

明 細 書

発明の名称：

暗号資産ブロックチェーン処理装置、処理方法、処理システム及び処理プログラム

技術分野

[0001] 本発明は、監査法人等で用いるための暗号資産ブロックチェーンデータを収集し、分析するためのシステムに関する。具体的には、暗号資産ブロックチェーンデータに含まれるブロック、トランザクション等に関する各種データを分析して、ビットコイン、イーサリアム等の各種仮想通貨（ここでは、「暗号資産」という）の取引情報（残高等）の監査を支援するためのシステムに関する。

背景技術

[0002] 不特定多数の個人または法人がインターネットを通じて商取引を実施する際の記録を共有し管理するための技術として、ブロックチェーンを用いた分散台帳技術がある。ブロックチェーンを用いた分散台帳技術は、その用途や目的等によって複数の実装方式が考案されており、それぞれの実装方式に応じたデータ記録の形式や方法が定義されている。

[0003] 一般的に、ビットコイン等の暗号資産の取引情報は、BLOCKCHAIR等のブロックエクスプローラ（非特許文献1）を用いて、インターネットを介して取得可能である。従来のブロックエクスプローラは、特定のアドレスまたはブロックを1つずつ指定して、所望の取引情報を得ることができる。また、各種暗号資産の取引情報が記録されたブロックチェーンにアクセスして、取引情報を取得することで、取引情報に基づいて取引内容の監査等を行うことができる（特許文献1）。

先行技術文献

特許文献

[0004] 特許文献1：特表2018-525729号公報

非特許文献

[0005] 非特許文献1：BLOCKCHAIR, URL <https://blockchair.com/>（2020年 8月27日検索）

発明の概要

発明が解決しようとする課題

- [0006] インターネット上で、従来のブロックエクスプローラのAPI（Application Programming Interface）を用いてブロックチェーンを検索するクエリを送信、取引情報を受信することは第三者にウォッチ（傍受）されるおそれがある。例えば、監査のために、インターネット上で、一定の期間に、あるコンピュータからブロックエクスプローラを用いてブロックチェーンを検索する複数のクエリを送信した場合には、そのコンピュータのIPアドレスとアドレス（暗号資産口座）の所有者との関係性や、同一の所有者に帰属する複数のアドレス等が特定され、互に関連付けられた（クラスタ化された）複数のアドレス、クエリの内容、及び、検索結果として得られた取引情報などを容易に紐づけること可能であり、悪用されるおそれがある。
- [0007] そこで、所定の期間を指定して、インターネット上に公開されているブロックチェーンを検索してデータ（ブロック、トランザクション等）を、プライベートネットワークにおけるサーバ等の計算機の記憶装置（データベース等）に、暗号資産の種別毎に蓄積することで、第三者に特定の取引に対するクエリや取引情報を傍受されることがないプライベートな環境下で、蓄積されたブロックチェーンデータを分析して、取引情報の監査等を行うことができる。
- [0008] しかしながら、ある暗号資産のブロックチェーンにおけるデータ（ブロック、トランザクション等）の記録を解釈するにあたり、通常はその実装方式を考案したソフトウェアの開発者が提供するソフトウェア（例えば、ノードソフトウェアのAPI）を用いて行う必要があるが、当該ソフトウェアの入出力方式も実装方式により異なるため、複数の異なる実装方式に応じたブロックチェーンデータを収集・分析するのは困難である。

- [0009] また、実装方式によっては、取引が実施された際の取引数量と取引に用いた単価に関する情報がそれぞれ別のデータレコードに記録されており、ある取引についてどれだけの金額の暗号資産が移動したかを知るためには、単価データと取引数量データをそれぞれ取得した上で、組み合わせて算出する（取引金額＝取引が実施された時間の単価×取引数量）必要があった。
- [0010] さらに、実装方式によっては、取引の参加者の暗号資産の持分残高は最新時点の情報しか記憶されておらず、過去に訴求した特定時点における残高情報を取得することができなかった。
- [0011] そのため、本発明では、複数の異なる実装方式で生成されたブロックチェーンデータを収集して、当該データを分析可能なデータに変換し、取引暗号資産の数量や単価、相手先等といった取引内容を標準化された形式に加工することで、会計監査等大量データの分析の利便性を向上させた暗号資産ブロックチェーン処理装置、処理方法、処理システム及び処理プログラム（以下、暗号資産ブロックチェーン処理装置等という）を提供する。

課題を解決するための手段

- [0012] 本発明に係る暗号資産ブロックチェーン処理装置の1つの実施形態として、前記暗号資産ブロックチェーン処理装置は、少なくとも
- データ収集部と、
 - データ変換部と、
- を含み、
- 前記データ収集部は、ユーザにより指定された暗号資産ブロックチェーンにアクセスして、所定の要求範囲に基づいて、前記暗号資産ブロックチェーンからブロックチェーンデータを収集し、
- 前記データ変換部は、前記ブロックチェーンデータを分析可能な取引データに変換し、
- 前記ブロックチェーンデータ及び前記分析可能な取引データは、前記暗号資産ブロックチェーン処理装置に接続されたデータ記憶装置に保存されることを特徴とする。

- [0013] 本発明に係る暗号資産ブロックチェーン処理装置の好ましい実施形態として、前記データ記憶装置は、前記暗号資産ブロックチェーン処理装置がネットワークを介してアクセス可能なクラウドストレージであることを特徴とする。
- [0014] 本発明に係る暗号資産ブロックチェーン処理装置の好ましい実施形態として、前記データ収集部は、スタティックモードで動作し、
前記スタティックモードで動作する前記データ収集部は、データバッチ毎の取引データ数を指定して前記要求範囲の終点を設定し、
前回収集したデータの最後の取引データの識別情報を、前記要求範囲の始点に設定することを特徴とする。
- [0015] 本発明に係る暗号資産ブロックチェーン処理装置の好ましい実施形態として、前記データ収集部は、ダイナミックモードで動作し、
前記ダイナミックモードで動作する前記データ収集部は、データバッチ毎のデータサイズを指定して前記要求範囲の終点を設定し、
前回収集したデータの最後の取引データの識別情報を、前記要求範囲の始点に設定することを特徴とする。
- [0016] 本発明に係る暗号資産ブロックチェーン処理装置の好ましい実施形態として、前記データ収集部は、自動収集モードで動作し、
前記自動収集モードで動作する前記データ収集部は、前記暗号資産ブロックチェーン上の最新データの識別情報を取得して、前記要求範囲の終点に設定し、
前記データ収集部により前回収集したデータの最後の取引データの識別情報を、前記要求範囲の始点に設定することを特徴とする。
- [0017] 本発明に係る暗号資産ブロックチェーン処理装置の好ましい実施形態として、前記データ収集部は、前回の収集モードが、データバッチ毎の取引データ数を指定したスタティックモード、又はデータバッチ毎のデータサイズを指定したダイナミックモードである場合に、前回収集したデータの最後の取引データの識別情報を、前記前回の収集モードの取引データ数又はデータサ

イズに基づいて再計算して、前記要求範囲の始点に設定することを特徴とする。

[0018] 本発明に係る暗号資産ブロックチェーン処理装置の好ましい実施形態として、前記ブロックチェーンデータは、識別可能なブロック番号が付与された、トランザクションデータを含み、

前記トランザクションデータは、1以上の単価設定用の単価トランザクションデータと、1以上の数量指定用の数量トランザクションデータとを少なくとも含み、

前記データ変換部は、前記1以上の数量トランザクションデータの各々について、該数量トランザクションデータに対して付与されたブロック番号に最も近いブロック番号が付与された単価トランザクションデータを検索し、検索した前記単価トランザクションデータの単価の値に、該数量トランザクションデータの数量を掛け合わせることで、取引に係る金額を算出することを特徴とする。

[0019] 本発明に係る暗号資産ブロックチェーン処理装置の好ましい実施形態として、前記データ記憶装置は、ブロックチェーンデータ記憶装置と取引データ記憶装置とを含み、

前記データ収集部によって収集された前記ブロックチェーンデータは、前記ブロックチェーンデータ記憶装置に保存され、

前記データ変換部によって算出された前記金額を含む取引データは前記取引データ記憶装置に保存されることを特徴とする。

[0020] 本発明に係る暗号資産ブロックチェーン処理装置の好ましい実施形態として、前記暗号資産ブロックチェーン処理装置は、データ分析部を更に含み、

前記データ分析部は、最初のブロック番号から特定時点のブロック番号までに合致する前記取引データを前記取引データ記憶装置から取得し、

取得した前記取引データの金額を、前記暗号資産ブロックチェーンにおける銀行口座番号に該当する記録単位であるアドレス毎に合算して残高を算出することを特徴とする。

[0021] 本発明に係る暗号資産ブロックチェーン処理装置の好ましい実施形態として、前記ブロックチェーンデータは、少なくともブロックデータとトランザクションデータとを含み、

前記データ変換部は、前記ブロックデータ及び前記トランザクションデータの各々に取引日時に関連する年月日の属性を付加して、年月日で区別可能な取引データに変換し、

前記取引データは年月日毎に分類されて前記データ記憶装置に保存されることを特徴とする。

[0022] 本発明に係る暗号資産ブロックチェーン処理装置の好ましい実施形態として、前記データ記憶装置は、ブロックチェーンデータ記憶装置と取引データ記憶装置とを含み、

前記データ収集部によって収集された前記ブロックチェーンデータは、前記ブロックチェーンデータ記憶装置に保存され、

前記データ変換部によって前記年月日の属性が付加され、年月日で区別可能な前記取引データは、前記取引データ記憶装置に保存されることを特徴とする。

[0023] 本発明に係る暗号資産ブロックチェーン処理装置の好ましい実施形態として、前記暗号資産ブロックチェーン処理装置は、データ分析部を更に含み、

前記データ変換部は、前記トランザクションデータを、トランザクション入力データとトランザクション出力データとに分け、

前記データ分析部は、前記暗号資産ブロックチェーンにおける銀行口座番号に該当する記録単位であるアドレス毎に、前記トランザクション入力データ及び前記トランザクション出力データに基づいて、特定のブロック番号の範囲で全収入及び全支出を計算することを特徴とする。

