

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7545330号
(P7545330)

(45)発行日 令和6年9月4日(2024.9.4)

(24)登録日 令和6年8月27日(2024.8.27)

(51)国際特許分類

F I

G 0 6 Q 30/0241(2023.01)

G 0 6 Q 30/0241 3 9 4

G 0 6 Q 50/10 (2012.01)

G 0 6 Q 50/10

請求項の数 47 (全53頁)

(21)出願番号	特願2020-546537(P2020-546537)	(73)特許権者	515280056
(86)(22)出願日	平成30年11月27日(2018.11.27)		ブランドシールド リミテッド
(65)公表番号	特表2021-504861(P2021-504861 A)		イスラエル国 ラマットーハシャロン ソ
(43)公表日	令和3年2月15日(2021.2.15)	(74)代理人	コロフ ストリート 8 1
(86)国際出願番号	PCT/IL2018/051287		100079108
(87)国際公開番号	WO2019/106659	(74)代理人	弁理士 稲葉 良幸
(87)国際公開日	令和1年6月6日(2019.6.6)		100109346
審査請求日	令和3年11月22日(2021.11.22)	(74)代理人	弁理士 大貫 敏史
(31)優先権主張番号	62/591,339		100117189
(32)優先日	平成29年11月28日(2017.11.28)	(74)代理人	弁理士 江口 昭彦
(33)優先権主張国・地域又は機関	米国(US)		100134120
		(72)発明者	弁理士 内藤 和彦
			ケレン, ヨアフ
			イスラエル国, ラマットーハシャロン
			4 7 2 1 2, エラ ストリート 1 8
			最終頁に続く

(54)【発明の名称】 保護された電子商取引および電子金融取引のシステム、デバイス、および方法

(57)【特許請求の範囲】

【請求項1】

(a) 少なくとも、

(i) ユーザに資産を販売する、または情報を提供する、オンライン宛先のコンテンツと、

(i i) 前記オンライン宛先における所有権に関するデータと、

(i i i) 不正の可能性がある、または虚偽の情報を公開している可能性があるとして、前記オンライン宛先にフラグを立てる、1つ以上のクラウドソースのユーザ提出レポートと、を組み合わせる分析するステップと、

(b) 前記ステップ(a)の分析に基づいて、前記資産を販売する、または前記情報を提供する、前記オンライン宛先のコンテンツが、虚偽または不正であるかどうかを判定するステップと、を含み、

コンピュータ化された装置によって自動的に実行される方法であって、更に、

(c) ブロックチェーンデータセットを通じて、少なくとも、

(i) 前記1つ以上のクラウドソースのユーザ提出レポート、および

(i i) 前記判定するステップにおいてコンテンツが虚偽又は不正ではないと判定された前記オンライン宛先の真正性に関する承認のスタンプ、又は、前記判定するステップにおいて虚偽又は不正のコンテンツを有すると判定された前記オンライン宛先の非真正性に関する不承認のスタンプ

を公開するステップ、

を含む、方法。

【請求項 2】

前記ステップ (a) の分析は、少なくとも、

(i) 前記オンライン宛先が、1つ以上の資産の不正な販売を申し出ている、または虚偽の情報を含んでいることを示す、複数のユーザ提出レポートを受信することと、

(ii) 合意に達するための1つ以上の条件を示す事前定義されたルールに基づいて、前記ユーザ提出レポートのうちの1つ以上の正確性に関して、ユーザの群衆の中で検出される少なくとも合意を考慮することにより、前記ステップ (b) の判定を実行することと、を含む、請求項 1 に記載の方法。

【請求項 3】

(i) オンライン購入のために1つ以上の資産を申し出る、または情報を公開する特定のオンライン催場が信頼できるということを判定することと、

(ii) 公的にアクセス可能な自己検証可能なブロックチェーンデータセットに、前記特定のオンライン催場が信頼できるという標識を公開することと、を含む、請求項 1～2 のいずれか一項に記載の方法。

【請求項 4】

前記資産の販売を申し出るオンライン催場が、正当であるということを判定することと、前記オンライン催場が真正であるという標識を前記ユーザに提供することと、を含む、請求項 1～3 のいずれか一項に記載の方法。

【請求項 5】

前記情報を公開する前記オンライン宛先が、信頼できる宛先であることを判定することと、前記オンライン宛先が、信頼できるという標識を前記ユーザに提供することと、を含む、請求項 1～4 のいずれか一項に記載の方法。

【請求項 6】

前記オンライン宛先が、不正または信頼できないということを判定することと、前記オンライン宛先が、不正または信頼できないという標識を前記ユーザに提供することと、を含む、請求項 1～5 のいずれか一項に記載の方法。

【請求項 7】

前記ユーザが、前記オンライン宛先を通じて偽造資産を購入しようとしているという通知を前記ユーザに提供することを含む、請求項 1～6 のいずれか一項に記載の方法。

【請求項 8】

前記ユーザが、前記オンライン宛先を通じて真正な資産を購入しようとしているという通知を前記ユーザに提供することと、前記資産が真正であるという返金保証を前記ユーザに提供することと、を含む、請求項 1～7 のいずれか一項に記載の方法。

【請求項 9】

前記ユーザ提出レポートの少なくとも1つが、

- a) 詐欺の重大度に関するスコア、
- b) 詐欺のタイプ、
- c) 詐欺の対象となっているブランド又は会社、
- d) 詐欺であると疑われる理由、
- e) 特有の詐欺事件のレポート

のうちの少なくとも1つを含む、請求項 1～8 のいずれか一項に記載の方法。

【請求項 10】

特定の電子メールメッセージがスパムであるかどうかに関する、複数のユーザ提出レポートを受信することと、

前記複数のユーザ提出レポート間の合意を判定することと、

(i) 前記ユーザ提出レポート、(ii) 前記合意の標識のうちの少なくとも1つをブロックチェーンデータセットに公開することと、

前記合意に一致するレポートを提出した少なくとも1人のユーザに報酬を提供することと、を含む、請求項 1～9 のいずれか一項に記載の方法。

10

20

30

40

50

【請求項 1 1】

特定のオンライン催場がフィッシング催場であるかどうかに関する、複数のユーザ提出レポートを受信することと、

前記複数のユーザ提出レポート間の合意を判定することと、

(i) 前記ユーザ提出レポート、(i i) 前記合意の標識のうちの少なくとも1つをブロックチェーンデータセットに公開することと、

前記合意に一致するレポートを提出した少なくとも1人のユーザに報酬を提供することと、を含む、請求項 1 ～ 1 0 のいずれか一項に記載の方法。

【請求項 1 2】

特定のオンライン催場が偽造品を販売しているかどうかに関する、複数のユーザ提出レポートを受信することと、

前記複数のユーザ提出レポート間の合意を判定することと、

(i) 前記ユーザ提出レポート、(i i) 前記合意の標識のうちの少なくとも1つをブロックチェーンデータセットに公開することと、

前記合意に一致するレポートを送信した少なくとも1人のユーザに報酬を提供することと、を含む、請求項 1 ～ 1 1 のいずれか一項に記載の方法。

【請求項 1 3】

組織内の複数のユーザに、特定のオンライン催場が、前記組織の1つ以上の偽造資産を販売している、または前記組織に関する虚偽の情報を公開しているという通知を提供することを含む、請求項 1 ～ 1 2 のいずれか一項に記載の方法。

【請求項 1 4】

前記ステップ (a) の分析が、

(i) 前記オンライン宛先の登録所有者である第1のエンティティを判定することと、

(i i) 第2の異なるエンティティが、前記オンライン宛先を通じた販売が申し出されている前記資産における商標の登録所有者であると判定することと、

(i i i) 前記第1のエンティティが前記第2のエンティティとは異なることに基づいて、前記オンライン宛先での前記資産の販売の申し出は不正であると判定することと、含む、請求項 1 ～ 1 3 のいずれか一項に記載の方法。

【請求項 1 5】

前記ステップ (a) の分析は、少なくとも、

(i) 前記オンライン宛先が、前記資産をエンドユーザへの販売を申し出る第1の価格を判定することと、

(i i) 前記資産の製造業者推奨小売価格 (M S R P) である第2の価格を判定することと、

(i i i) 前記第1の価格は、Nが所定の正の数である、少なくともNパーセントだけ前記第2の価格よりも安いことを判定することと、

(i v) 前記第1の価格は、少なくともNパーセントだけ前記第2の価格よりも安いことを判定することに基づいて、前記オンライン宛先での前記資産の販売の申し出は不正であると判定することと、を含む、請求項 1 ～ 1 4 のいずれか一項に記載の方法。

【請求項 1 6】

前記ステップ (a) の分析は、少なくとも、

(i) 前記オンライン宛先上の前記資産のテキストによる説明が、前記資産の製造業者による前記資産の正式な説明と比較して1つ以上の不一致を有することを判定することと、

(i i) 前記1つ以上の不一致を有することを判定することに基づいて、前記オンライン宛先での前記資産の販売の申し出が不正であると判定することと、を含む、請求項 1 ～ 1 5 のいずれか一項に記載の方法。

【請求項 1 7】

前記ステップ (a) の分析は、少なくとも、

(i) 前記オンライン宛先上の前記資産のテキストによる説明が、前記資産の製造業者による前記資産の正式な説明と比較して1つ以上の異なる特性を有することを判定すること

10

20

30

40

50

であって、前記特性が、規模、寸法、重量、色、使用される材料、量のうちの1つ以上を含む、特性を有することを判定することと、

(ii) 前記1つ以上の異なる特性を有することを判定することに基づいて、前記オンライン宛先での前記資産の販売の申し出が不正であると判定することと、を含む、請求項1～16のいずれか一項に記載の方法。

【請求項18】

前記ステップ(b)の判定はまた、前記オンライン宛先が、不正であると判定された別のオンライン宛先の所有者としてすでに識別されている、特定のエンティティによって所有されているという判定に基づくことを含む、請求項1～17のいずれか一項に記載の方法。

【請求項19】

前記ステップ(a)の分析は、少なくとも、

(i) 前記オンライン宛先が、1つ以上の資産の不正な販売を申し出ている、または虚偽の情報を含んでいることを示す複数のユーザ提出レポートを受信することであって、

各ユーザ提出レポートが、ユーザのレポート提出と一緒に、提出ユーザによって暗号通貨の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、

(ii) 合意に達するための1つ以上の条件を示す事前定義されたルールに基づいて、前記ユーザ提出レポートのうちの1つ以上の正確性に関して、ユーザの群衆の中で検出される少なくとも合意を考慮することにより、前記ステップ(b)の判定を実行することと、を含む、請求項1～18のいずれか一項に記載の方法。

【請求項20】

前記ステップ(a)の分析は、少なくとも、

(i) 前記オンライン宛先が、1つ以上の資産の不正な販売を申し出ている、または虚偽の情報を含んでいることを示す複数のユーザ提出レポートを受信することであって、

各ユーザ提出レポートが、ユーザのレポート提出と一緒に、提出ユーザによって法定額の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、

(ii) 合意に達するための1つ以上の条件を示す事前定義されたルールに基づいて、前記ユーザ提出レポートのうちの1つ以上の正確性に関して、ユーザの群衆の中で検出される少なくとも合意を考慮することにより、前記ステップ(b)の判定を実行することと、を含む、請求項1～19のいずれか一項に記載の方法。

【請求項21】

複数のユーザ提出レポートと一緒に受信された複数の支払いから報奨金源を作成することと、

特定の提出ユーザの特定のユーザ提出レポートが正しいと判定される場合、次に、前記特定の提出ユーザに、前記報奨金源の一部である支払いを、前記特定の提出ユーザが自分のユーザレポートの提出と一緒に支払った前記支払い以上の金額で分配することと、を含む、請求項1～20のいずれか一項に記載の方法。

【請求項22】

(i) 暗号通貨の支払いを暗号通貨ウォレットに受信するオンライン催場のコンテンツとメタデータを分析し、(I) 前記暗号通貨ウォレットの現実の所有者の実際のアイデンティティと、(II) 前記オンライン催場の現実の所有者の前記アイデンティティとの間の不一致を検出することと、

(ii) 前記不一致に基づいて、前記暗号通貨ウォレットへの暗号通貨の支払いを受信する前記オンライン催場が不正であることをエンドユーザに通知することと、を含む、請求項1～21のいずれか一項に記載の方法。

【請求項23】

(i) 暗号通貨の支払いを暗号通貨ウォレットに受信するオンライン催場のコンテンツとメタデータを、前記コンテンツとメタデータを、前記オンライン催場の外部で収集され

10

20

30

40

50

た少なくとも1つの外部情報のソースと比較することによって、分析することと、

(i i) 前記コンテンツとメタデータと、前記少なくとも1つの外部情報のソースとの不一致に基づいて、前記暗号通貨ウォレットへの暗号通貨の支払いを受信する前記オンライン催場が不正であることをエンドユーザに通知することと、を含む、請求項1～22のいずれか一項に記載の方法。

【請求項24】

(i) (i) エンドユーザから暗号通貨の支払いを受信することを意図された暗号通貨ウォレットの特定のアドレスをエンドユーザに提供するオンライン催場のコンテンツおよびメタデータと、(i i) 前記オンライン催場の外部で収集された外部情報の少なくとも1つのソースの間を比較することと、

(i i) 前記暗号通貨ウォレットの前記特定のアドレスが、前記オンライン催場に記載されている製品の正当な所有者に属していないことを判定することと、

(i i i) 前記オンライン催場には、暗号通貨ウォレットの不正なアドレスが含まれているという、少なくとも1人のエンドユーザへの通知を生成することと、を含む、請求項1～23のいずれか一項に記載の方法。

【請求項25】

(i) (i) エンドユーザから暗号通貨の支払いを受信することを意図された暗号通貨ウォレットの特定のアドレスをエンドユーザに提供するオンライン催場のコンテンツおよびメタデータと、(i i) 前記オンライン催場の外部で収集された外部情報の少なくとも1つのソースの間を比較することと、

(i i) 前記暗号通貨ウォレットの前記特定のアドレスが、前記オンライン催場に記載されている製品の正当な所有者に属していることを判定することと、

(i i i) 前記オンライン催場には、前記正当な所有者の暗号通貨ウォレットの真正なアドレスが含まれているという、少なくとも1人のエンドユーザへの通知を生成することと、を含む、請求項1～24のいずれか一項に記載の方法。

【請求項26】

前記方法は、

(i) 前記オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートを受信されることであって、各ユーザ提出レポートが、ユーザのレポート提出と一緒に、提出ユーザによって暗号通貨の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、

(i i) 提出ごとに暗号通貨の支払いを必ず必要とする前記提出機構を介して、すべて提出された前記複数のユーザ提出レポートを分析することにより、前記ステップ(b)の判定を実行することと、を含む、請求項1～25のいずれか一項に記載の方法。

【請求項27】

前記方法は、

(i) 前記オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートを受信することであって、各ユーザ提出レポートが、ユーザのレポート提出と一緒に、提出ユーザによって暗号通貨の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、

(i i) 提出ごとに暗号通貨の支払いを必ず必要とする前記提出機構を介して、すべて提出された前記ユーザ提出レポートのうちの1つ以上の正確性に関して、エンドユーザの群衆の中で到達された少なくとも合意を考慮することにより、前記ステップ(b)の判定を実行することと、を含む、請求項1～26のいずれか一項に記載の方法。

【請求項28】

前記方法は、

(i) 前記オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートを受信することであって、各ユーザ提出レポートが、ユーザのレポート提出と一緒に、提出ユーザによって暗号通貨の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、

(i i) 提出ごとに暗号通貨の支払いを必ず必要とする前記提出機構を介して、すべて提出された前記複数のユーザ提出レポートを分析することにより、前記ステップ (b) の判定を実行することと、

(i i i) 真正性が自己検証可能なブロックチェーンデータセットの一部として、前記ユーザ提出レポートの少なくとも1つを公開することと、を含む、請求項1～27のいずれか一項に記載の方法。

【請求項29】

前記方法は、

(i) 前記オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートを受信することであって、各ユーザ提出レポートが、ユーザのレポート提出と一緒に、提出ユーザによって暗号通貨の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、

(i i) 提出ごとに暗号通貨の支払いを必ず必要とする前記提出機構を介して、すべて提出された前記複数のユーザ提出レポートを分析することにより、前記ステップ (b) の判定を実行することと、

(i i i) 前記オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートと一緒に受信された複数の暗号通貨の支払いから報奨金源を作成することと、

(i v) 特定の提出ユーザの特定のユーザ提出レポートが正しいと判定される場合、次に、前記特定の提出ユーザに、前記報奨金源の一部である暗号通貨の支払いを、前記特定の提出ユーザが自分のユーザレポートの提出と一緒に支払った前記暗号通貨の支払い以上の金額で分配することと、を含む、請求項1～28のいずれか一項に記載の方法。

【請求項30】

前記方法は、

(i) 前記オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートを受信することであって、各ユーザ提出レポートが、ユーザのレポート提出と一緒に、提出ユーザによって暗号通貨の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、

(i i) 提出ごとに暗号通貨の支払いを必ず必要とする前記提出機構を介して、すべて提出された前記複数のユーザ提出レポートを分析することにより、前記ステップ (b) の判定を実行することと、

(i i i) 前記オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートと一緒に受信された複数の前記暗号通貨の支払いから報奨金源を作成することと、

(i v) 前記オンライン宛先が、1つ以上の資産の前記不正な販売を申し出ていることを示すユーザレポートを提出した提出ユーザの間で、前記報奨金源の少なくとも一部を分配することと、を含む、請求項1～29のいずれか一項に記載の方法。

【請求項31】

前記方法は、

(i) 前記オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートを受信することであって、各ユーザ提出レポートが、ユーザのレポート提出と一緒に、提出ユーザによって法定額の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、

(i i) 提出ごとに法定額の支払いを必ず必要とする前記提出機構を介して、すべて提出された前記複数のユーザ提出レポートを分析することにより、前記ステップ (b) の判定を実行することと、を含む、請求項1～30のいずれか一項に記載の方法。

【請求項32】

前記方法は、

(i) 前記オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートを受信することであって、各ユーザ提出レポートが、ユーザのレ

10

20

30

40

50

ポート提出と一緒に、提出ユーザによって法定額の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、

(i i) 提出ごとに法定額の支払いを必ず必要とする前記提出機構を介して、すべて提出された前記ユーザ提出レポートのうちの1つ以上の正確性に関して、エンドユーザの群衆の中で到達された少なくとも合意を考慮することにより、前記ステップ (b) の判定を実行することと、を含む、請求項 1 ～ 3 1 のいずれか一項に記載の方法。

【請求項 3 3】

前記方法は、

(i) 前記オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートを受信することであって、各ユーザ提出レポートが、ユーザのレ
ポート提出と一緒に、提出ユーザによって法定額の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、

(i i) 提出ごとに法定額の支払いを必ず必要とする前記提出機構を介して、すべて提出された前記複数のユーザ提出レポートを分析することにより、前記ステップ (b) の判定を実行することと、

(i i i) 真正性が自己検証可能なブロックチェーンデータセットの一部として、前記ユーザ提出レポートの少なくとも1つを公開することと、を含む、請求項 1 ～ 3 2 のいずれか一項に記載の方法。

【請求項 3 4】

前記方法は、

(i) 前記オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートを受信することであって、各ユーザ提出レポートが、自分のレポート提出と一緒に、提出ユーザによって法定額の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、

(i i) 提出ごとに法定額の支払いを必ず必要とする前記提出機構を介して、すべて提出された前記複数のユーザ提出レポートを分析することにより、前記ステップ (b) の判定を実行することと、

(i i i) 前記オンライン宛先が1つ以上の資産の不正な販売を申し出ていることを示す、複数のユーザ提出レポートと一緒に受信された複数の前記法定額の支払いから報奨金源を作成することと、

(i v) 特定の提出ユーザの特定のユーザ提出レポートが正しいと判定される場合、次に、前記特定の提出ユーザに、前記特定の提出ユーザが自分のユーザレポートの提出と一緒に支払った法定額以上の額で、前記報奨金源の一部である法定額の支払いを分配することと、を含む、請求項 1 ～ 3 3 のいずれか一項に記載の方法。

【請求項 3 5】

前記方法は、

(i) 前記オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートを受信することであって、各ユーザ提出レポートが、自分のレポート提出と一緒に、提出ユーザによって法定額の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、

(i i) 提出ごとに法定額の支払いを必ず必要とする前記提出機構を介して、すべて提出された前記複数のユーザ提出レポートを分析することにより、前記ステップ (b) の判定を実行することと、

(i i i) 前記オンライン宛先が1つ以上の資産の不正な販売を申し出ていることを示す、複数のユーザ提出レポートと一緒に受信された複数の前記法定額の支払いから報奨金源を作成することと、

(i v) 前記オンライン宛先が、1つ以上の資産の前記不正な販売を申し出ていることを示すユーザレポートを提出した提出ユーザの間で、前記報奨金源の少なくとも一部を分配することと、を含む、請求項 1 ～ 3 4 のいずれか一項に記載の方法。

【請求項 3 6】

前記方法は、

(i) オンライン購入のために1つ以上の資産を申し出ている特定のオンライン催場が、信頼できるということを判定することと、

(ii) 公的にアクセス可能な自己検証可能なブロックチェーンデータセットに、前記特定のオンライン催場が信頼できるという標識を公開することと、を含む、請求項1～35のいずれか一項に記載の方法。

【請求項37】

前記方法が、

(i) 暗号通貨トークンであるデジタル資産を生成して、前記暗号通貨トークンを電子デバイスのエンドユーザに配分することと、

(ii) ユーザレポートの提出が、事前定義された受信者への前記暗号通貨トークンの支払いと一緒に実行されることを条件として、不正の可能性があるオンライン催場に関する前記ユーザレポートの提出を受信するオンライン機構を生成することと、を含む、請求項1～36のいずれか一項に記載の方法。

【請求項38】

前記方法が、

(i) 暗号通貨のデジタルトークンを生成して、暗号通貨の前記デジタルトークンを電子デバイスの複数のエンドユーザに分配することと、

(ii) 各ユーザレポートの提出が、事前定義された受信者への前記暗号通貨のデジタルトークンの支払いと一緒に実行されることを条件として、不正の可能性があるオンライン催場に関するユーザレポートの提出を受信することと、

(iii) それぞれの支払いに関するデータと一緒に前記エンドユーザの各々によって実行された、前記ユーザレポートの提出のコンテンツおよびメタデータをその中に組み込むブロックチェーンデータセットを生成することと、を含む、請求項1～37のいずれか一項に記載の方法。

【請求項39】

前記方法が、

(i) 暗号通貨のデジタルトークンを生成して、前記暗号通貨のデジタルトークンを電子デバイスの複数のエンドユーザに分配することと、

(ii) 各ユーザレポートの提出が、事前定義された受信者への前記暗号通貨のデジタルトークンの支払いと一緒に実行されることを条件として、不正の可能性があるオンライン催場に関するユーザレポートの提出を受信することと、

(iii) 前記不正が起こり得るオンライン催場に関する1つ以上のユーザレポートの正確性に関して、コミュニティの合意が到達されると判定することと、

(iv) 少なくとも前記コミュニティの合意が到達されると判定することに基づいて、前記不正が起こり得るオンライン催場の承認または非承認のいずれかのデジタルスタンプを生成して、前記デジタルスタンプを、前記ユーザレポートをも含む自己検証可能なブロックチェーンデータセットに公開することと、を含む、請求項1～38のいずれか一項に記載の方法。

