

(19)日本国特許庁(JP)

(12)公表特許公報(A)

(11)公表番号

特表2022-511547

(P2022-511547A)

(43)公表日 令和4年1月31日(2022.1.31)

(51)国際特許分類

F I

G 0 6 F 21/32 (2013.01)

G 0 6 F 21/32

G 0 6 F 21/64 (2013.01)

G 0 6 F 21/64

G 0 6 F 21/44 (2013.01)

G 0 6 F 21/44

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2021-532187(P2021-532187)	(71)出願人	000002185
(86)(22)出願日	令和1年12月12日(2019.12.12)		ソニーグループ株式会社
(85)翻訳文提出日	令和3年7月29日(2021.7.29)		東京都港区港南1丁目7番1号
(86)国際出願番号	PCT/EP2019/084886	(74)代理人	110003339
(87)国際公開番号	WO2020/120672		特許業務法人南青山国際特許事務所
(87)国際公開日	令和2年6月18日(2020.6.18)	(74)代理人	100104215
(31)優先権主張番号	18212793.6		弁理士 大森 純一
(32)優先日	平成30年12月14日(2018.12.14)	(74)代理人	100168181
(33)優先権主張国・地域又は機関	欧州特許庁(EP)		弁理士 中村 哲平
(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,A T,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR ,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC, 最終頁に続く	(74)代理人	100117330
			弁理士 折居 章
		(74)代理人	100168745
			弁理士 金子 彩子
		(72)発明者	若林 秀治
			イギリス ベイジングストーク ハンプシ 最終頁に続く

(54)【発明の名称】 通信ネットワークノード、方法、およびモバイル端末

(57)【要約】

本開示は、データを分散型台帳に提供するための通信ネットワークノードであって、ノードは、スマートコントラクトへの入力として使用される入力データの検証を提供すること、および、スマートコントラクトからの出力に基づく出力データが、所定のデバイスで正しく受信されるかどうかの検証を提供することのうちの少なくとも1つを実行するように構成された回路を具備する通信ネットワークノードを提供する。

【選択図】 図7

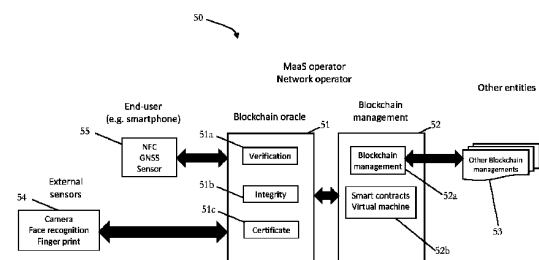


Fig. 7

【特許請求の範囲】

【請求項 1】

データを分散型台帳に提供するための通信ネットワークノードであって、ノードは、スマートコントラクトへの入力として使用される入力データの検証を提供すること、および、スマートコントラクトからの出力に基づく出力データが、所定のデバイスで正しく受信されるかどうかの検証を提供すること
のうちの少なくとも1つを実行するように構成された回路を具備する通信ネットワークノード。

【請求項 2】

請求項 1 に記載の通信ネットワークノードであって、
前記入力データは、ユーザを識別するセンサデータに基づいて検証される通信ネットワークノード。

【請求項 3】

請求項 2 に記載の通信ネットワークノードであって、
前記センサデータは、ユーザのモバイル端末に含まれる少なくとも1つのセンサによって提供される通信ネットワークノード。

【請求項 4】

請求項 2 に記載の通信ネットワークノードであって、
前記センサデータは、ユーザを検出する少なくとも1つのセンサによって提供される通信ネットワークノード。

【請求項 5】

請求項 2 に記載の通信ネットワークノードであって、
前記回路は、前記センサデータを提供するセンサの認証を提供するようにさらに構成される通信ネットワークノード。

【請求項 6】

請求項 2 に記載の通信ネットワークノードであって、
前記センサデータは、位置データまたは生体認証データを含む通信ネットワークノード。

【請求項 7】

請求項 6 に記載の通信ネットワークノードであって、
前記位置データは、検証のためにロケーションサーバに送信される通信ネットワークノード。

【請求項 8】

請求項 6 に記載の通信ネットワークノードであって、
前記生体認証データは、検証のために生体認証データサーバに送信される通信ネットワークノード。

【請求項 9】

請求項 1 に記載の通信ネットワークノードであって、
前記回路は、データ完全性機能に基づいてデータを受信または送信するようにさらに構成される通信ネットワークノード。

【請求項 10】

請求項 9 に記載の通信ネットワークノードであって、
前記データ完全性機能は、ハッシュ関数、デジタル署名、ブロックストリームアルゴリズムのうちの少なくとも1つに基づくものである通信ネットワークノード。

【請求項 11】

請求項 1 に記載の通信ネットワークノードであって、
前記回路は、前記スマートコントラクトの実行を引き起こすためのトリガを送信するようにさらに構成される
通信ネットワークノード。

【請求項 1 2】

請求項 1 1 に記載の通信ネットワークノードであって、
前記トリガは、入力データの検証が成功した場合に送信される
通信ネットワークノード。

【請求項 1 3】

請求項 1 に記載の通信ネットワークノードであって、
前記回路は、ユーザベースの識別とモバイル端末ベースの識別との間のバインディングを実行するようにさらに構成される
通信ネットワークノード。

10

【請求項 1 4】

請求項 1 3 に記載の通信ネットワークノードであって、
前記検証は、バインディングの検証を含む
通信ネットワークノード。

【請求項 1 5】

請求項 1 3 に記載の通信ネットワークノードであって、
前記モバイル端末ベースの識別は、セルラ国際移動体加入者識別番号およびセルラ国際移動体装置識別番号のうちの少なくとも1つを含む
通信ネットワークノード。

20

【請求項 1 6】

請求項 1 に記載の通信ネットワークノードであって、
前記回路は、接続されたデバイスの認証を検証するようにさらに構成される
通信ネットワークノード。

【請求項 1 7】

請求項 1 6 に記載の通信ネットワークノードであって、
前記接続されたデバイスの認証は、ハッシュ関数に基づく認証、規格ベース認証、前記接続されたデバイスの製造者識別番号、デバイスの事前設定、および、前記接続されたデバイスに関連する固有のネットワークまたはセルラ識別のうちの少なくとも1つに基づいて
検証される
通信ネットワークノード。

30

【請求項 1 8】

請求項 1 に記載の通信ネットワークノードであって、
前記分散型台帳は、ブロックチェーンを含む
通信ネットワークノード。

【請求項 1 9】

請求項 1 に記載の通信ネットワークノードであって、
前記分散型台帳は、モビリティ・アズ・ア・サービス用のデータを含む
通信ネットワークノード。

40

【請求項 2 0】

請求項 1 に記載の通信ネットワークノードであって、
前記分散型台帳へのアクセスは、許可権に基づいて付与される
通信ネットワークノード。

【請求項 2 1】

請求項 2 0 に記載の通信ネットワークノードであって、
前記ノードは、コンソーシアムの一部である
通信ネットワークノード。

【請求項 2 2】

50

スマートコントラクトを動作させるための方法であって、前記スマートコントラクトは、少なくとも2つの異なる状態を有し、トリガを受信することに応答して前記スマートコントラクトの状態を変更するステップを含む方法。

【請求項 2 3】

請求項 2 2 に記載の方法であって、前記少なくとも2つの異なる状態は、チェックイン状態、チェックアウト状態、使用中状態、未使用状態およびキャンセル状態のうちの少なくとも1つを含む方法。

10

【請求項 2 4】

請求項 2 2 に記載の方法であって、前記トリガは、信頼されたネットワーク通信ノードから受信される方法。

【請求項 2 5】

請求項 2 2 に記載の方法であって、前記トリガは、信頼されたセンサから受信される方法。

【請求項 2 6】

請求項 2 2 に記載の方法であって、前記スマートコントラクトは、前記トリガの受信に応答して実行される方法。

20

【請求項 2 7】

請求項 2 6 に記載の方法であって、前記スマートコントラクトの実行結果は、スマートコントラクトの状態によって決まる方法。

【請求項 2 8】

分散型台帳を提供するための複数のノードを具備する通信ネットワークを制御するための方法であって、スマートコントラクトへの入力として使用される入力データの検証を提供するステップと、スマートコントラクトからの出力に基づく出力データが、所定のデバイスで正しく受信されるかどうかの検証を提供するステップと、のうちの少なくとも1つを含む方法。

30

【請求項 2 9】

請求項 2 8 に記載の方法であって、前記入力データは、ユーザを識別するセンサデータに基づいて検証される方法。

【請求項 3 0】

請求項 2 9 に記載の方法であって、前記センサデータは、ユーザのモバイル端末に含まれる少なくとも1つのセンサによって提供される方法。

40

【請求項 3 1】

請求項 2 9 に記載の方法であって、前記センサデータは、ユーザを検出する少なくとも1つのセンサによって提供される方法。

【請求項 3 2】

請求項 2 9 に記載の方法であって、

50

前記センサデータを提供するセンサの認証を提供するステップをさらに含む方法。

【請求項 33】

請求項 29 に記載の方法であって、
前記センサデータは、位置データまたは生体認証データを含む方法。

【請求項 34】

請求項 33 に記載の方法であって、
検証のために前記位置データをロケーションサーバに送信するステップをさらに含む方法。

10

【請求項 35】

請求項 33 に記載の方法であって、
検証のために生体認証データを生体認証データサーバに送信するステップをさらに含む方法。

【請求項 36】

請求項 28 に記載の方法であって、
データ完全性機能に基づいてデータを受信または送信するステップをさらに含む方法。

【請求項 37】

請求項 36 に記載の方法であって、
前記データ完全性機能は、ハッシュ関数、デジタル署名およびブロックストリームアルゴリズムのうちの少なくとも1つに基づく方法。

20

【請求項 38】

請求項 28 に記載の方法であって、
前記スマートコントラクトの実行を引き起こすためのトリガを送信するステップをさらに含む方法。

【請求項 39】

請求項 38 に記載の方法であって、
前記トリガは、前記入力データの検証が成功した場合に送信される方法。

30

【請求項 40】

請求項 38 に記載の方法であって、
前記トリガは、ユーザの識別、ユーザのロケーションベースの検出、および、ユーザの生体認証に基づく検出のうちの少なくとも1つに基づいて送信される方法。

【請求項 41】

請求項 40 に記載の方法であって、
前記ロケーションベースの検出は、ユーザのデバイスによって提供されるロケーションデータと、ユーザのネットワークベースの測位とに基づいて、ユーザの位置を確認することを含む方法。

40

【請求項 42】

請求項 40 に記載の方法であって、
前記ロケーションベースの検出は、ユーザを識別するための視覚処理を含む方法。

【請求項 43】

請求項 28 に記載の方法であって、
ユーザベースの識別とモバイル端末ベースの識別との間のバインディングを実行するステ

50

ップをさらに含む

方法。

【請求項 4 4】

請求項 4 3 に記載の方法であって、
前記検証は、前記バインディングの検証を含む
方法。

【請求項 4 5】

請求項 4 3 に記載の方法であって、
前記モバイル端末ベースの識別は、セルラ国際移動体加入者識別番号およびセルラ国際移動体装置識別番号のうちの少なくとも1つを含む
方法。

10

【請求項 4 6】

請求項 2 8 に記載の方法であって、
接続されたデバイスの認証を検証するステップをさらに含む
方法。

【請求項 4 7】

請求項 4 6 に記載の方法であって、
前記接続されたデバイスの認証は、ハッシュ関数に基づく認証、規格ベース認証、前記接続されたデバイスの製造者識別番号、前記デバイスの事前設定、および、前記接続されたデバイスに関連する固有のネットワークまたはセルラ識別のうちの少なくとも1つに基づいて検証される
方法。

20

【請求項 4 8】

請求項 2 8 に記載の方法であって、
前記分散型台帳は、ブロックチェーンを含む
方法。

【請求項 4 9】

請求項 2 8 に記載の方法であって、
前記分散型台帳は、モビリティ・アズ・ア・サービス用のデータを含む
方法。

30

【請求項 5 0】

請求項 2 8 に記載の方法であって、
前記分散型台帳へのアクセスは、許可権に基づいて付与される
方法。

【請求項 5 1】

請求項 5 0 に記載の方法であって、
前記複数のノードは、コンソーシアムの一部である
方法。

【請求項 5 2】

請求項 2 8 に記載の方法であって、
前記検証の提供は、スマートコントラクトが改ざんされるリスクに基づく
方法。

40

【請求項 5 3】

請求項 5 2 に記載の方法であって、
前記検証は、前記リスクに基づいて省略または制限される
方法。

【請求項 5 4】

分散型台帳にデータを提供するためのネットワークノードと通信するためのモバイル端末であって、
スマートコントラクトへの入力として使用される入力データを提供するように構成された

50

回路を具備する

モバイル端末。

【請求項 5 5】

請求項 5 4 に記載のモバイル端末であって、

少なくとも 1 つのセンサをさらに備え、前記入力データは、前記少なくとも 1 つのセンサのセンサデータに基づいて提供される

モバイル端末。

【請求項 5 6】

請求項 5 5 に記載のモバイル端末であって、

前記少なくとも 1 つのセンサは、位置データまたは生体認証データを提供する

10

モバイル端末。

【請求項 5 7】

請求項 5 4 に記載のモバイル端末であって、

前記回路は、アプリケーションを実行するようにさらに構成され、前記アプリケーションは、前記ネットワークノードに前記入力データを提供するように構成される

モバイル端末。

【請求項 5 8】

請求項 5 7 に記載のモバイル端末であって、

前記アプリケーションは、モビリティ・アズ・ア・サービスのアプリケーションである

20

モバイル端末。

【請求項 5 9】

請求項 5 4 に記載のモバイル端末であって、

前記モバイル端末は、スマートフォンである

モバイル端末。

【請求項 6 0】

請求項 5 7 に記載のモバイル端末であって、

前記アプリケーションは、ユーザの認証を行うように構成される

モバイル端末。

【請求項 6 1】

請求項 5 8 に記載のモバイル端末であって、

30

前記アプリケーションは、前記モバイル端末のセンサによって提供されるセンサデータに基づいて、ユーザのチェックインを判定するように構成される

モバイル端末。

【請求項 6 2】

請求項 5 7 に記載のモバイル端末であって、

前記回路は、前記モバイル端末と前記アプリケーションとの間のバインディングを実行するようにさらに構成される

モバイル端末。

【請求項 6 3】

請求項 6 2 に記載のモバイル端末であって、

40

前記バインディングは、認証に基づいて実行される

モバイル端末。

【請求項 6 4】

請求項 6 2 に記載のモバイル端末であって、

前記認証は、前記ネットワークノードから受信される

モバイル端末。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は概して、通信ネットワークノード、スマートコントラクトを動作させるための方

50

法、通信ネットワークを制御するための方法、およびモバイル端末に関する。

【背景技術】

【0002】

一般に、デジタル取引を記録するエンティティ、例えば、電子デバイス、サーバ等の複数のノード上に台帳を分散させることが知られている。分散型台帳は、既知のブロックチェーン技術に基づくことができ、これに基づいて、例えば、既知の暗号通貨ビットコインがベースとされるが、周知のイーサリアムプロジェクトなどもベースとされる。

一般に、分散型台帳は、ブロックチェーン技術以外の他の技術に実装されてもよく、ブロックチェーンに基づいていない分散型台帳プロジェクトの例は、BigchainDBおよびIOTAなどである。たとえば、IOTAは、リンクリストを使用する暗号通貨である。

10

【0003】

また、モビリティ・アズ・ア・サービス(MaaS)が知られており、ユーザまたは旅行者(乗客)は例えば、自動車等を借りずにモビリティ・アズ・ア・サービス(MaaS)を使用する。モビリティ・アズ・ア・サービスは、関連する事業者またはプロバイダからの公共(例えば、列車、バスなど)および個人(例えば、カーシェアリング、自転車シェアリングなど)の輸送(トランスポート)サービスを組み合わせることができる。

【0004】

公知のMaaSソリューションは、典型的には旅行または旅行が計画され予約される中央の統一されたゲートウェイを含み、ユーザは、単一のアカウントで支払うことができる。

【0005】

分散型台帳、モビリティ・アズ・ア・サービスおよび関連する通信を提供するための技術が存在するが、一般に、分散型台帳を提供するための通信ネットワークノード、スマートコントラクトを動作させるための方法、および、通信ネットワークを制御するための方法を提供することが望ましい。

20

【発明の概要】

【0006】

第1の態様によれば、本開示は、データを分散型台帳に提供するための通信ネットワークノードであって、ノードは、スマートコントラクトへの入力として使用される入力データの検証を提供すること、および、スマートコントラクトからの出力に基づく出力データが、所定のデバイスで正しく受信されるかどうかの検証を提供することのうちの少なくとも1つを実行するように構成された回路を具備する通信ネットワークノードを提供する。

30

【0007】

第2の態様によれば、本開示は、スマートコントラクトを動作させるための方法であって、上記スマートコントラクトは、少なくとも2つの異なる状態を有し、トリガを受信することに応答して上記スマートコントラクトの状態を変更するステップを含む方法を提供する。