[0024] 本発明に係る暗号資産ブロックチェーン処理装置の好ましい実施形態として、前記暗号資産ブロックチェーン処理装置は、データ分析部を更に含み、

前記データ分析部は、前記暗号資産ブロックチェーンにおける銀行口座番号に該当する記録単位であるアドレス毎に、前記トランザクションデータ及

びスマートコントラクトの結果に基づいて、前記アドレス毎の残高を算出することを特徴とする。

[0025] 本発明に係る暗号資産ブロックチェーン処理装置の好ましい実施形態として、前記暗号資産ブロックチェーン処理装置は、整合性検証部を更に含み、前記取引データは、生成順にシーケンス番号が付与されたブロックデータを含み、

前記整合性検証部は、前記ブロックデータの前記シーケンス番号を順に照合することで、前記シーケンス番号の重複及び欠落のチェックを行い、

前記シーケンス番号に重複又は欠落があった場合には、前記シーケンス番号に対応する前記ブロックデータの不整合を通知することを特徴とする。

[0026] 本発明に係る暗号資産ブロックチェーン処理装置の好ましい実施形態として、前記整合性検証部は、所属するブロックのシーケンス番号を有するトランザクションデータについて、シーケンス番号ごとに前記トランザクションデータの数をカウントし、カウントした前記トランザクションデータの数と該シーケンス番号が付与されたブロックデータに記録されたトランザクション数とを比較し、

差分があった場合に、前記ブロックデータの不整合を通知することを特徴とする。

[0027] 本発明に係る暗号資産ブロックチェーン処理装置の好ましい実施形態として、前記暗号資産ブロックチェーン処理装置は、整合性検証部を更に含み、前記整合性検証部は、第三者が管理するブロックエクスプローラを用いて、ユーザにより指定されたアドレスの検証用残高を算出し、

前記データ分析部によって前記アドレス毎に算出された残高から、前記指定されたアドレスの残高を取得し、前記データ分析部により算出された前記残高と、前記検証用残高とを比較し、

差分があった場合に、前記指定されたアドレスのデータに不整合があることを通知することを特徴とする。

[0028] 本発明に係る暗号資産ブロックチェーン処理装置の好ましい実施形態とし

て、前記整合性検証部は、暗号資産のノードソフトウェアのバージョンを管理するサイトにアクセスし、所望の暗号資産のノードソフトウェアの最新バージョンを確認し、前記データ記憶装置に保存された前記暗号資産のノードソフトウェアのバージョンと比較し、バージョンに差異がある場合に、前記暗号資産のノードソフトウェアのバージョンに不整合があることを通知することを特徴とする。

[0029] 本発明に係る暗号資産ブロックチェーン処理方法の1つの実施形態として、前記方法は、ユーザにより指定された暗号資産ブロックチェーンにアクセスする段階と、

所定の要求範囲に基づいて、前記暗号資産ブロックチェーンからブロックチェーンデータを収集する段階と、

前記ブロックチェーンデータを分析可能な取引データに変換する段階と、
を含み、

前記ブロックチェーンデータ及び前記分析可能な取引データは、前記暗号資産ブロックチェーン処理装置に接続されたデータ記憶装置に保存される、
を含むことを特徴とする。

[0030] 本発明に係る暗号資産ブロックチェーン処理システムの1つの実施形態として、前記システムは、

情報処理端末と、

クラウドストレージと、

を含み、

前記暗号資産ブロックチェーン処理装置、前記情報処理装置及び前記クラウドストレージは、それぞれネットワークを介して接続されたことを特徴とする。

[0031] 本発明に係る暗号資産ブロックチェーン処理プログラムの1つの実施形態として、前記プログラムがコンピュータによって実行されることで、前記コンピュータを前記暗号資産ブロックチェーン処理装置の各部として機能させることを特徴とする。

[0032] 本発明に係る暗号資産ブロックチェーン処理プログラムの別の実施形態として、前記プログラムがコンピュータによって実行されることで、前記コンピュータに前記暗号資産ブロックチェーン処理方法の各段階を実行させることを特徴とする。

発明の効果

[0033] 本発明に係る暗号資産ブロックチェーン処理装置等は、インターネット上の暗号資産のブロックチェーンデータ（ブロック、トランザクション等）を収集して、第三者に特定の取引に対するクエリや取引情報を傍受されることがないプライベートな環境下にあるサーバ等の計算機の記憶装置（データベース等）に、暗号資産の種別毎に蓄積し、分析に適したデータ形式に変換することで、安全にブロックチェーンデータを分析して、監査のためにアドレス毎の残高等の算出を可能にするだけでなく、複数の異なる暗号資産の実装方式に応じたブロックチェーンデータを収集・分析を実現することができる。

[0034] また、暗号資産ブロックチェーン処理装置等は、暗号資産の実装方式によっては、取引が実施された際の取引数量と取引に用いた単価に関する情報がそれぞれ別のデータレコードに記録されているような場合に、単価データと取引数量データとから算出される取引金額（＝取引が実施された時間の単価×取引数量）が記録された仮想的なトランザクションデータ（取引データ）を生成することで、暗号資産の実装方式に影響されることなく、ある時点までの取引データを網羅的に集計することで、過去に訴求した特定時点における、取引の参加者の暗号資産の持分残高を容易に算出することができる。

[0035] さらに、収集したブロックチェーンデータの重複や欠落、暗号資産のノードソフトウェアのバージョンの違い等を検証することで、分析の対象となる取引データの整合性を担保することができる。

図面の簡単な説明

[0036] [図1]本発明の一実施形態に係る暗号資産ブロックチェーン処理システムの構成を示す図である。

[図2]本発明の一実施形態に係る暗号資産ブロックチェーン処理装置のハードウェア構成の一例を示すブロック図である。

[図3]本発明の一実施形態に係る暗号資産ブロックチェーン処理装置の構成を示すブロック図である。

[図4]ブロックチェーンデータを収集する処理の流れを示すフローチャートである。

[図5]収集したブロックチェーンデータ（レベル1データ）を、分析可能な取引データ（レベル2データ）に変換する処理の流れを示すフローチャートである。

[図6]ビットコインのブロックチェーンのデータを収集して分析する処理フローの概要を示す図である。

[図7]ブロックチェーン中の1つのブロック情報を表示するブロックエクスプローラの表示画面の一例を示す図である。

[図8]収集したブロック情報の一例を示す図である。

[図9]ブロックチェーン中の1つのトランザクション情報を表示するブロックエクスプローラの表示画面の一例を示す図である。

[図10]収集したトランザクション情報の一例を示す図である。

[図11]図8及び図10に示すブロック情報及びトランザクション情報（レベル1データ）を年月日で区別可能な情報（レベル2データ）にしてフォルダに格納した一例を示す図である。

[図12]図11に示す1つのフォルダに格納されたブロック情報の一例を示す図である。

[図13]ビットコインのレベル1データの構成と対応するレベル2データの構成の一例を示す図である。

[図14]ビットコインのレベル1データの構成と対応するレベル2データの構成の一例を示す図である。

[図15]イーサリアムのブロックチェーンのデータを収集して分析する処理フローの概要を示す図である。

[図16]イーサリアムのレベル1データの構成と対応するレベル2データの構成の一例を示す図である。

[図17]イーサリアムのレベル1データの構成と対応するレベル2データの構成の一例を示す図である。

[図18]イーサリアムのレベル1データの構成と対応するレベル2データの構成の一例を示す図である。

[図19]イーサリアムのレベル1データの構成と対応するレベル2データの構成の一例を示す図である。

[図20]イーサリアムのレベル1データの構成の一例を示す図である。

[図21]トランザクションにおいて単価と金額が分離して記録されたデータを対象とした金額算出方法の処理の流れを示すフローチャートである。

[図22]ノードソフトウェアのAPIで取得できるトランザクションデータの一例を示す図である。

[図23]図22に示すトランザクションデータに対して、図22に示す処理を行うことにより得られる仮想的なトランザクションデータの一例を示す図である。

[図24]変換したデータ（取引データ）の重複・欠落を検出する処理の流れを示すフローチャートである。

[図25]ブロックデータの欠落の一例を示す図である。

[図26]トランザクションデータの重複の一例を示す図である。

[図27]本発明の一実施形態に係る暗号資産ブロックチェーン処理装置により実現される残高確認の仕組みを説明する模式図である。

[図28]暗号資産のブロックチェーン上でのバージョンアップデートを随時比較して自動的に生成したレポートの一例を示す図である。

発明を実施するための形態

[0037] 以下に図面を参照して、本発明の実施形態についてそれぞれ説明する。なお、実施形態を説明するための全ての図において、同じものには原則として同一の符号を付し、その繰り返しの説明は省略する。本発明の個々の実施形

態は、独立したものではなく、それぞれ組み合わせて適宜実施することができる。

[0038] 図1は、本発明の一実施形態に係る暗号資産ブロックチェーン処理システムの構成を示す。暗号資産ブロックチェーン処理システムは、例示的に、暗号資産ブロックチェーン処理装置10と、情報処理端末20と、クラウドストレージ（オンラインストレージ）30とを含む。暗号資産ブロックチェーン処理装置10は、例えば、サーバ等のネットワークNに接続可能なコンピュータである。また、情報処理端末20は、例えば、パーソナルコンピュータ、ノートパソコン、スマートフォン、携帯電話等、ネットワークNに接続可能な端末である。

[0039] ネットワークNは、例えば、インターネット等のオープンなネットワークであっても良いし、専用回線で接続されたイントラネットであり、クローズドネットワークであっても良い。ネットワークNは、これに限定されるものではなく、要求されるセキュリティのレベル等に応じて、適宜、クローズドネットワークとオープンネットワークを組み合わせることもできる。

