(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6716745号
(P6716745)
(45)発行日　令和2年7月1日(2020.7.1)　(24)登録日　令和2年6月12日(2020.6.12)

(51)Int.Cl.　　F I
G06F 21/33 (2013.01)　　G06F 21/33
H04L 9/32 (2006.01)　　H04L 9/00 675D
H04L 9/00 675B

請求項の数 20　(全 29 頁)

(21)出願番号　特願2019-68034(P2019-68034)
(22)出願日　平成31年3月29日(2019.3.29)
(65)公開番号　特開2019-185775(P2019-185775A)
(43)公開日　令和1年10月24日(2019.10.24)
審査請求日　平成31年3月29日(2019.3.29)
(31)優先権主張番号　10-2018-0037131
(32)優先日　平成30年3月30日(2018.3.30)
(33)優先権主張国・地域又は機関
韓国(KR)

(73)特許権者　519112601
株式会社コインプラグ
Ｃｏｉｎｐｌｕｇ，Ｉｎｃ．
大韓民国　１３５２９　ギョンギド　ソン
ナムシ　ブンダング　パンギョヨクロ　１
４６ボンギル　２０、１１階
(74)代理人　100121728
弁理士　井関　勝守
(74)代理人　100165803
弁理士　金子　修平
(74)代理人　100170900
弁理士　大西　渉

最終頁に続く

(54)【発明の名称】ブロックチェーン基盤の権限認証方法、端末及びこれを利用したサーバ

(57)【特許請求の範囲】
【請求項１】
ブロックチェーン基盤の権限認証方法において、
（ａ）ユーザ端末の認証提携局アプリケーションからの検証確認値を含む認証要請情報に対応した前記ユーザ端末の認証局アプリケーションから電子署名値に対する電子署名値検証要請情報‐前記電子署名値検証要請情報は少なくとも前記検証確認値と前記検証確認値を前記認証局アプリケーションのプライベートキーを用いて電子署名した前記電子署名値を含む‐が獲得されると、認証支援サーバが、（ｉ）前記電子署名値を検証するように支援して、前記電子署名値が有効であると確認されるとアクセストークンを生成して前記ユーザ端末に転送するようにすることで前記ユーザ端末をもって前記認証局アプリケーションを介して前記アクセストークンを受信して前記アクセストークンを保存するようにして前記認証提携局アプリケーションを介して前記アクセストークンを利用して認証提携局サーバにログインを要請するように支援し、前記アクセストークンをブロックチェーンに登録するように支援するか、（ｉｉ）前記ブロックチェーンに前記電子署名値に対する検証を要請するようにすることで前記ブロックチェーンをもって前記電子署名値が有効であると確認されるとアクセストークンを生成して前記認証支援サーバに転送するようにして、前記アクセストークンを前記ブロックチェーンに登録するようにし、前記ブロックチェーンから前記アクセストークンが獲得されると前記アクセストークンを前記ユーザ端末に転送することで前記ユーザ端末をもって前記認証局アプリケーションを介して前記アクセストークンを受信して前記アクセストークンを保存するようにして前記認証提携局アプリ

ケーションを介して前記アクセストークンを利用して認証提携局サーバにログインを要請するように支援する段階と、
（ｂ）少なくとも前記アクセストークンを含むアクセストークン検証要請情報が前記認証提携局サーバから獲得されるか前記認証提携局サーバからの前記アクセストークン検証要請情報が認証局サーバを介して獲得されると、前記認証支援サーバが、（ｉ）前記アクセストークンを検証するようにするか、（ｉｉ）前記ブロックチェーンに前記アクセストークンに対する検証を要請するようにすることで前記ブロックチェーンをもって前記アクセストークンを検証するように支援して、前記アクセストークンが有効であると確認されると、アクセストークン検証結果情報を前記認証提携局サーバに転送するか前記認証局サーバを介して前記アクセストークン検証結果情報が認証提携局サーバに転送されるようにすることで前記認証提携局サーバをもってアクセストークン検証結果に対応して前記ユーザ端末の前記認証提携局アプリケーションを介した前記認証提携局サーバへのログインを許容するように支援する段階と、
を含むことを特徴とする方法。
【請求項２】
前記（ａ）段階で、
前記認証支援サーバは、前記認証局アプリケーションに対応されるパブリックキーを利用して前記電子署名値の署名に使用された検証確認値である電子署名検証確認値を確認して、前記確認された電子署名検証確認値が前記電子署名値検証要請情報に含まれた前記検証確認値と一致するか否かを確認することで前記電子署名値を検証するか、前記ブロックチェーンをもって前記認証局アプリケーションに対応されるパブリックキーを利用して前記電子署名値の署名に用いられた前記電子署名検証確認値を確認して、前記確認された電子署名検証確認値が前記電子署名値検証要請情報に含まれた前記検証確認値と一致するか否かを確認して前記電子署名値を検証するようにすることを特徴とする請求項１に記載の方法。
【請求項３】
前記アクセストークンはユーザ端末識別情報、及びユーザ識別情報のうち少なくとも一つ以上を含むか、前記ユーザ端末識別情報と前記ユーザ識別情報の関数値のうち少なくとも一つ以上を含むことを特徴とする請求項１に記載の方法。
【請求項４】
前記（ａ）段階で、
前記ユーザ端末の前記認証提携局アプリケーションから前記認証提携局サーバへのログイン要請には前記アクセストークン、ユーザ端末識別情報、及びユーザ識別情報のうち少なくとも一つ以上が含まれていることを特徴とする請求項１に記載の方法。
【請求項５】
前記（ｂ）段階で、
前記認証支援サーバは、前記認証提携局サーバをもって前記アクセストークン検証結果情報に対応して前記アクセストークンを前記認証提携局サーバに連動される記憶装置に保存するようにすることを特徴とする請求項１に記載の方法。
【請求項６】
前記（ｂ）段階で、
前記アクセストークン検証結果情報にユーザ端末識別情報、及びユーザ識別情報のうち少なくとも一つ以上をさらに含むことを特徴とする請求項５に記載の方法。
【請求項７】
前記（ｂ）段階で、
前記認証支援サーバは、前記アクセストークン検証結果情報にユーザ情報を加えて前記認証提携局サーバに転送するか前記認証局サーバをもって前記アクセストークン検証結果情報に前記ユーザ情報を加えて前記認証提携局サーバに転送するようにすることを特徴とする請求項５に記載の方法。
【請求項８】

ブロックチェーン基盤の権限認証方法において、
（ａ）ユーザ端末の認証提携局アプリケーションからの検証確認値を含む認証要請情報に対応した前記ユーザ端末の認証局アプリケーションから電子署名値に対する電子署名値検証要請情報が獲得されると前記電子署名値を検証するかブロックチェーンをもって前記電子署名値を検証するようにして、前記電子署名値の有効な結果に対応されてアクセストークンが生成されると前記アクセストークンを前記ブロックチェーンに登録されるようにして前記アクセストークンを前記ユーザ端末に転送されるようにすることで前記ユーザ端末をもって前記認証局アプリケーションを介して前記アクセストークンを受信して前記アクセストークンを保存するようにした状態で、前記ユーザ端末の前記認証提携局アプリケーションからの前記アクセストークンを利用したログイン要請に対応して前記アクセストークンを含むアクセストークン検証要請情報が認証提携局サーバから獲得されるか前記認証提携局サーバからの前記アクセストークン検証要請情報が認証局サーバを介して獲得されると、前記認証支援サーバが、（ｉ）前記アクセストークンを検証するようにするか、（ｉｉ）前記ブロックチェーンに前記アクセストークンに対する検証を要請するようにすることで前記ブロックチェーンをもって前記アクセストークンを検証するように支援する段階と、
（ｂ）前記アクセストークンが有効であると確認されると、前記認証支援サーバが、アクセストークン検証結果情報を認証提携局サーバに転送するようにすることで前記認証提携局サーバをもってアクセストークン検証結果に対応して前記ユーザ端末の前記認証提携局アプリケーションを介した前記認証提携局サーバへのログインを許容するように支援する段階と、
を含むことを特徴とする方法。
【請求項９】
前記（ａ）段階で、
前記アクセストークン検証要請情報は、（ｉ）前記ユーザ端末の前記認証提携局アプリケーションによる検証確認値を含む認証要請情報に対応して前記ユーザ端末の前記認証局アプリケーションを介した状態を確認して、（ｉ‐１）前記認証局アプリケーションがログイン状態である場合には、前記ユーザ端末の前記認証局アプリケーションが前記保存された前記アクセストークンを前記ユーザ端末の認証提携局アプリケーションに転送し、（ｉ‐２）前記認証局アプリケーションがログイン状態でない場合には、前記認証局アプリケーションが電子署名値に対する電子署名値検証要請情報‐前記電子署名値検証要請情報は少なくとも前記検証確認値と前記検証確認値を前記認証局アプリケーションのプライベートキーを用いて電子署名した前記電子署名値を含む‐を認証支援サーバに転送して、認証支援サーバが前記電子署名値を検証するか前記ブロックチェーンを介して前記電子署名値を検証するようにして、前記認証支援サーバから前記電子署名値が有効であると確認されると前記認証局アプリケーションが前記保存された前記アクセストークンを前記認証提携局アプリケーションに転送し、（ｉｉ）前記認証提携局アプリケーションからの前記アクセストークンを利用したログイン要請に対応して前記認証提携局サーバが生成することを特徴とする請求項８に記載の方法。
【請求項１０】
ブロックチェーン基盤の権限認証方法において、
（ａ）ユーザ端末が、認証提携局アプリケーションからの検証確認値を含む認証要請情報に対応して認証局アプリケーションを介して電子署名値に対する電子署名値検証要請情報‐前記電子署名値検証要請情報は少なくとも前記検証確認値と前記検証確認値を前記認証局アプリケーションのプライベートキーを用いて電子署名した前記電子署名値を含む‐を認証支援サーバに転送するようにすることで前記認証支援サーバをもって（ｉ）前記電子署名値を検証するように支援して、前記電子署名値が有効であると確認されるとアクセストークンを生成し、前記アクセストークンをブロックチェーンに登録するように支援して、前記アクセストークンを前記ユーザ端末に転送するように支援するようにするか、（ｉｉ）前記ブロックチェーンに前記電子署名値に対する検証を要請するようにし、前記ブ

ロックチェーンを介して前記電子署名値が有効であると確認されると前記アクセストークンを生成して前記ブロックチェーンに登録するようにして、前記アクセストークンを前記認証支援サーバに転送するようにして、前記ブロックチェーンから前記アクセストークンが獲得されると前記アクセストークンを前記ユーザ端末に転送するように支援するようにする段階と、

（ｂ）前記認証局アプリケーションを介して前記アクセストークンが獲得されると、前記ユーザ端末が、前記アクセストークンを保存し、前記認証提携局アプリケーションを介して前記アクセストークンを利用して認証提携局サーバにログインを要請するようにすることで前記認証提携局サーバをもって、（ｉ）少なくとも前記アクセストークンを含むアクセストークン検証要請情報を前記認証支援サーバに転送するように支援するか認証局サーバを介して前記アクセストークン検証要請情報が前記認証支援サーバに転送されるように支援して前記認証支援サーバを介して（ｉ‐１）前記アクセストークンを検証するようにするか、（ｉ‐２）前記ブロックチェーンに前記アクセストークンに対する検証を要請するように支援して、（ｉｉ）前記アクセストークンが有効であると確認されてアクセストークン検証結果情報が前記認証支援サーバまたは前記認証局サーバを介して獲得されるとアクセストークン検証結果に対応して前記ユーザ端末の前記認証提携局アプリケーションを介した前記認証提携局サーバへのログインを許容するように支援する段階と、

を含むことを特徴とする方法。

【請求項１１】

ブロックチェーン基盤の権限認証方法において、

（ａ）ユーザ端末の認証提携局アプリケーションからの検証確認値を含む認証要請情報に対応した前記ユーザ端末の認証局アプリケーションから電子署名値に対する電子署名値検証要請情報が獲得されると前記電子署名値を検証するかブロックチェーンをもって前記電子署名値を検証するようにして、前記電子署名値の有効な結果に対応されてアクセストークンが生成されると前記アクセストークンを前記ブロックチェーンに登録されるようにして前記アクセストークンを前記ユーザ端末に転送されるようにすることで前記ユーザ端末をもって前記認証局アプリケーションを介して前記アクセストークンを受信して前記アクセストークンを保存するようにした状態で、ユーザ端末が、前記認証提携局アプリケーションによる検証確認値を含む認証要請情報に対応して前記認証局アプリケーションを介したログイン状態を確認して、（ｉ）前記認証局アプリケーションがログイン状態である場合には、前記ユーザ端末の前記認証局アプリケーションが前記保存された前記アクセストークンを前記ユーザ端末の認証提携局アプリケーションに転送し、（ｉｉ）前記認証局アプリケーションがログイン状態でない場合には、前記認証局アプリケーションが電子署名値に対する電子署名値検証要請情報‐前記電子署名値検証要請情報は少なくとも前記検証確認値と前記検証確認値を前記認証局アプリケーションのプライベートキーを用いて電子署名した前記電子署名値を含む‐を認証支援サーバに転送して、認証支援サーバをもって前記電子署名値を検証するか前記ブロックチェーンを介して前記電子署名値を検証するように支援して、前記認証支援サーバから前記電子署名値が有効であると確認されると前記認証局アプリケーションが前記保存された前記アクセストークンを前記認証提携局アプリケーションに転送する段階と、

