(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7166380号
(P7166380)

(45)発行日　令和4年11月7日(2022.11.7)

(24)登録日　令和4年10月27日(2022.10.27)

(51)国際特許分類

Ｇ０６Ｑ　20/38　(2012.01)	Ｇ０６Ｑ	20/38	３１０
Ｇ０６Ｑ　20/40　(2012.01)	Ｇ０６Ｑ	20/40	
Ｇ０６Ｑ　40/02　(2012.01)	Ｇ０６Ｑ	40/02	

ＦＩ

請求項の数　11　（全23頁）

(21)出願番号　特願2021-51031(P2021-51031)
(22)出願日　令和3年3月25日(2021.3.25)
(65)公開番号　特開2021-106020(P2021-106020A)
(43)公開日　令和3年7月26日(2021.7.26)
審査請求日　令和3年3月25日(2021.3.25)
(31)優先権主張番号　202010256140.0
(32)優先日　令和2年4月2日(2020.4.2)
(33)優先権主張国・地域又は機関
中国(CN)

(73)特許権者　521125475
バイドゥ インターナショナル テクノロジー（シェンチェン）カンパニー，リミテッド
中華人民共和国，１０００８５ グァンドン プロヴィンス ５１８０００，シェンチェン，ナンシャン ディストリクト，ユエハイ ストリート，ビンハイ コミュニティ，ハイチャン ファースト ロード，バイドゥ インターナショナル ビルディング，ナンバー ６，イースト タワー，１階
(74)代理人　100079108
弁理士　稲葉 良幸
(74)代理人　100109346

最終頁に続く

(54)【発明の名称】　ブロックチェーンによる資産処理方法、装置、デバイス、記憶媒体、及びプログラム

(57)【特許請求の範囲】

【請求項１】

ブロックチェーンによる資産処理装置により以下の各ステップが実行される、ブロックチェーン実行方法であって、

取り戻される口座に対する対象口座の資産取り戻しトランザクション要求に応答して、前記対象口座の所有者が前記取り戻される口座の所有者であるか否かの投票を開始するステップと、

前記取り戻される口座により提出した過去トランザクションの対象参加者の投票に基づいて前記対象口座に本人確認を行うステップと、

前記対象口座の本人確認結果に基づいて前記取り戻される口座の資産を処理するステップとを含み、

前記取り戻される口座により提出した過去トランザクションの対象参加者の投票に基づいて前記対象口座に本人確認を行うステップは、

ブロックチェーンに格納されている過去トランザクションデータに基づいて、前記取り戻し口座により提出した過去トランザクションの対象参加者を決定するステップと、

前記対象参加者により投票された投票内容を検証して、検証された有効な対象投票を決定するステップと、

前記対象投票に基づいて前記対象口座に本人確認を行うステップとを含み、

前記対象投票に基づいて前記対象口座に本人確認を行うステップは、

前記対象参加者と取り戻される口座との過去トランザクション処理時間に基づいて、前記

対象参加者の重みを決定するステップと、
前記対象投票中の投票オプションと前記対象参加者の重みに基づいて、身元承認スコアと身元不承認スコアを決定するステップと、
前記身元承認スコア、前記身元不承認スコア、および投票最低スコアに基づいて、前記対象口座の本人確認結果を判定するステップとを含む、
ことを特徴とするブロックチェーンによる資産処理方法。
【請求項２】
前記対象参加者により投票された投票内容を検証して、検証された有効な対象投票を決定するステップは、
投票オプションと乱数に基づいて前記対象参加者によって生成された第１のハッシュ値を取得するステップと、
投票期限の到来が監視されると、前記対象参加者がブロックチェーンネットワークで公開している投票オプションと乱数を取得するステップと、
前記対象参加者がブロックチェーンネットワークで公開している投票オプションと乱数に基づいて、第２のハッシュ値を生成するステップと、
前記第１のハッシュ値と前記第２のハッシュ値とが同じである投票を、投票内容が有効であると検証された対象投票として決定するステップとを含む、
ことを特徴とする請求項１に記載の方法。
【請求項３】
前記身元承認スコア、前記身元不承認スコア、および投票最低スコアに基づいて、前記対象口座の本人確認結果を判定するステップは、
前記身元承認スコアが前記身元不承認スコアより大きく、且つ前記身元承認スコアが前記投票最低スコアより大きいことが検出された場合に、前記対象口座が前記取り戻される口座であることを承認する本人確認結果であると判定されるステップと、
前記身元承認スコアが前記身元不承認スコアより小さく、且つ前記身元不承認スコアが前記投票最低スコアよりも大きいことが検出された場合に、前記対象口座が前記取り戻される口座であることを承認しない本人確認結果であると判定されるステップと、
前記身元承認スコアと前記身元不承認スコアのうちの大きい方のスコアが前記投票最低スコアより小さいであることが検出された場合に、結論が出ない本人確認結果であると判定されるステップとを含む、
ことを特徴とする請求項１に記載の方法。
【請求項４】
前記対象口座の本人確認結果に基づいて前記取り戻される口座の資産を処理するステップは、
前記本人確認結果は前記対象口座が前記取り戻される口座であることを承認したものである場合に、前記取り戻される口座の資産を前記対象口座に移転するするステップを含む、
ことを特徴とする請求項１に記載の方法。
【請求項５】
前記対象口座の所有者が前記取り戻される口座の所有者であるか否かの投票を開始する前に、さらに、
前記対象口座の予め定められた資産額の資産を契約口座に移転し、前記予め定められた資産額の資産を凍結するステップを含む、
ことを特徴とする請求項１に記載の方法。
【請求項６】
前記対象口座の本人確認結果に基づいて前記取り戻される口座の資産を処理した後に、さらに、
前記対象口座の凍結資産に基づいて、前記対象参加者の重みにより、投票内容が有効であると検証された投票が属する対象参加者にインセンティブを与えるステップを含む、
ことを特徴とする請求項５に記載の方法。

【請求項７】
前記対象口座の所有者が前記取り戻される口座の所有者であるか否かの投票を開始した後に、さらに、
ブロックチェーンネットワーク内で前記取り戻される口座に対する介入口座からの身元宣言トランザクションが存在することが検出された場合に、前記取り戻される口座の公開鍵に基づいて前記介入口座の署名を検証するステップと、
前記介入口座の署名検証が合格した場合、前記介入口座が前記取り戻される口座の所有者であると判定されるステップと、
前記対象口座が前記取り戻される口座であるか否かの投票を終了させるステップを含む、ことを特徴とする請求項１に記載の方法。
【請求項８】
取り戻される口座に対する対象口座の資産取り戻しトランザクション要求に応答して、前記対象口座の所有者が前記取り戻される口座の所有者であるか否かの投票を開始する投票モジュールと、
前記取り戻される口座により提出した過去トランザクションの対象参加者の投票に基づいて前記対象口座に本人確認を行う本人確認モジュールと、
前記対象口座の本人確認結果に基づいて前記取り戻される口座の資産を処理する資産処理モジュールとを有し、
前記取り戻される口座により提出した過去トランザクションの対象参加者の投票に基づいて前記対象口座に本人確認を行うステップは、
ブロックチェーンに格納されている過去トランザクションデータに基づいて、前記取り戻し口座により提出した過去トランザクションの対象参加者を決定するステップと、
前記対象参加者により投票された投票内容を検証して、検証された有効な対象投票を決定するステップと、
前記対象投票に基づいて前記対象口座に本人確認を行うステップとを含み、
前記対象投票に基づいて前記対象口座に本人確認を行うステップは、
前記対象参加者と取り戻される口座との過去トランザクション処理時間に基づいて、前記対象参加者の重みを決定するステップと、
前記対象投票中の投票オプションと前記対象参加者の重みに基づいて、身元承認スコアと身元不承認スコアを決定するステップと、
前記身元承認スコア、前記身元不承認スコア、および投票最低スコアに基づいて、前記対象口座の本人確認結果を判定するステップとを含む、
ことを特徴とするブロックチェーンによる資産処理装置。
【請求項９】
少なくとも１つのプロセッサと、
前記少なくとも１つのプロセッサに通信可能に接続されたメモリとを有し、
前記メモリは、前記少なくとも１つのプロセッサによって実行可能な命令を記憶し、前記命令は、前記少なくとも１つのプロセッサが請求項１～７のいずれか１項に記載のブロックチェーンによる資産処理方法を実行することを可能にするように前記少なくとも１つのプロセッサによって実行される、ことを特徴とする電子デバイス。
【請求項１０】
コンピュータに請求項１～７のいずれか１項に記載のブロックチェーンによる資産処理方法を実行させるためのコンピュータ命令を格納した非一時的コンピュータ可読記憶媒体。
【請求項１１】
コンピュータにおいて、プロセッサにより実行されると、請求項１～７のいずれか１項に記載のブロックチェーンによる資産処理方法を実現することを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本願の実施形態は、コンピュータ技術の分野に関し、特にブロックチェーン技術の分野

