(19)日本国特許庁(JP)　(12)特　許　公　報(B1)　(11)特許番号
特許第6547079号
(P6547079)
(45)発行日　令和1年7月17日(2019.7.17)　(24)登録日　令和1年6月28日(2019.6.28)

(51)Int.Cl.　　F I
G06F 21/31 (2013.01)　　G06F 21/31
G06Q 20/02 (2012.01)　　G06Q 20/02

請求項の数 15　(全 18 頁)

(21)出願番号　特願2018-563628(P2018-563628)
(86)(22)出願日　平成28年12月23日(2016.12.23)
(86)国際出願番号　PCT/CN2016/111857
(87)国際公開番号　WO2018/112946
(87)国際公開日　平成30年6月28日(2018.6.28)
審査請求日　平成30年11月16日(2018.11.16)

早期審査対象出願

(73)特許権者　518409575
深▲セン▼前▲海▼▲達▼▲闥▼▲雲▼端智能科技有限公司
CLOUDMINDS (SHENZHEN) ROBOTICS SYSTEMS CO., LTD.
中国５１８０００▲広▼▲東▼省深▲セン▼市前▲海▼深▲港▼合作区前湾一路１号A▲棟▼２０１室　(入▲駐▼深▲セン▼市前▲海▼商▲務▼秘▲書▼有限公司)
ROOM 201, BLOCK A, NO. 1, QIANWAN ROAD 1, QIANHAISHEN PORT COOPERATIVE DISTRICT (SETTLED IN SHEN
最終頁に続く

(54)【発明の名称】登録・認可方法、装置及びシステム

(57)【特許請求の範囲】
【請求項１】
ブロックチェーンネットワークにおけるノードであり、認可情報を記憶するための複数のブロックからなるブロックチェーンを記憶している認可サーバに適用される登録方法であって、
ユーザ装置が送信した、ユーザに対してアイデンティティ認証を行うためのアイデンティティ確認情報を含む登録要求メッセージを受信するステップと、
前記ユーザがアクセス可能なサービスを指示するための認可情報を前記ユーザに割り当てるステップと、
前記認可サーバによって前記アイデンティティ確認情報及び前記認可情報をブロックチェーンのブロックに書き込むステップとを含むことを特徴とする登録方法。
【請求項２】
前記アイデンティティ確認情報はパスワードハッシュ値の暗号文、又は、ユーザ公開鍵であることを特徴とする請求項１に記載の方法。
【請求項３】
前記アイデンティティ確認情報に対応した認可情報を更新するための更新メッセージを受信するステップと、
前記認可サーバによって前記アイデンティティ確認情報及び更新後の認可情報を前記ブロックチェーンのブロックに書き込むステップとをさらに含むことを特徴とする請求項１又は２に記載の方法。

【請求項４】
ブロックチェーンネットワークにおけるノードであるアクセスサーバに適用される認可方法であって、
ユーザ装置が送信した、ユーザアイデンティティ情報を含むアクセス要求メッセージを受信するステップと、
前記アクセスサーバによって、前記ユーザアイデンティティ情報に基づいて、ブロックチェーンにおいてユーザのアイデンティティ確認情報及び認可情報を問い合わせるステップと、
前記アイデンティティ確認情報に基づいて、前記ユーザに対してアイデンティティ認証を行うステップと、
認証に通過した後、前記認可情報に基づいて、前記ユーザによる指定サービスへのアクセスを許可するステップとを含むことを特徴とする認可方法。
【請求項５】
前記アイデンティティ確認情報はパスワードハッシュ値の暗号文であり、前記ユーザアイデンティティ情報はユーザ名とパスワードハッシュ値とを含み、
前記アクセスサーバによって、前記ユーザアイデンティティ情報に基づいて、ブロックチェーンにおいてユーザのアイデンティティ確認情報及び認可情報を問い合わせる前記ステップは、
前記アクセスサーバによって、前記ユーザ名を用いて、前記ブロックチェーンにおいて対応したパスワードハッシュ値暗号文及び前記認可情報を検索するステップを含み、
前記アイデンティティ確認情報に基づいて、前記ユーザに対してアイデンティティ認証を行う前記ステップは、
前記パスワードハッシュ値の暗号文を復号して、復号して得た平文が前記ユーザアイデンティティ情報におけるパスワードハッシュ値と一致すると、認証に通過したと決定するステップを含むことを特徴とする請求項４に記載の方法。
【請求項６】
前記アイデンティティ確認情報はユーザ公開鍵であり、前記アイデンティティ確認情報に基づいて、前記ユーザに対してアイデンティティ認証を行う前記ステップは、
前記ユーザにアイデンティティ確認を提供するように指示するための指示情報を前記ユーザ装置に送信するステップと、
前記ユーザ装置が前記指示情報に基づいて送信した、ユーザ秘密鍵で署名した署名情報を受信するステップと、
前記ユーザ公開鍵に基づいて前記署名情報に対して署名認証を行い、署名認証に成功すると、アイデンティティ認証に通過したと決定するステップとを含むことを特徴とする請求項４に記載の方法。
【請求項７】
ブロックチェーンネットワークにおけるノードであり、認可情報を記憶するための複数のブロックからなるブロックチェーンを記憶している認可サーバに適用される登録装置であって、
ユーザ装置が送信した、ユーザに対してアイデンティティ認証を行うためのアイデンティティ確認情報を含む登録要求メッセージを受信するためのメッセージ受信ユニットと、
前記ユーザがアクセス可能なサービスを指示するための認可情報を前記ユーザに割り当てるための権限割当ユニットと、
前記認可サーバによって前記アイデンティティ確認情報及び前記認可情報をブロックチェーンのブロックに書き込むためのブロックチェーン書き込みユニットとを備えることを特徴とする登録装置。
【請求項８】
前記メッセージ受信ユニットはさらに、前記アイデンティティ確認情報に対応した認可情報を更新するための更新メッセージを受信し、
前記ブロックチェーン書き込みユニットはさらに、前記認可サーバによって前記アイデ

ンティティ確認情報及び更新後の認可情報を前記ブロックチェーンのブロックに書き込むことを特徴とする請求項７に記載の登録装置。

【請求項９】

ブロックチェーンネットワークにおけるノードであるアクセスサーバに適用される認可装置であって、

ユーザ装置が送信した、ユーザアイデンティティ情報を含むアクセス要求メッセージを受信するためのメッセージ受信ユニットと、

前記アクセスサーバによって、前記ユーザアイデンティティ情報に基づいて、ブロックチェーンにおいてユーザのアイデンティティ確認情報及び認可情報を問い合わせるためのブロックチェーン問い合わせユニットと、

前記アイデンティティ確認情報に基づいて、前記ユーザに対してアイデンティティ認証を行うためのアイデンティティ認証ユニットと、

前記アイデンティティ認証ユニットによる前記ユーザの認証に通過した後、前記認可情報に基づいて、前記ユーザによる指定サービスへのアクセスを許可するための認可アクセスユニットとを備えることを特徴とする認可装置。

【請求項１０】

前記アイデンティティ確認情報は、パスワードハッシュ値の暗号文であり、前記ユーザアイデンティティ情報は、ユーザ名とパスワードハッシュ値を含み、

前記ブロックチェーン問い合わせユニットは、前記アクセスサーバによって、前記ユーザ名を用いて、前記ブロックチェーンにおいて対応したパスワードハッシュ値暗号文及び前記認可情報を検索し、

