブル2に示される。

10

【0098】

【表2】

Obj'-Data		
対象物/バッチ/タイプのID	マーキング	読取スキーム
O1id	M1	O1RD

【0099】

この点に関して、いくつかの実施形態では、対象物参照データObj' Dataは、分散台帳に（例えば、ブロックチェーン580に、又は、ブロックチェーン500の別の1つに）登録もされる点で有利であることに、留意すべきである。これは、マーキングが、対象物の材料の固有の部分であるXRF要素マーキングのような、容易に/実質的に偽造できない場合に、特に重要である。これは、一般的に、マーキングM1で対象物O1を所有している第1実体、例えば、Ei、が、対象物O1の原本性の観点で信頼できるものと見なされるからである。したがって、分散台帳/ブロックチェーン、例えば、580、にObj' Dataを配置することは、そのような実体が、最初に、対象物参照データObj' - DataにそのマーキングM1で登録でき、そのような参照データは、非集中であり、及び、分散されており、及び、実際に偽造されることがない。対象物の材料の一部としてのこのような要素マーキングは、多くの場合、対象物から、実際に、除去できないので、実際に、このことは、XRFのような要素マーキングにとっては、より重要である。この目的のために、システム10は、選択的に、分散マーキング台帳580の対象物参照データObj' - Dataを用いて、対象物のマーキング登録できるように構成され、及び、動作可能なマーキング管理モジュール80を有してもよい。マーキング管理モジュール80は、ブロックチェーンシステム500、又は、580の一部を構成する管理ブロックチェーンとして実行でき、及び、対象物参照データObj' - Dataを保存し、管理するための特権を有する、そのブロックチェーンシステム500、又は、580の特権ノードを有してもよい。選択的に、対象物参照データObj' - Dataは、また、ブロックチェーンシステム500の残りとは共有されることがない保護されたデータであってもよい。

20

30

40

【0100】

現在の開示において、ここで使用される用語「マーキング」は、対象物に関連付けられた任意のタイプのマーク/タグ、及び、署名に関連するように、広く解釈されるべきであることを理解すべきである。これらは、例えば、対象物上に印刷されたQRコード、対象物に付着され/結合されたRFIDタグ、同様に、XRFマーキング、及び、署名であってもよい。XRFについては、いくつかの対象物（例えば、ダイヤモンド、又は、他の貴重な石）は、対象物に実行される能動的なマーキング活動をすることなく、対象物の本来的なマーキングとして働く、強力に特徴付けるXRF署名を、本来的に、有しているだろう。代替的に、人造の対象物では、対象物をマーキングするXRF署名は、任意の適切な技術によって、対象物の材料にいくつかのXRF応答性材料組成物/混合物を含めること

50

によって、又は、その対象物をコーティングすることによって、人工的に製造されてもよい。

【0101】

この目的のために、目的の対象物O1の特定のマーキング（それは、追加されたマーク/コード、又は、タグ、又は、本来的な要素署名である）を識別し、特徴づけ、又は、適用する実体E_iは、分散マーキング台帳580にアクセスし、及び、そのマーキングM1で、及び、おそらくは、マーキングを読み取るための適切な読取スキームO1RDを用いて、対象物のIDO1idを登録してもよい。選択的に、いくつかの実施形態では、分散マーキング台帳580は、分散マーキング台帳580に対象物マーキングを登録するために特権を与えられ、及び、対象にされる実体にそのような登録サービスを提供するように構成され、及び、動作可能なマーキング管理モジュール80によって監視されてもよい。さらに、いくつかの実施形態では、実体-読取装置参照データE-R-Dataは、分散台帳に登録されてもよい。例えば、読取ユニット、例えば、R_i、R₁からR_n、及び、R_f自体、は、実体E_i、E₁からE₂、及び、E_fへの、又は、からのその対象物取引が、対象物O1に関して、ここで記述されたのと同様に、台帳10に登録され、及び、システム100によって管理される対象物とみなされてもよい。例えば、読取装置をリースすることを望む実体は、台帳10に登録される対象物取引、例えば、320、又は、（この場合、実際に、実体-読取装置参照データE-R-Dataを保存するであろう）同様のものを介して、そのように動いてもよい。

10

【0102】

本発明の様々な実施形態によれば、参照データ60が保存される方法にかかわらず、対象処理管理モジュール30は、データ参照データ60を用いて、対象物O1の処理操作OP1を認証し、処理操作OP1が、前記実体E1によって、認証された対象物O1に実行されることを検証するように適合される。これは、例えば、以下を有する。

20

i. 対象物の前記特定のマーキングM1を用いて、前記対象物O1のIDO1idを認証する。より詳細には、対象物O1のIDO1idを認証することは、読取ユニットR1から取得された対象物O1の特定のマーキングM1のデータと、対象物O1がマークされる前記特定のマーキングM1を示す予め保存された参照データObj'-Dataとの間の一致を判断することによって認証される、及び、

ii. 前記読取ユニットR1の認証するデータR1idを利用し、読取ユニットR1の所有権を有し、及び、前記処理操作OP1を実行する実体E1を認証する。

30

読取ユニットR1を所有している実体E1のIDは、前記読取ユニットを識別するデータR1idと、前記1つ以上の読取ユニット{R_i、R₁、R₂、R_f}を所有する各実体{E_i、E₁、E₂、E_f}に関連付けられた前記1つ以上の読取ユニット{R_i、R₁、R₂、R_f}のIDR_i、R₁、R₂、及び、R_fを列挙する参照データE-R-Dataとの間の一致を判断することによって、認証されてもよい。

【0103】

いくつかの実行形態では、読取ユニットR1の操作の前に、対象処理管理モジュール30は、読取ユニットR1を認証し、対象物O1の特定のマーキングM1を読み取り、及び/又は、そのことと言えば、読取ユニットR1を認証し、それぞれの処理操作、例えば、OP1、の実行パラメータ411Mの他のいずれかを取得/測定するように、適合されている。例えば、上述したように、一部の実施形態では、対象処理管理モジュール30は、前記特定のマーキングM1を読み取る読取パラメータO1RDを示すデータを、読取ユニットR1と通信することによって、読取ユニットR1を認証し、前記特定のマーキングM1を読み取る。次に、読取ユニットR1は、実行パラメータO1RDに対応する特定の読取スキームを操作し、及び、それによって、判断し、及び、対象物O1の特定のマーキングM1を示すデータを、前記対象処理管理モジュール30と、通信する。この場合、対象物IDの認証、及び、検証のステップは、同調して実行されるとみなされてもよい。これは、対象物取引300の主題である、申し立てられた対象物のIDが、取り扱われた/読み込まれたOaである実際の対象物と一致せず、次に、結果として、実際の対象物O1の

40

50

不正な読み込みとなる場合、読み取られる実際の対象物 O 1 の不正な読取パラメータ O 1 R D は、対象物取引 3 0 0 の処理条件レジスタ 3 1 0 C から取得されるからである。

【 0 1 0 4 】

本発明のいくつかの実施形態では、処理操作 O P 1 の認証は、前記対象物に実行される処理操作 O P 1 の検証の次に行われ、例えば、O 1 は前記実体 E 1 によって認証される。

【 0 1 0 5 】

例えば、第 1 の分散台帳は、対象物 O 1 の対象物取引 3 1 0 に関するスマートコントラクト 3 1 0 S を含むスマートコントラクト台帳 1 0 S であってもよい。スマートコントラクト 3 1 0 S は、対象物 O 1 の対象物取引 3 1 0 に関して実行される 1 つ以上の各処理操作 { O P 1、O P 1、O P 3 } の実行条件 { 3 1 1 C、3 1 2 C、3 1 3 C } を含む予め定められた条件 3 1 0 C を示している。したがって、処理操作 { O P 1、O P 1、O P 3 } を検証することは、処理操作 { O P 1、O P 1、O P 3 } が、実行条件 { 3 1 1 C、3 1 2 C、3 1 3 C } によって示される各実体 { E 1、E 2、E 2 } によって、実行されていること、及び、認証された実行パラメータ { 4 1 1 A、4 1 2 A、4 1 3 A } が実行条件 { 3 1 1 C、3 1 2 C、3 1 3 C } にも対応すること、を判断することにより、達成されてもよい。

10

【 0 1 0 6 】

本発明のいくつかの実施形態によれば、物理的な対象物 { O 1、O 2 } は、物理的な対象物 { O 1、O 2 } に適用され、又は、その内部に埋め込まれ、又は、それらに要素的 / 本来的であり、及び、それら物理的な対象物 { O 1、O 2 } の I D を示す物理的なマーキング { M 1、M 2 } によってマークされる。この目的のために、各物理的な対象物 { O 1、O 2 } の物理的なマーキング { M 1、M 2 } は、特定の物理的な対象物のそれぞれ { O 1、O 2 } を識別してもよい。代替的に、又は、追加的に、各物理的な対象物 { O 1、O 2 } の物理的なマーキング { M 1、M 2 } は、物理的な対象物それぞれのタイプ、又は、バッチを識別してもよい。そのような場合のいずれにおいても、マーキングは、ここでは、対象物を識別することは、特定の対象物を識別すること、又は、その単なるタイプ / バッチの識別することとしてみなされる。

20

【 0 1 0 7 】

いくつかの実施形態では、物理的なマーキング { M 1、M 2 } は、それぞれの物理的な対象物 { O 1、O 2 } の X R F 分析を介して識別できる X 線-蛍光 (X R F) 署名である。このような場合、読取ユニット { R i、R 1、R 2、R f } は、前記 { M 1、M 2 } において X R F 測定を実行し、X R F 署名を読み取るように構成され、及び、動作可能である。この目的のために、マーキング { M 1、M 2 } は、対象物の材料組成に関連付けられた、したがって、前記対象物 { O 1、O 2 } から分離できない対象物 { O 1、O 2 } の要素マーキングであってもよい。読取ユニット { R i、R 1、R 2、R f } は、線の X 線で、前記対象物 { O 1、O 2 } の少なくとも一部を照射し、及び、前記対象物 { O 1、O 2 } の X R F 署名を示す X 線-蛍光応答を検出することによって、X R F 測定を実行するように構成され、及び、動作可能であってもよい。システム 1 0 0 () 例えば、処理管理モジュール 3 0) は、対象物 { O 1、O 2 } の X R F 署名を処理し、前記マーキング { M 1、M 2 } を、それぞれに、判定するように構成され、及び、動作可能であってもよい。X R F 署名 / マーキングを識別するために、処理管理モジュール 3 0、及び / 又は、読取ユニット R U によって実施、及び / 又は、実行され得る技術の例は、例えば、本出願の譲受人に譲渡され、完全な参照により本明細書に組み込まれる、P C T 特許出願国際公開 W O 2 0 1 6 / 1 5 7 1 8 5、W O 2 0 1 7 / 2 2 1 2 4 6、及び、W O 2 0 1 8 / 0 5 1 3 5 3 に、詳細に、開示されている。この目的のために、いくつかの実施形態では、読取ユニット R U、又は、少なくともその読取モジュール (図 2 C の 9 0)、及び / 又は、処理管理モジュール 3 0 は、本発明にしたがって、対象物の X R F 署名 / マーキングを読み取り、及び / 又は、測定し、及び / 又は、処理し、及び / 又は、分析するために、それらの P C T 国際公開に記載されている 1 つ以上の技術を実施するように、構成され、及び、動作可能であってもよい。

