

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6871393号
(P6871393)

(45) 発行日 令和3年5月12日(2021.5.12)

(24) 登録日 令和3年4月19日(2021.4.19)

(51) Int.Cl.		F I			
HO4L	9/32	(2006.01)	HO4L	9/00	675Z
GO6F	21/62	(2013.01)	GO6F	21/62	309
GO6F	21/60	(2013.01)	GO6F	21/60	320
GO6F	21/31	(2013.01)	GO6F	21/31	

請求項の数 14 (全 29 頁)

(21) 出願番号	特願2019-538134 (P2019-538134)	(73) 特許権者	520015461
(86) (22) 出願日	平成30年7月13日 (2018.7.13)		アドバンスド ニュー テクノロジーズ
(65) 公表番号	特表2020-510329 (P2020-510329A)		カンパニー リミテッド
(43) 公表日	令和2年4月2日 (2020.4.2)		英国領ケイマン諸島 グランド ケイマン
(86) 国際出願番号	PCT/US2018/042064		ケーワイ1-9008 ジョージ タウ
(87) 国際公開番号	W02019/014577		ン ホスピタル ロード 27 ケイマン
(87) 国際公開日	平成31年1月17日 (2019.1.17)		コーポレート センター
審査請求日	令和1年9月11日 (2019.9.11)	(74) 代理人	100188558
(31) 優先権主張番号	201710574655.3		弁理士 飯田 雅人
(32) 優先日	平成29年7月14日 (2017.7.14)	(74) 代理人	100205785
(33) 優先権主張国・地域又は機関	中国 (CN)		弁理士 ▲高▼橋 史生
早期審査対象出願			

最終頁に続く

(54) 【発明の名称】 ログイン情報処理の方法およびデバイス

(57) 【特許請求の範囲】

【請求項1】

情報処理デバイスによってログイン情報を処理するための方法であって、
ユーザデバイスが送ったログイン情報記憶要求を受信するステップであって、前記ログイン情報記憶要求が識別子を含む、ステップ(101)と、

前記ユーザデバイスに関連付けられたユーザに対応するログイン情報を判定するステップ(103)と、

ログイン情報処理のために使用される、所定のスマートコントラクトテンプレートに基づいて、前記ログイン情報を含むスマートコントラクトを作成するステップであって、ログイン情報処理のために使用される処理論理が、前記所定のスマートコントラクトテンプレート内に記録される、ステップ(105)と、

前記識別子に基づいて、前記作成されたスマートコントラクトをブロックチェーンネットワークにおいて記憶するステップ(107)と、

前記ユーザデバイスが送った、前記識別子を含むログイン情報クエリ要求を受信するステップ(109、202)と、

前記識別子に基づいて、ログイン情報処理のために使用される、少なくとも1つのスマートコントラクトを前記ブロックチェーンネットワークから読み取るステップ(111、608)と、

前記ユーザに対応する前記作成されたスマートコントラクトを前記少なくとも1つのスマートコントラクトから判定するステップ(608)と、

前記ユーザに対応する前記ログイン情報を取得するために前記作成されたスマートコントラクトを実行するステップ(113)と、

前記ユーザデバイスに前記ユーザに対応する前記取得されたログイン情報を送るステップ(610)とを含む、方法。

【請求項2】

前記識別子に基づいて、ログイン情報処理のために使用される、前記少なくとも1つのスマートコントラクトを前記ブロックチェーンネットワークから前記読み取るステップが、

前記識別子に基づいて、ログイン情報処理のために使用される前記少なくとも1つのスマートコントラクトの記憶アドレスを判定するステップ(604)と、

前記記憶アドレスに基づいて、前記少なくとも1つのスマートコントラクトを前記ブロックチェーンネットワークから読み取るステップ(608)とを含む、請求項1に記載の方法。

【請求項3】

前記識別子に基づいて、ログイン情報処理のために使用される前記少なくとも1つのスマートコントラクトの前記記憶アドレスを前記判定するステップが、

秘密-公開鍵対を取得するために前記識別子処理するステップと、

前記秘密-公開鍵対内に含まれた公開鍵に基づく計算によって第1のアドレスを取得するステップと、

前記第1のアドレスに基づいて、前記第1のアドレスと取引を行っている、少なくとも1つの第2のアドレスを判定するステップと、

前記第2のアドレスから前記少なくとも1つのスマートコントラクトの前記記憶アドレスを識別するステップと

を含む、請求項2に記載の方法。

【請求項4】

前記ログイン情報が、前記ユーザがインターネットサービスプラットフォームにログインするためであり、

前記ログイン情報記憶要求が、前記インターネットサービスプラットフォームの識別情報である識別情報を含み、

前記スマートコントラクトを前記作成するステップが、前記スマートコントラクトに前記識別情報を含めるステップを含む、請求項1から3のいずれか一項に記載の方法。

【請求項5】

前記ユーザに対応する前記作成されたスマートコントラクトを前記判定するステップが、

1つのスマートコントラクトが前記ブロックチェーンネットワークから読み取られた場合、前記スマートコントラクトが前記ユーザに対応する前記作成されたスマートコントラクトであると判定されるステップと、

2つ以上のスマートコントラクトが前記ブロックチェーンネットワークから読み取られた場合、指定された条件を満たすスマートコントラクトを前記少なくとも1つのスマートコントラクトから選択するステップと

を含む、請求項1から4のいずれか一項に記載の方法。

【請求項6】

前記指定された条件を満たすスマートコントラクトを前記少なくとも1つのスマートコントラクトから前記選択するステップが、

前記ログイン情報クエリ要求内に含まれた識別情報と同じ識別情報を有するスマートコントラクトを前記少なくとも1つのスマートコントラクト内に含まれた識別子から選択するステップ

を含む、請求項5に記載の方法。

【請求項7】

10

20

30

40

50

前記ユーザに対応する前記ログイン情報を取得するために前記ユーザに対応する前記作成されたスマートコントラクトを前記実行するステップが、

少なくとも1つのログイン情報を取得するために前記ユーザに対応する前記作成されたスマートコントラクトを実行するステップ(113、305、610)と、

前記ユーザが前記ユーザに対応する前記ログイン情報を確認するために、前記少なくとも1つのログイン情報を前記ユーザデバイスにフィードバックするステップ(610)とを含む、請求項1から6のいずれか一項に記載の方法。

【請求項8】

前記ユーザに対応する前記ログイン情報を取得するために前記ユーザに対応する前記作成されたスマートコントラクトを前記実行するステップが、

暗号化されたログイン情報を取得するために前記ユーザに対応する前記作成されたスマートコントラクトを実行するステップと、

前記ユーザに対応する前記ログイン情報を取得するために、前記暗号化されたログイン情報を解読するステップと

を含む、請求項1に記載の方法。

【請求項9】

前記暗号化されたログイン情報を前記解読するステップが、

秘密-公開鍵対を取得するために前記識別子処理するステップと、

前記秘密-公開鍵対内の秘密鍵を使用することによって、前記暗号化されたログイン情報を解読するステップと

を含む、請求項8に記載の方法。

【請求項10】

前記ユーザに対応する前記ログイン情報が取得された後、前記方法が、

受信された処理要求に基づいて前記ユーザに対応する前記ログイン情報を処理するステップ

をさらに含む、請求項1から9のいずれか一項に記載の方法。

【請求項11】

前記受信された処理要求に基づいて前記ユーザに対応する前記ログイン情報を前記処理するステップが、

前記受信された処理要求が更新要求である場合、前記ユーザに対応する前記ログイン情報を更新し、前記更新されたログイン情報を前記ブロックチェーンネットワークにおいて記憶するステップ

を含む、請求項10に記載の方法。

【請求項12】

前記受信された処理要求に基づいて前記ユーザに対応する前記ログイン情報を前記処理するステップが、

前記受信された処理要求が削除要求である場合、前記ユーザに対応する前記ログイン情報を前記ブロックチェーンネットワークから削除するステップ

を含む、請求項10に記載の方法。

【請求項13】

前記ユーザに対応する前記作成されたスマートコントラクトを記憶するステップが、

前記作成されたスマートコントラクトの記憶アドレスを判定するステップ

を含み、前記記憶アドレスを前記判定するステップが、

秘密-公開鍵対を取得するために前記識別子処理するステップと、

前記秘密-公開鍵対内の公開鍵に基づいて、第1のアドレスを取得するステップであって、前記第1のアドレスが、アルゴリズムに基づいて前記公開鍵を計算することによって取得される、ステップと、

前記第1のアドレスに基づいて第2のアドレスを取得するステップであって、前記第2のアドレスが、前記第1のアドレスにおいて開始した、指定された取引イベントに基づいて前記ブロックチェーンネットワークによって判定される、ステップと、

10

20

30

40

50

前記第2のアドレスが、前記ブロックチェーンネットワーク内の前記作成されたスマートコントラクトの前記判定された記憶アドレスであると判定するステップと、

前記作成されたスマートコントラクトを前記ブロックチェーンネットワーク内の前記判定された記憶アドレスに記憶するステップと
を含み、

前記少なくとも1つのスマートコントラクトを前記ブロックチェーンネットワークから前記読み取るステップが、

前記秘密-公開鍵対を取得するために前記識別子処理するステップと、

前記秘密-公開鍵対内の前記公開鍵に基づいて前記第1のアドレスを取得するステップであって、前記第1のアドレスが、前記アルゴリズムに基づいて前記公開鍵を計算することによって取得される、ステップと、

10

前記第1のアドレスに基づいて、少なくとも1つの第2のアドレスを判定するステップであって、前記少なくとも1つの第2のアドレスの各々が、前記第1のアドレスと取引を実行する、ステップと、

前記作成されたスマートコントラクトの前記判定された記憶アドレスを前記少なくとも1つの第2のアドレスから識別するステップと、

前記少なくとも1つのスマートコントラクトを前記判定された記憶アドレスから読み取るステップと

を含む、請求項1に記載の方法。

【請求項14】

20

ログイン情報を処理するためのデバイスであって、

前記デバイスが、情報処理デバイスの複数のモジュールを備え、

前記複数のモジュールが、請求項1から13のいずれか一項に記載の方法を実行するように構成される、デバイス。

【発明の詳細な説明】

【技術分野】

【0001】

関連出願の相互参照

本出願は、参照によりその全体が本明細書に組み込まれている、2017年7月14日に出願した中国特許出願第201710574655.3号の優先権を主張するものである。

30

【0002】

本出願は、ブロックチェーン技術の分野に関し、詳細には、ログイン情報処理の方法およびデバイスに関する。

【背景技術】

【0003】

インターネット技術の発展に伴い、インターネットサービスプラットフォームを使用することによって、多様なネットワークサービスをユーザに提供することができる。インターネットサービスプラットフォームに対応するサーバが様々なネットワークサービスをユーザに提供する前に、ユーザが提供したログイン情報を使用することによってユーザ識別情報が検証され得るように、ユーザはログイン情報(たとえば、サーバに登録したユーザ名およびパスワード)を提出する必要がある。したがって、識別情報が検証されるとき、サーバは、ネットワークサービスをユーザに提供することができ、したがって、提供されるネットワークサービスのセキュリティが保証される。

40

【0004】

しかしながら、ネットワークサービスをユーザに提供することができるインターネットサービスプラットフォーム数の急増に伴い、ログイン情報のセキュリティを保証するために、ユーザが異なるインターネットサービスプラットフォームに登録することができるログイン情報は、同じであるかまたは異なる場合があり、ユーザがログイン情報を維持するのに不都合をもたらす。