前記アイデンティティ認証ユニットは、前記パスワードハッシュ値の暗号文を復号して、復号して得た平文が前記ユーザアイデンティティ情報におけるパスワードハッシュ値と一致すると、認証に通過したと決定することを特徴とする請求項９に記載の認可装置。

【請求項１１】

前記アイデンティティ確認情報はユーザ公開鍵であり、前記アイデンティティ認証ユニットは、

前記ユーザにアイデンティティ確認を提供するように指示するための指示情報を前記ユーザ装置に送信し、

前記ユーザ装置が前記指示情報に基づいて送信した、ユーザ秘密鍵で署名した署名情報を受信し、

前記ユーザ公開鍵に基づいて前記署名情報に対して署名認証を行い、署名認証に成功すると、アイデンティティ認証に通過したと決定することを特徴とする請求項９に記載の認可装置。

【請求項１２】

ブロックチェーンネットワークにおけるノードであり、認可情報を記憶するための複数のブロックからなるブロックチェーンを記憶している認可サーバであって、

プロセッサ、通信インターフェース、記憶装置及び通信バスを備え、前記プロセッサ、前記通信インターフェース及び前記記憶装置は前記通信バスを介して相互通信を行い、

前記記憶装置はアプリケーションプログラムを記憶し、

前記プロセッサは、前記アプリケーションプログラムを実行して、請求項１から３のいずれか一項に記載の方法を実現することを特徴とする。

【請求項１３】

ブロックチェーンネットワークにおけるノードであるアクセスサーバであって、

プロセッサ、通信インターフェース、記憶装置及び通信バスを備え、前記プロセッサ、前記通信インターフェース及び前記記憶装置は前記通信バスを介して相互通信を行い、

前記記憶装置はアプリケーションプログラムを記憶し、

前記プロセッサは、前記アプリケーションプログラムを実行して、請求項４から６のいずれか一項に記載の方法を実現することを特徴とするアクセスサーバ。

【請求項１４】

不揮発性のコンピュータ可読記憶媒体であって、
請求項１から３のいずれか一項に記載の方法を実行するためのコマンドを含むコンピュータプログラムを記憶することを特徴とするコンピュータ可読記憶媒体。
【請求項１５】
不揮発性のコンピュータ可読記憶媒体であって、
請求項４から６のいずれか一項に記載の方法を実行するためのコマンドを含むコンピュータプログラムを記憶することを特徴とするコンピュータ可読記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワーク通信の分野に関し、特に登録・認可方法、装置及びシステムに関する。
【背景技術】
【０００２】
登録したコンピュータ又はネットワークシステムにおけるユーザは、アクセス可能なサービスが異なる場合があり、認可とは、ユーザのアイデンティティを認証して、認証に通過した後、ユーザが利用可能なサービスを決定する過程である。
【０００３】
従来の認可技術では、一般的に信頼できる第三者機関の参加が必要であり、手順は以下の通りである。即ち、ユーザがアクセスゲートウェイにログインして、パスワード又は証明書などのユーザアイデンティティ確認を提供し、アクセスゲートウェイがユーザアイデンティティ確認を認可サーバに伝送する。認可サーバが、ユーザアイデンティティの認証を行い、認証結果に基づいて、認証成功メッセージとアクセス可能なサービス、又は認証失敗メッセージをアクセスゲートウェイに送信する。認証に通過した場合、アクセスゲートウェイはユーザによる対応したアクセス可能なサービスへのアクセスを許可する。
【０００４】
上記プロセスから明らかなように、認可サーバは、集中化サーバとして機能し、ハッカーにより攻撃されたり、又は該認可サーバを提供する機関により能動的に改ざんされると、当事者の正当な権利と利益が侵害される。以上から明らかなように、従来の認可技術にはセキュリティが低い問題があった。
【発明の概要】
【発明が解決しようとする課題】
【０００５】
本開示の目的は、従来の認可技術のセキュリティが低いという技術的問題を解決するために、登録・認可方法、装置及びシステムを提供することである。
【課題を解決するための手段】
【０００６】
上記目的を達成させるために、本発明の第１態様は、
ブロックチェーンネットワークにおけるノードであり、認可情報を記憶するための複数のブロックからなるブロックチェーンを記憶している認可サーバに適用される登録方法であって、
ユーザ装置が送信した、ユーザに対してアイデンティティ認証を行うためのアイデンティティ確認情報を含む登録要求メッセージを受信するステップと、
前記ユーザがアクセス可能なサービスを指示するための認可情報を前記ユーザに割り当てるステップと、
前記認可サーバによって前記アイデンティティ確認情報及び前記認可情報をブロックチェーンのブロックに書き込むステップとを含む、登録方法を提供する。
【０００７】
本発明の第２態様は、
ブロックチェーンネットワークにおけるノードであるアクセスサーバに適用される認可

方法であって、
ユーザ装置が送信した、ユーザアイデンティティ情報を含むアクセス要求メッセージを受信するステップと、
前記アクセスサーバによって、前記ユーザアイデンティティ情報に基づいて、ブロックチェーンにおいてユーザのアイデンティティ確認情報及び認可情報を問い合わせるステップと、
前記アイデンティティ確認情報に基づいて、前記ユーザに対してアイデンティティ認証を行うステップと、
認証に通過した後、前記認可情報に基づいて、前記ユーザによる指定サービスへのアクセスを許可するステップとを含む、認可方法を提供する。
【０００８】
本発明の第３態様は、
ブロックチェーンネットワークにおけるノードであり、認可情報を記憶するための複数のブロックからなるブロックチェーンを記憶している認可サーバに適用される登録装置であって、
ユーザ装置が送信した、ユーザに対してアイデンティティ認証を行うためのアイデンティティ確認情報を含む登録要求メッセージを受信するメッセージ受信ユニットと、
前記ユーザがアクセス可能なサービスを指示するための認可情報を前記ユーザに割り当てる権限割当ユニットと、
前記認可サーバによって前記アイデンティティ確認情報及び前記認可情報をブロックチェーンのブロックに書き込むブロックチェーン書き込みユニットとを備える、登録装置を提供する。
【０００９】
本発明の第４態様は、
ブロックチェーンネットワークにおけるノードであるアクセスサーバに用いられる認可装置であって、
ユーザ装置が送信した、ユーザアイデンティティ情報を含むアクセス要求メッセージを受信するためのメッセージ受信ユニットと、
前記アクセスサーバによって、前記ユーザアイデンティティ情報に基づいて、ブロックチェーンにおいてユーザのアイデンティティ確認情報及び認可情報を問い合わせるためのブロックチェーン問い合わせユニットと、
前記アイデンティティ確認情報に基づいて、前記ユーザに対してアイデンティティ認証を行うためのアイデンティティ認証ユニットと、
前記アイデンティティ認証ユニットによる前記ユーザの認証に通過した後、前記認可情報に基づいて、前記ユーザによる指定サービスへのアクセスを許可するための認可アクセスユニットとを備える、認可装置を提供する。
【００１０】
本発明の第５態様は、
ブロックチェーンネットワークにおけるノードであり、認可情報を記憶するための複数のブロックからなるブロックチェーンを記憶している認可サーバであって、
プロセッサ、通信インターフェース、記憶装置及び通信バスを備え、前記プロセッサ、前記通信インターフェース及び前記記憶装置は前記通信バスを介して相互通信を行い、
前記記憶装置はアプリケーションプログラムを記憶し、
前記プロセッサは、前記アプリケーションプログラムを実行して、第１態様に記載の方法を実現する、認可サーバを提供する。
【００１１】
本発明の第６態様は、
ブロックチェーンネットワークにおけるノードであるアクセスサーバであって、
プロセッサ、通信インターフェース、記憶装置及び通信バスを備え、前記プロセッサ、前記通信インターフェース及び前記記憶装置は前記通信バスを介して相互通信を行い、