30

40

50

【0108】

例えば、読取装置によって監視される処理操作は、以下1つ以上を有してもよいことに留意すべきである。

(i) OP1 - 対象物O1の所有権の変更。図2Aの例では、識別された対象物O1の所有権が、実体E_iから実体E₁に転送され、及び、所有権の変更は、この例では、実体E₁の読取装置R₁によって認証される。したがって、システム100は、実体E_iから実体E₁への対象物O1の所有権の変更を検証/認証する。

(ii) OP2 - 対象物O1の移送/保存。(例えば、図2Aの例では、対象物O1は、そして、(対象物O1の所有権も獲得する実体E₂によって)実体E₁から実体E₂に転送される。識別された対象物O1移送は、この例では、実体E₂の読取装置R₂の読み取りによって、検証/認証される。したがって、システム100は、E₁からE₂への所有権の変更と同様に、実体E₂が、移送/保存操作OP2を実行したことを、検証し/認証する。

(iii) OP3 - 対象物O1と他の対象物O2との組み立て。この例では、実体E₂は、対象物O1、及び、O2の組み立てにも注意している。識別された対象物O1と他の対象物との組み立ては、実体E₂の読取装置R₂の読み取りによって検証/認証される。この例のように、別の他の対象物O2もシステム100によって識別され得る場合、対象物O2の識別は、実体E₂の読取装置R₂によって検証/認証されてもよい。したがって、システム100は、実体E₂が、組み立て操作OP3を実行したことを検証/認証する。

【0109】

当業者には理解されるように、追加的な処理操作OP1からOP_n、又は、処理操作の他タイプは、対象物取引310の当事者である、最初の実体E₁と最後の実体E_fとの間で、対象物O1(及び、できる限り、追加的な対象物、例えば、対象物取引に沿ってO1と組み立てられ、又は、取り込まれるO2)の取引310に関して要求されてもよい。OP1からOP_nは、例えば、当事者E_i、及び、E_fの間の対象物O1の対象物取引310の実行に要求されるサプライチェーン操作を表してもよい。認証された/検証された操作OP1からOP_n(すなわち、その実行パラメータ、411Mから413M(例えば、各操作を実行する実体、及び、操作が実行される対象物、及び、できる限り、追加的なパラメータを示す)は、システム100によって読み取られ/測定される。

【0110】

対象物、及び、実体を、及び、できる限り、追加のセンサ、例えば、S₁からS₃、によって、検証するために用いられる読取ユニットRUは、追加的な実行パラメータ(例えば、操作が実行される地理的位置、動作の環境/慣性条件、及び/又は、操作に関連付けられる他の対象物/材料)を測定するために、各読取装置r₁からR₃、又は、各実体E₁からE₃に関連付けられてもよい。システム100、例えば、場合によっては、読取装置RU自体、又は、より一般的には、操作管理モジュール30は、前述のように、実行パラメータ411Mから413Mを認証するために、参照データ60にアクセスし、及び、認証された実行パラメータ411Aから413Aを判定するように適合される。これに関連して、「認証」は、処理操作OP1からOP_nを実施/実行する実際の実体E₁からE_n、及び、処理操作が実行される際の、実際の対象物O1、及び、できる限り、O2の識別子を少なくとも識別するために、読取装置Rから(及び、できる限り、センサからも)得られた測定/読み取りを比較/解析する、システム100の操作として、理解されるべきである。このような認証の際に、真正の実行パラメータは、例えば、411Aから413Aは、判断され、そこで、各処理操作OP1からOP3に含まれる実際の実体E₁からE_n、及び、実際の対象物O1、O2、及び、識別子は、できる限り、追加的なセンサの測定/データとともに、読取装置に関連付けられるであろう追加的なセンサS₁からS₃から、これらの操作の間に、取得されてもよい。

【0111】

認証された実行パラメータ411Aから413Aは、第2の分散台帳20に管理されている記録処理操作400のレジストリ410Rとして、各処理操作OP1からOP_nが実

10

20

30

40

50

行されるべき各対象物取引 3 1 0 に関連付けて登録され、及び、記録される 4 1 0。図 2 A の非限定的な例に示されるように、認証された実行パラメータ、例えば、4 1 1 A から 4 1 3 A、は、第 2 の台帳 2 0 に記録され（例えば、測定された実行パラメータ、例えば、4 1 1 M が実行される場合）、及び、そして、結果として得られる各認証された実行パラメータ 4 1 1 A は、第 2 の台帳 2 0 に記録される。また、いくつかの代替的な実施形態では、生の / 測定された実行パラメータ 4 1 1 M から 4 1 3 M は、まず、第 2 の分散台帳 2 0 に記録され、及び、その後、上記の認証が、（例えば、処理操作が、各対象物取引 3 1 0 に要求される予め定められた処理条件 { 3 1 1 C から 3 1 3 C } を満たすことの検証と同時に）実行されてもよい。

【 0 1 1 2 】

当業者には容易に理解されるように、第 2 の分散台帳 2 0 は、ブロックチェーンシステム 5 2 0、又は、5 0 0 のノード（例えば、サーバ）、5 2 1 から 5 2 5、及び、できる限り、5 1 1 から 5 1 5、で、実行されてもよい。認証された実行パラメータ 4 1 1 A から 4 1 3 A の記録を実行するシステム 1 0 0、例えば、処理管理モジュール 3 0 は、ブロックチェーンシステム 5 2 0、又は、5 0 0 の、排他的に、第 2 の分散台帳 2 0 にレコードを書き込み / 保存し / 変更することを禁止される特定の特権ノード 5 2 4、及び、5 2 5、と関連付けられてもよい。したがって、ブロックチェーンシステム 5 2 0、及び、5 0 0 の他のノードは、実行パラメータ、例えば 4 1 1 A から 4 1 3 A を読み取るのみであってもよいので、分散台帳の記録実行パラメータは本物であると、信頼されてもよい。この目的のために、いくつかの実施形態では、第 2 の分散台帳 2 0 を実行するブロックチェーンシステム 5 2 0、又は、5 0 0 は、オープンシステムであって、任意の関心のある当事者、例えば、E i、E 1 から E n、E f、又は、他の当事者にアクセスし、第 2 の分散台帳 2 0 に登録されている実行パラメータ 4 1 1 A から 4 1 3 A を読み出すことを可能にしてもよい。他の当事者は、任意の他のエンティティ、又は、他のブロックチェーンシステム、例えば、対象物の対象物取引が登録されている第 1 の分散台帳 1 0（スマートコントラクト台帳であってもよい）を実行するブロックチェーンシステム 5 1 0、であってもよい。いくつかの実施形態では、第 2 の分散台帳 2 0 を実行するブロックチェーンシステム 5 2 0、又は、5 0 0 は、クローズドシステムであって、第 2 の分散台帳 2 0 の選択された当事者のメンバ、例えば、E i、E 1、E n、及び / 又は、5 1 0 にのみアクセスし

、第 2 の分散台帳 2 0 に登録されている実行パラメータ、例えば、4 1 1 A から 4 1 3 A を読み出すことを可能にしてもよい。選択された当事者は、例えば、各対象物取引 3 1 0 の当事者 E i、E f、及び / 又は、対象物の取引が登録 / 実行される第 1 の分散台帳 1 0（スマートコントラクト台帳であってもよい）を実行するブロックチェーンシステム 5 1 0 であってもよい。このことは、関連する当事者は、各対象物取引 3 1 0 に関連付けられた記録処理操作 4 1 0 の台帳 2 0 のレジストリ 4 1 0 R にアクセスして、彼らが、対象物取引の処理操作の実行パラメータ 4 1 1 A から 4 1 3 A が取引条件 3 1 0 C を満たすことを検証できることを許可する。

【 0 1 1 3 】

これに関連して、本発明のいくつかの実施形態では、システム 1 0 0 は、対象物取引、例えば、3 1 0、の処理条件 3 1 1 C から 3 1 3 C が記録されている処理条件レジスタ 3 1 0 C に関連付けられている選択的な検証モジュール 5 0 を有している。検証モジュール 5 0 は、処理条件レジスタ 3 1 0 C からこれらの処理条件 3 1 1 C から 3 1 3 C を検索し、各対象物取引 3 1 0 の処理条件が満たされたか否かを検証するために、これらと、システム 1 0 0 によって取得された（例えば、第 2 の分散台帳に記録された、又は、対象処理管理モジュール 3 0 によって判断された）各認証された実行パラメータ 4 1 1 A から 4 1 3 A と、を比較するように構成され、及び、動作可能である。

【 0 1 1 4 】

代替的に、又は、追加的に、許可された関心のある当事者、例えば、E i、E f は、自ら、第 2 の分散台帳 2 0 に記録されている認証された実行パラメータ 4 1 1 A から 4 1 3