【0008】

第3の態様によれば、本開示は、分散型台帳を提供するための複数のノードを具備する通信ネットワークを制御するための方法であって、スマートコントラクトへの入力として使用される入力データの検証を提供するステップと、スマートコントラクトからの出力に基づく出力データが、所定のデバイスで正しく受信されるかどうかの検証を提供するステップとのうちの少なくとも1つを含む方法を提供する。

40

【0009】

第4の態様によれば、本開示は、分散型台帳にデータを提供するためのネットワークノードと通信するためのモバイル端末であって、スマートコントラクトへの入力として使用される入力データを提供するように構成された回路を備えるモバイル端末を提供する。

【0010】

さらなる態様は、従属請求項、以下の説明および図面に記載される。

【図面の簡単な説明】

【0011】

50

本発明の実施形態は、添付の図面を参照して例として説明される。

【図 1】 1つのブロックチェーンを概略的に示す。

【図 2】 ブロックチェーンにおけるハッシュ法を概略的に示す。

【図 3】 コンセンサスプロトコルの一実施形態を示すフローチャートである。

【図 4】 1つのMaaSシステムにおけるデータフローを示す。

【図 5】 旅行ログデータを含むブロックチェーンの一実施形態を示す。

【図 6】 ブロックチェーンを提供するための通信ネットワークの一実施形態を示す。

【図 7】 ブロックチェーン・オラクルを実装するMaaSシステムの一実施形態のデータフローを示す。

【図 8】 スマートコントラクトの状態遷移を示す遷移図である。

【図 9】 ブロックチェーン・オラクルを用いてスマートコントラクトのトリガを実施する方法の一実施形態のフローチャートを示す。

【図 10】 ロケーションベースのチェックインの方法の一実施形態のフローチャートを示す。

【図 11】 生体認証ベースのチェックインの方法の一実施形態のフローチャートを示す。

【図 12】 バインディング手順の方法の一実施形態のフローチャートを示す。

【図 13】 検証手順の方法のフローチャートを示す。

【図 14】 汎用コンピュータの一実施形態を示しており、いくつかの実施形態においては、この汎用コンピュータに基づいて、ネットワーク機器または通信デバイスが実装される。

【図 15】 互いに通信するeNodeBおよびユーザ機器の一実施形態を示す。

【発明を実施するための形態】

【0012】

図 1 を参照して実施形態を詳細に説明する前に、一般的な説明をする。

【0013】

冒頭で述べたように、一般に、分散型台帳およびモビリティ・アズ・ア・サービス(MaaS)が知られている。

【0014】

本開示は一般に、いくつかの実施形態または態様において、モビリティ・アズ・ア・サービス(MaaS)アプリケーションのためのブロックチェーン/分散型台帳、特に、2つ以上のサービス・プロバイダ(複合一貫輸送)間のMaaSのアプリケーションに関する。

【0015】

また本開示は、概して、いくつかの実施形態または態様において、本開示をブロックチェーンに限定することなく、分散型台帳またはブロックチェーンを分散型台帳の一例として適用することに関する。

分散型台帳は、マルチプレーヤー間の旅行履歴(すなわち旅行データ)のための分散型データベース、すなわちサービス・プロバイダとしての複数のモビリティを必要とするので、分散型台帳またはブロックチェーンは、本開示のいくつかの態様によるモビリティ・アズ・ア・サービス(MaaS)アプリケーションに適していると認識される。

【0016】

分散型台帳およびその特別な例、すなわちブロックチェーンの技術についても、以下でさらに説明する。より一般的には、分散型台帳という用語は、ネットワークの複数のノードとデジタル的に記録されたデータを共有するデータベースの一種として使用される。

分散型台帳は、ピアツーピアネットワークで構成される場合がある。デジタル的に記録されたデータは、同じデータベース上の以前に記録されたデータからその一貫性を証明するための一種の情報を含んでもよい。

【0017】

分散型台帳は公開することができ、誰でもアクセスすることができるが、原則として、非公開とすることもでき、許可を有するユーザのみがそれらにアクセスすることができ、許可を有するエンティティ、ノード、人物、事業者(オペレータ)、プロバイダなどのグル

10

20

30

40

50

ープは以下でさらに説明するように、「コンソーシアム」とも呼ばれることがある。
また、階層化されたユーザ毎に、台帳のデータへのアクセス許可を区別することも可能である。

【0018】

分散型台帳は例えば、ビットコインに使用されるようなブロックチェーン技術から既知のメカニズムを使用することができる。このようなメカニズムには、発見方法、コンセンサスメカニズム、データの一貫性を保つメカニズムなどが含まれる。

コンセンサスメカニズムは、分散型台帳のコピーを有するすべてのノードまたは一定数より多いノード、一般的には電子機器が、分散型台帳のコンテンツに関するコンセンサスに達することを保証する。

いわゆる、暗号パズルの一種であり、例えば、ブロックチェーンの古いブロックが(容易に)変更され得ないことを保証する、いわゆる、プルーフ・オブ・ワークメカニズムを含む、多くのコンセンサスメカニズムがある。

例えば、ビットコイン・ブロックチェーンのマイニングプロセスには、プルーフ・オブ・ワークが用いられる。

【0019】

分散型台帳またはブロックチェーンでは、マイニングプロセスと呼ばれる、参加ノードにおけるブロックチェーン上のデータ更新に関するコンセンサスを作成する承認プロセスが、承認データにおいて以前に記録されたデータを含めることによって、ブロックチェーン上に記録された取引のシーケンスの不可逆性を達成することができる。

このようなマイニングプロセスは、新しい取引ブロックの分散タイム・スタンプ・サーバーを実装する。ビットコインでは(したがって、いくつかの実施形態では)、マイニングプロセスは、SHA256ハッシュ関数に基づく。

ハッシュ関数の入力が、ブロックチェーンの現在のブロックおよびブロックチェーンに追加されるべき取引の新しいブロックによって決まる一方で、マイニングプロセスに関与するブロックチェーンのノードは、事前定義されたプロパティを有するハッシュ出力を検索する。

【0020】

ハッシュ関数に基づくプルーフ・オブ・ワーク計算は、分散型台帳の不可逆性を実装するために必要とされることを除いて、それ自体では有用でなくてもよい。

【0021】

さらに、一般に、様々なデータを記憶するためにブロックチェーンを使用することが知られている。例えば、画像、ビデオ、測定値、およびテキストファイルは、取引の形式でブロックチェーンに記録できる。

【0022】

いくつかの実施形態では、MaaSブロックチェーンが、多数の旅行者(乗客)を取り扱うこと、様々なタイプの旅行履歴を記憶すること、大きなサイズのブロックを記憶すること、ラッシュアワーにおける処理のピークを記憶することなどを必要とし得る。

【0023】

いくつかの実施形態では一般に、分散型台帳またはブロックチェーンは、複数のプレーヤ間の旅行履歴用の分散型データベースを提供するので、MaaSアプリケーションに適しているが、その点に関して本開示を限定するものではない。

【0024】

さらに、いくつかの実施形態では、スマートコントラクトが、例えばMaaSのために使用される。例えば、チケットまたはMaaSサービスは、乗客とサービス・プロバイダ/事業者との間の合意に基づいて提供される。

したがって、いくつかの実施形態の通常の場合(例えば、チケットを購入すること)または通常以外の例外的な場合/手順(例えば、チケットを単に購入すること)が、スマートコントラクトで対処されてもよい。スマートコントラクトは、通常の手順に加えて、これらの例外的な手順を取り扱うことができる。

10

20

30

40

50

【0025】

いくつかの実施形態では、スマートコントラクトは、ブロックチェーンにおけるコンピュータ言語ベースのコントラクトである。

以下でさらに詳細に説明されるように、スマートコントラクトは、1つ以上のセンサからの所定の入力、人間からのユーザインターフェース入力、他のサーバからのアプリケーションインターフェース(API)呼び出しなど、所定の条件が満たされた場合に自動的に実行されてもよい。

【0026】

いくつかの実施形態では、スマートコントラクトの成功要因が、現実世界からの/への真正な入力(および出力)を保証することであってもよく、いくつかの実施形態ではブロックチェーン・オラクル(例えば、サーバ)が、外部入力(例えば、センサ)とスマートコントラクトとの間に提供され、スマートコントラクトに責任を負う。

10

【0027】

MaaSアプリケーション(または他のアプリケーション)のためのスマートコントラクトをどのように使用するかという課題が問題であり、いくつかの例では、スマートコントラクトが、実行のための信頼できる入力を得ることが重要であり得ることが認識されている。

【0028】

第1の例として、いくつかの実施形態ではスマートコントラクトは、ブロックチェーンだけで実行されないが、特定のアプリケーションに関連する入出力システムのようなシステムが必要とされ得る。

20

例えば、いくつかの実施形態ではMaaSアプリケーションは、乗客のチェックインを検出する必要があり、したがって、いくつかの実施形態ではこれに対処し、システムアーキテクチャ、ノード/サーバなどに対処する。

【0029】

第2の例として、スマートコントラクトは、センサまたは任意の入出力からの真正な入力/出力に依存し得る。

暗号通貨の場合、数字のみが転送され得るが、例えば、MaaSアプリケーションは、実際の物理的世界と関わる必要がある(例えば、列車に乗ること、自転車のロックを解除すること、正しい位置に乗車シェアを呼び出してそれに乗車することなど)。

いくつかの実施形態では、以下で「ブロックチェーン・オラクル」と呼ばれるノードが、スマートコントラクトに対する正しい入力/出力を保証するために提供されてもよい。

30

【0030】

さらに、いくつかの実施形態は、MaaSアプリケーションのための具体的な手順に関する。

以下に、本開示で論じられる実施形態の簡単な概要を示す。

【0031】

システムアーキテクチャ

MaaSシステムのデータフロー(先発明の要旨)

スマートコントラクト用の追加機能/ノード

スマートコントラクトの例

疑似コード例

スマートコントラクト実行のトリガ

従来のIDソリューション

位置ベースの(ジオフェンシング)ソリューション

生体認証ベースのソリューション

その他のブロックチェーン・オラクル関数

データ完全性チェック

センサ/端末の認証/信用証明書のチェック

ハードウェア/スマートフォン/ウェアラブルの固有IDを使用した

結合手順

40

50

検証手順

【0032】

以下では、ブロックチェーンおよびその一般的なデータ構造を、図1を参照して説明する。この実施形態のブロックチェーンの特徴は、ネットワーク/トポロジー、コンセンサスアルゴリズム、ハッシュ関数、参加認証、スケーラビリティ/ブロック構造およびパフォーマンスである。

【0033】

図1は、ブロックチェーン1の一般的な構造を示す。

ブロックチェーン1は、複数のデータブロック2a、2b、および2cのチェーンを含み、ブロック2bは、現在のブロック(ブロック#N)であり、ブロック2aは、前のブロック(ブロック#N-1)であり、ブロック2cは、今後すなわち後続のブロック(ブロック# N+1)である。

各ブロックは、前のブロックのハッシュ関数の結果、主要なデータ構造体、現在のブロックのハッシュ関数への入力値およびハッシュ関数の結果を含み、現在のブロック(2b)のハッシュ関数結果は、常に次のブロック(2c)への入力として使用される。

【0034】

また、各ブロックには、安全なブロックチェーン処理のための1回限りの乱数であり、反射攻撃(リプレイアタック)を防ぐことができる「ナンス (Number used once、一度だけ使用される使い捨ての数字)」が含まれている。

例えば、攻撃者が、以前に送信したデータをコピーし、再度コピーしたデータをスプーフィング(なりすまし)に再利用する場合、次のデータを別の「ナンス」で使用しなければならないため、受信者は、スプーフィング通信を検出することができる。この乱数は、暗号通貨では「ノンス」と呼ばれることもある。

【0035】

さらに、タイムスタンプが、ブロック2a、2b、および2cのそれぞれに挿入されてもよい。ブロックチェーン1は、例えば、いくつかの実施形態においてMaaSを提供するために使用され得る、分散型台帳の一例である。

【0036】

図2は、例えば図1のブロックチェーン1に使用されるハッシュ関数の入出力を示す。

【0037】

一般に、ハッシュ関数は、特定のアルゴリズムで入力データを出力データにマッピングするために使用可能な任意の関数である。入力データのサイズは大きく、様々であり、逆に、データの出力はコンパクトであり、固定サイズを有することが可能である。

いくつかのブロックチェーンの実施形態においてハッシングに使用される既知の(および有名な)アルゴリズムは、米国国家安全保障機関(例えば、SHA-2、SHA-256)によって設計されたセキュアハッシュアルゴリズム(SHA)である。

【0038】

ハッシュ関数への入力値は、以前のハッシュ出力、ナンス、および現在のブロック(例えば、図1のブロック2b)内のデータの本体である。ハッシュ関数の出力は、入力値に対する固有の応答値である。誰かがデータの本体を改ざんしようとする、ハッシュ関数の出力に一貫性がなくなる。

【0039】

本開示における分散型台帳(ブロックチェーン)の実施形態は、コンセンサスプロトコルまたはアルゴリズムを実装することができる。

例えば、いくつかの実施形態では、ビザンチン・フォールトトレラント性(BFT)がコンセンサスプロトコルに使用され、これはデータベースのスプーフィングおよびハードウェアの故障に対する回復機能がある。

【0040】

いくつかの実施形態で実施される周知のコンセンサスアルゴリズムは、いわゆる実用的なビザンチン・フォールトトレラント性(PBFT)である。

10

20

30

40

50

【0041】

いくつかの実施形態では、許可ブロックチェーンが使用され、比較的少数の許可ブロックチェーンノードがコンセンサス(ブロックの検証)を担当する。

【0042】

図3は、PBFTの処理10を例示している。

【0043】

リーダノード(非承認ピアとも呼ばれる)は、ステップ11において、他のノードにおいてブロックチェーンを検証する要求をする。ステップ12では、要求された各ノード(承認ピア)が、ハッシュ関数を使用してブロックチェーンの有効性を確認し、ステップ13においてその結果を他のノードに示す。

10

ステップ14において、1つのノードが、複数の他のピアから有効性結果を受信し、所定の基準よりも有効な結果を受信した場合には、ブロックチェーンのコンセンサスを確認する。コンセンサスがある場合、ステップ15で、そのノードは、ブロックチェーンを書き込み/終了する。

リーダピアは、他のノードにおける有効性確認の全体的な進行を確認し、ステップ16においてブロックチェーン手順を終了させる。

【0044】

回復力のために、ノードの総数は、いくつかの実施形態では $3f+1$ を超え、ここで、 f は許容される故障ノードの数である。たとえば、 $f=1$ の場合、合計4ノードがある。 $f=3$ の場合、合計10ノードがあり、その他の場合もある。

20

【0045】

いくつかの実施形態では、PBFTが本明細書で説明されるように、モビリティ・サービス・ブロックチェーンのための許可ブロックチェーンを有し、以下の特徴を少なくとも部分的に提供する。

セキュリティに関しては、PBFTは、いくつかの実施形態では、51%攻撃のわずかなリスクを提供するが、これはコンセンサスを担当するピアの許可が信頼されなければならないため、暗号通貨に共通である。

プライバシーに関しては、(許可ベースのブロックチェーンのため、かつ、エンドユーザがブロックチェーン全体にアクセスする許可を有さないため)モビリティ・サービス・プロバイダのみが、(ピア)ノードにおいてブロックチェーン全体を処理するので、エンドユーザは、ブロックチェーン全体にアクセスすることができない。

30

パフォーマンスに関しては、コンセンサスのための処理時間は、いくつかの実施形態では、高性能を有するピアの数が少ないため、非常に短い。柔軟性に関しては、ブロックチェーンのブロックサイズおよびフォーマットは、いくつかの実施形態ではパブリック・ブロックチェーンと比較して柔軟である。

【0046】

以下、MaaSシステム20のデータフローを、全体的なデータフローを示す図4を参照して説明する。MaaSシステム20では、エンドユーザが、例えばスマートフォン(または他の任意のタイプの電子(モバイル)デバイス)のような自身の端末21を有することが例示的に想定される。

40

いくつかのユーザ(例えば、海外からの訪問者)は、スマートフォンまたは同種のものを有していない場合があり、そのような場合、例えば、ユーザにゲートを提供する図4のプロキシ機能(プロキシ22)に基づく代替のソリューションを提供することができる。

【0047】

図4は、MaaSシステム20のデータフロー図を示し、3つの主要部、左側のエンドユーザ部、中央のモビリティ・サービス・オペレータ/プロバイダ部、および、右側の他のエンティティ部が提供され、ここでエンドユーザ部および他のエンティティ部は、中央のモビリティ・サービス・オペレータ部と通信する。

【0048】

この実施形態のMaaSシステム20では、モビリティ・サービス・プロバイダが、カスタ

50

マーサービス用のウェブサーバまたはクラウドと、ユーザプロフィール管理機能23aおよび乗客旅行管理機能23bとを備えたユーザ管理機能23を有するものとする。モビリティ・サービス・プロバイダは、ブロックチェーン管理機能24をさらに有する。ブロックチェーン管理機能24aを有するブロックチェーン機能24は、他のエンティティ部のブロックチェーン管理機能25と通信する。座席予約/シェアされる乗り物予約が、予約センタ26によって提供される場合、中央の予約サーバ/クラウドに提供される。

【0049】

エンドユーザは、例えばGNSS、NFCなどの例示的なユーザインターフェースおよびセンサを有する、自身の端末、すなわちこの実施形態ではスマートフォン21と通信する。