[0040] 暗号資産ブロックチェーン処理システムは、1つの実施形態として、少なくとも暗号資産ブロックチェーン処理装置10と、暗号資産ブロックチェーン処理装置10とネットワークNを介して接続された情報処理端末20とを備える。ユーザは、暗号資産ブロックチェーン処理装置10を直接操作すること又は、情報処理端末20を介して操作することで、インターネット上に公開された暗号資産に関するブロックチェーン（以下、暗号資産ブロックチェーンという）にアクセスして、ブロックチェーンに記録されたデータ（以下、ブロックチェーンデータという）を、暗号資産ブロックチェーン処理装置10の記憶装置に蓄積することができる。別の実施形態として、暗号資産ブロックチェーン処理システムは、暗号資産ブロックチェーン処理装置10の記憶装置に代えて、暗号資産ブロックチェーンから収集したブロックチェーンデータをクラウドストレージ30に蓄積することができる。

- [0041] 暗号資産ブロックチェーン処理装置10の記憶装置、クラウドストレージ30を、外部からのアクセスを遮断したクローズドな環境（プライベートな環境）下で運用することで、第三者に特定の取引に対するクエリや取引情報を傍受されることを防止することができる。
- [0042] 図2は、本発明の一実施形態に係る暗号資産ブロックチェーン処理装置のハードウェア構成の一例を示すブロック図である。なお、図中では、暗号資産ブロックチェーン処理装置10のハードウェアに対応する符号には括弧を付すことなく記載し、情報処理端末20のハードウェアに対応する符号には括弧を付して記載する。
- [0043] 暗号資産ブロックチェーン処理装置10は、例えばサーバ（コンピュータ）であり、例示的には、CPU（Central Processing Unit）11と、ROM（Read Only Memory）及びRAM（Random Access Memory）等からなるメモリ12と、バス13と、入出力インターフェース14と、入力部15と、出力部16と、記憶部17と、通信部18と、を備えている。
- [0044] CPU11は、メモリ12に記録されているプログラム、又は、記憶部17からメモリ12にロードされたプログラムにしたがって各種の処理を実行する。CPU11は、例えば、サーバ（コンピュータ）を本発明の暗号資産ブロックチェーン処理装置として機能させるためのプログラムを実行することができる。また、暗号資産ブロックチェーン処理装置の少なくとも一部の機能を、特定用途向け集積回路（ASIC）等でハードウェア的に実装することも可能である。
- [0045] メモリ12には、CPU11が各種の処理を実行する上において必要なデータ等も適宜記憶される。CPU11及びメモリ12は、バス13を介して相互に接続されている。このバス13には、入出力インターフェース14も接続されている。入出力インターフェース14には、入力部15と、出力部16と、記憶部17と、通信部18と、が接続されている。
- [0046] 入力部15は、各種ボタン、タッチパネルあるいはマイク等で構成され、

暗号資産ブロックチェーン処理装置 10 のユーザ等の指示操作に応じて各種情報を入力する。なお、入力部 15 は、暗号資産ブロックチェーン処理装置 10 の他の各部を収容する本体とは独立した、キーボードやマウス等の入力装置により実現されてもよい。

[0047] 出力部 16 は、ディスプレイやスピーカ等で構成されており、静止画又は動画などの画像データや音声データを出力する。出力部 16 が出力した画像データや音楽データは、ディスプレイやスピーカ等から、画像や音楽としてユーザが認識可能に出力される。

[0048] 記憶部 17 は、DRAM (Dynamic Random Access Memory) 等の半導体メモリ、ソリッドステートドライブ (SSD)、ハードディスク等の記憶装置で構成され、各種データを記憶することができる。

[0049] 通信部 18 は、他の装置との間で行う通信を実現する。例えば、通信部 18 は、ネットワーク N を介して、情報処理端末 20、クラウドストレージ 30 との間で相互に通信を行うことができる。

[0050] なお、暗号資産ブロックチェーン処理装置 10 には、不図示であるがドライブを必要に応じて適宜設けられる。ドライブには、例えば、磁気ディスク、光ディスク、光磁気ディスク、あるいは半導体メモリ等から構成されるリムーバブルメディアが適宜装着される。リムーバブルメディアには、暗号資産ブロックチェーンにアクセスして、ブロックチェーンデータの収集を実行するためのプログラムや、テキストデータ、画像データ等の各種データが格納される。ドライブによってリムーバブルメディアから読み出されたプログラムや、各種のデータは、必要に応じて記憶部 17 にインストールされる。

[0051] 次に、情報処理端末 20 のハードウェアの構成について説明する。情報処理端末 20 は、図 2 に示すように、例示的に、CPU 21 と、メモリ 22 と、バス 23 と、入出力インターフェース 24 と、入力部 25 と、出力部 26 と、記憶部 27 と、通信部 28 と、を備えている。これら各部は、上述の暗号資産ブロックチェーン処理装置 10 が備える、符号のみが異なる同名の各

部と同等の機能を有している。従って、重複する説明を省略する。なお、情報処理端末20を、携帯型の装置として構成する場合には、情報処理端末20が備える各ハードウェアと、ディスプレイやスピーカとを一体の装置として実現するようにしてもよい。

[0052] 図3を参照して、暗号資産ブロックチェーン処理システムに含まれる暗号資産ブロックチェーン処理装置10の機能的構成について説明する。図3は、本発明の一実施形態に係る暗号資産ブロックチェーン処理装置の構成を示すブロック図である。例えば、サーバ（コンピュータ）によって、ブロックチェーンデータの収集、変換、分析、整合性検証等の処理を行うためのプログラムが実行された場合に、当該サーバは、例示的に、暗号資産ブロックチェーン処理装置10として機能し、CPU11に加えてメモリ12等のハードウェア資源において、データ収集部111、データ変換部112、データ分析部113、整合性検証部114が機能する。

[0053] また、記憶部17の一部の記憶領域を用いて、記憶部17をブロックチェーンデータ記憶装置171及び取引データ記憶装置172として機能させることができる。別の実施形態として、ブロックチェーンデータ記憶装置171及び取引データ記憶装置172を、暗号資産ブロックチェーン処理装置10とは、別体の外部記憶装置で構成することもでき、外部記憶装置として例えばクラウドストレージ30を用いることもできる。これらの実施形態では、ブロックチェーンデータ記憶装置171と取引データ記憶装置172とに分けているが、分けずに1つのデータ記憶装置としてもよい。ブロックチェーンデータ記憶装置171及び取引データ記憶装置172に記憶される情報の詳細は後述する。

[0054] 暗号資産ブロックチェーン処理装置10は、従来のノードソフトウェアが提供するAPIを用いて、インターネット上に公開された暗号資産に関するブロックチェーンに記録されたデータを要求し、ダウンロードしたブロックチェーンデータ（ここでは、レベル1データとも称する）をデータ記憶装置であるブロックチェーンデータ記憶装置171に保存する。この処理をバツ

チ処理で行うことができる。暗号資産ブロックチェーンからブロックチェーンデータ（レベル1データ）をダウンロードするためには、暗号資産の異なる実装方式に対応したノードを展開する必要がある、暗号資産ブロックチェーン処理装置10を複数設けて、それぞれ暗号資産の異なる実装方式に対応したノードとして機能させることができる。ブロックチェーンデータ（レベル1データ）は、暗号資産ブロックチェーン処理装置10（ノード）において取引データ（レベル2データ）に変換され、当該ノード介してクラウドストレージ30に転送して保存することもできる。

[0055] 暗号資産ブロックチェーン処理システムでは、例えば、ビットコイン（Bitcoin）や、そこから派生したビットコインキャッシュ（Bitcoin Cash）等のUTXO型の暗号資産、イーサリアム（Ethereum）や、ネム（Nem）等のアカウント型の暗号資産などといった種類の暗号資産を取り扱うことができる。

[0056] 暗号資産ブロックチェーン処理装置10は、ネットワーク上に公開された暗号資産ブロックチェーンからブロックチェーンデータを収集するために、要求するデータの範囲を指定する。暗号資産ブロックチェーン処理装置10は、データの範囲指定のために3種類のモードを備え、いずれかのモードに設定することで、ブロックチェーンデータの収集を実行することができる。

[0057] 3種類のモードには、スタティックモード、ダイナミックモード、自動収集モードがある。スタティックモード及びダイナミックモードでは、ブロックチェーンデータの収集はバッチ処理で行われる。

[0058] スタティックモードでは、バッチ毎のデータ数（取引を記録したデータの数）が指定され、暗号資産ブロックチェーン処理装置10は、指定されたデータ数に応じて、ブロックチェーンデータを収集することができる。例えば、バッチ毎のデータ数が1000と指定されていた場合には、1000個のブロックチェーンデータ（すなわち、取引を記録したデータ）を収集し、ブロックチェーンデータ記憶装置171にフォルダ毎に分けて当該データを保存することができる。

[0059] ダイナミックモードでは、バッチ毎のデータサイズを指定され、暗号資産

ブロックチェーン処理装置10は、指定されたデータサイズに応じて、ブロックチェーンデータを収集することができる。例えば、バッチ毎のデータサイズが250MBと指定されていた場合には、250MBのブロックチェーンデータ（取引を記録したデータ）を収集することができる。なお、暗号資産ブロックチェーンにおけるブロック毎に、取引を記録したデータの数は一ではないため、データサイズを指定した場合には、同じデータサイズのブロックチェーンデータでも、ブロックの数は異なることもある。

[0060] 自動収集モードでは、暗号資産ブロックチェーン処理装置10において、ブロックチェーンの要求範囲等が自動で設定される。自動収集モードの処理の流れは、図4に示す。図4は、ブロックチェーンデータを収集する処理の流れを示すフローチャートである。ユーザは情報処理端末20等を用いて、指定された暗号資産ブロックチェーンに対応した暗号資産ブロックチェーン処理装置10（ノード）を起動する（ステップS101）。暗号資産ブロックチェーン処理装置10は、ユーザにより指定された暗号資産ブロックチェーンにアクセスする。