【請求項40】

前記方法が、

(i) 暗号通貨のデジタルトークンを生成して、前記暗号通貨のデジタルトークンを電子デバイスの複数のエンドユーザに分配することと、

(ii) 各ユーザレポートの提出が、事前定義された受信者への前記暗号通貨のデジタルトークンの支払いと一緒に実行されることを条件として、不正の可能性があるオンライン催場に関するユーザレポートの提出を受信することと、

(iii) ユーザレポートの提出と一緒に、前記事前定義された受信者に支払われた前記デジタルトークンの少なくとも一部を含む保証資金を生成することと、

(iv) その後、不正であると判定された前記オンライン催場からの資産を購入した特定のエンドユーザに、前記保証資金の少なくとも一部を分配することと、を含む、請求項1

10

20

30

40

50

～ 39 のいずれか一項に記載の方法。

【請求項 41】

前記方法が、

(i) 暗号通貨のデジタルトークンを生成して、前記暗号通貨のデジタルトークンを電子デバイスの複数のエンドユーザに分配することと、

(ii) 各ユーザレポートの提出が、事前定義された受信者への前記暗号通貨のデジタルトークンの支払いと一緒に実行されることを条件として、不正の可能性のあるオンライン催場に関するユーザレポートの提出を受信することと、

(iii) オンライン宛先のコンテンツとメタデータをレビューし、それらが真正であるか不正であるかを判定する欺瞞防止施行エンティティに、ユーザレポートの提出と一緒に前記事前定義の受信者に支払われた前記デジタルトークンの少なくとも一部を分配することと、を含む、請求項 1～40 のいずれか一項に記載の方法。

10

【請求項 42】

特定のオンライン催場で販売の申し出がされている特定の製品が、偽造であることを示す N 件のユーザ提出レポートを受信することと、

前記特定のオンライン催場で販売の申し出がされている前記特定の製品が、真正であることを示す M 件のユーザ提出レポートを受信することと、

前記 N 件のユーザ提出レポートおよび M 件のユーザ提出レポート以外の少なくとも 1 つの追加パラメータまたはデータを考慮する分析に基づいて、合意は、前記特定のオンライン催場で販売の申し出がされている前記特定の製品が真正であるということであると判定することと、

20

(i) 前記 N 件のユーザ提出レポート、(ii) 前記の M 件のユーザ提出レポート、(iii) 前記合意の標識のうちの少なくとも 1 つをブロックチェーンデータセットに公開することと、

前記特定の製品が真正であるという前記 M 件のユーザ提出レポートのうちの少なくとも 1 つを提出した少なくとも 1 人のユーザに報酬を提供することと、を含む、請求項 1～41 のいずれか一項に記載の方法。

【請求項 43】

特定のオンライン催場で販売の申し出がされている特定の製品が、偽造であることを示す N 件のユーザ提出レポートを受信することと、

30

前記特定のオンライン催場で販売の申し出がされている前記特定の製品が、真正であることを示す M 件のユーザ提出レポートを受信することと、

前記 N 件のユーザ提出レポートおよび M 件のユーザ提出レポート以外の少なくとも 1 つの追加パラメータまたはデータを考慮する分析に基づいて、合意は、前記特定のオンライン催場で販売の申し出がされている前記特定の製品が偽造であるということであると判定することと、

(i) 前記 N 件のユーザ提出レポート、(ii) 前記の M 件のユーザ提出レポート、(iii) 前記合意の標識のうちの少なくとも 1 つをブロックチェーンデータセットに公開することと、

前記特定の製品が偽造であるという前記 N 件のユーザ提出レポートのうちの少なくとも 1 つを提出した少なくとも 1 人のユーザに報酬を提供することと、を含む、請求項 1～41 のいずれか一項に記載の方法。

40

【請求項 44】

特定の電子メールメッセージが、スパムであることを示す N 件のユーザ提出レポートを受信することと、

前記特定の電子メールメッセージが、スパムでないことを示す M 件のユーザ提出レポートを受信することと、

前記 N 件のユーザ提出レポートおよび M 件のユーザ提出レポート以外の少なくとも 1 つの追加パラメータまたはデータを考慮する分析に基づいて、合意は、前記特定の電子メールがスパムでないということであると判定することと、

50

(i) 前記 N 件のユーザ提出レポート、(i i) 前記の M 件のユーザ提出レポート、(i i i) 前記合意の標識のうちの少なくとも 1 つをブロックチェーンデータセットに公開することと、

前記特定の電子メールがスパムでないという前記 M 件のユーザ提出レポートのうちの少なくとも 1 つを提出した少なくとも 1 人のユーザに報酬を提供することと、を含む、請求項 1 ～ 4 3 のいずれか一項に記載の方法。

【請求項 4 5】

特定の電子メールメッセージが、スパムであることを示す N 件のユーザ提出レポートを受信することと、

前記特定の電子メールメッセージが、スパムでないことを示す M 件のユーザ提出レポートを受信することと、

前記 N 件のユーザ提出レポートおよび M 件のユーザ提出レポート以外の少なくとも 1 つの追加パラメータまたはデータを考慮する分析に基づいて、合意は、前記特定の電子メールがスパムであるということであると判定することと、

(i) 前記 N 件のユーザ提出レポート、(i i) 前記 M 件のユーザ提出レポート、(i i i) 前記合意の標識のうちの少なくとも 1 つをブロックチェーンデータセットに公開することと、

前記特定の電子メールがスパムであるという前記 N 件のユーザ提出レポートのうちの少なくとも 1 つを提出した少なくとも 1 人のユーザに報酬を提供することと、を含む、請求項 1 ～ 4 3 のいずれか一項に記載の方法。

【請求項 4 6】

特定のオンライン催場がフィッシング催場であることを示す N 件のユーザ提出レポートを受信することと、

特定のオンライン催場がフィッシング催場でないことを示す M 件のユーザ提出レポートを受信することと、

前記 N 件のユーザ提出レポートおよび M 件のユーザ提出レポート以外の少なくとも 1 つの追加パラメータまたはデータを考慮する分析に基づいて、合意は、前記特定のオンライン催場がフィッシング催場でないということであると判定することと、

(i) 前記 N 件のユーザ提出レポート、(i i) 前記 M 件のユーザ提出レポート、(i i i) 前記合意の標識のうちの少なくとも 1 つをブロックチェーンデータセットに公開することと、

前記特定のオンライン催場がフィッシング催場でないという前記 M 件のユーザ提出レポートのうちの少なくとも 1 つを提出した少なくとも 1 人のユーザに報酬を提供することと、を含む、請求項 1 ～ 4 5 のいずれか一項に記載の方法。

【請求項 4 7】

特定のオンライン催場がフィッシング催場であることを示す N 件のユーザ提出レポートを受信することと、

特定のオンライン催場がフィッシング催場でないことを示す M 件のユーザ提出レポートを受信することと、

前記 N 件のユーザ提出レポートおよび M 件のユーザ提出レポート以外の少なくとも 1 つの追加パラメータまたはデータを考慮する分析に基づいて、合意は、前記特定のオンライン催場がフィッシング催場であるということであると判定することと、

(i) 前記 N 件のユーザ提出レポート、(i i) 前記 M 件のユーザ提出レポート、(i i i) 前記合意の標識のうちの少なくとも 1 つをブロックチェーンデータセットに公開することと、

前記特定のオンライン催場がフィッシング催場であるという前記 N 件のユーザ提出レポートのうちの少なくとも 1 つを提出した少なくとも 1 人のユーザに報酬を提供することと、を含む、請求項 1 ～ 4 5 のいずれか一項に記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

関連出願の相互参照

この特許出願は、2017年11月28日に出願されたUS 62 / 591, 339からの利益と優先権を主張し、その全体が参照により本明細書に組み込まれる。

【0002】

本発明は、電子商取引および電子金融取引の分野に関する。

【背景技術】

【0003】

世界中の何百万人もの人々が、毎日さまざまな電子デバイスを利用している。たとえば、ユーザは、さまざまな活動およびタスクを実行するために、デスクトップコンピュータ、ラップトップコンピュータ、スマートフォン、またはタブレットを利用することができる。

10

【0004】

たとえば、ユーザは、電子デバイスを利用して、電子メール（eメール）の送受信、ゲームのプレイ、インターネットの閲覧、オンラインショッピングの実行、デジタルコンテンツの利用、請求書の支払い、株式やその他の証券の取引、オンラインオークションへの参加、インスタントメッセージング（IM）やビデオ会議への従事などを行うことができる。

【発明の概要】

【0005】

20

本発明のいくつかの実施形態は、オンラインで販売の申し出がされている特定の製品が、実際には（または間違いなく、またはおそらく、またはそうであると推定される）偽造品、または偽物、または模倣品、または非純正品であることをユーザに警告し、またはユーザが訪問または従事したオンライン催場（たとえば、ウェブサイト、ウェブページ、モバイル「アプリ」またはアプリケーション）は、その性質上、不正なオンライン催場である（たとえば、所有者が、欺瞞または詐欺を犯したり、知的財産（IP）権を侵害したり、偽造グッズまたは偽造サービスを販売したりするために利用されている）ことをユーザに警告する、システム、デバイス、および方法を含み得る。

【0006】

本発明のいくつかの実施形態は、オンラインで販売の申し出がされている、またはオンラインでアクセスまたは使用できるウェブページまたはモバイル「アプリ」用に提供される、製品／サービスのリスクスコアを生成し、またはそのような製品／サービスに関して、またはそのようなウェブサイトまたはウェブページまたはモバイルアプリケーションに関して、「偽物」／「本物」の判定を生成するために、「群衆の知恵」および／または人工知能（AI）を利用することができる。

30

【0007】

いくつかの実施形態は、ユーザが訪問している特定の宛先（たとえば、ウェブサイト、ウェブページ）が、本物を本当に申し出ていることをユーザに確認する証明スタンプを生成してユーザに提示することができる。必要に応じて、証明スタンプデータはブロックチェーンベースのデータセットを使用して格納でき、これにより、そのような証明データの改ざんを防ぎ、および／またはユーザもしくはウェブブラウザは、証明スタンプが実際に有効であり、そのようなブロックチェーンの一部であるとして真正であることを自動的にチェックし検証できる。

40

【0008】

いくつかの実施形態では、ユーザは、偽造品または偽物の販売または販売を助長する、または欺瞞行為または海賊活動を実行する、ウェブサイトおよびウェブページおよび／またはモバイルアプリに関して、中央サーバに報告することができ、このような報告ユーザは、ブランド所有者、システム管理者、またはユーザ自身によって、この目的のために設立された報奨金資金から、暗号通貨の支払いなどの報酬を受け取る権利がある。

【0009】

50

本発明は、他のおよび／または追加の利点および／または利益を提供することができる。

【図面の簡単な説明】

【0010】

【図1】本発明のいくつかの例証的な実施形態によるシステムの概略図である。

【発明を実施するための形態】

【0011】

本発明は、オンラインおよびオフラインのブランド保護のためのシステムを含み、これは、販売の申し出がされている、潜在的な欺瞞または偽の活動または偽物をユーザに通知し、オンラインアイテムやその他の情報の自動分析に加えて、情報源として群衆の知恵を使用する。

【0012】

本明細書での説明では、「偽物／偽のサービス」は、偽造品、または模倣品、または非純正品もしくはサービス、または低品質の製品／サービスもしくは非オリジナル製品／サービス、違法な製品もしくは不法な製品（たとえば、ブランド名または知的財産（IP）権を侵害しているために製造または販売することが不法である製品）、ブランドを侵害する製品もしくはサービス、ブランドを侵害する製品もしくはサービス、ブランドを妨害する製品もしくはサービス、非オリジナル製品もしくはサービス、またはその製品のブランドの法的所有者またはブランドの法的所有者の認定代理人によって製造、分配、および／または販売されていない製品を含む。

【0013】

本明細書での説明において、「オンラインアイテム」は、ウェブサイト、ウェブページ、ソーシャルメディアページまたは要素、電子商取引市場のリスティング、ソーシャルメディアまたはソーシャルネットワークアイテムまたは要素（これらに限定されないが、投稿、ページ、ユーザ、イベント、グループなどを含む）、オンライン広告もしくはバナー、モバイルアプリケーションもしくは「アプリ」、アプリケーションもしくは「アプリ」ストアもしくは同様の場所からダウンロードできるアプリケーションまたは「アプリ」、ブログ、ビデオブログ（vlog）、マイクロブログプラットフォーム（たとえば、Twitter）、写真共有プラットフォーム（たとえば、Pinterest）、マルチメディア共有プラットフォーム（たとえば、YouTube）、電子商取引サイトもしくはベンダーもしくはオンライン商人（たとえば、Amazon）、オンラインオークションサイト（たとえば、eBay）、新製品および／または使用済みの製品および／また中古品を販売するためのオンラインウェブサイト（Amazon、eBayなど）などを含み得る。

【0014】

本明細書での説明において、「欺瞞オンラインアイテム」、または「不正オンラインアイテム」、または「不正製品オンラインアイテム」は、欺瞞を犯し、または犯そうとするために使用されるオンラインアイテム、および／または種々の欺く方法（たとえば、「フィッシング」）を実行して、ユーザの資格情報（たとえば、オンライン銀行口座へのログイン詳細）を盗もうとし、または試みるオンラインアイテム、（たとえば、攻撃者によって制御されている）間違った銀行口座への銀行電信振込を実行し、または暗号通貨を間違った暗号通貨のウォレットまたは受取人アドレスに振り替えるなど、意図された宛先に支払いを振り替えないようにし、または、送金者が意図した受取人に支払いの振替をしないようにユーザを欺こうとし、および／または偽造品の販売に使用され、および／または偽の製品または偽のサービスの販売または申し出に使用されているオンラインアイテム、および／またはブランド所有者の著作権、商標、サービスマーク、その他の知的財産権を侵害しているオンラインアイテム、および／または違法ダウンロードを許可（海賊行為）し、および／または海賊版デジタルコンテンツを格納し、および／またはリンクまたはハイパーリンクまたは奔流またはポイントの提供により、海賊版コンテンツの不法ダウンロードを助長するオンラインアイテム、および／またはビデオおよび／または音楽および／または他のコンテンツの違法ストリーミングを提供するオンラインアイテム、および／また

10

20

30

40

50

は他のIP侵害（複数可）または違反（複数可）を犯し、または犯すことを試みるオンラインアイテムを含む。

【0015】

本明細書での説明において、「電子デバイス」は、デスクトップコンピュータ、ラップトップコンピュータ、スマートフォン、タブレット、スマートウォッチ、ゲームコンソール、スマートテレビ、ケーブルボックス、インターネット端末、インターネット、接続デバイス、インターネットプロトコル（IP）接続デバイス、スマート器具（たとえば、食品のオンライン購入が可能な冷蔵庫）、モノのインターネット（IoT）デバイスなどを含み得る。

【0016】

出願人は、評判の良いオンライン商人（Amazon、eBayなど）に属するものを含む多くのオンラインアイテムが、偽造品、偽物、または模倣グッズの申し出で反発されており、ユーザは、高品質の本物の製品であると信じている製品をオンラインで購入するように騙されることがよくあるが、実際には低品質の偽の製品や模造品または非純正品を受け取っていることに気付いていた。出願人はまた、種々のオンラインアイテムを通じて実行される不正行為の多くが金融欺瞞であることに気付いていた。

【0017】

出願人は、オンラインで販売の申し出がされている偽物を特定できる独自のシステムを考案し、それは、オンラインユーザに、ユーザが、偽物であるか、おそらくまたはたぶん偽物である製品を閲覧または購入していることを警告し、および／または、それは、ユーザが、オンラインユーザに、欺瞞、詐欺、または偽物や非純正品の販売に使用されると推定されるオンラインアイテムを閲覧または訪問していることを警告する。

【0018】

本発明のいくつかの例証的な実施形態による、システム100の概略図である図1を参照する。たとえば、エンドユーザは、リモートリソース110（たとえば、ウェブサイト、ウェブページ、コンテンツを給するサーバ）にアクセスまたは相互作用するために、ブラウザ102および／またはネイティブアプリケーションまたは「アプリ」103を有する彼の電子デバイス101を利用している。電子デバイス101は、たとえばスタンドアロンアプリケーションまたは「アプリ」として、またはウェブブラウザの不可欠な部分として、または拡張機能、プラグインまたはアドオンとして実装され得る警告モジュール121を含み得、警告モジュール121はユーザへの警告通知を生成し、オンライン製品がおそらく偽物である、またはオンラインアイテムがおそらく欺瞞関連または不正であることをユーザに警報する。

【0019】

本発明のいくつかの実施形態は、たとえば、アプリケーションまたは「アプリ」またはプラグインまたはブラウザ拡張または局所的にインストールされたソフトウェアまたは他のモジュールもしくはユニットを含むことができ、それは、ユーザがオンラインで買うまたは注文するつもり、または検討している製品／サービス、または現在オンラインショッピングカートを見、閲覧、または追加している製品／サービスが、間違いなくまたは「おそらく」偽物／偽のサービスであることをユーザに警告し、および／またはユーザが現在閲覧または表示またはダウンロードしている、または消費している、または訪問しようとしている、または消費しようとしている、ダウンロードしようとしている、または閲覧しようとしている、オンラインアイテムは、間違いなくまたは「おそらく」欺瞞オンラインアイテムであることをユーザに警告する。

【0020】

たとえば、ユーザは「アプリ」、アプリケーション、プラグイン、ブラウザ拡張機能、ブラウザアドオン、局所的にインストールされたソフトウェア、ネイティブソフトウェアなどの警告モジュールを自分の電子デバイスにインストールする。警告モジュールは、バックグラウンドまたはフォアグラウンドで、特に、ユーザが任意のタイプのウェブページ（ウェブサイト、市場のリスティング、ソーシャルメディアページなど）にアクセスまた

10

20

30

40

50

は閲覧しているとき、またはアプリ（たとえば、専用の「ベンダー、商人、またはその他のエンティティのアプリ）を使用しているとき、走行している。

【0021】

いくつかの実施形態では、警告モジュールは、システムのリモートサーバによって実行された、ウェブサイトまたはウェブページまたは「アプリ」の事前スキャンに基づいて動作し、そのようなウェブサイトまたはウェブページまたは「アプリ」を介して実行できるコンテンツ、メタデータ、リンクおよび／または動作を事前走査して事前分析し、事前に収集および分析されるデータは、その後、ユーザがそのような宛先（複数可）をリアルタイムで閲覧するときに利用される。他の実施形態では、警告モジュールは、リアルタイムまたはほぼリアルタイムの走査、および／またはユーザが実際に訪問しているウェブサイトまたはウェブページまたは「アプリ」の分析に基づいて、そのような実際の訪問の開始直後、またはユーザがウェブブラウザまたは彼の電子デバイスにそのような宛先にアクセスするように指示した直後に動作する。さらに他の実施形態では、警告モジュールは、事前走査と事前分析との組み合わせを、リアルタイム走査およびリアルタイム分析と一緒に利用することができ、たとえば、現在訪問している宛先のリアルタイム走査および分析は、その宛先が以前にシステムによって走査または分析されていなかった場合に実行される。

【0022】

警告モジュールは、訪問されている（または、ユーザが後でアクセスする可能性があり、いまは、事前走査および事前分析されている）ウェブサイトまたはウェブページの1つ以上のパラメータであって、たとえば、コンテンツ、メタデータ、ドメイン名、販売の申し出がされているアイテムの説明と価格、走査および分析されたウェブサイトまたはウェブページまたは「アプリ」の一部であるリンクおよび／またはハイパーリンクなど、1つ以上のパラメータを分析する情報アナライザ122を含み、電子デバイスで局地的にまたはリモートでリスク分析を実行する（たとえば、情報またはハイパーリンクをリモートサーバ151またはクラウドベースのコンピューティングエンジンに送信または転送し、情報アナライザ152を介してリモートでリスク分析を実行し、リモートリスクスコアジェネレータ153を利用してリスクスコアを電子デバイスに送り返す）。ローカル警告モジュール121および／またはリモートサーバ151は、実行されたリスク分析の結果であるリスクスコアを検査、または1つ以上の事前定義された閾値または値の範囲と比較するリスクスコアコンパレータ161を備える。たとえば、リスクスコアが事前定義の閾値より大きい場合、警告モジュールは、ユーザへの即時通知を生成し、ウェブページまたはアプリの潜在的なリスクレベルに関してユーザに警報し、特に、閲覧されている、または購入を検討されている、または購入されている（たとえば、オンラインショッピングカートに追加されている、または追加されようとしている、または追加された）製品またはサービスが、間違いなく偽の製品／サービスである、またはおそらく偽物／偽のサービスである、または偽の製品／サービスであると推定されることを、警告モジュールが推定または判定したという事実をユーザに警告する。

【0023】

いくつかの実施形態では、リスクスコアジェネレータを介してリスクスコアを生成する代わりに、またはそれに加えて、システムは、ローカルまたはリモートの本物／偽のバッジジェネレータ154を利用することができ、特定の製品が、本物（真正、オリジナル、合法）、または偽造（偽造、模倣）と推定されるかどうかの判定を生成することができ、それに応じてバッジまたは指標またはラベルを生成し、ユーザに表示またはその他の方法で伝達する。

【0024】

リスクレベル（またはリスクスコア）は、たとえば、「高リスク」／「中リスク」／「低リスク」、すなわち、たとえば、「最も可能性が高いのは、偽物／詐欺です」、「おそらくこれは偽物／欺瞞です」、「おそらくこれは本物です」など、またはたとえば数値スコア（たとえば、0～100の範囲であって、100は間違いなく偽物を示し、85はおそらく偽物を示し、60はたぶん偽物を示し、15はおそらく本物の製品を示し、0は間違

10

20

30

40

50

いなく本物の製品を示す)、または色付きスコアないしは色分け配合、または好適な指標などの範囲またはスロットで、ユーザにさらに通知される。

【0025】

警告モジュールは、承認済み、事前承認済み、検証済み、または事前検証済みのウェブページまたはアプリについてユーザに通知する場合もある。この場合、リスクレベルは、たとえば「リスクなし」、または「認証済みウェブサイト」などになる。

【0026】

例証的な例において、ユーザAdamは彼のラップトップを使用して、Sonyのプレイステーション卓のワイヤレスコントローラを閲覧している。ユーザAdamがSony.comのオンラインストアを閲覧すると、警告モジュールが「リスクなし」または「間違いなく本物の製品」の通知を提示する場合がある。ユーザAdamがSony.co.ukのオンラインストアを閲覧すると、警告モジュールは同様に「リスクなし」または「間違いなく本物の製品」の通知を表示する場合がある。ただし、ユーザAdamが、たとえば身元不明の当事者が運営しているか、非常に低価格で（たとえば、閾値を下回る価格、または、この例では「Sony.com」自体など、本物の製品のベンダーであることがわかっているベンダーに比べて少なくともKパーセント安い）製品を販売している「Cheap-Sony-Items.com」のドメイン名を有するウェブサイトを閲覧するとき、警告モジュールは、「高リスク」または「おそらく偽物」の通知を生成して提示する場合がある。さらに、ユーザAdamがAmazonまたはeBayなどの評判の良い電子商取引ウェブサイトを閲覧したとき、たとえば、ユーザAdamがeBayのリスティングを閲覧していて、販売者「Cheap-Sony-Items-From-China」が、（たとえば、メーカー希望小売価格（MSRP）が、70ドルであるときに）そのジョイスティックを4ドルの価格で販売している場合、またはその販売者が、Amazon市場で同様の価格のサードパーティ販売者である場合、警告モジュールは、なお、「高リスク」／「おそらく偽物」の通知を生成する場合がある。