【0050】

また、図4から分かるように、エンドユーザは例えば、端末を用いて、またはプロキシ22を介して、以下のアクションを実行することができる。1日/1週間のチケットのサービス/購入のサブスクリプション、列車の予約、自動車/乗り物シェアの予約、輸送乗車/下車許可/記録、下車後の後処理(例えば、顧客調査、返金、または延滞の補償)など。

【0051】

ユーザプロフィール管理機能23aは、静的データ、例えば、氏名、年齢、連絡先住所、支払い方法(例えば、クレジットカード)、サービス加入状況、輸送の好み、IMEI (International Mobile Station Equipment Identity) のような任意の他の一意のIDなどを記憶し、端末21と通信するように構成される。

【0052】

乗客旅行管理機能23bは、いくつかのアクションを実行し、端末21と通信するように構成される。例えば、マルチモーダル・トランスポート・パスに関しては、乗客旅行管理機能23bは、例えば、MaaS月次サービスのサブスクリプション、および1日チケット、1週間チケット等の購入を管理する。

旅行計画(または旅行計画者)に関しては、乗客旅行管理機能23bは、目的地入力、経路選択/輸送オプション、予約/旅行手配を提供し、チケットを発行し、チケットIDを発行し、旅行者のための旅程を生成し、旅程IDなどを発行する。

旅行者/ユーザの旅行においては、乗客旅行管理機能23bは、その旅行計画を起動し、旅行の各セクション(旅程)について、パス/チケット保持を確認し、エンバンクメントを記録し、下車を記録し、旅行ログをブロックチェーンに追加し、旅行の終わりにその旅行計画を終了させ、旅程を閉じるように構成される。

【0053】

ブロックチェーン管理機能24aは、乗客旅行管理機能23bおよび他のブロック管理25と通信する。ブロックチェーン管理機能24aは、コンセンサスプロトコルを追加し、検証し/実行し、ブロックチェーンを読み取るように構成される。

さらに、図4から分かるように、パス、チケット、および旅行ログ情報が、少なくとも乗客旅行管理機能23bとブロックチェーン管理機能24aとの間、および、ブロックチェーン管理機能24aと他のブロックチェーン管理25との間で通信される。

【0054】

以下、図5を参照して、旅行者の旅行履歴を含むブロックチェーン30の一実施形態を説明する。

【0055】

ブロックチェーン30は、図1の参照の下に一般的に説明されるように、いくつかのブロック30a、30b、30cを有し、ここで、図5において、過去のブロック30a(ブロック#N-1)、現在のブロック30b(ブロック#N)および、後続すなわち次の/今後のブロック30c(ブロック#N+1)が例示されている。

【0056】

ブロック30a、30bおよび30cの各々は、最大所与のブロックサイズ内および関連するデータ構造内の取引において1つ以上の旅行者ログを含むことができる。図5において、左側のブロック30a(ブロック#N-1)は、2つの旅行者ログ31aおよび31bを取り扱う。

10

20

30

40

50

N-1ブロック30aからのハッシュ出力は、次のNブロック30b(現在のブロック)に供給される。ブロック30b(ブロック#N)は、旅行者AおよびBの次の旅行ログ32aおよび32b、さらに、旅行者Cの旅行の旅行ログ32cを処理する。

例えば、旅行者Dが新たな旅行ログを発行するが、同時にブロックサイズ制限を超える場合、このさらなる旅行ログは、次のブロック、すなわち、本例のブロック30cにおいて処理される。このブロック30cは、旅行者Bのさらなる旅行ログ33aの入力、搭乗者Cのさらなる旅行ログの入力33b、および搭乗者Dのさらなる旅行ログ33cの入力を含み、ブロック30c(ブロックN+1)は、旅行者CおよびDの次の旅行ならびに旅行者Dの残りのログを処理する。

その後、(N+1)のハッシュ出力が、次のブロック(N+2)(図5には図示せず)に供給される。

10

【0057】

一般に、ブロックチェーン30内の旅行ログは、以下の情報のうちの少なくとも1つを含むことができる。

- 発行者：マルチモーダル・トランスポート・バス発行者、モビリティ・サービス・プロバイダ/輸送業者、旅行者id(匿名データ)。
- チケット情報：チケットの種類、輸送の種類(鉄道、ライドシェア等)、座席予約(列車/座席番号)、価格またはチケット、規約および条件。
- 乗車記録：エンバנקメントの場所、乗車した時刻/日、下車した場所、下車した時刻/日、未使用/使用。
- 備考：特記事項(例えば、キャンセル、延滞)。

20

【0058】

いくつかの実施形態では、MaaSのブロックチェーンが、許可されたブロックチェーンを使用すると仮定される。許可されたブロックチェーンでは、(コンソーシアムを形成する)許可された事業者のみが、ブロックを追加/読み取ることができ、限定された参加者は、取引の検証(すなわち、信頼できるプレーヤとのコンセンサス)に参加することが許可される。

したがって、いくつかの実施形態では、例えば、モビリティ・サービス・プロバイダは、コンソーシアムにおいて編成され、また、それに応じた許可を有する者のみが、許可された分散型台帳またはブロックチェーンにアクセスすることが許可され、その一方で、悪意のある参加者または不正な参加者は、ブロックチェーンのコンソーシアムに参加することができない。

30

【0059】

以下、図6を参照して、MaaSのための(許可された)ブロックチェーンを提供するための通信ネットワーク40の一実施形態について説明する。

【0060】

回復力の観点から、通信ネットワーク40は例えば、サーバの中央に強く依存している従来のシステムにおいて、典型的にシステムの弱点である単一障害点(SPOF)のリスクを軽減する。

【0061】

図6から分かるように、通信ネットワーク40は、MaaSサービス・プロバイダ、鉄道事業者、カーシェアリング/ライドシェアリング事業者、バイクシェアリング事業者、およびバス事業者などの異なる事業者またはモビリティ・サービス・プロバイダに関連する複数のノード(またはエンティティ)41(大円)を有する。

40

【0062】

さらに、モビリティ・サービス・プロバイダのノード41と通信することができる複数の旅行者42(小円)が存在する。モビリティ・サービス・プロバイダ・ノード41は、MaaSのための許可されたブロックチェーン(例えば、図5のブロックチェーン30)を提供する通信ネットワーク40を共に形成することができる。

【0063】

50

旅行者42は例えば、旅行者の端末(例えば、図4の端末21)を用いて、関連するモビリティ・サービス・プロバイダと通信することによって、モビリティ・サービス・プロバイダによって提供される毎月のMaaSサービスに加入するか、または、マルチモーダル・トランスポート・サービスのための1日/1週間のパスを購入する。

【0064】

モビリティ・サービス・プロバイダ41は上述したように、自動車鉄道会社、電車事業者などの従来の輸送事業者に加えて、MaaS事業者(例えば、共用乗り物)、自転車共用サービス・プロバイダ、旅行代理店などの新しいサービス・プロバイダとすることができる。

【0065】

モビリティ・サービス・プロバイダ41は、論理接続である通信ネットワークを介して互いに接続され、ここで、輸送業者すなわちモビリティ・サービス・プロバイダ間の直接接続は必ずしも必要ではないが、低遅延および高スループットを必要とする場合がある。

【0066】

モビリティ・サービス・プロバイダのエンティティまたはノード41は、さまざまな機能を有することができるが、図4についても上述したように、2つの主要な機能、すなわち、旅行者管理機能およびブロックチェーン管理機能がある。

旅行者管理機能は、座席の予約、共用乗車/タクシー/レンタカー/列車の座席予約、月次加入、1日券の購入などをサポートする。通常の電子商取引サイトと同様に、旅行者管理機能は、ウェブサイトまたはスマートフォンのバックエンド処理の、ユーザインターフェースを提供する。

【0067】

その一方で、本実施形態ではブロックチェーンは、エンドユーザのために隠されるが、複数のモビリティ・サービス・プロバイダにアクセスされ、複数のモビリティ・サービス・プロバイダによってアクセスされる。

さらに、本実施形態では、コンソーシアム(許可された)ブロックチェーンが、ノード41の間に実装され、コンソーシアムのメンバであるモビリティ・サービス・プロバイダの間でブロックチェーン台帳を検証する。

【0068】

いくつかの実施形態では、上記の例は、国際的なMaaS運営(オペレーション)または異なる地域におけるMaaS運営に拡張される。そしてブロックチェーンは、多層構造として定義される。

第1の層のブロックチェーンは、国間または地域間で構成され、第2の層のブロックチェーンは、その地域のコンソーシアム内で構成される。例えば、地域コンソーシアムにおける代表的なプロバイダは、第1の層のブロックチェーンに参加し、国際サービスを取り扱うことができる。

【0069】

以下では、図4のMaaSシステム20の代替の実施形態を、MaaSシステム50のブロック図を示す図7を参照して説明する。

【0070】

図4の実施形態とは対照的に、本実施形態のMaaSシステム50では、検証ブロック/機能51a、インテグリティ(完全性、整合性)ブロック/機能51b、および認証ブロック/機能51cを含むブロックチェーン・オラクル51が提供される。

【0071】

さらに、ブロックチェーン管理52において、他のブロックチェーン管理53と通信するブロックチェーン管理ブロック/機能52aに加えて、スマートコントラクトおよび仮想マシンブロック/機能52bが提供される。

【0072】

さらに、ブロックチェーン・オラクル51(例えば、認証機能51c)と通信することができる、(顔認証用)カメラまたは他のセンサ(例えば、指紋検出用)などの外部センサ54が提供される。

10

20

30

40

50

【0073】

複数のセンサ(例えば、NFC、GNSS、または他のセンサ)を備えたスマートフォン55を有するエンドユーザは、ブロックチェーン・オラクル51(例えば、検証機能51a)と通信することもできる。

【0074】

ブロックチェーン管理機能52は、スマートコントラクトを処理することができ、新たな機能「ブロックチェーン・オラクル」51は、スマートコントラクトへの入力データ(例えば、センサ54からの入力および/またはスマートフォン55からのセンサからの入力)を処理することができる。

【0075】

スマートコントラクトは一種のソフトウェアコードであり、データに加えて(例えば、旅行データに加えて)ブロックチェーンに展開することができる。ただし、スマートコントラクトは一種のソフトウェアであるため、通常、実行には中央処理装置(CPU)が必要である。

したがって、スマートコントラクトのプラットフォームとして構成することができ、対応するコンピューティングリソースを提供することができる仮想マシンが提供される。

【0076】

ブロックチェーン・オラクル51は、この実施形態ではスマートコントラクトへの間違いのない入力の責任を負い、センサ54とスマートコントラクトとの間の一種のプロキシサーバである。

スマートコントラクトがセンサ54からのデータにアクセスした場合、対象センサは、Restful APIに基づいてUniform Resource Identifier(URI)すなわちUniform Resource Location(URL)でそのデータを示すことができる(例えば、<https://proxy.blockchainoracle.com/inputdevices/sensor1>)。

【0077】

この例では、URL "proxy.blockchainoracle.com/"は、ブロックチェーン・オラクルのサーバ名であり、その一部"inputdevices/sensor1"はブロックチェーン・オラクル51の下の対象センサの識別子である。

【0078】

この値は、Extensible Markup Language(XML)またはJavascript Object Notation(JSON)形式などで返すことができる。

【0079】

しかしながら、ブロックチェーン・オラクル51は、センサ54とそのスマートコントラクトとの間のプロキシサーバであるだけでなく、スマートコントラクトのための入力および出力の検証にも責任を負う。

【0080】

例えば、ブロックチェーン・オラクル51は、センサ54からの位置/タイムスタンプを検証することができる。さらに、データの完全性(不変)を確認してもよく、接続されたセンサが間違っていないセンサであるかどうかを認証することができる。

【0081】

前述のように、スマートコントラクトは、ソフトウェアコードの一種であり、したがって、物理的な展開に柔軟性がある。例えば、仮想マシンは、別の(または任意の)位置にある信頼できるクラウドコンピュータで個別に実行することもできる。

【0082】

一般に、様々な方法による各種センサの配備の多くの可能性/組み合わせが存在し、本開示は、その点で特定の例に限定されない。

【0083】

いくつかの実施形態では、検証のタイプ、または、任意の検証が実行されるかどうか、かつ/または、ブロックチェーン・オラクルに検証プロセスが含まれるかどうかは、スマートコントラクトに入力され、かつ/または、スマートコントラクトから受信されるデータ

10

20

30

40

50

が、改ざんされるリスクによって決まる。

例えば、MaaS事業者が、センサの設置状況/配備環境のデータベースを所有するか、または、このデータベースを(排他的に)制御し、修正/改ざんすることがほとんど不可能である場合(例えば、セキュリティカメラが高いタワーに設置され、人々が到達することができない場合)、簡略化された(検証)手順を適用することができる。

例えば、検証プロセスの一部はスキップされてもよい(例えば、ダブルチェックの代わりに、シングルチェックが実行される)、または、ブロックチェーン・オラクルによって実行される検証はスキップされてもよい(場合によっては、ブロックチェーン・オラクルが含まれない/必要とされない)。

言い換えれば、(複数の)センサの信頼度に応じて、いくつかの実施形態では妥当なレベルの検証が適用される。

10

【0084】

いくつかの実施形態では、簡素な方法/一般的な方法は、乗客のスマートフォン/ウェアラブルデバイス内のセンサを使用することである。代替的に(または追加的に)、例えば、鉄道駅、空港、バス停、自転車シェアの停留所、街路などの輸送施設に1つ以上の外部センサ(例えば、カメラ)が配備される。

例えば、空港または鉄道駅は、いくつかの実施形態ではMaaSセンサ用にすなわちMaaSセンサとして使用される複数の防犯カメラを有してもよい。

【0085】

MaaS事業者/輸送事業者は、この実施形態ではブロックチェーン・オラクル51を展開する。しかしながら、他の実施形態では、サードパーティが代わりにブロックチェーン・オラクル51のサービスを提供してもよい。

20

例えば、モノのインターネット(IoT)機能、ロケーションサーバ、セキュリティ機能、アプリケーション、およびサービスを有する電気通信事業者/モバイルネットワーク事業者は、いくつかの実施形態において、ブロックチェーン・オラクル機能を提供することもできる。

【0086】

以下では、スマートコントラクトの実施形態について説明する。

【0087】

スマートコントラクトは、ブロック内のデータに加えてコードとしてブロックチェーンに記憶される。

30

【0088】

スマートコントラクトの記述または内容は、人間が記述した自然言語コントラクトではなく、一種のソフトウェアコード(例えば、JavaScript、Solidity)である。したがって、いくつかの実施形態では、IF-THEN-ELSE構造および条件が存在する。

【0089】

一般に、スマートコントラクト(コンピュータ言語)は、いくつかの実施形態では以下のうちの少なくとも1つをサポートすることができる。

- ・ ループ構造(チューリング完全な言語の場合)
- ・ 複数の変数、三項演算子などの複雑な条件
- ・ 内部変数の値を保持する(ステートフルなスマートコントラクトの場合)
- ・ ブロックチェーン内のブロックの読み込み/書き込み/更新
- ・ 外部マシン/コンピュータ/ネットワークへの入出力
- ・ 人間の介入なしにマシン間で直接交渉する

40

【0090】

以下に、スマートコントラクトの一例を示す。しかしながら、スマートコントラクト用の多くのコンピュータ言語が存在し、スマートコントラクトの以下の例は、実際のコンピュータ言語ではなく、単純化された擬似コードで提供される。

Begin

変数: TicketState (オープン、使用中、クローズ)

50

```
If チケットが発行され、使用されていない場合 Then
TicketStateをオープンに変更する
End (If)
Repeat (メインループ)
外部からトリガを受信する
If トリガがチェックインされている場合 Then
TicketStateを使用中に変更する
End (If)
If トリガがチェックアウトされている場合 Then
TicketStateをクローズに変更する
ループを出す
End (If)
End (Repeat)
TicketStateを外部に送信する
End (Begin)
```

10

【0091】

この擬似コードは、チケットが使用されているか否か、使用されていない場合は「オープン」になるように設定されている。また、トリガが受信されたか否かが確認され、このトリガは、例えば「チェックイン」イベントまたは「チェックアウト」イベントである。

20

「チェックイン」イベントがトリガとして検出された場合、チケットの状態は「使用中」に設定され、「チェックアウト」イベントがトリガとして検出された場合、チケットの状態は「クローズ」に設定される。最後に、チケット状態は例えば、ブロックチェーン・オラクル51または別のインスタンスに送信される。

【0092】

一般に、スマートコントラクトは、任意のコンピュータ言語がサポートされていれば、その任意のコンピュータシステムで実施することができる。いくつかの実施形態では、スマートコントラストが真正であること、および、スマートコントラストを修正または変更する可能性がないことを保証することが重要である。

前述のように、ブロックチェーンでは、このような場合に変化するハッシュ関数出力により、変更/修正が検出可能である。

30

【0093】

以下では、ステートフルなスマートコントラクトにおける状態遷移に関する実施形態を、図8を参照して説明する。

【0094】

スマートコントラクトがステートフルである場合、スマートコントラクトは、現在の状態に応じて異なる挙動を有することができる。これは、(複雑な)旅行保険/輸送運賃表をカバーするために、いくつかの実施形態において有用である。