に関し、具体的には、ブロックチェーンによる資産処理方法、装置、デバイス、記憶媒体、及びプログラムに関する。

【背景技術】

【０００２】

ブロックチェーンネットワークの普及に伴い、それに伴う問題が徐々に現れてきた。ユーザの秘密鍵を紛失した場合、ユーザの資産をどのように取り戻すかは、早急に解決される課題となる。しかし、既存の技術は、いずれも中央集権的な方法に基づいてユーザの資産を取り戻すすることであり、実行方法が煩雑になるだけでなく、資産取り戻しの信頼性や効率性が低下する。

【発明の概要】

【０００３】

ブロックチェーンネットワーク上で口座の身元の有効性への分散型検証を実現した、ブロックチェーンによる資産処理方法、装置、デバイス、記憶媒体が提供される。

【０００４】

第１の側面によれば、ブロックチェーンによる資産処理方法を提供しており、当該方法は、

取り戻される口座に対する対象口座の資産取り戻しトランザクション要求に応答して、前記対象口座が前記取り戻される口座であるか否かの投票を開始するステップと、

前記取り戻される口座により提出した過去トランザクションの対象参加者の投票に基づいて前記対象口座に本人確認を行うステップと、

前記対象口座の本人確認結果に基づいて前記取り戻される口座の資産を処理するステップとを含む

【０００５】

第２の側面によれば、ブロックチェーンによる資産処理装置を提供しており、当該装置は、

取り戻される口座に対する対象口座の資産取り戻しトランザクション要求に応答して、前記対象口座が前記取り戻される口座であるか否かの投票を開始する投票モジュールと、

前記取り戻される口座により提出した過去トランザクションの対象参加者の投票に基づいて前記対象口座に本人確認を行う本人確認モジュールと、

前記対象口座の本人確認結果に基づいて前記取り戻される口座の資産を処理する資産処理モジュールとを有する。

【０００６】

第３の側面によれば、電子デバイスを提供しており、当該電子デバイスは、

少なくとも１つのプロセッサと、

前記少なくとも１つのプロセッサに通信可能に接続されたメモリとを有し、

前記メモリは、前記少なくとも１つのプロセッサによって実行可能な命令を記憶し、前記命令は、前記少なくとも１つのプロセッサが請求項１～９のいずれか１項に記載のブロックチェーンによる資産処理方法を実行することを可能にするように前記少なくとも１つのプロセッサによって実行される。

【０００７】

第４の側面によれば、コンピュータに本願のいずれかの実施形態に記載のブロックチェーンによる資産処理方法を実行させるためのコンピュータ命令を格納した非一時的コンピュータ可読記憶媒体を提供している。

【０００８】

本願の技術によれば、ブロックチェーンネットワーク上で口座の身元の有効性への分散型検証を実現し、口座の秘密鍵を紛失した場合でブロックチェーンネットワークに基づいて口座内の資産を取り戻すことは有益であり、資産取り戻しにおける本人確認の信頼性、可用性、検証効率、検証精度を向上させることが可能となる。

【０００９】

発明の概要の項に記載されていることは、本願の実施形態の主要なまたは重要な特徴を

限定することを意図したものではなく、本願の範囲を限定することを意図したものでもないことが理解されるべきである。本願のその他の特徴は、以下の説明で容易に理解できると思う。

【図面の簡単な説明】

【００１０】

添付の図面は、本実施形態をより良く理解するために使用され、本願に対する限定を構成するものではない。

【図１】本願の第１の実施形態に係るブロックチェーンによる資産処理方法のフローチャートである。

【図２】本願の第２の実施形態に係るブロックチェーンによる資産処理方法のフローチャートである。

【図３】本願の第２の実施形態に係るブロックチェーンによる資産処理の例の図である。

【図４】本願の第３の実施形態に係るブロックチェーンによる資産処理方法のフローチャートである。

【図５】本願の第３の実施形態に係るブロックチェーンによる資産処理の別の例の図である。

【図６】本願の第４の実施形態に係るブロックチェーンによる資産処理方法のフローチャートである。

【図７】本願の第５の実施形態に係るブロックチェーンによる資産処理装置の構造の模式図である。

【図８】本願の実施形態のブロックチェーンによる資産処理方法を実施するために使用される電子デバイスのブロック図である。

【発明を実施するための形態】

【００１１】

以下、図面を参照し、本発明の例示的な実施形態を説明し、理解を容易にするために本発明の実施形態の様々な詳細を含んでいるが、これらは単に例示的なものとみなされるべきである。したがって、当業者は、本発明の範囲および要旨から逸脱することなく、本明細書に記載された実施形態に様々な変更および修正を加えることができることを認識すべきである。同様に、以下の説明では、明瞭で簡潔にするために、既知の機能と構造の説明を省略している。

【００１２】

第１の実施形態

図１は、本願の第１の実施形態に係るブロックチェーンによる資産処理方法のフローチャートである。本実施形態はブロックチェーン口座を介して別の口座の資産を取り戻す場合、例えば秘密鍵を失った口座の資産を取り戻す場合に適用可能である。該方法は、ブロックチェーンノードに配備された資産取り戻しスマートコントラクトによって実行されてもよい。該方法は、ソフトウェアおよび／またはハードウェアで実装された、ブロックチェーンによる資産処理装置によって実行されてもよく、好ましくは、電子デバイス、例えば、資産取り戻しスマートコントラクトを配備しているブロックチェーンノードが属する電子デバイスに配置される。図１に示すように、本方法は、具体的に以下のステップを含む。

【００１３】

Ｓ１１０では、対象口座の取り戻される口座に対する資産取り戻しトランザクション要求に応じて、対象口座は取り戻される口座であるか否かの投票を開始する。

【００１４】

本願の特定の実施形態では、取り戻される口座とは、その秘密鍵または口座資産を取り戻そうとするブロックチェーン口座である。対象口座とは、ブロックチェーンネットワーク内での取り戻される口座、例えば、取り戻される口座の真の所有者や悪意のある資産窃盗者などの口座とは別のいずれかのブロックチェーン口座を指す。例えば、取り戻される口座の秘密鍵が失われた場合、真の所有者が、取り戻される口座を制御できなくなる時、

ブロックチェーンネットワークに基づいて対象口座により、取り戻される口座の制御を回復させることで、取り戻される口座の資産の損失を回避できる。

【００１５】

本実施形態では、資産取り戻しトランザクション要求とは、ブロックチェーンネットワークにおいて資産の取り戻しを開始するためのトランザクション処理要求である。資産取り戻しトランザクション要求は、対象口座から提出される。資産取り戻しトランザクション要求の提出は、対象口座が取り戻される口座の所有者であることを宣言するために使用されてもよく、取り戻される口座の管理権を得るために使用されてもよく、取り戻される口座内の資産を対象口座に移すすることを要求するために使用されてもよく、スマートコントラクトをトリガーして、投票プロセスを開始することで、ブロックチェーンネットワーク内の口座に、対象口座が取り戻される口座であるかどうかの本人確認の投票を行うように指示するために使用されてもよい。

【００１６】

本実施形態では、投票は、対象口座は取り戻される口座であるか否かの承認又は不承認をブロックチェーン口座により表すために使用される。その中で、ブロックチェーンネットワーク内の口座の投票内容は、少なくとも投票オプションと乱数とを含んでおり、投票オプションは「承認」または「不承認」を含んでいる。口座は自身の投票内容に基づいてハッシュ値を生成し、そのハッシュ値を利用して投票を行う。

【００１７】

本実施形態では、対象口座は、取り戻される口座の制御を回復させるために、ブロックチェーンノードを介してブロックチェーンネットワークに資産取り戻しトランザクション要求を提出する。ブロックチェーンネットワーク内のノードは、資産取り戻しトランザクション要求を受信し、資産取り戻しスマートコントラクトを呼び出して、資産取り戻しトランザクション要求に応答する。特に、資産取り戻しスマートコントラクトは、資産取り戻し機能を備えブロックチェーンネットワークの各ノード内に配備された実行可能なプログラムコードであり、システムレベルのスマートコントラクトである。

【００１８】

具体的には、資産取り戻しスマートコントラクトは、投票プロセスを開始する。したがって、ブロックチェーンネットワーク内の口座は、スマートコントラクトを追跡し、および/または、資産取り戻しトランザクション要求を提出した対象口座を追跡することにより、投票プロセスの開始が監視されると、資産取り戻しスマートコントラクトの投票機能を呼び出して、投票を行う。

【００１９】

ここで、対象口座は取り戻される口座であるかどうかの投票を開始する前に、対象口座の予め定められた資産額の資産を契約口座に移し、予め定められた資産額の資産を凍結することがある。ここで、凍結された資産は、有効な投票の投票者にインセンティブを与えることにより、ブロックチェーンネットワーク内の口座が積極的に投票を監視し、投票に参加することを促し、また、ブロックチェーンネットワーク内の口座が実際の有効な投票を行うことを促すために使用されてもよい。したがって、対象口座の資産が予め定められた資産額未満であることが検出された場合には、悪意のある口座による取り戻される口座への攻撃を回避するために、資産が不足している場合の対象口座の資産取り戻しトランザクションの要求に応答しなくてもよい。