【0027】

ユーザがウェブページまたはアプリにアクセスすると、（たとえば、バックグラウンドで走行する）警告モジュールは、ウェブページのURLまたはアプリの識別子を含む関連情報を自動的にチェックおよび／または分析し、電子デバイスに対してローカルであるか、リモートデバイスである場合（たとえば、クラウドコンピューティングデータベース）があり得る、本物のプロバイダのデータベースおよび／または偽のプロバイダのデータベースおよび／または他のデータベースでの一致のために、その情報を比較し、そのようなデータベースは、さまざまな製品、サービス、ウェブサイト、ウェブページ、ドメイン、アプリ、または他の要素について事前に分析され、事前にスコアが付けられた情報を含む場合がある。例証目的で、データベース177はサーバ151の一部として示されているが、それらは異なるマシンに常駐する場合もあれば、電子デバイス101に対してローカルである場合もあれば、部分的にローカルで部分的にリモートである場合もある。

【0028】

警告モジュールは、種々の方法でリスクレベルまたはリスクスコアを提示する場合がある。たとえば、それは、ブラウザのツールバーにリスクレベルを表示し、および／またはそれは、ポップアップウィンドウ、画面、タブ、またはウェブページや購入しようとしている製品／サービスに関する警告（または認証メッセージ）を含むメッセージを生成し、またはそれは、リスクスコアを分離されたウィンドウ（たとえば、分離されたアプリの携帯電話、分離された走行中のソフトウェアのPCまたはラップトップ）に表示する場合がある。

【0029】

リスク分析は、全体的または部分的に、あるいは「群衆の知恵」エンジン171またはサブシステムに基づくことができる。群衆は、たとえば、（a）1人のユーザまたは数人のユーザが、販売の申し出がされている偽物／偽のサービスまたはたぶん偽物／偽のサービスについて提出した標識、（b）1人のユーザまたは数人のユーザが欺瞞オンラインア

アイテムまたはたぶん欺瞞オンラインアイテムについて提出した標識、(c) (たとえば、関連するウェブページまたはアプリへの特定のハイパーリンクをも用いて、) 販売の申し出がされている偽物／偽のサービスまたはたぶん偽物／偽のサービスを示し、または詐欺のオンラインアイテムまたは詐欺の可能性があるオンラインアイテムを示す、ブランド所有者またはその代理人 (たとえば、組織、会社、個人、またはその他のエンティティ) からの情報、またはブランド所有者の代表 (たとえば、従業員、IP マネージャー、ブランドマネージャ) からの情報、(d) 各アナリストが、人間のアナリストでも、機械学習 (ML) アルゴリズムを走行させるマシンでも、そのような判定をするためにニューラルネットワーク (NN) を利用するマシンでもかまわない、オンラインブランド保護システムの初期分析を再調査する、専用アナリストからの入力 (以下で説明)、(e) 上記および／または他の情報源の任意の組み合わせ、であってもよい。

10

【0030】

システムはさらに、特定の製品／サービスが偽物である、または偽物であるかもしれない、および／またはオンラインアイテムが、欺瞞であるか、偽物に見えるか、不正に見えるか、偽物／偽のサービスを売っているかを示す、さまざまな「ユーザ標識」または「ユーザ提出」、または「本物の投票」または「偽物の投票」をユーザから受信または収集する。システムは、必要に応じて重み付けユニット 172 または重み付け機構を使用して、そのような標識または提出または投票を集計する (たとえば、一定のユーザからの投票または提出は、他のユーザの投票に比べて重みが増加する可能性があり、たとえば、すでに製品を購入し、それが偽物であると投票する検証済み購入者の投票は、最初の提出を実行したばかりで検証済みの購入者ではない「フレッシュ」ユーザの投票または提出に割り当てられた重みよりも大きな重みが割り当てられる場合がある)。集約されたデータに基づいて、システムは「たぶん偽物」／「たぶん欺瞞」のスコアもしくは指標、または偽の製品／サービスまたは詐欺のオンラインアイテムの起こり得るリスクについてユーザに通知するために、警告モジュールによって使用されるかもしれない他のタイプの潜在的なリスクスコア (または真正性指標) を生成する。

20

【0031】

リスク分析は、人工知能 (AI) エンジン 173 とビッグデータを利用するオンラインブランド保護システムによる自動分析に基づいているか、これを含むことができ、種々のウェブメトリックを分析して、分析中のオンラインアイテムの潜在的なリスクスコアを示し、および／または販売のために申し出されている製品／サービスが本物か偽物かを判定する。

30

【0032】

システムによって分析されるウェブメトリックには、これに限定されないが、コンテンツとキーワード、ウェブページ要素、検索エンジン最適化 (SEO) データ、すべての TLD のドメイン名 (ならびに、ブランド名の使用、またはブランド名のバリエーション、またはドメイン名におけるブランド名の誤植)、ホスティングプロバイダ、DNS データ、レジストラデータ、トラフィックと統計、トラフィック分析、検索エンジンの結果、ウェブサイト／アプリのテクノロジーと構造、メタタグと利用されたコーディング、使用されたプログラミング言語、ロゴおよび／または著作権で保護された画像および／または商標の使用、インバウンドおよびアウトバウンドリンク、ソーシャルメディアへのエンゲージメントまたはウェブサイトからソーシャルメディアへのリンク、またはその逆のリンク、市場での販売者のリスティングの量および／またはタイプ、ユーザおよび／または購入者および／または検証済みの購入者が、ウェブページまたはウェブサイトまたは特定の製品／サービスに関して、提出した投票またはスコアまたは再調査または評価が含まれる。

40

【0033】

システムは、ウェブサイト、電子商取引市場のリスティング、ソーシャルメディアアイテム、オンライン広告、モバイルアプリなど、分析対象のオンラインアイテムに基づいて、関連する種々のメトリックを自動的に分析する。

【0034】

50

種々のメトリックの分析に基づいて、システムはオンラインアイテムが欺瞞オンラインアイテムであるという潜在的なリスクのスコアもしくは評価、またはシステムが、製品／アイテムはどれぐらい本物または偽物であるかを推定する方法を示すスコア指標を自動的に作成する。

【0035】

ユーザがシステムによって分析されたオンラインアイテムにアクセスするとき、警告モジュールは、オンラインアイテムが、潜在的にまたはたぶん欺瞞オンラインアイテムであること、および／またはユーザが注文しようとしている製品／サービスが、潜在的に偽物／偽のサービスであること、および／またはオンラインアイテムのリスクレベル、または逆に、製品／サービスが本物または偽物ではないと判定される、ということをユーザに通知する。

10

【0036】

上述の動作は、全体的または部分的に、上述の「群衆の知恵」および／または上述のその集合体に、上述のオンラインブランド保護システムによって行われる自動分析と組み合わせ、基づくことができ、リスクスコアまたは偽物／本物の指標を生成するために、これらの様態のいくつかまたはすべてを集約し、または組み合わせて使用することができる。

【0037】

いくつかの実施形態では、システムは、群衆の知恵、もしくは「クラウド知恵」、すなわち複数のユーザからの集約された知恵、もしくは複数のユーザからの集約された洞察を、潜在的なリスクレベルの分析またはリスクスコアの生成における追加のパラメータとして使用することができ、さらにまた、群衆の知恵は、オンラインアイテムに優先順位を付け、および／またはスコアを付けるために、分析とAIの一部として使用される。

20

【0038】

いくつかの実施形態では、クラウド知恵は、システムの自律分析または自動分析に追加される追加の情報層として利用され、自動分析の結果を有効化することができる。他の実施形態では、集約されたクラウド知恵が提供した指標を、AI分析を利用して有効化または再確認することができる。さらに他の実施形態では、さまざまな情報およびパラメータのAI分析、ならびに集約された群衆の知恵の両方が、リスクスコアまたは偽物／本物の指標を生成するために組み合わせて使用されるように、加重式が利用され得る。

【0039】

システムは、クローラー174を操作して、まだシステムに知られていない（たとえば、まだクロールまたは分析されていない、またはシステムのデータベースにまだない）、さまざまなウェブページおよびオンラインアイテムを能動的にクロールするために、かつ、その情報を収集してデータベース177に格納し、そのウェブメトリックを分析して、それに応じてリスクスコアを生成するために、標識、リンク、ユーザ提出、またはその他の情報源を利用できる。

30

【0040】

本発明のいくつかの実施形態は、ウェブブラウザ、またはモバイルアプリ、またはショッピングアプリ（Amazonアプリ、eBayアプリなど）に専用の報告ボタン（または他の報告GUI要素）を備えることができ、これによりユーザは、偽物／偽のサービスの標識を簡単かつ迅速に提出し、および／または欺瞞オンラインアイテムの標識を提出できる。たとえば、報告ボタン機構133は、ブラウザの一部として、もしくはモバイルアプリの一部として、またはそれらの拡張機能、もしくはプラグイン、もしくはアドオンとして、またはスタンドアロンアプリケーションとして、電子デバイス101にインストールされ得る。

40

【0041】

たとえば、ユーザがウェブサイト、電子商取引市場、ソーシャルメディアプラットフォーム、モバイルアプリなどの一定のオンラインアイテムを閲覧していて、特定のオンラインアイテムが欺瞞オンラインアイテムである可能性がある、または彼が注文しようとしている（または販売の申し出がされている）製品／サービスは偽物／偽のサービスである可

50

能性があると思えるとき、ユーザは他のGUI要素の専用の報告ボタンを押すかタップでき（それにより、たとえば、「詐欺の可能性を報告します」、「この製品は疑わしい、または偽物であると報告します」などと電話をかけることができる）。次に、ボタンは、オンラインアイテムを本発明の中央システム、または別のオンラインブランド保護システムに報告する機能を開始する。

【0042】

ユーザは、欺瞞／偽の活動またはアイテムまたは製品の疑いがあるときだけでなく、これが欺瞞オンラインアイテムまたは偽物／偽のサービスであることをユーザが実際に知った後でも、その報告ボタンまたはGUI要素を押すか、または従事させることができ、たとえば、ユーザが特定のウェブサイトから一定の製品を既に注文していて、それを受け取った後、ユーザがその製品が偽造であることに気付いた場合、ユーザはボタンを利用してウェブサイトおよび／またはその特定の偽物を本発明のシステムに報告できる。

10

【0043】

いくつかの実施形態では、報告ボタン（または報告に使用される他のGUI要素）は、ユーザが疑わしいオンラインアイテムのURLを（たとえば、閲覧の履歴からカットアンドペーストすることにより）入力するデータ入力フィールドと組み合わせて、または疑わしい製品または偽物のSKU番号または製品番号または他の独自の識別子、またはオンラインで提示されるそのタイトルまたは価格または機能の識別子（たとえば、疑わしいアイテムの独自の非常に低い価格は、偽物の識別子として使用される場合がある）を入力することにより、動作することができる。

20

【0044】

報告ボタンは、正当なオンラインアイテムを報告するためにも同様に使用でき、antには複数のオプション、たとえば、「このウェブサイトは欺瞞です」、「このウェブサイトは正当です」などがある。

【0045】

本発明は、オンライン欺瞞および／または「フィッシング」攻撃および／またはサイバー攻撃およびサイバー詐欺および／または偽造販売を防止または低減するために、ブロックチェーン技術および／または暗号通貨技術をさらに利用することができる。たとえば、暗号通貨はブロックチェーン技術に基づくデジタルトークンであり、暗号通貨に関連する活動には、たとえば、暗号通貨のデジタル財布として機能するウェブサイト、暗号通貨のオンライン交換、初期コインオフリング（ICO）に使用されるウェブサイトまたはプログラム、暗号通貨および／または現在もしくは過去のレートに関する情報を提供するウェブサイト、暗号通貨を使用する製品またはサービスを提供するウェブサイト、証券または先物または暗号通貨の派生物を提供または記載するウェブサイトなどがある。

30

【0046】

本発明は、暗号通貨と「クラウド知恵」（潜在的な欺瞞オンラインアイテムおよび／または偽物／偽のサービスについての群衆からの標識の提出）との統合を可能にすることができる。たとえば、ユーザはそのような情報を提出するために暗号化コインを支払うことができ、および／または、ユーザは、彼の提出が、（上記のAIシステムによる自動分析によってなど）他の標識または偽物または欺瞞で、および／または他のユーザによる他の提出で、裏付けられている場合、暗号化コイン（任意選択で、より大きな金額）を受け取ることができる。

40

【0047】

ユーザは、まったく知られていないオンラインアイテム（たとえば、クロールされたことがなく、かつ偽物／偽のサービスの販売を申し出ているように見えるウェブページ）のシステムへの提出、および／または（たとえば、過去にクロールされたが、人間のユーザが彼の報告を提出するまで、AIシステムによって偽の製品が含まれていると必ずしもフラグ付けされていなかった）既知のオンラインアイテムのシステムへの提出で「ポイント」を蓄積することができる。ユーザがオンラインアイテムを疑わしいものとして提出したが、実際には正当なオンラインアイテムである場合、任意選択で、ユーザはポイントを失

50

うか、暗号化コインを支払うことができる。

【0048】

ユーザが彼の提出に対する暗号化コインを受け取るとき、彼がオンラインアイテムを提出した最初の1人である場合は、多く補償される可能性があり、および／またはユーザが提出により積極的である場合、たとえば、ユーザがそれに達するとき、検証済みの提出（複数可）に対してより多く補償される活動のレベル（たとえば、ユーザが、本当に欺瞞オンラインアイテムであることが判明した少なくともN個のオンラインアイテムを提出すると、増加する補償レベル）がある。

【0049】

システムとそのユーザとの間の暗号通貨の支払いは、たとえば、電子デバイス101にインストールされた支払い／受信暗号コインユニット135を介して、およびリモートサーバ151にインストールされた支払い／受信暗号コインユニット175を介して実行され得る。

【0050】

ユーザに対する補償は、種々のリソース、たとえば、ブランドの所有者（組織、会社、個人など）によって生み出された資金や「報奨金」、および／またはアプリまたはプラグインまたはブラウザ拡張機能または局所的にインストールされたソフトウェアの他のユーザの寄付によって生み出された資金、および／または提出を実行するために支払う他のユーザ、またはブランド所有者にブランド保護のサービスなどを提供する本発明のシステムの管理者によって生み出された資金、からもたらされる可能性がある。

【0051】

いくつかの実施形態は、偽物および／または欺瞞オンラインアイテムを検出するために、スパム（ジャンクメール、ジャンクメッセージ、不要電子メール、不要メッセージ）の分析について、上記の「群衆の知恵」をさらに利用することができる。従来のスパムフィルタは、「これはスパムです」というユーザからの標識を受け取り、電子メールアドレスを「スパムソース」としてマークするか、電子メールアドレスのブラックリストに追加するだけである。しかしながら、本発明のシステムのユーザが警告モジュールおよび報告ボタンを利用してスパムメッセージを報告する場合、システムはまた、スパムメッセージの内容を文脈的に分析して、欺瞞を犯し、および／または偽造グッズを販売し、および／または知的財産権または著作権または商標を侵害し、および／または違法ダウンロードまたは海賊版コンテンツを許可し、および／またはビデオ／音楽／その他のコンテンツの違法ストリーミングを提供し、および／または任意の他のIP侵害を犯す試みを識別し、システムは、疑わしいメッセージでオンラインアイテムへのリンクを識別し、次に、システムのデータベースを更新して、この特定のオンラインアイテム（スパムメッセージによってリンクされたもの）が、おそらく（または間違いなく）この特定の偽物を販売している、または他の不正活動を実行していることを知る。その情報は後で、システムの分析の一部として、オンラインアイテムの分析と採点の両方に、かつ、他のユーザのスパムフィルタリングに使用されることに加えて、オンラインアイテムを訪問し、製品／サービスの購入／注文、またはそのオンラインアイテムへの情報の提供を検討（または試行）するユーザ（他のユーザ）に警告するために使用される。これらの動作は、ユーザによってスパムとして報告された電子メール（またはメッセージ）のコンテンツを分析し、そこから、ウェブページを指し、次に、分析されて、それらが偽物／偽のサービスの販売のために申し出されていることが検出または推定される、ハイパーリンクを抽出するスパム電子メールコンテキストアナライザ136によって実行され得る。

【0052】

いくつかの実施形態では、任意選択で、暗号通貨の支払いまたは報酬は、スパムを報告したユーザ、または受信した電子メールを通じてリンクされている特定のウェブページまたはウェブサイトが、偽造または非純正グッズまたはサービスを販売している、または違法なコンテンツ、海賊版コンテンツ、または不正ウェブサイト（たとえば、フィッシングウェブサイト）などへのアクセスを提供またはアクセスを助長している、ように見えるこ

とを報告したユーザに振り替えられ、または支払われ、それにより、ユーザがそのようなリンクされた宛先を報告する動機を作成する。いくつかの実施形態では、暗号通貨の支払い、報告時直ちに、または他の実施形態では、報告された宛先が本当に欺瞞を助長しているという人間による検証の後でのみ、または少なくともN人のユーザがその宛先を報告した後でのみ、または報告された宛先が（たとえば、複数の種々のユーザからの集約された報告に基づいて）本当に欺瞞を助長していることを、群衆の知恵のアルゴリズムが確認した後でのみ、振り替えられる。

【0053】

いくつかの実施形態では、任意選択で、特定のタイプの宛先またはオンラインアイテムのみが、それらを報告するユーザが、たとえば、ブランド所有者配によって配分され、または割り当てられることができる「欺瞞報告報奨金」に基づく暗号通貨報酬の資格があるようなものであってもよい。たとえば、Sony Corporationなどの本物のブランド所有者は、偽造または非純正のSonyの模倣品を販売し、または販売を促進するオンラインアイテムを報告するユーザに支払われる暗号通貨報酬に資金を提供するため、報奨資金（たとえば、25,000ドル、または5ビットコイン）を配分する場合がある。任意選択で、本発明のシステムは、ブランド所有者から報奨資金の金額全体を収集し、次に、そのようなオンラインアイテムを報告する資格があるユーザに徐々に分配することができ、または、本発明のシステムは、ブランド所有者が（または彼に代わって第三者によって）保有するこのような補償資金から徐々に資金を引き出すか、または、これまでに収集された適格なレポートの数に基づいて利用可能な資金を時々補充することができる。いくつかの実施形態では、暗号通貨報酬の報奨資金は、事前定義された期間内のみ、たとえば11月と12月内（たとえば、多くのオンライン販売が行われるホリデーシーズン）のみ、または事前定義された地域内のみ（たとえば、米国からの報告ユーザにのみ暗号通貨報酬を提供する）、または特定のタイプまたは場所またはTLDのオンラインアイテムに関するもののみ（たとえば、「.co.uk」の宛先またはオンラインアイテムを報告したユーザにのみ通貨報酬を提供する）、または特定の製品または製品ラインに関してのみ（たとえば、偽造のプレイステーションアイテムを販売するオンラインアイテムを報告したユーザにのみ暗号通貨報酬を提供し、偽造のSonyイヤホンを販売するオンラインアイテムを報告したユーザには提供しない）、または少なくとも一定の価格の価値がある偽物を販売するオンラインアイテムに関してのみ（たとえば、少なくとも100米ドルなど、通常Nドル以上のコストがかかる偽造のSony製品を販売するオンラインアイテムを報告するユーザにのみ報酬を提供する）、または特定のブランドまたはブランド名に関してのみ（たとえば、Sony Corporationの「プレイステーション」ブランドであって、他のブランドではない偽造品を販売するオンラインアイテムを報告したユーザにのみ暗号通貨報酬を提供する）、に使用できるように事前定義されている場合がある。ブランド所有者、ブランド所有者の代理人、または本発明のシステムのシステム管理者である報奨資金を設立するエンティティは、報告ユーザへの暗号通貨報酬支払いのための他のルールおよび／または条件を定義および／または構成することができる。したがって、本発明のシステムは、ブランド所有者または彼のための代理人が、記載されているように、本発明のシステムが暗号通貨を利用して施行および実装することができる「アンチ偽造キャンペーン」を定義および構成することを可能にすることができる。

【0054】

例証目的で、本明細書での説明のいくつかの部分は、「偽造グッズの販売」に関連している可能性があり、これは、本発明のシステムが、監視、検出、防止、および／または治療することができる、他のさまざまなタイプの欺瞞または不正活動、あるいは違法活動または不合理活動の非限定的な例である。他のタイプの欺瞞およびオンライン不正活動は、本発明のシステムによって同様に監視され、検出され、防止され、および／または治療され得る。たとえば、ドメインとウェブサイト「chase.com」を所有するChase Bankなどの銀行サービスの正当な所有者は、模倣ウェブサイトまたは「フィッシング」ウェブサイトを報告するユーザに、暗号通貨の報奨金またはその他の報酬を申し出

10

20

30

40

50

る場合があり、それらは Chase Bank に属しているように見えるが、実際には正当なユーザからユーザ資格情報（ユーザ名やパスワードなど）を不正に取得しようとするハッカーまたは攻撃者または犯罪者によって制御されている。同様に、動画（映画）やオーディオ録音（歌）やその他の著作物（たとえば、電子ブックもしくは電子書籍）などの著作権で保護された素材の著作権所有者は、著作権で保護された資産の海賊版デジタルコピーまたは海賊版デジタルバージョンを分配するウェブサイトまたはウェブページまたはアプリケーションを報告するユーザに、またはそれ以外の場合は、（たとえば、リンク、ハイパーリンク、「奔流」ファイル、または海賊版コンテンツへの他のポインタを提供することによって）そのような分配を容易にする、ウェブサイトまたはウェブページまたはアプリケーションを報告するユーザに、暗号通貨の報奨金またはその他の報酬を申し出る場合がある。同様に、他のタイプの欺瞞が本発明によって検出および防止され得、同様に、そのような欺瞞を報告するユーザは、暗号通貨の支払いまたは他の報酬によって報いられ得る。同様に、本発明の証明スタンプは、訪問した目的地が、本当に真正および非欺瞞的な目的地であることをユーザおよび／またはブラウザに証明するために、真正および不正ではないウェブサイトまたはウェブページまたはアプリケーションに提供され得、かつ任意選択で、そのような証明スタンプは、本明細書に記載されているように、ブロックチェーンデータセットを利用することによって格納または検証することができる。

【0055】

いくつかの実施形態では、上記の「群衆の知恵」、および／または上記のその集合体を使用して、正当な（不正ではない）オンラインアイテムを認証または有効化することができる。この認証または有効化は、上記の AI 分析と組み合わせて行うことができる。そのような認証の結果として、システムは、オンラインアイテムのマネージャーに、たとえば、「このウェブサイト偽造防止システムによって有効化されています」、「このウェブサイトで販売の申し出がされている製品は、アンチ偽造システムによって本物として認定されています」などのアイコンやロゴなど、有効化スタンプまたは証明スタンプの形式で、肯定的で有効化済みのスコアをウェブサイトに提示するオプションを提供できる。