[0061] 暗号資産ブロックチェーン処理装置10は、ユーザにより指定された暗号資産ブロックチェーンと同期する（ステップS102）。例えば、暗号資産ブロックチェーン処理装置10が保持する記録台帳は、同一のブロックチェーンネットワーク上で、他のノードが保持する記録台帳と同期される。同期することにより、暗号資産ブロックチェーンにおいて、未収集のブロックチェーンデータを特定することができる。

[0062] 暗号資産ブロックチェーン処理装置10は、暗号資産ブロックチェーンにおいて最新取引を記録したデータを計算する。例えば、ブロックチェーンデータに含まれるブロックヘッダから、個々のブロックに付与された識別番号（識別情報）を取得して、最新取引を記録したデータを特定する（ステップS103）。そして、暗号資産ブロックチェーン処理装置10は、当該データのブロックヘッダに基づいて、データの要求範囲の終点を設定する（ステップS104）。

- [0063] 暗号資産ブロックチェーン処理装置10は、前回のデータ収集の実行で収集したデータにおいて、最後の取引が記録されたデータのブロックヘッダを、データ記憶装置（例えば、取引データ記憶装置172）に保存されたデータに基づいて計算する。例えば、ブロックチェーンデータに含まれるブロックヘッダから、個々のブロックに付与された識別番号（識別情報）を取得して、最後取引を記録したデータを特定する（ステップS105）。また、暗号資産ブロックチェーン処理装置10は、必要に応じて前回のデータ収集の実行で収集したデータにおいて、最後の取引が記録されたデータのブロックヘッダを、モード（スタティックかダイナミックか）に基づいて再計算する（ステップS106）。これは、前回実行したデータ収集を、スタティックモードで指定されたデータの数に応じて要求範囲を設定したのか、ダイナミックモードで指定されたデータサイズに応じて要求範囲を設定したのかを特定することで、今回のデータ収集で、始点となる最後の取引が記録されたデータのブロックヘッダを正確に特定することができる。
- [0064] 暗号資産ブロックチェーン処理装置10は、前回のデータ収集の実行で収集したデータにおいて、最後の取引が記録されたデータのブロックヘッダに基づいて、データの要求範囲の始点を設定する（ステップS107）。なお、初めてデータ収集を実行する場合には、暗号資産ブロックチェーン処理装置10は、ブロックチェーンの最初のブロック（ジェネシスブロック）をデータの要求範囲の始点として設定し、ステップS105及びS106のような処理を省略することができる。
- [0065] ブロックチェーンデータの要求範囲を設定すると、暗号資産ブロックチェーン処理装置10は、暗号資産ブロックチェーンが当該要求範囲の終点に同期するまで待ち（ステップS108）、同期した後、ブロックチェーンデータの要求範囲に基づいてデータ収集を開始する（ステップS109）。暗号資産ブロックチェーン処理装置10は、収集したブロックチェーンデータ（レベル1データ）をブロックチェーンデータ記憶装置に保存する。
- [0066] 図5は、収集したブロックチェーンデータ（レベル1データ）を、分析可

能な取引データ（レベル2データ）に変換する処理の流れを示すフローチャートである。暗号資産ブロックチェーン処理装置10は、ブロックチェーンデータ記憶装置171に蓄積されたブロックチェーンデータ（レベル1データ）を読み込み（ステップS121）、分析可能なデータ形式、すなわち、アドレス（口座）毎に暗号資産の残高等を計算することが可能なデータ形式の取引データ（レベル2データ）に変換し（ステップS122）、変換後のデータを取引データ記憶装置172に保存する（ステップS123）。そして、必要に応じて、暗号資産ブロックチェーン処理装置10は、暗号資産ブロックチェーンにおける銀行口座番号に該当する記録単位であるアドレスを、無作為に抽出して、変換したデータの整合性を検証する（ステップS124）。整合性の検証の詳細は、後述する（図21から図26、及びそれらの説明を参照）。暗号資産のレベル1データをレベル2データに変換する処理フローとして、ビットコインの例を図6、イーサリアムの例を図15に示す。

[0067] 図6は、ビットコインのブロックチェーンのデータを収集して分析する処理フローの概要を示す。ユーザは、情報処理端末20を用いて、ビットコイン（bitcoin）の実装方式に対応した暗号資産ブロックチェーン処理装置（図6におけるノード10a）を起動して、他のノードと同期する（図4中のステップS101からS102に対応）。同期後、ノード10aは、ブロックチェーンデータ（レベル1データ）を収集する（図4中のステップS103からS110に対応）。

[0068] レベル1データは、ノード10aを介して、ブロックチェーンから直接収集したブロックチェーンデータである。レベル1データはブロックデータ（図6中のblocks）とトランザクションデータ（図6中のtransactions）に分けられる。ブロックチェーンにおけるブロックとは、数十から数百のトランザクション（決済）を収納する箱のようなもので、一般的なブロックチェーンの構造として、ブロックチェーン上にある取引記録（トランザクション）の承認作業はブロックのレベルで行われる。

[0069] ノード10aにより収集されたブロックデータは、一番初めに記録されたブロック（ジェネシスブロック）を起源とし、最新取引のブロック又は指定された過去のブロックまでの全ブロックと、それぞれのブロック情報（ブロックの内容を一方方向性関数によりハッシュ化して算出されたハッシュ値（Hash）、ブロックID、ビット数（Bit）、ブロックが記録されたタイムスタンプ（Timestamp）等）とを含む。

[0070] ビットコインのブロックチェーンデータの各ブロック情報の一例を図7に示す。図7は、ブロックチェーン中の1つのブロック情報を表示するブロックエクスプローラ（例えば、BLOCKCHAIR）の表示画面の一例である。図7にあるブロック“80234”は前に承認された“80233”と後に承認された“80235”の間にある。この80234のブロック情報（ハッシュ値、タイムスタンプ（Mined on））のデータは、図8のフォーマットでノード10aから収集される。図8は、ノード10aにより収集したブロック情報の一例を示す。例えば、ブロック“80234”のブロック情報は、JSON形式のフォーマットで下記のとおり記述される。

```
{ "hash": "0000000002862a0885ec35cd86b8d95b1e1c0ba182845198b2a5b904d1dfb3e", "size": 473, "stripped_size": 473, "weight": 1864, "number": 80234, "version": 1, "merkle_root": "729dff922569517e33b6f0e72ea567e53155df30736ef8625e25cf5123c0af68", "timestamp": 1284707604, "nonce": "122e0a2", "bits": "1b5bede6", "coinbase_param": "04e6ed5b1b021c01", "transaction_count": 2 }
```

[0071] また、ブロック“80234”のブロック情報に含まれるトランザクションの一例は、図9に示すとおりである。図9は、ブロックチェーン中の1つのトランザクション情報を表示するブロックエクスプローラ（BLOCKCHAIR）の表示画面の一例を示す。図9に示す例では、トランザクションは、ビットコインの送り主（Senders）と受け取り主（Recipients）などが表記される。これらのデータは収集される際には図10に示すフォーマット（JSON）で収集される。

- [0072] 図10は、ノード10aにより、収集したトランザクション情報の一例を示し、図11は、図8及び図10に示すブロック情報及びトランザクション情報（レベル1データ）を年、月、日で区別可能な情報（レベル2データ）にしてフォルダに格納した一例を示す。レベル2データは、タイムスタンプ等の情報をもとに、全レベル1データに年月日の属性を付加して、年月日で検索可能なデータに変換される。レベル2データは、年月日毎にフォルダに保存される。
- [0073] 図12は、図11に示す1つのフォルダに格納されたブロック情報の一例を示す。図12に示す例では、ブロック情報の2009年12月18日のフォルダにはその日に記録されたブロックの情報が含まれる。同じようにトランザクションデータも年、月、日ごとに分けられる。またトランザクションデータはトランザクション入力（Transaction Input）とトランザクション出力（Transaction Output）とにも分けられる。なお、これはビットコイン特有のUTXO（Unspent Transaction Output）方式により、口座ごとの残高はある特定のブロック範囲で口座ごとの全支出と全収入を計算しなければならない。
- [0074] 図13及び図14は、ビットコインのレベル1データの構成と対応するレベル2データの構成の一例を示す。基本的には、ビットコインのブロックデータ（block）のレベル2データの項目は、レベル1データの項目に年月日（year, month, day）の項目が付加されている。従来のブロックエクスプローラのAPIを用いて取得できるビットコインのブロックに関する項目（hash, size, stripped_size等）は、図13に示すブロックのテーブルの中央の欄に記載され、テーブルの右の欄には各項目のデータ型（string, bigint等）が記載されている。図14に示すトランザクション（transactions, transaction_input, transaction_output）のテーブルについても、同様の表記である。
- [0075] ビットコインのトランザクションデータ（transactions）は、レベル2データとして、トランザクション入力データとトランザクション出力データに