10

20

30

40

50

A にアクセスし / を要求し、各対象物取引 3 1 0 の処理条件が満たされているか否かを検証するようにしてもよい。

【 0 1 1 5 】

さらに、代替的に、又は、追加的に、第 1 の分散台帳 1 0 は、認証された実行パラメータ 4 1 1 A から 4 1 3 A が記録され、例えば、第 2 の分散台帳 2 0 へのアクセスを得ることができてもよいスマートコントラクト台帳 1 0 S として実行されてもよい。スマートコントラクト台帳 1 0 S (例えば、「イーサリアム」ブロックチェーンの台帳) は、例えば、対象物取引 3 1 0 を実行するためのスマートコントラクト 3 1 0 S を有してもよく、これによって、対象物取引 3 1 0 のための処理条件レジスタ 3 1 0 C は、この場合、スマートコントラクト 3 1 0 S 自体に含まれてもよい。この場合、対象物取引、例えば、3 1 0 の処理条件 3 1 1 C から 3 1 3 C、は、スマートコントラクト 3 1 0 S のレコード (例えば、スクリプト、又は、コンピュータ実行可能なコード) として提示されてもよく、第 1 の分散台帳 1 0 におけるそれらの各実行によって、第 2 の台帳 2 0 から、認証された実行パラメータ 4 1 1 A から 4 1 3 A の各レコードを検索し / 読み出し、各処理条件 3 1 1 C から 3 1 3 C と、対応する認証された実行パラメータ 4 1 1 A から 4 1 3 A とを比較し、及び、スマートコントラクト 3 1 0 S の各処理条件 3 1 1 C から 3 1 3 C が、例えば、第 2 の台帳 2 0 からの各認証された実行パラメータ 4 1 1 A の読取を開始する、スマートコントラクト 3 1 0 S の処理条件 3 1 1 C に対応する / を表す実行可能なコード / スクリプトを満たすか否かを判断し、及び、処理条件 3 1 1 C のコード / スクリプトによって、認証された実行パラメータ 4 1 1 A を処理し、認証された実行パラメータ 4 1 1 A が、その各スクリプト / コードによって指定されるような処理条件 3 1 1 C の要求を満たすか否かを判断する。そのようにすることによって、スマートコントラクト 3 1 0 S の各処理条件 3 1 1 C から 3 1 3 C 毎に、台帳 1 0 のスマートコントラクト 3 1 0 S は、システム 1 0 0 の第 2 の台帳 2 0 を用い、自動的に、対象物取引 3 1 0 の条件が、対象物取引 3 1 0 の対象である物理的な対象物、例えば、O 1、及び、できる限り、O 2 も、に関して、満たされているか / 実行されているかを検証できる。

10

20

【 0 1 1 6 】

したがって、システムに関連付けられるスマートコントラクト 3 1 0 S、又は、処理条件レジスタ 3 1 0 C は、対象物 O 1 の対象物取引 3 1 0 の前記処理操作、例えば、O P 1 から O P 3 を実行するための少なくとも 1 つの予め定められた条件を有してもよい。処理操作実行するための予め定められた条件 3 1 1 C から 3 1 3 C は、各処理操作 O P 1 から O P 3 を実行するために、対象物 O 1 の所有権を有していると示された特定の实体を示してもよい。選択的に、各処理操作 O P 1 から O P 3 に関連して指定される、少なくとも 1 つの予め定められた条件、例えば、3 1 1 C から 3 1 3 C、は、さらに、以下の 1 つ以上を有してもよい。

30

- 取り扱い操作を実施するために必要とされる環境 / 周囲条件 (例えば、温度、湿度、照明条件、圧力、及び / 又は、慣性条件)。例えば、X R F センサ / 読取装置を介した、これらの条件のいくつかの監視、及び / 又は、対象物 O 1 に対するそれらの効果は、例えば、本出願の譲受人に譲渡され、参照により本明細書に組み込まれる W O 2 0 1 8 / 0 5 5 6 2 5 に記載されている。

40

- 前記処理操作を実行するための位置条件 (例えば、許容される地理的座標 / 場所)
 - 対象物取引 3 1 0 の条件下、対象物 O 1 と組み立てられるべき他の対象物、例えば、O 2、の識別。例えば、識別は、他の対象物 O 2 の X R F マーキングを介するものであり、及び、例えば、本出願の譲受人に譲渡され、参照により本明細書に組み込まれる W O 2 0 1 7 / 1 7 5 2 1 9 に記載されているように、必須の処理操作のように、対象物と他の対象物とのペアリングを介するものであってもよい。

【 0 1 1 7 】

実際に、これらの条件を監視することは、実体間の対象物 O 1 の所有権の移転などの処理操作 (例えば、O P 2) に関連してもよく、及び、対象物 O 1 の保存、又は、移送に関連付けられた他の操作に関して / 又は、操作において、及び / 又は、できる限り、対象物

50

01と他の対象物02との組み立てにおいても、要求されてもよい。

【0118】

これに関連して、対象処理管理モジュール30は、(各読取装置R1、R2、R3に含まれても、又は、関連付けられてもよい)1つ以上のセンサシステム(例えば、センサ)、S1、S2、S3に接続できてもよい。センサシステムS1、S2、S3は、処理操作OP1からOP3に関して、少なくとも1つの予め定められた条件311Cから313Cの実行条件を測定し、及び、したがって、処理操作OP1からOP3の実行パラメータ411Mから413Mを伴うこれらの実行条件を、対象処理管理モジュール30に通信するように構成され、及び、動作可能である。よって、読取ユニット、例えば、R1、R2、及び、R3に接続できる対象処理管理モジュール30は、(対象物01の特定のマーキングM1を読み取ることによって)対象物01を識別するように適合され、及び、1つ以上のセンサシステムS1、S2、S3は、読取ユニット、R1、R2、及び、R3に関連付けられ、及び、(読取ユニットによって読み取られる対象物01の識別とともに)各処理操作、例えば、OP1からOP3の実行条件を通信するように適合される。

10

【0119】

これに関連して、読取ユニット、例えば、R1、R2、R3は、適切なマーキング読取装置(例えば、XRFリーダ、QRコードリーダ、RFIDリーダ、及び、ライン)、読取装置の識別子R1idを搬送する識別モジュールメモリ、及び、読取装置の識別子R1id、及び、対象処理管理モジュール30に読み取られるマーキングM1を示すデータ01idを通信するための読み出しユーティリティを有してもよい。センサシステム(例えば、センサ)S1、S2、S3は、上述の少なくとも1つのセンサS1、S2、及び/又は、S3、及び、センサによって測定された実行データのパラメータを、対象処理管理モジュール30に通信するための読み出しユーティリティを有してもよい。少なくとも1つのセンサS1、S2、及び/又は、S3は、以下の少なくとも1つを有してもよい:温度センサ、湿度センサ、光センサ、位置センサ(例えば、GPS)、及び、慣性センサ。いくつかの実施形態では、読取ユニット、及び、センサシステムは、上述したように、追加の実行パラメータの検知と同様に、対象物のマーキングの読み取りの両方をできる1つのシステム/モジュールに結合されている。

20

【0120】

独立した、一体型(自立型)の対象物署名読取システム(例えば、上記の読取装置、又は、読取ユニットとも参照される)として構成された、本発明の実施形態にしたがうシステム100のブロック図である図2Cを参照する。本実施例の対象物署名読取システム100は、対象物の処理操作を監視/測定し、処理操作を認証し、及び、できる限り、認証する処理操作が予め定められた条件を満たしていることを検証し、及び、認証され、及び、できる限り、検証もされた処理操作を第2の台帳20に登録するために、独立して、動作するように構成され、及び、動作可能である。対象物署名読取装置は、1つ以上のブロックチェーンシステム500、及び、選択的に、デジタルウォレットDWSを有するブロックチェーンネットワーク501とデータ通信できてもよく、及び、それによって、1つ以上のブロックチェーンシステム500によって実行される第1の分散台帳10において対象物取引を検証できてもよい。この点に関して、対象物署名読取システム100は、ブロックチェーンシステム500のノード/サーバ(図示せず)との直接通信を介して、又は、ブロックチェーンシステム500のノード/サーバと、順次、通信するデジタルウォレットDWSとの間接通信を介して、処理操作、及び/又は、対象物取引を検証するために、ブロックチェーンシステム500と通信するように構成され、及び、動作可能であってもよいことに、注意すべきである。

30

40

【0121】

対象物署名読取装置100は、一体的に(例えば、1つの装置に)、以下を有する:
 (a)物理的な対象物01のマーキング/署名を読み取り、マーキング/署名を示すデータを判定するように構成され、及び、動作可能な署名/マーキング読取モジュールR、
 (b)対象物署名読取装置100を一意に識別する読取装置IDデータを搬送する識別モ

50

ジュール 90 (例えば、内部メモリ/保存モジュール)、

(c) 対象物署名読取装置 100 のデータ通信を提供し、参照データ 60 にアクセスするように構成され、及び、動作可能なネットワーク通信モジュール 70。参照データは、1 つ以上の物理的な対象物、例えば、01、及び、読取装置 ID データに関連付けられる対象物署名読取装置 100 の所有権を有する特定の实体を示す。ネットワーク通信モジュール 70 は、また、対象物署名読取装置 100 と、ブロックチェーンネットワーク 501、例えば、1 つ以上のブロックチェーンシステム 500、又は、それに関連付けられるとデジタルウォレット DWS、との間のデータ通信を提供するように構成され、及び、動作可能である。

(d) 署名/マーキング読取モジュール R、及び、通信モジュール 70 に接続される対象処理管理モジュール 30。対象処理管理モジュール 30 は、以下を実行することによって、物理的な対象物 01 に関して実行される少なくとも 1 つ以上の処理操作の実行パラメータを認証するために、上述したように、同様に、構成され、及び、動作可能であってもよい：

- 読み取りモジュール R から取得された物理的な対象物 01 のマーキング/署名のデータと、参照データ 60 によって保存される 1 つ以上の物理的な対象物のマーキング/署名との間の一致を判定することによって、物理的な対象物 01 の ID、又は、タイプ、又は、バッチを認証すること、
- 対象署名読取装置 100 を識別する読取装置 ID データ 90 と、参照データ 60 にリストされる実体の ID との一致を判定することにより、対象物署名読取装置 100 を所有している実体の ID を認証すること。

【0122】

対象処理管理モジュール 30 は、また、ネットワーク通信モジュール 70 を操作して、(例えば、ブロックチェーンネットワーク 501 を介して)、1 つ以上のブロックチェーンシステム 500 にアクセスし、及び、第 2 の分散台帳 20 における認証された処理操作の登録を妥当性検証するように構成され、及び、動作可能であってもよい。したがって、対象物署名読取装置 100 は、第 2 の台帳 20 におけるその対象取引と関連付けられた認証された処理操作の妥当性検証の際に、第 1 の台帳 10 に物理的な対象物 01 に関連付けられた対象取引を記録できる。