【0005】

50

現在、ログイン情報処理方法が提供されている。具体的には、異なるログイン情報は、インターネットサーバプラットフォームに対応するサーバと協働する第三者サーバ上に記憶される。ユーザがログイン情報を使用する必要があるとき、ユーザは、必要なログイン情報を第三者サーバから取得することができる。

【0006】

しかしながら、業界は、ログイン情報セキュリティを改善し得るログイン情報処理方法を必要とする。

【発明の概要】

【課題を解決するための手段】

【0007】

本明細書の実装形態は、ログイン情報セキュリティを改善するためのログイン情報処理の方法およびデバイスを提供する。

【0008】

本明細書の実装形態では、以下の技術的解決策が使用される。

【0009】

本明細書の一実装形態はログイン情報処理方法を提供し、ログイン情報処理方法は、ユーザが送った、識別子を含むログイン情報クエリ要求を受信するステップと、識別子に基づいて、ログイン情報処理のために使用されるスマートコントラクトをブロックチェーンネットワークから読み取るステップと、ユーザに対応するログイン情報を取得するためにスマートコントラクトを実行するステップとを含む。

【0010】

本明細書の一実装形態は、ログイン情報処理方法をさらに提供し、ログイン情報処理方法は、ユーザが送ったログイン情報記憶要求を受信するステップであって、ログイン情報記憶要求が識別子を含む、受信するステップと、ユーザに対応するログイン情報を判定するステップと、ログイン情報処理のために使用される、所定のスマートコントラクトテンプレートに基づいて、ログイン情報を含むスマートコントラクトを作成するステップと、識別子に基づいて、作成されたスマートコントラクトをブロックチェーンネットワークにおいて記憶するステップとを含む。

【0011】

本明細書の一実装形態は、ログイン情報処理デバイスをさらに提供し、ログイン情報処理デバイスは、ユーザが送った、識別子を含むログイン情報クエリ要求を受信するように構成された受信モジュールと、識別子に基づいて、ログイン情報処理のために使用されるスマートコントラクトをブロックチェーンネットワークから読み取るように構成された読取りモジュールと、ユーザに対応するログイン情報を取得するためにスマートコントラクトを実行するように構成された処理モジュールとを含む。

【0012】

本明細書の一実装形態は、ログイン情報処理デバイスをさらに提供し、ログイン情報処理デバイスは、ユーザが送ったログイン情報記憶要求を受信するように構成された受信モジュールであって、ログイン情報記憶要求が識別子を含む、受信モジュールと、ユーザに対応するログイン情報を判定するように構成された判定モジュールと、ログイン情報処理のために使用される、所定のスマートコントラクトテンプレートに基づいて、ログイン情報を含むスマートコントラクトを作成するように構成された作成モジュールと、識別子に基づいて、作成されたスマートコントラクトをブロックチェーンネットワークにおいて記憶するように構成された記憶モジュールとを含む。

【0013】

本明細書の一実装形態は、ログイン情報処理デバイスをさらに提供し、ログイン情報処理デバイスは、少なくとも1つのプロセッサとメモリとを含み、メモリはプログラムを記憶し、少なくとも1つのプロセッサは、次のステップ、すなわち、ユーザが送った、識別子を含むログイン情報クエリ要求を受信するステップと、識別子に基づいて、ログイン情報処理のために使用されるスマートコントラクトをブロックチェーンネットワークから読

10

20

30

40

50

み取るステップと、ユーザに対応するログイン情報を取得するためにスマートコントラクトを実行するステップとを実行するように構成される。

【0014】

本明細書の一実装形態は、ログイン情報処理デバイスをさらに提供し、ログイン情報処理デバイスは、少なくとも1つのプロセッサとメモリとを含み、メモリはプログラムを記憶し、少なくとも1つのプロセッサは、次のステップ、すなわち、ユーザが送ったログイン情報記憶要求を受信するステップであって、ログイン情報記憶要求が識別子を含む、受信するステップと、ユーザに対応するログイン情報を判定するステップと、ログイン情報処理のために使用される、所定のスマートコントラクトテンプレートに基づいて、ログイン情報を含むスマートコントラクトを作成するステップと、識別子に基づいて、作成されたスマートコントラクトをブロックチェーンネットワークにおいて記憶するステップとを実行するように構成される。

10

【0015】

本明細書の実装形態で使用される、少なくとも1つの技術的解決策は、以下の有益な効果を達成し得る。

【0016】

本明細書のこれらの実装形態では、所定のスマートコントラクトテンプレートに基づいて、一定のユーザのログイン情報を含むスマートコントラクトを作成することができ、スマートコントラクトはブロックチェーンネットワークにおいて記憶され、その結果、ユーザのログイン情報の記憶セキュリティが効果的に改善される。少なくとも1つの技術的解決策は、ブロックチェーンネットワークに基づいて実装され、その結果、ログイン情報が失われる、盗まれる、または改ざんされる可能性は低く、ログイン情報の記憶セキュリティが改善される。加えて、ユーザがログイン情報を必要とするとき、ユーザは、クエリによって、必要なログイン情報をブロックチェーンネットワークから迅速に取得することができ、ユーザがログイン情報を維持するのを便利にする。

20

【0017】

ここで添付の図面は、本出願のさらなる理解をもたらすために使用され、本出願の一部をなす。本出願の例示的な実装形態およびこれらの実装形態の説明は、本出願を説明するために使用され、本出願に対する不適切な限定ではない。添付の図面において：

【図面の簡単な説明】

30

【0018】

【図1】本明細書の一実装形態による、ログイン情報処理方法を示すフローチャートである。

【図2】本明細書の一実装形態による、ログイン情報処理方法を示すフローチャートである。

【図3】本明細書の一実装形態による、ログイン情報処理方法を示すフローチャートである。

【図4】本明細書の一実装形態による、ログイン情報処理デバイスを示す構造図である。

【図5】本明細書の一実装形態による、ログイン情報処理デバイスを示す構造図である。

【図6】本開示の一実装形態による、ログイン情報データを処理するためのコンピュータ実装方法の一例を示すフローチャートである。

40

【発明を実施するための形態】

【0019】

既存の技術で提供される技術的解決策に基づいて、ログイン情報は第三者サーバ上に記憶される。しかしながら、第三者サーバは多くのユーザのログイン情報を記憶するため、第三者サーバ上に記憶されたログイン情報が漏洩し、ユーザのログイン情報セキュリティを低減させるリスクが存在する。

【0020】

ユーザのログイン情報セキュリティを改善するために、本明細書の実装形態はログイン情報処理方法を提供する。ログイン情報処理方法は、情報処理デバイスによって実行され

50

得る。情報処理デバイスは、ユーザのログイン情報をブロックチェーンネットワークにおいて記憶し、ユーザのログイン情報セキュリティは、ブロックチェーンネットワークの改ざん防止および信頼性に依拠して改善される。

【0021】

図1は、本明細書の一実装形態による、ログイン情報処理方法を示すフローチャートである。ログイン情報処理方法は、以下のステップを含む：

【0022】

ステップ101:情報処理デバイスは、ユーザが送った、識別情報を含むログイン情報記憶要求を受信する。

【0023】

ステップ103:情報処理デバイスは、ログイン情報記憶要求に基づいて、ユーザのログイン情報を判定する。

【0024】

ステップ105:ユーザのログイン情報を取得した後、情報処理デバイスは、ユーザのログイン情報を含むスマートコントラクトを作成する。

【0025】

ステップ107:情報処理デバイスは、識別子に基づいて、スマートコントラクトをブロックチェーンネットワークにおいて記憶する。

【0026】

ステップ109:情報処理デバイスは、ユーザが送った、識別子を含むログイン情報クエリ要求を受信する。

【0027】

ステップ111:情報処理デバイスは、識別子に基づいて、ユーザに対応するスマートコントラクトをブロックチェーンネットワークから読み取る。

【0028】

ステップ113:情報処理デバイスは、ユーザに対応するログイン情報を取得するために、ブロックチェーンネットワーク内でスマートコントラクトを実行する。

【0029】

本明細書の実装形態のログイン情報処理方法に基づいて、ログイン情報はブロックチェーンネットワークにおいて記憶され、ログイン情報が、ブロックチェーンネットワークから問い合わせられ、取得され得る。ブロックチェーンネットワークは、ブロックチェーン技術に基づいて構築される。分散型台帳技術(distributed account book technology)と呼ばれるブロックチェーン技術は、分散化、透明性、改ざん防止、および信頼性によって特徴づけられる分散型インターネットデータベース技術である。したがって、ログイン情報が、失われ、盗まれ、または改ざんされる可能性は低く、ログイン情報の記憶およびクエリセキュリティが改善される。

【0030】

本出願の目的、技術的解決策、および利点を明瞭にするために、以下は、本出願の特定の実装形態および対応する添付の図面を参照しながら、本出願の技術的解決策について明瞭かつ包括的に説明する。明らかに、説明する実装形態は、本明細書のいくつかの実装形態に過ぎず、本明細書の実装形態のすべてではない。創造的な取組みなしに本出願の実装形態に基づいて当業者が取得するすべての他の実装形態は、本出願の保護範囲内に入る。

【0031】

本明細書の実装形態において提供される技術的解決策について、添付の図面を参照しながら下記で説明する。

【0032】

図2は、本明細書の一実装形態による、ログイン情報処理方法を示すフローチャートである。この方法は、次のように示される。本解決策は、ログイン情報を処理することが可能なアプリケーションクライアント(下記でクライアントと呼ばれる)、もしくはブラウザ内で実行するプラグイン、またはサーバによって実行され得る。実行主体の一実装形態の

10

20

30

40

50

形式は、本明細書の実装形態において限定されない。

【0033】

クライアントは、本明細書の実装形態に記録される技術的解決策を実装することができるアプリケーションクライアントであり、端末デバイス上でAPPとして実行し得る。

【0034】

ステップ202:ユーザが送ったログイン情報記憶要求を受信する、ログイン情報記憶要求は識別子を含む。

【0035】

実際の適用例では、ユーザが一定のインターネットサービスプラットフォームによって提供されるネットワークサービスを必要とするとき、ユーザは、通常、インターネットサービスプラットフォームにログインする必要がある。ユーザがインターネットサービスプラットフォームに初めてログインするとき、ユーザは、インターネットサービスプラットフォームに登録して、インターネットサービスプラットフォームにログインするためにユーザが使用するログイン情報を生成する必要がある。

10

【0036】

ユーザがインターネットサービスプラットフォームに後でログインするのを便利にするために、ユーザは、情報処理デバイスがユーザのログイン情報を処理するように(ここで、処理は、記憶、クエリなどを含み得る)、ログイン情報を取得した後、ログイン情報記憶要求を情報処理デバイスに送ることができる。情報処理デバイスは、ログイン情報処理デバイスであってよく、またはログイン情報処理能力および他の能力をやはり有する情報処理デバイスであってよい。

20

【0037】

本明細書の実装形態に記録される識別子は、識別子が受信された後でもユーザが容易に思い出す情報、識別され得る識別子を提供するユーザのログイン情報と理解され得る。ここで、識別子は、限定はしないが、パスワード、画像、文字列、2次元コードなどであってよい。識別子がパスワードである場合、パスワードは、数字、漢字、文字、またはシンボルのうちの1つまたは複数から構成され得る。

【0038】

加えて、本明細書の実装形態に記録される識別子は、ここで限定はしないが、ユーザによって設定されてよいか、またはユーザ用の情報処理デバイスまたはインターネットサービスプラットフォームによって設定されてもよい。