（ｂ）前記ユーザ端末が、前記認証提携局アプリケーションを介して前記アクセストークンを利用したログイン要請を認証提携局サーバに転送するようにすることで前記認証提携局サーバをもって、（ｉ）少なくとも前記アクセストークンを含むアクセストークン検証要請情報を前記認証支援サーバに転送するように支援するか認証局サーバを介して前記アクセストークン検証要請情報が前記認証支援サーバに転送されるように支援して前記認証支援サーバを介して（ｉ‐１）前記アクセストークンを検証するようにするか、（ｉ‐２）前記ブロックチェーンに前記アクセストークンに対する検証を要請するように支援して、（ｉｉ）前記アクセストークンが有効であると確認されてアクセストークン検証結果情報が前記認証支援サーバまたは前記認証局サーバを介して獲得されるとアクセストークン検証結果に対応して前記ユーザ端末の前記認証提携局アプリケーションを介した前記認

証提携局サーバへのログインを許容するように支援する段階と、
を含むことを特徴とする方法。
【請求項１２】
ブロックチェーン基盤の権限認証を遂行する認証支援サーバにおいて、
ユーザ端末の認証提携局アプリケーションからの検証確認値を含む認証要請情報に対応した前記ユーザ端末の認証局アプリケーションから電子署名値に対する電子署名値検証要請情報‐前記電子署名値検証要請情報は少なくとも前記検証確認値と前記検証確認値を前記認証局アプリケーションのプライベートキーを用いて電子署名した前記電子署名値を含む‐を獲得する通信部と、
前記通信部を介して獲得される前記電子署名値検証要請情報に対応して、（ｉ）前記電子署名値を検証するように支援して、前記電子署名値が有効であると確認されるとアクセストークンを生成して前記ユーザ端末に転送するようにすることで前記ユーザ端末をもって前記認証局アプリケーションを介して前記アクセストークンを受信して前記アクセストークンを保存するようにして前記認証提携局アプリケーションを介して前記アクセストークンを利用して認証提携局サーバにログインを要請するように支援し、前記アクセストークンをブロックチェーンに登録するように支援するか、（ｉｉ）前記ブロックチェーンに前記電子署名値に対する検証を要請するようにすることで前記ブロックチェーンをもって前記電子署名値が有効であると確認されるとアクセストークンを生成して前記認証支援サーバに転送するようにして、前記アクセストークンを前記ブロックチェーンに登録するようにし、前記ブロックチェーンから前記アクセストークンが獲得されると前記アクセストークンを前記ユーザ端末に転送するようにすることで前記ユーザ端末をもって前記認証局アプリケーションを介して前記アクセストークンを受信して前記アクセストークンを保存するようにして前記認証提携局アプリケーションを介して前記アクセストークンを利用して認証提携局サーバにログインを要請するように支援する第１プロセス、少なくとも前記アクセストークンを含むアクセストークン検証要請情報が前記認証提携局サーバから獲得されるか前記認証提携局サーバからの前記アクセストークン検証要請情報が認証局サーバを介して獲得されると、（ｉ）前記アクセストークンを検証するか、（ｉｉ）前記ブロックチェーンに前記アクセストークンに対する検証を要請することで前記ブロックチェーンをもって前記アクセストークンを検証するように支援して、前記アクセストークンが有効であると確認されると、アクセストークン検証結果情報を前記認証提携局サーバに転送するか前記認証局サーバを介して前記アクセストークン検証結果情報が前記認証提携局サーバに転送されるようにすることで前記認証提携局サーバをもってアクセストークン検証結果に対応して前記ユーザ端末の前記認証提携局アプリケーションを介した前記認証提携局サーバへのログインを許容するように支援する第２プロセスを遂行するプロセッサと、
を含むことを特徴とする認証支援サーバ。
【請求項１３】
前記プロセッサは、
前記第１プロセスで、
前記認証局アプリケーションに対応されるパブリックキーを利用して前記電子署名値の署名に用いられた検証確認値である電子署名検証確認値を確認して、前記確認された電子署名検証確認値が前記電子署名値検証要請情報に含まれた前記検証確認値と一致するか否かを確認することで前記電子署名値を検証するか、前記ブロックチェーンをもって前記認証局アプリケーションに対応されるパブリックキーを利用して前記電子署名値の署名に用いられた前記電子署名検証確認値を確認して、前記確認された電子署名検証確認値が前記電子署名値検証要請情報に含まれた前記検証確認値と一致するか否かを確認して前記電子署名値を検証するようにすることを特徴とする請求項１２に記載の認証支援サーバ。
【請求項１４】
前記アクセストークンはユーザ端末識別情報、及びユーザ識別情報のうち少なくとも一つ以上を含むか、前記ユーザ端末識別情報と前記ユーザ識別情報の関数値のうち少なくとも一つ以上を含むことを特徴とする請求項１２に記載の認証支援サーバ。

【請求項１５】
前記ユーザ端末の前記認証提携局アプリケーションから前記認証提携局サーバへのログイン要請には前記アクセストークン、ユーザ端末識別情報、及びユーザ識別情報のうち少なくとも一つ以上が含まれていることを特徴とする請求項１２に記載の認証支援サーバ。
【請求項１６】
前記プロセッサは、
前記認証提携局サーバをもって前記アクセストークン検証結果情報に対応して前記アクセストークンを前記認証提携局サーバに連動される記憶装置に保存するようにすることを特徴とする請求項１２に記載の認証支援サーバ。
【請求項１７】
ブロックチェーン基盤の権限認証を遂行する認証支援サーバにおいて、
ユーザ端末の認証提携局アプリケーションからの検証確認値を含む認証要請情報に対応した前記ユーザ端末の認証局アプリケーションから電子署名値に対する電子署名値検証要請情報が獲得されると前記電子署名値を検証するかブロックチェーンをもって前記電子署名値を検証するようにして、前記電子署名値の有効な結果に対応されてアクセストークンが生成されると前記アクセストークンを前記ブロックチェーンに登録されるようにして前記アクセストークンを前記ユーザ端末に転送されるようにすることで前記ユーザ端末をもって前記認証局アプリケーションを介して前記アクセストークンを受信して前記アクセストークンを保存するようにした状態で、前記ユーザ端末の前記認証提携局アプリケーションからの前記アクセストークンを利用したログイン要請に対応して前記アクセストークンを含むアクセストークン検証要請情報を認証提携局サーバから獲得するか前記認証提携局サーバからの前記アクセストークン検証要請情報を認証局サーバを介して獲得する通信部と、
前記通信部を介して獲得される前記アクセストークン検証要請情報に対応して、（ｉ）前記アクセストークンを検証するか、（ｉｉ）前記ブロックチェーンに前記アクセストークンに対する検証を要請するようにすることで前記ブロックチェーンをもって前記アクセストークンを検証するように支援する第１プロセス、前記アクセストークンが有効であると確認されると、アクセストークン検証結果情報を前記認証提携局サーバに転送するか前記認証局サーバを介して前記アクセストークン検証結果情報が前記認証提携局サーバに転送されるようにすることで前記認証提携局サーバをもってアクセストークン検証結果に対応して前記ユーザ端末の前記認証提携局アプリケーションを介した前記認証提携局サーバへのログインを許容するように支援する第２プロセスを遂行するプロセッサと、
を含むことを特徴とする認証支援サーバ。
【請求項１８】
前記アクセストークン検証要請情報は、（ｉ）前記ユーザ端末の前記認証提携局アプリケーションによる検証確認値を含む認証要請情報に対応して前記ユーザ端末の前記認証局アプリケーションを介したログイン状態を確認して、（ｉ‐１）前記認証局アプリケーションがログイン状態である場合には、前記ユーザ端末の前記認証局アプリケーションが前記保存された前記アクセストークンを前記ユーザ端末の認証提携局アプリケーションに転送し、（ｉ‐２）前記認証局アプリケーションがログイン状態でない場合には、前記認証局アプリケーションが電子署名値に対する電子署名値検証要請情報‐前記電子署名値検証要請情報は少なくとも前記検証確認値と前記検証確認値を前記認証局アプリケーションのプライベートキーを用いて電子署名した前記電子署名値を含む‐を認証支援サーバに転送して、認証支援サーバが前記電子署名値を検証するか前記ブロックチェーンを介して前記電子署名値を検証するようにして、前記認証支援サーバから前記電子署名値が有効であると確認されると前記認証局アプリケーションが前記保存された前記アクセストークンを前記認証提携局アプリケーションに転送し、（ｉｉ）前記認証提携局アプリケーションからの前記アクセストークンを利用したログイン要請に対応して前記認証提携局サーバが生成することを特徴とする請求項１７に記載の認証支援サーバ。
【請求項１９】

ブロックチェーン基盤の権限認証を遂行するユーザ端末において、
通信部と、
認証提携局アプリケーションからの検証確認値を含む認証要請情報に対応して認証局アプリケーションを介して電子署名値に対する電子署名値検証要請情報‐前記電子署名値検証要請情報は少なくとも前記検証確認値と前記検証確認値を前記認証局アプリケーションのプライベートキーを用いて電子署名した前記電子署名値を含む‐を前記通信部を介して認証支援サーバに転送するようにすることで前記認証支援サーバをもって（ｉ）前記電子署名値を検証するように支援して、前記電子署名値が有効であると確認されるとアクセストークンを生成し、前記アクセストークンをブロックチェーンに登録するように支援して、前記アクセストークンを前記ユーザ端末に転送するように支援するようにするか、（ｉｉ）前記ブロックチェーンに前記電子署名値に対する検証を要請するようにし、前記ブロックチェーンを介して前記電子署名値が有効であると確認されると前記アクセストークンを生成して前記ブロックチェーンに登録するようにして、前記アクセストークンを前記認証支援サーバに転送するようにして、前記ブロックチェーンから前記アクセストークンが獲得されると前記アクセストークンを前記ユーザ端末に転送するように支援するようにする第１プロセス、前記通信部を介して前記認証局アプリケーションを介して前記アクセストークンが獲得されると前記アクセストークンを保存し、前記認証提携局アプリケーションを介して前記アクセストークンを利用して認証提携局サーバにログインを要請するようにすることで前記認証提携局サーバをもって、（ｉ）少なくとも前記アクセストークンを含むアクセストークン検証要請情報を前記認証支援サーバに転送するように支援するか認証局サーバを介して前記アクセストークン検証要請情報が前記認証支援サーバに転送されるように支援して前記認証支援サーバを介して（ｉ‐１）前記アクセストークンを検証するか、（ｉ‐２）前記ブロックチェーンに前記アクセストークンに対する検証を要請するように支援して、（ｉｉ）前記アクセストークンが有効であると確認されてアクセストークン検証結果情報が前記認証支援サーバまたは前記認証局サーバを介して獲得されるとアクセストークン検証結果に対応して前記ユーザ端末の前記認証提携局アプリケーションを介した前記認証提携局サーバへのログインを許容するように支援する第２プロセスを遂行するプロセッサと、
を含むことを特徴とするユーザ端末。

【請求項２０】
ブロックチェーン基盤の権限認証を遂行するユーザ端末において、
通信部と、
ユーザ端末の認証提携局アプリケーションからの検証確認値を含む認証要請情報に対応した前記ユーザ端末の認証局アプリケーションから電子署名値に対する電子署名値検証要請情報が獲得されると前記電子署名値を検証するかブロックチェーンをもって前記電子署名値を検証するようにして、前記電子署名値の有効な結果に対応されてアクセストークンが生成されると前記アクセストークンを前記ブロックチェーンに登録されるようにして前記アクセストークンを前記ユーザ端末に転送されるようにすることで前記ユーザ端末をもって前記認証局アプリケーションを介して前記アクセストークンを受信して前記アクセストークンを保存するようにした状態で、前記認証提携局アプリケーションによる検証確認値を含む認証要請情報に対応して前記認証局アプリケーションを介したログイン状態を確認して、（ｉ）前記認証局アプリケーションがログイン状態である場合には、前記ユーザ端末の前記認証局アプリケーションが前記保存された前記アクセストークンを前記ユーザ端末の認証提携局アプリケーションに転送し、（ｉｉ）前記認証局アプリケーションがログイン状態でない場合には、前記認証局アプリケーションが電子署名値に対する電子署名値検証要請情報‐前記電子署名値検証要請情報は少なくとも前記検証確認値と前記検証確認値を前記認証局アプリケーションのプライベートキーを用いて電子署名した前記電子署名値を含む‐を前記通信部を介して認証支援サーバに転送して、認証支援サーバをもって前記電子署名値を検証するか前記ブロックチェーンを介して前記電子署名値を検証するように支援して、前記認証支援サーバから前記電子署名値が有効であると確認されると前記