【００２０】

さらに、投票の過程中に、介入口座が資産取り戻しスマートコントラクトを呼び出す宣言関数が存在すれば、ブロックチェーンネットワークに対して、介入口座自身は取り戻される口座の真の所有者であることを宣言するための身元宣言トランザクションを開始する。資産取り戻しスマートコントラクトは、取り戻される口座の公開鍵に基づいて介入口座の署名に本人確認できる。認証が合格した場合、介入口座は取り戻される口座の真の所有者であると決定するとともに、対象口座は取り戻される口座であるか否かの投票プロセスを適時に終了させることができる。

【００２１】
Ｓ１２０では、取り戻される口座が提出された過去トランザクションの対象参加者の投票に基づいて前記対象口座に本人確認を行う。
【００２２】
本願の特定の実施形態では、対象参加者は、取り戻される口座により提出されたいずれかの過去トランザクション処理に参加したブロックチェーン口座であり、例えば、振替取引の振込先または情報転送のやりとり相手などを指す。対象参加者は、取り戻される口座とのやりとりを行ったことがあるので、取り戻される口座をある程度理解し、既知の情報に基づいて、取り戻される口座であるかどうかを識別することができ、その投票にはある程度の信頼度がある。
【００２３】
本実施形態では、本人確認とは、対象参加者からの投票に基づいて、対象口座は取り戻される口座であるかどうかを確認することである。十分な投票数が確保された状態で、特定の票数統計手法でカウントし、多数決の原則に基づいて対象口座の本人認証を行う。本人確認の結果は、対象口座が取り戻される口座であることに承認するもの、対象口座が取り戻される口座であることに不承認するもの、対象参加者の数が不足して結論が出ないものに分けられる。
【００２４】
具体的には、ブロックチェーン中のトランザクションデータのトレーサビリティから、取り戻される口座が提出した過去トランザクションに参加したブロックチェーン口座を、ブロックチェーンに格納された過去トランザクションデータに基づいて、対象参加者として決定できる。投票権は、対象参加者に対して設定されてもよい。対象参加者のみが投票権を持っている。その結果、対象参加者からの投票のみを受け取る。あるいは、いずれかのブロックチェーン口座からの投票を受け取り、投票者を本人認証し、対象参加者の投票をすべての投票から選別してもよい。
【００２５】
これにより、対象参加者の投票を基に、特定の投票統計手法により身元承認スコアと身元不承認スコアが決定され、身元承認スコアと身元不承認スコアに基づいて本人確認結果が決定される。本実施形態は、投票統計方法が限定されなく、票を数えることができる方法をこの実施形態に適用することができる。たとえば、承認または不承認の投票数をそのまま合計するか、過去トランザクション処理時間が現在の時間に近いほど投票の信頼性が高くなる原則に基づいて、各対象参加者に重みを決定し、重みに基づいて投票をカウントすることなどでもよい。
【００２６】
ここで、ブロックチェーン口座は投票内容のハッシュ値により投票を行うなら、投票の終了時に、ブロックチェーン口座によりブロックチェーンネットワークにおいて発表された投票内容を取得し、発表された投票内容に基づいて再度ハッシュ値を算出し、投票中のハッシュ値と比較して投票を検証することにより、検証された有効投票に基づいて対象口座に本人確認するようにしてもよい。
【００２７】
Ｓ１３０では、対象口座の本人確認結果に基づいて、取り戻される口座の資産を処理する。
【００２８】
本願の特定の実施形態では、本人確認の結果として、対象口座が取り戻される口座であることに承認する場合、資産取り戻しスマートコントラクトは、資産移転操作を実行し、取り戻される口座内の資産を対象口座に移す。本人確認の結果として、対象口座が取り戻される口座であることに承認しない場合、または結論が出ていない場合は、資産取り戻しスマートコントラクトは資産移転操作を実行しない。対象口座が取り戻される口座の所有者であることが検証されると、取り戻される口座内の資産の全部を対象口座に移すことで、秘密鍵を紛失した口座を取り戻し、取り戻される口座内の資産の安全性とトレーサビ

リティが確保される。

【００２９】

ここで、口座の資産処理は、取り戻される口座への処理に限定されるものではなく、対象口座の資産を凍結する処理を含むものであってもよいし、凍結された資産に基づいて投票者にインセンティブを与える処理などを含むものであってもよい。例示的には、本人確認の結果に関係なく、対象口座の凍結資産で、検証された有効投票が属する投票者にインセンティブを与えてもよい。あるいは、介入口座が存在し、介入口座が取り戻される収口座の真の所有者であることが検証された場合には、対象口座の凍結資産の一部を補償として介入口座に移し、対象口座の凍結資産の別の一部を、検証された有効投票が属する投票者へインセンティブを与えてもよい。

【００３０】

本実施形態の技術案によれば、スマートコントラクトは、取り戻される口座に対する対象口座の資産取り戻しトランザクション要求に応答して、対象口座が取り戻される口座であるか否かの投票プロセスを開始する。取り戻される口座から提出した過去トランザクションの対象参加者を決定し、対象参加者の投票に基づいて対象口座に本人確認を行う。さらに、本人確認結果に基づいて、取り戻される口座の資産を処理する。本願の実施形態は、取り戻される口座と過去トランザクション処理関係を持つ口座を利用して投票の形式で対象口座に本人認証を行うことで、ブロックチェーンネットワーク上で口座の身元の有効性への分散型検証を実現する。これは、口座が秘密鍵を紛失した場合でもブロックチェーンネットワークを通して口座内の資産を取り戻すことに有益であり、資産を取り戻す処理での本人確認の信頼性、可用性、検証効率、検証精度を向上させることが可能となる。

【００３１】

第２の実施形態

図２は、本願の第２の実施形態に係るブロックチェーンによる資産処理方法のフローチャートである。本実施形態は、上述した第１の実施形態を基に、取り戻される口座から提出した過去トランザクションの対象参加者の投票により対象口座の本人確認を行うことをさらに説明する。これにより、対象参加者の投票内容を検証でき、検証された有効な投票にて対象口座に本人確認を行う。図２に示すように、本方法は、具体的には以下のステップを含む。

【００３２】

Ｓ２１０では、取り戻される口座に対する対象口座の資産取り戻しトランザクション要求に応答して、対象口座は取り戻される口座であるか否かの投票を開始する。

【００３３】

Ｓ２２０では、ブロックチェーンに格納されている過去トランザクションデータに基づいて、取り戻される口座から提出した過去トランザクションの対象参加者を決定する。

【００３４】

本願の特定の実施形態では、ブロックチェーン内のトランザクションデータのトレーサビリティに基づいて、取り戻される口座から提出したいずれかの過去トランザクションに参加したブロックチェーン口座、または取り戻される口座が参加したいずれかの過去トランザクションに参加した別の参加者の口座を、ブロックチェーン内に格納された過去トランザクションデータに基づいて、対象参加者として決定できる。例えば、振替取引の振込先又は情報転送のやりとり相手などを決定できる。

【００３５】

Ｓ２３０では、対象参加者から投票した投票内容を検証して、検証された有効な対象投票を決定する。

【００３６】

本願の特定の実施形態では、資産取り戻しスマートコントラクトは、対象参加者を決定した後、対象参加者に投票権限を設定でき、対象参加者のみが投票権を有し、それに応じて対象参加者からの投票のみが受け取られてもよい。あるいは、いずれかのブロックチェーン口座からの投票を受け取り、投票者に本人確認し、対象参加者の投票をすべての投票

から選別してもよい。

【００３７】

本実施形態では、秘密投票による投票、すなわち、ハッシュによるブロックチェーン口座の投票に鑑みるので、ブロックチェーンネットワークでは、投票される投票内容は不明である。したがって、投票の終了時に（すなわち他の口座の投票に影響を与えない時に）、ブロックチェーン口座が自らの投票内容をブロックチェーンネットワークに発表することが求められている。中でも、発表の過程で、インセンティブされるために他の投票内容をフォローして投票内容を変更することを防ぐためには、投票を統計する前に投票内容を検証する必要がある。

【００３８】

具体的には、投票内容を検証するための具体的なプロセスは、以下の通りであってもよい。

【００３９】

Ａ．投票オプションと乱数から対象参加者により生成された第１のハッシュ値を取得する。

【００４０】

本実施形態では、投票オプションは、対象口座の身元に対するブロックチェーン口座の投票意見であり、承認または不承認を含む。乱数とは、ブロックチェーン口座が資産スマートコントラクトの投票関数を呼び出して投票する際にランダムに生成されるデータである。第１のハッシュ値は、ブロックチェーン口座が資産スマートコントラクトの投票関数を呼び出して投票する際に、投票オプションと乱数に基づいて生成されるハッシュ値である。具体的には、ブロックチェーン口座が第１のハッシュ値を用いて投票し、それに応じて、スマートコントラクトは、対象参加者からの投票を受け取り、投票から第１のハッシュ値を取得する。