30

【0039】

ステップ204:ユーザに対応するログイン情報を判定する。

【0040】

本明細書の実装形態では、ユーザに対応するログイン情報は、ここで限定はしないが、ユーザによって設定されてよいか、またはユーザ用の情報処理デバイスによって自動的に生成されてもよい。

【0041】

ユーザに対応するログイン情報がユーザによって設定された場合、ユーザに対応するログイン情報を判定するステップは、ログイン情報記憶要求内に含まれたログイン情報をユーザに対応するログイン情報と判定するステップを含む。

40

【0042】

ログイン情報記憶要求がログイン情報を含まない場合、情報処理デバイスが、ユーザが送ったログイン情報記憶要求を受信した後、ユーザに対応するログイン情報を判定するステップは、ユーザに関するログイン情報を生成するステップと、生成されたログイン情報をユーザに対応するログイン情報と判定するステップとを含む。

【0043】

情報処理デバイスは、ログイン情報が容易に分解され得ず、高いセキュリティを有するように、異なるユーザに関するログイン情報をランダムかつ不規則に生成する。

【0044】

50

本明細書の実装形態に記録されるログイン情報は、ユーザまたは情報処理デバイスによって設定されたユーザ名およびログインパスワードを含んでよいが、またはユーザまたは情報処理デバイスが設定したログインパスワードのみを含んでもよい。ログイン情報がログインパスワードのみを含む場合、ユーザ名は、通常、ユーザによって設定される。

【0045】

ステップ206:ログイン情報処理のために使用される、所定のスマートコントラクトテンプレートに基づいて、ログイン情報を含むスマートコントラクトを作成する。

【0046】

本明細書の実装形態では、情報処理デバイスは、ログイン情報処理のために使用されるスマートコントラクトテンプレートを事前生成する。ログイン情報処理のために使用される処理論理は、スマートコントラクトテンプレート上に記憶される。具体的には、ログイン情報は、処理論理を実行することによって処理され得る。

10

【0047】

たとえば、ログイン情報を処理するための論理は、ログイン情報を記憶するための論理を含み得る。ログイン情報は、記憶論理に基づいて、ブロックチェーンネットワークにおいて記憶され得る。

【0048】

別の例の場合、ログイン情報を処理するための論理は、ログイン情報を問い合わせるための論理を含み得る。ログイン情報は、クエリ論理に基づいて、ブロックチェーンネットワークから問い合わせられてよい。

20

【0049】

さらに別の例の場合、ログイン情報を処理するための論理は、ログイン情報を更新または削除するための論理を含み得る。記憶されたログイン情報は、更新論理に基づいて更新され得、記憶されたログイン情報は、削除論理に基づいて削除され得る。

【0050】

特に、更新および削除は、ここで、ブロックチェーンネットワーク内の更新に関するサービスデータの生成(具体的には、更新されることになるログイン情報と更新されたログイン情報の両方がブロックチェーンネットワークにおいて記憶される)、および削除に関するサービスデータの生成と理解され得る。

【0051】

30

本明細書の実装形態では、ログイン情報処理のために使用される、所定のスマートコントラクトテンプレートは、情報処理デバイス上に記憶されてよいが、またはブロックチェーンネットワークにおいて記憶されてもよく、ここでは限定されない。

【0052】

スマートコントラクトテンプレートが情報処理デバイス上に記憶された場合、ユーザに対応するログイン情報を判定した後、情報処理デバイスは、スマートコントラクトテンプレートを起動させ、ユーザに対応するログイン情報を含むスマートコントラクトを作成する。スマートコントラクトテンプレートがブロックチェーンネットワークにおいて記憶される場合(具体的には、情報処理デバイスは、ブロックチェーンネットワークと折衝することによって、ブロックチェーンネットワーク内にスマートコントラクトテンプレートを作成する。言い換えれば、ブロックチェーンネットワークは、固定記憶アドレスをスマートコントラクトテンプレートに割り振り、固定記憶アドレスに基づいて、スマートコントラクトテンプレートをブロックチェーンネットワークにおいて記憶し、情報処理デバイスは、固定記憶アドレスに基づいて、スマートコントラクトテンプレートを取得することができる)、ユーザに対応するログイン情報を判定した後、情報処理デバイスは、ブロックチェーンネットワークからスマートコントラクトテンプレートを起動させ、ユーザに対応するログイン情報を含むスマートコントラクトを作成する。

40

【0053】

ログイン情報セキュリティを改善するために、暗号化されたログイン情報に基づいてスマートコントラクトを作成することができる。本明細書の実装形態では、ログイン情報を

50

含むスマートコントラクトを作成するステップは、秘密-公開鍵対を取得するために識別子を処理するステップと、秘密-公開鍵対内の公開鍵を使用することによって、ログイン情報を暗号化するステップと、ログイン情報処理のために使用される、所定のスマートコントラクトテンプレートに基づいて、暗号化されたログイン情報を含むスマートコントラクトを作成するステップとを含み得る。

【0054】

秘密-公開鍵対を取得するために識別子を処理するステップは、変換規則に基づいて、識別子をバイトコードに変換するステップ、たとえば、バイナリコードをバイトコードとして選択するステップと、計算論理に基づいて、バイトコードを使用することによって秘密-公開鍵対を生成するステップであって、秘密-公開鍵対が公開鍵および秘密鍵によって形成され、公開鍵がログイン情報を暗号化するために使用され、秘密鍵が暗号化されたログイン情報を解読するために使用され得る、生成するステップとを含み得る。

10

【0055】

スマートコントラクトがログイン情報に対して作成されるとき、ログイン情報記憶要求が識別情報を含む場合、識別情報とログイン情報とを含むスマートコントラクトが作成される。

【0056】

識別情報は、ここで、インターネットサービスプラットフォームの識別情報と理解され得る。

【0057】

ステップ208:識別子に基づいて、作成されたスマートコントラクトをブロックチェーンネットワークにおいて記憶する。

20

【0058】

本明細書の本実装形態では、識別子に基づいて、作成されたスマートコントラクトをブロックチェーンネットワークにおいて記憶するステップは、識別子に基づいて、ブロックチェーンネットワーク内のスマートコントラクトの記憶アドレスを判定するステップと、記憶アドレスに基づいて、スマートコントラクトをブロックチェーンネットワークにおいて記憶するステップとを含む。

【0059】

本明細書の本実装形態では、識別子に基づいて、ブロックチェーンネットワーク内のスマートコントラクトの記憶アドレスを判定するステップは、秘密-公開鍵対を取得するために識別子を処理するステップと、秘密-公開鍵対内に含まれた公開鍵に基づく計算によって第1のアドレスを取得するステップと、第1のアドレスに基づいて第2のアドレスを取得するステップであって、第2のアドレスが、第1のアドレスにおいて開始した、指定された取引イベントに基づいて、ブロックチェーンネットワーク内で判定される、取得するステップと、第2のアドレスをブロックチェーンネットワーク内のスマートコントラクトの記憶アドレスと判定するステップとを含む。

30

【0060】

本明細書の本実装形態に記録される、指定された取引イベントは、取引と理解され得る。たとえば、Ethereumネットワークにおいて、スマートコントラクトの記憶アドレスを取得するためには、特定の数量のEtherをEthereumネットワークに支払う必要がある。具体的には、Ethereumネットワーク内で取引が生成されるとき、取引のソースアドレスは第1のアドレスであり得、取引の宛先アドレスは第2のアドレスと呼ばれることがある(ここで、第2のアドレスはEthereumネットワーク内で割り振られ得る)。第1のアドレスと第2のアドレスとの間の取引が完了すると、第2のアドレスに対応する記憶スペースを使用して、ユーザのために作成されたスマートコントラクトを記憶することができる。この状況では、第2のアドレスは、スマートコントラクトの記憶アドレスと呼ばれることもある。

40

【0061】

ステップ206の秘密-公開鍵対を取得するための識別子の処理を参照されたい。詳細については、ここで説明しない。秘密-公開鍵対内に含まれた公開鍵に基づく計算によって第1

50

のアドレスを取得するステップは、第1のアドレスを取得するために、指定されたアルゴリズムに基づいて、秘密-公開鍵対内に含まれた公開鍵を計算するステップを含み、このステップは、固定長のハッシュ値を取得するために、ハッシュアルゴリズムに基づいて公開鍵を計算するステップであって、ハッシュ値が第1のアドレスである、計算するステップを含む。

【0062】

本明細書の本実装形態で提供されるログイン情報処理方法に基づいて、一定のユーザのログイン情報を含むスマートコントラクトを作成することができ、スマートコントラクトはブロックチェーンネットワークにおいて記憶され、その結果、ユーザのログイン情報の記憶セキュリティが効果的に改善される。これは、ブロックチェーンネットワークに基づいて実装され、その結果、ログイン情報が失われる、盗まれる、または改ざんされる可能性は低く、ログイン情報の記憶セキュリティが改善される。

10

【0063】

図3は、本明細書の一実装形態による、ログイン情報処理方法を示すフローチャートである。この方法は、次のように示される。本解決策は、ログイン情報処理能力を備えたアプリケーションクライアント(下記で、クライアントと呼ばれる)、もしくはブラウザ内で実行するプラグイン、またはサーバによって実行され得る。実行主体の一実装形態の形式は、本明細書の実装形態において限定されない。

【0064】

ステップ301:ユーザが送った、識別子を含むログイン情報クエリ要求を受信する。

20

【0065】

本明細書の本実装形態では、インターネットサービスプラットフォームにログインするとき、ユーザは、必要なログイン情報を取得するために、ログイン情報クエリ要求を情報処理デバイスに送ることができる。ユーザがログイン情報を必要とするとき、ユーザは、必要なログイン情報を取得するために、ログイン情報クエリ要求を情報処理デバイスに送ることができる。ユーザがログイン情報クエリ要求を送る使用シナリオは、ここで限定されない。

【0066】

識別子の内容に関しては、説明した実装形態に記録される関連内容を参照されたい。ここでは詳細について説明しない。

30

【0067】

ステップ303:識別子に基づいて、ログイン情報処理のために使用されるスマートコントラクトをブロックチェーンネットワークから読み取る。

【0068】

本明細書の本実装形態では、ログイン情報処理のために使用されるスマートコントラクトの記憶アドレスが、まず識別子に基づいて判定される。

【0069】

秘密-公開鍵対を取得するために識別子処理する。第1のアドレスは、秘密-公開鍵対内に含まれた公開鍵に基づく計算によって取得される。第1のアドレスに基づいて、第1のアドレスと取引を行っている、少なくとも1つの第2のアドレスが判定される。第2のアドレスからスマートコントラクトの記憶アドレスが識別される。

40

【0070】

本明細書の本実装形態では、秘密-公開鍵対を取得するための識別子の処理に関しては、ステップ208内の内容を参照されたい。ここでは詳細について説明しない。

【0071】

秘密-公開鍵対内に含まれた公開鍵に基づく計算によって第1のアドレスを取得するステップは、第1のアドレスを取得するために、指定されたアルゴリズムに基づいて、秘密-公開鍵対内に含まれた公開鍵を計算するステップを含む。

【0072】

本明細書の本実装形態では、スマートコントラクトの記憶アドレスは、指定された取引

50

イベントを使用することによって判定され得る。取引イベントが生じた後、取引イベントに対応する取引データがブロックチェーンネットワークにおいて記憶される。したがって、第1のアドレスをクエリキーワードとして使用することができ、第1のアドレスを含む取引データがブロックチェーンネットワーク内で問い合わせられ、少なくとも1つの第2のアドレスが取引データから読み取られる。