【0095】

例えば、チケットは、そのチケットが使用される前に返金することができるが、その一方で、チケットが使用されたときには返金は許可されるべきではない。

40

【0096】

図8は、関連するスマートコントラクトの3つの異なる内部状態を示す。

【0097】

最初に、チケットが発行されると、状態は「オープン」であり、すなわち、このチケットは有効であるが、まだ使用されていない。

【0098】

乗客が「チェックイン」のトリガ条件を満たすと、状態は「使用中」に遷移し、その後、チケットはもはや返金不能になる。

【0099】

乗客が「チェックアウト」のトリガ条件を満たす(例えば、目的地に到着する)と、状態は

50

「クローズ」となる。スマートコントラクトは、適切なクローリングの状態を確認することができる。例えば、列車が3時間遅れた場合、列車遅れ補償条件を満たすために、スマートコントラクトは、補償の手順を自動的に実行してもよい。

【0100】

状態/遷移条件の数は、実際のMaaSユースケースまで増加/減少させることができ、したがって、それに応じて調整することができる。例えば、航空旅行の実施形態においては、(カウンタでの)チェックインの状態と(搭乗ゲートでの)搭乗の状態とを別々に扱うことができる。

【0101】

いくつかの実施形態では、ブロックチェーン・オラクルによって実行される検証は、スマートコントラクトからの出力に基づく出力データが所定のデバイスで正しく受信されたかどうかを検証することを含む。

例えば、図8で説明したように、スマートコントラクトは、ブロックチェーン・オラクルに送信されるチケットの状態に関する出力を行い、ブロックチェーン・オラクルは次に、例えば、このチケットの状態が正しく、正しいチケットおよびユーザに関連付けられているかどうかを検証する。

例えば、補償が支払われる場合、ブロックチェーン・オラクルは、補償が正当化され、かつ、情報が正しい所定のデバイスに送信されることを検証することができると仮定する。また、例えば、チケットの状態がオープンである場合、この情報は例えば、正しいチェックインデバイス(またはMaaS事業者のデータベース)、および、正しいユーザ/旅行者の正しいモバイル端末に送信されるべきである。

さらに、ブロックチェーン・オラクルは例えば、改ざんされたスマートコントラクト出力データがチケット状態の変更、補償の取得などに使用されることを回避するために、出力データが正しいスマートコントラクトに基づくことを検証することができる。

【0102】

以下では、スマートコントラクト実行のトリガに関連する実施形態について説明する。

【0103】

スマートコントラクトの成功の1つの要因は、いくつかの実施形態ではスマートコントラクト用の正確な条件に加えて、信頼できるトリガをどのように取得するかである。

【0104】

スマートコントラクトの実行は上述したように、「(ブロックチェーン)オラクル」と呼ばれる信頼された/正確な入力に依存する。

【0105】

図9は、ブロックチェーン・オラクル61を有するスマートコントラクトトリガを実施する方法60の一実施形態のフローチャートを示す。旅行者62がMaaSサービスで旅行すると仮定する。旅行者62は、チェックインしようとしている。

この実施形態では、旅行者62は、列車の未使用チケットを所持している。

【0106】

チェックインエリアには、旅行者を検出可能なセンサ63(例えば、カメラ、チケット等をスキャンするスキャナ、近距離通信、顔認識用センサ、センサ指紋認識等)が設けられている。さらに、ブロックチェーン管理が提供され、ブロックチェーン管理は上述のように、例えば、旅行データなどを含むブロックチェーン64を管理する。

スマートコントラクト用の仮想マシン65は、スマートコントラクトをホストし、スマートコントラクトを実行する。

【0107】

チェックインの方法またはプロセスは、以下の通りである。

【0108】

66において、センサ63(すなわち、センサ群63の1つ以上のセンサ)は、特定のゾーン/場所(例えば、駅の入口、ゲート、プラットフォームなど)への旅行者の到着を認識し、ブロックチェーン・オラクル61へ旅行者の到着について通知する。

10

20

30

40

50

あるいは67において、旅行者のスマートフォン、ウェアラブルデバイスなどのセンサのうちの1つ以上のセンサが、特定の領域を検出し、旅行者62のチェックインまたは現在位置を示すトリガをブロックチェーン・オラクル61に、または、ブロックチェーン管理サーバ64に直接送信する。

【0109】

ブロックチェーン・オラクルサーバ61は、センサ(複数可)(66および/または67参照)から入力を受信し、位置、ブロックチェーン・オラクルサーバ61に送信されたセンサデータを提供したセンサのデータ完全性、接続されたセンサの認証など、センサの有効性を確認する。

【0110】

68において、ブロックチェーン管理機能64は、チェックインを示すトリガを受信し、スマートコントラクトの関連プロセスの実行を開始する。

【0111】

69において、ブロックチェーン管理は、トリガ/入力/条件変更に従って関連するスマートコントラクトの関連コードを実行する仮想マシン65にトリガを送信し、次に、図8を参照して説明したように、70において内部状態(例えば、チケットオープン→チェックイン完了)を変更し、71において対応するメッセージをブロックチェーン管理サーバに送信する。

【0112】

72において、ブロックチェーン管理機能は、(必要であれば)スマートコントラクト実行の結果に従って、ブロックにその状態変化を書き込む。例えば、複数の事業者間のチケットが無効にされた場合は、ブロックチェーンに記録されるべきである。

【0113】

73において、ブロックチェーン管理機能は、(オプションとして)旅行者にチケット状態を通知する。

例えば、旅行者は、対応するメッセージが表示される(またはチケット状態の変化を示す任意の他の印が表示される)スマートフォン画面またはウェアラブルデバイスからチケット状態の変化を取得することができる。

【0114】

いくつかの実施形態では、ブロックチェーン・オラクル61の1つの重要な責務は、入力情報が間違っている/不正確である場合、スマートコントラクトが正しく評されている場合であっても、間違った手順が実行されるので、スマートコントラクトへの正しい入力を保証することである。

ヒューマンエラー、マシンの不具合/故障、悪意のある攻撃(例えば、スプーフィング)などにかかわらず、ブロックチェーン・オラクル61は、間違った入力/条件によるスマートコントラクトの間違った実行を防止しなければならない。

【0115】

いくつかの実施形態では、オラクル61は例えば、センサおよび/またはサーバが信頼できるメンバによって配備され、他の誰かによってデータを変更または修正することが不可能である場合、省略されてもよい。

【0116】

以下では、旅行者の到着の検出(測位/領域検出)の一実施形態について説明する。

【0117】

チェックイン検出のために、対応する方法の実施形態が存在する。

【0118】

例えば、いくつかの実施形態ではQRコード(登録商標)/NFCなどが、(例えば、チケット上のQRコードをスキャンすること、旅行者のスマートフォンのNFCを使用することなどによって)旅行者の到着を検出するために使用される。

そのような技術自体は知られているが、いくつかの実施形態では、スマートコントラクトの検証が必要である。

10

20

30

40

50

【0119】

いくつかの実施形態では、正確な測位技術を含むことができるロケーションベースのソリューションが提供され、このソリューションはMaaSサービスにとって有用であり、それによって、旅行者の位置を正確に判定することができるためである。

他の実施形態では、MaaSアプリケーションにも有用である生体認証ベースのソリューションが実装される(いくつかの実施形態ではロケーションベースのソリューションと生体認証ベースのソリューションとが組み合わせられる)。

【0120】

以下において、旅行者の到着(すなわちチェックイン)を検出するための、従来のID(識別)に基づく一実施形態について説明する。

【0121】

従来のID/旅行者の到着検出の一例は、以下の通りである。

1. 旅行者名およびそのパスワードが、チェックインマシンで検出される。
2. (例えば、旅行者の個人データをスキャンするために)パスポートがチェックインマシンに示される。
3. スマートフォンなどのNFCセンサの接触を、チェックインゲートまたは搭乗ゲートにおいて検出する。
4. バーコード/QRコードの付いた電子チケットをゲートまたはリーダーに示す。
5. チェックイン場所においてスマートフォン/PCのユーザインタフェースで入力する。

【0122】

いくつかの実施形態では、この方法を使用することによって、多くの手動/人間ベースの確認がチェックインプロセスに関与する。

誰かが偽造チケットを作成してスマートフォンの画面上で使用し、それをゲートで示す場合、人間は、それを容易に検証することができず、このチケットが偽造チケットであることを認識することはできないであろう。

【0123】

以下では、ロケーションベース(ジオフェンシング)のソリューションが実装される一実施形態について説明する。

【0124】

例えば、旅行者が(ハイエンドの)スマートフォンまたは高機能なウェアラブルデバイスを有している場合、その中には様々なセンサが設けられている。

その場合、ロケーションベースの検出は、1つのセンサ(例えば、GPSセンサ)または2つ以上のセンサの組み合わせに適用可能である。

【0125】

例えば、前世代のGNSS(全地球航法衛星システム、例えばGPS衛星)は、30m~50mの精度を有する。現在の衛星システム(例えば、ガリレオ暗号化、QZSS、準天頂衛星システム)または複数の衛星の組み合わせは、デシメートルレベル(例えば、50cm)またはcmレベルの精度さえ達成することができ、このレベルの精度は、いくつかの実施形態におけるMaaSにとって有用である。

さらにいくつかの実施形態では、複数の屋内測位方法の組み合わせが実施され、これはMaaSに有用であり、この測位システムは、MaaSにも有用である非常に正確なクロック/タイムスタンプを有することができる。

【0126】

この実施形態では、ロケーションベースのソリューション用の以下のセンサ/測位方法のうちの少なくとも1つが実装され、それらの各々は、互いに任意の方法で組み合わせることができる。

GNSS測位(例えば、GPS)、高精度衛星測位システム(例えば、ガリレオ暗号化、QZSS、RTK(リアルタイムキネマティック)ベースの測位など)、Wi-Fi(登録商標、無線ネットワーク)ベースの測位、セルベースの測位(例えば、OTDOA(観測到達時間差)、UTDOA(アップリンク到達時間差)、基地局ビームフォーミング等)、慣性計測装置(IMU)ベースの測

10

20

30

40

50

位(例えば、ジャイロセンサ、加速度センサ、電子コンパス等)、ビーコン信号(例えば、低電力Bluetooth(登録商標、BLE))、スマートフォンカメラ/画像処理での測位メーカーの認識(例えば、特定の位置において印刷されたQRコード)、および/または、NFCベースの位置検出。

【0127】

旅行者、すなわち、旅行者のスマートフォン/ウェアラブルデバイスなどは、(チェックインのための)特定の領域を検出し、その位置またはトリガを、ブロックチェーン・オラクルに送信するか、または、ブロックチェーン管理サーバに直接送信する。

いくつかの実施形態では、この方法の課題は、GNSSスプーフィングまたは不正確な測位をいかに防止するかである。したがって、いくつかの実施形態では、ブロックチェーン・オラクルが以下で説明するように、異なる方法で旅行者の位置をダブルチェックしてもよい。

10

【0128】

以下では、位置/場所/タイムスタンプ検証を実施する一実施形態を説明する。

【0129】

ブロックチェーン・オラクルは、センサからの位置/場所の信頼性をダブルチェックしてもよい。場所に加えて、場所サービスは通常正確なクロックソースを使用するので、タイムスタンプ/クロックを検証することもできる。

その結果、ブロックチェーン・オラクルは、2つ以上のセンサのさらなる位置信号を考慮に入れることによって、位置の精度を改善することができる。

20

【0130】

例えば、2つのタイプの測位システムが組み合わされてもよい(または、3つ以上であってもよい)。例えば、GNSSと共に、ダブルチェック用にGPS(米国)、GLONASS(ロシア)、BeiDou(中国)、Galileo(ヨーロッパ)およびQZSS(日本)などの、複数の衛星が使用される。

屋内測位の一例では、ブロックチェーン・オラクルは、Bluetooth(登録商標)ビーコン、Wi-Fi(登録商標)信号測位、セル信号などを使用することができる。一般に、1つのシステムを改ざんすることは容易であるかもしれないが、同時に複数のシステムを改ざんすることは非常に困難であると想定される。

また、いくつかの実施形態の場合のように、使用中のシステムが3つ以上のシステムの中からランダムに選択される場合、改ざんすることは、より困難であるはずである。

30

【0131】

さらに、いくつかの実施形態では、ユーザ端末測位およびネットワークベース測位によるダブルチェックが提供される。

例えば、スマートフォンは、自身の現在位置をネットワークロケーションサーバに送信し、ネットワークロケーションサーバは、ネットワークベースの測位(UTDOA)で、その現在位置が正しいかどうかをダブルチェックすることができる。

【0132】

さらに、いくつかの実施形態では、タイムスタンプが確認されてもよい。例えば、UE(User Equipment)の内部クロックおよびネットワーククロック(例えば、ネットワークタイムプロトコル、NTP)または衛星クロック(GNSSクロック)は、関連するタイムスタンプを比較するために使用される。

40

【0133】

いくつかの実施形態では、以下で説明されるように、視覚ベースの位置識別が実施される。

【0134】

エンドユーザまたは任意の車両が、カメラ/ビデオ、画像/ビデオ処理/コンピュータビジョン機能などを有する場合、エンドユーザの現在位置/場所を識別するために使用することができる。自動運転車/先進安全自動車は、位置/状況を識別するためのカメラおよび同時位置決め地図作成(SLAM)の機能を有することができる。

50

例えば、カメラ/ビデオ処理は、高速道路/幹線道路の入口を認識し、次いで、(幹線道路上の)現在位置または状態変化をブロックチェーン・オラクルに送信することができる。

【0135】

図10は、ロケーションベースのチェックインの手順すなわち方法75の一実施形態におけるフローチャートである。図10では、ブロックチェーン・オラクルからのチェックインのトリガを受信した後の手順が、図9の実施形態と同一であるため省略されている。

【0136】

旅行者76のチケットは、ブロックチェーン77またはMaaSサーバに記憶される。ブロックチェーン管理77の機能は、79において、ブロックチェーン・オラクル78に、搭乗場所の情報または他のチェックイン条件を送信する。

ブロックチェーン・オラクル78は、旅行者76がスマートフォン/ウェアラブルデバイスを有しているかどうか、したがって、適切な測位能力を有しているかどうかを確認する。次に、ブロックチェーン・オラクル78は、ロケーションベースのチェックインを選択し、ブロックチェーン・オラクル78は、80において、ジオフェンシングの条件(例えば、経度、緯度、領域の半径、またはビーコン信号情報)の詳細を、旅行者76のスマートフォンに送信する。

81において、スマートフォンは、ジオフェンシングトリガの定義された領域に入っているかを監視する。スマートフォンがその領域の接近を検出すると、82において、スマートフォンは、セルラーネットワークまたは無線ネットワークを介してブロックチェーン・オラクル78にトリガメッセージを送信する。

任意選択的に、ブロックチェーン・オラクル78は、やはり上述したように、ユーザの位置をダブルチェックすることができる。例えば、ブロックチェーン・オラクル78は、ロケーションサーバ84への問い合わせを83において送信する(例えば、電気通信事業者またはサービス・プロバイダは、SUPL(セキュアなユーザ・プレーン位置決め)サーバまたはESMLC(サービスモバイル位置決めセンター)を有してもよい)。

ロケーションサーバ84は、85において位置をダブルチェックするために、上述のネットワークベースの測位を開始し、86において(例えば、位置が確認された場合)結果をブロックチェーン・オラクル78にフィードバックする。

位置が確認された場合、ブロックチェーン・オラクル78は、87において、チェックイン・トリガをブロックチェーン管理77に送信し、スマートコントラクトを実行する。

【0137】

以下では、チェックインを確認するための生体認証ベースのソリューションの一実施形態について説明する。

【0138】

旅行者が、ICチップパスポートのような生体認証IDを有しているか、または、任意の物理的なIDを有していないが、生体認証データが事前にサーバに登録されている場合、生体認証に基づくチェックインが、いくつかの実施形態において使用される。

【0139】

この方法の課題は、いくつかの実施形態では、生体認証データが非常に機密性の高い個人情報であるため、旅行者がMaaS事業者と生体認証データを共有することを望まない場合があることである。

【0140】

従って、いくつかの実施形態において、ブロックチェーン・オラクルは、生体認証データを持たず、その代わりに、人を識別するための信頼された生体認証サーバが提供される。

【0141】

いくつかの実施形態では、以下のセンサ/手段のうちの少なくとも1つが、生体認証ベースのソリューション用のセンサ/入力を実施するために使用される。セキュリティカメラ(顔認識)からの映像/画像、指紋センサ、虹彩認識、および/または生体認証ID(例えば、e-パスポート)。

【0142】

10

20

30

40

50

図11は、生体認証ベースのチェックインの方法90の一実施形態のフローチャートを示したものであり、ブロックチェーン・オラクルからのチェックインのトリガを受信した後の手順は、図9と同一であるため省略される。

【0143】

図11において、センサ63、旅行者62、ブロックチェーン・オラクル61、およびブロックチェーン管理64は、図9の対応するエンティティに対応し、それに関しては図9の説明を参照されたい。さらに、旅行者62の生体認証データを記憶する生体認証データベース91が設けられている。