分けられ、それぞれに年月日 (year, month, day) の項目が付加されている。

- [0076] 暗号資産の別の例として、イーサリアムのノードからブロックチェーンデータを収集する場合についても以下に説明する。図15は、イーサリアムのブロックチェーンのデータを収集して分析する処理フローの概要を示す。ユーザは、情報処理端末20を用いて、イーサリアム (ethereum) の実装方式に対応した暗号資産ブロックチェーン処理装置 (図15におけるノード10b) を起動して、他のノードと同期する (図4中のステップS101からS102に対応)。同期後、ノード10bは、ブロックチェーンデータ (レベル1データ) を収集する (図4中のステップS103からS110に対応)。イーサリアムを対象とした暗号資産ブロックチェーン処理装置による同期、収集、分析処理は、基本的には、ビットコインを対象とした場合の処理と実質的には同じ流れとなる。
- [0077] イーサリアムのレベル1データは、ビットコインのレベル1データとは異なるため、変換処理については、イーサリアム向けの変換が必要となる。例えば、イーサリアムは、ビットコインのUTXO方式ではないため、イーサリアムの方式に基づいたトランザクション及びスマートコントラクトの処理結果を計算に利用できるように変換する必要がある。図15に示されるように、イーサリアムのレベル1データは、CSV形式のブロックデータ (blocks) の他に、同じくCSV形式で、トークントランスファ (token_transfers)、コントラクト (contracts)、トークン (tokens) トレース (traces)、レシート (receipts)、ログ (logs)、トランザクション (transactions) といったデータを含む。
- [0078] 図16から図19は、イーサリアムのレベル1データの構成と対応するレベル2データの構成の一例を示し、図20は、イーサリアムのレベル1データの構成の一例を示す。図13及び14で示したビットコインのデータの構成と同様に、各テーブルは、中央の欄にデータの項目、及び右の欄にデータの型が記載されている。基本的には、イーサリアムのブロックデータ (block

s) のレベル 2 データの項目は、レベル 1 データの項目に年月日 (year, month, day) の項目が付加されている (図 16 参照)。

[0079] イーサリアムのレベル 2 データのトークントランスファ (token_transfers) では、レベル 1 データに含まれるトークントランスファ (token_transfers) とトークン (token) とがマージされ、マージの際にそれぞれ不要な項目が削除され、年月日 (year, month, day) の項目が付加されている (図 17 参照)。また、イーサリアムのレベル 2 データのインターナルトランザクション (internal_transactions) では、レベル 1 データに含まれるトレース (traces) に、ステータス (status)、タイムスタンプ (timestamp)、年月日 (year, month, day) の項目が付加されている (図 18 参照)。

[0080] さらに、イーサリアムのレベル 2 データのトランザクション (transactions) では、レベル 1 データに含まれるトランザクション (transactions) とレシート (receipts) とがマージされ、マージの際にそれぞれ不要な項目が削除され、タイムスタンプ (timestamp)、年月日 (year, month, day) の項目が付加されている (図 19 参照)。図 20 に示すレベル 1 データに含まれるコントラクト (contracts) とログ (logs) については、特にレベル 2 データに変換されない。

[0081] 本発明の暗号資産ブロックチェーン処理システムでは、ビットコインの例 (図 6 から図 14)、イーサリアムの例 (図 15 から図 20) のように、他の暗号資産についても、実装方式に対応した暗号資産ブロックチェーン処理装置 (ノード) を設けて、ユーザが指定する暗号資産に対応したノードにアクセスすることで、所望の暗号資産のブロックチェーンデータを収集することができる。

[0082] 各種暗号資産の実装方式に対応した暗号資産ブロックチェーン処理装置 10 (10a、10b 等) は、それぞれ、ブロックチェーンの P2P ネットワーク上の他のノードと同期して、ブロックチェーンデータ (レベル 1 データ) を収集して、残高等の計算である分析可能な取引データ (レベル 2 データ) に変換して、取引データの分析を行うといった処理の命令を定期的に行

する（バッチ処理を行う）。例えば、暗号資産ブロックチェーン処理装置 10 は、定期的にそれらの命令を実行することで、取引対象の単価設定に関するデータを取得し、特定時点の単価に関するデータとその単価が設定された時点に関するデータと組み合わせて、任意時点における単価を参照することを可能とするデータテーブルを作成し、データ記憶装置（例えば、ブロックチェーンデータ記憶装置 171）に記憶することができる。また、暗号資産ブロックチェーン処理装置 10 は、取引の時点及び数量に関するデータを取得し、ブロックチェーンデータ記憶装置 171 に記憶することもできる。

[0083] 図 21 は、トランザクションにおいて単価と金額が分離して記録されたデータを対象とした金額算出方法の処理の流れを示すフローチャートである。また、図 22 は、ノードソフトウェアの API で取得できるトランザクションデータの一例を示し、図 23 は、図 22 に示すトランザクションデータに対して、図 21 に示す処理を行うことにより得られる仮想的なトランザクションデータの一例を示す。

[0084] 暗号資産ブロックチェーン処理装置 10 は、単価と金額が分離して記録されたデータを分析対象とした場合に、例えば、図 21 に示すような処理の流れで、データから金額の算出が行われ、単価と数量と金額を記録した仮想的なトランザクションを生成して元のデータに記録された内容を更新したものを取引データ記憶装置 172 に保存する。このように、ブロックチェーンデータ記憶装置 171 に保存されたブロックチェーンデータを、分析可能なデータ形式、すなわち、アドレス毎の残高等を計算可能なデータ形式の取引データに変換して、取引データを取引データ記憶装置 172 に保存することができる。

[0085] 図 22 及び図 23 に示すトランザクションデータの一例を参照しながら、図 21 に示す処理の流れについて説明する。まず、暗号資産ブロックチェーン処理装置 10 は、単価設定用のトランザクションデータ（単価トランザクションデータという）をブロックチェーンデータ記憶装置 171 から取得し（ステップ S131）、数量指定用のトランザクションデータ（数量トラン

ザクションデータという)をブロックチェーンデータ記憶装置171から取得する(ステップS132)。図22に示す例では、例えば、単価トランザクションデータは、ブロックの識別番号であるブロック高(block height)が500、520、540、541のトランザクションであり、数量トランザクションデータは、ブロック高が510、530、550のトランザクションである。

[0086] 各データを取得した後、暗号資産ブロックチェーン処理装置10は、個々の数量トランザクションデータについて、ブロック番号が最も直近となる単価トランザクションデータを検索し(ステップS133)、検索した単価トランザクションデータの単価の値を、数量トランザクションデータに追加する(ステップS134)。例えば、ブロック高が510のトランザクションについて、ブロック高(番号)が最も直近となる単価トランザクションデータを検索すると、ブロック高が500のトランザクションが見つかり(図22参照)、当該トランザクションの単価(50)が、ブロック高が510のトランザクションに追加される(図23参照)。同様に、ブロック高が530のトランザクションには、ブロック高が520のトランザクションの単価(100)が追加され、ブロック高が550のトランザクションには、ブロック高が541のトランザクションの単価(110)が追加される。

[0087] 数量トランザクションデータに、単価トランザクションデータに記録された単価を追加した後、暗号資産ブロックチェーン処理装置10は、単価が追加された数量トランザクションデータ(図23中のブロック高が510、530、550のトランザクション)毎に、単価の値に、数量の値を掛け合わせることで、取引に係る金額を算出し、当該金額をそのトランザクションに追加し、取引データ記憶装置に保存する(ステップS135)。同様に、単価トランザクション(図23中のブロック高が500、520、540、541のトランザクション)も、取引データ記憶装置に保存する(ステップS136)。

[0088] 本発明に係る暗号資産ブロックチェーン処理システムのユーザは、任意の

タイミングで、暗号資産ブロックチェーン処理装置10によってデータ収集、データ変換（データ加工）等の命令を実行することで、暗号資産ブロックチェーン処理装置10は、ある時点までの取引データを網羅的に集計し、そのタイミングにおける取引の参加者の暗号資産の持分残高を算出し、アドレス（ブロックチェーンにおける銀行口座番号に該当する記録単位）毎の残高データ（TSV形式、CSV形式等）を作成した上で取引データ記憶装置172に保存することができる。

[0089] 暗号資産ブロックチェーン処理装置10は、特定時点のアドレス毎の残高の算出方法として、例えば、ジェネシスブロックから特定のブロック高までに合致するすべてのトランザクションデータを取引データ記憶装置172から取得し、取得したトランザクションデータの金額をアドレス毎に合算して、取引データ記憶装置172に保存することができる。取引データ記憶装置172に保存された取引データを用いることで、暗号資産ブロックチェーン処理装置10は、例えば、監査のために、アドレス毎の暗号資産の残高等を分析することができる。暗号資産ブロックチェーン処理システムのユーザは、作成された取引データや残高データを、任意に抽出することができ、情報処理端末20のモニター等に表示させ、内容を確認することができる。また、作成された取引データや残高データを、さらに別のデータ記憶装置等に記憶させ、ブロックチェーン以外から入手した帳簿記録等との比較を行うこともできる。

[0090] 暗号資産ブロックチェーン処理装置10は、定期的に取り引データ記憶装置172に保存した取引データの管理情報を用いて、インターネット上のブロックチェーンデータが重複、欠落なく記録されていることを検証し、不整合が発生した場合は、アラートを発生して、暗号資産ブロックチェーン処理システムのユーザに通知することができる。例えば、暗号資産ブロックチェーン処理装置10は、不整合を検出した場合に、ネットワークNを介して接続された情報処理端末20にアラートを通知して、ユーザに知らせることができる。

[0091] 図24は、変換したデータ（つまり、暗号資産の残高等を計算することが可能なデータ形式の取引データ）の重複・欠落を検出する処理の流れを示すフローチャートである。図25はブロックデータの欠落の一例を示し、図26はトランザクションデータの重複の一例を示す。暗号資産ブロックチェーン処理装置10は、ブロックデータ、及びトランザクションデータ等を含む取引データをデータ記憶装置（例えば、取引データ記憶装置172）から読み込む（ステップS141）。取引データに含まれるブロックデータは、生成順に0又は1（ジェネシスブロック番号）から始まる連続番号（シーケンス番号）が付与されている。暗号資産ブロックチェーン処理装置10は、ブロックデータのブロック番号（シーケンス番号）に重複がないか、欠落がないかを順に検証し（ステップS142）、重複又は欠落がある場合（ステップS142のいいえ）には、取引データに含まれるブロックに不整合がある旨を知らせる整合性エラーを（例えば、情報処理端末20を介して）ユーザーに通知する（ステップS145）。

[0092] 例えば、ブロックデータの欠損は、図25に示されるように、ブロックAからブロックCのブロック番号（ブロック高、height）1から順にみていくと、ブロック番号が3のブロックデータが、データ記憶装置（例えば、取引データ記憶装置172）には記憶されていないような状態である。