【0073】

同じユーザの場合、第1のアドレスはユーザによって提供される識別子に基づいて判定されるため、第1のアドレスを含む1つまたは複数の取引データが存在し得、各取引データは第2のアドレスを含む。したがって、第1のアドレスに基づいて、少なくとも1つの第2のアドレスが判定され得る。

10

【0074】

第2のアドレスからスマートコントラクトの記憶アドレスを識別するステップは、第1のアドレスと取引を行っている1つの第2のアドレスが存在すると判定された場合、第2のアドレスをスマートコントラクトの記憶アドレスと判定するステップ、または第1のアドレスと取引を行っている2つ以上の第2のアドレスが存在すると判定された場合、スマートコントラクトが記憶されている第2のアドレスを検索するステップと、識別された第2のアドレスをスマートコントラクトの記憶アドレスと判定するステップとを含み得る。この状況では、スマートコントラクトの2つ以上の記憶アドレスが存在し得る。

【0075】

次いで、記憶アドレスに基づいて、スマートコントラクトがブロックチェーンネットワークから読み取られる。

20

【0076】

1つのスマートコントラクトがブロックチェーンネットワークから読み取られた場合、そのスマートコントラクトはユーザに対応するスマートコントラクトであると判定される。

【0077】

2つ以上のスマートコントラクトがブロックチェーンネットワークから読み取られた場合、指定された条件を満たすスマートコントラクトが読み取られたスマートコントラクトから選択される。

【0078】

本明細書の本実装形態では、指定された条件を満たすスマートコントラクトを読み取られたスマートコントラクトから選択するステップは、読み取られたスマートコントラクト内に含まれた識別情報に基づいて、ログイン情報クエリ要求内に含まれた識別情報と同じ識別情報を有するスマートコントラクトを読み取られたスマートコントラクトから選択するステップを含む。

30

【0079】

ステップ305:ユーザに対応するログイン情報を取得するためにスマートコントラクトを実行する。

【0080】

本明細書の本実装形態では、少なくとも1つのログイン情報を取得するために、スマートコントラクトが実行される。

40

【0081】

ログイン情報がユーザニーズを満たしていることをユーザが確認するように、少なくとも1つのログイン情報がユーザにフィードバックされる。

【0082】

本明細書の本実装形態では、1つまたは複数のログイン情報はスマートコントラクトにおいて記憶され得る。

【0083】

スマートコントラクトを実行することによって1つのログイン情報が取得された場合、ログイン情報がユーザニーズを満たすと判定することができ、ログイン情報はユーザに直

50

接フィードバックされる。

【0084】

スマートコントラクトを実行することによって2つ以上のログイン情報が取得された場合、確認のためにログイン情報をユーザにフィードバックすることができる。

【0085】

代替として、ログイン情報が識別情報を含むとき、ログイン情報クエリ要求内に含まれた識別情報と同じ識別情報を有するログイン情報を選択し、選択されたログイン情報がユーザニーズを満たすと判定するように、各ログイン情報から識別情報がパースされる。

【0086】

スマートコントラクトにおいて記憶されたログイン情報は、非暗号化または暗号化され得る。暗号化されたログイン情報の場合、ユーザに対応するログイン情報を取得するためにスマートコントラクトを実行するステップは、暗号化されたログイン情報を取得するためにスマートコントラクトを実行するステップと、ユーザに対応するログイン情報を取得するために、暗号化されたログイン情報を解読するステップとを含む。

【0087】

暗号化されたログイン情報を解読するステップは、秘密-公開鍵対を取得するために識別子を処理するステップと、秘密-公開鍵対内の秘密鍵を使用することによって、暗号化されたログイン情報を解読するステップとを含む。

【0088】

ステップ206の一実装形態に基づいて、識別子を使用することによって、秘密-公開鍵対が生成され、秘密-公開鍵対内の公開鍵を使用することによって、ログイン情報が暗号化される。本ステップでは、公開鍵を使用することによって暗号化されたログイン情報は、秘密-公開鍵対内の秘密鍵を使用することによって解読され得る。

【0089】

取得されたログイン情報の平文がユーザに送られ、ユーザはログイン情報を使用してログインを完了することができる。

【0090】

本明細書の本実装形態では、ユーザはさらに、ログイン情報処理要求を情報処理デバイスに送ることができる。この状況では、ログイン情報が取得された後、ログイン情報処理方法は、受信された処理要求に基づいてログイン情報を処理するステップと、受信された処理要求が更新要求である場合、ログイン情報を更新し、更新されたログイン情報をブロックチェーンネットワークにおいて記憶するステップ、または受信された処理要求が削除要求である場合、ログイン情報をブロックチェーンネットワークから削除するステップをさらに含む。

【0091】

本明細書の本実装形態で提供されるログイン情報処理方法に基づいて、ユーザがログイン情報を必要とするとき、ユーザは、クエリによって、必要なログイン情報をブロックチェーンネットワークから迅速に取得することができ、ユーザがログイン情報を維持するのを便利にする。

【0092】

図4は、本明細書の一実装形態による、ログイン情報処理デバイスを示す構造図である。ログイン情報処理デバイスは、ユーザが送ったログイン情報クエリ要求を受信するように構成された受信モジュール41であって、要求が識別子を含む、受信モジュール41と、識別子に基づいて、ログイン情報処理のために使用されるスマートコントラクトをブロックチェーンネットワークから読み取るように構成された読取りモジュール42と、ユーザに対応するログイン情報を取得するためにスマートコントラクトを実行するように構成された処理モジュール43とを含む。

【0093】

場合によっては、読取りモジュール42は、識別子に基づいて、ログイン情報を処理するために使用されるスマートコントラクトの記憶アドレスを判定し、記憶アドレスに基づい

10

20

30

40

50

て、スマートコントラクトをブロックチェーンネットワークから読み取るように構成される。

【0094】

場合によっては、読取りモジュール42は、秘密-公開鍵対を取得するために識別子を処理し、秘密-公開鍵対内に含まれた公開鍵に基づく計算によって第1のアドレスを取得し、第1のアドレスに基づいて、第1のアドレスと取引を行っている、少なくとも1つの第2のアドレスを判定し、第2のアドレスからスマートコントラクトの記憶アドレスを識別するように構成される。

【0095】

場合によっては、読取りモジュール42は、第1のアドレスを取得するために、指定されたアルゴリズムに基づいて、秘密-公開鍵対内に含まれた公開鍵を計算するように構成される。

10

【0096】

場合によっては、読取りモジュール42は、2つ以上のスマートコントラクトがブロックチェーンネットワークから読み取られた場合、指定された条件を満たすスマートコントラクトを読み取られたスマートコントラクトから選択するように構成される。

【0097】

場合によっては、読取りモジュール42は、ログイン情報クエリ要求内に含まれた識別情報と同じ識別情報を有するスマートコントラクトを読み取られたスマートコントラクト内に含まれた識別情報から選択するように構成される。

20

【0098】

場合によっては、処理モジュール43は、ユーザに対応する、少なくとも1つのログイン情報を取得するためにスマートコントラクトを実行し、ログイン情報がユーザニーズを満たしていることをユーザが確認するように、少なくとも1つのログイン情報をユーザにフィードバックするように構成される。

【0099】

場合によっては、処理モジュール43は、ユーザに対応する、暗号化されたログイン情報を取得するためにスマートコントラクトを実行し、ユーザに対応するログイン情報を取得するために、暗号化されたログイン情報を解読するように構成される。

【0100】

場合によっては、処理モジュール43は、秘密-公開鍵対を取得するために識別子を処理し、秘密-公開鍵対内の秘密鍵を使用することによって、暗号化されたログイン情報を解読するように構成される。

30

【0101】

場合によっては、ログイン情報を取得した後、処理モジュール43は、受信された処理要求に基づいてログイン情報を処理する。

【0102】

場合によっては、処理モジュール43は、受信された処理要求が更新の要求である場合、ログイン情報を更新し、更新されたログイン情報をブロックチェーンネットワークにおいて記憶するように構成される。

40

【0103】

場合によっては、処理モジュール43は、受信された処理要求が削除の要求である場合、ログイン情報をブロックチェーンネットワークから削除するように構成される。

【0104】

特に、本明細書の本実装形態に記録されるログイン情報処理デバイスは、ここで限定はしないが、ソフトウェアまたはハードウェアによって実装され得る。

【0105】

したがって、ユーザは、ログイン情報処理デバイスを使用することによってブロックチェーンネットワークからログイン情報を問い合わせ、ログイン情報をさらに処理することができる。ログイン情報処理デバイス(短縮して、情報処理デバイスと呼ばれることがあ

50

る)は、単一のログイン情報処理機能を有してよいか、またはログイン情報処理機能に加えて他の情報処理機能を有してもよい。

【0106】

同じ開示概念に基づいて、本明細書の一実装形態は、ログイン情報処理デバイスをさらに提供する。ログイン情報処理デバイスは、少なくとも1つのプロセッサとメモリとを含む。メモリはプログラムを記憶し、少なくとも1つのプロセッサは、次のステップ、すなわち、ユーザが送った、識別子を含むログイン情報クエリ要求を受信するステップと、識別子に基づいて、ログイン情報処理のために使用されるスマートコントラクトをブロックチェーンネットワークから読み取るステップと、ユーザに対応するログイン情報を取得するためにスマートコントラクトを実行するステップとを実行するように構成される。

10

【0107】

プロセッサの別の機能に関しては、上記で説明した実装形態に記録されている内容を参照されたい。ここでは詳細について説明しない。

【0108】

同じ開示概念に基づいて、本明細書の一実装形態は、コンピュータ可読記憶媒体をさらに提供する。コンピュータ可読記憶媒体は、電子デバイスと組み合わせて使用されるプログラムを含み、プロセッサは、次のステップ、すなわち、ユーザが送った、識別子を含むログイン情報クエリ要求を受信するステップと、識別子に基づいて、ログイン情報処理のために使用されるスマートコントラクトをブロックチェーンネットワークから読み取るステップと、ユーザに対応するログイン情報を取得するためにスマートコントラクトを実行するステップとを実行するためにプログラムを実行し得る。

20

【0109】

プロセッサの別の機能に関しては、上記で説明した実装形態に記録されている内容を参照されたい。ここでは詳細について説明しない。

【0110】

したがって、コンピュータ可読記憶媒体は、ブロックチェーンネットワークからログイン情報を問い合わせるための方法のキャリアを提供する。

【0111】

図5は、本明細書の一実装形態による、ログイン情報処理デバイスを示す構造図である。ログイン情報処理デバイスは、ユーザが送ったログイン情報記憶要求を受信することであって、ログイン情報記憶要求が識別子を含む、受信することを行うように構成された受信モジュール51と、ユーザに対応するログイン情報を判定するように構成された判定モジュール52と、ログイン情報処理のために使用される、所定のスマートコントラクトテンプレートに基づいて、ログイン情報を含むスマートコントラクトを作成するように構成された作成モジュール53と、識別子に基づいて、作成されたスマートコントラクトをブロックチェーンネットワークにおいて記憶するように構成された記憶モジュール54とを含む。

30

【0112】

場合によっては、判定モジュール52は、ユーザに関するログイン情報を生成し、生成されたログイン情報をユーザに対応するログイン情報と判定するように構成される。

【0113】

場合によっては、判定モジュール52は、ログイン情報記憶要求内に含まれたログイン情報をユーザに対応するログイン情報と判定するように構成される。

40

【0114】

場合によっては、記憶モジュール54は、識別子に基づいて、ブロックチェーンネットワーク内のスマートコントラクトの記憶アドレスを判定し、記憶アドレスに基づいて、スマートコントラクトをブロックチェーンネットワークにおいて記憶するように構成される。