【0123】

最適には、対象処理管理モジュール 30 は、読取モジュール R を認証し、物理的な対象物 01 のマーキング/署名を読み取るように適合されている。このような認証は、上述のように、読取パラメータを示すデータを読取モジュール R 1 に提供し、それによって、特定の対象物 01 のマーキング/署名を読み取ることによって、実行されてもよい。次に、読取モジュールは、読取パラメータに対応する特定の読取スキームを動作し、及び、それによって、特定の対象物 01 のマーキング/署名を示すデータを判定するように適合されてもよい。

【0124】

選択的に、対象署名読取装置 100 は、また、上述したように、処理操作の予め定められた条件を示すデータを取得し、及び、認証された処理操作の実行パラメータが、予め定められた条件に適合することを検証する際にのみ、第 2 の分散台帳への認証された処理操作の登録を妥当性検証するように適合されてもよい条件検証モジュール 50 を有している。

【0125】

選択的に、対象物署名読取装置 100 は、また、上述したように、対象物処理管理モジュール 30、又は、ネットワーク通信モジュール 70 に接続可能であり、及び、1 つ以上のブロックチェーンシステムにおける少なくとも 1 つの予め定められた取引の際に、処理操作を認証/検証できるように構成され、及び、動作可能である、トークン管理モジュール 40 を有している。

【0126】

10

20

30

40

50

選択的に、対象署名読取装置 100 は、物理的なオブジェクト 01 に関して埋め込まれた要素 XRF 署名を読み取り / 認識するように構成され、及び、動作可能である。そのような実施形態では、読取モジュールは、物理的な対象物の XRF 測定を実行し、(例えば、前記対象物の少なくとも一部を X 線、又は、線で照明し、及び、前記 XRF 署名 / マーキングを示す X 線 - 蛍光応答を検出し、及び、選択的に、前記応答についての分光分析を実行することによって) XRF 署名 / マーキングを読み取るように構成され、及び、動作可能である XRF 測定モジュール (図示せず) を有してもよい。

【0127】

場合によっては、対象物署名読取装置 100 は、また、処理操作が実行されるときに存在する 1 つ以上の実行条件 (例えば、上述のような、環境 / 周囲条件、位置、タイミング、及び / 又は、慣性条件) を測定するように構成され、及び、動作可能な 1 つ以上のセンサを有している。これらは、認証された処理操作に関連付けて、第 2 の台帳 20 に、(例えば、対象処理管理モジュール 30 によって) 登録されてもよく、及び、処理操作が、第 1 の台帳 10 の対象物取引の予め定められた条件を満たしていることを検証するために用いられてもよい。

10

【0128】

選択的に、参照データ 60 の少なくとも一部、又は、処理操作を認証するために対象物署名読取装置 100 によって使用される全ての参照データ 60 は、1 つ以上のブロックチェーンシステム 500 によって、非集中の分散された方式で保存されることに留意すべきである。この目的のために、対象処理管理モジュール 30 は、対象物の処理操作を認証するために必要とされる参照データ 60 の少なくとも必要とされる部分を検索するために、1 つ以上のブロックチェーンシステム 500 に、直接的に、又は、は間接的に、アクセスするように適合されてもよい。

20

【0129】

この目的のために、(いずれの集中型サーバ / サーバ、又は、モジュールに関連付けられていない) 独立型 / 統合型の対象物署名読取装置としてのシステム 100、及び / 又は、ブロックチェーンの非集中でされた方式での処理操作の認証、及び、物理的な対象物 01 から分離できない要素マーキング / 署名の使用のために使用される参照データ 60 のストレージ (システム) の構成は、実質的に、偽造可能でなく、又は、偽造されない堅牢な処理操作認証技術を、一緒に、提供する。さらに、第 2 の分散台帳 20 への認証された処理操作の登録は、一方では、任意の関心のある当事者、例えば、デジタルウォレット、又は、実体が、処理操作が対象物取引に関連付けられたならば、認証されたデータにアクセスできるようにしてもよく、他方で、実質的に、偽造できず、よって、物理的な対象物に関連する対象物取引の登録のために要求される認証された処理操作の発生を検証する堅牢な方法を容易にする。

30

【0130】

したがって、図 2 C のシステム 100 は、物理的な対象物に、それによって実行される処理操作を認証し、及び、台帳 20 に同じものを記録するために、他の実態から、又は、集中型のサーバ / 実態から、独立に、このようなシステムを利用できる、様々な独立した実体に、サプライチェーンに沿って、提供されてもよい。

40

【0131】

図 2 C のシステム 100 の更なる詳細、及び、実行は、当業者には理解されるように、図 2 A のシステムを参照して記述されたものと同様であっても、部分的には、そのようなシステムを一体化するための適切な変更を伴ってもよいことを理解すべきである。

【0132】

本発明のシステムの他の実施形態が、スマートコントラクトを実施するための本発明の特定の実施形態にしたがうシステム 100 の一般的な構造の概略図である図 3 に示される。同様の参照番号は、同様の要素モジュール、又は、システム、又は、モジュール、又は、本発明の異なる実施形態において同様の機能を有するシステムを指定するために、本出願の全ての図面に用いられる。

50

【0133】

図3のシステム100は、図1、及び、2Aの管理システムと同様の管理システム30、選択的なトークン管理ツール40、及び、複数のブロックチェーンシステムBC1、BC2からBCnを有している。管理システム30は、図1、又は、2Aの読取装置R1からRnと同様である複数の読取ユニットR1、R2からRnと通信する。各ブロックチェーンシステムBC1からBCnは、図1、及び、2Aを参照して上述したデジタルウォレットDW1、DW2からDWnと同様であってもよい複数のデジタルウォレット（図3には詳細に示されていない）と相互作用する。トークン管理ツール40は、ブロックチェーンシステムBC1からBCnと相互作用し、すなわち、トークン管理システムは、管理システム30によって提供される（例えば、マークされた対象物のマーキングを読み取るために必要とされる）管理システム、及び/又は、サービスによって保存されるデータにアクセスできる。ブロックチェーンシステムBC1からBCnの一部、又は、全部は、（例えば、10として上述で参照される）第1の台帳を実行してもよく、及び、対応するネイティブトークン/（そのネイティブトークンを伴う各ブロックチェーンである）通貨の所有、及び、取引の記録を管理してもよい。例えば、トークン管理システム40は、これらのネイティブトークンのいずれかに実行されてもよい（各ブロックチェーンに関連付けられる予め選択されるデジタルウォレットでなされる）支払いに応じて、アクセスできてよい。1つ以上のブロックチェーンシステムBC1からBCnは、（そのネイティブトークンに加えて）マークされた対象物を含む記録、及び、取引を管理してもよい。

10

【0134】

本発明のシステム100は、マークされた対象物を含んでも含まなくてもよい、様々なタイプのスマートコントラクトを実行してもよい。例えば、本発明のシステムは、一般的なスクリプト言語を提供するイーサリアムブロックチェーンのようなプラットフォームによって実行されてもよい。加えて、トークン管理ツールを用いることによって、本発明は、マークされた対象物を含むか、又は、管理システムからのデータの抽出を含むスマートコントラクトの実行できてよい。

20

【0135】

操作の第1のタイプは、ブロックチェーンシステム上のマークされた対象物の記録の登録/作成であり、すなわち、マークされた対象物が、例えば、公開鍵によって識別される特定の当事者（デジタルウォレット）に属するとして記録されることである。このタイプの操作は、トークンの量の転送（すなわち、操作は、トークンの支払いを必要とする）に条件付けられてもよい。

30

【0136】

本発明のシステム100によって実行されてもよいスマートコントラクトのタイプは、マークされる対象物が特定の署名、又は、コードによってマークされていることの検証に条件付けられている、マークされた対象物の所有権の変更である。例えば、所有権を受け取る当事者は、対象物が特定のマーキングを有しているか否か（例えば、このようなマーキングは、製造過程において、対象物に適用されてもよい）をチェックすることによって、対象物が本物であることの検証を望んでもよい。

40

【0137】

例として、対象物上の署名の読み取りは、正しい署名が識別された場合にのみスマートコントラクトが実行される初期段階で実行される。代替的に、署名は、所有権を受け取る当事者が、対象物が真正であることを検証する取引の最終段階でのみ読み取られてもよい。さらに別の例では、対象物上の署名は、例えば、正しい署名を検索することが、スマートコントラクトの次の段階を実行するための条件である初期段階、及び、取引を確定する最終段階の両方で、複数回、読み取られる。

【0138】

本発明に係るスマートコントラクトを実行するシステム100の概略図である図4を参照する。

【0139】

50

マークされた対象物の新しい記録を作成する際に、対象物を所有する当事者 E i (例えば、対象物の製造者) が対象物をマークし、及び、システムに対象物の記録、すなわち、管理システムにおけるマーキングに対応する記録、及び、ブロックチェーンシステムにおけるその所有権の記録、を創ることを望んでもよい。当事者 E i は、当事者 E i が対象物の所有権を証明できるデータ (例えば、秘密鍵) を含む、対象物に対するデータが保存されるデジタルウォレット D W i を有している。

【0140】

さらに、D W i は、また、トークンに関連付けられたデータ、特に、トークン量を所有する当事者 E i を証明するデータ、を保存する。D W i は、ブロックチェーンシステム 500 と通信する。対象物は、マークし、読取装置、すなわち、管理システム 30 によって、その ID が登録された読取装置、を用いてマーキングを読み取ることによって、システム 100 に登録される。読取装置は、対象物の読み取り、及び、管理システム 30 へのマーキングに対応するデータの送信を実行するための許可を受信するために、管理システム 40 と通信する。管理システム 30 は、対象物上のマーキングに対応するデータ、及び、選択的に、追加のデータ、を送信するために、ブロックチェーンシステム 500 と通信する。例えば、追加のデータは、マークされた対象物のタイプ、読み取りの時間、及び / 又は、位置を示すデータ、当事者 E i、及び / 又は、マーキングを読み取るために使用される特定の読取装置を識別するデータ、等に関連してもよい。選択的に、ブロックチェーンシステム 500 における対象物の登録は、マークされた対象物の読み取りに関するデータ (例えば、読み取りの時間や場所、読取装置を操作する当事者、又は、マークされた対象物の所有者を識別するデータ等) を提供するために、読取装置からブロックチェーンシステム 500 への情報の送信によって条件付けられてもよい。さらに、ブロックチェーンシステムへのマークされた対象物の記録の登録は、トークンの量を、例えば、当事者 E i に転送するための必要条件 / 条件であってもよい。予め選択されたデジタルウォレット / アカウントは、トークン管理ツールによって検証されてもよい (例えば、対象物が登録された状態で、トークンはデジタルウォレットに転送されてもよい)。マークされた対象物の所有権の移転において、所有権は、当事者 E i に、そのデジタルウォレット D w i を用いて転送され、対象物のその所有権を証明し、及び、デジタルウォレット d w I を使用する当事者 E i (例えば、ディストリビュータ、又は、クライアント) に所有権を移転する指示を提供してもよい。このような取引は、当事者 E i によって、管理システム 30 に関連付けられる読取装置によって対象物のマーキングを読み取り、管理システム 30 に読み取ったマーキングを示すデータを通信し、及び、管理システム 30 によって対象物のマーキングを認証することによって、のみ確定されてもよい。通信は、読み取りのために必要とされるデータを読み出し、及び / 又は、受信を実行する許可を受信するようないくつかの他の段階を有してもよい。