認証局アプリケーションが前記保存された前記アクセストークンを前記通信部を介して前記認証提携局アプリケーションに転送する第１プロセス、前記認証提携局アプリケーションを介して前記アクセストークンを利用したログイン要請を前記通信部を介して認証提携局サーバに転送するようにすることで前記認証提携局サーバをもって、（ｉ）少なくとも前記アクセストークンを含むアクセストークン検証要請情報を前記認証支援サーバに転送するように支援するか認証局サーバを介して前記アクセストークン検証要請情報が前記認証支援サーバに転送されるように支援して前記認証支援サーバを介して（ｉ‐１）前記アクセストークンを検証するようにするか、（ｉ‐２）前記ブロックチェーンに前記アクセストークンに対する検証を要請するように支援して、（ｉｉ）前記アクセストークンが有効であると確認されてアクセストークン検証結果情報が前記認証支援サーバまたは前記認証局サーバを介して獲得されるとアクセストークン検証結果に対応して前記ユーザ端末の前記認証提携局アプリケーションを介した前記認証提携局サーバへのログインを許容するように支援する第２プロセスを遂行するプロセッサと、

を含むことを特徴とするユーザ端末。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明はブロックチェーン基盤の権限認証方法、端末及びこれを利用したサーバに関し、より詳細には、ユーザ端末の認証提携局アプリケーションからの検証確認値を含む認証要請情報に対応した認証局アプリケーションから電子署名値に対する電子署名値検証要請情報を獲得し、電子署名値を検証して有効であると確認されるとアクセストークンを生成してユーザ端末に転送されるようにすることで認証提携局アプリケーションをもってアクセストークンを保存するようにして、アクセストークンを利用して認証提携局サーバにログインを要請するように支援し、アクセストークンをブロックチェーンに登録して、アクセストークンを含むアクセストークン検証要請情報が認証提携局サーバから獲得されると、アクセストークンを検証して有効である場合、アクセストークン検証結果情報を認証提携局サーバに転送することで前記認証提携局サーバをもってアクセストークン検証結果に対応してユーザ端末の認証提携局アプリケーションを介した認証提携局サーバへのログインを許容するように支援するブロックチェーン基盤の権限認証方法、端末及びこれを利用したサーバに関する。

【背景技術】

【０００２】

ＯＡｕｔｈは一つのＯｐｅｎＩＤに基づいて、複数のウェブサイトまたは応用プログラム（ａｐｐｌｉｃａｔｉｏｎ）に認証を遂行することができるように開発された標準認証方式であり、ＯＡｕｔｈプロトコルは別途の認証手順なしで応用プログラム同士で認証を共有することができる。即ち、ＯＡｕｔｈプロトコルはクライアントの識別子や証明書を公開せずにウェブサイトや応用プログラムでリソースに対するアクセス権限を付与されるためのプロトコルである。

【０００３】

そして、ＯＡｕｔｈは２００７年１２月、ＯＡｕｔｈ　ｃｏｒｅ１．０から最近ＯＡｕｔｈ２．０までクライアントごとにアクセス権限を設定し、クライアントの情報をサードパーティに露出不可能にする方法などを改正しており、ＯＡｕｔｈプロトコルは認証サーバから発給されたトークンを利用してリソースサーバにあるリソースに対するアクセス権限を獲得することができる。

【０００４】

しかし、現在制定されたＯＡｕｔｈプロトコル標準ではクライアントが使用することができるトークンの回数に対する制限が明確でない。

【０００５】

従って、ＯＡｕｔｈプロトコルでは正常的にトークンを獲得した悪意のあるクライアントがリソースサーバに数回アクセスして悪意のある行動を試みる場合がある。

【０００６】
特に、従来のＯＡｕｔｈではユーザの認証情報が攻撃者によって奪取される場合、ＯｐｅｎＩＤと関連したすべての提携サービスに攻撃者がアクセスできるようにするという問題がある。
【０００７】
従って、ＯＡｕｔｈのように別途の認証手順なしで応用プログラム同士が認証を共有することができるようにしながらも、個人情報のようなユーザ認証情報を外部攻撃から効果的に保護できる新たな保安アルゴリズム（ａｌｇｏｒｉｔｈｍ）の必要性が台頭している。
【発明の概要】
【発明が解決しようとする課題】
【０００８】
本発明は上述した問題点をすべて解決することをその目的とする。
【０００９】
また、本発明はブロックチェーン技術を利用してユーザの認証情報を外部攻撃から効果的に保護できるようにする権限認証を提供することを他の目的とする。
【００１０】
また、本発明はアクセストークンをハッシュ関数と暗号化技術を利用してブロックチェーンに登録して保安が保障されて偽／変造が不可能な権限認証を提供することを他の目的とする。
【００１１】
また、本発明は偽／変造が不可能なブロックチェーンを介して権限認証のためのアクセストークンを検証するので、ユーザ情報の盗用による問題点を未然に防止できるようにする権限認証を提供することを他の目的とする。
【課題を解決するための手段】
【００１２】
上記目的を達成するための本発明の代表的な構成は次の通りである。
【００１３】
本発明の一実施例によれば、ブロックチェーン基盤の権限認証方法において、（ａ）ユーザ端末の認証提携局アプリケーションからの検証確認値を含む認証要請情報に対応した前記ユーザ端末の認証局アプリケーションから電子署名値に対する電子署名値検証要請情報‐前記電子署名値検証要請情報は少なくとも前記検証確認値と前記検証確認値を前記認証局アプリケーションのプライベートキーを用いて電子署名した前記電子署名値を含む‐が獲得されると、認証支援サーバが、（ｉ）前記電子署名値を検証するか前記認証支援サーバに連動される他装置をもって前記電子署名値を検証するように支援して、前記電子署名値が有効であると確認されるとアクセストークンを生成して前記ユーザ端末に転送するか前記認証支援サーバに連動される他装置を介して前記ユーザ端末に転送されるようにすることで前記ユーザ端末をもって前記認証局アプリケーションを介して前記アクセストークンを受信して前記アクセストークンを保存するようにして前記認証提携局アプリケーションを介して前記アクセストークンを利用して認証提携局サーバにログインを要請するように支援し、前記アクセストークンをブロックチェーンに登録するか前記認証支援サーバに連動される他装置を介して前記ブロックチェーンに前記アクセストークンを登録するように支援するか、（ｉｉ）前記ブロックチェーンに前記電子署名値に対する検証を要請するか前記認証支援サーバに連動される他装置を介して前記ブロックチェーンに前記電子署名値に対する検証を要請するようにすることで前記ブロックチェーンをもって前記電子署名値が有効であると確認されるとアクセストークンを生成して前記認証支援サーバに転送するようにして、前記アクセストークンを前記ブロックチェーンに登録するようにし、前記ブロックチェーンから前記アクセストークンが獲得されると前記アクセストークンを前記ユーザ端末に転送するか前記認証支援サーバに連動される他装置を介して前記ユーザ端末に転送されるようにすることで前記ユーザ端末をもって前記認証局アプリケーションを

介して前記アクセストークンを受信して前記アクセストークンを保存するようにして前記認証提携局アプリケーションを介して前記アクセストークンを利用して認証提携局サーバにログインを要請するように支援する段階、及び（ｂ）少なくとも前記アクセストークンを含むアクセストークン検証要請情報が前記認証提携局サーバから獲得されるか前記認証提携局サーバからの前記アクセストークン検証要請情報が認証局サーバを介して獲得されると、前記認証支援サーバが、（ｉ）前記アクセストークンを検証するか前記認証支援サーバに連動される他装置を介して前記アクセストークンを検証するようにするか、（ｉｉ）前記ブロックチェーンに前記アクセストークンに対する検証を要請するか前記認証支援サーバに連動される他装置を介して前記ブロックチェーンに前記アクセストークンに対する検証を要請するようにすることで前記ブロックチェーンをもって前記アクセストークンを検証するように支援して、前記アクセストークンが有効であると確認されると、アクセストークン検証結果情報を前記認証提携局サーバに転送するか前記認証支援サーバに連動される他装置または前記認証局サーバを介して前記アクセストークン検証結果情報が前記認証提携局サーバに転送されるようにすることで前記認証提携局サーバをもって前記アクセストークン検証結果に対応して前記ユーザ端末の前記認証提携局アプリケーションを介した前記認証提携局サーバへのログインを許容するように支援する段階、を含むことを特徴とする方法が提供される。

【００１４】

一例として、前記（ａ）段階で、前記認証支援サーバは、前記認証局アプリケーションに対応されるパブリックキーを利用して前記電子署名値の署名に使用された検証確認値である電子署名検証確認値を確認して、前記確認された電子署名検証確認値が前記電子署名値検証要請情報に含まれた前記検証確認値と一致するか否かを確認することで前記電子署名値を検証するか、前記ブロックチェーンをもって前記認証局アプリケーションに対応されるパブリックキーを利用して前記電子署名値の署名に用いられた前記電子署名検証確認値を確認して、前記確認された電子署名検証確認値が前記電子署名値検証要請情報に含まれた前記検証確認値と一致するか否かを確認して前記電子署名値を検証するようにする。

【００１５】

一例として、前記アクセストークンはユーザ端末識別情報、及びユーザ識別情報のうち少なくとも一つ以上を含むか、前記ユーザ端末識別情報と前記ユーザ識別情報の関数値のうち少なくとも一つ以上を含む。

【００１６】

一例として、前記（ａ）段階で、前記ユーザ端末の前記認証提携局アプリケーションから前記認証提携局サーバへのログイン要請には前記アクセストークン、ユーザ端末識別情報、及びユーザ識別情報のうち少なくとも一つ以上が含まれている。

【００１７】

一例として、前記（ｂ）段階で、前記認証支援サーバは、前記認証提携局サーバをもって前記アクセストークン検証結果情報に対応して前記アクセストークンを前記認証提携局サーバに連動される記憶装置に保存するようにする。

【００１８】

一例として、前記（ｂ）段階で、前記アクセストークン検証結果情報にユーザ端末識別情報、及びユーザ識別情報のうち少なくとも一つ以上をさらに含む。

【００１９】

一例として、前記（ｂ）段階で、前記認証支援サーバは、前記アクセストークン検証結果情報にユーザ情報を加えて前記認証提携局サーバに転送するか前記認証支援サーバに連動される他装置または前記認証局サーバをもって前記アクセストークン検証結果情報に前記ユーザ情報を加えて前記認証提携局サーバに転送するようにする。

【００２０】

また、本発明の一実施例によれば、ブロックチェーン基盤の権限認証方法において、（ａ）ユーザ端末の認証提携局アプリケーションからの検証確認値を含む認証要請情報に対応した前記ユーザ端末の認証局アプリケーションから電子署名値に対する電子署名値検証

要請情報が獲得されると前記電子署名値を検証するかブロックチェーンをもって前記電子署名値を検証するようにして、前記電子署名値の有効な結果に対応されてアクセストークンが生成されると前記アクセストークンを前記ブロックチェーンに登録されるようにして前記アクセストークンを前記ユーザ端末に転送されるようにすることで前記ユーザ端末をもって前記認証局アプリケーションを介して前記アクセストークンを受信して前記アクセストークンを保存するようにした状態で、前記ユーザ端末の前記認証提携局アプリケーションからの前記アクセストークンを利用したログイン要請に対応して前記アクセストークンを含むアクセストークン検証要請情報が前記認証提携局サーバから獲得されるか前記認証提携局サーバからの前記アクセストークン検証要請情報が認証局サーバを介して獲得されると、前記認証支援サーバが、（ｉ）前記アクセストークンを検証するか前記認証支援サーバに連動される他装置を介して前記アクセストークンを検証するようにするか、（ｉｉ）前記ブロックチェーンに前記アクセストークンに対する検証を要請するか前記認証支援サーバに連動される他装置を介して前記ブロックチェーンに前記アクセストークンに対する検証を要請するようにすることで前記ブロックチェーンをもって前記アクセストークンを検証するように支援する段階、及び（ｂ）前記アクセストークンが有効であると確認されると、前記認証支援サーバが、アクセストークン検証結果情報を前記認証提携局サーバに転送するか前記認証支援サーバに連動される他装置または前記認証局サーバを介して前記アクセストークン検証結果情報が前記認証提携局サーバに転送されるようにすることで前記認証提携局サーバをもって前記アクセストークン検証結果に対応して前記ユーザ端末の前記認証提携局アプリケーションを介した前記認証提携局サーバへのログインを許容するように支援する段階、を含むことを特徴とする方法が提供される。