【0115】

場合によっては、記憶モジュール54は、秘密-公開鍵対を取得するために識別子を処理することと、秘密-公開鍵対内に含まれた公開鍵に基づく計算によって第1のアドレスを取得することと、第1のアドレスに基づいて第2のアドレスを取得することとであって、第2の

50

アドレスが、第1のアドレスにおいて開始した、指定された取引イベントに基づいてブロックチェーンネットワーク内で判定される、取得することと、第2のアドレスをブロックチェーンネットワーク内のスマートコントラクトの記憶アドレスと判定することを行うように構成される。

【0116】

場合によっては、記憶モジュール54は、第1のアドレスを取得するために、指定されたアルゴリズムに基づいて、秘密-公開鍵対内に含まれた公開鍵を計算するように構成される。

【0117】

場合によっては、作成モジュール53は、秘密-公開鍵対を取得するために識別子を処理し、秘密-公開鍵対内の公開鍵を使用することによってログイン情報を暗号化し、ログイン情報処理のために使用される、所定のスマートコントラクトテンプレートに基づいて、暗号化されたログイン情報を含むスマートコントラクトを作成するように構成される。

【0118】

特に、本明細書の本実装形態に記録されるログイン情報処理デバイスは、ここで限定はしないが、ソフトウェアまたはハードウェアを使用することによって実装され得る。

【0119】

したがって、ユーザは、ログイン情報処理デバイスを使用することによって、ログイン情報をブロックチェーンネットワークにおいて記憶することができる。ログイン情報処理デバイスは、単一のログイン情報処理機能を有してよく、またはログイン情報処理機能に加えて、他の情報処理機能を有してもよい。

【0120】

同じ開示概念に基づいて、本明細書の一実装形態は、ログイン情報処理デバイスをさらに提供する。ログイン情報処理デバイスは、少なくとも1つのプロセッサとメモリとを含む。メモリはプログラムを記憶し、少なくとも1つのプロセッサは、次のステップ、すなわち、ユーザが送ったログイン情報記憶要求を受信するステップであって、ログイン情報記憶要求が識別子を含む、受信するステップと、ユーザに対応するログイン情報を判定するステップと、ログイン情報処理のために使用される、所定のスマートコントラクトテンプレートに基づいて、ログイン情報を含むスマートコントラクトを作成するステップと、識別子に基づいて、作成されたスマートコントラクトをブロックチェーンネットワークにおいて記憶するステップとを実行するように構成される。

【0121】

プロセッサの別の機能に関しては、説明した実装形態に記録されている内容を参照されたい。ここでは詳細について説明しない。

【0122】

同じ開示概念に基づいて、本明細書の一実装形態は、コンピュータ可読記憶媒体をさらに提供する。コンピュータ可読記憶媒体は、電子デバイスと組み合わせて使用されるプログラムを含み、プロセッサは、次のステップ、すなわち、ユーザが送ったログイン情報記憶要求を受信するステップであって、ログイン情報記憶要求が識別子を含む、受信するステップと、ユーザに対応するログイン情報を判定するステップと、ログイン情報処理のために使用される、所定のスマートコントラクトテンプレートに基づいて、ログイン情報を含むスマートコントラクトを作成するステップと、識別子に基づいて、作成されたスマートコントラクトをブロックチェーンネットワークにおいて記憶するステップとを実行するためにプログラムを実行し得る。

【0123】

プロセッサの別の機能に関しては、説明した実装形態に記録されている内容を参照されたい。ここでは詳細について説明しない。

【0124】

したがって、ユーザは、ログイン情報処理デバイスまたはコンピュータ可読記憶媒体との対話を通じて、ログイン情報をブロックチェーンネットワークにおいて記憶することが

10

20

30

40

50

できる。

【 0 1 2 5 】

1990年代には、ハードウェアの改善(たとえば、ダイオード、トランジスタ、またはスイッチなどの回路構造に対する改善)とソフトウェアの改善(方法手順に対する改善)との間で技術の改善を明瞭に区別することが可能であった。しかしながら、技術の発展に伴い、多くの方法プロセスの改善は、ハードウェア回路構造の直接的な改善と見なされ得る。設計者はほぼすべて、対応するハードウェア回路構造を取得するために、ハードウェア回路に対して改善された方法をプログラムする。したがって、ハードウェアエンティティモジュールを使用することによって、方法手順の改善を実装することはできないとは言えない。たとえば、プログラマブル論理デバイス(PLD)(たとえば、フィールドプログラマブルゲートアレイ(FPGA))は、そのような集積回路である。プログラマブル論理デバイスの論理機能は、ユーザが実行するコンポーネントプログラミングによって判定される。設計者は、専用の集積回路チップを設計および生産することをチップ製造会社に要求せずに、デジタルシステムを単一のPLD内に「統合する」ために自主的プログラミングを実行する。加えて、集積回路チップを手動で生産する代わりに、プログラミングは、プログラム開発の間に使用されるソフトウェアコンパイラと同様の「論理コンパイラ」ソフトウェアによって主に実装される。コンパイル前の元のコードも、ハードウェア記述言語(HDL)と呼ばれる特定のプログラミング言語で書き込まれ、ABEL(Advanced Boolean Expression Language)、AHDL(Altera Hardware Description Language)、Confluence、CUPL(Cornell University Programming Language)、HDCal、JHDL(Java(登録商標) Hardware Description Language)、Lava、Lola、MyHDL、PALASM、およびRHDL (Ruby Hardware Description Language)など、2つ以上のタイプのHDLが存在する。現在、VHDL(Very-High-Speed Integrated Circuit Hardware Description Language)およびVerilogが最も一般的に使用されている。方法手順は、論理方法プロセスを実装するハードウェア回路が容易に取得され得るように、論理的にプログラムされ、前述のハードウェア記述言語を使用することによって集積回路に対してプログラムされることのみを必要とすることを当業者はやはり理解されたい。

【 0 1 2 6 】

適切な方法を使用することによって、コントローラが実装され得る。たとえば、コントローラは、マイクロプロセッサもしくはプロセッサ、またはコンピュータ可読媒体、論理ゲート、スイッチ、特定用途向け集積回路(ASIC)、プログラマブル論理コントローラ、あるいはマイクロプロセッサまたはプロセッサによって実行され得るコンピュータ可読プログラムコード(ソフトウェアまたはファームウェアなど)を記憶する埋込み式マイクロプロセッサであってよい。コントローラの例は、限定はしないが、次のマイクロプロセッサ、すなわち、ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20、およびSilicone Labs C8051F320を含む。メモリコントローラは、メモリの制御論理の一部として実装されてもよい。コントローラは、純粋なコンピュータ可読プログラムコードの意味で実装されてよく、方法のステップは、コントローラが、論理ゲート、スイッチ、特定用途向け集積回路、プログラマブル論理コントローラ、埋込み式マイクロコントローラなどの形式で同じ機能をさらに実装することを可能にするために論理的にプログラムされ得ることを当業者はやはり理解している。したがって、コントローラは、ハードウェア構成要素と見なされてよく、コントローラ内に含まれ、かつ様々な機能を実装するように構成された装置はやはり、ハードウェア構成要素内の構造と見なされてよい。代替として、様々な機能を実装するように構成された装置は、方法を実装するためのソフトウェアモジュールとハードウェア構成要素内の構造の両方と見なされてよい。

【 0 1 2 7 】

説明した実装形態で説明したシステム、装置、モジュール、またはユニットは、コンピュータチップまたはエンティティによって実装されてよく、または一定の機能を備えた製品によって実装されてもよい。典型的な実装デバイスはコンピュータである。コンピュータは、たとえば、パーソナルコンピュータ、ラップトップコンピュータ、セルラーフォン、カメラフォン、スマートフォン、携帯情報端末、メディアプレイヤー、ナビゲーションデ

10

20

30

40

50

バイス、電子メールデバイス、ゲームコンソール、タブレットコンピュータ、もしくは装着可能デバイス、またはこれらのデバイスのうちのいずれかの組合せであってよい。

【0128】

説明を簡単にするために、説明する装置は、機能を様々なユニットに分割することによって説明される。確かに、本出願が実装される時、これらのユニットの機能は、1つまたは複数のソフトウェアおよび/またはハードウェアの形で実装され得る。

【0129】

本開示の実装形態は、方法、システム、またはコンピュータプログラム製品として提供され得ることを当業者は理解されたい。したがって、本開示は、ハードウェア専用実装形態、ソフトウェア専用実装形態、またはソフトウェアとハードウェアの組合せを用いた実装形態の形式を使用し得る。加えて、本開示は、コンピュータ使用可能プログラムコードを含む、1つまたは複数のコンピュータ使用可能記憶媒体(限定はしないが、ディスクメモリ、CD-ROM、光メモリなど)上で実装されるコンピュータプログラム製品の形式を使用し得る。

【0130】

本開示の実装形態による、方法、デバイス(システム)、およびコンピュータプログラム製品のフローチャートおよび/またはブロック図を参照しながら本開示について説明する。コンピュータプログラム命令を使用して、フローチャートおよび/またはブロック図の各プロセスおよび/または各ブロック、ならびにフローチャートおよび/またはブロック図のプロセスおよび/またはブロックの組合せを実装することができることを理解されたい。これらのコンピュータプログラム命令は、任意の他のプログラマブルデータ処理デバイスのコンピュータまたはプロセッサによって実行される命令がフローチャートの1つまたは複数のプロセスまたはブロック図の1つまたは複数のブロック内の特定の機能を実装するための装置を生成するように、汎用コンピュータ、専用コンピュータ、埋込み式プロセッサ、または機械を生成するための任意の他のプログラマブルデータ処理デバイスのプロセッサに対して提供され得る。

【0131】

これらのコンピュータプログラム命令は、コンピュータ可読メモリにおいて記憶された命令が命令装置を含むアーティファクトを生成するように、特定の様式で動作するようにコンピュータまたは任意の他のプログラマブルデータ処理デバイスに命令することができるコンピュータ可読メモリにおいて記憶され得る。この命令装置は、フローチャートの1つまたは複数のプロセスおよび/またはブロック図の1つまたは複数のブロック内で特定機能を実装する。

【0132】

これらのコンピュータプログラム命令は、一連の動作およびステップがコンピュータまたは別のプログラマブルデバイス上で実行され、それにより、コンピュータ実装処理を生成するように、コンピュータまたは別のプログラマブルデータ処理デバイスにロードされ得る。したがって、コンピュータまたは別のプログラマブルデバイス上で実行される命令は、フローチャートの1つまたは複数のプロセスまたはブロック図の1つまたは複数のブロック内の特定の機能を実装するためのステップを提供する。

【0133】

典型的な構成では、コンピューティングデバイスは、1つまたは複数の中央処理装置(CPU)と、入出力インターフェースと、ネットワークインターフェースと、メモリとを含む。

【0134】

メモリは、読取り専用メモリ(ROM)またはフラッシュメモリ(フラッシュRAM)など、コンピュータ可読媒体内に、揮発性メモリ、ランダムアクセスメモリ(RAM)、および/または不揮発性メモリなどの形式を含み得る。メモリはコンピュータ可読媒体の一例である。