【0141】

他の例では、所有権の移転は、当事者 E f に渡される前に、当事者 E i によって保持されている間に、対象物のマーキングを読み取ることによって実行されてもよい。さらなる例では、マークされた対象物の所有権を転送する取引は、マーキングされた対象物を受け取った後に、(当事者 E i によって) 当事者 E f に渡される前に、及び、当事者 E f によって、マーキングを読み取ることを必要とする。

【0142】

本発明の面では、管理システム 30 は、ブロックチェーンシステム 500 に登録されるべき対象物がマークされ、及び、管理システム 30 に登録されていることを検証する目的で、初期段階でのみ、ブロックチェーンシステム 500 と通信する。管理システムは、対象物がマークされ、及び、登録されたことを、ブロックチェーンシステム 500 に確認すると、管理システム 30 からの任意の追加のデータは、デジタルウォレットを介して転送されてもよい。例えば、管理システム 30 は、対象物がマークされ、及び、登録されていることを、ブロックチェーンシステム 500 に確認すると、管理システム 30 は、デジタルウォレットを介して、デジタルウォレットが実行している取引は、認証されたマークさ

れた対象物に関係し、及び、取引が読み取りを必要とする場合、マーキングが管理システム30によって読み取られ、及び、認証されたことを確認するデータ（例えば、対象物に関連付けられたデジタル署名）を転送するように、マークされた対象物に関連付けられた公開鍵、又は、鍵のセットを（公開鍵暗号、及び/又は、デジタル署名方式を用いて）生成してもよい。

【0143】

ブロックチェーンシステム500は、2つの異なる対象物のタイプ：マークされた対象物、及び、トークンに、所有権、及び、取引の記録を有してもよい。これにより、第1の資産のタイプを含む取引、及び、手続きが、他のものを含む取引で条件付けされるスマートコントラクトの実行が可能になる。例えば、予め選択された量のトークンを当事者Efから当事者Eiに転送する平行取引を実行する際にのみ、（当事者Eiから当事者Efへの）マークされた対象物の所有権の移転が、実行されてもよい。すなわち、（対象物の所有権を転送する）第1の取引は、（トークンを転送する）第2の取引に条件付けされる。代替的に、条件付けを逆にえきる。すなわち、第2の取引は、第1の取引の実行に依存させることができる。第3の例では、両方の取引は、共同で、実行され、及び、確定されてもよい。すなわち、他方の実行なく、いずれの取引も実行されない

10

【0144】

このような条件付き取引は、第1の取引に条件付けられていると示されている、以前に実行された第2の取引が、取引のブロックのチェーンに発見される場合にのみ、ブロックチェーンシステムのノードが、第1の取引ブロックを含むことができるようにすることによって実行され得る。したがって、取引を妥当性検証するように動作するノードは、ブロックのチェーンにおける第2の取引の存在を検証する際にのみ、第2の取引を妥当性検証するだろう。

20

【0145】

所有権の転送が、管理システム30からマークされた対象物に関連する受信情報に関連付けられる、マークされた対象物所の所有権の移転のためのスマートコントラクトを実行する本発明の一実施形態による方法600のフローチャートである図5を参照する。

【0146】

ステップ602において、ブロックチェーンシステム500は、一方当事者（当事者Ei）を表すデジタルウォレットからの要求を受信し、マークされた対象物の所有権が、対象物に存在する署名の読み取りに関連付けられた（すなわち、その真正性を検証する）当事者Eiから当事者Efに、転送されるスマートコントラクトを開始する（すなわち、ブロックチェーン500に含まれる新しいブロックに所有権の移転を記録する）。

30

【0147】

ステップ604において、当事者Eiのデジタルウォレットは、ブロックチェーンシステム500と通信し、及び、要求されたデータ、例えば、当事者Eiが公開鍵暗号プロトコルに秘密鍵を保持していることをブロックチェーンシステムに証明するデータ、を提供することによって、マークされた対象物の所有権を証明する。

【0148】

ステップ606において、スマートコントラクトの当事者の一方は、（当事者Ei、又は、当事者Efnいずれか）は、トークン管理ツール40に要求を送信し、マークされた対象物に関連する管理システム30によって管理される特定の情報にアクセスする。例えば、このような情報は、対象物の署名（例えば、署名のハッシュ）を示すデータであってもよい。他の例では、情報は、読取ユニットによって読み取られるような対象物の署名であってもよく、さらに他の例では、情報は、読取ユニットによって読み取られる署名が、管理システム30によって保存される署名と同一であることの単なる確認であってもよい。

40

【0149】

ステップ608において、一方、又は、両方の当事者は、トークン管理システム40に、彼らが、ステップ606で要求された情報を提供するために必要とされる量である予め

50

選択されたトークン量を所有することの証明を提供する。トークン量は、管理システム 30 から要求されたデータを提供するための認証、又は、支払である。

【0150】

ステップ 610 において、要求されたデータは、管理システムから受信される。

【0151】

ステップ 612 において、ブロックチェーンシステム 500 は、管理システム (30) から受信したデータにしたがって、ブロックチェーンシステム 500 内の新しいデータブロックに当事者 E i から当事者 E f への所有権の移転の記録を生成する。例えば、読取ユニットによって読み取られたマークされた対象物の署名が、管理システム 30 によって保存されている対応する署名に一致することの確認を、管理システム 30 から、受信した際のみ、新しい記録は、生成されてもよい。

10

【0152】

いくつかの実施形態によれば、本発明のシステム 100 は、様々な製品、及び、商品（以下、対象物とも呼ぶ）の供給の連鎖を管理し、監視するように構成され、及び、動作可能である。例えば、サプライチェーンを通過する対象物は、ブロックチェーンシステム 500 にマークされ、及び、記録されてもよい。ブロックチェーンの記録は、所与の時間において、対象物を所有する当事者を特定してもよい。対象物が、サプライチェーンを通過して進むにしたがい、所有権の連鎖が、製造者から最終目的地（例えば、エンドユーザ、販売元、別の製造者）までブロックチェーンに記録される（対象物の所有権を有する全ての当事者のリストである）ように、追加の記録が、ブロックチェーン 500 に追加される。

20

【0153】

対象物の占有する当事者は、対象物を所有する当事者とは異なってもよい。例えば、製品、又は、部品は、それが製造される前であっても、当事者によって売買されてもよいので、既に工場では、対象物は、製造者ではなく、クライアントによって所有されている。本発明の一態様では、ブロックチェーンは、対象物を占有する当事者、及び、対象物を所有する当事者の両方の記録を保持する。この目的のために、ここで記載されるブロックチェーンシステム 500 は、1つ以上の台帳、例えば、1つは対象物の所有権を記録する用、他のものは対象物を実際に占有する実体の変化の記録用、及び、選択的に、追加の台帳、例えば、対象物のマーキングを示す台帳、又は、占有する本発明の読取ユニットを有する実体、及び、各読取ユニットの ID を示す台帳、と考えられてもよい。

30

【0154】

上記 2 つのタイプの記録の更新、又は、変更（すなわち、所有権の変更、及び、占有の記録の変更）は、を更新または変更することは、管理システム 30 からの確認、又は、データ、及び / 又は、対象物のマーキングを読み取り、及び、妥当性検証するための読取装置の使用、を必要としてもよい。トークン管理ツール 40 は、異なる取引に関して異なる認証 / トークンの支払いを要求することによって、これらのタイプの記録更新の間で区別してもよい。

【0155】

例えば、トークン管理ツール 40 は、トークンの転送（すなわち、トークンの支払い）という平行取引が存在する場合にのみ、所有権の変更目的で、管理システム 30（及び、読取装置）に、アクセスできるようにする一方、占有の記録の変更目的で、管理システム 30 に、アクセスできるようにしてもよい。

40

【0156】

サプライチェーン管理システムは、環境条件（例えば、温度、湿度等）、及び / 又は、サプライチェーンに沿って進行する対象物の状態（例えば、出荷中）を監視する（例えば、製品、又は、パッケージに取り付けられる）センサのシステムを、利用し、又は、有してもよい。センサによって取得されたデータは、ブロックチェーンシステム 500 に記録され、センサデータの変更できないログを提供する。ブロックチェーン 500 に記録されたセンサデータは、全て（又は、許可されたブロックチェーンの場合は、少なくとも認証された全ての当事者）に対してオープンであってもよく、例えば、対象物、又は、製品を

50

受け取る当事者 E f は、予め選択された時間の間（例えば、出荷中の間）は、環境条件が、許可された範囲を超えていないことを検証してもよい。加えて、センサデータ用のブロックチェーンシステム 500 は、予め選択された期間中に対象物に関連するセンサによって取得されたデータを含むスマートコントラクトを実行できる。例えば、所有権が一の当事者から他方へ移転される取引は、環境条件の逸脱が記録されていなければ（例えば、食品、又は、医薬品は、適切な温度に、継続して、維持される）に、実行されてもよい。

【0157】

本発明のいくつかの実施形態によれば、システム 100 は、関連する当事者、例えば、E i、E f、及び、サプライチェーンに沿って介在する当事者/実体が、製品、又は、パッケージ用のブロックチェーンにアップロードされたセンサデータが、正しい製品に属していることを検証できるようにすることによって、このようなスキームに、安全性、及び、信頼性の追加の層を提供してもよい。