【0144】

92において、センサ63は例えば、顔認識または他の生体認証データ取得を実行し、93において、旅行者62の到着の検出を、ブロックチェーン・オラクル61に送信する。

【0145】

例えば、セキュリティカメラからの映像/画像、無人チェックインカウンタでの指紋/パスポートデータ等がデータとして送信される。

センサ自体が人/旅行者を識別することができる場合(例えば、センサが顔認識機能を有する場合)、関連するIDがブロックチェーン・オラクル61に送信され、かつ/または、生データまたは圧縮データがブロックチェーン・オラクル61に送信され、ブロックチェーン・オラクル61は旅行者62の顔を認識する。

生データが送信されても、データ送信のために暗号化が規定される場合がある。

【0146】

あるいは、旅行者62が例えば、顔認識機能または指紋読取装置を有する(ハイエンド)スマートフォンを有する場合、スマートフォンは94において、認識結果をブロックチェーン・オラクル61に送信する。

例えば、より正確な顔認識のために、デュアルカメラ、3D深度カメラ(例えば、飛行時間ベースの画像センシング)などを実装してもよい。

現在、そのような機能は、典型的にはハイエンドのスマートフォンにおいて実装されるが、そのような機能が多くのスマートフォンにおいて近い将来に広く使用されることになり、また、スマートフォンがコンピュータビジョン(例えば、GPU)または同様のもののための、より高い性能のプロセッサを有することになり、これが、いくつかの実施形態において、顔認識のようなMaaSアプリケーションのために使用されることになることが予想される。

【0147】

ブロックチェーン・オラクル61が生体認証データを記憶しないか、または、旅行者を識別するのに十分な詳細を記憶しない場合、ブロックチェーン・オラクル61は、95において、生体認証データ/この詳細を確認するための要求を、外部の生体認証サーバ91に送信する。

例えば、政府/輸送機関は、生体認証パスポート用の生体認証データのデータベース91を有することができる。次に、ブロックチェーン・オラクル61は、暗号化されたセンサデータを生体認証データベース91に送信し、その後、生体認証データベースサーバ91は、96において、入力データからの人物を、その人物自身の生体認証データベース91に従って識別することができる。

旅行者62が96において正常に識別された場合、生体認証データベース(サーバ)91は、97において、その確認をブロックチェーン・オラクル61に送信する。ブロックチェーン・オラクル61が、旅行者IDを確認すると、ブロックチェーン・オラクル61は、98においてブロックチェーン管理64にチェックインのトリガを送信し、スマートコントラクトを実行する。

【0148】

いくつかの実施形態では、ブロックチェーン・オラクル61自体が、センサ(複数可)からの生データを記憶せず、かつ、生体認証データサーバにおいて登録された生体認証データにアクセスしなくてもよい。

10

20

30

40

50

しかし、ブロックチェーン・オラクル61は、データソース(すなわち、センサ)と、そのデータソースが真正であるかどうか(例えば、センサが真正であるかどうか)と、生体認証サーバが真正であるかどうかとを確認する。

このデータは、センサから生体認証サーバへの途中で修正または変更されない。ブロックチェーン・オラクル61は、暗号化されているのでデータを読み取ることはできないが、以下でさらに説明するように、完全性機能のために、ブロックチェーン・オラクル61は、データの修正を検出することができる。

ブロックチェーン・オラクル61は、旅行者が生体認証サーバによって識別されたことを単に知るのみである。これは、いくつかの実施形態で実施される一種のゼロ知識証明プロトコルである。

【0149】

以下では、ブロックチェーン・オラクルでのデータの完全性チェックに関する実施形態について説明する。

【0150】

ブロックチェーン・オラクルは、センサ(複数可)からデータを受信し、そのデータの完全性を確認する必要がある。

【0151】

データ完全性チェックに関する種々の実施形態がある。1つの典型的な実施形態は、ハッシュ関数を使用するが、他の実施形態は、完全性データストリームを使用する。

【0152】

ハッシュ関数を使用する実施形態:

例えば、センサ群およびブロックチェーン・オラクルプロセッサが、ブロックチェーン内のコンソーシアムのメンバに加わり、センサデータのハッシュ関数が、ブロックチェーンの関連ブロック内に記録されるので、ハッシュ関数およびブロックチェーンは、データ完全性に適している。

誰かがブロック内のセンサデータを修正した場合、(例えば、コンソーシアムの)他のメンバのブロックチェーン内のハッシュ値との不一致があるであろう。例えば、SHA-2、SHA-3、その他のスポンジ関数のようなハッシュ関数のさまざまな提案および実装がある。要件/ユースケースに応じて、ハッシュ関数および関連するパラメータ(例えばナンス)は、静的または半静的(例えば変更可能)に選択される。

【0153】

完全性アルゴリズム(ストリーム)に関する実施形態:

暗号化ストリームと同様に、センサデータシーケンスは、キーを用いて送信機側で完全性シーケンスが乗じられる(例えば、Ex-OR計算)。

受信機側では全く同じシーケンスが同一のキーで適用され、その結果、受信機側では保護されたデータが元のデータになる。誰かが途中でデータを修正した場合、受信機での出力結果は、同じではない(例えば、CRC(巡回冗長検査)による誤り検出)。

アルゴリズムのキーが定期的または時折変更されたり、または、タイムスタンプ/タイムカウンタ/パケットシーケンス番号などの組み合わせが使用されたりすると、コピーされたデータで反射攻撃(リプレイアタック)を実行することが(より)困難になるため、保護がより強力になる。

【0154】

以下では、ブロックチェーン・オラクルを有するセンサ/端末の認証/信用証明書チェックに関する実施形態について説明する。

【0155】

この実施形態では、入力データが真正のセンサ/端末から来ることを確認することが重要である。なぜなら、偽造センサまたは改ざんされた端末が使用された場合、スマートコントラクトが乱用され得、これはこの実施形態では回避されるべきであるからである。

【0156】

入力センサ/デバイスの認証において種々の実施形態が存在し、このメカニズムは、アク

10

20

30

40

50

チューエータ、ディスプレイ等の出力装置の検証にも使用される。

【0157】

いくつかの実施形態は、ハッシュ関数/X.509証明書を実装し、このハッシュ関数は、送信者の署名である。このアイデアは、公開鍵基盤(PKI)および公開鍵と共に広く使用され、既知のものである。

いくつかの実施形態では、MaaS事業者(または他の誰か)が認証局(CA)を提供し、適切に設置されたセンサ/デバイスに証明書を発行する。

【0158】

センサ/デバイスが特定の位置に物理的に設置されている場合、証明書もセンサ/デバイスに設定される。この方法は、(少なくとも一部の実施形態では)専門家によって設置され設定される固定センサに役立つ。

【0159】

いくつかの実施形態では、ハードウェア製造業者のID/シリアル番号が再使用される。このような場合、証明書の構成は作業負荷を必要とし、インストール後に何らかの管理を必要とすることがある。

いくつかの実施形態で実施される単純かつ容易な方法は、製造(シリアル)番号、モデル番号、製造/工場の場所などの製造者のIDを再使用することである。

しかしながら、セキュリティレベル/一意性はより低くなり得るが、結果として、本方法は、証明書または証明のインストール/セットアップを回避することができるので、非専門家またはエンドユーザによってセットアップされたセンサに有用であり得る。

【0160】

あるいは、製造業者がX.509証明書(上記のソリューションを参照)を、工場のセンサ/デバイスにインストールするか、または、以下にさらに説明するように、より信頼性の高い他のIDが再使用される。

【0161】

製造業者のIDは、サイドチャネル攻撃を防ぐためにセキュアなメモリ/ストレージに記憶される。そうしないと、誰かがそのIDを書き換えたり改ざんしたりする可能性があるためである。

【0162】

いくつかの実施形態では、セルラーネットワーク/携帯電話IDが再使用される。製造業者のIDと比較して、標準ベースのIDは信頼性があり、一意である。

【0163】

3GPP固有IDの例は、国際移動体装置識別番号(IMS I)、国際移動体加入者識別番号(IMS I)、(ネットワークからの)C-RNTI(セル無線ネットワーク送信識別子)、(ネットワークからの)P-TMSI(パケット一時移動体加入者識別番号)、(ネットワークからの)GUTI(グローバル一意一時識別子)などである。

【0164】

しかしながら、いくつかの実施形態では、グローバルなケースにおける固有のIDのために、IDの長さが長すぎる場合がある。このIDは、MaaS事業者の外部によって管理されている。

【0165】

さらに、例えば、旅行者は、2つのSIMカードスロットおよび2つの挿入されるSIMカードを有するスマートフォンを有し、その結果、通信用のIMS Iは、接続される電気通信事業者に応じて変更可能であり、かつ/または、旅行者は、古い端末を新しいモデルに交換して、その結果、IMEIが突然変更され得る。

【0166】

したがって、これに対処するために、いくつかの実施形態では、以下でさらに説明するように、セルラID(関連する携帯電話情報/一意の番号)とMaaSユーザIDとの間のバインディング手順が提供される。

【0167】

10

20

30

40

50

いくつかの実施形態では、別の固有のIDが使用される。したがって、ここで説明される実施形態は、セルラIDに基づくが、別の固有のIDであってもよい。例えば、イーサネットインタフェース内のMACアドレスは、ネットワークカード/インタフェース内で一意である。

オペレーティングシステム/プラットフォームがインストールされているマシンに固有のものである汎用一意識別子(UUID)、1台のコンピュータに一意に割り当てられるグローバル一意識別子(GUID)、Bluetooth(登録商標)デバイスアドレス、iPhone(登録商標)の一意識別子(UDID)、ANDROID(登録商標)_IDなどが使用され得る。

【0168】

IPv6(IPアドレスバージョン6)は、グローバルに一意ではないが、アドレスの不足のために再割り当てされる可能性が高いIPv4と比較して、制限されたネットワーク内で競合する可能性が低い。IPv6が信頼された組織に割り当てられ、重複していない場合、一意のIDとして使用されてもよい。

【0169】

いくつかの実施形態では、短いIDが固有のIDとして使用される。

【0170】

IDがグローバルIDとして使用するには短すぎる場合(例: C-RNTIが16ビットで、他のセルの同じIDと競合する可能性がある場合)、追加のプレフィックスまたはサフィックスを割り当てることができる(例: MaaS IDなど)。

【0171】

いくつかの実施形態では、ランダム値が固有のIDとして使用される。

【0172】

生成された番号が特定の領域において良好な一意性を有し、競合の可能性が低い場合、いくつかの実施形態では、乱数を固有のIDとして使用することができる。

【0173】

ランダムな値の範囲に関しては、ランダム性の分布が必要とされる。例えば、値は擬似乱数発生器を用いて生成され、さらに、タイムスタンプ/カウンタ/場所情報などに基づいて生成されるが、そのような値は、十分に固有なものである。

【0174】

その場合、ブロックチェーンオラクル(または端末)は、そのランダム値を、固有IDとして生成し、サイドチャネル攻撃を防ぐためにセキュアなメモリ/ストレージに保存する。

【0175】

以下では、ユーザアカウントおよびセルラ固有IDのバインディング/検証手順/方法に関する実施形態について説明する。

【0176】

図12は、ユーザアカウントおよびセルラ固有IDのバインディング手順の方法100の一実施形態のフローチャートを示す。ブロックチェーン・オラクルサーバ101は、旅行者102とブロックチェーン管理103とユーザ・プロファイル・サーバ104との間の通信のために提供される。

【0177】

この実施形態では、バインディングは、ユーザ・プロファイル・サーバ104のデータベースに記憶される、固有IDとユーザアカウントとの間のマッピングを意味する。

【0178】

旅行者102が自身のユーザプロファイルをMaaS事業者に登録すると、サーバ104は、(例えば、旅行者のスマートフォン上で実行されているMaaSアプリケーションを使用して)105でバインディングを要求する。

旅行者102が携帯電話IDの使用を受け入れると、MaaSアプリケーションは、固有IDを読み取り、106においてユーザ・プロファイル・サーバ104に固有IDを送信する。このIDは、送信用に暗号化する必要がある。

【0179】

10

20

30

40

50

次に、ユーザ・プロフィール・サーバ104は、107において、ユーザアカウントと固有ID(携帯電話ID)とをバインドする。

【0180】

旅行者102は、2つ以上のIDを選択することができる。例えば、いくつかのスマートフォンは、2つ以上のIMSIを選択できるように、2つ以上のSIMカード、すなわち2つ以上のIMSIを有する。

【0181】

ユーザ・プロフィール・サーバ104は、ユーザアカウントとその固有IDとの関係を記憶する。ユーザ・プロフィール・サーバ104は、ユーザアカウントと固有IDとの間のマッピング情報をブロックチェーン・オラクル101に送信することができる(108)。

10

【0182】

あるいは、バインディングが、端末で(例えば、MaaSアプリケーションによって)処理することができる。

次に、ユーザ・プロフィール・サーバ104は、108'において、特定のユーザに対して認証をブロックチェーン・オラクル101に発行する要求を送信し、この要求には、固有IDに基づいて暗号化された情報が含まれていてもよい。

次いで、ブロックチェーン・オラクル101は、109において、認証を端末(例えば、端末上で実行されているMaaSアプリケーション)に送信する。次に、MaaSアプリケーションは、107'において、固有IDと端末内の受信された認証との間のバインディングを進める。

20

【0183】

バインディングは、携帯電話(端末)に加えて、従来の信用証明書と組み合わせることができる。これは、さらに強力なセキュリティを提供することができる。例えば、ユーザ端末が、旅行者のパスポート、運転免許証などのICチップからデータをスキャンまたは読み取ってもよい。

そのような同様の文書が、信頼された民間組織によって発行される場合、例えば、コーポレートIDカードまたはクレジットカードのようなプライベートIDもまた、いくつかの実施形態において使用され得る。

信用証明書がユーザプロフィールと一致しない場合、バインディングは受け入れられない。

30

【0184】

しかしながら、携帯電話や他の端末を使用すると、紛失したり盗まれたりする危険性がある。他人の電話機を交通チケットとして使用することは、旅行者に金銭的損害をもたらすだけでなく、交通会社または社会の深刻なセキュリティリスクも引き起こす。

列車/飛行機の乗車/搭乗のために紛失/盗難された電話機を使用することを防止することが重要である。

【0185】

いくつかの実施形態は、そのようなリスクに関連し、したがって、例えば、適切な電話機または紛失/盗難された電話機を追跡するための情報を記憶するIMEI(国際移動体装置識別番号)データベースが提供される(いわゆるIMEIブラックリスト)。

40

通信事業者は、契約されたSIMカードおよびIMSIのための加入者データベースを有する。そのような実施形態では、ブロックチェーン・オラクルが、これらの信頼できるデータベースと通信し、このプロセスに関与する携帯電話(すなわち他の端末)の状態を定期的に確認することができる。

【0186】

いくつかの実施形態ではバインディング後であっても、ブロックチェーン・オラクルは、必要に応じて、バインディングの再確認を要求することができる。例えば、端末は、元の旅行者が移動する可能性が低い予期しない場所/国で使用されると、ブロックチェーン・オラクルは、バインディングのダブルチェック/再確認を要求することができる。

【0187】

50

図13は、ユーザデータソースの検証手順の方法110の一実施形態のフローチャートを示す。

ブロックチェーン・オラクルサーバ111は、旅行者112とブロックチェーン管理113とユーザ・プロファイル・サーバ114との間の通信のために提供される。

【0188】

旅行者112は、センサ等を有するスマートフォン/ウェアラブルデバイスを有し、従って、115においてブロックチェーン・オラクル111にセンサデータまたはトリガを送信する。

【0189】

ブロックチェーン・オラクル111がバインディング情報を有する場合、ブロックチェーン・オラクル111は、116において、センサデータ/トリガの発信元、および、ユーザアカウントと登録されたモバイル情報との間のバインディングを検証する。

【0190】

ブロックチェーン・オラクル111が、(代替ソリューションとして)バインディング・データを記憶しない場合、ブロックチェーン・オラクル111は、117において、固有IDを検証する要求を、MaaS事業者サイトのユーザ・プロファイル・サーバ114に送信する。ここで、ユーザ・プロファイル・サーバ114は、118で検証を実行し、検証が成功した場合、119で確認をブロックチェーン・オラクル111に送信する。

【0191】

ブロックチェーン・オラクル111は、ユーザ・プロファイル・サーバ114からその確認を受信し、その後、ブロックチェーン・オラクル111は、120において、スマートコントラクトを実行するトリガをブロックチェーン管理113に送信する。

【0192】

あるいは、バインディングが端末(アプリケーション)で実行される場合、121において端末側で検証を実行し、122でトリガをブロックチェーン管理113に送ることができる。

【0193】

このような場合、スマートフォン/ウェアラブルデバイスは、上述されているように、それ自体のセンサによってトリガを開始する。

アプリケーションは、端末におけるバインディングの固有ID(例えば、IMSI)を読み取り、正しい(固有の)IDを検証する。端末は、記憶された認証を有するデータ/トリガをブロックチェーン・オラクル111に送る。

【0194】

ブロックチェーン・オラクルは上述したように、固有IDを知らなくても、認証を使用して真正のデータソースを検証することができる。

【0195】

本明細書の実施形態は、使用事例としてMaaSに焦点を当てているが、本開示の一般的な概念は、IoT(モノのインターネット)スマートコントラクト、フィンテック(金融取引)、電気通信/インターネットサービスなどの他のアプリケーションにも適用することができる。

