

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7448191号
(P7448191)

(45)発行日 令和6年3月12日(2024.3.12)

(24)登録日 令和6年3月4日(2024.3.4)

(51)国際特許分類

F I

H O 4 L 9/32 (2006.01)

H O 4 L 9/32 2 0 0 Z

G O 6 F 21/62 (2013.01)

G O 6 F 21/62 3 1 8

請求項の数 22 (全39頁)

(21)出願番号	特願2020-22974(P2020-22974)	(73)特許権者	319002393
(22)出願日	令和2年2月14日(2020.2.14)		シスナ株式会社
(65)公開番号	特開2021-129221(P2021-129221 A)		愛知県名古屋市長穂区萩山町3-4 1
(43)公開日	令和3年9月2日(2021.9.2)	(74)代理人	100094569
審査請求日	令和5年1月6日(2023.1.6)		弁理士 田中 伸一郎
		(74)代理人	100103610
			弁理士 ▲吉▼田 和彦
		(74)代理人	100109070
			弁理士 須田 洋之
		(74)代理人	100067013
			弁理士 大塚 文昭
		(74)代理人	100086771
			弁理士 西島 孝喜
		(74)代理人	
			上杉 浩

最終頁に続く

(54)【発明の名称】 データ管理システム

(57)【特許請求の範囲】

【請求項1】

端末と、
前記端末と第1のネットワークを介して接続されたコロニーサーバと、
前記コロニーサーバと第2のネットワークを介して接続されたセンターサーバと
を少なくとも備え、
前記端末は、管理対象データに関する要求を前記コロニーサーバに送信し、
前記コロニーサーバは、前記管理対象データに関する要求に応じて取得又は生成した管理対象データを、先頭から所定のサイズまでのデータを含む部分データと、前記所定のサイズ+1以降のデータを含む本体データとに分割して、前記部分データを前記センターサーバに送信する分割送信部と、
前記センターサーバからハッシュ値を受け取り、前記本体データに関連付けて前記ハッシュ値を記憶する本体データ管理部と、
前記ハッシュ値を更新するハッシュ更新部と
を含み、
前記センターサーバは、前記部分データを少なくとも含む暗号化したデータである暗号化キーを生成し、前記暗号化キーと共に該暗号化キーを識別するための前記ハッシュ値を記憶する部分データ管理部と、
前記暗号化キーと共に記憶された前記ハッシュ値を前記コロニーサーバに送信するハッシュ通知部と、

前記ハッシュ値を用いて前記暗号化キーを識別して取得する暗号化キー取得部とを含み、

前記ハッシュ通知部は、前記暗号化キーと共に記憶された前記ハッシュ値を、所定の間隔で、前記本体データに関連付けて記憶された前記ハッシュ値とは一致しない新たなハッシュ値に更新して、前記新たなハッシュ値を前記コロニーサーバに送信し、

前記ハッシュ更新部は、前記新たなハッシュ値を受け取り、前記本体データに関連付けて記憶された前記ハッシュ値を前記新たなハッシュ値に更新し、

前記暗号化キー取得部は、前記暗号化キーと共に記憶された前記ハッシュ値が更新された場合には、前記コロニーサーバからの前記新たなハッシュ値を含む、管理対象データに関する要求に応じて、前記新たなハッシュ値を用いて前記暗号化キーを識別して取得し、