[0093] 暗号資産ブロックチェーン処理装置10は、ブロック番号に基づいて順にブロックAからブロックCを確認すると、ブロック番号が3のブロックデータが欠落していることを検出することができる。

[0094] ブロックデータに重複及び欠損がない場合（ステップS142のはい）には、暗号資産ブロックチェーン処理装置10は、トランザクションデータの各々にある所属ブロックのシーケンス番号を用いて、シーケンス番号毎にブロックデータに関連するトランザクションの数をカウントし（ステップS143）、カウントした結果（トランザクションの数）と、ブロックデータに記録されたトランザクション数（図26中の“tra_cnt”）とを比較し（ステップS144）、差分があった場合（一致しない場合）（ステップS144

のいいえ)には、取引データに含まれるトランザクションに不整合がある旨を知らせる整合性エラーを(例えば、情報処理端末20を介して)ユーザに通知する(ステップS145)。

[0095] 例えば、トランザクション数の不一致は、図26に示されるように、ブロック番号(ブロック高)が2(height:2)であるブロックデータに含まれるトランザクション数が2である(tra_cnt:2)のに対して、ブロック番号2のブロックデータに関連するトランザクションA、B、Cの数(トランザクションのハッシュの数(tra_hash))をカウントした結果が3であるような状態である。

[0096] 暗号資産ブロックチェーン処理装置10は、ブロック番号毎にブロックデータ(height:2)に関連するトランザクションA、B、Cをカウントし、カウントした結果(図26の例では、3)と、ブロックデータに記録されたトランザクション数(tra_cnt)(図26の例では、2)とを比較して、図26に示されるように「ブロック中のトランザクション数(tra_cnt) 2 < トランザクションのハッシュの数 3」であるから、暗号資産ブロックチェーン処理装置10は、ブロックデータに記録されたトランザクション数(tra_cnt)と、実際のカウント結果とが不一致であること、つまり、トランザクションデータの重複があることを検出することができる。

[0097] カウントしたトランザクションの数が、ブロックデータに記録されたトランザクション数(tra_cnt)と一致する場合(ステップS144のはい)、取引データの整合性検証の処理が正常に終了される。

[0098] 図24に示した不整合検証の処理の他に、暗号資産ブロックチェーンにおける銀行口座番号に該当する記録単位であるアドレスの残高に基づいて、不整合を検出することができる。例えば、暗号資産ブロックチェーン処理装置10は、信頼性の高い第三者が管理、運営するブロックエクスプローラを用いて、指定するアドレス(例えば、自動収集モードで無作為に抽出されたアドレス(図5中のステップS124))の残高を計算する。

[0099] 次に、第三者のブロックエクスプローラから得られた残高と、暗号資産ブ

ロックチェーン処理装置 10 により計算された同じアドレスの残高とを比較し、残高が一致しない場合には、ユーザに不整合である旨の通知を行うとともに、特定のフォルダにどのアドレスが不整合であったかを示すメッセージ等を記憶することができる。フォルダに記憶されるメッセージは、例えば、下記のようなものである。

```
address, data_bricks balance, external_explorer balance, difference  
1DFuBFLwJjXQapEBE36h3MmuHXMvjBUneA, 701, 600, 101  
1DPkMBvGTjUFJ621z1RkXjDBg1oJykniYL, 117125, 117124, 1
```

当該メッセージは、指定されたアドレス (address) について、暗号資産ブロックチェーン処理装置 10 により計算された残高 (data_bricks balance) と、第三者のブロックエクスプローラを利用して計算された残高 (external_explorer) とが一致しない (difference) 旨を示す。

- [0100] この第三者のブロックエクスプローラを介した残高確認の仕組みにより、暗号資産ブロックチェーン処理装置 10 により提供される計算結果の信頼性および客観性をさらに高めることができる。図 27 は、本発明の一実施形態に係る暗号資産ブロックチェーン処理装置により実現される残高確認の仕組みを説明する模式図である。
- [0101] 暗号資産ブロックチェーン処理装置 10 はブロックチェーンのノードとして機能することでブロックチェーンデータそのものを取得し、上述のとおりブロックチェーンデータを処理することで、アドレスごとの残高 (Balance) を算出する。また、一方で暗号資産ブロックチェーン処理装置 10 は信頼できる第三者が管理、運営するブロックエクスプローラのホスト 40 と通信する。暗号資産ブロックチェーン処理装置 10 は、無作為に選択したアドレスの残高をブロックエクスプローラ (ホスト 40) に要求する。ブロックエクスプローラは、要求された残高を暗号資産ブロックチェーン処理装置 10 に送信する。暗号資産ブロックチェーン処理装置 10 は、第三者のブロックエクスプローラから得られた残高と、暗号資産ブロックチェーン処理装置 10 により計算された同じアドレスの残高とを比較し、両者の整合性をチェッ

クする。このチェックは、周期的に行われてもよいし、ユーザの要求に応じて行われてもよい。

[0102] 暗号資産ブロックチェーン処理装置10と取引データ記憶装置172は、例えば、ある監査法人のクローズドな環境で作動するクラウド（例えば、社内のクラウド）で運用することができる。そのようなクラウドで運用することによって、取引データの検証とアドレス残高が公のインターネットとは隔離された環境で処理され、クライアントの秘匿情報の保護が確実に確保することができる（一方で、ブロックエクスプローラのAPI等を使うと、アドレスや取引情報をインターネット上でクエリをかけなければならない、そのクエリ情報が保護されない）。

[0103] また、クラウド技術を使うことによって、例えば、監査法人グループのクローズドネットワークを介して、同じグループの国内または国外のファーム（その他の監査法人等）から、暗号資産ブロックチェーン処理装置10にアクセスすることができる。暗号資産の取引は国境に左右されないため、取引の不正検知などは、同じグループに属する各国のファーム（監査法人等）で同じデータにアクセスできることが不可欠である。

[0104] 一般的に、各種暗号資産の実装方式は、異なる上に、頻繁に実装バージョンが更新されている。例えば、暗号資産の実装が更新された場合には、その暗号資産の実装方式に対応する暗号資産ブロックチェーン処理装置（ノード）について、当該暗号通貨の実装方式の更新内容に合わせてデータ収集等の処理内容を変更する必要がある、ブロックチェーンデータの整合性を確保するためには、常にノードを最新のバージョンに対応できるものにしなければならない。

[0105] しかしながら、暗号資産のノードソフトウェアのバージョンの更新について、必ずしもユーザに通知されるとは限らない。これは、P2Pでブロックチェーンデータを分散して各ノードで管理される分散式ブロックチェーンの特徴であるが、ビットコイン等の暗号資産を管理やメンテナンスをする管理会社が全く存在しないからである。その代わりに、実際には、暗号資産のノ

ードソフトウェアのバージョンは、当該暗号資産を使用するプログラマー同士が共同で管理やメンテナンスを行っている（例えば、ビットコインコアのグループなど）。

[0106] 一般に、いつ、どのような理由で、暗号資産のノードソフトウェアのバージョンを更新するかは、チャットやニュースから知る場合が多い。個別に、チャットやニュースから所望の暗号資産のノードソフトウェアのバージョンの更新情報を取得することは、情報が不完全であったり、更新自体を見逃してしまったりするというリスクがあるため、本発明に係る暗号資産ブロックチェーン処理システムでは、暗号資産フォークチェッカーを提供する。

[0107] 本発明の暗号資産フォークチェッカーは、暗号資産ブロックチェーン処理装置10にインストールされているノードソフトウェアのバージョンと、ノードソフトウェアのバージョンを管理するサイト（Git Hub, Docker Hub等）で管理されている、同ノードソフトウェアの最新バージョンを比較してレポートを自動的に作成し、差異があればアラートを出す仕組みである。なお、フォークとはブロックチェーン上でのバージョンアップデートのことを指す。

[0108] 本発明に係る暗号資産ブロックチェーン処理システムにおける暗号資産フォークチェッカーは、図28に示すようなレポートを自動的に生成することができる。図28は、暗号資産ブロックチェーン処理装置10にインストールされているノードソフトウェアのバージョンと、第三者の管理サイト（Git Hub, Docker Hub等）で管理されている、同ノードソフトウェアの最新バージョンを比較して自動的に生成したレポートの一例を示す。暗号資産フォークチェッカーは、各暗号資産について、暗号資産ブロックチェーン処理システムにおける暗号資産のノードソフトウェアのバージョンと、第三者の管理サイト（例えば、GitHub, Docker Hub等）に記録された同ノードソフトウェアの最新バージョンを比較して、比較結果を記載したレポートを自動的に生成することができる。なお、GitHub, Docker Hub等に記録された暗号資産のノードソフトウェアのバージョンは常に最新である。

[0109] 比較の結果、暗号資産ブロックチェーン処理システムにおける暗号資産のノードソフトウェアのバージョンと、管理サイト（GitHub, Docker Hub等）に記録された暗号資産のノードソフトウェアのバージョンとの間に差異がある場合には、例えば、暗号資産ブロックチェーン処理装置１０が、情報処理端末２０にアラート（不整合であること）を通知してユーザに知らせることができる。

[0110] 図２８に示すレポートの項目は次のとおりである。

[表１]

Currency name	暗号資産（仮想通貨）の名称
Current version (in CAPP2)	本発明に係る暗号資産ブロックチェーン処理システムで現在対応している暗号資産のノードソフトウェアのバージョン
Current version date (in CAPP2)	本発明に係る暗号資産ブロックチェーン処理システムで現在対応している暗号資産のノードソフトウェアのバージョンが公に使用され始めた日付
Latest version (in Github)	ノードソフトウェアのバージョンを管理するサイトの１つである Github に記録されたバージョン
Latest version date (in Github)	ノードソフトウェアのバージョンを管理するサイトの１つである Githubにあるバージョンが公に使用され始めた日付
Need to Update?	アップデートの必要があるかどうか
Reference	参照データ
Remarks	コメント