【００４１】

Ｂ．投票期限の到来が監視されると、対象参加者からのブロックチェーンネットワークで公開している投票オプションと乱数を取得する。

【００４２】

本実施形態では、投票期限は、資産取り戻しスマートコントラクトで予め指定された投票プロセスの合計時間を指す。具体的には、投票プロセスが開始された時点から、投票期限に達することが監視されると、対象参加者は、自らの投票オプションと乱数をブロックチェーンネットワークに公開する。これに応じて、スマートコントラクトは、対象参加者が公開した投票オプションと乱数を取得する。その中で、投票期限の配置は、投票時間を限定するだけでなく、投票プロセスと発表プロセスとを明確に区分けして、これにより、投票処理中に投票内容を発表して投票されていない口座の投票内容に影響を与えることを避ける。

【００４３】

Ｃ．対象参加者によりブロックチェーンネットワークで公開された投票オプションと乱数に基づいて、第２のハッシュ値を生成する。

【００４４】

本実施形態では、第２のハッシュ値は、投票プロセスが終了し、且つ対象参加者が投票内容を公開した後に、公開された投票オプションと乱数に基づいて資産取り戻しスマートコントラクトによって再計算され生成されたハッシュ値である。ここで、ハッシュ値に関する「第１」及び「第２」は、異なる段階で生成されたハッシュ値を区別するために限定されており、実質的な違いはない。

【００４５】

Ｄ．第１のハッシュ値と第２のハッシュ値との同じ投票を、投票内容が検証された有効な対象投票として決定する。

【００４６】

本実施形態では、第１のハッシュ値は投票中のハッシュ値であり、第２のハッシュ値は

資産取り戻しスマートコントラクトによって再計算されたハッシュ値である。対象投票とは、第１のハッシュ値と第２のハッシュ値とが同じである投票である。

【００４７】

具体的には、資産取り戻しスマートコントラクトは、第１のハッシュ値と第２のハッシュ値とを比較し、第１のハッシュ値と第２のハッシュ値とが同じであれば、ブロックチェーン口座が投票内容を公開したときに他の投票内容をフォローして投票内容を変更していないこと、すなわち、公開された投票内容と投票時の投票内容とが同じであることを意味する。そのため、そのような投票は、確認された有効な対象投票として判断される。

【００４８】

その中に、対象参加者は第１のハッシュ値を用いて投票しているため、投票内容は不明である。さらに、投票が終了し、即ち、投票内容が変更されることができない場合に、対象参加者により公開された投票内容に基づいて投票を統計する。ここで、投票内容を公開する際に対象参加者が他の口座の投票内容に基づいて投票内容を変更することを防止するために、投票内容のハッシュ値を再計算して比較することで、投票内容の真正性と信頼性が確保される。

【００４９】

Ｓ２４０では、対象投票に基づいて、対象口座に本人確認を行う。

【００５０】

本願の特定の実施形態では、対象投票は、投票内容が検証された有効な投票であるので、対象投票を元に、特定の投票統計手法で投票を統計して、多数決の原則に基づいて、対象口座に本人確認を行う。

【００５１】

具体的には、対象ユーザの身元を検証する具体的なプロセスは、以下の通りであってもよい。

【００５２】

Ａ．対象参加者と取り戻される口座との過去トランザクション処理時間に基づいて、対象参加者の重みを決定する。

【００５３】

本実施形態では、過去トランザクション処理時間は、対象参加者が取り戻される口座と一緒に同一のトランザクションに参加した過去時間を指す。過去トランザクション処理時間が現在の時刻に近ければ近いほど、取り戻される口座について対象参加者により知られた情報が明確になって、現在の実際の状況に近づくと理解すべきである。そこで、過去トランザクション処理時間が現在の時間に近いほど投票の信憑性が高いという原則に基づいて、対象参加者ごとに重みを決定している。

【００５４】

具体的には、まず、ブロックチェーンネットワークに格納されているトランザクションデータに基づいて、対象参加者と取り戻される口座の過去トランザクション処理時間を決定する。次に、過去トランザクション処理時間と現在の時間との時間差を決定する。最後に、所定の重み設定ルールに基づいて、時間差に応じて、対象参加者の重み、すなわち、時間差が小さいほど重みが大きくなるように決定する。特に、本実施形態は、重み設定ルールが限定されなく、時間差が小さいほど重みを大きくするという原則に基づいて重みを設定することができる方法であれば、いずれも適用可能である。

【００５５】

例示的には、各対象参加者の時間差は、小さい順に順序付けれて、距離パラメータdistanceに１、２、３などの数値を順番に付与する。例えば、時間差が最も小さい対象参加者の距離パラメータdistanceに１が与えられ、時間差が２番目に小さい対象参加者の距離パラメータdistanceに２が与えられ、以降同様である。すると、重みweightの計算式は、weight＝１／distance、またはweight＝１／ｌｏｇ（Ｎ＋distance）としてもよく、ただし、Ｎは定数である。

【００５６】

Ｂ．対象投票中の投票オプションと対象参加者の重みに基づいて、身元承認スコアと身元不承認スコアを決定する。

【００５７】

本実施形態では、投票オプションに基づいて、同じ投票オプションを有する対象投票が属する対象参加者の重みを合計して、その投票オプションのスコアを得ることができる。例えば、投票オプションは承認であるすべての対象投票が属する対象参加者の重みを合計して身元承認スコアを求め、投票オプションは不承認であるすべての対象投票が属する対象参加者の重みを合計して身元不承認スコアを求める。

【００５８】

Ｃ．身元承認スコア、身元不承認スコア、および投票最低スコアに基づいて、対象口座の身元確認結果を決定する。

【００５９】

本実施形態では、投票最低スコアとは、資産取り戻しスマートコントラクトで予め指定されたスコアの最小値を指す。投票最低スコアの具体的な数値は、重み設定ルールに基づいて設定される。そして、投票最低スコアは通常、対象参加者の人数に応じて変更することはなく、例えば、対象参加者の数が減少しても低減されることはできない。

本実施形態では、身元承認スコアと身元不承認スコアとを比較することによって本人確認結果を決定して、身元承認スコアまたは身元不承認スコアと投票最低スコアとを比較することによって本人確認結果が有効であるかどうかを決定する。

【００６０】

この中で、過去トランザクションの処理時間が現在の時刻に近いほど、対象参加者が取り戻される口座について知られた身元情報は明確となり、現在の実際の状況に近いものとなるため、過去トランザクションの処理時間に基づいて、異なる対象参加者に異なる重みを設定することで、重みと投票オプションに基づいて投票統計を行い、異なる対象参加者の本人確認への貢献度を大きくしたり小さくしたりして、投票統計の精度を向上させ、本人確認の精度をさらに向上させることが可能となる。

【００６１】

例示的には、身元承認スコアが身元不承認スコアよりも大きく、かつ、身元承認スコアが投票最低スコアよりも大きいことが検出された場合、身元の検証結果は、対象口座が取り戻される口座であることを承認すると判定され得る。身元承認スコアが身元不承認スコアよりも小さく、かつ、身元不承認スコアが投票最低スコアよりも大きいことが検出された場合には、本人確認結果は、対象口座が取り戻される口座であることを承認しないと判定され得る。身元承認スコアと身元不承認スコアのうち大きい方のスコアが投票最低より小さいであることが検出された場合、本人確認結果は、結論が出ないと判定され得る。

【００６２】

投票最低スコアを設定することで、対象参加者の人数不足による投票統計の不正確を防止でき、投票統計の正確さを向上でき、本人確認の精度をさらに向上できる。

【００６３】

Ｓ２５０では、対象口座の本人確認結果に基づいて、取り戻される口座の資産を処理する。

【００６４】

例示的に、図３は、ブロックチェーンによる資産処理の一例の図を示す。図３に示すように、対象口座は、資産取り戻しトランザクション要求を提出して、取り戻される口座の秘密鍵の紛失を宣言し、取り戻される口座の資産の対象口座への移転を申し込む。同時に、対象口座の予め定められた資産額の資産をスマートコントラクトの口座に移転し、担保とする。資産取り戻しスマートコントラクトは、資産取り戻しトランザクション要求に応答し、投票プロセスを開始し、取り戻される口座によって提出過去トランザクションの対象参加者からの投票を受け取る。したがって、資産取り戻しスマートコントラクトは、対象参加者に重みを設定し、重みと秘密投票の投票オプションに基づいて対象口座に本人確認を行う。図３に示すように、対象参加者１と対象参加者２の両方が不承認で投票を行う

のに対し、対象参加者３だけが承認で投票を行う。つまり、不承認である投票がもっと多い。しかし、対象参加者１の重みが低く、対象参加者２の重みは中等であり、対象参加者３の重みが高いので、資産取り戻しスマートコントラクトは、投票統計を実行した後、本人確認結果が転覆されて承認となる可能性が非常に高い。

【００６５】

本実施形態の技術案は、対象参加者の投票内容を検証し、検証された有効な投票に基づいて本人確認を行うことにより、対象参加者が利益の原因で他の投票内容をフォローして投票することを回避し、投票内容の真正性と信頼性を確保し、本人確認の精度をさらに向上させることができる。