前記記憶装置はアプリケーションプログラムを記憶し、
前記プロセッサは、前記アプリケーションプログラムを実行して、第２態様に記載の方法を実現する、アクセスサーバを提供する。
【００１２】
本発明の第７態様は、
認可サーバとアクセスサーバとを備え、前記認可サーバは、ブロックチェーンネットワークにおけるノードであり、前記アクセスサーバはブロックチェーンネットワークにおけるノードであり、ネットワークサービスを提供するサーバに接続され、
前記認可サーバは第１態様に記載の方法を実行し、
前記アクセスサーバは第２態様に記載の方法を実行する、認可システムを提供する。
【００１３】
本発明の第９態様は、
上記第１態様に記載の方法を実行するためのコマンドを含むコンピュータプログラムを記憶するコンピュータ可読記憶媒体を提供する。
【００１４】
本発明の第１０態様は、
第２態様に記載の方法を実行するためのコマンドを含むコンピュータプログラムを記憶するコンピュータ可読記憶媒体を提供する。
【発明の効果】
【００１５】
上記技術案によれば、認可サーバは、ユーザのアイデンティティ情報及び認可情報をブロックチェーンに書き込み、これにより、アクセスサーバは、ユーザ装置が送信したアクセス要求メッセージを受信したとき、ブロックチェーンに記憶されたアイデンティティ確認情報を用いてアクセスに対してアイデンティティ認証を行い、認証に通過した後、認可情報に基づいてユーザによる指定サービスへのアクセスを許可することができる。ブロックチェーンのトラストフリー化により、認可過程における信頼できる第三者機関による承認が不要となり、同時に、ブロックチェーンの分散化により、個人や組織がユーザの関連情報を改ざんすることが不可能になることで、認可のセキュリティと信頼性が確保される。
【図面の簡単な説明】
【００１６】
本発明の実施例又は従来技術における技術案をより明瞭に説明するために、以下、実施例の説明に使用される図面を簡単に説明し、勿論、以下の説明における図面は本発明の実施例の一部に過ぎず、当業者であれば、創造的な努力を必要とせずに、これら図面に基づいてほかの図面を想到し得る。
【図１】本発明の実施例による登録方法の概略フローチャートである。
【図２】本発明の実施例による認可方法の概略フローチャートである。
【図３】本発明の実施例による登録・認可方法の概略フローチャートである。
【図４】本発明の実施例による登録装置の構造模式図である。
【図５】本発明の実施例による認可装置の構造模式図である。
【図６】本発明の実施例による別の認可サーバの構造模式図である。
【図７】本発明の実施例による別のアクセスサーバの構造模式図である。
【図８】本発明の実施例による認可システムの構造模式図である。
【発明を実施するための形態】
【００１７】
本発明の実施例の目的、技術案及び利点をより明瞭にするために、以下、本発明の実施例における図面を参照しながら、本発明の実施例における技術案を明瞭且つ完全に説明するが、勿論、説明する実施例は本発明の実施例の一部に過ぎず、すべての実施例ではない。本発明における実施例に基づいて、当業者が創造的な努力を必要とせずに想到し得るすべてのその他の実施例は本発明の保護範囲に属する。

【００１８】
当業者が本発明の実施例による技術案をより容易に把握できるように、以下、まずかかる関連技術について簡単に説明する。
【００１９】
ブロックチェーンは、ブロックチェーンネットワークにおけるすべてのノードが参加したりメンテナンスをしたりする非中央集権性化分散型データベースシステムであり、暗号学方法により生成した一連のデータブロックからなり、データブロックがそれぞれブロックチェーンの１つのブロックとなる。生成順番に応じて、ブロックは規則的にリンクされて１本のデータチェーンを構成し、このようなデータチェーンはブロックチェーンと呼ばれる。ブロックチェーンは、その特有なブロック、取引発生、認証プロトコルを有し、変更、偽造ができず、完全に追跡可能なセキュリティ特性を有する。
【００２０】
＜ブロックチェーン技術における関連概念の説明＞
ユーザアイデンティティ：ブロックチェーンにおけるユーザアイデンティティは公開鍵で示され、前記公開鍵に対応した秘密鍵はネットワークへ開示されずユーザだけに保有され、公開鍵は特定のハッシュとコーディングを経て「アドレス」となり、「アドレス」はユーザを代表し、自由に公開可能である。
【００２１】
ブロックチェーンデータの書き込み：ブロックチェーンノードは、ブロックチェーンネットワークに「取引」（Ｔｒａｎｓａｃｔｉｏｎ）を開示することによりブロックチェーンにデータを書き込む。取引には、ユーザが自分の秘密鍵を用いて取引に対して署名を行い、ユーザのアイデンティティを証明することが含まれる。取引が、「マイナー」（ブロックチェーンコンセンサス競争メカニズムを実行するブロックチェーンノード）により生成した新ブロックに記録され、次にブロックチェーンネットワークに開示されて、その他のブロックチェーンノードによる認証に通過し且つ受信された後、取引データがブロックチェーンに書き込まれる。
【００２２】
＜ブロックチェーンに備える特性＞
分散化：ブロックチェーンシステム全体に亘って、集中化されたハードウェア又は管理機関がなく、すべてのノードの権利や義務が等しく、且ついずれかのノードの破損又は喪失によりシステム全体の作動に影響を与えることがない。従って、ブロックチェーンは優れた堅牢性を有すると言える。
トラストフリー化：ブロックチェーンシステム全体における各々のノードの間のデータ交換には相互信頼を必要とせず、システム全体の作動ルールは開示されており、すべてのデータコンテンツも公開されているため、システムにより指定されたルールや時間内では、ノードはノードを欺くことができない。
【００２３】
本発明の実施例は、ブロックチェーン技術に基づいて登録方法を提供し、該方法は、認可サーバに適用され、該認可サーバはブロックチェーンネットワークにおけるノードであり、図１に示されるように、該方法は、ステップＳ１０１－Ｓ１０３を含む。
【００２４】
Ｓ１０１において、ユーザ装置が送信した、アイデンティティ確認情報を含む登録要求メッセージを受信する。
前記アイデンティティ確認情報は、ユーザに対してアイデンティティ認証を行うために使われる。
【００２５】
Ｓ１０２において、前記ユーザがアクセス可能なサービスを指示するための認可情報を前記ユーザに割り当てる。
なお、認可サーバは、あらかじめ設定された認可ルールに基づいてユーザに認可情報を割り当てて、ユーザがアクセス可能なサービスを制御することができる。たとえば、具体

的に実施する過程において、認可サーバは、異なるアイデンティティ、異なるアクセス地点、異なるアクセス方式、異なる安全状態を有するユーザに合理的なネットワークアクセス権限を設定することができ、本発明では、それについて限定しない。