【００２１】

一例として、前記（ａ）段階で、前記アクセストークン検証要請情報は、（ｉ）前記ユーザ端末の前記認証提携局アプリケーションによる検証確認値を含む認証要請情報に対応して前記ユーザ端末の前記認証局アプリケーションを介した状態を確認して、（ｉ‐１）前記認証局アプリケーションがログイン状態である場合には、前記ユーザ端末の前記認証局アプリケーションが前記保存された前記アクセストークンを前記ユーザ端末の認証提携局アプリケーションに転送し、（ｉ‐２）前記認証局アプリケーションがログイン状態でない場合には、前記認証局アプリケーションが電子署名値に対する電子署名値検証要請情報‐前記電子署名値検証要請情報は少なくとも前記検証確認値と前記検証確認値を前記認証局アプリケーションのプライベートキーを用いて電子署名した前記電子署名値を含む‐を認証支援サーバに転送して、認証支援サーバが前記電子署名値を検証するか前記認証支援サーバに連動される他装置または前記ブロックチェーンを介して前記電子署名値を検証するようにして、前記認証支援サーバから前記電子署名値が有効であると確認されると前記認証局アプリケーションが前記保存された前記アクセストークンを前記認証提携局アプリケーションに転送し、（ｉｉ）前記認証提携局アプリケーションからの前記アクセストークンを利用したログイン要請に対応して前記認証提携局サーバが生成する。

【００２２】

また、本発明の一実施例によれば、ブロックチェーン基盤の権限認証方法において、（ａ）ユーザ端末が、認証提携局アプリケーションからの検証確認値を含む認証要請情報に対応して認証局アプリケーションを介して電子署名値に対する電子署名値検証要請情報‐前記電子署名値検証要請情報は少なくとも前記検証確認値と前記検証確認値を前記認証局アプリケーションのプライベートキーを用いて電子署名した前記電子署名値を含む‐を認証支援サーバに転送するか前記ユーザ端末に連動される他装置を介して前記電子署名値要請情報を認証支援サーバに転送するようにすることで前記認証支援サーバをもって（ｉ）前記電子署名値を検証するか前記認証支援サーバに連動される他装置をもって前記電子署名値を検証するように支援して、前記電子署名値が有効であると確認されるとアクセストークンを生成し、前記アクセストークンをブロックチェーンに登録するか前記認証支援サーバに連動される他装置を介して前記ブロックチェーンに前記アクセストークンを登録するように支援して、前記アクセストークンを前記ユーザ端末に転送するか前記認証支援サ

ーバに連動される他装置を介して前記アクセストークンが前記ユーザ端末に転送されるように支援するようにするか、（ｉｉ）前記ブロックチェーンに前記電子署名値に対する検証を要請するか前記認証支援サーバに連動される他装置を介して前記ブロックチェーンに前記電子署名値に対する検証を要請するようにし、前記ブロックチェーンを介して前記電子署名値が有効であると確認されると前記アクセストークンを生成して前記ブロックチェーンに登録するようにして、前記アクセストークンを前記認証支援サーバに転送するようにして、前記ブロックチェーンから前記アクセストークンが獲得されると前記アクセストークンを前記ユーザ端末に転送するか前記認証支援サーバに連動される他装置を介して前記ユーザ端末に転送されるように支援するようにする段階、及び（ｂ）前記認証局アプリケーションを介して前記アクセストークンが獲得されると、前記ユーザ端末が、前記アクセストークンを保存し、前記認証提携局アプリケーションを介して前記アクセストークンを利用して認証提携局サーバにログインを要請するか前記ユーザ端末に連動される他装置を介して前記認証提携局サーバにログインを要請するようにすることで前記認証提携局サーバをもって、（ｉ）少なくとも前記アクセストークンを含むアクセストークン検証要請情報を前記認証支援サーバに転送するように支援するか認証局サーバを介して前記アクセストークン検証要請情報が前記認証支援サーバに転送されるように支援して前記認証支援サーバを介して（ｉ‐１）前記アクセストークンを検証するか前記認証支援サーバに連動される他装置を介して前記アクセストークンを検証するようにするか、（ｉ‐２）前記ブロックチェーンに前記アクセストークンに対する検証を要請するか前記認証支援サーバに連動される他装置を介して前記ブロックチェーンに前記アクセストークンに対する検証を要請するように支援して、（ｉｉ）前記アクセストークンが有効であると確認されてアクセストークン検証結果情報が前記認証支援サーバまたは前記認証局サーバを介して獲得されると前記アクセストークン検証結果に対応して前記ユーザ端末の前記認証提携局アプリケーションを介した前記認証提携局サーバへのログインを許容するように支援する段階、を含むことを特徴とする方法が提供される。

【００２３】

また、本発明の一実施例によれば、ブロックチェーン基盤の権限認証方法において、（ａ）ユーザ端末の認証提携局アプリケーションからの検証確認値を含む認証要請情報に対応した前記ユーザ端末の認証局アプリケーションから電子署名値に対する電子署名値検証要請情報が獲得されると前記電子署名値を検証するかブロックチェーンをもって前記電子署名値を検証するようにして、前記電子署名値の有効な結果に対応されてアクセストークンが生成されると前記アクセストークンを前記ブロックチェーンに登録されるようにして前記アクセストークンを前記ユーザ端末に転送されるようにすることで前記ユーザ端末をもって前記認証局アプリケーションを介して前記アクセストークンを受信して前記アクセストークンを保存するようにした状態で、ユーザ端末が、前記認証提携局アプリケーションによる検証確認値を含む認証要請情報に対応して前記認証局アプリケーションを介したログイン状態を確認して、（ｉ）前記認証局アプリケーションがログイン状態である場合には、前記ユーザ端末の前記認証局アプリケーションが前記保存された前記アクセストークンを前記ユーザ端末の認証提携局アプリケーションに転送し、（ｉｉ）前記認証局アプリケーションがログイン状態でない場合には、前記認証局アプリケーションが電子署名値に対する電子署名値検証要請情報‐前記電子署名値検証要請情報は少なくとも前記検証確認値と前記検証確認値を前記認証局アプリケーションのプライベートキーを用いて電子署名した前記電子署名値を含む‐を認証支援サーバに転送して、認証支援サーバをもって前記電子署名値を検証するか前記認証支援サーバに連動される他装置または前記ブロックチェーンを介して前記電子署名値を検証するように支援して、前記認証支援サーバから前記電子署名値が有効であると確認されると前記認証局アプリケーションが前記保存された前記アクセストークンを前記認証提携局アプリケーションに転送する段階、及び（ｂ）前記ユーザ端末が、前記認証提携局アプリケーションを介して前記アクセストークンを利用したログイン要請を前記認証提携局サーバに転送するか前記ユーザ端末に連動される他装置を介して前記ログイン要請を前記認証提携局サーバに転送するようにすることで前記認証

提携局サーバをもって、（ｉ）少なくとも前記アクセストークンを含むアクセストークン検証要請情報を前記認証支援サーバに転送するように支援するか認証局サーバを介して前記アクセストークン検証要請情報が前記認証支援サーバに転送されるように支援して前記認証支援サーバを介して（ｉ‐１）前記アクセストークンを検証するか前記認証支援サーバに連動される他装置を介して前記アクセストークンを検証するようにするか、（ｉ‐２）前記ブロックチェーンに前記アクセストークンに対する検証を要請するか前記認証支援サーバに連動される他装置を介して前記ブロックチェーンに前記アクセストークンに対する検証を要請するように支援して、（ｉｉ）前記アクセストークンが有効であると確認されてアクセストークン検証結果情報が前記認証支援サーバまたは前記認証局サーバを介して獲得されると前記アクセストークン検証結果に対応して前記ユーザ端末の前記認証提携局アプリケーションを介した前記認証提携局サーバへのログインを許容するように支援する段階、を含むことを特徴とする方法が提供される。

【００２４】

また、本発明の一実施例によれば、ブロックチェーン基盤の権限認証を遂行する認証支援サーバにおいて、ユーザ端末の認証提携局アプリケーションからの検証確認値を含む認証要請情報に対応した前記ユーザ端末の認証局アプリケーションから電子署名値に対する電子署名値検証要請情報‐前記電子署名値検証要請情報は少なくとも前記検証確認値と前記検証確認値を前記認証局アプリケーションのプライベートキーを用いて電子署名した前記電子署名値を含む‐を獲得する通信部、及び前記通信部を介して獲得される前記電子署名値検証要請情報に対応して、（ｉ）前記電子署名値を検証するか前記認証支援サーバに連動される他装置をもって前記電子署名値を検証するように支援して、前記電子署名値が有効であると確認されるとアクセストークンを生成して前記ユーザ端末に転送するか前記認証支援サーバに連動される他装置を介して前記ユーザ端末に転送されるようにすることで前記ユーザ端末をもって前記認証局アプリケーションを介して前記アクセストークンを受信して前記アクセストークンを保存するようにして前記認証提携局アプリケーションを介して前記アクセストークンを利用して認証提携局サーバにログインを要請するように支援し、前記アクセストークンをブロックチェーンに登録するか前記認証支援サーバに連動される他装置を介して前記ブロックチェーンに前記アクセストークンを登録するように支援するか、（ｉｉ）前記ブロックチェーンに前記電子署名値に対する検証を要請するか前記認証支援サーバに連動される他装置を介して前記ブロックチェーンに前記電子署名値に対する検証を要請するようにすることで前記ブロックチェーンをもって前記電子署名値が有効であると確認されるとアクセストークンを生成して前記認証支援サーバに転送するようにして、前記アクセストークンを前記ブロックチェーンに登録するようにし、前記ブロックチェーンから前記アクセストークンが獲得されると前記アクセストークンを前記ユーザ端末に転送するか前記認証支援サーバに連動される他装置を介して前記ユーザ端末に転送されるようにすることで前記ユーザ端末をもって前記認証局アプリケーションを介して前記アクセストークンを受信して前記アクセストークンを保存するようにして前記認証提携局アプリケーションを介して前記アクセストークンを利用して認証提携局サーバにログインを要請するように支援する第１プロセス、少なくとも前記アクセストークンを含むアクセストークン検証要請情報が前記認証提携局サーバから獲得されるか前記認証提携局サーバからの前記アクセストークン検証要請情報が認証局サーバを介して獲得されると、（ｉ）前記アクセストークンを検証するか前記認証支援サーバに連動される他装置を介して前記アクセストークンを検証するようにするか、（ｉｉ）前記ブロックチェーンに前記アクセストークンに対する検証を要請するか前記認証支援サーバに連動される他装置を介して前記ブロックチェーンに前記アクセストークンに対する検証を要請するようにすることで前記ブロックチェーンをもって前記アクセストークンを検証するように支援して、前記アクセストークンが有効であると確認されると、アクセストークン検証結果情報を前記認証提携局サーバに転送するか前記認証支援サーバに連動される他装置または前記認証局サーバを介して前記アクセストークン検証結果情報が前記認証提携局サーバに転送されるようにすることで前記認証提携局サーバをもって前記アクセストークン検証結果に対応して

前記ユーザ端末の前記認証提携局アプリケーションを介した前記認証提携局サーバへのログインを許容するように支援する第２プロセスを遂行するプロセッサ、を含むことを特徴とする認証支援サーバが提供される。

【００２５】

一例として、 前記プロセッサは、前記第１プロセスで、前記認証局アプリケーションに対応されるパブリックキーを利用して前記電子署名値の署名に用いられた検証確認値である電子署名検証確認値を確認して、前記確認された電子署名検証確認値が前記電子署名値検証要請情報に含まれた前記検証確認値と一致するか否かを確認することで前記電子署名値を検証するか、前記ブロックチェーンをもって前記認証局アプリケーションに対応されるパブリックキーを利用して前記電子署名値の署名に用いられた前記電子署名検証確認値を確認して、前記確認された電子署名検証確認値が前記電子署名値検証要請情報に含まれた前記検証確認値と一致するか否かを確認して前記電子署名値を検証するようにする。

【００２６】

一例として、前記アクセストークンはユーザ端末識別情報、及びユーザ識別情報のうち少なくとも一つ以上を含むか、前記ユーザ端末識別情報と前記ユーザ識別情報の関数値のうち少なくとも一つ以上を含む。

【００２７】

一例として、前記ユーザ端末の前記認証提携局アプリケーションから前記認証提携局サーバへのログイン要請には前記アクセストークン、ユーザ端末識別情報、及びユーザ識別情報のうち少なくとも一つ以上が含まれている。

【００２８】

一例として、 前記プロセッサは、前記認証提携局サーバをもって前記アクセストークン検証結果情報に対応して前記アクセストークンを前記認証提携局サーバに連動される記憶装置に保存するようにする。