【００６６】

第３の実施形態

図４は、本願の第３の実施形態に係るブロックチェーンによる資産処理方法のフローチャートであり、本実施形態は、上述した第１の実施形態を元に、資産処理をさらに説明する。対象口座の凍結資産に基づいて、投票内容が有効であると検証された投票が属する対象参加者にインセンティブを与える。図４に示すように、当該方法は、具体的には以下のステップを含む。

【００６７】

Ｓ４１０では、取り戻される口座に対する対象口座の資産取り戻しトランザクション要求に応答して、対象口座の予め定められた資産額の資産を契約口座に移し、予め定められた資産額の資産を凍結する。

【００６８】

本願の特定の実施形態では、契約口座とは、資産取り戻しスマートコントラクトの口座を指し、ブロックチェーン口座の資産に凍結または抵当に入れるために用いられる。本実施形態では、予め定められた資産額が限定されなく、口座に抑止効果や損失を与えることができる値であれば、本実施形態で適用することができる。これにより、悪意のある口座の恣意的な取り戻し操作を回避する。

【００６９】

具体的には、取り戻される口座に対する対象口座の資産取り戻しトランザクション要求に応答して、対象口座が取り戻される口座であるか否かの投票を開始する前に、好ましくは、対象口座の予め定められた資産額の資産を契約口座に移すことにより、対象口座の資産の一部に凍結または抵当に入れることが達成される。対象口座の資産を凍結し、資産を取り戻すための一定の代価を対象口座に支払わせることは、悪意のある口座による恣意的な資産取り戻しを回避し、資産取り戻しの安全性を向上させることができる。また、有効な投票を行った投票者にインセンティブを与えることで、ブロックチェーンネットワーク内の口座が積極的に投票を監視し、投票に参加することを促し、また、ブロックチェーンネットワーク内の口座が実際の有効な投票を行うことを促すために使用されてもよい。

【００７０】

Ｓ４２０では、対象口座が取り戻される口座であるか否かの投票を開始する。

【００７１】

Ｓ４３０では、取り戻される口座から提出した過去トランザクションの対象参加者の投票に基づいて対象口座に本人確認を行う。

【００７２】

Ｓ４４０では、対象口座の本人確認結果に基づいて取り戻される口座の資産を処理する。

【００７３】

Ｓ４５０では、対象口座の凍結資産に基づいて、投票内容が有効であると確認された投票が属する対象参加者に、対象参加者の重みにより、インセンティブを与える。

【００７４】

本願の特定の実施形態では、投票統計段階では、資産取り戻しスマートコントラクトは、過去トランザクション処理時間が現在の時間に近いほど、投票の信頼度が高いという原則に基づいて、各対象参加者の重みを決定する。また、投票統計段階では、資産取り戻し

スマートコントラクトは、投票に含まれるハッシュ値と、対象参加者により公開された投票内容に基づいて再計算して生成されたハッシュ値とに基づいて、投票内容が有効であると検証された投票として、２つのハッシュ値が同じである投票を決定する。

【００７５】

本実施形態では、本人確認の結果に関わらず、対象口座の凍結資産で、検証された有効な投票が属する投票者にインセンティブを与えてもよい。具体的には、以下の式に応じて、各検証された有効投票が属する投票者へのインセンティブを決定する。検証された有効な投票が属する投票者のそれぞれへのインセンティブ＝当該投票者の重み／総重み×総凍結資産である。ここで、総重みは、すべての検証された有効な投票が属する投票者の重みの合計であり、即ち、無効な投票が考慮されない。

【００７６】

図５は、図示的には、ブロックチェーンによる資産処理の別の一例の図である。図５に示すように、本人確認の結果に関わらず、対象口座の凍結資産で、検証された有効な投票が属する投票者にインセンティブを与えてもよい。すなわち、公開された投票内容と投票中の投票内容と一致すると検証された対象参加者には、投票行動に対するインセンティブが与えられる。公開された投票内容と投票中の投票内容と一致しないと検証された対象参加者には、他の投票内容をフォローして投票するおそれがあるため、インセンティブが与えられない。

【００７７】

本実施形態の技術案では、対象口座の凍結資産に基づいて、投票内容が有効に検証された投票が属する対象参加者にインセンティブが与えることにより、資産を取り戻すための一定の代価を対象口座に支払わせ、悪意のある口座による恣意的な資産取り戻しを回避するだけでなく、ブロックチェーン口座が投票プロセスの追跡と対象口座の正しい投票を行うことを促し、本人確認の精度を向上させることができる。

【００７８】

第４の実施形態

図６は、本願の第４の実施形態に係るブロックチェーンによる資産処理方法のフローチャートであり、本実施形態は、上述した第１の実施形態を元に、投票プロセスをさらに説明する。投票過程中に取り戻される口座の真の所有者が検出されたときに投票プロセスを終了する。図６に示すように、当該方法は、具体的には以下のステップを含む。

Ｓ６１０では、取り戻される口座に対する対象口座の資産取り戻しトランザクション要求に応答して、対象口座が取り戻される口座であるか否かの投票を開始する。

Ｓ６２０では、ブロックチェーンネットワーク内で介入口座からの取り戻される口座に対する身元宣言トランザクションが存在することが検出された場合に、取り戻される口座の公開鍵に基づいて介入口座の署名を検証する。

【００７９】

本願の特定の実施形態では、身元宣言トランザクションは、提出者が取り戻される口座の所有者であることをブロックチェーンネットワークに宣言するためのトランザクションである。介入口座とは、投票の過程で身元宣言トランザクションを提出するブロックチェーン口座であり、それは取り戻される口座の真の所有者である可能性があり、取り戻される口座の真の所有者ではない可能性がある。

【００８０】

具体的には、投票の過程中に、介入口座は、資産取り戻しスマートコントラクトの宣言関数を呼び出して、介入口座の秘密鍵により署名を行い、ブロックチェーンネットワークへ身元宣言トランザクションを提出することができる。したがって、資産取り戻しスマートコントラクトは、従来の署名検証処理に従い、取り戻される口座の公開鍵により介入口座の署名を検証する。

【００８１】

Ｓ６３０では、介入口座の署名検証が合格した場合、介入口座が取り戻される口座の所有者であると判定される。

【００８２】
本願の特定の実施形態では、スマートコントラクトは、取り戻される口座の公開鍵により署名検証を行うので、署名検証が合格した場合、介入口座の秘密鍵が取り戻される口座の秘密鍵であること、すなわち、取り戻される口座の秘密鍵が失われていないことを意味している。したがって、介入口座が取り戻される口座の所有者であると判定される。逆に言えば、介入口座は取り戻される口座の所有者ではない。
【００８３】
Ｓ６４０では、対象口座が取り戻される口座であるか否かの投票を終了する。
本願の特定の実施形態では、取り戻される口座の真の所有者が存在し、且つ対象口座ではないと判定された場合、取り戻される口座の資産に対して対象口座が悪意を持って盗んだ行為があることを意味するので、資産取り戻し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のリソースを無駄にしないように、適時に投票プロセスを終了させることができる。
【００８４】
また、資産取り戻しトランザクション要求に応答するとき対象口座に資産の一部を凍結するなら、対象口座の凍結資産の一部を介入口座に移し、残りの資産で、検証された有効な投票が属する投票者にインセンティブを与えることにより、介入口座及び検証された有効な投票が属する投票者に補償するとともに、対象口座を罰することができる。
本実施形態の技術案によれば、身元宣言トランザクションを提出した介入口座に署名検証を行うことにより、投票の過程中に取り戻される口座の真の所有者を識別できることを確保し、悪意のある口座の資産盗難の行動を適時に終了させ、取り戻される口座の安全性を確保することができる。
【００８５】
第５の実施形態
図７は、本願の第５の実施形態に係るブロックチェーンによる資産処理装置の構造模式図である。本実施形態は、ブロックチェーン口座を介して別の口座の資産を取り戻す場合、例えば、秘密鍵を失った口座の資産を取り戻す場合に適用することができる。当該装置では、本願のいずれかの実施形態に記載のブロックチェーンによる資産処理方法を実現できる。
【００８６】
当該装置７００は、取り戻される口座に対する対象口座の資産取り戻しトランザクション要求に応答して、前記対象口座が前記取り戻される口座であるか否かの投票を開始する投票モジュール７１０と、
前記取り戻される口座により提出した過去トランザクションの対象参加者の投票に基づいて前記対象口座に本人確認を行う本人確認モジュール７２０と、
前記対象口座の本人確認結果に基づいて前記取り戻される口座の資産を処理する資産処理モジュール７３０とを有する。
【００８７】
オプションとして、前記本人確認モジュール７２０は、
ブロックチェーンに格納された過去トランザクションデータに基づいて、前記取り戻される口座から提出した過去トランザクションの対象参加者を決定する参加者決定ユニット７２０１と、
前記対象参加者の投票される投票内容を検証して、検証された有効な対象投票を決定する投票検証ユニット７２０２と、
前記対象投票に基づいて前記対象口座に本人確認を行う本人確認ユニット７２０３とを有する。
【００８８】
オプションとして、前記投票検証ユニット７２０２は、具体的には、以下のように使用される。
【００８９】