【００２６】

Ｓ１０３において、前記認可サーバによって前記アイデンティティ確認情報及び前記認可情報をブロックチェーンのブロックに書き込む。

【００２７】

上記ブロックチェーンデータへの書き込みについての説明を参照すると、認可サーバが少なくともブロックチェーン取引に参加する機能を具備するように、該認可サーバは、ブロックチェーンネットワークにおける１つのブロックチェーンノードである。ブロックチェーンネットワークにおけるノードとして、認可サーバは認可情報を記憶するための複数のブロックからなるブロックチェーンを記憶している。なお、認可サーバはマイニングに参加しなくてもよく、このような場合、上記ステップＳ１０３では、認可サーバは、アイデンティティ確認情報及び認可情報をブロックチェーンネットワークにおけるほかのノードにブロードキャストして、その他のノードによりブロックを生成するときに書き込む。認可サーバは、マイニングに参加してもよく、このような場合、認可サーバは、自分でブロックを生成してブロック書き込み権限を取得するときに、アイデンティティ確認情報及び認可情報をブロックに書き込んでもよく、アイデンティティ確認情報及び認可情報をブロックチェーンネットワークにおけるその他ノードへブロードキャストして、その他ノードによりブロックを生成するときに書き込んでもよい。

【００２８】

上記方法によれば、アクセスサーバは、ブロックチェーンネットワークにおけるノードとして、ユーザ装置が送信したアクセス要求メッセージを受信したときに、ブロックチェーンに記憶されたアイデンティティ確認情報を用いてアクセスに対してアイデンティティ認証を行い、認証に通過した後、認可情報に基づいてユーザによる指定サービスへのアクセスを許可することができる。ブロックチェーンのトラストフリー化により、認可過程における信頼できる第三者機関による承認が不要となり、同時に、ブロックチェーンの分散化により、個人や組織がユーザの関連情報を改ざんすることが不可能になることで、認可のセキュリティと信頼性が確保される。

【００２９】

さらに、本発明の実施例はさらに認可方法を提供し、前記方法はアクセスサーバに適用され、前記アクセスサーバはブロックチェーンネットワークにおけるノードであり、図２に示されるように、該方法はステップＳ２０１－Ｓ２０１を含む。

【００３０】

Ｓ２０１において、ユーザ装置が送信した、ユーザアイデンティティ情報を含むアクセス要求メッセージを受信する。

【００３１】

Ｓ２０２において、前記アクセスサーバによって、前記ユーザアイデンティティ情報に基づいて、ブロックチェーンにおいてユーザのアイデンティティ確認情報及び認可情報を問い合わせる。

アクセスサーバは、少なくともブロックチェーン問い合わせ機能を具備するように、ブロックチェーンネットワークにおける１つのブロックチェーンノードである。本発明の実施例の一実施形態において、該アクセスサーバと図１に示される登録方法における認可サーバは同一サーバであってもよい。

なお、ブロックチェーンにおけるユーザアイデンティティについての上記説明を参照すると、ユーザアイデンティティとブロックチェーンノードには１対１対応関係がなく、ユーザはいずれかのブロックチェーンノードにおいて自分の秘密鍵を使用することができ、これにより、アクセスサーバは、秘密鍵を用いてブロックチェーンにおいていずれかのブロックを検索して、ユーザのアイデンティティ確認情報及び認可情報を問い合わせて取得することができる。該アクセスサーバは、ブロックチェーンにおいてユーザのアイデンテ

ィティ確認情報と認可情報が見つからなかった場合、ユーザ装置にアクセス失敗メッセージを返送する。

【００３２】

Ｓ２０３において、前記アイデンティティ確認情報に基づいて、前記ユーザに対してアイデンティティ認証を行う。

【００３３】

Ｓ２０４において、前記ユーザアイデンティティ情報認証に通過した後、前記認可情報に基づいて、前記ユーザによる指定サービスへのアクセスを許可する。

このように、ユーザ装置によるアクセス要求メッセージを受信した後、信頼できる第三者機関でユーザ認証を行う必要のある従来技術によるアクセスサーバに比べて、本発明の実施例による認可方法では、ブロックチェーンネットワークには集中化されたハードウェア又は管理機関がないので、すべてのノードの権利と義務が等しく、且ついずれかのノードの破損又は喪失によりシステム全体の作動に影響を与えることがないため、認可過程はより安全で信頼できる。

【００３４】

以下、アイデンティティ確認情報とユーザアイデンティティ情報に基づくユーザ認証を具体的に説明する。

【００３５】

＜形態１＞

上記ステップＳ１０１において、アイデンティティ確認情報はパスワードハッシュ値の暗号文であってもよく、具体的に実施するとき、アクセスサーバの公開鍵でパスワードハッシュ値の平文を暗号化して該アイデンティティ確認情報を取得してもよいし、予め設定された秘密鍵で対称暗号化アルゴリズムによりパスワードハッシュ値の平文を暗号化して取得してもよく、ここで、前記予め設定された秘密鍵は、認可サーバとアクセスサーバにより独立して記憶されて使用されることができる。

これにより、ステップＳ２０３では、ユーザアイデンティティ情報はユーザ名とパスワードハッシュ値を含むことができ、アクセスサーバは、ユーザアイデンティティ情報を受信した後、ユーザ名に基づいてブロックチェーンに記憶されたパスワードハッシュ値暗号文を検索し、さらに、自分の秘密鍵又は予め設定された秘密鍵でアイデンティティ確認情報を復号してパスワードハッシュ値の平文を取得し、復号して得たパスワードハッシュ値の平文とユーザアイデンティティ情報におけるパスワードハッシュ値が一致すると、ユーザアイデンティティ認証に通過したとし、一致しないと、ユーザアイデンティティ認証に通過しないとする。

【００３６】

＜形態２＞

上記ステップＳ１０１では、アイデンティティ確認情報はユーザ公開鍵であってもよく、ステップＳ２０３では、ユーザアイデンティティ情報はユーザ公開鍵であってもよい。これにより、アクセスサーバは、ユーザ公開鍵に基づいてブロックチェーンにユーザ公開鍵と認可情報が記録されていると決定すると、前記ユーザにアイデンティティ確認を提供するように指示するための指示情報を前記ユーザ装置に送信し、且つ前記ユーザ装置が前記指示情報に基づいて送信したユーザ秘密鍵で署名した署名情報を受信し、該署名情報に対して署名認証を行うことができ、署名認証に成功すると、ユーザアイデンティティ認証に通過したとし、署名認証が失敗すると、ユーザアイデンティティ認証が失敗したとする。