【００２９】

また、本発明の一実施例によれば、ブロックチェーン基盤の権限認証を遂行する認証支援サーバにおいて、ユーザ端末の認証提携局アプリケーションからの検証確認値を含む認証要請情報に対応した前記ユーザ端末の認証局アプリケーションから電子署名値に対する電子署名値検証要請情報が獲得されると前記電子署名値を検証するかブロックチェーンをもって前記電子署名値を検証するようにして、前記電子署名値の有効な結果に対応されてアクセストークンが生成されると前記アクセストークンを前記ブロックチェーンに登録されるようにして前記アクセストークンを前記ユーザ端末に転送されるようにすることで前記ユーザ端末をもって前記認証局アプリケーションを介して前記アクセストークンを受信して前記アクセストークンを保存するようにした状態で、前記ユーザ端末の前記認証提携局アプリケーションからの前記アクセストークンを利用したログイン要請に対応して前記アクセストークンを含むアクセストークン検証要請情報を前記認証提携局サーバから獲得するか前記認証提携局サーバからの前記アクセストークン検証要請情報を認証局サーバを介して獲得する通信部、及び前記通信部を介して獲得される前記アクセストークン検証要請情報に対応して、（ｉ）前記アクセストークンを検証するか前記認証支援サーバに連動される他装置を介して前記アクセストークンを検証するようにするか、（ｉｉ）前記ブロックチェーンに前記アクセストークンに対する検証を要請するか前記認証支援サーバに連動される他装置を介して前記ブロックチェーンに前記アクセストークンに対する検証を要請するようにすることで前記ブロックチェーンをもって前記アクセストークンを検証するように支援する第１プロセス、前記アクセストークンが有効であると確認されると、アクセストークン検証結果情報を前記認証提携局サーバに転送するか前記認証支援サーバに連動される他装置または前記認証局サーバを介して前記アクセストークン検証結果情報が前記認証提携局サーバに転送されるようにすることで前記認証提携局サーバをもって前記アクセストークン検証結果に対応して前記ユーザ端末の前記認証提携局アプリケーションを介した前記認証提携局サーバへのログインを許容するように支援する第２プロセスを遂行するプロセッサ、を含むことを特徴とする認証支援サーバが提供される。

【００３０】
一例として、前記アクセストークン検証要請情報は、（ｉ）前記ユーザ端末の前記認証提携局アプリケーションによる検証確認値を含む認証要請情報に対応して前記ユーザ端末の前記認証局アプリケーションを介したログイン状態を確認して、（ｉ‐１）前記認証局アプリケーションがログイン状態である場合には、前記ユーザ端末の前記認証局アプリケーションが前記保存された前記アクセストークンを前記ユーザ端末の認証提携局アプリケーションに転送し、（ｉ‐２）前記認証局アプリケーションがログイン状態でない場合には、前記認証局アプリケーションが電子署名値に対する電子署名値検証要請情報‐前記電子署名値検証要請情報は少なくとも前記検証確認値と前記検証確認値を前記認証局アプリケーションのプライベートキーを用いて電子署名した前記電子署名値を含む‐を認証支援サーバに転送して、認証支援サーバが前記電子署名値を検証するか前記認証支援サーバに連動される他装置または前記ブロックチェーンを介して前記電子署名値を検証するようにして、前記認証支援サーバから前記電子署名値が有効であると確認されると前記認証局アプリケーションが前記保存された前記アクセストークンを前記認証提携局アプリケーションに転送し、（ｉｉ）前記認証提携局アプリケーションからの前記アクセストークンを利用したログイン要請に対応して前記認証提携局サーバが生成する。
【００３１】
また、本発明の一実施例によれば、ブロックチェーン基盤の権限認証を遂行するユーザ端末において、通信部、及び認証提携局アプリケーションからの検証確認値を含む認証要請情報に対応して認証局アプリケーションを介して電子署名値に対する電子署名値検証要請情報‐前記電子署名値検証要請情報は少なくとも前記検証確認値と前記検証確認値を前記認証局アプリケーションのプライベートキーを用いて電子署名した前記電子署名値を含む‐を前記通信部を介して認証支援サーバに転送するか前記ユーザ端末に連動される他装置を介して前記電子署名値要請情報を認証支援サーバに転送するようにすることで前記認証支援サーバをもって（ｉ）前記電子署名値を検証するか前記認証支援サーバに連動される他装置をもって前記電子署名値を検証するように支援して、前記電子署名値が有効であると確認されるとアクセストークンを生成し、前記アクセストークンをブロックチェーンに登録するか前記認証支援サーバに連動される他装置を介して前記ブロックチェーンに前記アクセストークンを登録するように支援して、前記アクセストークンを前記ユーザ端末に転送するか前記認証支援サーバに連動される他装置を介して前記アクセストークンが前記ユーザ端末に転送されるように支援するようにするか、（ｉｉ）前記ブロックチェーンに前記電子署名値に対する検証を要請するか前記認証支援サーバに連動される他装置を介して前記ブロックチェーンに前記電子署名値に対する検証を要請するようにし、前記ブロックチェーンを介して前記電子署名値が有効であると確認されると前記アクセストークンを生成して前記ブロックチェーンに登録するようにして、前記アクセストークンを前記認証支援サーバに転送するようにして、前記ブロックチェーンから前記アクセストークンが獲得されると前記アクセストークンを前記ユーザ端末に転送するか前記認証支援サーバに連動される他装置を介して前記ユーザ端末に転送されるように支援するようにする第１プロセス、前記通信部を介して前記認証局アプリケーションを介して前記アクセストークンが獲得されると前記アクセストークンを保存し、前記認証提携局アプリケーションを介して前記アクセストークンを利用して認証提携局サーバにログインを要請するか前記ユーザ端末に連動される他装置を介して前記認証提携局サーバにログインを要請するようにすることで前記認証提携局サーバをもって、（ｉ）少なくとも前記アクセストークンを含むアクセストークン検証要請情報を前記認証支援サーバに転送するように支援するか認証局サーバを介して前記アクセストークン検証要請情報が前記認証支援サーバに転送されるように支援して前記認証支援サーバを介して（ｉ‐１）前記アクセストークンを検証するか前記認証支援サーバに連動される他装置を介して前記アクセストークンを検証するようにするか、（ｉ‐２）前記ブロックチェーンに前記アクセストークンに対する検証を要請するか前記認証支援サーバに連動される他装置を介して前記ブロックチェーンに前記アクセストークンに対する検証を要請するように支援して、（ｉｉ）前記アクセストークンが有効

であると確認されてアクセストークン検証結果情報が前記認証支援サーバまたは前記認証局サーバを介して獲得されると前記アクセストークン検証結果に対応して前記ユーザ端末の前記認証提携局アプリケーションを介した前記認証提携局サーバへのログインを許容するように支援する第２プロセスを遂行するプロセッサ、を含むことを特徴とするユーザ端末が提供される。

【００３２】

また、本発明の一実施例によれば、ブロックチェーン基盤の権限認証を遂行するユーザ端末において、通信部、及びユーザ端末の認証提携局アプリケーションからの検証確認値を含む認証要請情報に対応した前記ユーザ端末の認証局アプリケーションから電子署名値に対する電子署名値検証要請情報が獲得されると前記電子署名値を検証するかブロックチェーンをもって前記電子署名値を検証するようにして、前記電子署名値の有効な結果に対応されてアクセストークンが生成されると前記アクセストークンを前記ブロックチェーンに登録されるようにして前記アクセストークンを前記ユーザ端末に転送されるようにすることで前記ユーザ端末をもって前記認証局アプリケーションを介して前記アクセストークンを受信して前記アクセストークンを保存するようにした状態で、前記認証提携局アプリケーションによる検証確認値を含む認証要請情報に対応して前記認証局アプリケーションを介したログイン状態を確認して、（ｉ）前記認証局アプリケーションがログイン状態である場合には、前記ユーザ端末の前記認証局アプリケーションが前記保存された前記アクセストークンを前記ユーザ端末の認証提携局アプリケーションに転送し、（ｉｉ）前記認証局アプリケーションがログイン状態でない場合には、前記認証局アプリケーションが電子署名値に対する電子署名値検証要請情報‐前記電子署名値検証要請情報は少なくとも前記検証確認値と前記検証確認値を前記認証局アプリケーションのプライベートキーを用いて電子署名した前記電子署名値を含む‐を前記通信部を介して認証支援サーバに転送して、認証支援サーバをもって前記電子署名値を検証するか前記認証支援サーバに連動される他装置または前記ブロックチェーンを介して前記電子署名値を検証するように支援して、前記認証支援サーバから前記電子署名値が有効であると確認されると前記認証局アプリケーションが前記保存された前記アクセストークンを前記通信部を介して前記認証提携局アプリケーションに転送する第１プロセス、前記認証提携局アプリケーションを介して前記アクセストークンを利用したログイン要請を前記通信部を介して前記認証提携局サーバに転送するか前記ユーザ端末に連動される他装置を介して前記ログイン要請を前記認証提携局サーバに転送するようにすることで前記認証提携局サーバをもって、（ｉ）少なくとも前記アクセストークンを含むアクセストークン検証要請情報を前記認証支援サーバに転送するように支援するか認証局サーバを介して前記アクセストークン検証要請情報が前記認証支援サーバに転送されるように支援して前記認証支援サーバを介して（ｉ‐１）前記アクセストークンを検証するか前記認証支援サーバに連動される他装置を介して前記アクセストークンを検証するようにするか、（ｉ‐２）前記ブロックチェーンに前記アクセストークンに対する検証を要請するか前記認証支援サーバに連動される他装置を介して前記ブロックチェーンに前記アクセストークンに対する検証を要請するように支援して、（ｉｉ）前記アクセストークンが有効であると確認されてアクセストークン検証結果情報が前記認証支援サーバまたは前記認証局サーバを介して獲得されると前記アクセストークン検証結果に対応して前記ユーザ端末の前記認証提携局アプリケーションを介した前記認証提携局サーバへのログインを許容するように支援する第２プロセスを遂行するプロセッサ、を含むことを特徴とするユーザ端末が提供される。

【００３３】

また、本発明の一実施例によれば、上記の方法を遂行するためのユーザ端末及び認証支援サーバが提供される。

【００３４】

この他にも、本発明の方法を実行するためのコンピュータープログラムを記録するためのコンピュータで判読可能な記録媒体がさらに提供される。

【発明の効果】

【００３５】
本発明によれば、次のような効果がある。
【００３６】
本発明はブロックチェーン技術を利用して権限認証を具現することでユーザの認証情報を外部攻撃から効果的に保護できるようになる。
【００３７】
また、本発明はアクセストークンをハッシュ関数と暗号化技術を利用して保護することで保安が保障されて偽／変造が不可能な権限認証を提供できるようになる。
【００３８】
また、本発明は偽／変造が不可能なブロックチェーンを介して権限認証のためのアクセストークンを検証するので、ユーザ情報の盗難による問題点を未然に防止できるようにする権限認証を提供できるようになる。
【図面の簡単な説明】
【００３９】
【図１】図１は本発明の一実施例にかかるブロックチェーン基盤の権限認証システムを概略的に示したものであり、
【図２】図２は本発明の一実施例にかかるブロックチェーン基盤の権限認証を遂行する方法を概略的に示したものであり、
【図３－４】図３と図４は本発明の一実施例にかかるブロックチェーン基盤の権限認証方法で権限認証と関連したトランザクションをブロックチェーンに登録する他の例を概略的に示したものであり、
【図５】図５は本発明の一実施例にかかるブロックチェーン基盤の権限認証を遂行する他の方法を概略的に示したものである。
【発明を実施するための形態】
【００４０】
後述する本発明に対する詳細な説明は、本発明が実施され得る特定の実施例を例示として示す添付の図面を参照する。これらの実施例は当業者が本発明を実施することができるように充分詳細に説明される。本発明の多様な実施例は相互異なるが、相互排他的である必要はないことを理解されたい。例えば、ここに記載されている特定の形状、構造及び特性は一実施例にかかる本発明の精神及び範囲を逸脱せずに他の実施例で具現され得る。また、各々の開示された実施例内の個別構成要素の位置または配置は本発明の精神及び範囲を逸脱せずに変更され得ることを理解されたい。従って、後述する詳細な説明は限定的な意味で捉えようとするものではなく、本発明の範囲は、適切に説明されると、その請求項が主張することと均等なすべての範囲と、併せて添付された請求項によってのみ限定される。図面で類似する参照符号はいくつかの側面にかけて同一か類似する機能を指称する。
【００４１】
以下、本発明が属する技術分野で通常の知識を有する者が本発明を容易に実施することができるようにするために、本発明の好ましい実施例について添付の図面を参照して詳細に説明することとする。
【００４２】
図１は本発明の一実施例にかかるブロックチェーン基盤の権限認証を遂行するシステムを概略的に示したものであり、システムはユーザ端末１００、認証支援サーバ２００、ブロックチェーン３００、認証局サーバ４００、及び認証提携局サーバ５００を含み得る。
【００４３】
まず、ユーザ端末１００は認証局アプリケーション１２０及び認証提携局アプリケーション１１０によってユーザにサービスされる情報を表示して権限認証を遂行するデバイスとして、ＰＣ、モバイルコンピュータ、ＰＤＡ／ＥＤＡ、携帯電話、スマートフォン、タブレットなどを含み得る。そして、ユーザ端末１００はこれに限定されず、有線・無線通信機能を有する携帯用ゲーム機、デジタルカメラ、パーソナルナビゲーションなどのすべての通信デバイスを含み得る。また、ユーザ端末１００は情報の送受信を支援する通信部