【0056】

いくつかの実施形態では、有効化スタンプまたは証明スタンプ（たとえば、「このウェブサイトは本物／非偽造品を販売しています」）は、ブロックチェーン技術を使用して実装されてもよい。たとえば、オンラインアイテムに関して肯定的または有効化スコアを作成したシステムまたはユニットは、データベースまたはデータセットまたはリンクリストまたは、ブロックチェーンを利用するか、ブロックチェーンとして実装されるその他のデータ構造にデータを格納する場合がある。オンラインアイテムの証明書として（たとえば、SSL 証明書と同様に）実装することもできる有効化スタンプまたは証明スタンプの真正性および／または有効性は、ブロックチェーンベースのデータベースまたはデータセットまたはリンクされたリストに接続し（または読み取り）、オンラインアイテムが元帳にあるかどうかを確認することによって、（たとえば、ユーザがウェブブラウザまたは「アプリ」によって独立して）チェックできる。このようなブロックチェーンデータセットの安全な構造（たとえば、データセット内の各レコードには、それ自体の中に前のレコードのデジタルハッシュが含まれている）により、オンラインアイテムの（有効な証明スタンプを提示する資格がある認定オンラインアイテムのリストから、またはリストへの）削除または追加は、使用されている特定のブロックチェーンプロトコルに基づいて、ブロックチェーンのノードの過半数がそのような変更に同意した場合、またはその他の方法に基づいて「合意」に達した場合にのみ行うことができる。そのような有効化スタンプまたは証明スタンプをクリックするユーザは、ブロックチェーンデータベースでスタンプの有効化を実行する手順を開始またはトリガーし、またはいくつかの実施形態では、任意選択で、そのような有効化は、ウェブブラウザによって、またはオペレーティングシステムによって、またはスタンドアロンソフトウェアモジュールによって、またはプラグインまたはアドオンまたは拡張機能によって、そのような証明スタンプまたは有効化スタンプに関連付けられている宛先にアクセスするか、訪問するか、閲覧するとすぐに、自動的におよび／

10

20

30

40

50

または自律的に実行されてもよい。チェックされている特定のオンラインアイテムが、元帳内にない場合、ユーザは警告通知または証明スタンプが有効でないという通知、およびその逆の通知を獲得する。オンラインアイテムが元帳に存在する場合、ユーザは確認通知または証明スタンプが有効であるという肯定通知を獲得する。有効な有効化スタンプまたは証明スタンプのインストールは、公開キーとプライベートキーの組み合わせを利用することによって可能になる場合があり、これは、上記のようにオンラインブランド保護システムの運営者によって提供される。

【0057】

本発明のいくつかの実施形態は、ウェブブラウザ、アドオンモジュール、プラグインモジュール、拡張モジュール、またはその他の好適なモジュール、として任意選択で実装された、または、これらを含んだ、システム、方法、デバイス、アプリケーション、モバイルアプリケーションもしくは「アプリ」を含み得、これにより、ブランド所有者または他の第三者は、オンラインアイテムを介したオンライン欺瞞および／または不正取引および／または不正なオンライン活動および／または偽造グッズおよび／または模倣グッズおよび／または非純正グッズのオンライン販売、および／または「フィッシング」攻撃、および／または不正または違法または不合理または海賊版コンテンツを、そのような検出された事件およびそのようなブランド侵害のオンラインアイテム、およびそのような不正なオンラインアイテムについて、真正なブランド所有者に通知を提供するのではなく、その代わりに、またはそれに加えて、特に、オンラインの目的地を訪問したり、オンラインアイテムとやり取りしたり、オンラインアイテムにアクセスしたり、またはオンラインアイテムからサービスや商品をオンラインで購入することを検討したり、デジタルコンテンツをダウンロードまたは取得したりすることを検討しているエンドユーザに警告する方法で、検出、防止、削減、排除および／または修正することができる。

【0058】

いくつかの実施形態では、報奨金報酬機構を利用して、エンドユーザがシステムに、ウェブサイト、ウェブページ、ドメイン名またはドメイン、特定の製品、ハイパーリンク、リンク、トレント、アイテムへのポインタ、「アプリ」またはアプリケーションについて報告する動機を付与することができ、それらは、不正なオンラインアイテムまたは欺瞞オンラインアイテムまたは不正な活動または海賊版コンテンツまたは非純正グッズまたは偽造グッズまたは他の不合理なアイテムに関連付けられている（または助長または提供している）と、エンドユーザが疑っている、またはエンドユーザにわかっている。報奨金報酬機構は、任意選択で、デジタル通貨または暗号通貨（たとえば、ビットコイン、イーサリアムなど）の形態でエンドユーザに報酬を提供できる。

【0059】

いくつかの実施形態では、群衆の知恵および／または複数のエンドユーザからの集約されたフィードバックは、特定のオンラインアイテムが不正であること、または逆に、特定のオンラインアイテムが不正ではない、または本物である、または信頼できるという追加の情報層として、または指標として、分析および／または生成されおよび／または利用され得る。

【0060】

いくつかの実施形態では、証明スタンプまたは有効化スタンプまたは真正性スタンプは、特定のウェブサイトまたはウェブページまたは「アプリ」などの特定のオンラインアイテムに関して、または、そのような宛先を通じて販売または消費の申し出がされている特定の商品またはサービスに関してさえシステムによって生成され、エンドユーザおよび／または彼のウェブブラウザまたは彼の電子デバイス（ラップトップ、パーソナルコンピュータ、スマートフォン、タブレット、スマートウォッチなど）に示してもよい。任意選択で、特定のオンラインアイテムに付与された真正性スタンプまたは確認スタンプを格納および／または有効化するために、ブロックチェーンベースのデータセットまたはデータ構造を使用できる。

【0061】

本発明は、革新的な分散型アンチ詐欺プラットフォームおよびシステムを提供し、不正なウェブサイト、オンライン偽造販売、および他のタイプのオンライン詐欺に達するたびにユーザに警報することができる。このシステムは、偽造や海賊行為のコストが高い電子商取引およびオンライン市場に信頼をもたらす可能性がある。システムは、フィッシング、欺瞞、ブランドジャッキング、およびその他の詐欺にあふれている暗号通貨業界に焦点を合わせるように構成できる。このシステムは、詐欺および暗号化取引の有効化に対する警報をユーザに提供する。システムは2つの知能のソース、すなわち、コミュニティと共有しているユーザによる潜在的な詐欺に関するレポートと、AI搭載サイバーインテリジェンスのプロバイダを使用する場合がある。両方のソースからの情報はブロックチェーンに記録され、ブロックチェーンは、既存のブロックチェーンの上または一部として（または新しいブロックチェーンとして）起動でき、警報と有効化のソースとして使用できる。

10

【0062】

分散型プラットフォームには、コミュニティのメンバに潜在的な詐欺を報告するよう奨励するために、会社、組織、ユーザが作成した報奨金が含まれている。暗号通貨トークンは「信頼のトークン」である。それは、コミュニティの合意に達した後、オンラインウェブサイトで行われた取引が、プラットフォームによって信頼されているとマークされることをユーザに保証する。

【0063】

このプラットフォームは、種々の利害関係者を1つのエコシステムに統合し、これらの利害関係者には、ユーザ、会社、AI搭載サイバーインテリジェンスプロバイダ、保証プロバイダ、および施行サービスプロバイダが含まれる。プラットフォームは、インターネットを監視し、種々のオンライン脅威の潜在的なリスクを分析するための堅牢なテクノロジーを活用する場合がある。このプラットフォームは、AI搭載サイバーインテリジェンスのプロバイダによって使用される可能性がある。

20

【0064】

出願人は、デジタル時代が多くの点で我々の生活を変えたことに気付いていた。進行中の情報革命とデジタル変革の急速なペースは、前例のないレベルと新しいタイプのサイバー犯罪の触媒となっている。今日のほとんどのサイバーセキュリティソリューションは、基本的に組織の管理下にある組織とそのITインフラストラクチャに焦点を当てている。しかしながら、インターネットでは、組織の直接的な管理下でない領域で種々の脅威が展開する可能性があった。不正な活動、フィッシング、オンライン偽造販売、およびその他の詐欺は、絶え間なく変化するオンラインプラットフォームとソフトウェア／ハードウェアインフラストラクチャによって急速に展開する種々の種類のオンライン詐欺である。これは、すべてのオンライン業界にわたって難しい問題であるが、暗号通貨業界は集中管理と規制のない、分散モデルに基づいているため、さらに深刻な問題に直面している。ほとんどの場合、不正であるかどうかにかかわらず、いったん金融取引が行われると、それらを取り消す、元に戻す、またはキャンセルすることはできない。

30

【0065】

これまでこれらの問題に対処するために開発されたソリューションは、会社および組織が最初にそれらを検出し、次にインターネットからの削除を施行する（たとえば、それらを取り壊す）ことによってこれらの詐欺と戦うのに役立つことに焦点を当ててきた。残念ながら、デジタル犯罪は盛んであるが、政府および法施行当局からの有意義な対応はまだ行われていない。これらの詐欺は衰えることなく増殖し続け、個人と会社の両方に等しくかなりのリスクをもたらし続けている。

40

【0066】

今日のインターネットエンドユーザにとって、サイバーセキュリティの主なレイヤーはアンチウイルスとアンチスパムである。既存のソリューションは、会社および組織にサイバー欺瞞の基本的または部分的な保護を提供するが、今日のインターネットのエンドユーザと消費者は、展開し続けるオンライン詐欺に対する保護を何も持っていない。特にサイバー欺瞞の影響を受けやすい暗号通貨業界の台頭により、今日のインターネットエンド

50

ユーザは、さらに大きな金融的リスクおよびその他のリスクに直面している。

【0067】

本発明は、革新的な分散型アンチ詐欺プラットフォームおよびシステムを提供する。それは、影響を受けるすべての関係者がこれらの問題に取り組み、オンライン取引に自信と信頼を作成することを可能にするエコシステムを作成する。例証的な実施形態では、暗号通貨業界に信用が提供され、それにより、より多くのユーザが市場に参入できるようになる。市場が展開するにつれて、本発明のソリューションは、電子商取引およびオンラインエコシステム全体に対応するように適合または構成され得る。このシステムは、フィッシング、欺瞞、偽造、その他の詐欺を含むオンライン詐欺についてユーザに警報するソリューションをユーザに提供する。分散型プラットフォームは、ブロックチェーンに格納された2つのデータソース、すなわち、ユーザが作成した潜在的な詐欺に関するレポートと、AI搭載サイバーインテリジェンスプロバイダに基づいている。

10

【0068】

本発明のシステムは、コミュニティの使用および利益のために潜在的な詐欺を報告するユーザに、(a) システムの運営者、および／または (b) 自社のブランドに関連するそのような報告を奨励することに関心のある会社および組織、および／または動機を提供したい他の利害関係者または参加者（たとえば、システムの恩恵を受け、数百ドルの費用がかかる可能性のあるオンライン詐欺を回避した別のエンドユーザ、政府機関または当局、法施行機関または当局、公正取引またはより良い商習慣をサポートするプライベートまたはコミュニティ組織、および／または他の参加者または利害関係者）から報いることができる。

20

【0069】

システムのユーザは、自分のオンライン取引に信頼と自信を得ることができる。さらに、トークンを使用することを選択した人のために、プラットフォームは、本発明の「プラットフォームによって信頼される」とマークされたオンラインアイテムに関して行われた取引の保証を提供することができる。

【0070】

本発明の暗号通貨トークンは「信頼のトークン」である。トークンは、ユーザが作成した詐欺レポートに最初に価値を提供し、次に、プラットフォームがそれらのレポートに基づいて提供することを保証することにより、信頼の価値を表す。

30

【0071】

プラットフォーム向けの第1のAI搭載サイバーインテリジェンスプロバイダは、インターネットを監視し、種々のオンライン脅威の潜在的なリスクを分析するためのテクノロジーを利用することができる。このシステムからのサイバーインテリジェンス情報は、会社がオンライン詐欺および欺瞞と戦うために使用される場合があり、プラットフォームを介して一般的な個人インターネットユーザも利用できる場合がある。

【0072】

このプラットフォームは、これまでにないオンライン詐欺と戦うための群衆の知恵をさらに追加する。これにより、オンライン詐欺、欺瞞、および偽造との戦いにコミュニティが関与できるようになり、関与は信用のトークンである暗号通貨によって動機付けられる。

40

【0073】

このシステムとプラットフォームは、個人インターネットユーザに役立つだけでなく、すべての利害関係者、会社、組織、ソリューションプロバイダ、法施行機関、その他のエンティティにも利益をもたらす。種々のニーズまたは役割を満たすことに基づいて、すべての利害関係者間の同盟関係を作成する、すなわち、それは、ユーザには自信を、会社には侵害の阻止に役立ち、ソリューションプロバイダには情報と収益化のオプションを提供する。

【0074】

したがって、システムは、プラットフォームとその信頼トークンに基づいて、信頼の経済を作成する可能性がある。デジタル価値を振り替える手段であるブロックチェーンテク

50

ノロジーは、オンライン取引におけるコミュニティの信頼の価値を確立し、それを収益化するためにシステムによって利用される。このシステムは、4つのコンポーネントまたは柱、分散した信頼の投票、信頼のコンセンサス、技術に基づく信頼の分析、およびそれらに基づく保証、に基づいている可能性がある。これらは、オンライン取引に自信と信頼を注入するために、システムがコミュニティにもたらす価値の柱である。

【0075】

このシステムは、世界初のアンチ詐欺プラットフォームである。それは、オンラインブランド保護、アンチ偽造、およびアンチ欺瞞のために、堅牢で革新的なAI搭載サイバーインテリジェンスシステムを利用している。このシステムは、インターネットを走査して動的に監視し、ウェブサイト、電子商取引市場（たとえば、Amazon、eBay）、ソーシャルメディアプラットフォーム、アプリ、およびクリック課金（PPC）広告で、欺瞞、偽造、商標侵害などを含む、種々のタイプの詐欺を見つける。

【0076】

このシステムは、銀行、金融、暗号通貨、保険、消費財、ファッション、製薬、エンターテインメント、テクノロジー、IT、電子商取引、ゲーム、ソフトウェア、非営利団体など、種々の業界のブランド所有者にサービスを提供する。プラットフォームは、任意選択で、「サービスとしてのソフトウェア」（SaaS）として実装できる。このシステムは、オンラインブランド保護、アンチ欺瞞、およびアンチ偽造のための最高レベルのビジネスインテリジェンスを提供することにより、会社や組織がデジタルブランドを管理および保護する方法を改善する可能性がある。全体的なアプローチは、独自のテクノロジーと施行サービスの両方で構成されている。これらの機能により、オンライン詐欺の状況とこの業界のプレーヤーの特性を深く理解できるようになる。ブランド保護の分野で蓄積された知識および技術は、本発明の技術および申し出のビルディングブロックを提供するために活用され得る。

【0077】

出願人は、インターネットの成長と発展が新たなリスクを作成していることに気付いていた。これらのリスクには、欺瞞、フィッシング、偽造、知的財産権の違反、ブランド名の搾取、なりすまし、個人情報盗難、模倣、中傷、顧客の誤解などが含まれる。オンライン「詐欺」は、欺瞞、フィッシング、偽造販売などにデジタルメディアを使用する複数の方法を表す一般的な用語である。偽造グッズや海賊版グッズの被害は甚大である。オンラインでのブランドの乱用と偽造品の販売は、どちらも急激に増加しています。これは、電子商取引の成長とハッカーの高度化に牽引され、あらゆる規模の会社にとって大きな脅威となっている。従来のサイバーセキュリティの脅威の増加、新しい汎用トップレベルドメインの導入、オンライン市場の進化など、インターネット分野の他の同時変化により、問題は加速している。

【0078】

出願人はまた、暗号通貨エコシステムには多くの詐欺があることに気付いていた。暗号通貨業界の急速な成長により、この業界に不慣れで、したがってオンラインの暗号通貨詐欺に対してより脆弱な人々が何百万人にも達している。発行されたブロックチェーンベースのウォレットの数は、暗号通貨スペースに参加する新しいユーザの数の増加に伴い、劇的に増えている。暗号通貨業界では、業界全体が集中型のガバナンスと規制のない分散モデルで機能しているため、フィッシングや欺瞞を含む種々のタイプのオンライン詐欺がさらに大きな課題を引き起こしている。ほとんどの場合、不正であるかどうかにかかわらず、いったん金融取引が行われると、それらを取り消す、またはキャンセルすることはできない。2018年までにICOで調達された資金の10%以上が盗まれたと見積もられている。フィッシングは、ICO中の資金窃盗の一般的な形式である。その人気は、そのシンプルさと効果に起因している。詐欺師は、ウォレットへの送金をリクエストするか、秘密キーを投資家のウォレットに騙し取る。

【0079】

出願人は、特にICOと暗号通貨エコシステムを一般的にリスク、盗難、欺瞞、詐欺に

対して脆弱にするパラメータがあることに気付いていた。(a) 大金とガバナンスがないことが不正者を引き付ける。ICO市場のスピードと規模は、ハッカーの注目を集めている。ハッカーは、大需要、集中的な権限の欠如、ブロックチェーンランザクションの不可逆性、および情報の混乱によって引き付けられる。(b) セキュリティ上の低重視：暗号通貨会社の創設者は、資金調達段階に集中し、しばしばセキュリティを優先することなく投資家を引き付けることがよくある。この状況が詐欺師によって搾取されている。(c) それが大きいほど、それは詐欺師にとって魅力的である。暗号通貨の誇大宣伝と、成功したICOの広範なメディア報道は、投資家と詐欺師の両方を問わず、この市場に誰もが注目を集めている。(d) ハッキングは、間接的な損失、たとえば、プロジェクトの評判の喪失や投資家の機密個人データの喪失などにもつながる。

10

【0080】

出願人は、信頼が、あらゆる経済、とりわけ暗号通貨などの新興経済機構において重要な要素であることに気付いていた。信頼の欠如は市場の成長を遅らせる可能性がある。より多くの人々が暗号通貨を使用するように引き付けるためには、暗号通貨の世界で取引を実行するユーザに、それらが意図したエンティティを実際に扱っていることを保証する必要がある。暗号通貨業界の持続可能な成長を可能にすると同時に、ユーザプールを早期の採用者からより広い公衆に拡大するために、信頼を育み、欺瞞を防止するソリューションを提供する必要がある。

【0081】

暗号通貨ユーザに対する詐欺の影響：すべての欺瞞事件は、市場への信頼の欠如に波及効果をもたらす。「信頼」は「達成」するのが困難でありながら「失う」ことが非常に簡単な品質であるため、信頼の欠如が転換点に達すると、発生期の暗号通貨エコシステムに固有のリスクと危険が壊滅的になる可能性がある。このような高まる危機への着実な歩みの証拠と、信頼の欠如における転換点が現れ始めている。データは、「暗号通貨詐欺」という用語を検索するユーザ数の驚くべき増加を示している。合理的なプロキシとして、これは暗号通貨コミュニティの懸念の高まりと、信頼の欠如の増加を示している可能性がある。これは、暗号通貨の概念の浸透に壊滅的な影響を及ぼし、この虚弱で初期の業界の成長を阻害する可能性がある。

20

【0082】

暗号通貨エコシステムの一部としての詐欺：暗号通貨会社は、ICOプロセスから日常業務まで、ライフサイクルのすべての段階で多数の脅威にさらされている。その上、資金調達段階から「翌日」への移行にはさまざまなリスクが伴う。進行中の詐欺の可能性、欺瞞の試み、および盗難の例は、IOTAの事例で判明でき、このケースでは、約4,000,000ドルがプライベートウォレットから盗まれ、これはネットワークまたはウォレットの欠陥の結果ではなく、欺瞞の結果であった。正当なIOTAシードジェネレータであるに見えるフィッシングウェブサイトを使用することで、詐欺師は長期間にわたって多数のシードを収集することができた。彼らはコミュニティの信頼をえじきにし、ページを注意深く最適化して検索エンジンの結果で上位に見えるように時間を費やし、疑いを持たないコミュニティメンバの目に詐欺をさらに正当化した。脅威の進化、詐欺師の複雑さと巧妙さのレベルは、アンチ詐欺の取り組みの関連性を必要性にまで広げる。

30

【0083】

痛みはユーザと会社の両方に関係がある。本発明のシステムは、すべての関係者の利益のために相乗効果を作成するエコシステムを作りながら、すべての利害関係者に役立つという独自の立場にある。これは、事実上の標準として暗号世界への変換を支援し、ユーザの自信を確立するのに役立つ。

40

【0084】

例証的な実施形態では、システムは、複数のエンティティ、たとえば、暗号通貨や暗号コインなどの製品を購入したいエンドユーザ、製品または暗号通貨を販売または発行する会社、1つ以上のAI搭載サイバーインテリジェンスエンティティ、報告ユーザのコミュニティ、1つ以上のコミュニティ施行者またはコミュニティベースの施行エンティティ、

50

購入した製品または暗号通貨の真正性に関して、および／または取引全体に関して、および／または取引の少なくとも特定の部分に関して、保証人または被保証人を提供する保証人プロバイダまたは被保証人プロバイダを含む。

【0085】

本発明の分散型アンチ詐欺プラットフォームは、ユーザが完全な自信をもって日常のオンライン取引を実行することを可能にする。プラットフォームには、アプリケーション、ブロックチェーン（たとえば、新しいブロックチェーン、または任意選択で起動した既存のブロックチェーン）、AI搭載サイバーインテリジェンスプロバイダ、施行サービスプロバイダ、保証プロバイダ、報奨金、および信頼スタンプが含まれる場合がある。エコシステムには、アプリケーションのエンドユーザだけでなく、自社のブランド、ウェブサイト、投資、およびクライアントを保護しようとしている会社や組織も含まれる。

10

【0086】

アプリケーションには3つの主な機能がある。（a）欺瞞、フィッシング、偽造品の販売などの実行を試みる詐欺のオンラインアイテム（ウェブサイト、ソーシャルメディアの投稿、市場のリ스팅など）に、ユーザが達するときに、ユーザに警報する詐欺に対する警報。警報は種々の詳細レベルで提供される。一般的潜在的なリスクスコアと、ユーザのレポートとAI搭載サイバーインテリジェンスプロバイダに基づく特有のスコアが表示される。（b）ウォレット番号とウェブサイトに一致する有効化プロセスを実行する暗号化取引の有効化。ユーザが暗号通貨取引を実行しようとするとき、取引が行われるウォレットが、ウェブサイトの有効化ウォレットと一致しないとき、アプリはユーザに警報する。これは、トークンを盗もうとする種々のタイプのハッキングや欺瞞の事例からユーザを保護する。取引有効化プロセスは、ブロックチェーンに基づいてアプリによって実行される。（c）報告詐欺：このアプリケーションを使用すると、ユーザは、潜在的な詐欺（欺瞞、フィッシング、偽造販売など）の疑いがあるオンラインアイテム（ウェブサイト、ソーシャルメディアの投稿、電子商取引市場の特有のリ스팅など）を報告できる。ユーザは、信頼できると考えるウェブサイト、ソーシャルメディア投稿、または市場のリ스팅に肯定的なレポートを提供することもできる。ユーザが提出したレポートはブロックチェーンに記録され、公衆に表示される。

20

【0087】

詐欺報告機能は、分散型のアンチ詐欺エコシステムにおける重要なコンポーネントである。ユーザによるレポートは、詐欺と闘い、詐欺を認識するために共同で行動するコミュニティを作成する。ユーザによって提供されたレポートは、ブロックチェーンに記録され、特有のオンラインアイテムもしくは製品、または宛先もしくはURLもしくはURI、またはウェブサイトもしくはウェブページの状態、または暗号化コインもしくは暗号化通貨に関するコンセンサスを作成するために集約され、ユーザのコミュニティ全体と共有される。