【００３７】

上記は例示的に説明するに過ぎず、具体的に実施するとき、ほかの形態でユーザに対してアイデンティティ認証を行って構わず、本発明では、それについて限定しない。

【００３８】

本発明の実施例の一実施形態において、図１に示される登録方法はさらに、認可サーバが、前記アイデンティティ確認情報に対応した認可情報を更新するための更新メッセージ

を受信し、且つ前記認可サーバによって前記アイデンティティ確認情報及び更新後の認可情報を前記ブロックチェーンのブロックに書き込むステップを含む。

【００３９】

つまり、認可サーバで設定された認可ルールに基づいて、ユーザが認可情報変更条件を満たすと、認可サーバは、管理システムのコントロールに基づいてユーザの認可範囲を変更し得る。これにより、ブロックチェーンにユーザアイデンティティ確認情報及び認可情報を記憶した複数のブロックが存在する可能性がある。従って、上記ステップＳ２０２では、アクセスサーバによって前記ユーザアイデンティティ情報を用いて前記ブロックチェーンにおいて前記ユーザのアイデンティティ確認情報及び認可情報を記憶した複数ブロックを見つけた場合、アクセスサーバが最新認可情報に基づいてユーザによるネットワークサービスへのアクセスを許可するように、前記複数のブロックのうち、最新ブロックから前記ユーザのアイデンティティ確認情報及び認可情報を取得する。

【００４０】

当業者が本発明の実施例による技術案をさらに把握できるように、以下、本発明の実施例による登録・認可方法を例示的に説明し、図３に示されるように、該方法は、ステップＳ３０１－Ｓ３０９を含む。

【００４１】

Ｓ３０１において、ユーザ装置が、認可サーバにユーザ公開鍵を含む登録要求メッセージを送信する。

【００４２】

Ｓ３０２において、認可サーバが、ユーザに認可情報を割り当てて、前記ユーザ公開鍵と前記認可情報をブロックチェーンに書き込む。

【００４３】

Ｓ３０３において、ユーザ装置が、アクセスサーバにユーザ公開鍵を含むアクセス要求メッセージを送信する。

【００４４】

Ｓ３０４において、アクセスサーバが、前記ユーザ公開鍵に基づいてブロックチェーンにおいて該ユーザ公開鍵がブロックチェーンに書き込まれているか否かを問い合わせる。さらに、前記ユーザ公開鍵によりブロックチェーンにおいて該ユーザ公開鍵がブロックチェーンに書き込まれていないと検出された場合、ステップＳ３０５を実行し、前記ユーザ公開鍵によりブロックチェーンにおいて該ユーザ公開鍵がブロックチェーンに書き込まれていると検出された場合、ステップＳ３０６及び後続ステップを実行する。

【００４５】

Ｓ３０５において、アクセスサーバがユーザ装置にアクセス拒否メッセージを返送する。

【００４６】

Ｓ３０６において、アクセスサーバが、ユーザに公開秘密鍵に基づくアイデンティティ確認を提供するように指示するためのメッセージをユーザ装置に送信する。

【００４７】

Ｓ３０７において、ユーザ装置が、アクセスサーバにユーザ秘密鍵で署名した署名情報を送信する。

【００４８】

Ｓ３０８において、アクセスサーバが、ユーザ公開鍵に基づいて該署名情報に対して署名認証を行う。

さらに、署名認証が失敗すると、ステップＳ３０５を実行し、署名認証に成功すると、ステップＳ３０９を実行する。

【００４９】

Ｓ３０９において、アクセスサーバが、前記認可情報に基づいて、ユーザ装置による認可範囲内のネットワークサービスへのアクセスを許可する。

【００５０】

上記方法によれば、ブロックチェーンのトラストフリー化により、認可過程における信頼できる第三者機関の承認が不要となり、同時に、ブロックチェーンの分散化により、個人や組織がユーザの関連情報を改ざんすることが不可能になることで、認可のセキュリティと信頼性が確保される。

【００５１】

なお、上記方法では、ユーザ公開鍵をアイデンティティ確認情報とする場合を例にして説明しているが、具体的に実施するとき、アイデンティティ確認情報は、パスワードハッシュ値の暗号文としてもよい。さらに、上記方法の実施例では、説明し易さから、一連の動作を組み合わせたが、当業者にとって明らかなように、本発明は説明された動作の順番により制限されない。また、当業者にとって明らかなように、明細書に説明された実施例のいずれも好適実施例であり、関する動作は必ず本発明にとって必須なものであると限らない。

【００５２】

本発明の実施例はさらに登録装置４０を提供し、前記登録装置４０は認可サーバに適用され、前記認可サーバはブロックチェーンネットワークにおけるノードであり、認可情報を記憶するための複数のブロックからなるブロックチェーンを記憶しており、前記登録装置４０は、上記方法の実施例による図１に示される登録方法を実施し、図４に示されるように、該登録装置４０は、

ユーザ装置が送信した、ユーザに対してアイデンティティ認証を行うためのアイデンティティ確認情報を含む登録要求メッセージを受信するためのメッセージ受信ユニット４０１と、

前記ユーザがアクセス可能なサービスを指示するための認可情報を前記ユーザに割り当てる権限割当ユニット４０２と、

前記認可サーバによって前記アイデンティティ確認情報及び前記認可情報をブロックチェーンのブロックに書き込むブロックチェーン書き込みユニット４０３とを備える。

【００５３】

上記登録装置によれば、該登録装置を用いた認可サーバは、ユーザのアイデンティティ情報及び認可情報をブロックチェーンに書き込むことができ、これにより、アクセスサーバは、ユーザ装置が送信したアクセス要求メッセージを受信したときに、ブロックチェーンに記憶されたアイデンティティ確認情報を用いてアクセスに対してアイデンティティ認証を行い、認証に通過した後、認可情報に基づいてユーザによる指定サービスへのアクセスを許可する。ブロックチェーンのトラストフリー化により、認可過程における信頼できる第三者機関の承認が不要となり、同時に、ブロックチェーンの分散化により、個人や組織がユーザの関連情報を改ざんすることが不可能になることで、認可のセキュリティと信頼性が確保される。

【００５４】

なお、前記アイデンティティ確認情報はパスワードハッシュ値の暗号文、又は、ユーザ公開鍵である。具体的には、上記方法の実施例における形態１と形態２を参照すればよいため、ここで詳細な説明を省略する。

【００５５】

前記メッセージ受信ユニット４０１はさらに、前記アイデンティティ確認情報に対応した認可情報を更新するための更新メッセージを受信し、前記ブロックチェーン書き込みユニット４０３はさらに、前記認可サーバによって前記アイデンティティ確認情報及び更新後の認可情報を前記ブロックチェーンのブロックに書き込むようにしてもよい。

【００５６】

つまり、認可サーバで設定された認可ルールに基づいて、ユーザが認可情報変更条件を満たすと、認可サーバは、管理システムのコントロールに基づいてユーザの認可範囲を変更することができる。これにより、ブロックチェーンには、ユーザアイデンティティ確認情報及び認可情報を記憶した複数のブロックが存在する可能性がある。

【００５７】

当業者にとって明らかなように、説明の便利さ及び簡素化から、上記各機能ユニットの分割を例にして説明するに過ぎず、実際に適用されるとき、必要に応じて上記機能を異なる機能ユニットで行うことができ、すなわち、以上説明したすべて又は一部の機能を行うように、装置の内部構造を異なる機能ユニットに分割することができる。上記説明した機能ユニットの具体的な作動過程について、前述方法の実施例における対応過程を参照すればよいため、ここで詳細な説明を省略する。