【0196】

以下では、汎用コンピュータ130の一実施形態を、図14を参照して説明する。

コンピュータ130は、基本的に本明細書で説明するように、任意のタイプのネットワーク機器、例えば、基地局または新しい無線基地局、送受信ポイント、または、ユーザ機器、(末端の)(モバイル)端末デバイスなどの通信デバイスとして機能することができるように実装される。

コンピュータは本明細書に記載されるように、ネットワーク装置および通信デバイスの回路のうちの任意の1つのような回路を構成することができる構成要件131乃至141を有する。

【0197】

ソフトウェア、ファームウェア、プログラム等を用いて本明細書に記載されている方法を

10

20

30

40

50

実行する実施形態は、次いで具体的な実施形態に適するように構成されたコンピュータ130にインストールされる。

【0198】

コンピュータ130は、CPU131(中央演算処理装置)を有し、CPU131は例えば、読取り専用メモリ(ROM)132に記憶され、ストレージ137に記憶され、ランダム・アクセス・メモリ(RAM)133にロードされ、それぞれのドライブ139に挿入された記録媒体(メディア)140に記憶されるなどのプログラムに従って、本明細書に記載される様々なタイプの手順および方法を実行することができる。

【0199】

CPU 131、ROM 132およびRAM 133はバス141で接続されており、このバス141は、入出インターフェース134に接続されている。CPU、メモリ、およびストレージの数は、単に例示的なものであり、コンピュータ130は、基地局としてまたはユーザ機器(エンド端末)として機能するときに生じる特定の要件を満たすように適応および構成されることを、当業者は理解するであろう。

【0200】

入出インターフェース134には、入力部135、出力部136、ストレージ137、通信インターフェース138、および、記録媒体140(CD、デジタルビデオディスク、コンパクトフラッシュ(登録商標)メモリなど)を挿入することができるドライブ139のようないくつかの構成要件が接続される。

【0201】

入力部135は、ポインタデバイス(マウス、ペンタブレットなど)、キーボード、マイクロフォン、カメラ、タッチスクリーンなどとすることができる。

【0202】

出力部136は、ディスプレイ(液晶ディスプレイ、陰極線管ディスプレイ、発光ダイオードディスプレイ等)、スピーカ等を有することができる。

【0203】

ストレージ137は、ハードディスク、ソリッドステートドライブ等を有することができる。

【0204】

通信インターフェース138は例えば、ローカルエリアネットワーク(LAN)、無線ローカルエリアネットワーク(WLAN)、モバイル・テレコミュニケーション・システム(GSM、UMTS、LTE、NR等)、Bluetooth(登録商標)、赤外線等を介して通信するように構成される。

【0205】

上記の説明は、コンピュータ130の構成例にのみ関係することに留意されたい。代替の構成は、追加または他のセンサ、ストレージデバイス、インターフェースなどを用いて実装されてもよい。例えば、通信インターフェース138は、言及したUMTS、LTE、およびNR以外の他の無線アクセス技術をサポートし得る。

【0206】

コンピュータ130が基地局として機能する場合、通信インターフェース138は、(例えば、E-UTRAプロトコルOFDMA(ダウンリンク)およびSC-FDMA(アップリンク)を提供する)それぞれのエアインターフェース、および、(例えば、S1-AP、GTP-U、S1-MME、X2-APなどのプロトコルを実装する)ネットワークインターフェースをさらに有することができる。

さらに、コンピュータ130は、1つ以上のアンテナおよび/またはアンテナアレイを有してもよい。本開示は、そのようなプロトコルのいかなる特殊性にも限定されない。

【0207】

本開示の実施形態を実装するために使用される、ユーザ機器UE 150として構成されたモバイル端末およびeNB 155(またはNR eNB/gNB)、ならびにUE 150とeNB 155との間の通信経路154の実施形態を、図15を参照して説明する。

10

20

30

40

50

UE 150は通信デバイスの一例であり、eNBは基地局(すなわち、ネットワーク機器)の一例であるが、この点に関して本開示を限定するものではない。

【0208】

UE 150は送信機151、受信機152およびコントローラ153を有し、ここで一般に、送信機151、受信機152およびコントローラ153の技術的機能性は当業者には既知であり、従って、それらのより詳細な説明は省略される。

【0209】

eNB 155は送信機156、受信機157およびコントローラ158を有し、ここでも一般に、送信機156、受信機157およびコントローラ158の機能性は当業者には既知であり、したがって、それらのより詳細な説明は省略される。

【0210】

通信経路154は、UE 150からeNB 155へのアップリンク経路154aと、eNB 155からUE 150へのダウンリンク経路154bとを有する。

【0211】

動作中、UE 150のコントローラ153は、受信機152においてダウンリンク経路154bを介してダウンリンク信号の受信を制御し、コントローラ153は、送信機151によってアップリンク経路154aを介してアップリンク信号の送信を制御する。

【0212】

同様に、動作中、eNB 155のコントローラ158は、送信機156によってダウンリンク経路154bを介してダウンリンク信号の送信を制御し、コントローラ158は、受信機157においてアップリンク経路154aを介してアップリンク信号の受信を制御する。

【0213】

さらに要約すると、本明細書から明らかなように、いくつかの実施形態は、分散型台帳にデータを提供するための通信ネットワークノードに関する。

ここで、ノードは、スマートコントラクトへの入力として使用される入力データの検証を提供すること、および、スマートコントラクトからの出力に基づく出力データが所定のデバイスで正しく受信されるかどうかの検証を提供することのうちの少なくとも1つを実行するように構成された回路を有する。

【0214】

通信ネットワークノードは、基地局、eNodeBなどのネットワーク機器であってもよいが、ノードは、状況に応じて構成される回路を有するユーザ装置、(末端の)端末デバイスなどの通信デバイス(例えば、携帯電話、スマートフォン、コンピュータ、ラップトップ、ノートブックなど)として構成されてもよい。

特に、通信ネットワークノードは、本明細書で説明されるようなブロックチェーン・オラクルであってもよい。

【0215】

いくつかの実施形態では分散型台帳は、ブロックチェーンを含み(またはブロックチェーンであり)、ブロックチェーンは複数のブロックを含むことができる。

【0216】

いくつかの実施形態では、分散型台帳は、モビリティ・アズ・ア・サービス用のデータを含む。

【0217】

いくつかの実施形態では、分散型台帳へのアクセスが許可権に基づいて付与され、ノードは、コンソーシアムの一部であってもよい。

コンソーシアムは、モビリティ・アズ・ア・サービスによって提供されてもよく、ここで、各ノードは例えば、1つのモビリティ・サービス・プロバイダに相当するか、または、関連付けられてもよい。

【0218】

前述のように、分散型台帳はブロックチェーンを含むことができ、ブロックチェーンは、複数のブロックを含むことができ、ブロックは機密事項でないユーザデータを含み、分散

10

20

30

40

50

型台帳は、モビリティ・アズ・ア・サービス用のデータを含むことができる。

したがって、いくつかの実施形態では、通信ネットワークおよびそのノードは、MaaSを提供するように構成される。

【0219】

入力データは、ユーザを識別するセンサデータに基づいて検証されてもよい。センサデータは、ユーザのモバイル端末に含まれる少なくとも1つのセンサ(例えば、測位センサ、画像センサ、指紋センサなど)によって提供されてもよい。

【0220】

センサデータは、ユーザを検出する少なくとも1つのセンサ(例えば、ユーザが立ち入り、ユーザが検出される、到着場所またはチェックイン、搭乗場所などに配置されたセンサ)によって提供されてもよい。

10

【0221】

回路は、センサデータを提供するセンサの認証を提供するようにさらに構成されてもよく、それによって、センサが信頼できるものであることが保証されてもよい。

【0222】

センサデータは、位置データまたは生体認証データを含んでもよい。

【0223】

位置データは、検証のためにロケーションサーバに送信されてもよい。

【0224】

生体認証データは、検証のために生体認証データサーバに送信されてもよい。

20

【0225】

回路は、データ完全性機能に基づいてデータを受信または送信するようにさらに構成されてもよく、このデータ完全性機能は、ハッシュ関数、デジタル署名、ブロックストリームアルゴリズムのうちの少なくとも1つに基づいていてもよい。

【0226】

回路は、スマートコントラクトの実行を引き起こすためのトリガを送信するようにさらに構成されてもよい。

【0227】

トリガは、入力データの検証が成功した場合に送信されてもよい。

【0228】

回路は、ユーザベースの識別とモバイル端末ベースの識別との間のバインディングを実行するようにさらに構成されてもよい。

30

【0229】

検証は、バインディングの検証を含んでもよい。

【0230】

モバイル端末ベースの識別は、セルラ国際移動体加入者識別番号、セルラIMEI(国際移動体装置識別番号)のうちの少なくとも1つを含んでもよい。

【0231】

回路は、接続されたデバイスの認証を検証するようにさらに構成されてもよい。

【0232】

接続されたデバイスの認証は、ハッシュ関数に基づく認証、規格ベース認証、接続されたデバイスの製造者識別番号、デバイスの事前設定、接続されたデバイスに関連する固有のネットワークまたはセルラ識別のうちの少なくとも1つに基づいて検証されてもよい。

40

【0233】

いくつかの実施形態は、スマートコントラクトを動作させるための方法に関し、スマートコントラクトは少なくとも2つの異なる状態を有し、この方法は、トリガを受信することに応答してスマートコントラクトの状態を変更するステップを含む。

【0234】

この少なくとも2つの異なる状態は、チェックイン状態、チェックアウト状態、使用中状態、未使用状態およびキャンセル状態のうちの少なくとも1つを含んでもよい。

50

【0235】

トリガは、本明細書で説明するように、信頼されたネットワーク通信ノード(例えば、ブロックチェーン・オラクル)から受信されてもよい。

【0236】

トリガは、(例えば、認証に基づいて検証された)信頼されたセンサから受信されてもよい。

【0237】

スマートコントラクトは、トリガの受信に応答して実行されてもよい。

【0238】

スマートコントラクトの実行結果は、スマートコントラクトの状態によって決まり得る。

【0239】

いくつかの実施形態は、分散型台帳を提供するための複数のノードを備える通信ネットワークを制御するための方法に関し、この方法は、スマートコントラクトへの入力として使用される入力データの検証を提供するステップと、スマートコントラクトからの出力に基づく出力データが、所定のデバイスで正しく受信されるかどうかの検証を提供するステップとのうちの少なくとも1つを含む。

本方法は、本明細書で説明される通信ネットワークの1つ以上のノードによって、かつ/もしくは、モバイル端末または任意の他の処理デバイスまたは回路によって実行され得る。

【0240】

入力データは、ユーザを識別するセンサデータに基づいて検証されてもよい。

【0241】

センサデータは、ユーザのモバイル端末に含まれる少なくとも1つのセンサによって提供されてもよい。

【0242】

センサデータは、ユーザを検出する少なくとも1つのセンサによって提供されてもよい。

【0243】

本方法は、センサデータを提供するセンサの認証を提供するステップをさらに含んでもよい。

【0244】

センサデータは、位置データまたは生体認証データを含んでもよい。

【0245】

本方法は、検証のために位置データをロケーションサーバに送信するステップをさらに含んでもよい。

【0246】

この方法は、検証のために生体認証データを生体認証データサーバに送信するステップをさらに含んでもよい。

【0247】

本方法は、データ完全性機能に基づいてデータを受信または送信するステップをさらに含んでもよい。

【0248】

このデータ完全性機能は、ハッシュ関数、デジタル署名およびブロックストリームアルゴリズムのうちの少なくとも1つに基づいてもよい。

【0249】

本方法は、スマートコントラクトの実行を引き起こすためのトリガを送信するステップをさらに含んでもよい。

【0250】

トリガは、入力データの検証が成功した場合に送信されてもよい。

【0251】

トリガは、ユーザの識別、ユーザのロケーションベースの検出、および、ユーザの生体認

10

20

30

40

50

証に基づく検出のうちの少なくとも1つに基づいて送信されてもよい。

【0252】

ロケーションベースの検出は、ユーザのデバイスによって提供されるロケーション（位置）データと、ユーザのネットワークベースの測位とに基づいて、ユーザの位置を確認することを含んでもよい。

【0253】

ロケーションベースの検出は、ユーザを識別するための視覚処理を含んでもよい。

【0254】

本方法は、ユーザベースの識別とモバイル端末ベースの識別との間のバインディングを実行するステップをさらに含んでもよい。

【0255】

検証は、バインディングの検証を含んでもよい。

【0256】

モバイル端末ベースの識別は、セルラ国際移動体加入者識別番号、セルラIMEIのうちの少なくとも1つを含んでもよい。

【0257】

本方法は、接続されたデバイスの認証を検証するステップをさらに含んでもよい。

【0258】

接続されたデバイスの認証は、ハッシュ関数に基づく認証、規格ベース認証、接続されたデバイスの製造者識別番号、デバイスの事前設定、接続されたデバイスに関連する固有のネットワークまたはセルラ識別のうちの少なくとも1つに基づいて検証されてもよい。

【0259】

分散型台帳は、ブロックチェーンを含んでもよい。

【0260】

分散型台帳は、モビリティ・アズ・ア・サービス用のデータを含んでもよい。

【0261】

分散型台帳へのアクセスは、許可権に基づいて付与されてもよい。

【0262】

ノードは、コンソーシアムの一部であってもよい。

【0263】

検証の提供は、スマートコントラクトが改ざんされるリスクに基づいてもよく、この検証は、リスクに基づいて省略または制限されてもよい(例えば、ダブルチェックの代わりに1回のチェックなど)。

【0264】

いくつかの実施形態は本明細書で説明されるように、分散型台帳にデータを提供するために(本明細書で説明されるような)ネットワークノードと通信するためのモバイル端末に関し、モバイル端末は、スマートコントラクトへの入力として使用される入力データを提供するように構成された回路を有する。

【0265】

モバイル端末は、少なくとも1つのセンサを有してもよく、入力データは、少なくとも1つのセンサ(例えば、画像センサ、指紋センサ、生体計測センサ、位置/ナビゲーションセンサ等)のセンサデータに基づいて提供される。

少なくとも1つのセンサは、位置データまたは生体認証データを提供することができる。

【0266】

回路は、アプリケーションを実行するようにさらに構成されてもよく、アプリケーションは、ネットワークノードに入力データを提供するように構成されてもよく、アプリケーションは、モビリティ・アズ・ア・サービスのアプリケーションであってもよい。

【0267】

モバイル端末は、スマートフォン(または任意の他のスマートデバイス、ウェアラブルデバイスなど)であってもよい。

10

20

30

40

50

【0268】

アプリケーションは、ユーザの認証(例えば、顔認識、指紋検出または他の生体認証データ検証)を行うように構成されてもよい。

【0269】

アプリケーションは、モバイル端末のセンサによって提供されるセンサデータに基づいて、ユーザのチェックイン(例えば、ロケーションベースのチェックインおよび/または生体認証ベースのチェックイン)を判定するように構成されてもよい。

【0270】

回路は、モバイル端末とアプリケーションとの間のバインディングを実行するようにさらに構成されてもよく、バインディングは、ネットワークノードから受信される認証に基づいて実行されてもよい。

10

【0271】

以下では、いくつかの用語の定義が与えられ、それらはいくつかの実施形態において(本開示を以下に与えられる定義に限定することなく)適用され得る。これらの定義は、本開示の理解を高めるために与えられた例にすぎず、MaaSおよび分散型台帳の技術分野は、非常に動的であり、定義は今後変化し得るので、与えられたものにすぎない。

【0272】

「分散型台帳」という用語は、「分散型台帳(共有台帳、または分散型台帳技術、DLTとも呼ばれる)は、複数のサイト、国、または機関に地理的に分散した、複製、共有、および同期化されたデジタルデータのコンセンサスであり、中央管理者または集中型データストレージは存在しない」と定義するWikipediaから既知である。

20

【0273】

「モビリティ・アズ・ア・サービス(MaaS)」という用語は、「モビリティ・アズ・ア・サービス(MaaS)は、個人所有の輸送モードから離れ、サービスとして消費されるモビリティソリューションに向かうシフトを説明する。

これは、単一のアカウントでユーザが支払うことができる、旅行を作成し管理する統合ゲートウェイを介して、公共および民間の輸送プロバイダからの輸送サービスを組み合わせることによって可能になる。

ユーザは旅行ごとに支払うことができ、または、限られた距離の月額料金を支払うことができる。MaaSの背後にある重要な概念は、旅行のニーズに基づいて旅行者のモビリティソリューションを提供することである。」と定義するWikipediaからも既知である。

30

【0274】

「パブリック・ブロックチェーン/分散型台帳」とは、いくつかの実施形態では、上記のように、誰でも分散データベース(台帳)を共有し、参加してコンセンサスプロトコルを実行することができることを意味する。

【0275】

これとは対照的に、「許可されたブロックチェーン/分散型台帳」とは、許可されたメンバーのみが分散データベース(台帳)を共有し、参加してコンセンサスプロトコルに実行することができることを意味する。

ブロックチェーンにアクセスする許可を有する許可されたメンバーは、上述のように「コンソーシアム」と呼ばれる。いくつかの実施形態では、許可された/コンソーシアムタイプのブロックチェーンは、MaaSアプリケーションに適しており、公共のものではないので、誰もがアクセスすることはできない。