と情報を処理するプロセッサを含み得る。

【００４４】

次に、認証支援サーバ２００はブロックチェーン基盤の権限認証を遂行するものとして、通信部とプロセッサを含み得る。同一の参照符号を利用して示したのは説明の便宜のために過ぎず、これらの個別装置が同一であるという意味で意図されたものではない。そして、本発明の他の実施例における方法は、サーバを別に構成して当該方法を遂行するか同一の認証支援サーバ２００を介して当該方法を遂行する場合もある。また、認証支援サーバ２００はブロックチェーンの各々のノードに対応するサーバであるか、ブロックチェーンのノードを管理するサーバまたはトランザクションサーバであり得る。

【００４５】

具体的に、認証支援サーバ２００は典型的にコンピューティング装置（例えば、コンピュータプロセッサ、メモリ、ストレージ、入力装置及び出力装置、その他既存のコンピューティング装置の構成要素を含み得る装置と、ルータ、スイッチなどのような電子通信装置と、ネットワーク接続ストレージ（ＮＡＳ）及びストレージエリアネットワーク（ＳＡＮ）のような電子情報ストレージシステム）とコンピュータソフトウェア（即ち、コンピューティング装置をもって特定の方式で機能させるインストラクション）の組み合わせを利用して所望のシステム性能を達成するものであり得る。

【００４６】

かかるコンピューティング装置の通信部は連動される他のコンピューティング装置と要請と応答を送受信し得て、一例示としてかかる要請と応答は同一のＴＣＰセッションによってなされ得るが、これに限定されず、例えばＵＤＰデータグラムとして送受信される場合もある。

【００４７】

また、コンピューティング装置のプロセッサはＭＰＵ（Ｍｉｃｒｏ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）またはＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）、キャッシュメモリ（Ｃａｃｈｅ　Ｍｅｍｏｒｙ）、データバス（Ｄａｔａ　Ｂｕｓ）などのハードウェア構成を含み得る。また、運営体制、特定の目的を遂行するアプリケーションのソフトウェア構成をさらに含む場合もある。

【００４８】

次に、ブロックチェーン３００はデータに対するブロックをチェーンで連結して分散元帳に記録するデータ分散処理を遂行する主体であり得る。この時、ブロックチェーン３００は多数のブロックチェーンから構成され得て、各々のブロックチェーンはプライベートブロックチェーンまたはパブリックブロックチェーンであり得る。

【００４９】

次に、認証局サーバ４００はユーザ端末の認証局アプリケーション１２０を介してユーザが使用し得る多様なサービスを提供しながら、他のサーバとの通信のためのインタフェースを提供するものとして、情報の送受信を支援する通信部と情報を処理するプロセッサを含み得る。

【００５０】

次に、認証提携局サーバ５００はユーザ端末の認証提携局アプリケーション１２１を介してユーザが使用し得る多様なサービスを提供するものとして、認証局サーバ４００との提携を介して認証局サーバ４００におけるユーザ識別情報などを利用してユーザ端末１００の認証提携局アプリケーション１１０に権限認証を提供し得て、情報の送受信を支援する通信部と情報を処理するプロセッサを含み得る。

【００５１】

このように構成されたシステムを介して本発明の一実施例にかかるブロックチェーン基盤の権限認証方法を説明すると次の通りである。

【００５２】

まず、図２を参照して本発明の一実施例にかかるブロックチェーン基盤の権限認証方法を説明する。

【００５３】
ユーザがユーザ端末１００を介して認証提携局サーバ５００で提供されるサービスを利用するために、ユーザ端末１００の認証提携局アプリケーション１１０を介して認証要請を生成するようにする（Ｓ１）。この時、認証提携局アプリケーション１１０はＵＲＬｓｃｈｅｍｅによって認証局アプリケーション１２０を呼び出して認証局アプリケーション１２０を介して検証確認値を署名して転送するようにし得て、認証要請情報は電子署名のための検証確認値を含み得て、検証確認値はノンス（ｎｏｎｃｅ）、ＯＴＰ（ｏｎｅ ｔｉｍｅ ｐａｓｓｗｏｒｄ）、またはタイムスタンプなどを含み得る。
【００５４】
そして、ユーザ端末１００の認証局アプリケーション１２０は認証要請情報に含まれた検証確認値を認証局アプリケーション１２０のプライベートキーを利用して電子署名して電子署名値を生成する（Ｓ２）。この時、認証局アプリケーション１２０のプライベートキーは認証局アプリケーション１２０のユーザ認証のために生成されたＰＫＩ証明書におけるプライベートキーであり、プライベートキーに対応されるパブリックキーはブロックチェーン３００に登録された状態であり得る。また、認証局アプリケーション１２０のプライベートキーを利用した電子署名でユーザ端末１００はユーザにパスワード、ＰＩＮコード、ユーザの指紋情報、及びユーザの生体情報のうち少なくとも一つを含み得るパス情報の入力を要請し得て、ユーザによって入力されるパス情報が既設定されたパス情報と一致する場合にのみ電子署名が可能なようにし得る。
【００５５】
その後、ユーザ端末１００の認証局アプリケーション１２０は認証支援サーバ２００に電子署名値に対する検証を要請する（Ｓ３）。この時、電子署名値に対する検証を要請するための電子署名値検証要請情報には認証要請情報から獲得された検証確認値と電子署名値を含み得る。また、電子署名値検証要請情報にはＵＵＩＤ（ｕｎｉｖｅｒｓａｌｌｙ ｕｎｉｑｕｅ ｉｄｅｎｔｉｆｉｅｒ）などのユーザ端末識別情報、及び電話番号などのユーザ識別情報のうち少なくとも一つ以上を含み得る。
【００５６】
そして、認証支援サーバ２００は通信部を介して獲得される電子署名値検証要請情報に対応して電子署名値を検証するか電子署名値を検証するように支援し得る。
【００５７】
一例として、認証支援サーバ２００は認証支援サーバ２００に連動された他装置に保存された認証局アプリケーション１２０に対応されるパブリックキー、即ち、ユーザ識別情報またはユーザ端末識別情報に対応して保存されたパブリックキーを獲得するかブロックチェーン３００から認証局アプリケーション１２０に対応されるパブリックキーを獲得して、認証局アプリケーションに対応されるパブリックキーを利用して電子署名値の署名に使用された検証確認値である電子署名検証確認値を確認し、確認された電子署名検証確認値が電子署名値検証要請情報に含まれた検証確認値と一致するか否かを確認することで電子署名値を検証し得る。そして、電子署名値が有効であると確認されると認証支援サーバ２００はアクセストークンを生成してユーザ端末１００に転送するか認証支援サーバ２００に連動される他装置を介してユーザ端末１００に転送されるようにする（Ｓ７）。また、認証支援サーバ２００は生成されたアクセストークンをブロックチェーン３００に登録するか認証支援サーバ２００に連動される他装置を介してブロックチェーン３００にアクセストークンを登録するように支援する。この時、アクセストークンはユーザ端末識別情報、ユーザ識別情報、及び電子署名値の少なくとも一つ以上を含むか、これらの関数値のうち少なくとも一つ以上を含み得る。この時、所定の値の関数値は所定の値に特定関数、即ちハッシュ関数を適用して計算されたハッシュ値であり得るがこれに限定されない。
【００５８】
他の例として、認証支援サーバ２００はブロックチェーン３００に電子署名値に対する検証を要請するか認証支援サーバ２００に連動される他装置を介してブロックチェーン３００に電子署名値に対する検証を要請するようにする（Ｓ４）。そして、ブロックチェー

ン３００は認証局アプリケーション１２０に対応されるパブリックキーを利用して電子署名値の署名に使用された電子署名検証確認値を確認して、確認された電子署名検証確認値が電子署名値検証要請情報に含まれた検証確認値と一致するか否かを確認して電子署名値を検証し得る（Ｓ５）。そして、電子署名値が有効であると確認されると、ブロックチェーン３００はアクセストークンを生成してブロックチェーンに登録し、生成されたアクセストークンを認証支援サーバ２００に転送して（Ｓ６）、認証支援サーバ２００はブロックチェーン３００から獲得されるアクセストークンをユーザ端末１００に転送するか認証支援サーバ２００に連動される他装置を介してユーザ端末１００に転送されるようにする（Ｓ７）。

【００５９】

上記ではアクセストークンをブロックチェーン３００に登録したが、ブロックチェーン３００が多数からなる場合があり、一例として、ブロックチェーン３００が第１ブロックチェーンと第２ブロックチェーンから構成される場合、認証支援サーバ２００がアクセストークンを第１ブロックチェーンと第２ブロックチェーンに登録する過程を詳細に説明すると次の通りである。

【００６０】

認証支援サーバ２００はアクセストークンを第１ブロックチェーンに登録するか認証支援サーバ２００に連動される他装置をもって第１ブロックチェーンに登録するようにする。

【００６１】

そして、第２ブロックチェーンに所定の関数値を登録するためのトリガリング条件が満たされると、認証支援サーバ２００はアクセストークンに特定関数を適用して生成した特定関数値と特定関数値にマッチングされる少なくとも一つの関連関数値を演算することで代表関数値または代表関数値を加工した値を生成する。

【００６２】

また、認証支援サーバ２００は生成された代表関数値または代表関数値を加工した値を第２ブロックチェーンに登録するか認証支援サーバ２００に連動される他装置または第１ブロックチェーンをもって代表関数値または代表関数値を加工した値を第２ブロックチェーンに登録するようにし得る。

【００６３】

一方、認証支援サーバ２００は第１特定関数値と少なくとも一つの関連関数値を所定のデータ構造で保存して管理し得る。ここで、データ構造は多様であり得るが、一例として、マークルツリー（ｍｅｒｋｌｅ　ｔｒｅｅ）構造またはパトリシアツリー（Ｐａｔｒｉｃｉａ　ｔｒｅｅ）構造になる場合もあるが、これに限定されるものではない。

【００６４】

即ち、認証支援サーバ２００は特定関数値、即ち、特定ハッシュ値が特定のリーフノードに割り当てられたマークルツリー（Ｍｅｒｋｌｅ　ｔｒｅｅ）を生成するか生成するように支援し得て、トリガリング条件が満たされると、特定ハッシュ値とマッチングされる少なくとも一つの他のリーフノードに割り当てられた関数値、即ちハッシュ値を演算して生成されたマークルルートである代表関数値、即ち代表ハッシュ値、または代表ハッシュ値を加工した値を第２ブロックチェーンに登録するか認証支援サーバ２００に連動される他装置または第１ブロックチェーンをもって第２ブロックチェーンに登録するように支援し得る。

【００６５】

もう少し具体的に説明すると、（ｘ１）認証支援サーバ２００は、（ｉ）特定ハッシュ値と（ｉｉ）特定ハッシュ値が割り当てられたノードの兄弟ノードに割り当てられたハッシュ値を演算するか認証支援サーバ２００に連動された他装置をもって演算するように支援し、演算値のハッシュ値をノードの親ノードに割り当てるか認証支援サーバ２００に連動された他装置をもって親ノードに割り当てるように支援し得る。（ｘ２）万一、親ノードがマークルツリーのルートノードであれば、親ノードに割り当てられたハッシュ値が代

表ハッシュ値または代表ハッシュ値を加工した値になる。（ｘ３）一方、親ノードがマークルツリーのルートノードでなければ、認証支援サーバ２００は、親ノードに割り当てられたハッシュ値を特定ハッシュ値にして（ｘ１）ないし（ｘ３）を反復して遂行する。

【００６６】

そして、認証支援サーバ２００は最終的にマークルツリーのルートノードに割り当てられたハッシュ値を代表ハッシュ値または代表ハッシュ値を加工した値として第２ブロックチェーンに登録するか認証支援サーバ２００に連動された他装置または第１ブロックチェーンをもって第２ブロックチェーンに登録するように支援する。この時、代表ハッシュ値を加工した値は、例えば、代表ハッシュ値にｈｅｘ演算が遂行された結果値であり得る。

【００６７】

一方、認証支援サーバ２００が特定ハッシュ値と少なくとも一つの関連ハッシュ値を所定の第１‐１データ構造で保存し、その後第１‐１データ構造と同一の形態の第１‐２データ構造を保存して管理する場合、第１‐１データ構造と第１‐２データ構造はチェーン形態で連結され得る。

【００６８】

特に、上述した例でのように、第１‐１データ構造及び第１‐２データ構造がマークルツリーである場合、第１‐１データ構造の代表値、即ちルート値、またはルート値のハッシュ値が第１‐２データ構造の一番目リーフノードに割り当てられ得る。

【００６９】

また、第１‐２データ構造を生成する時は第１‐１データ構造に対する検証がなされることでデータｉｎｔｅｇｒｉｔｙがさらに保証され得る。第１‐２データ構造の検証に対しては後述することにする。

【００７０】

また、チェーン形態で連結された少なくとも一つのマークルツリーのうち一番目マークルツリーの場合、一番目マークルツリーの一番目リーフノードにはテキスト、数字、または記号からなる所定のメッセージデータのハッシュ値またはこれを加工した値が割り当てられ得る。例えば、マークルツリー生成時に認証支援サーバ２００によって最初に付与された入力メッセージのハッシュ値が割り当てられ得る。