【００５８】

さらに、上記機能ユニットの物理的な形態も複数種の方式があり、たとえば、一例示的な実施形態では、登録装置４０は１つ又は複数ＡＳＩＣ（Ａｐｐｌｉｃａｔｉｏｎ Ｓｐｅｃｉｆｉｃ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ、特定用途向け集積回路）、ＤＳＰ（Ｄｉｇｉｔａｌ Ｓｉｇｎａｌ Ｐｒｏｃｅｓｓｏｒ、デジタル信号プロセッサ）、ＤＳＰＤ（Ｄｉｇｉｔａｌ Ｓｉｇｎａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｄｅｖｉｃｅ、デジタル信号処理装置）、ＰＬＤ（Ｐｒｏｇｒａｍｍａｂｌｅ Ｌｏｇｉｃ Ｄｅｖｉｃｅ、プログラマブルロジックデバイス）、ＦＰＧＡ（Ｆｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ、フィールドプログラマブルゲートアレイ）、コントローラ、マイクロコントローラ、マイクロプロセッサー又はほかの電子部品によって実現されて、図１による方法を実行してもよい。

【００５９】

本発明の実施例はさらに、認可装置５０を提供し、前記認可装置５０は、アクセスサーバに適用され、前記アクセスサーバは、ブロックチェーンネットワークにおけるノードであり、前記認可装置５０は、上記方法の実施例による図２に示される認可方法を実施し、図５に示されるように、該認可装置５０は、

ユーザ装置が送信した、ユーザアイデンティティ情報を含むアクセス要求メッセージを受信するためのメッセージ受信ユニット５０１と、

前記アクセスサーバによって、前記ユーザアイデンティティ情報に基づいて、ブロックチェーンにおいてユーザのアイデンティティ確認情報及び認可情報を問い合わせるためのブロックチェーン問い合わせユニット５０２と、

前記アイデンティティ確認情報に基づいて、前記ユーザに対してアイデンティティ認証を行うためのアイデンティティ認証ユニット５０３と、

前記アイデンティティ認証ユニットによる前記ユーザの認証に通過した後、前記認可情報に基づいて、前記ユーザによる指定サービスへのアクセスを許可するための認可アクセスユニット５０４とを備える。

【００６０】

ブロックチェーンのトラストフリー化により、認可過程における信頼できる第三者機関の承認が不要となり、同時に、ブロックチェーンの分散化により、個人や組織がユーザの関連情報を改ざんすることが不可能になることで、認可のセキュリティと信頼性が確保される。

【００６１】

前記ブロックチェーン問い合わせユニット５０２は、

前記ユーザアイデンティティ情報に基づいて前記ブロックチェーンにおいて前記ユーザのアイデンティティ確認情報及び認可情報を記憶した複数のブロックが検出されたとき、前記複数のブロックのうち、最新ブロックから前記ユーザのアイデンティティ確認情報及び認可情報を取得するようにしてもよい。

【００６２】

前記アイデンティティ確認情報は、パスワードハッシュ値の暗号文であり、前記ユーザアイデンティティ情報はユーザ名とパスワードハッシュ値を含み、前記ブロックチェーン問い合わせユニット５０２は、前記アクセスサーバによって、前記ユーザ名を用いて、前記ブロックチェーンにおいて対応したパスワードハッシュ値暗号文及び前記認可情報を検索し、前記アイデンティティ認証ユニット５０３は、前記パスワードハッシュ値の暗号文を復号して、復号して得た平文が前記ユーザアイデンティティ情報におけるパスワードハ

ッシュ値と一致すると、認証に通過したと決定するようにしてもよい。
【００６３】
前記アイデンティティ確認情報はユーザ公開鍵であり、前記アイデンティティ認証ユニット５０３は、前記ユーザにアイデンティティ確認を提供するように指示するための指示情報を前記ユーザ装置に送信し、前記ユーザ装置が前記指示情報に基づいて送信したユーザ秘密鍵で署名した署名情報を受信し、前記ユーザ公開鍵に基づいて前記署名情報に対して署名認証を行い、署名認証に成功すると、アイデンティティ認証に通過したと決定するようにしてもよい。
【００６４】
具体的に実施するとき、アクセスサーバはユーザ装置がアクセスすべきネットワーク境界に位置してもよく、ネットワークはインターネットＩｎｔｅｒｎｅｔ又はローカルエリアネットワークであってもよい。ユーザ装置は、認証に通過した後、ネットワーク、ネットワークのすべてのサービスにアクセスできる。ネットワークサービスを提供するのはクラウドサービスであってもよく、ユーザ装置は、アイデンティティ認証に通過した後、認可範囲内の対応サービスにアクセスし得る。
【００６５】
当業者にとって明らかなように、説明の便利さ及び簡素化から、上記説明したアクセスサーバの各ユニットの具体的な作動過程について、前述方法の実施例における対応過程を参照すればよいため、ここで詳細な説明を省略する。
【００６６】
さらに、上記アクセスサーバを構成するユニットの分割は、ロジック機能に応じた分割だけであり、実際に実施するときに、別の分割方式を用いてもよい。且つ、各個ユニットの物理的な実現形態も複数種の方式があり、本発明では、それについて限定しない。
【００６７】
本発明の実施例はさらに認可サーバ６０を提供し、該認可サーバ６０はブロックチェーンネットワークにおけるノードであり、図６に示されるように、該認可サーバ６０は、プロセッサ６０１、通信インターフェース６０２、記憶装置６０３及び通信バス６０４を備え、前記プロセッサ６０１、前記通信インターフェース６０２及び前記記憶装置６０３は前記通信バス６０４を介して相互通信を行う。
プロセッサ６０１はマルチコア中央プロセッサＣＰＵ、又は特定用途向け集積回路ＡＳＩＣ（Ａｐｐｌｉｃａｔｉｏｎ Ｓｐｅｃｉｆｉｃ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）、又は発明の実施例を実施するように設置される１つ又は複数の集積回路としてもよい。
【００６８】
記憶装置６０３は、コンピュータオペレーションコマンドとネットワークフロー図を含むプログラムコードを格納する。記憶装置６０３は高速ＲＡＭ記憶装置を備えてもよく、さらに不揮発性メモリ（ｎｏｎ－ｖｏｌａｔｉｌｅ ｍｅｍｏｒｙ）、たとえば少なくとも１つのディスク記憶装置を含んでもよい。
【００６９】
前記通信インターフェース６０２は、これら装置間の接続通信を実施する。
【００７０】
前記プロセッサ６０１はプログラムコードを実行し、前記プログラムコードは、実行されると、
ユーザ装置が送信した、ユーザに対してアイデンティティ認証を行うためのアイデンティティ確認情報を含む登録要求メッセージを受信する方法と、
前記ユーザがアクセス可能なサービスを指示するための認可情報を前記ユーザに割り当てる方法と、
前記アイデンティティ確認情報及び前記認可情報をブロックチェーンのブロックに書き込む方法とを実現する。
【００７１】

前記アイデンティティ確認情報は、パスワードハッシュ値の暗号文、又は、ユーザ公開鍵であるようにしてもよい。

【００７２】

前記方法は、

前記アイデンティティ確認情報に対応した認可情報を更新するための更新メッセージを受信し、

前記アイデンティティ確認情報及び更新後の認可情報を前記ブロックチェーンのブロックに書き込むことを含むようにしてもよい。

【００７３】

上記認可サーバによれば、該認可サーバは、ユーザのアイデンティティ情報及び認可情報をブロックチェーンに書き込み、これにより、アクセスサーバは、ユーザ装置が送信したアクセス要求メッセージを受信したとき、ブロックチェーンに記憶されたアイデンティティ確認情報を用いてアクセスに対してアイデンティティ認証を行い、認証に通過した後、認可情報に基づいてユーザによる指定サービスへのアクセスを許可することができる。ブロックチェーンのトラストフリー化により、認可過程における信頼できる第三者機関の承認が不要となり、同時に、ブロックチェーンの分散化により、個人や組織がユーザの関連情報を改ざんすることが不可能になることで、認可のセキュリティと信頼性が確保される。