30

【0088】

何らかの詐欺の対象となっている、またはオンラインアイテムが詐欺の疑いのあるユーザは、アプリを通じて潜在的な詐欺を報告できる。レポートは、種々のレベル、たとえば基本レポートであって、「詐欺を報告」などのボタンをクリックし、任意選択で、詐欺の重大度に関するスコアも（たとえば、1つ星～5つ星のスケールで）提供する基本レポート、または詳細レポートであって、詐欺のタイプ（フィッシング、偽造、不実表示など）、詐欺の対象となっているブランド／会社、詐欺であると疑われる理由（たとえば：暗号ウォレットの番号が本物ではない、ウェブサイトの所有者が会社のウェブサイトの所有者と同じではない、ウェブサイトがメインのウェブサイトのホスティングとは無関係のホスティングプロバイダでホストされている、提供されている製品が偽造である、など）、特有の詐欺事件のレポート（日付、被った損害など）のような追加のデータを提供する詳細レポートで提供される。

40

【0089】

レポートはブロックチェーンに格納され、公衆に、または、いくつかの実施形態では、

50

少なくともユーザのグループ（たとえば、レポートにアクセスするため、またはそれらをデコードするために解読キーを購入するプレミアム加入者）に、さらされ、またはアクセス可能になる。集計されたタイプとレポートの数は、アプリケーションの警報セクションでシステムのユーザに表示される場合がある。詐欺の疑いのあるオンラインアイテムを調査し、追加の入力を提供するようにユーザを奨励するために、プラットフォームマネージャーは、当初に報告され、ユーザがまだ合意に達していない、報告された詐欺のリストをウェブサイトに公開し得る。

【0090】

報告プロセスで「スパム」を防止することを意図された方法として、任意選択で作業証明の概念に基づいて詐欺を報告するユーザは、トークンを預ける必要がある場合がある。実際の金額はプラットフォームマネージャーによって時間とともに変化する可能性があるが、詐欺の報告を申請するにはわずかな料金（たとえば、50セントまたは1ドルに相当する金額）が必要である。これは、種々のタイプのスパム活動、または報告された詐欺のデータベースにノイズまたは「誤ったデータ」を注入する活動を防ぐのに役立つ。

【0091】

本明細書に記載されている合意プロセスの一部としてレポートが真実であり、ユーザが報奨金から報酬を得る資格があると判明した場合、預けられトークンは、（たとえば、報奨金の受け取りに加えて）ユーザに返される。レポートが間違っている、正しくない、または誤っていることが判明した場合、預けられたトークンは、本明細書に記載されているように一般的な報奨金に追加され、報告ユーザには返されない。

【0092】

アカウントを開設すると、ユーザにはトークンのクレジットが付与され、初期費用なしで、最初の量の詐欺レポート（たとえば、最大5つのレポート）が許可される。これらのトークンは、ブロックチェーンでマークされ、ユーザがそれらを取引、交換、または振替できないようにロックされる場合がある。これらの最初の「無料」レポートの後、ユーザは、詐欺の報告を続行するためには市場でトークンを取得または購入する必要がある。

【0093】

採点システム：アプリによって提供される警報は、潜在的なリスクスコア、たとえば、高リスク、中リスク、低リスクの形式になる。信頼できるウェブサイト、ソーシャルメディアページ、または市場のリ스팅はアプリによって「信頼できる」とマークされる。採点アルゴリズムは、サイバーインテリジェンスプロバイダのAIおよびビッグデータエンジンと、アプリのユーザから収集されたクラウド知恵との組み合わせに基づいている。ユーザには、AI搭載スコアと群集ベースのスコアとともに一般的なスコアが提示され、リスクスコアのソースをよりよく理解できるようになる。群衆ベースのスコアは、一定のオンラインアイテムについて、それが詐欺であるか信頼できるかどうかの、ユーザの合意に達することによって生成される。群集ベースの採点に関して、合意に達した後、矛盾するレポートが（たとえば、最小閾値数またはパーセンテージを超えて）提出された場合、それらは再採点プロセスを開始またはトリガーする可能性がある。

【0094】

報奨金は、ユーザによる潜在的な詐欺の報告を奨励し、報いるために作成される。報奨金は、以下のもの、すなわち、（a）一般的な報奨金に寄付される、（下記の保証が含まれる）プレミアム寄付金に寄付したユーザが支払ったトークンの20%、および合意プロセスでレポートが正しくないと判明したユーザが預けたトークンの80%などの一般的な報奨金によって寄付されるトークンを使用して作成される。（b）ブランド報奨金—とりわけ、そのブランドに関連する詐欺を報告するようユーザを奨励することに関心のある会社または組織が、それに応じて報奨金を作成することができる。ブロックチェーン、アプリ、有効化プロセス、報奨金プログラムなどを含む、エコシステムと運営を維持するために、会社や組織が作成した報奨金の20%が運営コストに対して支払われる。（c）詐欺を報告するように他のユーザを奨励することに関心があるユーザが、コミュニティ報奨金を開始することができるコミュニティ報奨金。コミュニティ報奨金は、一定のブランド、

または任意のその他のタイプの名前や原因を保護することを指す。

【0095】

報酬の原則：報奨金は、報告されたアイテムごとの報酬額、レポートのタイプとその報酬（ウェブサイト詐欺、ソーシャルメディア詐欺など）、報告されたアイテムについてユーザごとの最大報酬、合意を作成し、賞金を適用するために必要なレポートを作成したユーザの数など、事前定義されたパラメータに基づいて、潜在的な詐欺について報告するユーザ間で分配される。これらのパラメータの定義は、一般的な報奨金と各会社または組織のブランド報奨金、および各ユーザのコミュニティ報奨金によって、そのために定義される。これらの定義は、今後変更される可能性がある。通常、報奨金は、潜在的な詐欺を報告した最初のユーザに、レポートを有効化して合意作成プロセスに参加する他のユーザよりも高額で報われるように構成される。詳細レポートは、ユーザがレポートでより多くの情報を提供できるように奨励し、コミュニティがレポートの有効性をよりよく理解し、合意作成プロセスを迅速化できるようにするために、基本レポートよりも高額で報われる。サイバーインテリジェンスプロバイダに知られていない潜在的な詐欺のユーザによるレポートは、サイバーインテリジェンスプロバイダにすでに知られた潜在的な詐欺（つまり、すでにスコアレベルがあり、アプリケーションで警告されているオンラインアイテム）のレポートよりもより多く報われる。サイバーインテリジェンスプロバイダによって詐欺ではないと既に評価されたウェブサイトを実効化するレポートは、詐欺に関するレポートよりも低いレベルの報酬で報われることがある。

10

【0096】

合意プロセス：詐欺レポートに割り当てられた報奨金を分配するには、合意に達する必要がある。合意には、プラットフォームに報告するユーザ間の同意が必要であり、任意選択でサイバーインテリジェンスプロバイダのスコアを遵守することもできる。合意に達するために必要なユーザ数は、（一般的な報奨金、会社、組織のブランド報奨金について）報奨金マネージャーによって定義される。この数は、報告されているオンラインアイテムのタイプ（ウェブサイト、ソーシャルメディアの投稿であるかどうかなど）に基づいて変わる場合がある。

20

【0097】

例示のみを目的として、群集とAI搭載サイバーインテリジェンスプロバイダの間で合意に達するプロセスに適用される可能性のあるシナリオを以下に示す。この例示を簡略化するために、スコアは、赤（詐欺）と緑（信頼済み）に分けられている。（a）合意に到達：群衆とプロバイダが達したスコアの間に合意があるとき、つまり、プロバイダのスコアが赤で群衆のスコアが赤、またはプロバイダのスコアが緑で群衆のスコアが緑のとき、合意に達している。目標は詐欺を報告することである。プロバイダの緑スコアの場合、緑の群衆レポートには、一般的な報奨金からの報奨金は付与されない。（b）合意なしのシナリオ1、プロバイダのスコアが赤、群衆スコアが緑：この場合、プロバイダの赤いコアのため、詐欺警報が引き続き見える。詐欺師がシステムを悪用しようとするケースを回避するために、オンラインアイテム（たとえば、ウェブサイト）を所有または管理するエンティティが正当なエンティティであり、赤いプロバイダに異議を唱えたい場合、エンティティは、有効化プロセスが実行される信頼スタンプの要求を申請する必要がある。信頼スタンプの有効化プロセスが終了した場合、緑の群衆レポートに報奨金が付与される。（c）合意なしのシナリオ2、プロバイダのスコアが緑、群衆のスコアが赤：この場合、緑のスコアはあるが前もって有効化されていない（つまり、信頼スタンプがない）ウェブサイトに対して、ユーザから詐欺レポートが提供されるとき、サイバーインテリジェンスプロバイダに警報が提供されて、緑のスコアを実行および有効化する。

30

40

【0098】

いくつかの実施形態では、ユーザが、信頼スタンプを有するウェブサイトに対して報告を申請する場合、ユーザは所定の金額を預けることが要求される。このようなレポートが申請されると、信頼スタンプの有効化手順と同様の調査手順がトリガーされ開始される。この場合のレポートの一部としてのユーザによる供託の要件は、正当な組織を傷つけることに関

50

心があるユーザによる誤ったレポートを防ぐことを意図している。調査プロセスでレポートが偽であることが見つかる場合、供託されたトークンは報告ユーザ（複数可）に返されない。調査プロセスでレポートが真実であることが見つかる場合、供託されたトークンが報告ユーザ（複数可）に返され、報奨金が報告ユーザ（複数可）に分配される。調査プロセスのプロセスに使用されるトークンは、このような場合のために割り当てられた報奨金から取得される。

【0099】

セキュリティ：システムは、自動化されたスクリプトまたは「ボット」による悪用、または報奨金を搾取するか、偽陽性を提供するか、誤報により危害を加える意図のあるユーザを防ぐためのセキュリティ対策を実装する場合がある。報告プロセスでスパムを防止することを意図した方法は、作業証明の概念と同様に、詐欺の報告に対してユーザがわずかな金額を支払うことを要求する。

【0100】

信頼スタンプは、たとえば、電子商取引市場、ソーシャルメディアアカウントもしくはページなどの特有のリスティングを含む、ウェブサイトやウェブページなどの検証および有効化されたオンラインアイテムによって提供される証明スタンプを意図している。スタンプを押すと、ユーザは到達したウェブサイトが本物のウェブサイトであり、フィッシングや欺瞞のウェブサイトではないこと、または特有の市場のリスティングが本物であることなどを知ることができる。信頼スタンプを得るには、ウェブサイトの所有者、市場の販売者、ソーシャルメディアアカウントの所有者などがシステム運営者による有効化を申し込む。有効化プロセスは、オンラインアイテムの背後にある組織の有効化、住所、電子メール、電話番号、法人設立文書、主要人物、商標文書、現在および／または過去のドメイン所有権記録、証明およびパートナーシップ（たとえば、一定の販売者がブランドまたは一定の製品の公式販売者または流通業者であるかどうか）などの有効化を含む、Know Your Customer (KYC) プロセスと同様のプロセスで、種々の情報をチェックするAI搭載サイバーインテリジェンスプロバイダ有効化担当者によって実行される。プロセスには、オンラインアイテムの所有者（たとえば、ドメイン名の登録者）が実際に所有権を主張するエンティティであるという検証が含まれる場合がある。要件は、有効化されているオンラインアイテム（ウェブサイト、ソーシャルメディアページ、市場の販売者またはリストなど）に基づいて変更される場合がある。スタンプは、AI搭載サイバーインテリジェンスシステムの高い信頼スコア（または低いリスクスコア）と、群衆による高い信頼スコア（または低いリスクスコア）を有するオンラインアイテムにのみ付与できる。プロバイダ有効化証担当者に加えて、有効化プロセスごとに2人の公的有効化担当者が必要になる。公的有効化担当者は、プロバイダ有効化担当者に必要なものと同様の一連の有効化を実行する必要がある。

【0101】

2人の公的または群衆有効化担当者が担当者の有効化を実行すると、信頼スタンプが申請者に付与され、プロバイダ有効化担当者によって収集された有効化ドキュメントと群衆有効化担当者が、ブロックチェーン上の公衆と（または少なくともユーザのグループと）共有される。有効化スタンプを申請する当事者は、トークンを使用して有効化プロセスの料金を支払う必要がある。申請者が支払ったトークンは、システム管理者、AI搭載サイバーインテリジェンスプロバイダ、および公的有効化担当者の間で分けられる。特有の有効化の有効化担当者になるために、任意のアプリケーションユーザが申請できる。担当者は、公開される先着順のプロセスで、または、（たとえば、特定の地理的地域に居住している、または特定の言語に習熟している、など）他のルールまたは基準に基づいて選ばれる。ただし、担当者は限られた期間内に有効化を実行する義務があり、そうでない場合、有効化は、並んでいる次のユーザに移動される。特有の有効化の有効化担当者になるための申請は、自分に関して完全なKYCプロセスを実行したプレミアムユーザのみが利用できる。

【0102】

信頼スタンプは暗号化され、ブロックチェーンに格納される。スタンプをブロックチェーンに格納することで、証明データの改ざんを防ぎ、システムのSDKを使用するブラウザとアプリケーションが、ユーザに提示されるスタンプの真正性を検証できるようになる。信頼スタンプの真正性と有効性は、ブロックチェーンのデータセットまたはデータベースに接続し、オンラインアイテムが元帳にあるかどうかをチェックすることでチェックできる。このようなブロックチェーンデータセットまたはデータベースのセキュリティ保護された構造により、オンラインアイテムの（有効な信頼スタンプを提示する資格がある認定オンラインアイテムのリストから、またはリストへの）削除または追加は、ブロックチェーンのノードの大部分が、このような変更に同意するか、使用されている特定のブロックチェーンプロトコルに基づいて「合意」に達した場合にのみできる。これにより、信頼スタンプの誤った提示が防止される。

10

【0103】

信頼済みウォレットスタンプ：信頼スタンプと同様に、システムは、信頼済みウォレットスタンプを、ウェブサイト、市場の販売者、ソーシャルメディアアカウントなどの検証済みエンティティに発行する場合がある。信頼済みウォレットスタンプには、一定の暗号通貨ウォレットの所有者が検証される有効化の追加レベルがある。スタンプは、到達したウェブサイトが一定の会社の本物のウェブサイトであり、フィッシングや欺瞞のウェブサイトではないこと、または特有の市場のリストが本物であることをユーザに検証するだけでなく、トークンを振り替えるつもりウォレットが、実際にトークンの振替先のエンティティによって所有されていることも検証する。

20

【0104】

たとえば、ユーザが信頼済みのウォレットスタンプのあるウェブサイトを使用および／またはウェブサイトへ到達した場合、本発明のアプリまたはシステムは、ユーザがトークンを送信するつもりウォレット番号が、ウェブサイトの所有者が所有するものとして実際に有効化されたウォレット番号であることを検証する。ユーザが暗号通貨を送信するつもりウォレットが、ユーザが閲覧しているウェブサイトと一致しない場合、ユーザはアプリまたはシステムから警報を獲得する。さらに、ユーザがトークンを送信するつもりエンティティについてシステムによって認められ検証されたデータが、ユーザに提示され、ユーザが標的エンティティをさらに検証できるようにする。信頼スタンプと同様に、信頼済みウォレットスタンプのデータは暗号化され、ブロックチェーンに格納される。SDKの統合を通じて有効化ブロックチェーンをサポートするアプリ、ウォレット、アプリおよび／またはブラウザを使用するユーザは、暗号通貨の振替先のウォレットが、意図したエンティティと一致しない場合に警報される。

30

【0105】

信頼済みウォレットスタンプと、ウォレットが一致しない場合に作成されたアラートにより、ユーザは、公開されたウォレット番号が改ざんされているウェブサイトへのハッキングなど、さまざまな種類の詐欺や欺瞞の対象となることを防ぐのに役立つ。

【0106】

上記で説明したように、ウォレット所有者の有効化は、信頼スタンプに対して実行された同様の有効化の別のステップになる。種々のセキュリティ対策を使用して、プロバイダ有効化担当者と公的有效化担当者は、ウォレットの所有者を検証する。いくつかの実装形態では、信頼済みウォレットスタンプを獲得することができる有効化エンティティは、ウェブサイト、市場の販売者、ソーシャルメディアアカウントなどのオンラインアイテムに限定されず、むしろ、信頼済みウォレットスタンプは、プライベートな人々または組織に提供される場合もある。

40

【0107】

アプリとSDKを含むエコシステムの一部としての信頼済みウォレットスタンプの実装形態により、エンティティとユーザの信頼済みネットワークの作成が可能になり、詐欺や欺瞞を防ぎ、暗号通貨コミュニティに安全で信頼される取引ができるようにする。

【0108】

50

システムは、種々の形式、たとえば、モバイルアプリ、デスクトップアプリ、ブラウザ拡張機能またはアドオンまたはプラグイン、SDKの他のアプリケーション、ソフトウェア（クライアント）またはスタンドアロンのクライアント側ソフトウェア、JavaScriptウィジェットまたはコード、リモートサーバに常駐し、ウェブページ、ウェブサイト、ウィジェット、またはモバイルアプリケーションによって追加、呼び出し、または呼び出されるJavaScript/HTML5/CSSコード、上記のアプリケーションをまだインストールしておらず、ウェブサイトを通じてシステムのデータベースを使用してクエリを実行できるユーザ向けのシステム管理者のウェブサイト、保護サーバーネットワークの一部としてプラットフォームまたはアプリケーションを使用し、潜在的な詐欺についてユーザに警報する機能をインターネットサービスプロバイダまたは組織に提供するソリューションである、保護サーバーネットワーク、でユーザが利用できる場合がある。

10

【0109】

いくつかの実施形態では、プラットフォームは、ユーザの閲覧を監視せず、ユーザの閲覧データを保存しない。これは、プラットフォームのプライバシーポリシーの主要な原則である可能性がある。アプリケーションは、各閲覧インスタンスのデータベースの特有の一時的なクエリに基づいて、潜在的な詐欺についてのみユーザに警報する。たとえば、保証が適用される取引に関連する場合など、明示的に要求され、明記されていない限り、クエリに関連するユーザデータは、いつでもシステムによって保存されない。

【0110】

信頼済みパートナーコミュニティ：このシステムは、オンラインコミュニティ全般と、具体的には暗号通貨コミュニティが、詐欺のない信頼済みの方法で毎日の取引とオンライン商取引を実行するのに役立つ。その結果、同じビジョンを共有し、そのユーザまたはコミュニティがAIを利用し、クラウド知恵ベースのアンチ詐欺プラットフォームをエンjoyできることに関心のある任意の正当な当事者を許可する可能性がある。そのため、システムは、アプリケーションプロバイダ、暗号ウォレットプロバイダ、ブラウザ、セキュリティソフトウェアおよびハードウェアベンダなどが、ソフトウェアに統合できるようにする種々のソフトウェア開発キット（SDK）を作成する場合がある。この統合により、これらのアプリケーション、ウォレット、ブラウザ、ソフトウェアなどのユーザは、潜在的な詐欺について使用中に直接アラートを獲得するようになる。具体的には、SDKをウォレットプロバイダに統合すると、信頼済みウォレットモデルの実装形態が可能になるため、ウォレットプロバイダのアプリケーション上の信頼済みウォレットへの取引を保証できる。

20

30

【0111】

本発明のプラットフォームは、AI搭載サイバーインテリジェンスプロバイダとしてブランドシールドシステムの1つ以上の機能を利用して、オンラインリスクのAIおよびビッグデータ分析を実行し、これは、サイバーインテリジェンスのコアソースであり、ユーザに詐欺に対する警報を提供する。このようなAI搭載サイバーインテリジェンスプロバイダは、AI搭載オンラインブランド保護およびサイバーインテリジェンスシステムであるか、これらを含む可能性があり、銀行、金融、暗号通貨、保険、ソフトウェア、IT、ゲーム、ファッション、製薬、スポーツ、消費財、旅行、自動車、非営利など、さまざまな分野において、組織が、（フィッシングやブランドジャッキングのタイプを含む）欺瞞、偽造、商標権侵害、海賊行為などを含む種々のタイプの詐欺と闘うのに役立つように動作する。人工知能（AI）、機械学習、およびビッグデータテクノロジーは、オンラインリスクの高度で自動化されたメトリック主導分析を実行する。その強力なテクノロジーは、ウェブサイト、市場、ソーシャルメディア、モバイルアプリ、PPC広告を含む、複数のプラットフォームにわたる欺瞞、偽造、商標侵害、ブランドの悪用などの詐欺を見つける。

40

【0112】

AI搭載サイバーインテリジェンスプロバイダは、たとえば、コンテンツとメトリックを分析し、アルゴリズムを使用してリスクのレベルに自動的に優先順位を付け、機械学習

50

を使用してアクションに基づいて結果を改善し、主要な詐欺師を見つけるパターン認識を実装し、予防的な施行ツールを含む。

【0113】

システムは、サービスソリューション（SaaS）としての寄付金ベースのオンラインソフトウェアであってもよい。それはまた、SaaSにサブスクライブする会社および組織に、1つ以上のオプションの施行および削除サービスを提供する。奥深い分析機能により、洗練されたメトリックベースの施行戦略が可能になり、専門チームに、ブランドへの最も有害な脅威と主要な悪用者に施行努力を集中させる機能を提供する。

【0114】

システムは次のモジュールを含む。（a）ウェブサイトモジュール—コンテンツ、ロゴ、すべてのccTLDおよびgTLDの侵害ドメイン名などを含むウェブ上の詐欺を監視する。（b）市場モジュール—自動化されたアルゴリズムベースのソリューションで、eBay、AliExpress、TAOBaoなどの市場での偽造販売を防ぐように監視する。（c）モバイルアプリモジュール—主要なアプリストアを走査し、悪用アプリを見つける。（d）PPC Adsモジュール—GoogleおよびBingの広告を走査して監視し、トラフィックを競合他社または偽造ウェブサイトへ誘導する詐欺師を特定する。（e）ソーシャルメディアモジュール—主要なソーシャルメディアプラットフォームを走査して、詐欺活動や偽造販売を見つける。

【0115】

詐欺を実行するウェブサイトの監視：システムはインターネットを走査して監視し、フィッシング、欺瞞、偽造、海賊行為、商標権侵害など、さまざまな種類の詐欺を実行するウェブサイトを見つける。システムは、不審なウェブサイトに関するデータを測定および収集し、（NLP自然言語処理を使用する）ウェブコンテンツ、SEOデータ、現在および／または過去の所有権記録を含むドメイン名、トラフィックと統計、検索エンジンの結果、ウェブサイトの技術と構造、メタタグとコーディング、ロゴの使用などの複数のメトリックを自動的に分析する。システムは、アルゴリズムと自動化されたメトリクス主導の分析を使用してリスクに優先順位を付ける。システムは、監視対象の各ウェブサイトへリスクスコアを提供する。これにより、最もリスクの高いウェブサイトへ注目して警報することができる。