【００７１】

図３及び図４は本発明の一実施例によって生成されたマークルツリーの例を示したものである。

【００７２】

図３ではリーフノードの個数が４個のマークルツリーが示される。図示されたマークルツリーは一番目マークルツリーのため（ｔｒｅｅ＿ｉｄ　＝　０）、一番目リーフノードであるｈ０ノードには所定のメッセージデータのハッシュ値（ｓｈａ２５６（ｃｏｉｎｐｌｕｇ＿ｕｎｉｑｕｅ＿ｍｅｓｓａｇｅ））が割り当てられたことがわかる。記録データに対する登録要請がある場合、認証支援サーバ２００は現在構成中であるマークルツリーの最後のリーフノードの次のリーフノードを生成して特定ハッシュ値または特定ハッシュ値を加工した値を割り当てるか割り当てるように支援する。例えば、図３のマークルツリーで二番目リーフノードであるｈ１ノードまで値の割り当てが完了した状態で新たなリーフノードを生成しなければならない場合、次のリーフノードであるｈ２ノードを生成して特定ハッシュ値または特定ハッシュ値を加工した値（ｓｈａ２５６（ｉｎｐｕｔ２））を割り当て得る。また、認証支援サーバ２００は（ｉ）ｈ２ノードに割り当てられた特定ハッシュ値と（ｉｉ）ｈ２ノードの兄弟ノードであるｈ３ノードに割り当てられたハッシュ値を演算するか演算するように支援し得る。演算値に対するハッシュ値はｈ２ノードとｈ３ノードの親ノード（ｈ２３ノード）に割り当てられる。親ノード（ｈ２３ノード）がマークルツリーのルートノードではないので、認証支援サーバ２００はｈ２３ノードに割り当てられたハッシュ値を特定ハッシュ値にして前記過程を反復して遂行し得る。即ち、ｈ２３ノードに割り当てられたハッシュ値を特定ハッシュ値にし、ｈ２３ノードに割り当てられたハッシュ値とｈ０１ノードに割り当てられたハッシュ値を演算してｈ２３ノードと

ｈ０１ノードの親ノード（ｈ０１２３ノード）に割り当て得る。この時、ｈ０１２３ノードがマークルツリーのルートノードなので、認証支援サーバ２００は、ｈ０１２３ノードに割り当てられたハッシュ値を加工した値（ｈｅｘ（ｈ｛ｎｏｄｅ＿ｉｎｄｅｘ｝））を第２ブロックチェーンに登録するか認証支援サーバ２００に連動された他装置または第１ブロックチェーンをもって第２ブロックチェーンに登録するように支援し得る。

【００７３】

一方、上述したトリガリング条件とは、（ｉ）所定の個数分アクセストークンとトランザクションが生成される条件、（ｉｉ）所定の時間が経過する条件、（ｉｉｉ）第１ブロックチェーンでブロックが生成される条件、（ｉｖ）サービス特性に対する条件のうち少なくとも一つを含み得る。

【００７４】

一方、例えば、アクセストークンと関連したトランザクションがマークルツリーのリーフノードの数だけ獲得されるとマークルツリーを生成し、マークルツリーのルート値を第２ブロックチェーンに登録するか他装置をもって登録するように支援し得る。

【００７５】

また、認証支援サーバ２００は所定の時間単位で、上述のマークルツリーのルート値を生成し得る（前記（ｉｉ）の条件）。この場合、認証支援サーバ２００は所定の時間が経過されるとその時までの入力値を利用してマークルツリーを生成してマークルツリーのルート値を第２ブロックチェーンに登録するか認証支援サーバ２００に連動された他装置または第１ブロックチェーンをもって第２ブロックチェーンに登録するように支援し得る。

【００７６】

ところが、この場合には所定の時間が経過したにもかかわらず、マークルツリーの特定ハッシュ値が割り当てられたノードの兄弟ノードに値が割り当てられない可能性がある。このようにトリガリング条件が満たされたにもかかわらず、特定ハッシュ値が割り当てられたノードの兄弟ノードにハッシュ値が割り当てられていない場合、認証支援サーバ２００は、兄弟ノードに所定のハッシュ値を割り当てるか割り当てるように支援して上述の方式でマークルツリーのルート値が算出されるようにし得る。例えば、認証支援サーバ２００は特定ハッシュ値を複製して兄弟ノードに割り当てるか割り当てるように支援し得る。

【００７７】

そして、サービス特性とは、アクセストークンと関連したトランザクションを発行した発行者が提供した費用情報、アクセストークン関連トランザクション登録がなされる時間帯情報、アクセストークン関連トランザクション登録サービスがなされる地域情報、アクセストークン関連トランザクション登録要請をした会社タイプ情報のうち少なくとも一部がなり得る。但し、ここで記載したものに限定されず、通常認められる差別的サービスが提供され得る多様な条件情報を含む。

【００７８】

一方、新たなマークルツリー生成が始まり、アクセストークン関連トランザクションがない状態でトリガリング条件が満たされると、認証支援サーバ２００は、所定のメッセージデータが一番目リーフノードと二番目リーフノードに割り当てられたマークルツリーを作成するか作成するように支援し、マークルツリーのルート値またはこれを加工した値を第２ブロックチェーンに登録するか認証支援サーバ２００に連動された他装置または第１ブロックチェーンをもって第２ブロックチェーンに登録するように支援し得る。この場合には、リーフノード２個のマークルツリーが生成される場合もある。

【００７９】

また、上述したように認証支援サーバ２００が特定ハッシュ値と少なくとも一つの関連ハッシュ値を所定の第１－１のデータ構造で保存し、その後第１－１のデータ構造と同一の形態の第１－２データ構造を保存して管理する場合、第１－１データ構造と第１－２データ構造はチェーン形態で連結され得る。特に、第１－１データ構造及び第１－２データ構造がマークルツリーである場合、第１－１データ構造のルート値またはルート値のハッシュ値が第１－２データ構造の一番目リーフノードに割り当てられ得る。

【００８０】
図４は本発明の一実施例によって第１‐２データ構造として生成されたマークルツリーを示した図面である。
【００８１】
図４を参照すれば、図３のマークルツリー（ｔｒｅｅ＿ｉｄ＝０）のルート値（ｈｅｘ（ｈ０１２３））が新たなマークルツリーの一番目リーフノード（ｈ４ノード）に割り当てられたことがわかる（ｓｈａ２５６（ｉｎｐｕｔ４））。本発明はこのようにトランザクション発生時に生成される複数のデータ構造を連結することで中間にデータ変造が発生する場合でも容易にトラッキングが可能であり、データｉｎｔｅｇｒｉｔｙを向上させる長所を有する。
【００８２】
再び図２を参照すると、認証支援サーバ２００からアクセストークンが転送されると、ユーザ端末１００は認証局アプリケーション１２０を介してアクセストークンを受信し、受信されたアクセストークンを保存する（Ｓ８）。この時、アクセストークンの保存はユーザ端末のＳＥ領域に保存され得る。そして、ユーザ端末１００の認証局アプリケーション１２０はアクセストークンを認証提携局アプリケーション１１０に伝達して（Ｓ９）、認証提携局アプリケーション１１０を介してアクセストークンを利用して認証提携局サーバ５００にログインを要請するようにする（Ｓ１０）。この時、ログイン要請情報にはアクセストークン、ユーザ端末識別情報、及びユーザ識別情報のうち少なくとも一つ以上が含まれ得るが、これに限定されずこれらのハッシュ値のうち少なくとも一つ以上が含まれる場合もある。
【００８３】
そして、認証提携局サーバ５００はユーザ端末１００の認証提携局アプリケーション１１０からのログイン要請に対応してログイン要請情報から獲得されたアクセストークンに対する検証を認証支援サーバ２００に要請するか認証局サーバ４００を介して認証支援サーバ２００にアクセストークン検証要請がなされるようにし得る（Ｓ１１）（Ｓ１２）。この時、アクセストークン検証要請情報にはアクセストークン、ユーザ端末識別情報、及びユーザ識別情報のうち少なくとも一つ以上を含むか、これらのハッシュ値のうち少なくとも一つ以上を含み得る。
【００８４】
そして、認証支援サーバ２００はアクセストークン検証要請情報が認証提携局サーバ５００から獲得されるか認証提携局サーバ５００からのアクセストークン検証要請情報が認証局サーバ４００を介して獲得されることに応じて、アクセストークンを検証するか認証支援サーバ２００に連動される他装置を介してアクセストークンを検証するようにし得る。また、認証支援サーバ２００はブロックチェーン３００にアクセストークンに対する検証を要請するか認証支援サーバ２００に連動される他装置を介してブロックチェーン３００にアクセストークンに対する検証を要請（Ｓ１３）するようにすることでブロックチェーン３００をもってアクセストークンを検証（Ｓ１４）するように支援し得る。
【００８５】
この時、アクセストークンの検証は、検証要請されたアクセストークンがユーザ端末識別情報またはユーザ識別情報に対応してブロックチェーン３００に登録されたアクセストークンと一致するかを確認することでなされ得る。
【００８６】
一方、ブロックチェーン３００が第１ブロックチェーンと第２ブロックチェーンから構成された場合には、ユーザ識別情報またはユーザ端末識別情報に対応して第２ブロックチェーンに登録された代表ハッシュ値または代表ハッシュ値を加工した値を確認し、第２ブロックチェーンで確認された代表ハッシュ値または代表ハッシュ値を加工した値と対応して第１ブロックチェーンに登録されたマークルツリー情報及びリーフノード情報を確認して、マークルツリー情報及びリーフノード情報を参照して第１ブロックチェーンに登録されたアクセストークンを確認するか他装置をもって確認するように支援し得る。

【００８７】
その後、アクセストークンが有効であると確認されると（Ｓ１５）、認証支援サーバ２００はアクセストークン検証結果情報を認証提携局サーバ５００に転送するか認証支援サーバ２００に連動される他装置または認証局サーバ４００を介してアクセストークン検証結果情報が認証提携局サーバ５００に転送されるようにする（Ｓ１６）（Ｓ１８）。この時、認証支援サーバ２００はユーザ端末識別情報またはユーザ識別情報に対応するユーザ情報を確認して（Ｓ１７）確認されたユーザ情報をアクセストークン検証結果情報に加えて認証提携局サーバ５００に転送するか、認証支援サーバ２００に連動される他装置または認証局サーバ４００をもってユーザ端末識別情報またはユーザ識別情報に対応するユーザ情報を確認して（Ｓ１７）確認されたユーザ情報をアクセストークン検証結果情報に加えて認証提携局サーバ５００に転送するようにし得る。

【００８８】
そして、認証提携局サーバ５００はアクセストークン検証結果情報に対応してユーザ端末１００の認証提携局アプリケーション１１０を介した認証提携局サーバ５００へのログインを許容するように支援し得る（Ｓ１９）。この時、認証提携局サーバ５００はユーザ端末識別情報またはユーザ識別情報に対応してアクセストークンを保存させるようにし得て、アクセストークンに加えて獲得されたユーザ情報を追加で保存する場合もある。

【００８９】
次に、図５を参照して本発明の他の実施例にかかるブロックチェーン基盤の権限認証方法を説明する。

【００９０】
まず、図２でのような方法によってユーザ端末１００にアクセストークンが保存され得る。

【００９１】
即ち、ユーザ端末１００の認証提携局アプリケーション１１０からの検証確認値を含む認証要請情報に対応したユーザ端末１００の認証局アプリケーション１２０から電子署名値に対する電子署名値検証要請情報が獲得されると電子署名値を検証するかブロックチェーン３００をもって電子署名値を検証するようにして、電子署名値の有効な結果に対応されてアクセストークンが生成されるとアクセストークンをブロックチェーン３００に登録されるようにしてアクセストークンをユーザ端末１００に転送されるようにすることでユーザ端末１００をもって認証局アプリケーション１２０を介してアクセストークンを受信してアクセストークンを保存するようにし得る。

【００９２】
この時、ブロックチェーン３００は図２における説明のように、第１ブロックチェーンと第２ブロックチェーンから構成され得て、第１ブロックチェーンにはアクセストークンが登録され、第２ブロックチェーンにはアクセストークンに対応されるマークルルートが登録され得る。

【００９３】
上記のように、ユーザ端末１００にアクセストークンが保存された状態で、ユーザがユーザ端末１００を介して認証提携局サーバ５００で提供されるサービスを利用するために、ユーザ端末１００の認証提携局アプリケーション１１０を介して認証要請を生成するようにする（Ｓ５１）。この時、認証提携局アプリケーション１１０はＵＲＬ　ｓｃｈｅｍｅによって認証局アプリケーション１２０を呼び出して認証局アプリケーション１２０を介して検証確認値を署名して転送するようにし得て、認証要請情報は電子署名のための検証確認値を含み得て、検証確認値はノンス（ｎｏｎｃｅ）、ＯＴＰ（ｏｎｅ　ｔｉｍｅ　ｐａｓｓｗｏｒｄ）、またはタイムスタンプなどを含み得る。