【0135】

コンピュータ可読媒体は、揮発性および不揮発性の、リムーバブル媒体および非リムーバブル媒体を含み、任意の方法または技術を使用することによって情報を記憶することが

10

20

30

40

50

できる。情報は、コンピュータ可読命令、データ構造、プログラムモジュール、または他のデータであり得る。コンピュータ記憶媒体は、限定はしないが、パラメータランダムアクセスメモリ (PRAM)、スタティックランダムアクセスメモリ (SRAM)、ダイナミックランダムアクセスメモリ (DRAM)、別のタイプのランダムアクセスメモリ (RAM)、読取り専用メモリ (ROM)、電氣的消去可能プログラマブル読取り専用メモリ (EEPROM)、フラッシュメモリ技術もしくは別のメモリ技術、コンパクトディスク読取り専用メモリ (CD-ROM)、デジタル多用途ディスク (DVD) もしくは別の光記憶装置、磁気テープ、磁気ディスク記憶装置、別の磁気記憶デバイス、またはコンピューティングデバイスによってアクセスされ得る情報を記憶するために使用され得る任意の他の不送信媒体 (non-transmission media) を含む。本明細書で定義される、コンピュータ可読媒体は、一時的媒体、たとえば、被変調データ信号およびキャリアを含まない。

10

【 0 1 3 6 】

特に、「含む」、「包含する」という用語、またはそれらの任意の他の変形は、非排他的な包含を対象とすることを意図し、その結果、一連の要素を含む、プロセス、方法、物品、またはデバイスは、これらの要素を含むのみならず、明示的に列挙されない他の要素をやはり含むか、またはそのようなプロセス、方法、物品、またはデバイスに固有の要素をさらに含む。それ以上の制約が存在しないとき、その要素を含む、プロセス、方法、製品、またはデバイス内に別の同じかまたは同等の要素が存在する場合もある。

【 0 1 3 7 】

本出願は、プログラムモジュールなど、コンピュータによって実行されるコンピュータ実行可能命令の一般的な文脈で説明される場合がある。概して、プログラムモジュールは、特定のタスクを実行するための、または特定の抽象データタイプを実装するための、ルーチン、プログラム、オブジェクト、構成要素、データ構造などを含む。本出願は、通信ネットワークを使用することによって接続された遠隔処理デバイスによってタスクが実行される分散型コンピューティング環境内で実践されてもよい。分散型コンピューティング環境では、プログラムモジュールは、記憶デバイスを含む、ローカルコンピュータ記憶媒体とリモートコンピュータ記憶媒体の両方の中に配置され得る。

20

【 0 1 3 8 】

本明細書の実装形態はすべて、実装形態の同じまたは同様の部分に関して、互いに参照しながら、漸進的な方法で説明し、それぞれの実装形態は、他の実装形態とは異なる実装形態に焦点を当てる。具体的には、システム実装形態は方法実装形態と同様であり、したがって、手短かに説明され、関連部分に関しては、方法実装形態の部分説明を参照することである。

30

【 0 1 3 9 】

前述の説明は、本出願の実装形態に過ぎず、本出願を限定することを意図しない。当業者にとって、本出願は様々な修正および変更を有し得る。本出願の趣旨および原理内で行われるいずれの修正、同等の置換、改善などは、本出願の特許請求の範囲内に入るものとする。

【 0 1 4 0 】

図6は、本開示の一実装形態による、ログイン情報データ処理のためのコンピュータ実装方法600の一例を示すフローチャートである。提示を明瞭にするために、続く説明は、概して、本明細書内の他の図面の文脈で方法600について説明する。しかしながら、方法600は、たとえば、任意のシステム、環境、ソフトウェア、およびハードウェア、または、適宜に、システム、環境、ソフトウェア、およびハードウェアの組合せによって実行され得ることを理解されよう。いくつかの実装形態では、方法600の様々なステップは、並行して、組み合わせ、ループで、または任意の順序で実行されてよい。

40

【 0 1 4 1 】

602において、情報処理デバイスは、所定のスマートコントラクトテンプレートに基づいて、スマートコントラクトを作成する。作成されたスマートコントラクトは、ユーザに対応するログイン情報を含む。ログイン情報は、ユーザが送ったログイン情報記憶要求に

50

基づいて判定され、ログイン情報記憶要求は識別子を含む。いくつかの実装形態では、情報処理デバイスは、ログイン情報を処理することが可能なアプリケーションクライアントであり得る。アプリケーションクライアントは、本明細書の実装形態に記録される技術的解決策を実装することができ、端末デバイス上でAPPとして実行し得る。いくつかの実装形態では、情報処理デバイスは、ブラウザ内で実行するプラグイン、またはサーバであってもよい。

【0142】

ユーザが一定のインターネットサービスプラットフォームによって提供されるネットワークサービスを必要とするとき、ユーザは、通常、インターネットサービスプラットフォームにログインする必要がある。ユーザがインターネットサービスプラットフォームに初めてログインするとき、ユーザは、インターネットサービスプラットフォームに登録して、インターネットサービスプラットフォームにログインするためにユーザが使用するログイン情報を生成する必要がある。ユーザがインターネットサービスプラットフォームにログインするのを便利にするために、ユーザは、情報処理デバイスがログイン情報を処理する(たとえば、記憶または問い合わせる)ように、ログイン情報を取得した後、ログイン情報記憶要求を情報処理デバイスに送ることができる。情報処理デバイスは、ログイン情報処理デバイスであってよいが、またはログイン情報処理能力および本開示に整合する他の能力を有する情報処理デバイスであってもよい。

10

【0143】

いくつかの実装形態では、ユーザに対応するログイン情報は、ユーザによって設定されてよく、またはユーザ用の情報処理デバイスによって自動的に生成されてもよい。情報処理デバイスは、ログイン情報がセキュアであり、容易に判定され得ないように、ランダムに、異なるユーザのためにログイン情報を生成することができる。

20

【0144】

記録された識別子は、ユーザが容易に思い出すことができる情報である。識別子が受信された後、その識別子を提供するユーザのログイン情報が識別され得る。いくつかの実装形態では、識別子は、限定はしないが、パスワード、画像、文字列、または2次元コードであってよい。識別子がパスワードである場合、パスワードは、数字、漢字、文字、またはシンボルのうちの1つまたは複数を含み得る。加えて、記録された識別子は、ユーザ、情報処理デバイス、またはユーザ用のインターネットサービスプラットフォームによってユーザのために設定されてよい。

30

【0145】

いくつかの実装形態では、情報処理デバイスは、ログイン情報処理のために使用されるスマートコントラクトテンプレートを事前生成することができる。ログイン情報処理のために使用される処理論理は、スマートコントラクトテンプレート上に記録される。具体的には、ログイン情報は、処理論理を実行することによって処理され得る。たとえば、ログイン情報を処理するための論理は、ログイン情報を記憶するための論理を含み得る。ログイン情報は、記憶論理に基づいてブロックチェーンネットワークにおいて記憶され得る。別の例では、ログイン情報を処理するための論理は、ログイン情報を問い合わせるための論理を含み得る。ログイン情報は、クエリ論理に基づいて、ブロックチェーンネットワークから問い合わせられてよい。さらに別の例では、ログイン情報を処理するための論理は、ログイン情報を更新または削除するための論理を含み得る。記憶されたログイン情報は、更新論理に基づいて更新されてよく、記憶されたログイン情報は、削除論理に基づいて削除されてよい。更新および削除は、ブロックチェーンネットワーク内の更新に関するサービスデータを生成すること(たとえば、更新されることになるログイン情報および更新されたログイン情報はブロックチェーンネットワークにおいて記憶される)、および削除に関するサービスデータを生成することと理解され得る。

40

【0146】

いくつかの実装形態では、ログイン情報処理のために使用される、所定のスマートコントラクトテンプレートは、情報処理デバイス上に記憶され得る。いくつかの実装形態では

50

、所定のスマートコントラクトテンプレートは、ブロックチェーンネットワークであってよく、またはブロックチェーンネットワークにおいて記憶されてよい。情報処理デバイスは、ブロックチェーンネットワークと折衝することによって、ブロックチェーンネットワーク内にスマートコントラクトテンプレートを作成する。ブロックチェーンネットワークは、固定記憶アドレスをスマートコントラクトテンプレートに割り振り、固定記憶アドレスに基づいて、スマートコントラクトテンプレートをブロックチェーンネットワークにおいて記憶する。情報処理デバイスは、固定記憶アドレスに基づいて、スマートコントラクトテンプレートを取得することができる。

【0147】

いくつかの実装形態では、ログイン情報セキュリティを改善するために、暗号化されたログイン情報に基づいてスマートコントラクトを作成することができる。たとえば、ログイン情報を含むスマートコントラクトを作成するステップは、秘密-公開鍵対を取得するために識別子を処理するステップと、秘密-公開鍵対内の公開鍵を使用することによって、ログイン情報を暗号化するステップと、ログイン情報処理のために使用される、所定のスマートコントラクトテンプレートに基づいて、暗号化されたログイン情報を含むスマートコントラクトを作成するステップとを含み得る。いくつかの実装形態では、秘密-公開鍵対を取得するために識別子を処理するステップは、変換規則に基づいて、識別子をバイトコードに変換するステップ、たとえば、バイナリコードをバイトコードとして選択するステップと、計算論理に基づいて、バイトコードを使用することによって秘密-公開鍵対を生成するステップであって、秘密-公開鍵対が公開鍵および秘密鍵によって形成され、公開鍵がログイン情報を暗号化するために使用され、秘密鍵が暗号化されたログイン情報を解読するために使用され得る、生成するステップとを含み得る。

【0148】

いくつかの実装形態では、ログイン情報記憶要求が識別情報(たとえば、インターネットサービスプラットフォームの識別情報)を含む場合、作成されたスマートコントラクトは識別情報をやはり含む。602から、方法600は604に進む。

【0149】

604において、ログイン情報記憶要求に関連する識別子に基づいて、作成されたスマートコントラクトをブロックチェーンネットワーク内の記憶アドレスに記憶する。いくつかの実装形態では、スマートコントラクトを記憶するために、記憶アドレスがまず判定され、次いで、判定された記憶アドレスにスマートコントラクトが記憶される。

【0150】

いくつかの実装形態では、各スマートコントラクトの記憶アドレスを判定するために、秘密-公開鍵対を取得するために識別子がまず処理され、秘密-公開鍵対内の公開鍵に基づいて第1のアドレスが取得され、アルゴリズムに基づいて公開鍵を計算することによって第1のアドレスが判定される。たとえば、固定長のハッシュ値を取得するために、ハッシュアルゴリズムに基づいて公開鍵を計算することができ、ハッシュ値は第1のアドレスである。次いで、第1のアドレスに基づいて第2のアドレスをやはり判定することができ、第1のアドレスにおいて開始した、指定された取引イベントに基づいて、ブロックチェーンネットワークによって第2のアドレスが判定される。最終的に、第2のアドレスがブロックチェーンネットワーク内のスマートコントラクトの記憶アドレスと判定される。いくつかの実装形態では、指定された取引イベントは、取引と理解され得る。たとえば、Ethereumネットワークでは、スマートコントラクトの記憶アドレスを取得するために、特定の数量のEtherがEthereumネットワークに支払われる必要がある。具体的には、Ethereumネットワークにおいて取引が生成されるとき、取引のソースアドレスは第1のアドレスであり得、取引の宛先アドレスは第2のアドレスと呼ばれることがある(第2のアドレスはEthereumネットワークにおいて割り振られ得る)。第1のアドレスと第2のアドレスとの間の取引が完了すると、第2のアドレスに対応する記憶空間を使用して、ユーザのために作成されたスマートコントラクトを記憶することができる。ここで、第2のアドレスは、スマートコントラクトの記憶アドレスと呼ばれることもある。604から、方法600は606に進む。