【0116】

ソーシャルメディアの監視：このシステムは、Facebook、Twitterなどの主要なソーシャルメディアネットワークを監視して、ブランドのすべての使用を見つけ、潜在的に、詐欺やそれらへのリンクを実行したり、欺瞞やフィッシングを実行したり、偽造品を販売したり、商標を侵害したりするそれらへ高いリスクスコアを付与することによって、リスクに優先順位を付ける。システムは、侵害の疑いのある投稿、アカウント、ページ、人物、イベント、グループ、ショップなどの分析と優先順位付けを実行する。ウェブサイトモジュールと同様に、ソーシャルメディアモジュールでは、システムは複数のテクノロジーを使用して、詐欺師へ高いリターンを提供するウェブメトリックを分析する。システムは、（NLP自然言語処理を使用する）投稿、ページなどのコンテンツ、ソーシャルエンゲージメントデータ、アカウントとユーザ名、トラフィックデータ、検索結果、メタタグとコーディング、グラフィックアイテム内のロゴを特定し、データを優先順位付けと並べ替えに使用することによって開発された先端テクノロジーをカットするロゴの使用など、複数のメトリックを分析する。ソーシャルメディアモジュールは、アルゴリズムと自動化されたメトリック主導の分析を使用して、投稿、ページ、グループなどの潜在的なリスクに優先順位を付ける。システムは、監視されている各ソーシャルメディアアイテムへリスクスコアを付与し、これにより、最もリスクが高い投稿、ページ、グループなどに注目して警報することができる。

【0117】

市場監視：オンライン販売の大部分は、Amazon、eBay、AliBaba、TAOBaoなどの市場で行われる。多くの詐欺師は、これらの市場をプラットフォーム

10

20

30

40

50

ムとして使用して偽造製品を分配している。このシステムには、自動化されたアルゴリズムベースのソリューションが含まれており、市場を監視して潜在的な偽造品を見つける。システムは、種々の市場にわたって、侵害の疑いのあるリスティングの分析と優先順位付けを実行する。ウェブサイトモジュールと同様に、市場モジュールでは、システムは複数のテクノロジーを使用して、詐欺師に高いリターンを提供するウェブメトリックを分析する。システムは、（NLP自然言語処理を使用する）リスティングのコンテンツ、販売者名、リスティングと販売者の統計およびエンゲージメントデータ、検索結果、メタタグとコーディング、ロゴの使用など、複数のメトリックを分析する。市場モジュールは、アルゴリズムと自動化されたメトリック主導の分析を使用して、リスティングの潜在的なリスクに優先順位を付ける。システムは、監視対象の各リスティングにリスクスコアを付与し、これにより、偽造である可能性が最も高いリスティングに注目して警報することができる。

10

【0118】

モバイルアプリ監視モジュール：申請者は、モバイルアプリでの商標侵害、偽造品の販売、およびブランドの悪用が、ブランドに絶えず進化する脅威をもたらすこと気付いていた。モバイルアプリモジュールは、主要なアプリストアを走査して、種々のタイプの詐欺の実行が疑われるアプリに優先順位を付ける。システムは、侵害の疑いがあるアプリの分析と優先順位付けを実行し、システムは、（NLP自然言語処理を使用する）アプリの説明のコンテンツ、アプリ名、アプリの特徴、開発者の名前と統計、ダウンロード統計、ロゴの使用、ユーザの評価と再調査など、複数のメトリックを分析する。モバイルアプリモジュールは、アルゴリズムと自動化されたメトリック主導の分析を使用して、アプリの潜在的なリスクに優先順位を付ける。システムは、監視対象の各アプリにリスクスコアを付与し、これにより、詐欺であるリスクが最も高いアプリに注目して警報することができる。

20

【0119】

PPC広告の監視：申請者は、多くの詐欺が、詐欺を実行するオンラインページにつながる偽の広告を公開することから始まることに気付いていた。PPC（クリック課金）広告での商標およびブランド名の悪用は日ごとに増加している。詐欺師は、欺瞞、フィッシングを犯し、または偽造品を販売する他のウェブサイト潜在的な顧客を誘導する。「PPC広告モジュール」は、主要な検索エンジンで検索用語を走査し、公開された広告とそのリンクを分析して、不正な広告の発見、分析を可能にし、アラート提供をする。

30

【0120】

AIとビッグデータを活用したサイバーインテリジェンスプロバイダは、そのモジュールにわたって人工知能（AI）とビッグデータ分析を使用できる。実装されたテクノロジーにより、比類のないアンチ詐欺情報に到達できる。このテクノロジーには、たとえば、リスクパターン認識、機械学習（ML）または深層学習、およびビッグデータ分析が含まれる。

【0121】

リスクパターン認識システムは、ウェブサイト、ソーシャルメディアアイテム、市場のリスティング、アプリ、およびPPC広告にわたって種々のデータポイントをクロスチェックする。これにより、人間の目から隠された類似点を共有するリスクを見つけることができる。システムのこの機能は、ウェブサイトのネットワーク、接続されたソーシャルメディアの投稿やページ、リンクされたリスティング、アプリなど、詐欺師の主要なネットワークを見つける。

40

【0122】

機械学習機械学習と深層学習テクノロジーにより、システムはユーザの活動、種々のオンラインアイテムのメトリックの変更などに基づく結果を改善できる。機械学習により、システムはより多くのデータとアクションを収集および測定するため、スコアとパターン認識を改善できる。

【0123】

履歴データのビッグデータ分析：システムはインターネットの進行中の走査を実行して

50

、潜在的な詐欺に関する情報を収集する。システムは、定期的なスキャンごとにそれが収集したデータをデータベースに記録する。ビッグデータ分析は、記録された履歴データに基づく重要なインテリジェンスの発見を容易にし、時間の経過に伴う変化、時間の経過に伴うデータパターンなどを見つけて分析する。

【0124】

プラットフォームとエコシステム：AIとビッグデータを活用したサイバーインテリジェンスは、エコシステムが構築されるコアテクノロジーである。システムのテクノロジーは、プラットフォームへの最初のAI搭載サイバーインテリジェンスプロバイダとして利用できる。これまで会社や組織がブランドを悪用する詐欺師と戦うためのソースであったインテリジェンスは、今では、プラットフォームとアプリケーション（複数可）を通じて公衆に利用可能とされ、コミュニティと購入者を詐欺から保護する。このシステムは、ウェブサイト、ソーシャルメディア、アプリ、市場、PPC広告など、種々のプラットフォームにわたってオンラインでブランド名を監視するために使用できる。潜在的なオンライン詐欺によって、そのために実行される採点は、システムによって検出および分析されたオンラインアイテムに到達したユーザに警報を提供するために使用される。いくつかの実施形態では、当初、監視とアラートは、暗号通貨とブロックチェーン関連のブランド（会社と組織）に焦点を当てるが、それが進化するにつれて、欺瞞、フィッシング、偽造販売、海賊行為など、種々の詐欺に関するアラートを許可する他の業界と製品に拡張される。生成されたスコアは、暗号化されてブロックチェーンに格納され、潜在的なハッキングやリスクスコアの変更からの保護を強化できる。

【0125】

プラットフォームとコミュニティは、オンラインブランド保護とアンチ詐欺のためにこれまで利用できなかった情報の層、つまりクラウド知恵を作成する。ユーザは、詐欺を実行する潜在的なオンラインアイテムに関する独自のレポートとフィードバックを提供する。この情報は、ブロックチェーンに格納され、AI搭載サイバーインテリジェンスプロバイダと共有され、プラットフォームの最初のプロバイダとなる。エンドユーザによる未知の潜在的な詐欺の警報は、独自のテクノロジーに基づいてリスクを分析するために走査をトリガーする。分析は、ブロックチェーンなどにフィードバックされる。これにより、群衆とサイバーインテリジェンスプロバイダの間で進行中のフィードバックプロセスが作成され、追加のインテリジェンスと機械学習を通じた採点の改善が可能になる。さらに、システムは、種々のテクノロジーとデータソースを利用して、詐欺（欺瞞、フィッシング、偽造など）についてウェブを自動的に監視する。このクラウド知恵の追加層により、システムは、ブランドがそれらのユーザをよりよく保護し、コミュニティから報告された詐欺に対してより効果的に施行できるようになる。システムへの寄付に関心があり、システムによって提供される完全なアンチ詐欺およびサイバーインテリジェンスシステムを受け取る企業および組織は、トークンを使用してそれを行うことができる。

【0126】

保証と保証プロバイダ：システムとモデルは、AI搭載サイバーインテリジェンスプロバイダ、コミュニティからのレポート、信頼スタンプの検証プロセスなど、情報とプロセスの複数のソースに基づいている。情報とプロセスは、欺瞞またはフィッシングのウェブサイト、偽造販売など、オンラインアイテムが詐欺となる潜在的なリスクを評価するために使用される。潜在的なリスクを分析することで、リスクの低いオンラインアイテムを特定し、それに応じてユーザに取引の保証を提供できる。

【0127】

それらのトークンを使用することができるユーザは、プレミアムユーザとして寄付できる。プレミアムユーザは、寄付することで、基本的な返金保証と、トークンを使用してシステム管理者または他の保証プロバイダから種々のレベルの追加保証を購入するオプションを獲得する。基本的な返金保証に加えて、プレミアム寄付金には、詐欺の報告を奨励するために生み出された報奨金からユーザが利益を得る権利が含まれる。

【0128】

返金保証の意義は、ユーザが信頼済みオンラインアイテム（ウェブサイト、ウェブページ、市場など）としてマークされたウェブサイトで行った取引を実行した場合、オンラインアイテムが実際には詐欺（フィッシング、偽造など）であるのに、ユーザは取引で支払われたお金を（たとえば、保証プロバイダから）取り戻す能力と権利を有するということである。この保証は、ユーザに、とりわけ暗号通貨業界において、高レベルの自信と信頼で取引できる能力と、暗号通貨ベースのサービスおよび電子商取引を提供する。プレミアム寄付金で提供される基本的な保証は、取引ごとに一定の値で、一定期間の一定量の取引に対して上限が設定される。プレミアム寄付金で提供された基本的な保証に加えて、他の保証プロバイダは種々の保証プログラムを提供する。保証プログラムにより、ユーザはより多くのトークンの数または量を支払うことができ、取引ごと、時間の経過などによって、より高いレベル（上限）の保証を獲得することができる。

10

【0129】

当初、暗号通貨ベースの取引によって提供される保証は、暗号通貨ベースの取引に限定され、信頼済みウォレットスタンプのあるウェブサイト限定される場合がある。ブロックチェーンテクノロジーの固有の特性である透過性により、取引を追跡できるため、実際に詐欺ウェブサイトであったときに、システム管理者から信頼されていると提示されたウェブサイトで行われた取引に関する主張を簡単かつ透過的に調査できる。システム管理者および／または他のプロバイダは、ウェブサイトまたは種々の電子商取引市場での偽造販売から保護するための保証プログラムを提供する場合がある。

【0130】

20

システム自体に対するユーザによる欺瞞を防止するために、種々の対策が講じられ、たとえば、システムのアプリは、行われた取引の詳細と、訪問またはアクセスされたウェブページを記録し、保証された取引および／または取引に至った操作および／または取引を形成した操作の透過的な再調査を可能にするため、それらをブロックチェーンに保存する。さらに、ユーザは、主張プロセスの一部として、または一定の保証プログラムの一部として、または保証を呼び出すための条件として、KYCまたは同様のプロセスを実行する必要がある場合がある。

【0131】

システムが保証する詐欺は、種々のブランドの乗っ取り、もしくは「ブランドジャッキング」、およびフィッシング、偽造品の販売など、あるエンティティから別のエンティティへの「なりすまし」に起因するものである。システムのモデルは、AIとビッグデータ分析およびコミュニティレポートに基づいており、このような不正活動を検出できる。種々の種類の金融欺瞞またはビジネス欺瞞に起因する詐欺（または詐欺に対する保証）を必ずしも検出しない場合があり、たとえば、ICOを実行し、資金とともに消失することで詐欺を実行する会社は、システムが保証する詐欺のタイプではない。さらに、そのような欺瞞を実行する会社のウェブサイトは、当初のAI信頼済みスコアを得て、信頼スタンプまたは信頼済みウォレットスタンプを獲得するが、それでもなお上記のタイプの欺瞞を実行する可能性はある。システムがユーザにこのような潜在的な欺瞞を報告することを許可し、この情報をユーザに提示することを決定する場合があるが、これは必ずしも保証を提供できるタイプの欺瞞ではない。いくつかの実施形態は、プロバイダが保証プログラムに加えて保険契約を提供することを可能にすることができる。

30

40

【0132】

エコシステム向けのAI搭載サイバーインテリジェンスプロバイダである、プラットフォームは、信頼済みオンラインアイテムでの取引を保証するために、詐欺警報を提供し、およびリスク分析を実行する場合がある。これは、（ユーザレポートを通じた）公的コミュニティとAI搭載サイバーインテリジェンスプロバイダという2つの情報源に基づいている場合がある。本発明のプラットフォーム、または本発明の他のコンポーネントの最初のAIサイバーインテリジェンスプロバイダは、特許出願番号US 14 / 782, 791（公開US 2016 / 0055490）に記載されている1つ以上の機能またはモジュールまたはユニットまたは動作を利用でき、これは参照によりその全体が本明細書に組み込

50

まれている。

【0133】

このシステムは、分散型プラットフォームとして、他のAI搭載サイバーインテリジェンスプロバイダがエコシステムに参加できるようにする。実装された初期モデルと同様に、AI搭載サイバーインテリジェンスプロバイダは、ブロックチェーン上のユーザのレポートデータにアクセスできる。これは、彼らが、彼らのプロセス、データ、および価値提案に組み込むことができるようになる貴重なクラウド知恵を彼らに提供する。AI搭載サイバーインテリジェンスプロバイダは、暗号化された形式でブロックチェーンにスコアを保存する（他のプロバイダには明らかにされない）。プロバイダは、自分自身の寄付金プログラムと自分自身の保証プログラムをユーザに提供できる。プロバイダは保証プロバイダになることもでき、彼らの保証プログラムの一部としてユーザが行った主張に対して責任を負う。ユーザは、プレミアムユーザとして寄付するときに、種々の寄付金から選択して、AI搭載サイバーインテリジェンスプロバイダによって作成されるプログラムを保証するオプションを有することができる。保証主張の寄付金および返金は、トークンおよび／または他の暗号通貨、および／または法定通貨、および／または他の支払い形式（たとえば、クレジットカード、デビットカード、電子振替（EFS）、電信振替、テレフォニープロバイダまたは携帯電話会社経由の支払いなど）で支払うことができる。AIとビッグデータプロバイダのデータソースの分散化により、エコシステムを単一のAI搭載サイバーインテリジェンスプロバイダに依存させず、ユーザに複数の保証プログラムオプションを提供し、また、種々のプロバイダが詐欺関連データを連携および交換し、ユーザに合

10

20

【0134】

施行サービスプロバイダ：プラットフォームには、会社と施行サービスプロバイダが出会い、取引する市場が含まれる場合がある。たとえば、法律家、弁護士、ブランド保護サービスプロバイダ、プライベート機関、政府機関、その他の関連エンティティは、プラットフォームの執行サービスプロバイダにサインアップできる。システムは、これらのプロバイダに対して、詳細な有効化プロセスと「顧客を知る」（KYC）プロセスを実行する場合がある。プロバイダは、トークンを使用して、および／または他の支払い方法を介して、有効化プロセスの料金を支払う必要がある。生態系で識別された詐欺を施行することに関心のある会社や組織は、プラットフォームを通じて作業指示書を公開できるようになる。プロバイダの選択は、作業指示書を公開する会社の裁量に委ねられ、施行プロバイダによる入札、および／または公開されたデータに基づく選択の形式にすることができる。施行プロバイダに関してプラットフォームで公開される情報には、たとえば、証明、（採用した会社によって提供される）市場での以前の作業の再調査、保有するトークンの量または数による（たとえば、エコシステムへの関与または利害関係を表す）評価などが含まれる。

30

【0135】

暗号通貨トークン：上で記載したように、このトークンは本発明のエコシステムでいくつかの用途を有する。たとえば、（a）プレミアム寄付金またはプレミアムサービス。トークンは、アプリケーションのプレミアム寄付金を獲得するために使用され、プレミアム寄付金には、基本的なレベルの保証と、ユーザが潜在的なオンライン詐欺について報告した場合に報奨金から得る能力が含まれる。（b）保証プログラム—プレミアム寄付金で提供された基本的な保証プログラムに加えて、ユーザは自分のトークンを使用して、オンライン取引用の追加の保証プログラムを購入できる。（c）レポート詐欺の報告に関心があり、報奨金から報酬を受けるユーザは、報告するときにトークンを預ける必要がある。彼らが正しいと判明した場合、報奨金での取り分に加えて、預金トークンが彼らに返される。それらが正しくないことが判明した場合、トークンの80%が一般的な報奨金にクレジットされる。（d）報奨金。このトークンは、ユーザが潜在的なオンライン詐欺について報告するよう促すために会社や組織によって使用される。プレミアム寄付金に対してユーザが支払うトークンの20%（またはその他のパーセンテージ）は、一般的な報奨金に

40

50

寄付される。会社や組織は、ブランド特有の報奨金を作成して、特定のブランド、または、彼らが製造または販売する特定の製品またはアイテムにさえ関連する詐欺レポートや偽造品レポートの提出を奨励することができる。(e) 信頼スタンプ（または真正性スタンプ）および信頼済みウォレットスタンプ（または真正な暗号ウォレットスタンプ）の支払いと有効化—信頼スタンプと信頼済みウォレットスタンプの獲得に関心のある会社や組織は、トークンを使用してスタンプの支払いを行なう。たとえば、彼らが支払うトークンの50%は、スタンプの公的有効化担当者に支払われ、公的有効化担当者は、その後、トークンをプレミアム寄付金および保証プログラムに使用できる。(f) 会社や組織によるシステムへの寄付金の支払い—システムへの寄付と、偽造品の販売や偽の情報の公開を削減または緩和するためのアンチ詐欺インテリジェンスまたは情報の受信に関心のある会社および組織は、トークンを使用してこれを行うことができる。この使用は、トークン生成イベント（TGE）の時点で利用できる。(g) 施行者への支払い—施行サービスの市場をプラットフォームの一部として使用する会社は、トークンを使用して、彼らのアクションに対して施行者に支払うことができる。

【0136】

例証的な実施形態では、使用され得るトークンは、好適な記号（たとえば、「MSLD」）を有する、ERC-20ベースのトークンまたは暗号通貨または暗号コインである。例証的な実装形態では、システムは事前定義された有限数のトークン（たとえば、1,000,000,000（10億）個のトークン）を作成する。インフレやトークンの追加作成はない。

【0137】

例証的な例では、生成されたトークンは、以下のような事前定義された比率または数量に従って、分配および／または割り当ておよび／または予約および／または利用されてもよい。

【表1】

エンティティ：	パーセンテージ：	トークンの数：
創設者、チーム、および株主	20%	200,000,000
将来の運営のための資金	30%	300,000,000
報告報奨金	4.5%	45,000,000
マーケティングとバグ報告の報奨金	0.5%	5,000,000
保証資金	5%	50,000,000
公衆に申し出されたトークン	40%	400,000,000
合計	100%	1,000,000,000

【0138】

任意選択で、創設者、チーム、および株主に分配されたトークンは、1年またはその他の期間にわたって権利が確定し、トークン生成イベント（TGE）の日に5%（たとえば、1,000万トークン）が分配される。将来の運営のための資金は、将来の開発、システムのメンテナンス、マーケティング活動などに使用するために保留されている。報告報奨金は、詐欺を報告したユーザを奨励し、報酬を与えるために設立された最初の一般的な報奨金である。保証資金は、保証を提供したオンラインアイテムに関する詐欺事件に対するユーザの主張があった場合のために保存された資金である。公衆に申し出されるトークンは、トークンセールが続く先行販売プロセスで販売される。公開販売は、制限された個人、または制限された管轄区域のエンティティおよび個人には申し出されない。いくつかの実施形態では、TGEまたは先行販売は、早期参加者に提供されるボーナスを備えた、公開先行販売の一部としてトークンを提供することができる。トークンは、一定のタイプのその他の暗号通貨（たとえば、ビットコイン、イーサリアム）、および／または法定通貨で購入できる。

【0139】

本発明のプラットフォームは、オンライン取引を実行人々に自信を提供することができる。仮想通貨エコシステムは、本発明のアンチ詐欺プラットフォームの実証的な実装形態である。暗号通貨エコシステムでは、詐欺からの恐怖は甚大であり、会社、トークン購入者、ウォレット保有者を含むすべての利害関係者にとって毎日の課題である。この新しい進化する世界の将来の成長は、暗号通貨エコシステムの基本的な要素である、価値の交換をより高いレベルで信頼できるようにすることにかかっている。このプラットフォームは、すべての利害関係者、会社、およびユーザの間で珍しい関心の一致を提供する。エンドユーザの聴取を支援し、新しいユーザをオンボーディングし、既存のユーザのエンゲージメントを維持する必要がある。プラットフォームの信頼メトリックは、エコシステムの「信頼の印」となり、デジタル取引と電子商取引のすべての部分をリードするために活用される。

10

【0140】

プラットフォームは、バリューチェーンの2つの側、すなわち、エンドユーザ中心であり、ユーザを対象としてエンゲージメントの向上に重点を置き、トークンエコノミーが主なツールである（a）、ビジネス中心であり、信頼済みパートナープランの採用、報奨金への会社の参加、会社や組織による信頼済みスタンプと信頼済みウォレットスタンプのユーザの拡大である（b）、からニーズに対応できる。

【0141】

プラットフォームは、認識からエンゲージメントおよびオンラインアイテムの購入まで、顧客の全過程に基づいて動作する。社会的影響：アプリケーションは、計画されたネットワーク効果をサポートする複数の要素を有するように設計されており、分配が迅速でバイラル（viral）でインパクトがあることを確認できる。各ユーザをネットワークに追加すると、潜在的な詐欺の報告に参加できる追加のユーザは、コミュニティの残りのユーザに利益をもたらすから、残りのユーザに利益をもたらす。セグメント化されたマーケティングを使用して、行動、市場での成熟度、以前のオンラインの行動、ユーザが調査した取引の規模および／または複雑さを含む、暗号通貨ペルソナに基づいて潜在的な顧客をセグメント化できる。プラットフォームは、複数のマーケティング目標または態様を達成するために、たとえば、（a）認識作成から積極的なユーザまでの取得、（b）オンボーディングからロイヤリティまで、コミュニティをサポートし、エンゲージメントを生かし、ウォレットのシェアと使用頻度と保持を拡大するコミュニティ、（c）モバイル、ブラウザのバージョン、デスクトップなど、種々の製品を活用する複数の取得チャネル、（d）（d1）顧客との関わりを望んでいる会社が、コミュニティを登録して信頼を交換し、報酬を獲得する標的聴取、（d2）会社がコミュニティとトークンに参加する際の傘となる次認定パートナープログラムである、ビジネスセントリック（B2B）マーケティング計画のガイドラインを、マーケティングまたは実装できる。パートナープログラムにより、メンバは種々のツールやサービスとのエンゲージメントのレベルを選択できる。パートナープログラムは、新しいサービスをすべての会社のユーザに伝達することに焦点を置き、B2Cマーケティング計画をサポートし、認識と効果的なアクションの呼び出しを作成する。（d3）さまざまなサービスによって、たとえば、信頼スタンプ、信頼済みウォレットスタンプ、報奨金プログラムなど、正しいソリューションを調整できる。

20

30

40

【0142】

本発明のいくつかの実施形態は、（a）少なくとも、（i）ユーザに資産を販売する、または情報を提供する、オンライン宛先（またはオンライン催場）のコンテンツと、および／または（ii）オンライン宛先における所有権に関するデータ（たとえば、ドメイン所有権データ）、および／または（iii）不正の可能性がある、または虚偽の情報を公開している可能性があるとして、オンライン宛先にフラグを立てる、1つ以上のクラウドソースのユーザ提出と、を組み合わせることで分析することと、（b）ステップ（a）の分析に基づいて、資産を販売する、または情報を提供する、オンライン宛先のコンテンツが、虚偽または不正であるということとを判定することと、を含む方法であって、方法は、コンピ