【００９４】
そして、ユーザ端末１００の認証局アプリケーション１２０は認証要請に対応するアクセストークンを確認して（Ｓ５２）、確認されたアクセストークンを認証提携局アプリケーション１１０に転送する（Ｓ５３）。

【００９５】
これをもう少し詳細に説明すると次の通りである。
【００９６】
ユーザ端末１００の認証局アプリケーション１２０は認証要請情報に対応して認証局アプリケーション１２０を介したログイン状態を確認する。
【００９７】
この時、認証局アプリケーション１２０がログイン状態である場合には、ユーザ端末１００の認証局アプリケーション１２０が保存されたアクセストークンをユーザ端末１００の認証提携局アプリケーション１１０に転送するようになる。
【００９８】
しかし、認証局アプリケーション１２０がログイン状態でない場合には、ユーザ端末１００の認証局アプリケーション１２０は認証要請情報に含まれた検証確認値を認証局アプリケーション１２０のプライベートキーを利用して電子署名して電子署名値を生成する。そして、ユーザ端末１００の認証局アプリケーション１２０は認証支援サーバ２００に電子署名値に対する検証を要請する。そして、認証支援サーバ２００は通信部を介して獲得される電子署名値検証要請情報に対応して電子署名値を検証するか電子署名値を検証するように支援し得る。
【００９９】
一例として、認証支援サーバ２００は認証支援サーバ２００に連動された他装置に保存された認証局アプリケーション１２０に対応されるパブリックキー、即ち、ユーザ識別情報またはユーザ端末識別情報に対応して保存されたパブリックキーを獲得するかブロックチェーン３００から認証局アプリケーション１２０に対応されるパブリックキーを獲得して、認証局アプリケーションに対応されるパブリックキーを利用して電子署名値の署名に使用された検証確認値である電子署名検証確認値を確認し、確認された電子署名検証確認値が電子署名値検証要請情報に含まれた検証確認値と一致するか否かを確認することで電子署名値を検証し得る。
【０１００】
他の例として、認証支援サーバ２００はブロックチェーン３００に電子署名値に対する検証を要請するか認証支援サーバ２００に連動される他装置を介してブロックチェーン３００に電子署名値に対する検証を要請するようにする。そして、ブロックチェーン３００は認証局アプリケーション１２０に対応されるパブリックキーを利用して電子署名値の署名に使用された電子署名検証確認値を確認して、確認された電子署名検証確認値が電子署名値検証要請情報に含まれた検証確認値と一致するか否かを確認して電子署名値を検証し得る。
【０１０１】
上記でのような方法によって、アクセストークンがユーザ端末１００の認証提携局アプリケーション１１０に伝達されると、認証提携局アプリケーション１１０は認証提携局サーバ５００にログインを要請する（Ｓ５４）。この時、ログイン要請情報にはアクセストークン、ユーザ端末識別情報、及びユーザ識別情報のうち少なくとも一つ以上が含まれ得るが、これに限定されずこれらのハッシュ値のうち少なくとも一つ以上が含まれ得る。
【０１０２】
そして、認証提携局サーバ５００はログイン要請情報に対応してアクセストークンに対する検証を認証支援サーバ２００に要請するか認証局サーバ４００を介して認証支援サーバ２００にアクセストークン検証要請がなされるようにし得る（Ｓ５５）（Ｓ５６）。この時、アクセストークン検証要請情報にはアクセストークン、ユーザ端末識別情報、及びユーザ識別情報のうち少なくとも一つ以上を含むか、これらのハッシュ値のうち少なくとも一つ以上を含み得る。
【０１０３】
そして、認証支援サーバ２００はアクセストークン検証要請情報が認証提携局サーバ５００から獲得されるか認証提携局サーバ５００からのアクセストークン検証要請情報が認

証局サーバ４００を介して獲得されることに応じて、アクセストークンを検証するか認証支援サーバ２００に連動される他装置を介してアクセストークンを検証するようにし得る。また、認証支援サーバ２００はブロックチェーン３００にアクセストークンに対する検証を要請するか認証支援サーバ２００に連動される他装置を介してブロックチェーン３００にアクセストークンに対する検証を要請（Ｓ５７）するようにすることでブロックチェーン３００をもってアクセストークンを検証（Ｓ５８）するように支援し得る。

【０１０４】

この時、アクセストークンに対する検証は、検証要請されたアクセストークンがユーザ端末識別情報またはユーザ識別情報に対応してブロックチェーン３００に登録されたアクセストークンと一致するかを確認することでなされ得る。

【０１０５】

一方、ブロックチェーン３００が第１ブロックチェーンと第２ブロックチェーンから構成された場合には、ユーザ識別情報またはユーザ端末識別情報に対応して第２ブロックチェーンに登録された代表ハッシュ値または代表ハッシュ値を加工した値を確認し、第２ブロックチェーンで確認された代表ハッシュ値または代表ハッシュ値を加工した値と対応して第１ブロックチェーンに登録されたマークルツリー情報及びリーフノード情報を確認して、マークルツリー情報及びリーフノード情報を参照して第１ブロックチェーンに登録されたアクセストークンを確認するか他装置をもって確認するように支援し得る。

【０１０６】

その後、アクセストークンが有効であると確認されると（Ｓ５９）、認証支援サーバ２００はアクセストークン検証結果情報を認証提携局サーバ５００に転送するか認証支援サーバ２００に連動される他装置または認証局サーバ４００を介してアクセストークン検証結果情報が認証提携局サーバ５００に転送されるようにする（Ｓ６０）（Ｓ６１）。

【０１０７】

そして、認証提携局サーバ５００はアクセストークン検証結果情報に対応してユーザ端末１００の認証提携局アプリケーション１１０を介した認証提携局サーバ５００へのログインを許容するように支援し得る（Ｓ６２）。

【０１０８】

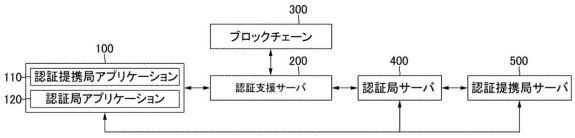
また、以上で説明された本発明にかかる実施例は多様なコンピュータ構成要素を通じて遂行され得るプログラム命令語の形態で具現されてコンピュータで判読可能な記録媒体に記録され得る。前記コンピュータで判読可能な記録媒体はプログラム命令語、データファイル、データ構造などを単独または組み合わせて含まれ得る。前記コンピュータで判読可能な記録媒体に記録されるプログラム命令語は本発明のために特別に設計されて構成されたものか、コンピュータソフトウェア分野の当業者に公知となって使用可能なものでもよい。コンピュータで判読可能な記録媒体の例には、ハードディスク、フロッピィディスク及び磁気テープのような磁気媒体、ＣＤ－ＲＯＭ、ＤＶＤのような光記録媒体、フロプティカルディスク（ｆｌｏｐｔｉｃａｌ　ｄｉｓｋ）のような磁気－光媒体（ｍａｇｎｅｔｏ－ｏｐｔｉｃａｌ　ｍｅｄｉａ）、及びＲＯＭ、ＲＡＭ、フラッシュメモリなどのようなプログラム命令語を保存して遂行するように特別に構成されたハードウェア装置が含まれる。プログラム命令語の例には、コンパイラによって作られるものような機械語コードだけではなく、インタプリタなどを用いてコンピュータによって実行され得る高級言語コードも含まれる。前記ハードウェア装置は本発明にかかる処理を遂行するために一つ以上のソフトウェアモジュールとして作動するように構成されることがあり、その逆も同様である。

【０１０９】

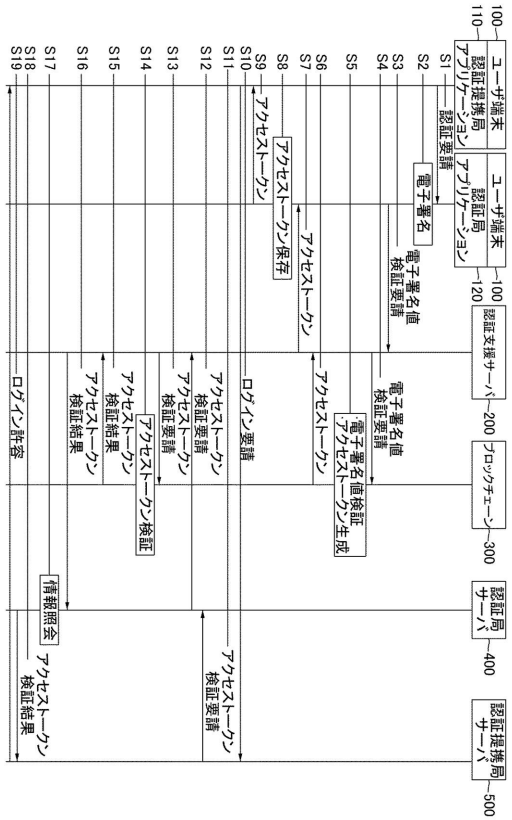
以上、本発明が具体的な構成要素などのような特定の事項と限定された実施例及び図面によって説明されたが、これは本発明のより全般的な理解を助けるために提供されたものであるに過ぎず、本発明が前記実施例に限定されるものではなく、本発明が属する技術分野において通常の知識を有する者であればかかる記載から多様な修正及び変形が行なわれ得る。

【０１１０】
従って、本発明の思想は前記説明された実施例に極限されて定められてはならず、後述する特許請求の範囲だけではなく、本特許請求の範囲と均等または等価的に変形されたすべてのものは本発明の思想の範疇に属するといえる。
【符号の説明】
【０１１１】
１００　ユーザ端末
１１０　認証提携局アプリケーション
１２０　認証局アプリケーション
２００　認証支援サーバ
３００　ブロックチェーン
４００　認証局サーバ
５００　認証提携局サーバ

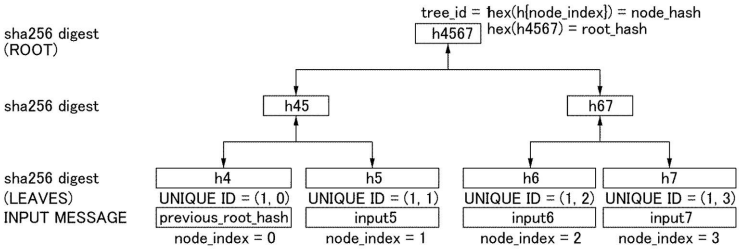
【図１】



【図２】



【図４】



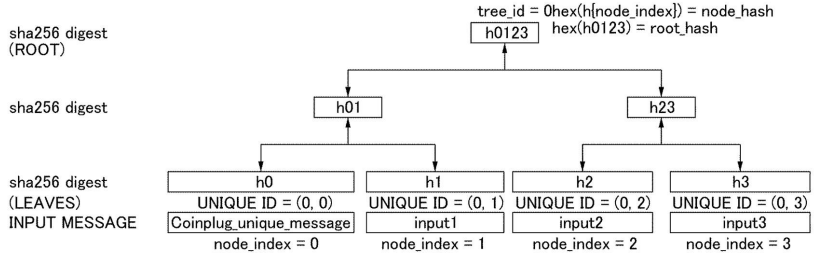
input4 = previous_root_hash
input5 = TrxD
input6 = RN+SigPrivB(RN)+PubB (= User B registration)
input7 = delta_1

h4 = sha256(input4)
h5 = sha256(input5)
h6 = sha256(input6)
h7 = sha256(input7)

h45 = sha256(h4 + h5)
h67 = sha256(h6 + h7)

h4567 = sha256(h45 + h67)

【図３】



input0 = PrivBCM_unique_message
input1 = RN+SigPrivA(RN)+PubA (= User A registration)
input2 = TrxA
input3 = delta_0

h0 = sha256(input0)
h1 = sha256(input1)
h2 = sha256(input2)
h3 = sha256(input3)

h01 = sha256(h0 + h1)
h23 = sha256(h2 + h3)

h0123 = sha256(h01 + h23)

【図５】

フロントページの続き

(72)発明者　オ　ジュンソン
大韓民国　１３５５８　ギョンギド　ソンナムシ　ブンダング　ヌティロ　２２　ビー１７１０
(72)発明者　ホン　ジェウ
大韓民国　０３３３６　ソウル　ウンピョング　ヨンソロ　１４９、１２０３
(72)発明者　ソ　ムンギュ
大韓民国　０６７０７　ソウル　ソチョグ　ミョンダルロ　３３、１０２－６０２

審査官　岸野　徹

(56)参考文献　国際公開第２０１７／１０７９７６（WO，Ａ１）
特表２０１９－５００７９９（ＪＰ，Ａ）
中国特許出願公開第１０６９１１６４１（ＣＮ，Ａ）
特開２００２－２９７５４８（ＪＰ，Ａ）
特開２０１７－０５０７６３（ＪＰ，Ａ）
米国特許出願公開第２０１８／０２４１５５１（ＵＳ，Ａ１）
特開２０１０－１１３４６２（ＪＰ，Ａ）
特開２０１７－２１６５９６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３３
Ｈ０４Ｌ　９／３２