40

【0276】

「インスタンス」という用語は、クラウド上で実行されるソフトウェアプロセスとして理解される。インスタンスは、分散クラウド内のどこかに移動してもよい。

【0277】

「パブリッククラウド」とは、(<https://azure.microsoft.com/en-gb/overview/what-are-private-public-public-hybrid-clouds/>):「パブリッククラウドは、クラウドコンピューティングを展開する最も一般的な方法である。クラウドリソース(

50

サーバやストレージなど)は、サードパーティのクラウドサービスプロバイダによって所有され、運営され、インターネット経由で配信される」ものとして定義されている。

【0278】

いくつかの実施形態では、以下の用語が所与の理解において使用される。

【0279】

「マルチモーダル・トランスポート・パス」という用語は、有効期間または利用可能な輸送、許容できないサービスなどの特定の条件を有する複数のモビリティ・サービスに有効なパスのことである。

例えば、1日券、1週間券、毎月のMaaSサービス契約、シーズンチケットなどがある。

【0280】

「モビリティ・サービス・プロバイダ」という用語は、任意のタイプのサービス・プロバイダMaaSの包括的なものの名称である。いくつかの実施形態では、モビリティ・サービス・プロバイダは、典型的には鉄道会社、バス/コーチ、トラムおよびタクシー、カーシェアリング、ライドシェアリング、バイクシェアリングなどの輸送機関である。

モビリティ・サービス・プロバイダの中には、実際の輸送手段を提供しないものもあるが、旅行代理店またはオンライン予約サイトなどに匹敵する予約/手配のみを提供してもよい。

【0281】

「パス」という用語は、トランジットパスまたはトラベルカード(UK)とする(https://en.wikipedia.org/wiki/transit_passも参照)。

本開示では、マルチモーダルパスも「パス」という用語に該当するものとし、これは、パスが2人以上の輸送事業者(またはモビリティサービス提供者)の間で有効であり得ることを意味し、したがって、公共交通だけでなく、ライドシェア、バイクシェアなどの他のタイプのモビリティにも及び得ることを意味する。

パスは、許容可能な輸送、有効期間、および、チケット発行/輸送乗車の任意の他の条件の情報を含むことができる。いくつかの実施形態では、MaaSは、サービスレベルのいくつかの選択肢を、月次サービスサブスクリプションに提供することができる。

旅行者(乗客)またはユーザは、特定の期間のパスのサービスサブスクリプション料金すなわち入手を、(通常、パスを発行するモビリティ・サービス・プロバイダとすることができ)パス発行者に支払うことができる。このパスは、(すべて、上述のモビリティ・サービス・プロバイダという用語に該当する)輸送事業者または旅行代理店、MaaSサービス・プロバイダなどによって発行される。

したがって、上述したように、パス発行者のうちの一部は、パスを販売するが、実際の輸送サービスまたは輸送手段を提供しなくてもよい。

【0282】

「チケット」という用語は、座席予約を伴う(または伴わない)片道列車チケットのような特定のセクションの片道旅行のためのチケットであってもよい。このチケットは、いくつかの実施形態では、マルチモーダル・トランスポート・パスおよびその条件の下で発行されてもよく、選択された輸送、座席番号、価格などの情報を含んでもよい。

いくつかの実施形態では、座席の予約が再び要求されないか、または、無制限の旅行が許可される場合であっても、チケットは、複数のモビリティ・サービス・プロバイダ間での収益共有のために発行されてもよい。

さらに、旅行者(ユーザ)は、チケット発行者に直接支払わなくてもよいが、パス発行者が、旅行者の代わりにチケット発行者に支払うことができ、チケットは、輸送事業者またはサービス・プロバイダ、すなわちモビリティ・サービス・プロバイダによって発行される。

【0283】

「旅行ログ」という用語は、チケットに基づいた片道旅行記録である旅行ログを含んでもよい。

旅行ログは、例えばエンバクメントの位置、その時刻/日、降車位置、その時刻/日、

10

20

30

40

50

チケットが使用されたか未使用であるか等に関する情報を含んでもよく、これについても以下でさらに説明する。

【0284】

「スマートコントラクト」という用語は、一般的に知られており、例えばWikipediaは、以下のように説明している(https://en.wikipedia.org/wiki/smart_contract)。

「スマートコントラクトは、契約の交渉または履行をデジタル的に容易にし、検証し、または実施することを意図したコンピュータプロトコルである。スマートコントラクトは、サードパーティ（第三者）なしで信頼できる取引を実行することを可能にする。

この取引は追跡可能であり、不可逆的である。スマートコントラクトは、1994年にこの用語を作ったニック・ズザボによって最初に提案された。スマートコントラクトの提案者は、多くの種類の契約条項が部分的または完全に自己実行、自己実施、またはその両方を行うことができると主張している。

スマートコントラクトの目的は、従来の契約法よりも優れたセキュリティを提供し、契約に関連する他の取引コストを削減することである。さまざまな暗号通貨が、スマートコントラクトのタイプを実装している。」

【0285】

本開示を限定することなく、いくつかの実施形態で使用されるスマートコントラクト言語は、ブロックチェーン内のスマートコントラクトを記述するためのコンピュータ言語であり、ブロックチェーン用の仮想マシン上で動作/実行することができる。

さらに、スマートコントラクト言語には使用される様々な言語がある。例えば、EthereumプロジェクトのSolidityチームは、スマートコントラクト言語「Solidity」を開発した。

【0286】

「ブロックチェーン・オラクル」という用語は、「オラクルとは何か」という<https://blog.apla.io/what-is-a-blockchain-oracle-2ccca433c026>でも開示されているように、ある程度はいくつかの実施形態において理解されている。

各種オンライン辞書によれば、オラクルは、「権威的または賢明な表現または回答」もしくは「何かについての絶対的な権威と見なされる人または物」と定義されている。実際、辞書自体は、オラクルと見なしているが、オラクルは、ブロックチェーンとどのような関係があるのだろうか？ブロックチェーン・オラクルとは何だろうか？

【0287】

ブロックチェーン・オラクルを理解するためには、読者は、まずブロックチェーンとスマートコントラクトとに精通しておく必要がある。スマートコントラクトは、EthereumやAplaなどのブロックチェーンネットワークで実行され、特定のイベントに基づいてアクションまたはタスクを実行するソフトウェアコードである。

最も明白な例は、Ethereumネットワーク上で取引を送ることであり、ここで、当事者は、受信者のアドレスと、当事者が有し、資金を所有するプルーフとを、ネットワークに提供する。すべてがチェックアウトした場合、ネットワークは、その資金を受信者に「振り替える」。

さらに、現在の天気温度、株価、またはFIFAワールドカップ決勝の結果などの外部データを必要とする分散型アプリケーションの場合、問題は、スマートコントラクト、すなわち、言い換えれば、ブロックチェーン上のコードのピースがどのように情報を取得するかであり、そのような場合、ブロックチェーンアプリケーション用のオラクルが使用されることが説明される。

【0288】

さらに、「オラクルは、スマートコントラクトのための世界の状態についての情報を提供するか、または、請求に署名する、信頼できるデータソースまたはエンティティである。オラクルは、現実世界のイベントとブロックチェーンプラットフォームのデジタル世界との間のリンクである。オラクルは、未来についての予測を行うのではなく、過去からのイベントを報告する。」

【0289】

「ステートフル/ステートレススマートコントラクト」という用語は、いくつかの実施形態では以下のように理解される。ステートフルとは、ブロックチェーンの内部状態を把握・維持することを意味する。

これは、ループプロセスを含むコンピュータプログラムに類似しており、複雑な条件を記述するのに適している。ステートレスとは、ブロックチェーンの内部状態を把握・維持しないことを意味する。このプロセスは簡単である。単純な条件を記述することが適切である。

【0290】

「データ完全性」という用語は、Wikipedia(https://en.wikipedia.org/wiki/Data_integrity)によって定義されるように理解される。

「データ完全性は、データのライフサイクル全体にわたるデータの精度および一貫性の維持および保証であり、データを記憶、処理、または検索する任意のシステムの設計、実装、および使用にとって重要な態様である。」

【0291】

「認証局(CA)」という用語は、Wikipedia(https://en.wikipedia.org/wiki/Certificate_authority)によって定義されているように理解される。

「暗号技術において、認証局または証明機関(CA)は、デジタル証明書を発行するエンティティである。デジタル証明書は、証明書の名前付きサブジェクトによって公開鍵の所有権を証明する。これにより、他者(依頼当事者)は、署名または認証された公開鍵に対応する秘密鍵について行われたアサーションを信頼することができる。」

CAは、証明書のサブジェクト(所有者)と証明書に依頼する当事者の両方によって信頼される、信頼されたサードパーティとして機能する。これらの証明書のフォーマットは、X.509規格で規定される。」

【0292】

「スプーフィング」という用語は、Wikipedia(https://en.wikipedia.org/wiki/spoofing_attack#GPS_spoofing)によって定義されているように理解される。

「スプーフィング」- 情報セキュリティ、特にネットワークセキュリティのコンテキストにおいて、スプーフィング攻撃とは、不正な利点を得るために、人またはプログラムが別の人物として偽装することに成功した状況である。

【0293】

(GPS/GNSSスプーフィング)

GPSスプーフィング攻撃は、一連の正常なGPS信号に似たように構成された誤ったGPS信号をブロードキャストすることによって、または、他の場所または異なる時間にキャプチャされた真の信号を再ブロードキャストすることによって、GPS受信機をだますことを試みる。

これらのスプーフィングされた信号は、受信機に、攻撃者によって判定されるように、受信機の位置を、実際の場所以外のどこかに推定させるように、または、受信機がある場所に配置されているが異なる時間に位置するように、修正され得る。

一般にキャリアオフ攻撃と呼ばれるGPSスプーフィング攻撃の1つの一般的な形態は、対象受信機によって観測された真の信号と同期した信号をブロードキャストすることから始まる。次いで、偽造信号の電力は徐々に増加し、真の信号から引き離される。

【0294】

用語「サイドチャネル攻撃」は、Wikipedia(https://en.wikipedia.org/wiki/Side-channel_attack)によって定義されるように理解される。

「コンピュータセキュリティにおけるサイドチャネル攻撃は、実装されたアルゴリズム自体の弱点(例えば、暗号解析およびソフトウェアバグ)ではなく、コンピュータシステムの実装から得られる情報に基づく任意の攻撃である。

時間情報、電力消費、電磁漏れ、または音声さえも、利用可能な追加の情報源を提供することができる。」

10

20

30

40

50

【0295】

用語「ゼロ知識証明/プロトコル」は、Wikipedia(https://en.wikipedia.org/wiki/Zero-knowledge_proof)によって定義されるように理解される。

「暗号技術では、ゼロ知識証明またはゼロ知識プロトコルは、一方の当事者(証明者)が値 x を知っていることを他方の当事者(検証者)に証明することができる手法であり、一方の当事者が値 x を知っている事実以外の情報を伝達することはない。

ゼロ知識証明の本質は、ゼロ知識証明を単に明らかにすることによって、一方の当事者が特定の情報の知識を所有することを証明することが自明であることであり、この命題は、情報自体または追加情報を明らかにすることなくその所有を証明することである。」

【0296】

いくつかの実施形態では、セル測位に関連する以下の用語が含まれる。

- ・UEベースの測位: 観測到達時間差(OTDOA)、セルIDベース
- ・ネットワークベースの測位: アップリンク到達時間差(UTDOA)
- ・電気通信ネットワークのロケーションサーバ: セキュアユーザプレーンロケーション(SUPL)サーバ、Enhanced Serving Mobile Location Center(E-SMLC)

【0297】

本明細書に記載される方法は、いくつかの実施形態では、コンピュータおよび/またはプロセッサおよび/または回路上で実行されるときに、コンピュータおよび/またはプロセッサおよび/または回路に本方法を実行させるコンピュータプログラムとしても実装される。

いくつかの実施形態では、上述のプロセッサによって実行されると、本明細書に記載の方法を実行させるコンピュータプログラム製品を記憶する非一時的なコンピュータ可読記録媒体も提供される。

【0298】

本発明の実施形態は、方法ステップの例示的な順序付けを伴う方法を説明することを理解されたい。しかしながら、方法ステップの特定の順序付けは、例示のみを目的として与えられており、拘束力のあるものとして解釈されるべきではない。

【0299】

本明細書に記載され、添付の特許請求の範囲に請求されるすべてのユニットおよびエンティティは、別段の記載がない限り、例えばチップ上の集積回路ロジックとして実装され、そのようなユニットおよびエンティティによって提供される機能は、別段の記載がない限り、ソフトウェアによって実装される。

【0300】

上述の本開示の実施形態が、少なくとも部分的に、ソフトウェア制御されるデータ処理装置を使用して実施される限り、そのようなソフトウェア制御を提供するコンピュータプログラム、およびそのようなコンピュータプログラムが提供される送信、ストレージ、または他の媒体が、本開示の態様として想定されることが理解される。

【0301】

なお、本技術は以下のように構成されてもよい。

(1) データを分散型台帳に提供するための通信ネットワークノードであって、ノードは、スマートコントラクトへの入力として使用される入力データの検証を提供すること、および、スマートコントラクトからの出力に基づく出力データが、所定のデバイスで正しく受信されるかどうかの検証を提供すること
のうちの少なくとも1つを実行するように構成された回路を具備する通信ネットワークノード。

(2) (1)に記載の通信ネットワークノードであって、前記入力データは、ユーザを識別するセンサデータに基づいて検証される通信ネットワークノード。

10

20

30

40

50

(3) (2)に記載の通信ネットワークノードであって、
前記センサデータは、ユーザのモバイル端末に含まれる少なくとも1つのセンサによって提供される
通信ネットワークノード。

(4) (2)または(3)に記載の通信ネットワークノードであって、
前記センサデータは、ユーザを検出する少なくとも1つのセンサによって提供される
通信ネットワークノード。

(5) (2)から(4)のいずれか1つに記載の通信ネットワークノードであって、
前記回路は、前記センサデータを提供するセンサの認証を提供するようにさらに構成される
通信ネットワークノード。

10

(6) (2)から(5)のいずれか1つに記載の通信ネットワークノードであって、
前記センサデータは、位置データまたは生体認証データを含む
通信ネットワークノード。

(7) (6)に記載の通信ネットワークノードであって、
前記位置データは、検証のためにロケーションサーバに送信される
通信ネットワークノード。

(8) (6)または(7)に記載の通信ネットワークノードであって、
前記生体認証データは、検証のために生体認証データサーバに送信される
通信ネットワークノード。

20

(9) (1)から(8)のいずれか1つに記載の通信ネットワークノードであって、
前記回路は、データ完全性機能に基づいてデータを受信または送信するようにさらに構成される
通信ネットワークノード。

(10) (9)に記載の通信ネットワークノードであって、
前記データ完全性機能は、ハッシュ関数、デジタル署名、ブロックストリームアルゴリズムのうちの少なくとも1つに基づくものである
通信ネットワークノード。

(11) (1)から(10)に記載の通信ネットワークノードであって、
前記回路は、前記スマートコントラクトの実行を引き起こすためのトリガを送信するようにさらに構成される
通信ネットワークノード。

30

(12) (11)に記載の通信ネットワークノードであって、
前記トリガは、入力データの検証が成功した場合に送信される
通信ネットワークノード。

(13) (1)から(12)に記載の通信ネットワークノードであって、
前記回路は、ユーザベースの識別とモバイル端末ベースの識別との間のバインディングを実行するようにさらに構成される
通信ネットワークノード。

(14) (13)に記載の通信ネットワークノードであって、
前記検証は、バインディングの検証を含む
通信ネットワークノード。

40

(15) (13)または(14)に記載の通信ネットワークノードであって、
前記モバイル端末ベースの識別は、セルラ国際移動体加入者識別番号およびセルラ国際移動体装置識別番号のうちの少なくとも1つを含む
通信ネットワークノード。

(16) (1)から(15)に記載の通信ネットワークノードであって、
前記回路は、接続されたデバイスの認証を検証するようにさらに構成される
通信ネットワークノード。

(17) (16)に記載の通信ネットワークノードであって、

50

前記接続されたデバイスの認証は、ハッシュ関数に基づく認証、規格ベース認証、前記接続されたデバイスの製造者識別番号、デバイスの事前設定、および、前記接続されたデバイスに関連する固有のネットワークまたはセルラ識別のうちの少なくとも1つに基づいて検証される