50

ユーザ化された装置によって自動的に実行される。本発明は、データ（ドメイン所有権、ウェブサイトまたはオンライン催場によって表示されるコンテンツ、ウェブサイトの複雑さや高度化などのメタデータ、製品の製造元からの正式なデータと比較した、ウェブサイトまたは催場に表示されるデータの正確性または不正確さなど）のＡＩ処理と、事前定義された合意ルール（複数可）に基づいて、任意選択により合意を検出または判定することにより分析され、複数のユーザ提出レポートから取得されたクラウドソースデータの両方を考慮に入れる独自の組み合わせ分析を利用することができる。本発明は、単に「疑わしい」または「ウイルスを有している」または「マルウェアを有している」として、ウェブサイトまたはウェブページにフラグを立てるだけではなく、むしろ、偽造品や偽造製品の販売を試みるコンテンツ部分として、ウェブサイトの特定のコンテンツ部分にフラグを立てるか、虚偽または偽の情報を提供する。いくつかの実施形態では、たとえば、システムは、特定の製造業者のブランドおよび／または製品を保護する場合があります、そのような製造業者から、製造業者が認可した流通業者または再販業者の事前定義済みおよび／またはクロズドリストまたは「ホワイトリスト」を事前に受け取ることができ、また、その製造業者の製品を販売するオンライン催場のドメインまたはＵＲＬまたはＵＲＩを、事前に定義されたリストまたはホワイトリストと比較する場合があります、検査されたオンライン催場は、製造業者が承認した認定再販業者または認定流通業者のリストに含まれるエンティティが所有していない場合、本発明のシステムは、ユーザまたはエンドユーザまたは消費者に、彼が偽造製品を購入しようとしていること、および／または彼が虚偽もしくは偽の情報を消費していることを通知する。

【０１４３】

いくつかの実施形態では、ステップ（ａ）の分析は、少なくとも、（ｉ）オンライン宛先が、１つ以上の資産の不正な販売を申し出ている、または虚偽の情報を含んでいるということを示す、複数のユーザ提出レポートを受信することと、（ｉｉ）合意に達するための１つ以上の条件を示す事前定義されたルールに基づいて、ユーザ提出レポートのうちの１つ以上の正確性に関して、ユーザの群衆の中で検出される少なくとも合意を考慮することにより、ステップ（ｂ）の判定を実行することと、を含む。たとえば、システムは、特定のウェブサイトが、偽造品を販売している、または虚偽もしくは偽の情報を公開していることを示す５０件のユーザ提出レポート、およびウェブサイトまたは催場が、正当であること、および／または真正なグッズを販売していること、および／または信頼できる情報を公開していることを示す６件のユーザ提出を受けると、システムは、事前に定義された多数決票のサイズ（たとえば、投じられた５６票のうち５０票）が偽造資産および／または虚偽の情報を示していると判定し、したがって、システムはそのような結果に関して合意に達したと判定し、達した合意に従ってユーザに通知する。

【０１４４】

いくつかの実施形態では、方法は、（ｉ）オンライン購入のために１つ以上の資産を申し出る、または情報を公開する特定のオンライン催場が信頼できるということを判定することと、（ｉｉ）公的にアクセス可能な自己検証可能なブロックチェーンデータセットに、特定のオンライン催場が信頼できるという標識を公開することと、を含む。たとえば、ユーザが提出した各レポート、または信頼性を示すユーザ提出レポートのみ、または信頼できないことを示すユーザ提出レポートのみ、さらに、そのような各ユーザ提出の（任意選択で）日時などのメタデータ、各提出者のＩＰアドレス、提出者のユーザ名もしくは電子メールアドレス、各提出者の独自の識別子など、がブロックチェーンのデータセットに書き込まれる。

【０１４５】

いくつかの実施形態では、方法は、資産の販売を申し出るオンライン催場が、正当であるということを判定することと、オンライン催場が真正であるという標識をユーザに提供することと、を含む。たとえば、システムは、（ｉ）製品を販売するウェブサイトをホストするドメインの所有権レコードと、（ｉｉ）その製品の製造業者または輸入業者から、事前に提供された（または実際に動的に取得された）製品の認定再販業者のホワイトリス

トを比較する。一致が判明した場合は、信頼性スタンプまたは真正性スタンプまたは通知が生成および表示され、任意選択でブロックチェーンデータセットに格納される。

【0146】

いくつかの実施形態では、方法は、情報を公開するオンライン宛先が、信頼できる宛先であることを判定することと、オンライン宛先が、信頼できるという標識をユーザに提供することと、を含む。たとえば、システムは、特定の会社のCEOから、その会社によって、その会社に関する情報を分配することを認定されたFacebookアカウント、Twitterアカウント、YouTubeアカウント、および認定されたブログアカウントの事前定義またはクローズドホワイトリストを受け取り、次に、システムに、ウェブサイトまたはソーシャルメディアアカウントが会社に関する（否定的または肯定的な）情報を公開したことが判明し、システムは、公開者のデータまたはメタデータと、会社が提供したホワイトリストを比較することがある（または、このようなホワイトリストは、「Company.com/Whitelists」など、会社が排他的に管理している、事前に定義されたリソースロケータまたはURLからリアルタイムで動的にフェッチされる）。公開者のデータが、会社に関するデータの公開を認定されているエンティティまたは個人のホワイトリストにあるアイテムの少なくとも1つと一致する場合、信頼性スタンプまたは通知が生成される。そうでない場合、虚偽の情報または「偽のニュース」の通知またはスタンプが生成される。任意選択で、そのような通知やスタンプをブロックチェーンのデータセットに記録または格納できる。したがって、いくつかの実施形態では、方法は、オンライン宛先が、不正または信頼できないということを判定することと、オンライン宛先が、不正または信頼できないという標識をユーザに提供することと、を含む。同様に、いくつかの実施形態では、方法は、ユーザが、オンライン宛先を通じて偽造資産を購入しようとしているという通知をユーザに提供することを含む。

【0147】

という返金保証いくつかの実施形態では、方法は、ユーザが、オンライン宛先を通じて真正な資産を購入しようとしているという通知をユーザに提供することと、資産が真正であるという返金保証をユーザに提供することと、を含む。上記のような判定に対して、さらに、システムは、製品が真正であるという、および彼が、この認証されたウェブサイトまたは催場から買った製品が、偽造であることがわかった場合、ユーザは彼のお金を取り戻すという、被保証または保証をユーザに提供する。

【0148】

いくつかの実施形態では、方法は、ブロックチェーンデータセットを通じて、少なくとも、（i）オンライン宛先の真正性に関する1つ以上のユーザ提出レポート、および（ii）オンライン宛先の真正性に関する承認のスタンプを公開することを含む。これにより、ブロックチェーンデータセットへのアクセスコードを受け取る公衆、ユーザ、またはプレミアムユーザは、特定のオンライン宛先または催場が、真正であるかどうか、および／または真正な製品を販売しているかどうか、および／または正当な情報を公開しているかどうかを自動的に検索できる。同様に、いくつかの実施形態では、方法は、ブロックチェーンデータセットを通じて、少なくとも、（i）オンライン宛先の非真正性に関する1つ以上のユーザ提出レポート、および（ii）オンライン宛先の非真正性に関する不承認のスタンプを公開することを含む。

【0149】

いくつかの実施形態では、方法は、特定の電子メールメッセージがスパムであるかどうかに関する、複数のユーザ提出レポートを受信することと、複数のユーザ提出レポート間の合意を判定するステップと、（i）ユーザ提出レポート、（ii）合意の標識のうちの少なくとも1つをブロックチェーンデータセットに公開することと、合意に一致するレポートを提出した少なくとも1人のユーザに報酬を提供することと、を含む。この独自のシステムは、動機のない自発的なユーザに依存する従来のシステムとは異なり、スパム電子メールを報告するユーザに真の効果的な動機を提供する。したがって、本発明のシステムは、ユーザからはるかに大量のスパム電子メールまたはジャンク電子メールのレポートを

収集することができ、これは次に、スパム分析モジュールまたはユニットによって使用され、合意を決定し、および／または提出された電子メールにおけるスパムコンポーネントまたはスパムの足跡を検出し、それにより、本発明に従って動作するそのようなスパムフィルタリングエンジンの信頼性を向上させる。したがって、いくつかの実施形態は、上記の動作に基づいて、スパム電子メール／ジャンク電子メール検出システムまたはフィルタリングシステムを含むことができる。

【0150】

いくつかの実施形態では、特定のオンライン催場がフィッシング催場であるかどうかに関する、複数のユーザ提出レポートを受信することと、複数のユーザ提出レポート間の合意を判定することと、(i) ユーザ提出レポート、(ii) 合意の標識のうちの少なくとも1つをブロックチェーンデータセットに公開することと、合意に一致するレポートを提出した少なくとも1人のユーザに報酬を提供することと、を含む。この独自のシステムは、動機のない自発的なユーザに依存する従来のシステムとは異なり、ユーザにフィッシング催場やサイト、電子メールを報告する真の効果的な動機を提供する。したがって、本発明のシステムは、ユーザからはるかに大量のフィッシング催場を収集することができ、これは次に、フィッシング分析モジュールまたはユニットによって使用され、合意を決定し、および／または提出された催場またはウェブサイトまたはウェブページにおけるフィッシングコンポーネントまたはフィッシング足跡またはフィッシング要素を検出し、それにより、本発明に従って動作するそのようなフィッシング検出／フィルタリングエンジンの信頼性を向上させる。したがって、いくつかの実施形態は、上記の動作に基づいて、フィッシング検出システムまたはフィルタリングシステムを備え得る。

【0151】

いくつかの実施形態では、特定のオンライン催場が偽造品を販売しているかどうかに関する、複数のユーザ提出レポートを受信することと、複数のユーザ提出レポート間の合意を判定することと、(i) ユーザ提出レポート、(ii) 合意の標識のうちの少なくとも1つをブロックチェーンデータセットに公開するステップと、合意に一致するレポートを送信した少なくとも1人のユーザに報酬を提供することと、を含む。たとえば、60人のユーザは、特定のウェブサイトが既知の製造業者の偽物または真正ではないシャツを販売していると報告したのに対し、4人のユーザはその反対だと報告した場合、また、任意選択で、その特定のウェブサイトのドメインの所有権が、認定小売業者の事前定義済み（または動的に取得された）ホワイトリストであって、製造業者自身によって提供されるホワイトリストに含まれないエンティティの名前に記録されていることも考慮に入れて、次に、システムは、販売用に申し出された製品が偽造品であるという通知を生成する。

【0152】

いくつかの実施形態では、方法は、組織内の複数のユーザに、特定のオンライン催場が、組織の1つ以上の偽造資産を販売している、または組織に関する虚偽の情報を公開しているという通知を提供することを含む。たとえば、靴の製造業者は500人の従業員を雇用し、本発明のシステムの管理者から、販売されている偽造靴を検出するためにインターネット催場を監視するよう要求する。本発明のシステムは、任意選択で、製造業者の従業員500人のラップトップコンピュータおよび／またはスマートフォンおよび／またはタブレットおよび／またはデスクトップコンピュータにモジュールまたはプログラムをインストールすることができ、従業員は、そのようなデバイスを利用してインターネットをサーフ(surf)し、および電子商取引を実行でき、いく人かの従業員が不審なウェブサイトまたはオンライン催場を発見すると、そのようなユーザ（その製造業者の従業員でもある）はそれをシステムに報告する場合がある。任意選択で、特定のウェブサイトで販売されている偽物の靴に関するレポートには、その組織（靴メーカーの会社）の外部にいる非従業員ユーザが提出した同様のレポートと比較して、より大きな重みまたはより高いスコアが割り当てられる。いくつかの実施形態では、自社によって販売のために申し出されている真正な製品に精通している、および／または組織に忠実な、製造業者の組織のそのような従業員は、非従業員ユーザによって提出されたユーザ提出レポートの評価（または

投票) のタスクをさらに割り当てられ得る。

【0153】

いくつかの実施形態では、方法は、(i) オンライン宛先の登録所有者である第1のエンティティを判定することと、(ii) 第2の異なるエンティティが、オンライン宛先を通じた販売が申し出されている資産における商標の登録所有者であると判定することと、(iii) 第1のエンティティが第2のエンティティとは異なることに基づいて、オンライン宛先での資産の販売の申し出は不正であると判定することと、を含む。たとえば、システムは、コンテンツ分析に基づいて、および／またはユーザ提出に基づいて、ウェブサイト「My-Best-Deals.com」が「Nike Air Shoes」販売の申し出をしていることを検出することができ、さらに、そのウェブサイトのWHOISレコードを取得またはフェッチして、ドメインが中国北京の「Tai Chang」によって所有されていることを見つけ出す場合があり、さらに、Nike社のCEOによってシステムに提供された、またはNike社の事前定義されたURLまたはリソースロケータから自動的かつ／またはリアルタイムで取得またはダウンロードされた、Nikeシューズの認定小売業者または認定流通業者の事前定義されたホワイトリスト（たとえば、Nike.com/white-list）と照らして、その名前をチェックする場合があり、および／または（たとえば、TESSデータベースまたはUSPTO商標データベースまたはその他のデータベースを使用して）製品の説明に見える「Nike」という単語について商標所有者の記録を自動的にチェックする場合があり、したがって、販売者「Tai Chang」は商標所有者ではなく、認定再販業者でもないと判定する場合があり、これにより、申し出されたアイテムは、偽物または偽造品であるという通知または警告がトリガーされる。

【0154】

いくつかの実施形態では、方法は、(i) オンライン宛先が、資産をエンドユーザへの販売を申し出る第1の価格を判定することと、(ii) 資産の製造業者推奨小売価格(MSRP)である第2の価格を判定することと、(iii) 第1の価格は、Nが所定の正の数である、Nパーセントだけ前記第2の価格よりも安いことを判定することと、(iv) ステップ(iii)に基づいて、オンライン宛先での資産の販売の申し出は不正であると判定することと、を含む。たとえば、システムは、MSRP価格の事前定義されたリストにおける、そのSKU番号またはシリアル番号またはモデル番号またはモデル名に基づいて、および／またはウェブサイトまたは、既知であり製造業者が正当に所有するシステムで事前定義されている（たとえば、「Nike.com」では、販売アイテムが「Nike Air Shoes」の場合、Nike社の公式ストアである）オンラインストア上のアイテムの価格と照合して、アイテムの価格をチェックし、または、信頼性が高く、偽物でないアイテムのみを販売することが知られている特定の電子商取引のサイト（たとえば、Neuman Marcusウェブサイト）であっても、「My-Best-Deals.com」のウェブサイトの価格が37ドルであるのに対し、システムは、このような真正なウェブサイトのこの特定の靴モデルの価格が100ドルであって、価格の差が事前定義されたパーセント値または比率よりも大きい（たとえば、MSRPに比べて価格が33%以上安い）ことを検出し、これにより、そのウェブサイトで提供されている製品が偽造品であるという決定がトリガーされる。

【0155】

いくつかの実施形態では、方法は、(i) オンライン宛先上の資産のテキストによる説明が、資産の製造業者による資産の形式的な説明と比較して1つ以上の不一致を有することを判定することと、(ii) ステップ(i)に基づいて、オンライン宛先での資産の販売の申し出が不正であると判定することと、を含む。たとえば、上記のシナリオで、システムは「Nike Air Shoes」のサイズ9が、2.5ポンドの重量と12×10×8インチの靴箱を有しているとして製造業者のウェブサイトに表示されていることを検出できるが、疑わしいウェブサイト上の同じ靴は、重量が2.1ポンドで、靴箱は異なるサイズ（たとえば、9×11かける13インチ）であると示されていることを検出し、こ

れにより、そのウェブサイトで提供されている製品は偽造品であるという決定がトリガーされる。同様に、いくつかの実施形態では、方法は、(i) オンライン宛先上の資産のテキストによる説明が、資産の製造業者による前記資産の正式な説明と比較して1つ以上の異なる特性を有することを判定することであって、特性が、規模、寸法、重量、色、使用される材料、量のうちの1つ以上を含む、特性を有することを判定することと、(ii) ステップ(i)に基づいて、オンライン宛先での資産の販売の申し出が不正であると判定することと、を含む。

【0156】

いくつかの実施形態では、ステップ(b)の判定はまた、オンライン宛先が、不正であると判定された別のオンライン宛先の所有者としてすでに識別されている、特定のエンティティによって所有されているという判定に基づくことを含む。たとえば、本発明のシステムは、ウェブサイト「My-Best-Nike.com」が、偽物のナイキ靴を販売しており、中国北京の「Tai-Chang」によって所有されていることをすでに検出または決定しており、システムは、アディダスの靴であるとされる靴を販売しているウェブサイト「MY-Best-Adidas.com」のコンテンツと所有権をいま調べており、また、この人物が偽物のナイキシューズを販売する前述のウェブサイトを所有または運営しているという事前の決定に基づいて、システムは、他のウェブサイトが偽者のアディダスシューズを販売していると推論および決定する場合もある。これは、他のウェブサイトが偽物のアディダス靴を販売している可能性があると報告した、ユーザ提出などのクラウドソースデータによってさらに裏付けられ得る。

【0157】

いくつかの実施形態では、方法、(i) オンライン宛先が、1つ以上の資産の不正な販売を申し出ている、または虚偽の情報を含んでいることを示す複数のユーザ提出レポートを受信することであって、各ユーザ提出レポートが、ユーザのレポート提出と一緒に、提出ユーザによって暗号通貨の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、(ii) 合意に達するための1つ以上の条件を示す事前定義されたルールに基づいて、ユーザ提出レポートのうちの1つ以上の正確性に関して、ユーザの群衆の中で検出される少なくとも合意を考慮することにより、ステップ(b)の判定を実行することと、を含む。たとえば、偽造製品を販売している、および／または虚偽もしくは偽の情報を公開しているウェブサイトまたはオンライン催場に関するユーザレポートの提出は、提出したユーザによるそのような支払いを伴う場合にのみ実行でき、これにより、偽のまたは悪意のあるユーザレポートの機会を減らし、システムが下す決定の正確性を高める。

【0158】

いくつかの実施形態では、方法は、(i) オンライン宛先が、1つ以上の資産の不正な販売を申し出ている、または虚偽の情報を含んでいることを示す複数のユーザ提出レポートを受信することであって、各ユーザ提出レポートが、ユーザのレポート提出と一緒に、提出ユーザによって法定額の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、(ii) 合意に達するための1つ以上の条件を示す事前定義されたルールに基づいて、ユーザ提出レポートのうちの1つ以上の正確性に関して、ユーザの群衆の中で検出される少なくとも合意を考慮することにより、ステップ(b)の判定を実行することと、を含む。たとえば、偽造製品を販売している、および／または虚偽もしくは偽の情報を公開しているウェブサイトまたはオンライン催場に関するユーザレポートの提出は、提出したユーザによるそのような支払いを伴う場合にのみ実行でき、これにより、偽のまたは悪意のあるユーザレポートの機会を減らし、システムが下す決定の正確性を高める。

【0159】

いくつかの実施形態では、方法は、複数のユーザ提出レポートと一緒に受信された(少なくとも)複数の法定額の支払いおよび／または暗号通貨の支払いから報奨金源を作成することと、特定の提出ユーザの特定のユーザ提出レポートが正しいと判定される場合、次

に、特定の提出ユーザに、報奨金源の一部である支払いを、特定の提出ユーザが自分のユーザレポートの提出と一緒に支払った支払い以上の金額で分配することと、を含む。たとえば、偽造製品を販売している、および／または虚偽もしくは偽の情報を公開しているウェブサイトまたはオンライン催場に関するユーザレポートの提出は、提出したユーザによるそのような支払いを伴う場合にのみ実行でき、これにより、偽のまたは悪意のあるユーザレポートの機会を減らし、システムが下す決定の正確性を高める。さらに、報奨金機構は、（ユーザがそれを提出するために支払った）レポートが正しいと判明した場合に報酬を受けることを知りながら、レポートを提出するために努力、時間、およびお金（法定額または暗号通貨）を費やした、正当なユーザに動機を提供する。

【0160】

いくつかの実施形態では、方法は（i）暗号通貨の支払いを暗号通貨ウォレットに受信するオンライン催場のコンテンツとメタデータを分析し、（I）暗号通貨ウォレットの現実の所有者の実際のアイデンティティと、（II）オンライン催場の現実の所有者のアイデンティティとの間の不一致を検出することと、（ii）不一致に基づいて、暗号通貨ウォレットへの暗号通貨の支払いを受信するオンライン催場が不正であることをエンドユーザに通知することと、を含む。たとえば、システムは新しいコインのICOを公開し、特定の暗号ウォレットへの支払いを要求するウェブサイト「My-Best-Coin.com」を調べる場合があり、さらに、この特定の暗号ウォレットは現実には「Tai-Ching」が実際に所有しているデータを取得する可能性があるが、そのウェブサイトは「John-Smith」が所有していて、不一致は（一部の実装形態では）不正の可能性のあるフラグを立て、エンドユーザに暗号ウォレットが必ずしもそのウェブサイトまたはドメインの真の所有者に属していない可能性があることを通知するのに十分な場合がある。他の実施形態では、システムの管理者は、特定の慈善団体のCEOから、匿名の寄贈を暗号通貨で受け取る目的で、その慈善団体によって利用される、その慈善団体の単一の公式暗号ウォレット（#123456のウォレットIDを有する）を受け取ることがあり、次に、システムはインターネットを検索またはクロールして、「Jack-Smith」が所有する特定のウェブサイトが、申し立てによれば、その特定の慈善団体に寄贈するとされる寄贈を求めているが、エンドユーザから#123789の識別子を有する暗号ウォレットへの暗号通貨寄贈の送信を要求していることを発見する場合があり、不一致は、その「Jack-Smith」が所有または運営するこのウェブサイトまたはウェブページ（またはウェブサイトの所有者が不明な場合でも）に、公式の暗号ウォレットとは異なる不正な暗号ウォレット識別子が含まれていることを示し、欺瞞フラグが、トリガーされ、その偽のまたは不正な暗号ウォレットへの暗号通貨の寄贈を検討しているエンドユーザに向けて生じさせる。同様に、いくつかの実施形態では、方法は、（i）コンテンツとメタデータを、記オンライン催場の外部で収集された少なくとも1つの外部情報のソースと比較することによって、暗号通貨の支払いを暗号通貨ウォレットに受信するオンライン催場のコンテンツとメタデータを分析することと、（ii）不一致に基づいて、暗号通貨ウォレットへの暗号通貨の支払いを受信するオンライン催場が不正であることをエンドユーザに通知することと、を含む。

【0161】

いくつかの実施形態では、方法は、（i）（i）エンドユーザから暗号通貨の支払いを受信することを意図された暗号通貨ウォレットの特定のアドレスをエンドユーザに提供するオンライン催場のコンテンツおよびメタデータと、（ii）オンライン催場の外部で収集された外部情報の少なくとも1つのソースの間を比較することと、（iii）暗号通貨ウォレットの特定のアドレスが、オンライン催場に記載されている製品の正当な所有者に属していないことを判定することと、（iii）オンライン催場には、暗号通貨ウォレットの不正なアドレスが含まれているという、少なくとも1人のエンドユーザへの通知を生成することと、を含む。上記の前述のシナリオと同様に、いくつかの実装形態は、申し立てによれば、ウェブサイト「My-Best-Nike.com」が「Nikeシューズ」を販売し、申し立てによれば、Nike社の認定再販業者の暗号ウォレット識別子である