【００７４】

本発明の実施例はさらにアクセスサーバ７０を提供し、該アクセスサーバはブロックチェーンネットワークにおけるノードであり、図７に示されるように、該アクセスサーバ７０は、

プロセッサ（ｐｒｏｃｅｓｓｏｒ）７０１、通信インターフェース（Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ　Ｉｎｔｅｒｆａｃｅ）７０２、記憶装置（ｍｅｍｏｒｙ）７０３及び通信バス７０４を備え、前記プロセッサ７０１、前記通信インターフェース７０２及び前記記憶装置７０３は前記通信バス７０４を介して相互通信を行う。

【００７５】

プロセッサ７０１は、マルチコア中央プロセッサＣＰＵ、又は特定用途向け集積回路ＡＳＩＣ（Ａｐｐｌｉｃａｔｉｏｎ　Ｓｐｅｃｉｆｉｃ　Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）、又は本発明の実施例を実施するように配置される１つ又は複数の集積回路としてもよい。

【００７６】

記憶装置７０３は、コンピュータオペレーションコマンドとネットワークフロー図を含むプログラムコードを格納する。記憶装置７０３は、高速ＲＡＭ記憶装置を備えてもよく、さらに不揮発性メモリ（ｎｏｎ－ｖｏｌａｔｉｌｅ　ｍｅｍｏｒｙ）、たとえば少なくとも１つのディスク記憶装置を含んでもよい。

【００７７】

前記通信インターフェース７０２は、これら装置間の接続通信を実施する。

【００７８】

前記プロセッサ７０１はプログラムコードを実行し、前記プログラムコードは、実行されると、

ユーザ装置が送信した、ユーザアイデンティティ情報を含むアクセス要求メッセージを受信する方法と、

前記ユーザアイデンティティ情報に基づいて、ブロックチェーンにおいてユーザのアイデンティティ確認情報及び認可情報を問い合わせる方法と、

前記アイデンティティ確認情報に基づいて、前記ユーザに対してアイデンティティ認証を行う方法と、

認証に通過した後、前記認可情報に基づいて、前記ユーザによる指定サービスへのアクセスを許可する方法とを実現する。

【００７９】

前記ユーザアイデンティティ情報に基づいて、ブロックチェーンにおいてユーザのアイデンティティ確認情報及び認可情報を問い合わせる前記方法は、
前記ユーザアイデンティティ情報に基づいて、前記ブロックチェーンにおいて前記ユーザのアイデンティティ確認情報及び認可情報を記憶した複数のブロックが検出されたとき、前記複数のブロックのうち、最新ブロックから前記ユーザのアイデンティティ確認情報及び認可情報を取得することを含むようにしてもよい。

【００８０】

前記アイデンティティ確認情報はパスワードハッシュ値の暗号文であり、前記ユーザアイデンティティ情報はパスワードを含み、前記アイデンティティ確認情報に基づいて、前記ユーザに対してアイデンティティ認証を行う前記方法は、
前記ユーザアイデンティティ情報のハッシュ値を計算するステップと、
前記ユーザアイデンティティ情報を復号して、復号して得られた平文が前記ユーザアイデンティティ情報の平文と一致すると、認証に通過したと決定するステップとを含むようにしてもよい。

【００８１】

前記アイデンティティ確認情報はユーザ公開鍵であり、前記アイデンティティ確認情報に基づいて、前記ユーザに対してアイデンティティ認証を行う前記方法は、
前記ユーザにアイデンティティ確認を提供するように指示するための指示情報を前記ユーザ装置に送信するステップと、
前記ユーザ装置が前記指示情報に基づいて送信したユーザ秘密鍵で署名した署名情報を受信するステップと、
前記ユーザ公開鍵に基づいて前記署名情報に対して署名認証を行い、署名認証に成功すると、アイデンティティ認証に通過したと決定するステップとを含むようにしてもよい。

【００８２】

本発明の実施例はさらに認可システム８０を提供し、前記認可システム８０は認可サーバ６０とアクセスサーバ７０を含み、前記認可サーバ６０はブロックチェーンネットワークにおけるノードであり、前記アクセスサーバ７０はブロックチェーンネットワークにおけるノードであり、前記アクセスサーバ５０はネットワークサービスを提供するサーバに接続される。前記認可サーバ６０は、具体的には、上記図６の説明を参照すればよいため、ここで詳細な説明を省略する。前記アクセスサーバ７０は、具体的には、上記図７の説明を参照すればよいため、ここで詳細な説明を省略する。

【００８３】

なお、本願による複数の実施例では、開示されているシステム、装置及び方法は、ほかの形態によっても実現できる。たとえば、以上に説明した装置の実施例は例示的なものに過ぎず、たとえば、前記ユニットの分割は、ロジック機能に応じた分割だけであり、実際に実施されるときに、別の分割方式を用いてもよく、たとえば複数のユニット又はモジュールが、別のシステムに結合又は集積されてもよく、又は一部の特徴を無視にしたり又は実行しないようにしてもよい。また、表示又は検討した相互結合又は直接結合又は通信接続は一部のインターフェース、装置又はユニットを介した間接的な結合又は通信接続であってもよく、電気的、機械的又はほかの形としてもよい。

【００８４】

分離した部材として説明された前記ユニットは物理的に分離してもよく、物理的に分離しなくてもよく、ユニットとして表示される部材は物理ユニットであってもよく、物理ユニットでなくてもよく、すなわち、１つの位置に位置してもよく、又は複数のネットワークユニットに分布してもよい。必要に応じて、そのうちの一部又はすべてのユニットを用いて本実施例の形態を実現できる。

【００８５】

さらに、本発明の各実施例では、各機能ユニットが１つの処理ユニットに集積されてもよく、各ユニットが独立して物理的に存在してもよく、２つ又は２つ以上のユニットが１つのユニットに集積されてもよい。上記集積されたユニットはハードウェアの形態として

実現されてもよいし、ハードウェアとソフトウェア機能ユニットを組み合わせた形態として実現されてもよい。

【００８６】

上記はソフトウェア機能ユニットの形態として実現された集積ユニットは、１つのコンピュータリーダブル記憶媒体に記憶してもよい。上記ソフトウェア機能ユニットは、記憶媒体に記憶されて、コンピュータ装置（パーソナルコンピュータ、サーバ、又はネットワーク装置等）に本発明の各実施例の前記方法の一部のステップを実行させるいくつかのコマンドを含む。前述記憶媒体には、ＵＳＢメモリ、モバイルハードディスク、ランダムアクセスメモリ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ、　ＲＡＭ）、磁気ディスク又は光ディスクなどのデータ記憶可能な各種媒体が含まれる。