投票オプションと乱数に基づいて前記対象参加者によって生成された第１のハッシュ値を取得する。

【００９０】

投票期限の到来が監視されると、前記対象参加者によりブロックチェーンネットワークで公開された投票オプションと乱数を取得する。

【００９１】

前記対象参加者によりブロックチェーンネットワークで公開された投票オプションと乱数に基づいて、第２のハッシュ値を生成する。

【００９２】

前記第１のハッシュ値と前記第２のハッシュ値とが同じである投票を、投票内容が有効に検証された対象投票として判定する。

【００９３】

オプションとして、前記本人確認ユニット７２０３は、具体的には、以下のように使用される。

【００９４】

前記対象参加者と取り戻される口座との過去トランザクション処理時間に基づいて、前記対象参加者の重みを決定する。

【００９５】

前記対象投票中の投票オプションと前記対象参加者の重みに基づいて、身元承認スコアと身元不承認スコアを決定する。

【００９６】

前記身元承認スコア、前記身元不承認スコア、および投票最低スコアに基づいて、前記対象口座の本人確認結果を決定する。

【００９７】

オプションとして、前記本人確認ユニット７２０３は、具体的には、以下のように使用される。

【００９８】

前記身元承認スコアが前記身元不承認スコアより大きく、且つ前記身元承認スコアが前記投票最低スコアより大きいことが検出された場合に、前記対象口座が前記取り戻される口座であることを承認する本人確認結果であると判定される。

【００９９】

前記身元承認スコアが前記身元不承認スコアより小さく、且つ前記身元不承認スコアが前記投票最低スコアよりも大きいことが検出された場合に、前記対象口座が前記取り戻される口座であることを不承認しない本人確認結果であると判定される。

【０１００】

前記身元承認スコアと前記身元不承認スコアのうちの大きい方のスコアが前記投票最低スコアより小さいであることが検出された場合に、結論が出ない本人確認結果であると判定される。

【０１０１】

オプションとして、前記資産処理モジュール７３０は、具体的には、以下のように使用される。

【０１０２】

前記対象口座が前記取り戻される口座であることを承認した前記本人確認結果である場合に、前記取り戻される口座の資産を前記対象口座に移す。

【０１０３】

さらに、前記装置７００は、資産凍結モジュール７４０をさらに有し、具体的には、以下のように使用される。

【０１０４】

前記対象口座が前記取り戻される口座であるか否かの投票を開始する前に、前記対象口座の予め定められた資産額の資産を契約口座に移し、前記予め定められた資産額の資産を

凍結する。
【０１０５】
さらに、前記装置７００は、インセンティブモジュール７５０をさらに有し、具体的には、以下のように使用される。
【０１０６】
前記対象口座の本人確認結果に基づいて前記取り戻される口座の資産を処理した後に、前記対象口座の凍結資産を基に、前記対象参加者の重みにより、投票内容が有効に検証された投票が属する対象参加者にインセンティブを与える。
【０１０７】
さらに、前記装置７００は、身元介入モジュール７６０をさらに有し、具体的には、以下のように使用される。
【０１０８】
前記対象口座が前記取り戻される口座であるか否かの投票を開始した後に、ブロックチェーンネットワーク内で介入口座からの前記取り戻される口座に対する身元宣言トランザクションが存在することが検出された場合に、前記取り戻される口座の公開鍵に基づいて前記介入口座の署名を検証する。
【０１０９】
前記介入口座の署名検証が合格した場合、前記介入口座が前記取り戻される口座の所有者であると判定される。
【０１１０】
前記対象口座が前記取り戻される口座であるか否かの投票を終了させる。
【０１１１】
本実施形態の技術案は、各機能モジュール間の協力により、資産取り戻しトランザクション要求への応答、資産の凍結、投票プロセスの開始、投票者の決定、投票内容の検証、本人確認、資産の移転、およびインセンティブなどの機能を達成する。本願の実施形態では、取り戻される口座と過去トランザクション処理関係がある口座を利用して、投票という形で、対象口座に本人確認を行うことで、ブロックチェーンネットワーク上で口座の身元の有効性への分散型検証を実現する。これは、口座が秘密鍵を紛失した場合でもブロックチェーンネットワークにて口座内の資産を取り戻すことに有益であり、資産取り戻しにおける本人確認の信頼性、可用性、検証効率、検証精度を向上させることが可能となる。
【０１１２】
第６の実施形態
本願の実施形態によれば、本願はまた、電子デバイスおよび可読記憶媒体を提供する。
【０１１３】
図８に示すように、本願の実施形態に係るブロックチェーンによる資産処理方法のための電子デバイスのブロック図である。電子デバイスは、様々な形態のデジタルコンピュータ、例えば、ラップトップコンピュータ、デスクトップコンピュータ、ワークステーション、パーソナルデジタルアシスタント、サーバ、ブレードサーバ、メインフレームコンピュータ、及び他の好適なコンピュータを表してもよい。また、電子デバイスはまた、様々な形態のモバイルデバイス、例えば、パーソナルデジタル処理、携帯電話、スマートフォン、ウェアラブルデバイス、及び他の類似のコンピューティングデバイスを表してもよい。本明細書に示された部品、それらの接続及び関係、ならびにそれらの機能は、例としてのみ示されており、本明細書に記載及び／又は要求された本願の実現を限定することを意図するものではない。
【０１１４】
図８に示すように、電子デバイスは、１つ以上のプロセッサ８０１、メモリ８０２、及び各コンポーネントを接続するための、高速インタフェース及び低速インタフェースを含むインタフェースを有する。様々な部品は、異なるバスを介して相互に接続されており、共通のマザーボード上に実装されてもよいし、要求に応じて他の方式で実装されてもよい。プロセッサは、電子装置内で実行するための命令を処理してもよく、当該命令は外部入

出力装置（例えば、インタフェースに結合されたディスプレイ装置）にグラフィカルユーザインタフェース（Graphical User Interface、ＧＵＩ）のグラフィカル情報を表示させるためにメモリまたはメモリ上に記憶された命令を含む。他の実施形態では、要求に応じて、複数のプロセッサ及び／又は複数のバスが複数のメモリと一緒に使用されてもよい。同様に、複数の電子デバイスが接続されて、個々のデバイスにより必要な操作のいずれかを提供してもよい（例えば、サーバアレイ、ブレードサーバのグループ、またはマルチプロセッサシステムとする）。一つのプロセッサ８０１を一例として図８に示す。

【０１１５】

メモリ８０２は、本願によって提供される非一時的コンピュータ可読記憶媒体である。ここで、前記メモリは、本願に提供されるブロックチェーンによる資産処理方法を前記少なくとも１つのプロセッサに実行させるために、前記少なくとも１つのプロセッサにより実行可能な命令を記憶している。本願の非一時的コンピュータ可読記憶媒体は、本願によって提供されるブロックチェーンによる資産処理方法をコンピュータに実行させるために使用されるコンピュータ命令を記憶している。

【０１１６】

メモリ８０２は、非一時的コンピュータ可読記憶媒体として、非一時的なソフトウェアプログラム、非一時的なコンピュータ実行可能なプログラム、及びモジュール、例えば、本願の実施形態におけるブロックチェーンによる資産処理方法に対応するプログラム命令／モジュール（例えば、添付の図７に示す投票モジュール７１０、本人確認モジュール７２０、資産処理モジュール７３０、資産凍結モジュール７４０、インセンティブモジュール７５０、身元介入モジュール７６０）を格納するために用いられる。プロセッサ８０１は、メモリ８０２に記憶された非一時的なソフトウェアプログラム、命令、及びモジュールを実行することにより、サーバの各種機能アプリケーション及びデータ処理を実行して、上述した方法の実施形態におけるブロックチェーンによる資産処理方法を実施する。

【０１１７】

メモリ８０２は、プログラム記憶領域とデータ記憶領域とを含んでもよい。プログラム記憶領域は、オペレーティングシステム、少なくとも１つの機能に必要なアプリケーションプログラムを格納してもよい。データ記憶領域は、ブロックチェーンによる資産処理方法のための電子デバイスの使用により作成されたデータなどを格納してもよい。さらに、メモリ８０２は、高速ランダムアクセスメモリを含んでもよく、また、少なくとも１つのディスクメモリ装置、フラッシュメモリ装置、または他の非一時的な固体状態のメモリ装置などの非一時的なメモリを含んでもよい。いくつかの実施形態では、メモリ８０２は、オプションとして、プロセッサ８０１と遠隔的に配置されたメモリを含み、これらの遠隔メモリは、ネットワークを介して、ブロックチェーンによる資産処理方法のための電子デバイスに接続されてもよい。前記ネットワークの例としては、インターネット、企業のイントラネット、ローカルエリアネットワーク、移動体通信ネットワーク、及びそれらの組合せが挙げられるが、これらに限定されるものではない。