10

20

30

40

50

3 3 3 4 4 4 を提供していることをチェックし見つけ出せるが、事前に定義されたリストまたはホワイトリストまたはブラックアップテーブルが、（たとえば、N i k e 社の C F O によって）本発明のシステムに N i k e の認可された再販業者に属する唯一の暗号ウォレットの識別子のリストを提供することができ、そのホワイトリストからの暗号化ウォレット識別子 # 3 3 3 4 4 4 の欠如は、このウェブサイトが、おそらく偽のウェブサイト、または偽物または偽造製品を販売しているウェブサイトであるということをエンドユーザに通知するためにシステムによって利用される。同様に、いくつかの実施形態では、方法は、（i）（I）エンドユーザから暗号通貨の支払いを受信することを意図された暗号通貨ウォレットの特定のアドレスをエンドユーザに提供するオンライン催場のコンテンツおよびメタデータと、（II）オンライン催場の外部で収集された外部情報の少なくとも1つのソースの間を比較することと、（ii）暗号通貨ウォレットの特定のアドレスが、オンライン催場に記載されている製品の正当な所有者に属していることを判定することと、（iii）オンライン催場には、正当な所有者の暗号通貨ウォレットの真正なアドレスが含まれているという、少なくとも1人のエンドユーザへの通知を生成することと、を含む。
【0162】

10

いくつかの実施形態では、方法は、（i）オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートを受信されるステップであって、各ユーザ提出レポートが、ユーザのレポート提出と一緒に、提出ユーザによって暗号通貨の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、（ii）提出ごとに暗号通貨の支払いを必ず必要とする提出機構を介して、すべて提出された複数のユーザ提出レポートを分析することにより、ステップ（b）の判定を実行することと、を含む。

20

【0163】

いくつかの実施形態では、方法は、（i）オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートを受信するステップであって、各ユーザ提出レポートが、ユーザのレポート提出と一緒に、提出ユーザによって暗号通貨の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、（ii）提出ごとに暗号通貨の支払いを必ず必要とする提出機構を介して、すべて提出されたユーザ提出レポートのうちの1つ以上の正確性に関して、エンドユーザの群衆の中で到達された少なくとも合意を考慮することにより、ステップ（b）の判定を実行することと、を含む。

30

【0164】

いくつかの実施形態では、方法は、（i）オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートを受信するステップであって、各ユーザ提出レポートが、ユーザのレポート提出と一緒に、提出ユーザによって暗号通貨の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、（ii）提出ごとに暗号通貨の支払いを必ず必要とする提出機構を介して、すべて提出された複数のユーザ提出レポートを分析することにより、ステップ（b）の判定を実行することと、（iii）真正性が自己検証可能なブロックチェーンデータセットの一部として、ユーザ提出レポートの少なくとも1つを公開するステップと、を含む。

40

【0165】

いくつかの実施形態では、方法は、（i）オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートを受信するステップであって、各ユーザ提出レポートが、ユーザのレポート提出と一緒に、提出ユーザによって暗号通貨の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、（ii）提出ごとに暗号通貨の支払いを必ず必要とする提出機構を介して、すべて提出された複数のユーザ提出レポートを分析することにより、ステップ（b）の判定を実行することと、（iii）オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートと一緒に受信された複数の暗号通貨の支払いから報奨金源を作成することと、（iv）特定の提出ユーザの特定のユーザ提出レ

50

ポートが正しいと判定される場合、次に、特定の提出ユーザに、報奨金源の一部である暗号通貨の支払いを、特定の提出ユーザが自分のユーザレポートの提出と一緒に支払った暗号通貨の支払い以上の金額で分配することと、を含む。

【0166】

いくつかの実施形態では、方法は、(i) オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートを受信するステップであって、各ユーザ提出レポートが、ユーザのレポート提出と一緒に、提出ユーザによって暗号通貨の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、(ii) 提出ごとに暗号通貨の支払いを必ず必要とする提出機構を介して、すべて提出された複数のユーザ提出レポートを分析することにより、ステップ(b)の判定を実行することと、(iii) オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートと一緒に受信された複数の暗号通貨の支払いから報奨金源を作成することと、(iv) オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示すユーザレポートを提出した提出ユーザの間で、報奨金源の少なくとも一部を分配することと、を含む。

10

【0167】

いくつかの実施形態では、方法は、(i) オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートを受信するステップであって、各ユーザ提出レポートが、ユーザのレポート提出と一緒に、提出ユーザによって法定額の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、(ii) 提出ごとに法定額の支払いを必ず必要とする提出機構を介して、すべて提出された複数のユーザ提出レポートを分析することにより、ステップ(b)の判定を実行することと、を含む。

20

【0168】

いくつかの実施形態では、方法は、(i) オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートを受信するステップであって、各ユーザ提出レポートが、ユーザのレポート提出と一緒に、提出ユーザによって法定額の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、(ii) 提出ごとに法定額の支払いを必ず必要とする提出機構を介して、すべて提出されたユーザ提出レポートのうちの1つ以上の正確性に関して、エンドユーザの群衆の中で到達された少なくとも合意を考慮することにより、ステップ(b)の判定を実行することと、を含む。

30

【0169】

いくつかの実施形態では、方法は、(i) オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートを受信するステップであって、各ユーザ提出レポートが、ユーザのレポート提出と一緒に、提出ユーザによって法定額の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、(ii) 提出ごとに法定額の支払いを必ず必要とする提出機構を介して、すべて提出された複数のユーザ提出レポートを分析することにより、ステップ(b)の判定を実行することと、(iii) 真正性が自己検証可能なブロックチェーンデータセットの一部として、ユーザ提出レポートの少なくとも1つを公開することと、を含む。

40

【0170】

いくつかの実施形態では、方法は、(i) オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートを受信するステップであって、各ユーザ提出レポートが、自分のレポート提出と一緒に、提出ユーザによって法定額の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、(ii) 提出ごとに法定額の支払いを必ず必要とする提出機構を介して、すべて提出された複数のユーザ提出レポートを分析することにより、ステップ(b)の判定を実行することと、(iii) オンライン宛先が1つ以上の資産の不正な販売を申し出ていることを示す、複数のユーザ提出レポートと一緒に受信された複数の暗号通貨の支払い

50

から報奨金源を作成することと、(i v) 特定の提出ユーザの特定のユーザ提出レポートが正しいと判定される場合、次に、特定の提出ユーザに、特定の提出ユーザが自分のユーザレポートの提出と一緒に支払った法定額以上の額で、報奨金源の一部である法定額の支払いを分配することと、を含む。

【0171】

いくつかの実施形態では、方法は、(i) オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示す複数のユーザ提出レポートを受信するステップであって、各ユーザ提出レポートが、自分のレポート提出と一緒に、提出ユーザによって法定額の支払いを必ず必要とする提出機構を介して排他的に受信される、ユーザ提出レポートを受信することと、(i i) 提出ごとに法定額の支払いを必ず必要とする提出機構を介して、すべて提出された複数のユーザ提出レポートを分析することにより、ステップ(b)の判定を実行することと、(i i i) オンライン宛先が1つ以上の資産の不正な販売を申し出ていることを示す、複数のユーザ提出レポートと一緒に受信された複数の暗号通貨の支払いから報奨金源を作成することと、(i v) オンライン宛先が、1つ以上の資産の不正な販売を申し出ていることを示すユーザレポートを提出した提出ユーザの間で、報奨金源の少なくとも一部を分配することと、を含む。

【0172】

いくつかの実施形態では、方法は、(i) オンライン購入のために1つ以上の資産を申し出ている特定のオンライン催場が、信頼できるということを判定することと、(i i) 公的にアクセス可能な自己検証可能なブロックチェーンデータセットに、前記特定のオンライン催場が信頼できるという標識を公開することと、を含む。

【0173】

いくつかの実施形態では、方法は、(i) 暗号通貨トークンであるデジタル資産を生成して、暗号通貨トークンを電子デバイスのエンドユーザに配分することと、(i i) ユーザレポートの提出が、事前定義された受信者への暗号通貨トークンの支払いと一緒に実行されることを条件として、不正の可能性があるオンライン催場に関するユーザレポートの提出を受信するオンライン機構を生成することと、を含む。

【0174】

いくつかの実施形態では、方法は、(i) 暗号通貨のデジタルトークンを生成して、暗号通貨の前記デジタルトークンを電子デバイスの複数のエンドユーザに分配することと、(i i) 各ユーザレポートの提出が、事前定義された受信者への暗号通貨のデジタルトークンの支払いと一緒に実行されることを条件として、不正の可能性があるオンライン催場に関するユーザレポートの提出を受信することと、(i i i) それぞれの支払いに関するデータと一緒にエンドユーザの各々によって実行された、ユーザレポートの提出のコンテンツおよびメタデータをその中に組み込むブロックチェーンデータセットを生成することと、を含む。

【0175】

いくつかの実施形態では、方法は、(i) 暗号通貨のデジタルトークンを生成して、暗号通貨のデジタルトークンを電子デバイスの複数のエンドユーザに分配することと、(i i) 各ユーザレポートの提出が、事前定義された受信者への暗号通貨のデジタルトークンの支払いと一緒に実行されることを条件として、不正の可能性があるオンライン催場に関するユーザレポートの提出を受信することと、(i i i) 不正が起こり得るオンライン催場に関する1つ以上のユーザレポートの正確性に関して、コミュニティの合意が到達されると判定するステップと、(i v) 少なくともステップ(i i i)に基づいて、不正が起こり得るオンライン催場の承認または非承認のいずれかのデジタルスタンプを生成して、デジタルスタンプを、ユーザレポートをも含む自己検証可能なブロックチェーンデータセットに公開することと、を含む。

【0176】

いくつかの実施形態では、方法は、(i) 暗号通貨のデジタルトークンを生成して、暗号通貨のデジタルトークンを電子デバイスの複数のエンドユーザに分配することと、(i

i) 各ユーザレポートの提出が、事前定義された受信者への暗号通貨のデジタルトークンの支払いと一緒に実行されることを条件として、不正の可能性のあるオンライン催場に関するユーザレポートの提出を受信することと、(iii) ユーザレポートの提出と一緒に、事前定義された受信者に支払われた前記デジタルトークンの少なくとも一部を含む保証資金を生成することと、(iv) その後、不正であると判定されたオンライン催場からの資産を購入した特定のエンドユーザに、保証資金の少なくとも一部を分配することと、を含む。

【0177】

いくつかの実施形態では、方法は、(i) 暗号通貨のデジタルトークンを生成して、暗号通貨のデジタルトークンを電子デバイスの複数のエンドユーザに分配することと、(ii) 各ユーザレポートの提出が、事前定義された受信者への暗号通貨のデジタルトークンの支払いと一緒に実行されることを条件として、不正の可能性のあるオンライン催場に関するユーザレポートの提出を受信することと、(iii) コンテンツとメタデータのオンライン宛先をレビューし、それらが真正であるか不正であるかを判定する欺瞞防止施行エンティティに、ユーザレポートの提出と一緒に事前定義の受信者に支払われたデジタルトークンの少なくとも一部を分配することと、を含む。

【0178】

いくつかの実施形態では、方法は、特定のオンライン催場で販売の申し出がされている特定の製品が、偽造であることを示すN件のユーザ提出レポートを受信することと、特定のオンライン催場で販売の申し出がされている特定の製品が、真正であることを示すM件のユーザ提出レポートを受信することと、N件のユーザ提出レポートおよびM件のユーザ提出レポート以外の少なくとも1つの追加パラメータまたはデータを考慮する分析に基づいて、合意は、特定のオンライン催場で販売の申し出がされている特定の製品が真正であるということであると判定することと、(i) N件のユーザ提出レポート、(ii) のM件のユーザ提出レポート、(iii) 合意の標識のうちの少なくとも1つをブロックチェーンデータセットに公開することと、特定の製品が真正であるというM件のユーザ提出レポートのうちの少なくとも1つを提出した少なくとも1人のユーザに報酬を提供することと、を含む。

【0179】

いくつかの実施形態では、方法は、特定のオンライン催場で販売の申し出がされている特定の製品が、偽造であることを示すN件のユーザ提出レポートを受信することと、特定のオンライン催場で販売の申し出がされている特定の製品が、真正であることを示すM件のユーザ提出レポートを受信することと、N件のユーザ提出レポートおよびM件のユーザ提出レポート以外の少なくとも1つの追加パラメータまたはデータを考慮する分析に基づいて、合意は、特定のオンライン催場で販売の申し出がされている前記特定の製品が偽造であるということであると判定することと、(i) N件のユーザ提出レポート、(ii) のM件のユーザ提出レポート、(iii) 合意の標識のうちの少なくとも1つをブロックチェーンデータセットに公開することと、特定の製品が偽造であるというN件のユーザ提出レポートのうちの少なくとも1つを提出した少なくとも1人のユーザに報酬を提供することと、を含む。

【0180】

いくつかの実施形態では、方法は、特定の電子メールメッセージが、スパムであることを示すN件のユーザ提出レポートを受信することと、特定の電子メールメッセージが、スパムでないことを示すM件のユーザ提出レポートを受信することと、N件のユーザ提出レポートおよびM件のユーザ提出レポート以外の少なくとも1つの追加パラメータまたはデータを考慮する分析に基づいて、合意は、特定の電子メールがスパムでないということであると判定することと、(i) N件のユーザ提出レポート、(ii) のM件のユーザ提出レポート、(iii) 合意の標識のうちの少なくとも1つをブロックチェーンデータセットに公開することと、特定の電子メールがスパムでないというM件のユーザ提出レポートのうちの少なくとも1つを提出した少なくとも1人のユーザに報酬を提供することと、を

10

20

30

40

50

含む。

【0181】

いくつかの実施形態では、方法は、特定の電子メールメッセージが、スパムであることを示すN件のユーザ提出レポートを受信することと、特定の電子メールメッセージが、スパムでないことを示すM件のユーザ提出レポートを受信することと、N件のユーザ提出レポートおよびM件のユーザ提出レポート以外の少なくとも1つの追加パラメータまたはデータを考慮する分析に基づいて、合意は、特定の電子メールがスパムであるということであると判定することと、(i) N件のユーザ提出レポート、(ii) M件のユーザ提出レポート、(iii) 合意の標識のうちの少なくとも1つをブロックチェーンデータセットに公開することと、特定の電子メールがスパムであるというN件のユーザ提出レポートのうちの少なくとも1つを提出した少なくとも1人のユーザに報酬を提供することと、を含む。

10

【0182】

いくつかの実施形態では、方法は、特定のオンライン催場がフィッシング催場であることを示すN件のユーザ提出レポートを受信することと、特定のオンライン催場がフィッシング催場でないことを示すM件のユーザ提出レポートを受信することと、N件のユーザ提出レポートおよびM件のユーザ提出レポート以外の少なくとも1つの追加パラメータまたはデータを考慮する分析に基づいて、合意は、特定のオンライン催場がフィッシング催場でないということであると判定することと、(i) N件のユーザ提出レポート、(ii) M件のユーザ提出レポート、(iii) 合意の標識のうちの少なくとも1つをブロックチェーンデータセットに公開することと、特定のオンライン催場がフィッシング催場でないというM件のユーザ提出レポートのうちの少なくとも1つを提出した少なくとも1人のユーザに報酬を提供することと、を含む。

20

【0183】

いくつかの実施形態では、方法は、特定のオンライン催場がフィッシング催場であることを示すN件のユーザ提出レポートを受信することと、特定のオンライン催場がフィッシング催場でないことを示すM件のユーザ提出レポートを受信することと、N件のユーザ提出レポートおよびM件のユーザ提出レポート以外の少なくとも1つの追加パラメータまたはデータを考慮する分析に基づいて、合意は、特定のオンライン催場がフィッシング催場であるということであると判定することと、(i) N件のユーザ提出レポート、(ii) M件のユーザ提出レポート、(iii) 合意の標識のうちの少なくとも1つをブロックチェーンデータセットに公開することと、特定のオンライン催場がフィッシング催場であるというN件のユーザ提出レポートのうちの少なくとも1つを提出した少なくとも1人のユーザに報酬を提供することと、を含む。

30

【0184】

いくつかの実装形態では、上述のMおよび／またはNは、正の数もしくは正の整数であり得、またはゼロ以上の数の場合があり、またはゼロ以上の整数であり得る。いくつかのシナリオでは、MはNより大きい場合があり、他のシナリオでは、MはNよりも小さい場合があり、いくつかのシナリオでは、MはNに等しい場合がある。いくつかの実施形態では、合意は、票数に排他的に依存するのではなく（たとえば、 $M > N$ か $N < M$ かだけに基

づいているわけではなく）、少なくとも1つの追加のパラメータまたはデータ項目または条件またはルールに基づく、特に上記のオンライン催場によって供給されたコンテンツの分析に基づく、および／またはそのようなコンテンツのメタデータに基づく、および／またはドメインの所有権またはウェブサイトの所有権に関するデータに基づく、および／または上記のウェブサイト上の製品の説明に関するデータに基づく、および／または外部データソースから取得したデータ（たとえば、製造業者が提供する認定流通業者または認定再販業者のホワイトリスト、商標とそのそれぞれの所有者のデータベース、組織またはブランドによって正当に所有または関連付けられている、認定または正当なエンティティまたは催場のリストまたはホワイトリストなど）に基づく方法で到達または判定される。いくつかの実施形態では、ブロックチェーンデータセットへのデータの公開または格納は、

40

50

任意選択のステップであり得、データは、プライベートデータベース、つまり、一定のユーザへの、および／または公衆への（たとえば、寄付金、またはクエリごとの料金、またはその他の料金の支払い時の）選択的アクセスを可能にし得る、プライベートデータベースに格納され得る。

【0185】

本明細書の説明の一部は、例証目的で、有線リンクおよび／または有線通信に関連しているが、いくつかの実施形態は、この点に限定されず、1つ以上の有線またはワイヤレスリンクを含み得、ワイヤレス通信の1つ以上のコンポーネントを利用し得、ワイヤレス通信の1つ以上の方法またはプロトコルを利用することなどができる。いくつかの実施形態は、有線通信および／またはワイヤレス通信を利用し得る。

【0186】

本発明のシステム（複数可）は、好適なハードウェアコンポーネントおよび／またはソフトウェアコンポーネント、たとえば、プロセッサ、プロセッサコア、中央処理装置（CPU）、デジタルシグナルプロセッサ（DSP）、回路、集積回路（IC）、コントローラ、メモリユニット、レジスタ、アキュムレータ、ストレージユニット、入力ユニット（たとえば、タッチスクリーン、キーボード、キーパッド、スタイラス、マウス、タッチパッド、ジョイスティック、トラックボール、マイクロフォン）、出力ユニット（たとえば、スクリーン、タッチスクリーン、モニター、ディスプレイユニット、オーディオスピーカなど）、音響マイクロフォン（複数可）および／またはセンサ（複数可）、光学マイクロフォン（複数可）および／またはセンサ（複数可）、レーザーまたはレーザーベースのマイクロフォン（複数可）および／またはセンサ（複数可）、有線またはワイヤレスのモデムまたはトランシーバまたはトランスミッタまたはレシーバ、GPSレシーバまたはGPS要素またはその他のロケーションベースまたはロケーション決定ユニットまたはシステム、ネットワーク要素（たとえば、ルータ、スイッチ、ハブ、アンテナ）、および／または他の好適なコンポーネントおよび／またはモジュール、を任意選択で備えてもよく、またはこれらを利用することによって実装されてもよい。本発明のシステム（複数可）は、同じ場所に配置されたコンポーネント、リモートコンポーネントまたはモジュール、「クラウドコンピューティング」サーバまたはデバイスまたはストレージ、クライアント／サーバアーキテクチャ、ピアツーピアアーキテクチャ、分散アーキテクチャ、および／または他の好適なアーキテクチャまたはシステムトポロジまたはネットワークトポロジを利用して、任意選択で実装されてもよい。

【0187】

本発明の実施形態によれば、計算、動作、および／または判定は、単一のデバイス内でローカルに実行するか、複数のデバイスによって、または複数のデバイスにわたって実行するか、部分的にローカルで、および、生データおよび／または処理済みデータおよび／または処理結果を交換するために、任意選択で通信チャネルを利用して、（たとえば、リモートサーバで）部分的にリモートで実行することができる。

【0188】

本発明の1つ以上の実施形態を参照して本明細書に記載された機能、動作、コンポーネントおよび／または特徴は、本発明の1つ以上の他の実施形態を参照して本明細書に記載された、1つ以上の他の機能、動作、コンポーネントおよび／または特徴と組み合わせるか、または組み合わせて利用することができる。したがって、本発明は、たとえそれらが上記説明の種々の箇所または種々の章で説明されているとしても、またはそれらが種々の図面または複数の図面にわたって示されているとしても、本明細書に記載されたモジュールまたは機能またはコンポーネントのいくつかまたはすべてのあらゆる可能なまたは好適な組み合わせ、再配設、組立、再組立、または他の利用を含むことができる。

【0189】

本発明のいくつかの例証的な実施形態の一定の特徴を本明細書で図示し記載してきたが、当業者にはさまざまな改変、置換、変更、および均等が思い浮かぶ可能性がある。したがって、特許請求の範囲は、そのようなすべての改変、置換、変更、および均等を網羅す

10

20

30

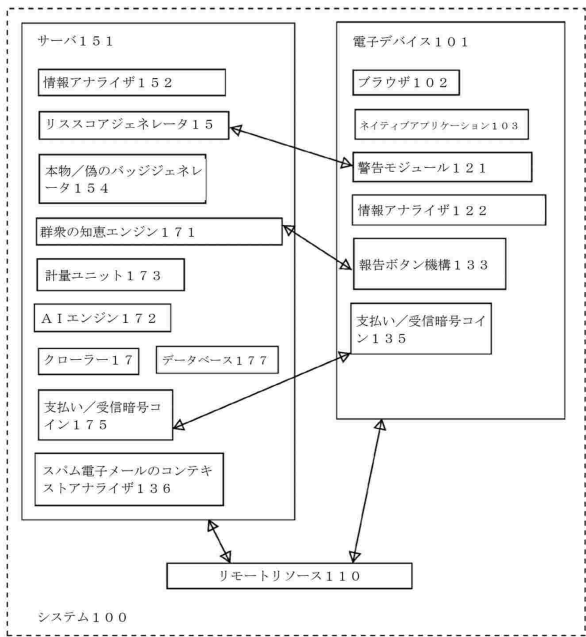
40

50

ることを意図している。

【図面】

【図 1】



10

20

30

40

50

フロントページの続き

審査官 加舎 理紅子
(56)参考文献 特開 2 0 0 6 - 2 8 5 8 4 4 (J P , A)
特開 2 0 1 7 - 2 0 4 7 0 7 (J P , A)
特開 2 0 0 9 - 1 1 0 3 3 4 (J P , A)
特表 2 0 1 6 - 5 2 4 2 0 2 (J P , A)
特開 2 0 1 5 - 1 8 7 7 7 9 (J P , A)
特表 2 0 0 9 - 5 0 0 7 2 9 (J P , A)
特開 2 0 1 6 - 1 2 6 6 1 5 (J P , A)
(58)調査した分野 (Int.Cl., D B 名)
G 0 6 Q 1 0 / 0 0 - 9 9 / 0 0