10

【0158】

すなわち、対象物のマーキングを読み取ることによって、対象物（例えば、製品、パッケージ、又は、容器）に、センサ（及び、センサデータ）との間の 1対1 の対応を生成することは、センサの ID に対応すべきである。例えば、センサに保存されるデータは、システム上のマーキングによって提供される署名に対応する ID 番号を有してもよい。センサの ID 番号、及び、センサと対象物署名との対応は、管理システム 30 に保存されてもよい。代替的に、又は、追加的に、センサ自体は、読取装置によって読み取られ、及び、識別され得るマーキングによってマークされてもよい。

20

【0159】

システム 100 は、本発明のいくつかの実施形態によれば、対象物のマーキングを読み取り、及び、「正しい」結果を取得する際にのみ、センサデータがブロックチェーンに記録され得るようにしてもよい。追加的に、本発明のシステムは、記録されるセンサデータが予め選択された範囲からの逸脱を含まないこと、及び、センサが付着される対象物に対応することを検証する際にのみ、マークされた対象物の所有権の変化、又は、占有の変更が記録されるスマートコントラクトを実行してもよい。

【0160】

別の態様では、本発明は、占有の連鎖、及び、選択的に追加の期間、及び、条件が、特権当事者によって設定されるスマートコントラクトを実行するためのシステムを提供する。一例では、特権当事者は、対象物、又は、製品の所有者である。他の例では、特権当事者は、対象物の製造者、又は、ブロックチェーンシステム内の特権当事者、例えば、許可されたブロックチェーンの認証された当事者であってもよい。占有の連鎖に沿って対象物を占有する当事者は、例えば、製品の、製造業者、配送会社、出荷会社、ディストリビュータ、及び、エンドクライアント、又は、所有者、又は、将来の所有者のような製品のサプライチェーンの部分を形成する様々な実体であってもよい。製品の製造業者（又は、代替的には、所有者）は、ここで、製造業者からエンドクライアント、又は、クライアントのグループ（例えば、同じエリアからのクライアント）が、製造業者によって設定されるスマートコントラクトを開始してもよい。

30

【0161】

本発明の実施例にしたがいスマートコントラクトを実行し、サプライチェーンを管理するシステム 100 の実施例の概略図である図 6 を参照する。システム 100 は、ブロックチェーンシステム 500 を有しても、又は、と関連付けられており、及び、管理システム 30、及び、選択的に、トークン管理ツール 40 を有している。追加的に、システム 100 は、図 6 に示されるように、複数の読取装置、例えば、R 1、及び、R 2、を有してもよい。読取装置は、管理システム 30、及び、ブロックチェーンシステム 500 と通信する。図 6 は、また、ブロックチェーンシステム 500、及び、管理システム 30 と通信し、及び、さらに、取引を実行し、及び、デジタルウォレット、又は、システムアプリケーション（図 6 に特に示されていない）を介して、スマートコントラクトを実行する複数の当事者 E i、E 1、E 2、及び、E f を示している。システム 100 は、複数の当事者が

40

50

、管理システム40（例えば、ブロックチェーンシステム500）によって記録されるマークされた物理的な資産/対象物に関連するスマートコントラクトを実行できるようにし、それによって、スマートコントラクトは、また、ネイティブトークン、又は、暗号通貨のような仮想資産を有してもよい。当事者E_iは、例えば、当事者E₁、及び、E₂を介して、対象物の占有する、最終保持者である当事者E_fに対象物を移送することを望んでもよい。特別な実施例では、当事者E_iは、対象物の、製造者、又は、最初の所有者であり、当事者E_fは、対象物の最終所有者（言うなれば、対象物を購入するクライアント）であるのに対して、当事者E₁は、輸送者、又は、配送会社であり、当事者E₂は、ディストリビュータであってもよい。他の例では、当事者E_iは、他の当事者E_f（言うなれば、美術館、又は、ギャラリー）に、展示のために、移送を望む美術作品の所有者であつてもよい。当事者E_iは、対象物の所有権の連鎖が、自身の要求にしたがって設定されるスマートコントラクトを開始してもよい。すなわち、当事者E_iは、対象物が、特定の配送、及び/又は、運送会社、又は、認証された会社のグループによってのみ、対配達され得るようにしてもよい。さらに、当事者E_iは、対象物のマーキングを読み取る際に、サプライチェーンの占有の一部、又は、全ての変更を条件づけし、それによって、承認された当事者が対象物を与えられたことを、読取装置を含む占有の任意の転送で、証明してもよい。図6を参照すると、スマートコントラクトは、占有の連鎖を設定し、及び、追加で、対象物のマーキングの読み取りによって（読取装置R₁、及びR₂のそれぞれによって）、当事者E₁から当事者E₂、及び、E₂から当事者E_fへの占有の変更を条件付ける一方、この例では、当事者E_iから当事者E₁への占有の移転は、マーキングの読み取りを必要としなかった。対象物の占有が変更された取引の記録は、（例えば、上述した第1の台帳10に保存されてもよい）所有権の記録と同様に、ブロックチェーン500に（例えば、上述の第2の台帳20に）、保存される。スマートコントラクトは、また、マーキングの読み取りで条件付けされても、されなくてもよい、対象物の所有権の変更を含んでもよい。

10

20

30

40

50

【0162】

当事者E_i（又は、対象物を所有する任意の他の当事者）は、（対象物のマーキングの読み取りに加えて）様々な要因で条件付けられてもよいスマートコントラクトを実行してもよい。占有（又は、所有権）の移転は、（例えば、GPSを使用することによって検証される）読み取りの時間、及び/又は、位置、特定の読取装置、及び、（デジタルウォレット、又は、システムのアプリケーションを介して）管理システム、又は、ブロックチェーンシステムに送信されてもよい読取装置のIDによって検証されてもよい読取装置を操作するヒト/会社、及び、読取装置を操作するヒト、で条件付けられてもよい。システム100の別の態様では、対象物が2つの異なるタイプのマーキングによってマークされ、それぞれが異なるレベルの妥当性を提供する場合、当事者E₁は、多数の当事者の間での占有の移転の連鎖を含むスマートコントラクトを開始することができ、そこで、ある占有の移転は、あるタイプの読取装置を要求し、及び、他の占有の移転は、（異なるレベルの安全性、妥当性、又は、信頼性を提供する）その他のタイプの読取装置の利用を要求する。一例では、対象物は、XRF感受性マーキング、及び、バーコード、又は、QRコードによってマークされてもよい。スマートコントラクトは、ある占有の移転時に、高いレベルの安全性、及び、信頼性を提供するXRFマーキングの読み取り、及び、他の占有の移転時に、バーコード、QRコードの読み取りを、要求してもよい（及び、管理システム30からデータを要求してもよい）。

【0163】

上述したように、システム100は、また、様々な目的のために様々なタイプの、例えば、サプライチェーンに沿って、環境条件を追跡し、及び、記録するようなセンサを利用してよい。スマートコントラクトは、また、センサによって記録されたデータに条件付けられてもよい。ブロックチェーンシステム500は、スマートコントラクトの条件、及び、期間が満たされない場合には、対象物の所有権、又は、占有の変更を拒否してもよい。代替的に、ブロックチェーンシステム500は、所有権、又は、占有の変更を記録し、

及び、これを認証された変更として記録してもよい。他の例では、ブロックチェーンは、スマートコントラクトの期間を予め選択されたデジタルウォレット（例えば、所有者のデジタルウォレット、又は、スマートコントラクトを開始した当事者）に合わせることに失敗した当事者、又は、当事者群に関連付けられるアカウント、又は、デジタルウォレットから、ブロックチェーンシステム500のネイティブトークンで、支払われる料料、又は、料金を引き出してもよい。

【0164】

別の態様では、本発明に係るシステム100は、対象物、又は、製品の両方、及び、そのコンポーネント、及び、サブコンポーネントのマーキング、及び、単一の対象物/製品に結合するコンポーネント、及び、サブコンポーネントの占有の連鎖の記録、を許可する。すなわち、ブロックチェーン500は、複数の占有の連鎖を表すコンポーネント、及び、サブコンポーネント（及び、できる限り、最終製品）の占有の「ツリー」を記録してもよい。これは、例えば、前述の図2Aの操作OP3によって示されており、ここでは、第1の対象物O1と第2のオブジェクトO2とが一緒に組み立てられ、それによって、選択的に、両方の対象物のマーキングは、読み取られ、及び、処理操作を妥当性検証するために認証されてもよい。このことは、事実上、ツリーは、その発祥（最初の各実体Ei）から、それらが最終の/受取人である実体Efに到達する（例えば、一緒に組み立てられる）までの、複数の対象物の位置の連鎖を表すブロックチェーン500に記録される、という結果になる。

【0165】

したがって、（最終製品、又は、そのコンポーネントの1つ）の製造者によって受け取られるコンポーネントは、それがマークされていること、及び、マーキングが読み取られ、及び、ブロックチェーンに記録されていることという条件で、コンポーネントを利用してもよい。ブロックチェーンシステム上で、コンポーネントをマーキングし、及び、それらを記録するこのスキームは、マークされたコンポーネント（又は、それらの一部）が「正しい」ものであるという保証を提供する。さらに、最終製品の製造業者は、受け取るコンポーネントが本物であるだけでなく、そのサブコンポーネントは（基本コンポーネントに戻るまでずっと）本物であり、及び、正しいソースから発祥することを保証される。