[0111] 図２８に示すレポートの例では、ビットコイン（Bitcoin）、ビットコインキャッシュ（Bitcoin Cash）及びイーサリアム／イーサリアムクラシック（Ethereum/Ethereum Classic）のノードソフトウェアは、“Need to Update?”の欄が“True”なので、アップデートが必要であることを、情報処理端末２０等を介してユーザに知らせることができる。

[0112] 以上のように、本発明に係る暗号資産ブロックチェーン処理装置等は、インターネット等のオープンネットワーク上の暗号資産のブロックチェーンデータ（ブロック、トランザクション等を含む）を収集して、第三者に特定の取引に対するクエリや取引情報を傍受されることがないプライベートなネットワーク環境下にあるサーバ等の計算機（ノード）及びデータ記憶装置に、暗号資産の種別毎に蓄積し、分析に適したデータ形式に変換することで、安

全にブロックチェーンデータを分析して、監査のためにアドレス毎の残高等の算出を可能にするだけでなく、複数の異なる暗号資産の実装方式に応じたブロックチェーンデータを収集・分析を実現することができる。

[0113] また、本発明に係る暗号資産ブロックチェーン処理装置等は、暗号資産の実装方式によっては、取引が実施された際の取引数量と取引に用いた単価に関する情報がそれぞれ別のデータレコードに記録されているような場合に、単価データと取引数量データとから算出される取引金額（＝取引が実施された時間の単価×取引数量）が記録された仮想的なトランザクションデータ（取引データ）を生成することで、暗号資産の実装方式に影響されることなく、ある時点までの取引データを網羅的に集計することで、過去に訴求した特定時点における、取引の参加者の暗号資産の持分残高を容易に算出することができる。

[0114] さらに、本発明に係る暗号資産ブロックチェーン処理装置等は、収集したブロックチェーンデータの重複や欠落、暗号資産のノードソフトウェアのバージョンの違い等を検証することで、分析の対象となる取引データの整合性を担保することができる。

産業上の利用可能性

[0115] 本発明に係る暗号資産ブロックチェーン処理装置等は、例えば、監査法人において、監査対象のアドレス毎に、暗号資産の持分残高を算出して、監査を支援すること等に利用可能である。

符号の説明

[0116] 1 0 : 暗号資産ブロックチェーン処理装置（ノード）
1 0 a : ノード
1 0 b : ノード
1 1 : CPU
1 2 : メモリ
1 3 : バス
1 4 : 入出力インターフェース

1 5	: 入力部
1 6	: 出力部
1 7	: 記憶部
1 8	: 通信部
2 0	: 情報処理端末
2 1	: C P U
2 2	: メモリ
2 3	: バス
2 4	: 入出力インターフェース
2 5	: 入力部
2 6	: 出力部
2 7	: 記憶部
2 8	: 通信部
3 0	: クラウドストレージ
4 0	: ホスト
1 1 1	: データ収集部
1 1 2	: データ変換部
1 1 3	: データ分析部
1 1 4	: 整合性検証部
1 7 1	: ブロックチェーンデータ記憶装置
1 7 2	: 取引データ記憶装置
N	: ネットワーク

請求の範囲

- [請求項1] 暗号資産ブロックチェーン処理装置であって、少なくとも
データ収集部と、
データ変換部と、
を含み、
前記データ収集部は、ユーザにより指定された暗号資産ブロックチェーンにアクセスして、所定の要求範囲に基づいて、前記暗号資産ブロックチェーンからブロックチェーンデータを収集し、
前記データ変換部は、前記ブロックチェーンデータを分析可能な取引データに変換し、
前記ブロックチェーンデータ及び前記分析可能な取引データは、前記暗号資産ブロックチェーン処理装置に接続されたデータ記憶装置に保存される、
暗号資産ブロックチェーン処理装置。
- [請求項2] 前記データ記憶装置は、前記暗号資産ブロックチェーン処理装置がネットワークを介してアクセス可能なクラウドストレージである、
請求項1に記載の暗号資産ブロックチェーン処理装置。
- [請求項3] 前記データ収集部は、スタティックモードで動作し、
前記スタティックモードで動作する前記データ収集部は、データバッチ毎の取引データ数を指定して前記要求範囲の終点を設定し、
前回収集したデータの最後の取引データの識別情報を、前記要求範囲の始点に設定する、
請求項1又は2に記載の暗号資産ブロックチェーン処理装置。
- [請求項4] 前記データ収集部は、ダイナミックモードで動作し、
前記ダイナミックモードで動作する前記データ収集部は、データバッチ毎のデータサイズを指定して前記要求範囲の終点を設定し、
前回収集したデータの最後の取引データの識別情報を、前記要求範囲の始点に設定する、

請求項 1 又は 2 に記載の暗号資産ブロックチェーン処理装置。

[請求項5]

前記データ収集部は、自動収集モードで動作し、

前記自動収集モードで動作する前記データ収集部は、前記暗号資産ブロックチェーン上の最新データの識別情報を取得して、前記要求範囲の終点に設定し、

前記データ収集部により前回収集したデータの最後の取引データの識別情報を、前記要求範囲の始点に設定する、

請求項 1 又は 2 に記載の暗号資産ブロックチェーン処理装置。

[請求項6]

前記データ収集部は、前回の収集モードが、データバッチ毎の取引データ数を指定したスタティックモード、又はデータバッチ毎のデータサイズを指定したダイナミックモードである場合に、前回収集したデータの最後の取引データの識別情報を、前記前回の収集モードの取引データ数又はデータサイズに基づいて再計算して、前記要求範囲の始点に設定する、

請求項 5 に記載の暗号資産ブロックチェーン処理装置。

[請求項7]

前記ブロックチェーンデータは、識別可能なブロック番号が付与された、トランザクションデータを含み、

前記トランザクションデータは、1 以上の単価設定用の単価トランザクションデータと、1 以上の数量指定用の数量トランザクションデータとを少なくとも含み、

前記データ変換部は、前記 1 以上の数量トランザクションデータの各々について、該数量トランザクションデータに対して付与されたブロック番号に最も近いブロック番号が付与された単価トランザクションデータを検索し、検索した前記単価トランザクションデータの単価の値に、該数量トランザクションデータの数量を掛け合わせることで、取引に係る金額を算出する、

請求項 1 から 6 のいずれか 1 項に記載の暗号資産ブロックチェーン処理装置。

- [請求項8] 前記データ記憶装置は、ブロックチェーンデータ記憶装置と取引データ記憶装置とを含み、
前記データ収集部によって収集された前記ブロックチェーンデータは、前記ブロックチェーンデータ記憶装置に保存され、
前記データ変換部によって算出された前記金額を含む取引データは前記取引データ記憶装置に保存される、
請求項7に記載の暗号資産ブロックチェーン処理装置。
- [請求項9] 前記暗号資産ブロックチェーン処理装置は、データ分析部を更に含み、
前記データ分析部は、最初のブロック番号から特定時点のブロック番号までに合致する前記取引データを前記取引データ記憶装置から取得し、
取得した前記取引データの金額を、前記暗号資産ブロックチェーンにおける銀行口座番号に該当する記録単位であるアドレス毎に合算して残高を算出する、
請求項8に記載の暗号資産ブロックチェーン処理装置。
- [請求項10] 前記ブロックチェーンデータは、少なくともブロックデータとトランザクションデータとを含み、
前記データ変換部は、前記ブロックデータ及び前記トランザクションデータの各々に取引日時に関連する年月日の属性を付加して、年月日で区別可能な取引データに変換し、
前記取引データは年月日毎に分類されて前記データ記憶装置に保存される、
請求項1から6のいずれか1項に記載の暗号資産ブロックチェーン処理装置。
- [請求項11] 前記データ記憶装置は、ブロックチェーンデータ記憶装置と取引データ記憶装置とを含み、
前記データ収集部によって収集された前記ブロックチェーンデータ

は、前記ブロックチェーンデータ記憶装置に保存され、

前記データ変換部によって前記年月日の属性が付加され、年月日で
区別可能な前記取引データは、前記取引データ記憶装置に保存される
、

請求項 10 に記載の暗号資産ブロックチェーン処理装置。

[請求項12] 前記暗号資産ブロックチェーン処理装置は、データ分析部を更に含
み、

前記データ変換部は、前記トランザクションデータを、トランザク
ション入力データとトランザクション出力データとに分け、

前記データ分析部は、前記暗号資産ブロックチェーンにおける銀行
口座番号に該当する記録単位であるアドレス毎に、前記トランザクシ
ョン入力データ及び前記トランザクション出力データに基づいて、特
定のブロック番号の範囲で全収入及び全支出を計算する、

請求項 7 から 11 のいずれか 1 項に記載の暗号資産ブロックチェーン
処理装置。

[請求項13] 前記暗号資産ブロックチェーン処理装置は、データ分析部を更に含
み、

前記データ分析部は、前記暗号資産ブロックチェーンにおける銀行
口座番号に該当する記録単位であるアドレス毎に、前記トランザクシ
ョンデータ及びスマートコントラクトの結果に基づいて、前記アドレ
ス毎の残高を算出する、

請求項 7 から 11 のいずれか 1 項に記載の暗号資産ブロックチェーン
処理装置。

[請求項14] 前記暗号資産ブロックチェーン処理装置は、整合性検証部を更に含
み、

前記取引データは、生成順にシーケンス番号が付与されたブロック
データを含み、

前記整合性検証部は、前記ブロックデータの前記シーケンス番号を

順に照合することで、前記シーケンス番号の重複及び欠落のチェックを行い、

前記シーケンス番号に重複又は欠落があった場合には、前記シーケンス番号に対応する前記ブロックデータの不整合を通知する、
請求項 1 から 6 のいずれか 1 項に記載の暗号資産ブロックチェーン処理装置。

[請求項15] 前記整合性検証部は、所属するブロックのシーケンス番号を有するトランザクションデータについて、シーケンス番号ごとに前記トランザクションデータの数をカウントし、カウントした前記トランザクションデータの数と該シーケンス番号が付与されたブロックデータに記録されたトランザクション数とを比較し、