10

20

30

40

50

【0151】

606において、情報処理デバイスにおいて、ユーザからログイン情報クエリ要求を受信する。ログイン情報クエリ要求は識別子を含む。

【0152】

いくつかの実装形態では、インターネットサービスプラットフォームにログインするとき、ユーザは、必要なログイン情報を取得するために、ログイン情報クエリ要求を情報処理デバイスに送ることができる。ユーザがログイン情報を必要とするとき、ユーザは、必要なログイン情報を取得するために、ログイン情報クエリ要求を情報処理デバイスに送ることができる。ユーザがログイン情報クエリ要求を送る使用シナリオは、限定的ではない。606から、方法600は608に進む。

10

【0153】

608において、ログイン情報クエリ要求に関連する識別子に基づいて、少なくとも1つのスマートコントラクトをブロックチェーンネットワークから取り出す。ユーザに対応するスマートコントラクトは、少なくとも1つの取り出されたスマートコントラクトから判定される。

【0154】

いくつかの実装形態では、ブロックチェーンネットワーク内の記憶アドレスからスマートコントラクトを取り出すために、識別子に基づいて、ログイン情報処理のために使用されるスマートコントラクトの記憶アドレスがまず判定される。たとえば、秘密-公開鍵対を取得するために、ログイン情報クエリ要求に関連する識別子がまず処理される。秘密-公開鍵対内の公開鍵に基づいて、第1のアドレスが取得され得る。第1のアドレスは、アルゴリズムに基づいて、公開鍵を計算することによって取得され得る。第1のアドレスに基づいて、少なくとも1つの第2のアドレスを取得することができ、第2のアドレスはそれぞれ第1のアドレスとの取引を実行する。具体的には、指定された取引イベントが生じた後、取引イベントに対応する取引データはブロックチェーンネットワークにおいて記憶される。第1のアドレスをクエリキーワードとして使用することができ、ブロックチェーンネットワーク内で第1のアドレスを含む取引データを問い合わせることができ、少なくとも1つの第2のアドレスを取引データから読み取ることができる。同じユーザの場合、第1のアドレスはユーザによって提供された識別子に基づいて判定されるため、取引データは、第1のアドレスと第2のアドレスとを含み得る。したがって、少なくとも1つの第2のアドレスは第1のアドレスに基づいて判定され得、判定された、少なくとも1つの第2のアドレスからスマートコントラクトの記憶アドレスが識別され得る。最終的に、少なくとも1つのスマートコントラクトを記憶アドレスから取り出すことができる。

20

30

【0155】

いくつかの実装形態では、第1のアドレスと取引を実行している1つの第2のアドレスが存在すると判定された場合、第2のアドレスをスマートコントラクトの記憶アドレスと判定し、または第1のアドレスと取引を実行している2つ以上の第2のアドレスが存在すると判定された場合、スマートコントラクトが記憶されている第2のアドレスを探索し、識別された第2のアドレスをスマートコントラクトの記憶アドレスと判定する。この状況では、スマートコントラクトの1つまたは複数の記憶アドレスが存在する場合があります、それに

40

【0156】

いくつかの実装形態では、1つのスマートコントラクトがブロックチェーンネットワークから読み取られた場合、そのスマートコントラクトはユーザに対応するスマートコントラクトと判定される。いくつかの実装形態では、2つ以上のスマートコントラクトがブロックチェーンネットワークから取り出された場合、指定された条件を満たすスマートコントラクトが取り出されたスマートコントラクトから選択され得る。たとえば、ログイン情報クエリ要求内に含まれた識別情報と同じ識別情報を有するスマートコントラクトが取り出されたスマートコントラクトから選択され得る。608から、方法600は610に進む。

【0157】

50

610において、ユーザに対応するログイン情報を取得するために、取り出されたスマートコントラクトを実行する。取得されたログイン情報は、次いで、ユーザに送り返されてよい。ユーザがログイン情報を使用してログインを完了することができるように、たとえば、平文形式で取得されたログイン情報はユーザに送られてよい。

【0158】

いくつかの実装形態では、スマートコントラクトを実行することによって、ログイン情報が取得された場合、ログイン情報はユーザのニーズを満たすと判定することができ、ログイン情報がユーザに提供され得る。いくつかの実装形態では、スマートコントラクトを実行することによって、複数のログイン情報データが取得された場合、確認のためにログイン情報がユーザに提供され得る。

10

【0159】

代替として、いくつかの実装形態では、ログイン情報が識別情報を含むとき、ログイン情報クエリ要求内に含まれた識別情報と同じ識別情報を有する特定のログイン情報を選択するために、ログイン情報から識別情報をパースし、選択されたログイン情報がユーザのニーズを満たすと判定することができる。

【0160】

いくつかの実装形態では、スマートコントラクトにおいて記憶されたログイン情報が暗号化された場合、スマートコントラクトを実行し、ユーザに対応するログイン情報を取得するために、暗号化されたログイン情報を取得するためにスマートコントラクトがまず実行される。秘密-公開鍵対を取得するために、ログイン情報クエリ要求に関連する識別子が処理され得る。解読されたログイン情報を取得するために、秘密-公開鍵対内の秘密鍵を使用することによって、暗号化されたログイン情報はさらに解読され得る。取得された、解読されたログイン情報はユーザに提供され得、ユーザは受信されたログイン情報を確認することができる。

20

【0161】

いくつかの実装形態では、ユーザはログイン情報処理要求を情報処理デバイスに送ることができる。ここで、取得されたログイン情報は、受信された処理要求に基づいてさらに処理され得る。いくつかの実装形態では、受信された処理要求が更新要求である場合、ログイン情報を更新することができ、更新されたログイン情報はブロックチェーンネットワークにおいて記憶され得る。いくつかの実装形態では、受信された処理要求が削除要求である場合、ログイン情報をブロックチェーンネットワークから削除することができる。610の後、方法600は停止する。

30

【0162】

本出願の実装形態は、ログイン情報を処理する際の技術的問題を解決し得る。既存の技術では、ログイン情報は第三者サーバ上に記憶される。しかしながら、第三者サーバは多くのユーザに関するログイン情報を記憶するため、記憶されたログイン情報が不適切に開示またはアクセスされ、ユーザに対するログイン情報セキュリティを低減させ得るリスクが存在する。説明した方法論は、ログイン情報データセキュリティを改善するためにこの問題の回避を可能にする。

【0163】

本明細書の実装形態は、ログイン情報処理方法について説明する。ログイン情報処理方法は、情報処理デバイスによって実行され得る。本明細書の実装形態で提供されるログイン情報処理方法に基づいて、一定のユーザのログイン情報を含むスマートコントラクトを作成することができ、スマートコントラクトはブロックチェーンネットワークにおいて記憶される。次いで、ログイン情報がブロックチェーンネットワークから問い合わせられ、取得され得る。ブロックチェーンネットワークは、ブロックチェーン技術に基づいて構築される。分散型台帳技術と呼ばれるブロックチェーン技術は、分散化、透明性、改ざん防止、および信頼性によって特徴づけられる分散型インターネットデータベース技術である。本開示で開示する解決策は、ブロックチェーンネットワークに基づいて実装され、その結果、ログイン情報が失われる、盗まれる、または改ざんされる可能性は低く、ログイン情

40

50

報の記憶セキュリティが改善される。さらに、本明細書の実装形態で提供されるログイン情報処理方法に基づいて、ユーザがログイン情報を必要とするとき、ユーザは、クエリによって、必要とされるログイン情報をブロックチェーンネットワークから迅速に取得することができ、ユーザがログイン情報を維持するのを便利にする。

【0164】

本明細書で説明した実施形態および動作は、デジタル電子回路の形で、もしくは、本明細書で開示した構造を含めて、コンピュータソフトウェア、ファームウェア、またはハードウェアの形で、あるいはそれらのうちの1つまたは複数の組合せの形で実装され得る。これらの動作は、1つまたは複数のコンピュータ可読記憶デバイス上に記憶された、または他のソースから受信されたデータに対してデータ処理装置によって実行される動作として実装され得る。データ処理装置、コンピュータ、またはコンピューティングデバイスは、例として、プログラマブルプロセッサ、コンピュータ、システムオンチップ、もしくは複数のプログラマブルプロセッサ、コンピュータ、システムオンチップ、または前述の組合せを含めて、データを処理するための装置、デバイス、および機械を包含し得る。この装置は、専用論理回路、たとえば、中央処理装置(CPU)、フィールドプログラマブルゲートアレイ(FPGA)、または特定用途向け集積回路(ASIC)を含み得る。この装置はまた、当該コンピュータプログラムに対する実行環境を作成するコード、たとえば、プロセッサファームウェア、プロトコルスタック、データベース管理システム、オペレーティングシステム(たとえば、1つのオペレーティングシステムまたはオペレーティングシステムの組合せ)、クロスプラットフォームランタイム環境、仮想機械、またはそれらのうちの1つまたは複数の組合せを構成するコードを含み得る。この装置および実行環境は、ウェブサービス、分散型コンピューティングインフラストラクチャ、およびグリッドコンピューティングインフラストラクチャなど、様々な異なるコンピューティングモデルインフラストラクチャを実現し得る。

【0165】

コンピュータプログラム(たとえば、プログラム、ソフトウェア、ソフトウェアアプリケーション、ソフトウェアモジュール、ソフトウェアユニット、スクリプト、またはコードとしても知られている)は、コンパイル型言語またはインタープリタ型言語、宣言型言語または手続き型言語を含めて、任意の形式のプログラミング言語で書き込まれてよく、スタンドアロンプログラムとして、またはモジュール、構成要素、サブルーチン、オブジェクト、またはコンピューティング環境において使用するのに適切な他のユニットなどを含めて、任意の形式で展開されてよい。プログラムは、他のプログラムまたはデータ(たとえば、マークアップ言語文書で記憶された、1つまたは複数のスクリプト)を保持するファイルの一部の中に、当該プログラム専用の単一のファイル内に、または複数の協調ファイル(たとえば、1つまたは複数のモジュール、サブプログラム、またはコードの部分記憶するファイル)において記憶され得る。コンピュータプログラムは、1つのコンピュータ上で、または1つのサイトに位置するか、または複数のサイトにわたって分散され、通信ネットワークによって相互接続された複数のコンピュータ上で実行され得る。

【0166】

コンピュータプログラムの実行のためのプロセッサは、例として、汎用マイクロプロセッサと専用マイクロプロセッサの両方、および任意の種類デジタルコンピュータの任意の1つまたは複数のプロセッサを含む。概して、プロセッサは、読取り専用メモリ、もしくはランダムアクセスメモリ、または両方から命令およびデータを受信することになる。コンピュータの必須要素は、命令に従って行為を実行するためのプロセッサ、および命令およびデータを記憶するための1つまたは複数のメモリデバイスである。概して、コンピュータはまた、データを記憶するための1つまたは複数の大容量記憶デバイスを含むことになるか、またはそこからデータを受信する、もしくはそこにデータを転送する、または両方のために1つまたは複数の大容量記憶デバイスに動作可能に結合されることになる。コンピュータは、別のデバイス、たとえば、モバイルデバイス、携帯情報端末(PDA)、ゲームコンソール、全地球測位システム(GPS)受信機、またはポータブル記憶デバイス内に