【０１１８】

ブロックチェーンによる資産処理方法のための電子デバイスはまた、入力装置８０３と出力装置８０４を含んでもよい。プロセッサ８０１、メモリ８０２、入力装置８０３および出力装置８０４は、バスを介して接続されていてもよく、他の方式で接続されていてもよいが、図８ではバスを介した接続を例に挙げている。

【０１１９】

入力装置８０３は、入力されたデータまたは文字情報を受信するとともに、ブロックチェーンによる資産処理方法のための電子デバイスのユーザ設定及び機能制御に関連するキー信号入力を生成してもよく、例えば、タッチスクリーン、キーパッド、マウス、トラックパッド、タッチパッド、インジケータスティック、１つ以上のマウスボタン、トラックボール、ジョイスティックなどの入力装置などが挙げられる。出力装置８０４は、表示装置、補助照明装置（例えば、発光ダイオード（Light Emitting Diode、ＬＥＤ））、ハプティックフィードバック装置（例えば、振動モータ）などを含んでもよい。当該表示装

置としては、液晶ディスプレイ（Liquid Crystal Display、ＬＣＤ）、ＬＥＤディスプレイ、プラズマディスプレイなどが挙げられるが、これらに限定されるものではない。いくつかの実施形態では、表示装置はタッチスクリーンであってもよい。

【０１２０】

本明細書に記載されたシステム及び技術の様々な実施形態は、デジタル電子回路システム、集積回路システム、専用集積回路（Application Specific Integrated Circuit、ＡＳＩＣ）、コンピュータハードウェア、ファームウェア、ソフトウェア、及び／又はそれらの組合せで実施することができる。これらの様々な実施形態は、以下を含み得る：１つ以上のコンピュータプログラムで実施し、当該１つ以上のコンピュータプログラムは、少なくとも１つのプログラマブルプロセッサを含むプログラマブルシステム上で実行および／又は解釈され、当該プログラマブルプロセッサは、記憶システム、少なくとも１つの入力装置、および少なくとも１つの出力装置からデータおよび指示を受信し、且つデータ及び指示を当該記憶システム、当該少なくとも１つの入力装置、及び当該少なくとも１つの出力装置へ転送することができる専用または汎用のプログラマブルプロセッサであってもよい。

【０１２１】

これらのコンピュータプログラム（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、またはコードとも呼ばれ）は、プログラマブルプロセッサのための機械命令を含み、高レベル手順及び／又はオブジェクト指向のプログラミング言語、及び／又はアセンブリ／機械語を使用してこれらのコンピュータプログラムを実装することができる。本明細書で使用されるように、「機械可読媒体」及び「コンピュータ可読媒体」という用語は、機械命令及び／又はデータをプログラマブルプロセッサに提供するために使用される任意のコンピュータプログラム製品、デバイス、及び／又は装置（例えば、磁気ディスク、光ディスク、メモリ、プログラマブルロジックデバイス（Programmable Logic Device、ＰＬＤ））を指し、機械読取信号である機械命令を受け取る機械読取媒体を含む。「機械可読信号」という用語は、機械命令及び／又はデータをプログラマブルプロセッサに提供するために使用される任意の信号を指す。

【０１２２】

ユーザとのマンマシンインタフェースを提供するために、本明細書に記載されているシステム及び技術は、ユーザに情報を表示するための表示装置（例えば、陰極線管（Cathode Ray Tube、ＣＲＴ）またはＬＣＤモニタ）と、ユーザがコンピュータに入力を提供するためのキーボード及びポインティング装置（例えば、マウスまたはトラックボール）とを有するコンピュータ上に実装されてもよい。他の種類の装置もまた、ユーザとのマンマシンインタフェースを提供するために使用されてもよく、例えば、ユーザに提供されるフィードバックは、任意の形態の感覚フィードバック（例えば、視覚フィードバック、聴覚フィードバック、またはハプティックフィードバック）であってもよく、ユーザからの入力は、任意の形態（例えば、音響入力、音声入力、またはハプティック入力）で受信されてもよい。

【０１２３】

本明細書に記載されているシステム及び技術は、バックエンドコンポーネントを含むコンピューティングシステム（例えば、データサーバー）、ミドルウェアコンポーネントを含むコンピューティングシステム（例えば、アプリケーションサーバー）、またはフロントエンドコンポーネントを含むコンピューティングシステム（例えば、グラフィカルユーザインタフェースまたはWebブラウザーを備えたユーザーコンピューター。当該グラフィカルユーザインタフェースまたは当該Webブラウザーを介して、ユーザはここで説明するシステムおよび技術の実施方式と対話できる）、又はそのようなバックエンドコンポーネント、ミドルウェアコンポーネント、またはフロントエンドコンポーネントの任意の組合せを含むコンピューティングシステムで実装されてもよい。システムのコンポーネントは、任意の形態または媒体のデジタルデータ通信、例えば、通信ネットワークを介して相互に接続されていてもよい。通信ネットワークの例としては、ローカルエリアネットワーク

（Local Area Network、ＬＡＮ）、ワイドエリアネットワーク（Wide Area Network、ＷＡＮ）、インターネット、ブロックチェーンネットワークなどがある。

【０１２４】

コンピュータシステムは、クライアントとサーバを含むことができる。クライアントとサーバは一般的に互いに遠隔地にあり、通常は通信ネットワークを介して相互に作用する。クライアント－サーバ関係は、対応するコンピュータ上で実行され、互いにクライアント－サーバ関係を有するコンピュータプログラムによって生成される。

【０１２５】

本願の実施形態の技術案によれば、取り戻される口座と過去トランザクション処理関係がある口座を利用して、投票という形で、対象口座に本人確認を行うことで、ブロックチェーンネットワーク上で口座の身元の有効性への分散型検証を実現した。これは、口座が秘密鍵を紛失した場合でもブロックチェーンネットワークに基づいて口座内の資産を取り戻すことに有益であり、資産取り戻しにおける本人確認の信頼性、可用性、検証効率、検証精度を向上させることが可能となる。

【０１２６】

また、上記出願の一つの実施形態は、以下のような利点または有益な効果を有する。対象参加者の投票内容を検証し、検証された有効な投票に基づいて本人確認を行うことにより、対象参加者が利益の原因で他の投票内容をフォローして投票することを回避し、投票内容の真正性と信頼性を確保し、本人確認の精度をさらに向上させることができる。

【０１２７】

また、上記出願の一つの実施形態は、以下のような利点または有益な効果を有する。対象参加者は第１のハッシュ値を用いて投票しているため、投票内容は不明である。さらに、投票が終了し、即ち、投票内容を変更することができない場合に、対象参加者により公開された投票内容に基づいて投票を統計する。ここで、投票内容を公開する際に、対象参加者が他の口座の投票内容に基づいて投票内容を変更することを防止するために、投票内容のハッシュ値を再計算して比較することで、投票内容の真正性と信頼性が確保される。

【０１２８】

また、上記出願の一つの実施形態は、以下のような利点または有益な効果を有する。過去トランザクションの処理時間が現在の時刻に近いほど、対象参加者が取り戻される口座について了解された身元情報が明確となり、現在の実際の状況に近いものとなる。したがって、過去トランザクションの処理時間に基づいて異なる対象参加者に異なる重みを設定することにより、重みと投票オプションに基づいて投票統計を行い、異なる対象参加者の本人確認への貢献度を大きくしたり小さくしたりして、投票統計の精度を向上させ、本人確認の精度をさらに向上させることが可能となる。

【０１２９】

また、上記出願の一つの実施形態は、以下のような利点または有益な効果を有する。投票最低スコアを設定することで、対象参加者の人数不足による投票統計の不正確を防止でき、投票統計の正確さを向上でき、本人確認の精度をさらに向上できる。

【０１３０】

また、上記出願の一つの実施形態は、以下のような利点または有益な効果を有する。対象口座は取り戻される口座の所有者であることが検証されると、取り戻される口座内の資産の全部を対象口座に移転することで、秘密鍵を紛失した取り戻される口座の取り戻しが実現され、取り戻される口座内の資産の安全性とトレーサビリティが確保される。

【０１３１】

また、上記出願の一つの実施形態は、以下のような利点または有益な効果を有する。対象口座の資産を凍結することで、資産を取り戻すための一定の代価を対象口座に支払わせて、悪意のある口座による恣意的な資産取り戻しを回避し、資産取り戻しの安全性を向上させることができる。また、有効な投票を行った投票者にインセンティブを与えることで、ブロックチェーンネットワーク内の口座が積極的に投票を監視し投票に参加することを促し、また、ブロックチェーンネットワーク内の口座が実際の有効な投票を行うことを

促すために使用されてもよい。

【０１３２】

また、上記出願の一つの実施形態は、以下のような利点または有益な効果を有する。対象口座の凍結資産に基づいて、投票内容が有効に検証された投票が属する対象参加者にインセンティブを与えることにより、資産を取り戻すための一定の代価を対象口座に支払わせ、悪意のある口座による恣意的な資産の取り戻しを回避し、また、ブロックチェーン口座が投票プロセスの追跡と対象口座の正しい投票を行うことを促し、本人確認の精度を向上させることができる。