【0166】

本発明のいくつかの実施形態によれば、システム100は、ID（例えば、製品、又は、シリアルナンバー）、及び、対象物、又は、製品に適用されるXRFマーキングとの間の対応関係を生成することによって、対象物、及び、処理取引のオフライン認証をできるように構成され、及び、動作可能であってもよい。この点について、用語「オフライン認証」は、対象物をマークするマーキング、及び、対象物の各IDの間の対応関係を示す、「先天的に」保存される参照データを必要としない（例えば、上記図2Aに参照で記述されたObj'-Data参照へのアクセスを、本質的に、要求しない）認証として理解されるべきである。したがって、参照データへのアクセスを必要としなくてもよいように、処理操作の認証は、オフラインで実行されてもよい。これは、マークで対象をマーキングすることによって、達成され、その署名（例えば、特定の製品の製品ID、又は、シリアル番号に対応する署名）は、識別されるべき対象物、又は、バッチのIDに対応する（例えば、示す）。したがって、IDは、単一の対象物、又は、対象物のバッチに対応してもよい。IDは、製品を識別するID、又は、シリアル番号のような製造中、又は、製造後に対象物に適用される公開のマークであってもよい。IDは、バーコード、又は、QRコードのような機械読み取り可能なマーキングであってもよい。さらなる例では、適切な手段で、又は、適切な条件下で、識別可能な、IDは、秘密にできる。XRFマーキングは、IDに対応して対象物に適用されてもよい。すなわち、マーキングに含まれる材料、及び、要素は、符号化システムに沿って、マーキング材料の量、及び/又は、濃度、及び、できる限り、XRF応答スペクトルに反応する追加の要因（例えば、対象物に存在する材料、応答信号を励起する一時放射物のエネルギーを有する計測条件、及び、ソース-オブジェクト検出器の幾何学的位置関係）を、対象物のIDの署名を表すコード（例えば、バ

10

20

30

40

50

イナリーコード)に、変換している。署名は、IDの関数であり、例えば、ハッシュ関数、又は、IDの暗号化ハッシュ関数である。XRFマーキングは、投薬機械によって準備されてもよい。XRFマーキングは、印刷、スタンプ、スプレー、インジェクション、ブラッシング、及び、エアブラシを含む様々な技術によって対象物に適用されてもよい。

【0167】

XRFマーキングは、参照により本明細書に組み込まれる国際特許出願国際公開PCT/IL2018/050527に記載されているタイプのマーキング装置を用いて、対象物に適用され、又は、配置されてもよい。

【0168】

対象物のIDを用いるあらゆる変更、及び、偽造の試行は、対象物のXRFマーキングを読み取ることによって、検知できるため、ID、及び、XRFマーキングの間の対応関係は、追加の認証、及び、偽造防止層を追加してもよい。

10

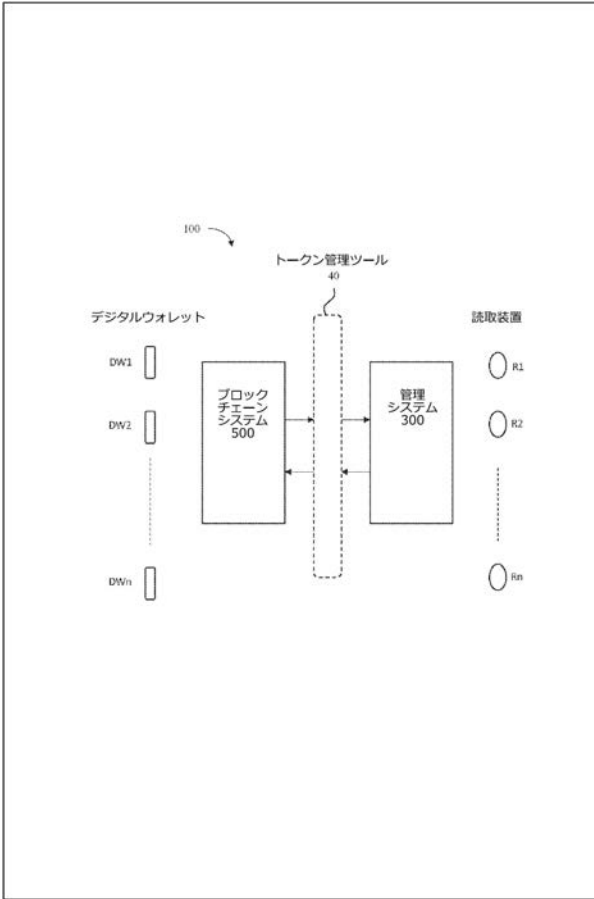
【0169】

さらに、この対応関係は、オフライン認証を可能にするように、(図6の実施例のスキームのような)サプライチェーン管理スキームで使用されてもよい。例えば、システム100は、スマートコントラクトを実行し、そこでは、占有の連鎖が、スマートコントラクトを開始する当事者によって設定される。占有の変更が生ずる前に、マーキングは読み取られるという条件の下での2当事者間での占有の移転は、オフラインで実行されてもよい。すなわち、読取装置とブロックチェーンシステム500、及び/又は、管理システム30の間に接続がない状態でマーキングが読み取られ、また、XRFマーキングが読み取られ、及び、対象物のIDに対応することが判明したことを条件に、接続が確立されると、移転は、ブロックチェーンシステムに記録される。このタイプのオフライン認証は、トークン管理システム40からの認可を必要としてもよい。