10

20

30

40

50

埋め込まれてもよい。コンピュータプログラム命令およびデータを記憶するのに適切なデバイスは、例として半導体メモリデバイス、磁気ディスク、および光磁気ディスクを含めて、不揮発性メモリデバイス、媒体デバイスおよびメモリデバイスを含む。プロセッサおよびメモリは、専用論理回路によって補足されてよいが、またはその中に組み込まれてもよい。

【0167】

モバイルデバイスはハンドセット、ユーザ機器(UE)、モバイル電話(たとえば、スマートフォン)、タブレット、装着可能デバイス(たとえば、スマートウィッチおよびスマート眼鏡)、人体内に埋め込まれたデバイス(たとえば、バイオセンサー、蝸牛インプラント)、または他のタイプのモバイルデバイスを含み得る。モバイルデバイスは、様々な通信ネットワーク(下記で説明する)に対して(たとえば、無線周波数(RF)信号を使用して)ワイヤレスで通信し得る。モバイルデバイスは、モバイルデバイスの現在の環境の特性を判定するためのセンサーを含み得る。これらのセンサーは、カメラ、マイクロフォン、近接度センサー、GPSセンサー、モーションセンサー、加速度計、周辺光センサー、湿度センサー、ジャイロスコープ、コンパス、気圧計、指紋センサー、顔認識システム、RFセンサー(たとえば、Wi-Fiおよびセルラー無線)、温度センサー、または他のタイプのセンサーを含み得る。たとえば、カメラは、可動レンズもしくは固定レンズ、フラッシュ、画像センサー、および画像プロセッサを備えた前方カメラまたは後方カメラを含み得る。カメラは、顔および/または虹彩認識のための詳細を捕捉することが可能なメガピクセルカメラであり得る。カメラは、データプロセッサ、およびメモリにおいて記憶された、または遠隔にアクセスされる認証情報とともに、顔認識システムを形成し得る。顔認識システムまたは1つまたは複数のセンサー、たとえば、マイクロフォン、モーションセンサー、加速度計、GPSセンサー、またはRFセンサーをユーザ認証のために使用することができる。

【0168】

ユーザとの対話を提供するために、ディスプレイデバイスおよび入力デバイス、たとえば、ユーザに情報を表示するための液晶ディスプレイ(LCD)または有機発光ダイオード(OLET)/仮想現実(VR)/拡張現実(AR)ディスプレイ、ならびにそれによりユーザがコンピュータに入力を提供することができる、タッチスクリーン、キーボード、およびポインティングデバイスを有するコンピュータ上で実施形態を実装することができる。他の種類のデバイスを使用して、ユーザとの対話を提供することも同様に可能であり、たとえば、ユーザに提供されるフィードバックは、任意の形式の知覚フィードバック、たとえば、視覚フィードバック、聴覚フィードバック、または触覚フィードバックであってよく、ユーザからの入力は、音響入力、音声入力、または触覚入力を含めて、任意の形式で受信され得る。加えて、コンピュータは、ユーザが使用するデバイスに文書を送ること、およびそのデバイスから文書を受信することによって、たとえば、ユーザのクライアントデバイス上でウェブブラウザから受信された要求に応じて、そのウェブブラウザにウェブページを送ることによって、ユーザと対話することができる。

【0169】

実施形態は、任意の形式のまたは媒体のワイヤラインまたはワイヤレスのデジタルデータ通信(または、それらの組合せ)、たとえば、通信ネットワークによって相互接続されたコンピューティングデバイスを使用して実装され得る。相互接続されたデバイスの例は、典型的には通信ネットワークを通して対話する、概して互いから離れたクライアントおよびサーバである。クライアント、たとえば、モバイルデバイスは、取引を自ら実行すること、サーバを用いて実行すること、またはサーバを通して実行すること、たとえば、購入取引、販売取引、支払い取引、提供取引、送信取引、またはローン取引を実行すること、またはそれらを認証することができる。そのような取引は、行為および応答が時間的に近接するように、たとえば、個人が実質的に同時に生じる行為および応答を認知するように、個人の行為に続く応答に対する時間差が1ミリ秒(ms)に満たないか、または1秒に満たないように、または応答はシステムの処理制限を考慮に入れた意図的な遅延を伴わないように、リアルタイムであり得る。

【0170】

通信ネットワークの例は、ローカルエリアネットワーク(LAN)、無線アクセスネットワーク(RAN)、メトロポリタンエリアネットワーク(MAN)、および広域ネットワーク(WAN)を含む。通信ネットワークは、インターネットのすべてまたは一部、別の通信ネットワーク、または通信ネットワークの組合せを含み得る。情報は、ロングタームエボリューション(LTE)、5G、IEEE802、インターネットプロトコル(IP)、もしくは他のプロトコル、またはプロトコルの組合せを含めて、様々なプロトコルおよび規格に従って通信ネットワーク上で送信され得る。通信ネットワークは、接続されたコンピューティングデバイス同士の間で、音声データ、ビデオデータ、生体データ、もしくは認証データ、または他の情報を送信することができる。

10

【0171】

別個の実装形態として説明した特徴は、組み合わせて、単一の実装形態で実装され得るが、単一の実装形態として説明した特徴は、複数の実装形態で、別個に、または任意の適切な部分組合せで実装されてもよい。特定の順序で説明し、特許請求した動作は、その特定の順序を必要とすると解釈されるべきではなく、すべての示した動作が実行されなければならないと解釈されるべきでもない(いくつかの動作は、任意であってよい)。適宜に、マルチタスキングもしくは並行処理(または、マルチタスキングと並行処理の組合せ)が実行され得る。

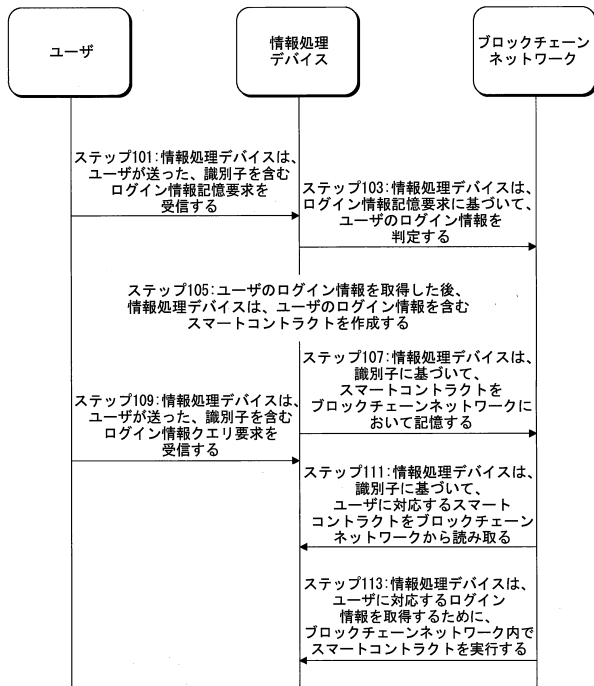
【符号の説明】

【0172】

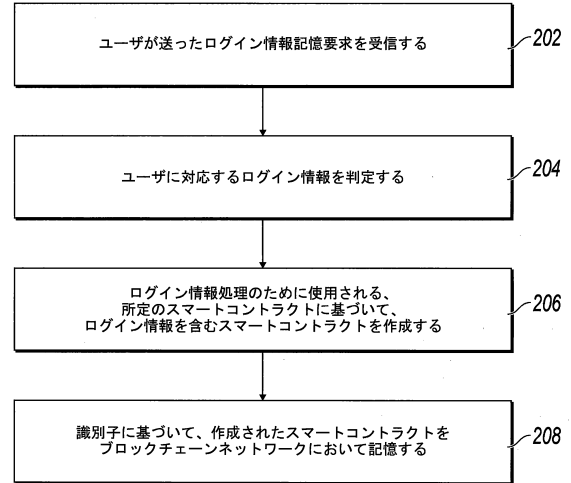
- 41 受信モジュール
- 42 読取りモジュール
- 43 処理モジュール
- 51 受信モジュール
- 52 判定モジュール
- 53 作成モジュール
- 54 記憶モジュール
- 600 方法

20

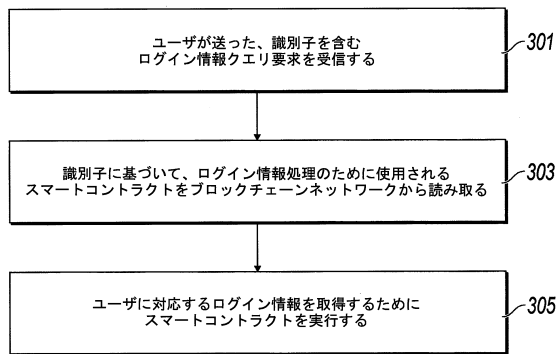
【図1】



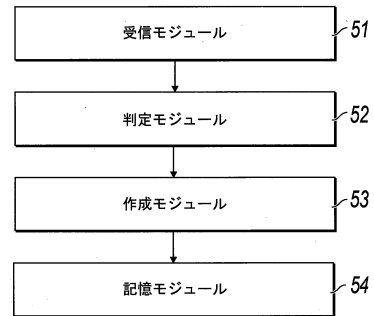
【図2】



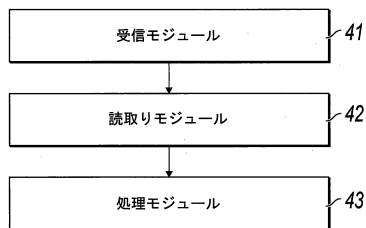
【図3】



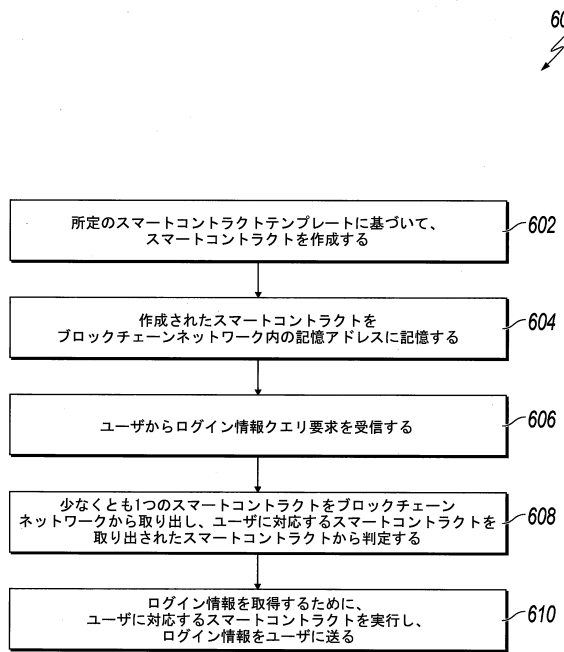
【図5】



【図4】



【図6】



フロントページの続き

(72)発明者 ハオ・リ

中華人民共和国・311121・ゼジャン・ハンジョウ・ユ・ハン・ディストリクト・ウェスト・
ウェン・イ・ロード・ナンバー・969・ビルディング・3・5 / エフ・アリババ・グループ・リ
ーガル・デパートメント

審査官 松平 英

(56)参考文献 国際公開第2016/179334 (WO, A1)

米国特許出願公開第2017/0177855 (US, A1)

米国特許出願公開第2016/0306982 (US, A1)

(58)調査した分野(Int.Cl., DB名)

G06F12/14

19/00

21/00 - 21/88

G06Q10/00 - 10/10

30/00 - 30/08

50/00 - 50/20

50/26 - 99/00

G09C 1/00 - 5/00

H04K 1/00 - 3/00

H04L 9/00 - 9/38