【０１３３】

また、上記出願の一つの実施形態は、以下のような利点または有益な効果を有する。身元宣言トランザクションを提出する介入口座に署名検証を行うことにより、投票の過程中に取り戻される口座の真の所有者を識別することを確保でき、悪意のある口座の資産盗難を適時に終了させることができ、取り戻される口座の安全性が確保される。

【０１３４】

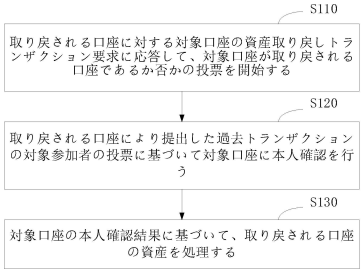
上述した処理の様々な実施形態を用いて、順序を変えたり、ステップを追加/削除したりすることができると理解されるべきである。例えば、本願に開示された技術案の所望の結果が達成される限り、本願に記載された各ステップは、本明細書に限定されるものではなく、並行して実行されてもよいし、順次実行されてもよいし、異なる順序で実行されてもよい。

【０１３５】

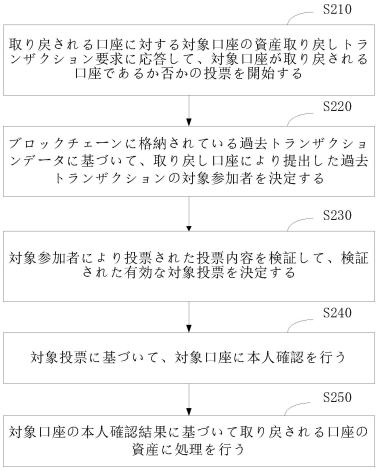
上記の具体的な実施形態は、本発明の保護範囲の制限を構成するものではない。設計要件および他の要因に応じて、様々な変更、組み合わせ、サブ組み合わせおよび置換が行われ得ることは、当業者によって理解されるべきである。本発明の要旨および原則の範囲内で行われた修正、同等の代替、改良等は、本発明の保護範囲に含まれるものとする。

【図面】

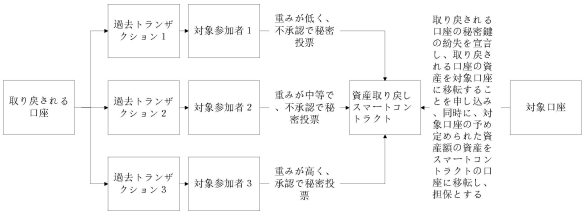
【図１】


S110
取り戻される口座に対する対象口座の資産取り戻しトランザクション要求に応答して、対象口座が取り戻される口座であるか否かの投票を開始する
S120
取り戻される口座により提出した過去トランザクションの対象参加者の投票に基づいて対象口座に本人確認を行う
S130
対象口座の本人確認結果に基づいて、取り戻される口座の資産を処理する

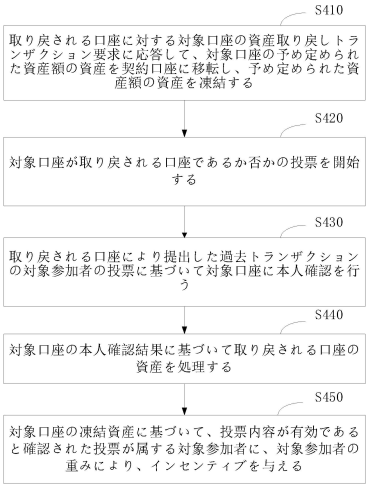
【図２】


S210
取り戻される口座に対する対象口座の資産取り戻しトランザクション要求に応答して、対象口座が取り戻される口座であるか否かの投票を開始する
S220
ブロックチェーンに格納されている過去トランザクションデータに基づいて、取り戻し口座により提出した過去トランザクションの対象参加者を決定する
S230
対象参加者により投票された投票内容を検証して、検証された有効な対象投票を決定する
S240
対象投票に基づいて、対象口座に本人確認を行う
S250
対象口座の本人確認結果に基づいて取り戻される口座の資産に処理を行う

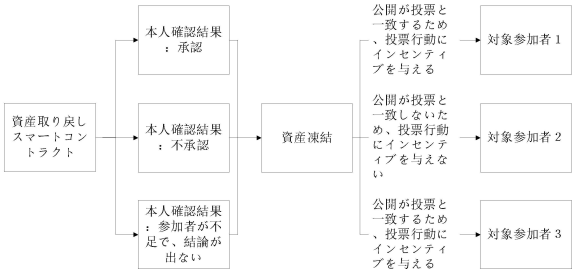
【図３】


取り戻される口座
過去トランザクション１
過去トランザクション２
過去トランザクション３
対象参加者１
対象参加者２
対象参加者３
重みが低く、不承認で秘密投票
重みが中等で、不承認で秘密投票
重みが高く、承認で秘密投票
資産取り戻しスマートコントラクト
取り戻される口座の秘密鍵の紛失を宣言し、取り戻される口座の資産を対象口座に移転することを申し込み、同時に、対象口座の予め定められた資産額の資産をスマートコントラクトの口座に移転し、担保とする
対象口座

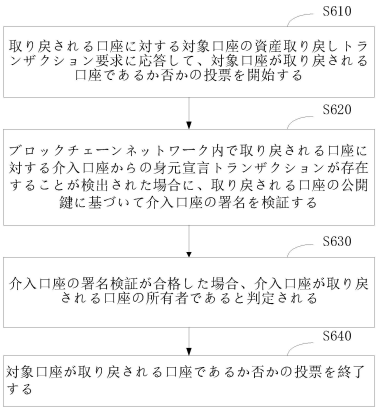
【図４】


S410
取り戻される口座に対する対象口座の資産取り戻しトランザクション要求に応答して、対象口座の予め定められた資産額の資産を契約口座に移転し、予め定められた資産額の資産を凍結する
S420
対象口座が取り戻される口座であるか否かの投票を開始する
S430
取り戻される口座により提出した過去トランザクションの対象参加者の投票に基づいて対象口座に本人確認を行う
S440
対象口座の本人確認結果に基づいて取り戻される口座の資産を処理する
S450
対象口座の凍結資産に基づいて、投票内容が有効であると確認された投票が属する対象参加者に、対象参加者の重みにより、インセンティブを与える

【図５】


資産取り戻しスマートコントラクト
本人確認結果：承認
本人確認結果：不承認
本人確認結果：参加者が不足で、結論が出ない
資産凍結
公開が投票と一致するため、投票行動にインセンティブを与える
公開が投票と一致しないため、投票行動にインセンティブを与えない
公開が投票と一致するため、投票行動にインセンティブを与える
対象参加者１
対象参加者２
対象参加者３

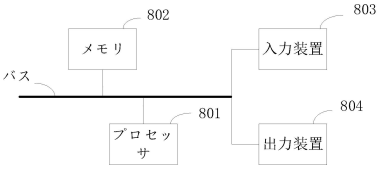
【図６】


S610
取り戻される口座に対する対象口座の資産取り戻しトランザクション要求に応答して、対象口座が取り戻される口座であるか否かの投票を開始する
S620
ブロックチェーンネットワーク内で取り戻される口座に対する介入口座からの身元宣言トランザクションが存在することが検出された場合に、取り戻される口座の公開鍵に基づいて介入口座の署名を検証する
S630
介入口座の署名検証が合格した場合、介入口座が取り戻される口座の所有者であると判定される
S640
対象口座が取り戻される口座であるか否かの投票を終了する

【図７】


700
ブロックチェーンによる資産処理装置
710
投票モジュール
740
資産凍結モジュール
760
身元介入モジュール
720
本人確認モジュール
7201
参加者決定ユニット
7202
投票検証ユニット
7203
本人確認ユニット
730
資産処理モジュール
750
インセンティブモジュール

【図８】


802
メモリ
803
入力装置
バス
801
プロセッサ
804
出力装置

フロントページの続き

弁理士　大貫 敏史
(74)代理人　100117189
弁理士　江口 昭彦
(74)代理人　100134120
弁理士　内藤 和彦
(74)代理人　100108213
弁理士　阿部 豊隆
(72)発明者　ジン，ボ
中華人民共和国，１０００８５ グァンドン プロヴィンス ５１８０００，シェンチェン，ナンシャン ディストリクト，ユエハイ ストリート，ビンハイ コミュニティ，ハイチャン ファースト ロード，バイドゥ インターナショナル ビルディング，ナンバー ６，イースト タワー，１階
審査官　貝塚 涼
(56)参考文献　特開２００３－０６７５３２（ＪＰ，Ａ）
国際公開第２０１９／０４３５８９（WO，Ａ１）
特開２０２０－０３５４３６（ＪＰ，Ａ）
Yanlin Zhu et al.，A Proposal For Account Recovery in Decentralized Applications，2019 IEEE International Conference on Blockchain (Blockchain)，IEEE，2019年07月14日，第148-155頁，DOI: 10.1109/Blockchain.2019.00028
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　１０／００ － ９９／００