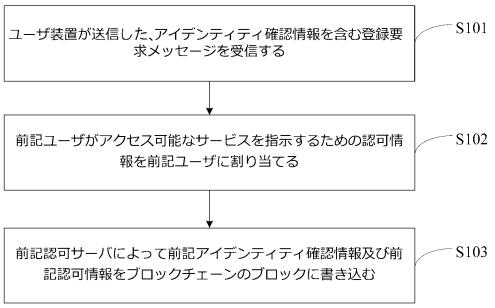
【００８７】

以上は、本発明の実施形態に過ぎず、本発明の保護範囲はそれらに制限されず、当業者であれば、本発明で開示されている技術範囲を逸脱せずに容易に想到し得る変化又は置換はすべて本発明の保護範囲に含まれる。従って、本発明の保護範囲は特許請求の範囲による保護範囲を基準にする。

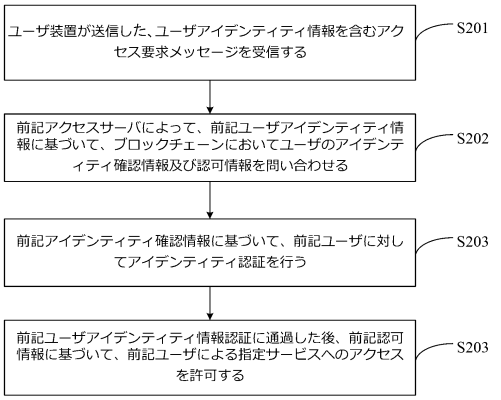
【要約】

従来の認可技術のセキュリティが低い技術的問題を解決するための登録・認可方法、装置及びシステムを提供する。前記方法は、認可サーバに適用され、前記認可サーバは、ブロックチェーンネットワークにおけるノードであり、それぞれ認可情報を記憶するための複数ブロックからなるブロックチェーンを記憶しており、前記方法は、ユーザ装置が送信した、ユーザに対してアイデンティティ認証を行うためのアイデンティティ確認情報を含む登録要求メッセージを受信するステップと、前記ユーザがアクセス可能なサービスを指示するための認可情報を前記ユーザに割り当てるステップと、前記認可サーバによって前記アイデンティティ確認情報及び前記認可情報をブロックチェーンのブロックに書き込むステップとを含む。

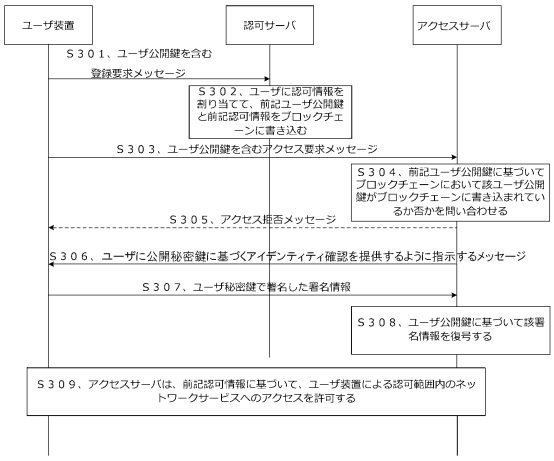
【図１】



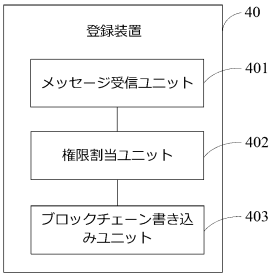
【図２】



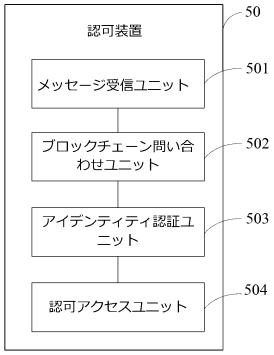
【図３】



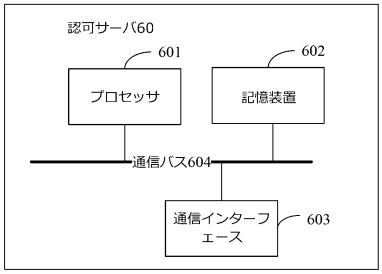
【図４】



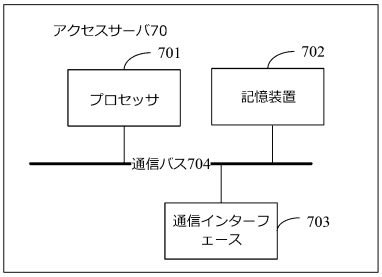
【図５】


認可装置
50
メッセージ受信ユニット
501
ブロックチェーン問い合わせユニット
502
アイデンティティ認証ユニット
503
認可アクセスユニット
504

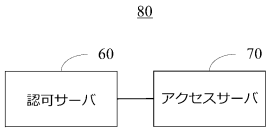
【図６】


認可サーバ60
601
602
プロセッサ
記憶装置
通信バス604
通信インターフェース
603

【図７】


アクセスサーバ70
701
702
プロセッサ
記憶装置
通信バス704
通信インターフェース
703

【図８】


80
60
70
認可サーバ
アクセスサーバ

フロントページの続き

(73)特許権者 518409575
深▲セン▼前▲海▼▲達▼▲闥▼▲雲▼端智能科技有限公司
ＣＬＯＵＤＭＩＮＤＳ （ＳＨＥＮＺＨＥＮ） ＲＯＢＯＴＩＣＳ ＳＹＳＴＥＭＳ ＣＯ．，ＬＴＤ．
中国５１８０００▲広▼▲東▼省深▲セン▼市前▲海▼深▲港▼合作区前湾一路１号Ａ▲棟▼２０１室 （入▲駐▼深▲セン▼市前▲海▼商▲務▼秘▲書▼有限公司）
ＲＯＯＭ ２０１， ＢＬＯＣＫ Ａ， ＮＯ．１， ＱＩＡＮＷＡＮ ＲＯＡＤ １， ＱＩＡＮＨＡＩＳＨＥＮ ＰＯＲＴ ＣＯＯＰＥＲＡＴＩＶＥ ＤＩＳＴＲＩＣＴ （ＳＥＴＴＬＥＤ ＩＮ ＳＨＥＮＺＨＥＮ ＱＩＡＮＨＡＩ ＢＵＳＩＮＥＳＳ ＳＥＣＲＥＴＡＲＹ ＣＯ．，ＬＴＤ．） ＳＨＥＮＺＨＥＮ， ＧＵＡＮＧＤＯＮＧ ５１８０００， ＣＨＩＮＡ
(74)代理人 110001818
特許業務法人Ｒ＆Ｃ
(72)発明者 謝 輝
中国５１８０００▲広▼▲東▼省深▲セン▼市前▲海▼深▲港▼合作区前湾一路１号Ａ▲棟▼２０１室 （入▲駐▼深▲セン▼市前▲海▼商▲務▼秘▲書▼有限公司）
(72)発明者 王 健
中国５１８０００▲広▼▲東▼省深▲セン▼市前▲海▼深▲港▼合作区前湾一路１号Ａ▲棟▼２０１室 （入▲駐▼深▲セン▼市前▲海▼商▲務▼秘▲書▼有限公司）

審査官 和平 悠希

(56)参考文献 特開２０１８－０５５２０３（ＪＰ，Ａ）
米国特許出願公開第２０１４／０２７０４０１（ＵＳ，Ａ１）
中国特許出願公開第１０５７０１３７２（ＣＮ，Ａ）
国際公開第２０１６／０９００９５（ＷＯ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／３１
Ｇ０６Ｑ ２０／０２