通信ネットワークノード。

(18) (1) から (17) に記載の通信ネットワークノードであって、前記分散型台帳は、ブロックチェーンを含む

通信ネットワークノード。

(19) (1) から (18) に記載の通信ネットワークノードであって、前記分散型台帳は、モビリティ・アズ・ア・サービス用のデータを含む

10

通信ネットワークノード。

(20) (1) から (19) に記載の通信ネットワークノードであって、前記分散型台帳へのアクセスは、許可権に基づいて付与される

通信ネットワークノード。

(21) (20) に記載の通信ネットワークノードであって、前記ノードは、コンソーシアムの一部である

通信ネットワークノード。

(22) スマートコントラクトを動作させるための方法であって、前記スマートコントラクトは、少なくとも2つの異なる状態を有し、

トリガを受信することに応答して前記スマートコントラクトの状態を変更するステップを含む

20

方法。

(23) (22) に記載の方法であって、

前記少なくとも2つの異なる状態は、チェックイン状態、チェックアウト状態、使用中状態、未使用状態およびキャンセル状態のうちの少なくとも1つを含む

方法。

(24) (22) または (23) に記載の方法であって、前記トリガは、信頼されたネットワーク通信ノードから受信される

方法。

(25) (22) から (24) のいずれか1つに記載の方法であって、前記トリガは、信頼されたセンサから受信される

30

方法。

(26) (22) から (25) のいずれか1つに記載の方法であって、前記スマートコントラクトは、前記トリガの受信に応答して実行される

方法。

(27) (26) に記載の方法であって、

前記スマートコントラクトの実行結果は、スマートコントラクトの状態によって決まる

方法。

(28) 分散型台帳を提供するための複数のノードを具備する通信ネットワークを制御するための方法であって、

40

スマートコントラクトへの入力として使用される入力データの検証を提供するステップと、

スマートコントラクトからの出力に基づく出力データが、所定のデバイスで正しく受信されるかどうかの検証を提供するステップと

のうちの少なくとも1つを含む

方法。

(29) (28) に記載の方法であって、

前記入力データは、ユーザを識別するセンサデータに基づいて検証される

方法。

(30) (29) に記載の方法であって、

50

前記センサデータは、ユーザのモバイル端末に含まれる少なくとも1つのセンサによって提供される

方法。

(31) (29) または (30) に記載の方法であって、
前記センサデータは、ユーザを検出する少なくとも1つのセンサによって提供される方法。

(32) (29) から (31) のいずれか1つに記載の方法であって、
前記センサデータを提供するセンサの認証を提供するステップをさらに含む方法。

(33) (29) から (32) のいずれか1つに記載の方法であって、
前記センサデータは、位置データまたは生体認証データを含む方法。

10

(34) (33) に記載の方法であって、
検証のために前記位置データをロケーションサーバに送信するステップをさらに含む方法。

(35) (33) または (34) に記載の方法であって、
検証のために生体認証データを生体認証データサーバに送信するステップをさらに含む方法。

(36) (28) から (35) のいずれか1つに記載の方法であって、
データ完全性機能に基づいてデータを受信または送信するステップをさらに含む方法。

20

(37) (36) に記載の方法であって、
前記データ完全性機能は、ハッシュ関数、デジタル署名およびブロックストリームアルゴリズムのうちの少なくとも1つに基づく方法。

(38) (28) から (37) のいずれか1つに記載の方法であって、
前記スマートコントラクトの実行を引き起こすためのトリガを送信するステップをさらに含む方法。

(39) (38) に記載の方法であって、
前記トリガは、前記入力データの検証が成功した場合に送信される方法。

30

(40) (38) または (39) に記載の方法であって、
前記トリガは、ユーザの識別、ユーザのロケーションベースの検出、および、ユーザの生体認証に基づく検出のうちの少なくとも1つに基づいて送信される方法。

(41) (40) に記載の方法であって、
前記ロケーションベースの検出は、ユーザのデバイスによって提供されるロケーションデータと、ユーザのネットワークベースの測位とに基づいて、ユーザの位置を確認することを含む方法。

40

(42) (40) または (41) に記載の方法であって、
前記ロケーションベースの検出は、ユーザを識別するための視覚処理を含む方法。

(43) (28) から (42) のいずれか1つに記載の方法であって、
ユーザベースの識別とモバイル端末ベースの識別との間のバインディングを実行するステップをさらに含む方法。

(44) (43) に記載の方法であって、
前記検証は、前記バインディングの検証を含む

50

方法。

(45) (43) または (44) に記載の方法であって、
前記モバイル端末ベースの識別は、セルラ国際移動体加入者識別番号およびセルラ国際移動体装置識別番号のうちの少なくとも1つを含む

方法。

(46) (28) から (45) のいずれか1つに記載の方法であって、
接続されたデバイスの認証を検証するステップをさらに含む

方法。

(47) (46) に記載の方法であって、
前記接続されたデバイスの認証は、ハッシュ関数に基づく認証、規格ベース認証、前記接続されたデバイスの製造者識別番号、前記デバイスの事前設定、および、前記接続されたデバイスに関連する固有のネットワークまたはセルラ識別のうちの少なくとも1つに基づいて検証される

10

方法。

(48) (28) から (47) のいずれか1つに記載の方法であって、
前記分散型台帳は、ブロックチェーンを含む

方法。

(49) (28) から (48) のいずれか1つに記載の方法であって、
前記分散型台帳は、モビリティ・アズ・ア・サービス用のデータを含む

20

方法。

(50) (28) から (49) のいずれか1つに記載の方法であって、
前記分散型台帳へのアクセスは、許可権に基づいて付与される

方法。

(51) (50) に記載の方法であって、
前記複数のノードは、コンソーシアムの一部である

方法。

(52) (28) から (51) のいずれか1つに記載の方法であって、
前記検証の提供は、スマートコントラクトが改ざんされるリスクに基づく

方法。

(53) (52) に記載の方法であって、
前記検証は、前記リスクに基づいて省略または制限される

30

方法。

(54) 分散型台帳にデータを提供するためのネットワークノードと通信するためのモバイル端末であって、
スマートコントラクトへの入力として使用される入力データを提供するように構成された回路を具備する

モバイル端末。

(55) (54) に記載のモバイル端末であって、
少なくとも1つのセンサをさらに備え、前記入力データは、前記少なくとも1つのセンサのセンサデータに基づいて提供される

40

モバイル端末。

(56) (55) に記載のモバイル端末であって、
前記少なくとも1つのセンサは、位置データまたは生体認証データを提供する

モバイル端末。

(57) (54) から (56) のいずれか1つに記載のモバイル端末であって、
前記回路は、アプリケーションを実行するようにさらに構成され、前記アプリケーションは、前記ネットワークノードに前記入力データを提供するように構成される

モバイル端末。

(58) (57) に記載のモバイル端末であって、
前記アプリケーションは、モビリティ・アズ・ア・サービスのアプリケーションである

50

モバイル端末。

(59) (54) から (58) のいずれか 1 つに記載のモバイル端末であって、
前記モバイル端末は、スマートフォンである

モバイル端末。

(60) (57) に記載のモバイル端末であって、
前記アプリケーションは、ユーザの認証を行うように構成される

モバイル端末。

(61) (58) から (60) のいずれか 1 つに記載のモバイル端末であって、
前記アプリケーションは、前記モバイル端末のセンサによって提供されるセンサデータに
基づいて、ユーザのチェックインを判定するように構成される

10

モバイル端末。

(62) (57) から (61) のいずれか 1 つに記載のモバイル端末であって、
前記回路は、前記モバイル端末と前記アプリケーションとの間のバインディングを実行す
るようさらに構成される

モバイル端末。

(63) (62) に記載のモバイル端末であって、
前記バインディングは、認証に基づいて実行される

モバイル端末。

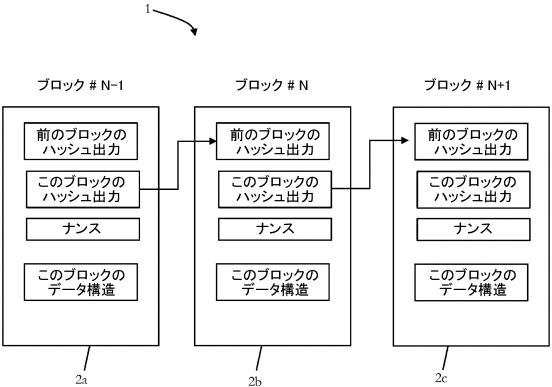
(64) (62) または (63) に記載のモバイル端末であって、
前記認証は、前記ネットワークノードから受信される

20

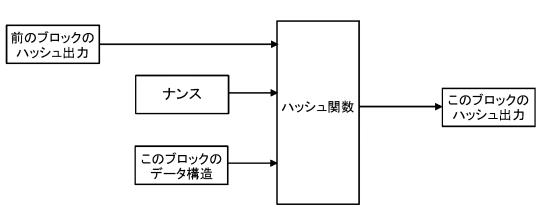
モバイル端末。

【図面】

【図 1】



【図 2】

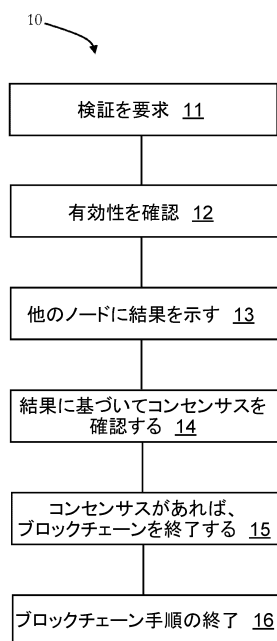


30

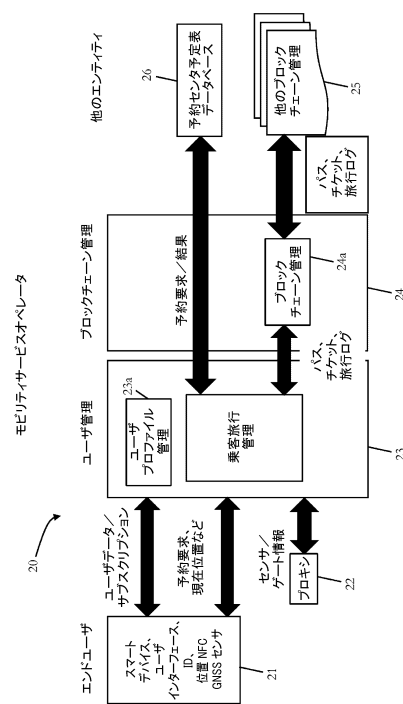
40

50

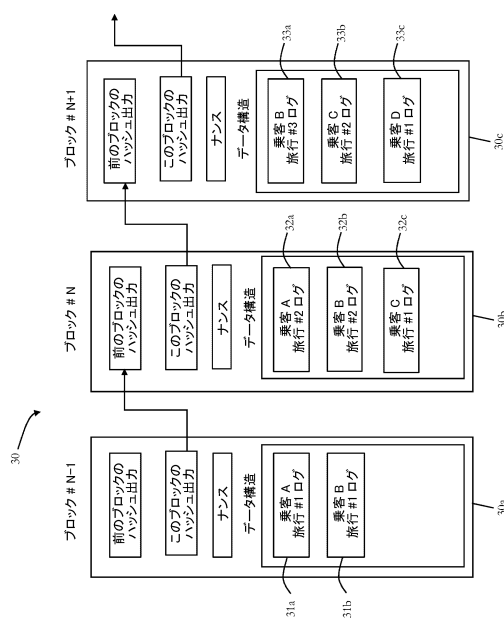
【圖 3】



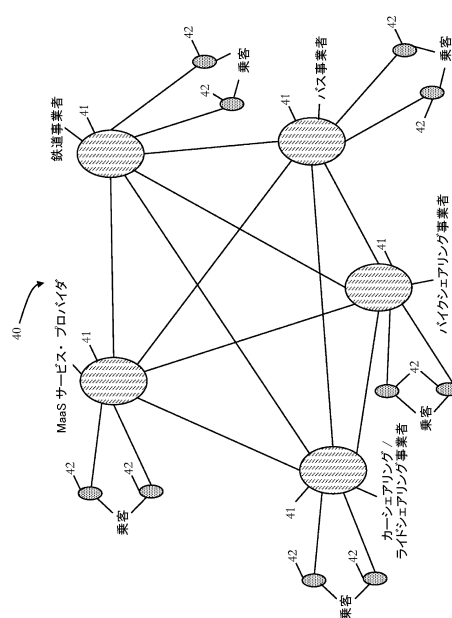
【図 4】



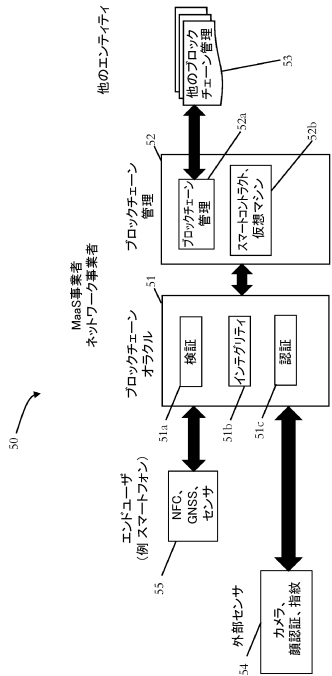
【図 5】



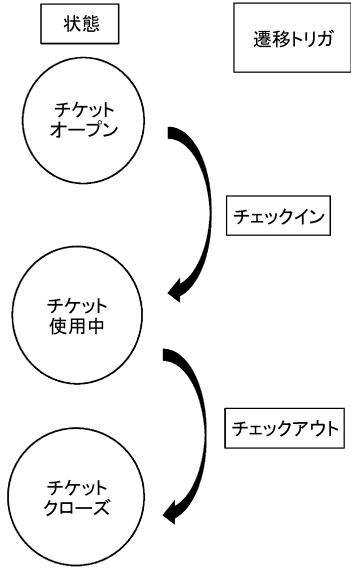
【図 6】



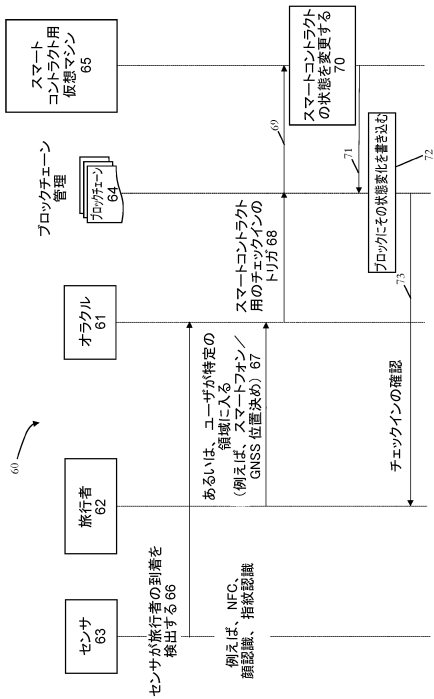
【図 7】



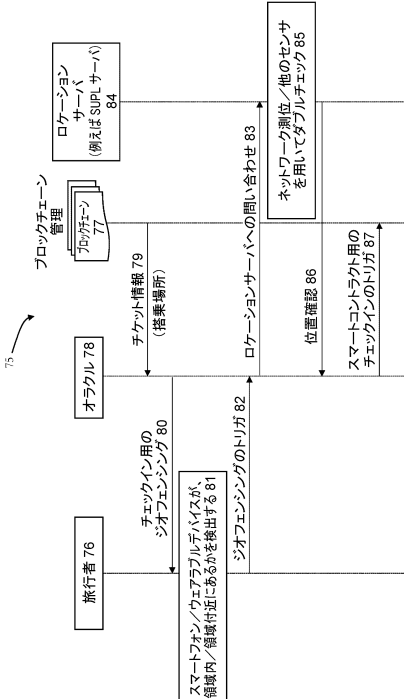
【図 8】



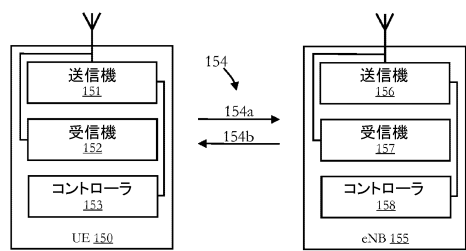
【図 9】



【図 10】



【図 15】



10

20

30

40

50

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2019/084886

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06Q20/22
ADD.

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)

G06Q G07G

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)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	VICTOR FRIEDHELM ET AL: "Geofences on the Blockchain: Enabling Decentralized Location-Based Services", 2018 IEEE INTERNATIONAL CONFERENCE ON DATA MINING WORKSHOPS (ICDMW), IEEE, 17 November 2018 (2018-11-17), pages 97-104, XP033516118, DOI: 10.1109/ICDMW.2018.00021 [retrieved on 2019-02-07] the whole document ----- -/--	1-64

☒ Further documents are listed in the continuation of Box C.

☐ 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

"Z" document member of the same patent family

Date of the actual completion of the international search

11 March 2020

Date of mailing of the international search report

20/03/2020

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Moynihan, Maurice

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2019/084886

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Vitalik Buterin: "FACTS & FIGURES 2009, RECURRING FEATURE;2010 SRI C8052-13.410.1", 1 January 2010 (2010-01-01), XP055491222, Retrieved from the Internet: URL:https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf [retrieved on 2020-03-09] the whole document	1,11,22, 26-28, 38,52,54
A	----- Tony Sabetti: "Secure Technology Alliance 2017 A SECURE TECHNOLOGY ALLIANCE MOBILE COUNCIL WHITE PAPER Mobile Identity Authentication", 31 March 2017 (2017-03-31), XP055675492, Retrieved from the Internet: URL:https://www.securetechalliance.org/wp-content/uploads/Mobile-Identity-Authentication-WP-FINAL-March-2017.pdf [retrieved on 2020-03-10] the whole document -----	1,13,14, 16,43, 44,46, 63,64

フロントページの続き

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,N
E,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,K
G,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,N
I,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,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(特許庁注：以下のものは登録商標)

1. J A V A S C R I P T

2. 3 G P P

ャー アールジー 2 2 4 エスビー ビアブルズ ジェイズ クローズ アイピー ヨーロッパ ソニー
ヨーロッパ リミテッド内