差分があった場合に、前記ブロックデータの不整合を通知する、
請求項 1 4 に記載の暗号資産ブロックチェーン処理装置。

[請求項16] 前記暗号資産ブロックチェーン処理装置は、整合性検証部を更に含み、

前記整合性検証部は、第三者が管理するブロックエクスプローラを用いて、ユーザにより指定されたアドレスの検証用残高を算出し、

前記データ分析部によって前記アドレス毎に算出された残高から、前記指定されたアドレスの残高を取得し、前記データ分析部により算出された前記残高と、前記検証用残高とを比較し、

差分があった場合に、前記指定されたアドレスのデータに不整合があることを通知する、

請求項 9 又は 1 3 に記載の暗号資産ブロックチェーン処理装置。

[請求項17] 前記整合性検証部は、暗号資産のノードソフトウェアのバージョンを管理するサイトにアクセスし、所望の暗号資産のノードソフトウェアの最新バージョンを確認し、前記データ記憶装置に保存された前記暗号資産のノードソフトウェアのバージョンと比較し、バージョンに差異がある場合に、前記暗号資産のノードソフトウェアのバージョン

に不整合があることを通知する、

請求項 14 から 16 のいずれか 1 項に記載の暗号資産ブロックチェーン処理装置。

- [請求項18] 暗号資産ブロックチェーン処理方法であって、
 ユーザにより指定された暗号資産ブロックチェーンにアクセスする段階と、
 所定の要求範囲に基づいて、前記暗号資産ブロックチェーンからブロックチェーンデータを収集する段階と、
 前記ブロックチェーンデータを分析可能な取引データに変換する段階と、
 を含み、
 前記ブロックチェーンデータ及び前記分析可能な取引データは、前記暗号資産ブロックチェーン処理装置に接続されたデータ記憶装置に保存される、暗号資産ブロックチェーン処理方法。

- [請求項19] 前記データ記憶装置は、前記暗号資産ブロックチェーン処理装置がネットワークを介してアクセス可能なクラウドストレージである、
請求項 18 に記載の暗号資産ブロックチェーン処理方法。

- [請求項20] ユーザにより指定されたスタティックモードに応じて、データバッチ毎の取引データ数を指定して前記要求範囲の終点を設定し、前回収集したデータの最後の取引データの識別情報を、前記要求範囲の始点に設定する段階を含む、請求項 18 又は 19 に記載の暗号資産ブロックチェーン処理方法。

- [請求項21] ユーザにより指定されたスタティックモードに応じて、データバッチ毎のデータサイズを指定して前記要求範囲の終点を設定し、前回収集したデータの最後の取引データの識別情報を、前記要求範囲の始点に設定する段階を含む、請求項 18 又は 19 に記載の暗号資産ブロックチェーン処理方法。

- [請求項22] ユーザにより指定された自動収集モードに応じて、前記暗号資産ブ

ロックチェーン上の最新データの識別情報を取得して、前記要求範囲の終点に設定する段階と、

前記データ収集部により前回收集したデータの最後の取引データの識別情報を、前記要求範囲の始点に設定する段階と、

を含む、請求項 18 又は 19 に記載の暗号資産ブロックチェーン処理方法。

[請求項23] 前回の収集モードが、データバッチ毎の取引データ数を指定したステティックモード、又はデータバッチ毎のデータサイズを指定したダイナミックモードである場合に、前回收集したデータの最後の取引データの識別情報を、前記前回の収集モードの取引データ数又はデータサイズに基づいて再計算して、前記要求範囲の始点に設定する段階を含む、請求項 22 に記載の暗号資産ブロックチェーン処理方法。

[請求項24] 前記ブロックチェーンデータは、識別可能なブロック番号が付与された、トランザクションデータを含み、

前記トランザクションデータは、1 以上の単価設定用の単価トランザクションデータと、1 以上の数量指定用の数量トランザクションデータとを少なくとも含み、

前記暗号資産ブロックチェーン処理方法は、

前記 1 以上の数量トランザクションデータの各々について、該数量トランザクションデータに対して付与されたブロック番号に最も近いブロック番号が付与された単価設定のトランザクションデータを検索する段階と、

検索した前記単価トランザクションデータの単価の値に、該数量トランザクションデータの数量を掛け合わせることで、取引に係る金額を算出する段階と、

を含む、請求項 18 から 23 のいずれか 1 項に記載の暗号資産ブロックチェーン処理方法。

[請求項25] 前記データ記憶装置は、ブロックチェーンデータ記憶装置と取引デ

ータ記憶装置とを含み、

前記ブロックチェーンデータを収集する段階は、収集した前記ブロックチェーンデータを前記ブロックチェーンデータ記憶装置に保存することを含み、

前記暗号資産ブロックチェーン処理方法は、

算出した前記金額を含む取引データを前記取引データ記憶装置に保存する段階を含む、請求項24に記載の暗号資産ブロックチェーン処理方法。

[請求項26] 最初のブロック番号から特定時点のブロック番号までに合致する前記取引データを前記取引データ記憶装置から取得する段階と、

取得した前記取引データの金額を、前記暗号資産ブロックチェーンにおける銀行口座番号に該当する記録単位であるアドレス毎に合算して残高を算出する段階と、

を含む請求項25に記載の暗号資産ブロックチェーン処理方法。

[請求項27] 前記ブロックチェーンデータは、少なくともブロックデータとトランザクションデータとを含み、

前記暗号資産ブロックチェーン処理方法は、

前記ブロックデータ及び前記トランザクションデータの各々に取引日時に関連する年月日の属性を付加して、年月日で区別可能な取引データに変換する段階と、

前記取引データを年月日毎に分類して前記データ記憶装置に保存する段階と、

を含む請求項18から23いずれか1項に記載の暗号資産ブロックチェーン処理方法。

[請求項28] 前記データ記憶装置は、ブロックチェーンデータ記憶装置と取引データ記憶装置とを含み、

前記ブロックチェーンデータを収集する段階は、収集した前記ブロックチェーンデータを、前記ブロックチェーンデータ記憶装置に保存

することを含み、

前記暗号資産ブロックチェーン処理方法は、

前記データ変換部によって前記年月日の属性が付加され、年月日で区別可能な前記取引データを、前記取引データ記憶装置に保存する段階を含む、請求項27に記載の暗号資産ブロックチェーン処理方法。

[請求項29] 前記トランザクションデータを、トランザクション入力データとトランザクション出力データとに分ける段階と、

前記暗号資産ブロックチェーンにおける銀行口座番号に該当する記録単位であるアドレス毎に、前記トランザクション入力データ及び前記トランザクション出力データに基づいて、特定のブロック番号の範囲で全収入及び全支出を計算する段階と、
を含む請求項24から28のいずれか1項に記載の暗号資産ブロックチェーン処理方法。

[請求項30] 前記暗号資産ブロックチェーンにおける銀行口座番号に該当する記録単位であるアドレス毎に、前記トランザクションデータ及びスマートコントラクトの結果に基づいて、前記アドレス毎の残高を算出する段階を含む請求項24から28のいずれか1項に記載の暗号資産ブロックチェーン処理方法。

[請求項31] 前記取引データは、生成順にシーケンス番号が付与されたブロックデータを含み、

前記暗号資産ブロックチェーン処理方法は、

前記ブロックデータの前記シーケンス番号を順に照合することで、前記シーケンス番号の重複及び欠落のチェックを行う段階と、

前記シーケンス番号に重複又は欠落があった場合には、前記シーケンス番号に対応する前記ブロックデータの不整合を通知する段階と、
を含む請求項18から23のいずれか1項に記載の暗号資産ブロックチェーン処理方法。

[請求項32] 所属するブロックのシーケンス番号を有するトランザクションデー

タについて、シーケンス番号ごとに前記トランザクションデータの数をカウントし、カウントした前記トランザクションデータの数と該シーケンス番号が付与されたブロックデータに記録されたトランザクション数とを比較する段階と、

差分があった場合に、前記ブロックデータの不整合を通知する段階と、

を含む請求項 31 に記載の暗号資産ブロックチェーン処理方法。

[請求項33] 第三者が管理するブロックエクスプローラを用いて、ユーザにより指定されたアドレスの検証用残高を算出する段階と、

前記データ分析部によって前記アドレス毎に算出された残高から、前記指定されたアドレスの残高を取得し、前記データ分析部により算出された前記残高と、前記検証用残高とを比較する段階と、

差分があった場合に、前記指定されたアドレスのデータに不整合があることを通知する段階と、

を含む請求項 26 又は 30 に記載の暗号資産ブロックチェーン処理方法。

[請求項34] 暗号資産のノードソフトウェアのバージョンを管理するサイトにアクセスする段階と、

所望の暗号資産のノードソフトウェアの最新バージョンを確認する段階と、

前記データ記憶装置に保存された前記暗号資産のノードソフトウェアのバージョンと比較する段階と、

バージョンに差異がある場合に、前記暗号資産のノードソフトウェアのバージョンに不整合があることを通知する段階と、

を含む請求項 31 から 33 のいずれか 1 項に記載の暗号資産ブロックチェーン処理方法。

[請求項35] 請求項 1 から 17 のいずれか 1 項に記載の暗号資産ブロックチェーン処理装置と、

情報処理端末と、
クラウドストレージと、
を含み、

前記暗号資産ブロックチェーン処理装置、前記情報処理装置及び前記クラウドストレージは、それぞれネットワークを介して接続された暗号資産ブロックチェーン処理システム。

[請求項36] コンピュータによって実行されることで、前記コンピュータを請求項1から17のいずれか1項に記載の暗号資産ブロックチェーン処理装置の各部として機能させるための暗号資産ブロックチェーン処理プログラム。

[請求項37] コンピュータによって実行されることで、前記コンピュータに請求項18から34のいずれか1項に記載の暗号資産ブロックチェーン処理方法の各段階を実行させるための暗号資産ブロックチェーン処理プログラム。