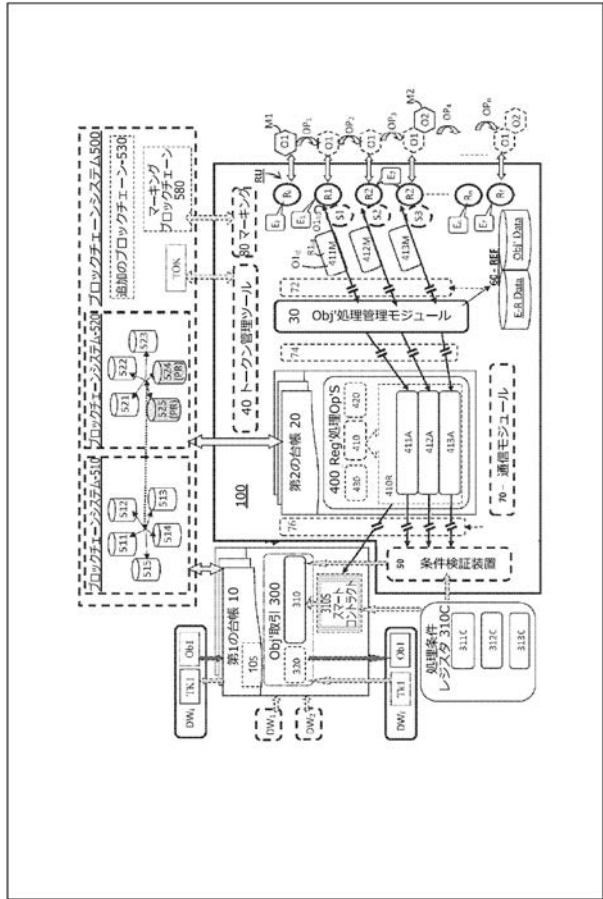
20

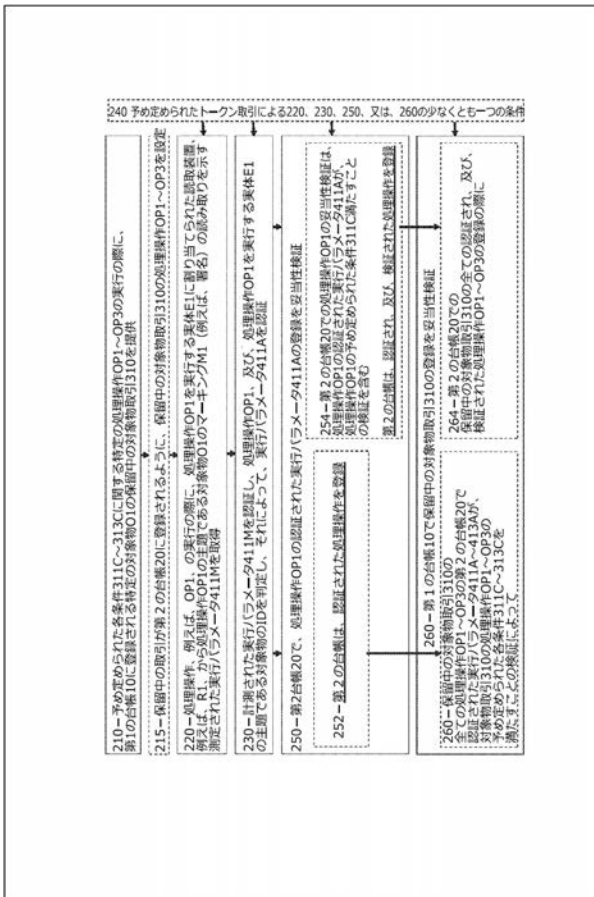
【 図 1 】



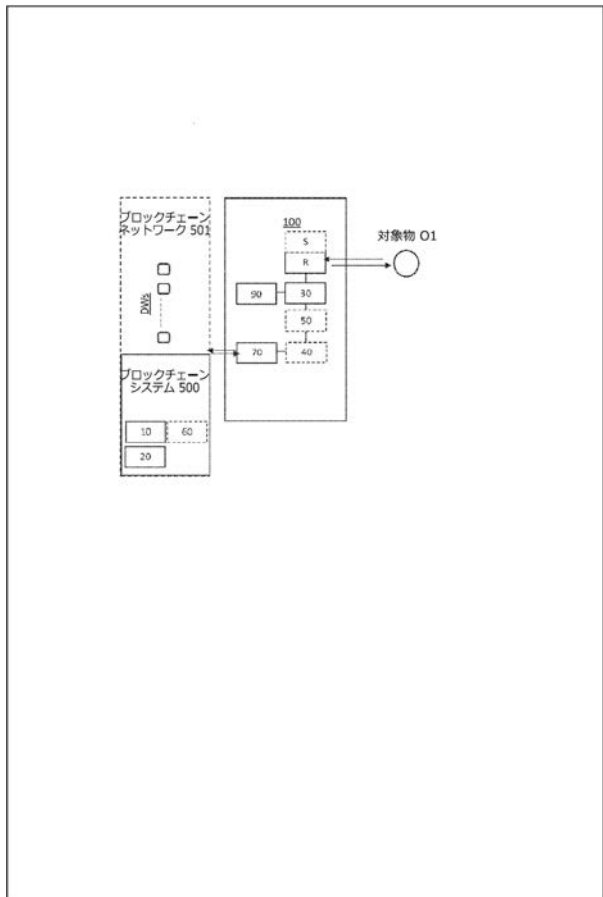
【 図 2 A 】



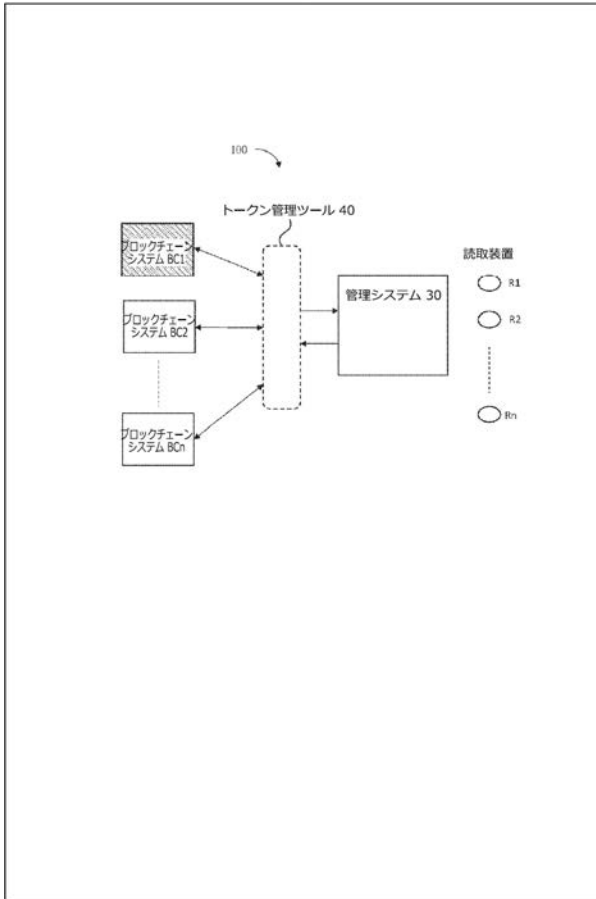
【 図 2 B 】



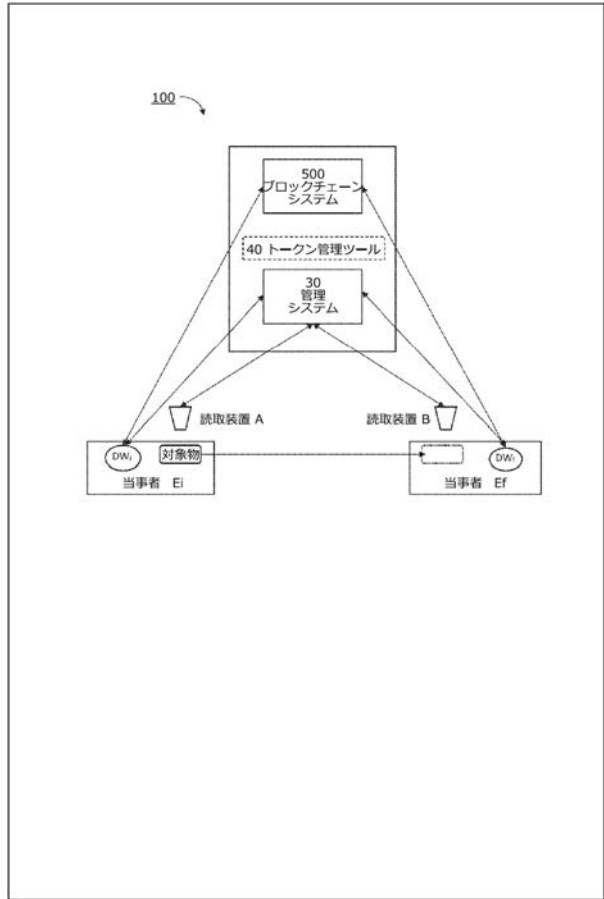
【 図 2 C 】



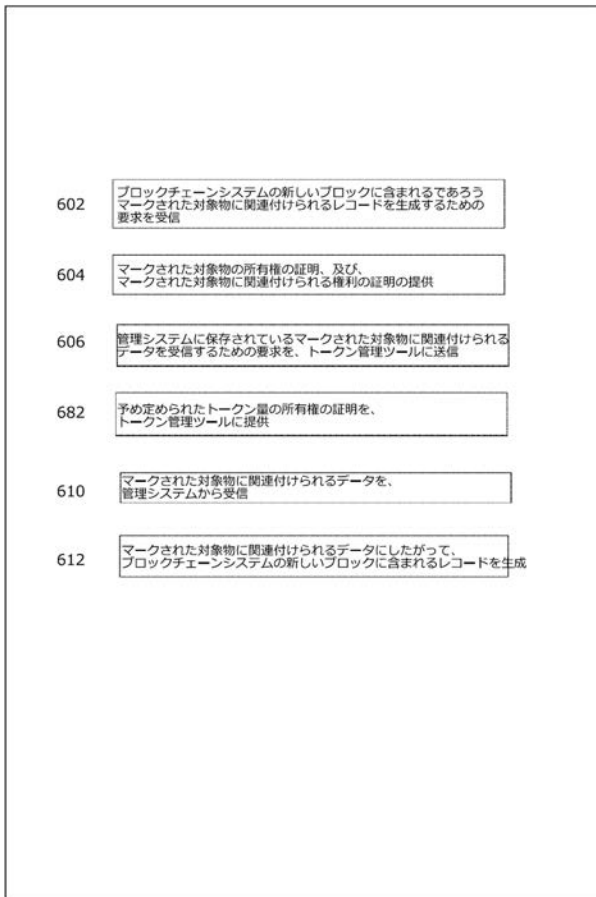
【 図 3 】



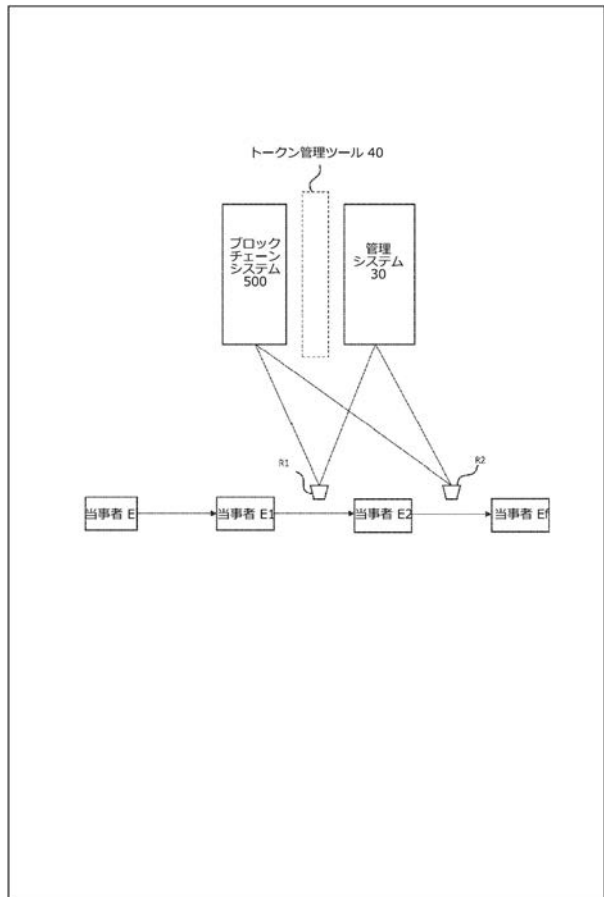
【 図 4 】



【 図 5 】



【 図 6 】



【 国際調査報告 】

INTERNATIONAL SEARCH REPORT		International application No. PCT/IL2019/050283
A. CLASSIFICATION OF SUBJECT MATTER IPC (20190101) G06F 17/50, G06Q 30/06, G06Q 10/08, G06Q 20/40, G01N 23/22, H04L 29/06, H04L 12/24, G06F 21/60 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC (20190101) G06F 17/50, G06Q 30/06, G06Q 10/08, G06Q 20/40, G01N 23/22, H04L 29/06, H04L 12/24, G06F 21/60 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) Databases consulted: Esp@cenet, Google Patents, Google Scholar, Orbit Search terms used: supply chain ledgers peer distributed transactions smart contract ownership manufacturing physical authentication reader marks transportation		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2017331896 A1 HOLLOWAY et al. 16 Nov 2017 (2017/11/16) The whole document	1-21,27-30
Y	The whole document	22-26,31-43
A	The whole document	44-51
Y	WO 2017221246 A1 SOREQ NUCLEAR RESEARCH CENTER [IL] 28 Dec 2017 (2017/12/28) The whole document	22-26,31-43
A	The whole document	44-51
A	US 2018012311 A1 SMALL et al. 11 Jan 2018 (2018/01/11) The whole document	1-51
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 30 May 2019		Date of mailing of the international search report 30 May 2019
Name and mailing address of the ISA: Israel Patent Office Technology Park, Bldg.5, Malcha, Jerusalem, 9695101, Israel Facsimile No. 972-2-5651616		Authorized officer DRUCKER Ekaterina Telephone No. 972-73-9327221

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL2019/050283

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2018042427 A1 SOREQ NUCLEAR RESEARCH CENTER [IL] 08 Mar 2018 (2018/03/08) The whole document	1-51

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/IL2019/050283

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
US 2017331896 A1	16 Nov 2017	US 2017331896 A1	16 Nov 2017
		EP 3455802 A1	20 Mar 2019
		GB 201608431 D0	29 Jun 2016
		GB 201608432 D0	29 Jun 2016
		GB 201608435 D0	29 Jun 2016
		WO 2017194976 A1	16 Nov 2017
WO 2017221246 A1	28 Dec 2017	WO 2017221246 A1	28 Dec 2017
		WO 2017221246 A8	22 Feb 2018
		AU 2017283257 A1	17 Jan 2019
		EP 3472600 A1	24 Apr 2019
		KR 20190028446 A	18 Mar 2019
US 2018012311 A1	11 Jan 2018	US 2018012311 A1	11 Jan 2018
		CA 3025064 A1	23 Nov 2017
		CN 109690589 A	26 Apr 2019
		EP 3459029 A1	27 Mar 2019
		KR 20190010628 A	30 Jan 2019
		SG 11201810306X A	28 Dec 2018
		US 2018136633 A1	17 May 2018
		WO 2017201489 A1	23 Nov 2017
WO 2018042427 A1	08 Mar 2018	WO 2018042427 A1	08 Mar 2018
		AU 2017319785 A1	21 Mar 2019
		CA 3034063 A1	08 Mar 2018

フロントページの続き

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

(特許庁注：以下のものは登録商標)

1. QRコード

(72)発明者 ローゼンブラット、デビッド マーク

アメリカ合衆国、07670 ニュージャージー、テナフライ、ヨーク プレイス 17

Fターム(参考) 5L049 AA16

【要約の続き】

つ以上の物理的な対象物に関連付けられ対象物取引を記録できる。

【選択図】【図2A】