前記部分データは、前記暗号化キーから復元され、

前記管理対象データは、前記部分データと前記本体データとを結合することで復元される、

データ管理システム。

【請求項 2】

前記部分データ管理部は、前記部分データの他に、前記管理対象データのファイル名及び時間の少なくとも一方を含めて、暗号化を行い、

前記暗号化キーは、前記部分データの他に、前記ファイル名及び前記時間の少なくとも一方を含む、

請求項 1 に記載のデータ管理システム。

【請求項 3】

前記管理対象データに関する要求は、前記端末においてアップロードされた、前記管理対象に対応する管理対象データを含む、

請求項 1 又は 2 に記載のデータ管理システム。

【請求項 4】

前記管理対象データに関する要求は、前記コロニーサーバにおいて前記管理対象に対応する管理対象データを生成させる要求である、

請求項 1 又は 2 に記載のデータ管理システム。

【請求項 5】

前記所定のサイズは、前記管理対象データの先頭から 30 バイト以下である、

請求項 1 から 4 のいずれか 1 項に記載のデータ管理システム。

【請求項 6】

前記所定の間隔は、24 時間以下の間隔である、

請求項 1 から 5 のいずれか 1 項に記載のデータ管理システム。

【請求項 7】

前記第 1 のネットワークはインターネットであり、前記第 2 のネットワークはクローズドネットワークである、

請求項 1 から 6 のいずれか 1 項に記載のデータ管理システム。

【請求項 8】

前記コロニーサーバの分割送信部は、前記管理対象データを先頭から所定のサイズまでのデータに代えて、前記管理対象データの任意の一部分から所定のサイズのデータを前記部分データとし、

前記所定のサイズ + 1 以降のデータに代えて、前記管理対象データの任意の一部分以外の残余部分のデータを前記本体データとするように分割する、

請求項 1 から 7 のいずれか 1 項に記載のデータ管理システム。

【請求項 9】

端末と、

前記端末と第 1 のネットワークを介して接続されたコロニーサーバと、

前記コロニーサーバと第 2 のネットワークを介して接続されたセンターサーバと

を少なくとも備えたデータ管理システムによって実行されるデータ管理方法において、

10

20

30

40

50

前記端末が管理対象データに関する要求を前記コロニーサーバに送信するステップと、
前記コロニーサーバが前記管理対象データに関する要求に応じて取得又は生成した管理対象データを先頭から所定のサイズまでのデータを含む部分データと、前記所定のサイズ＋１以降のデータを含む本体データとに分割して、前記部分データを前記センターサーバに送信するステップと、

前記センターサーバが、前記部分データを少なくとも含む暗号化したデータである暗号化キーを生成するステップと、

前記センターサーバが、前記暗号化キーと共に該暗号化キーを識別するためのハッシュ値を記憶するステップと、

前記センターサーバが、前記ハッシュ値を前記コロニーサーバに送信するステップと、
前記コロニーサーバが、前記本体データに関連付けて前記ハッシュ値を記憶するステップと

を含み、

前記センターサーバは、前記暗号化キーと共に記憶された前記ハッシュ値を、所定の間隔で、前記本体データに関連付けて記憶された前記ハッシュ値とは一致しない新たなハッシュ値に更新して、前記新たなハッシュ値を前記コロニーサーバに送信し、

前記コロニーサーバは、前記本体データに関連付けて記憶された前記ハッシュ値を、前記新たなハッシュ値に更新し、

前記センターサーバは、前記暗号化キーと共に記憶された前記ハッシュ値が更新された場合には、前記コロニーサーバからの前記新たなハッシュ値を含む、管理対象データに関する要求に応じて、前記新たなハッシュ値を用いて前記暗号化キーを識別して取得し、

前記部分データは、前記暗号化キーから復元され、

前記管理対象データは、前記部分データと前記本体データとを結合することで復元される、

データ管理方法。

【請求項１０】

前記センターサーバは、前記暗号化キーを生成するステップにおいて、前記部分データの他に、前記管理対象データのファイル名及び時間の少なくとも一方を含めて、暗号化を行い、

前記暗号化キーは、前記部分データの他に、前記ファイル名及び前記時間の少なくとも一方を含む、

請求項９に記載のデータ管理方法。

【請求項１１】

前記管理対象データに関する要求は、前記端末においてアップロードされた、前記管理対象に対応する管理対象データを含む、

請求項９又は１０に記載のデータ管理方法。

【請求項１２】

前記管理対象データに関する要求は、前記コロニーサーバにおいて前記管理対象に対応する管理対象データを生成させる要求である、

請求項９又は１０に記載のデータ管理方法。

【請求項１３】

前記所定のサイズは、前記管理対象データの先頭から３０バイト以下である、

請求項９から１２のいずれか１項に記載のデータ管理方法。

【請求項１４】

前記所定の間隔は、２４時間以下の間隔である、

請求項９から１３のいずれか１項に記載のデータ管理方法。

【請求項１５】

前記第１のネットワークはインターネットであり、前記第２のネットワークはクロースドネットワークである、

請求項９から１４のいずれか１項に記載のデータ管理方法。

10

20

30

40

50

【請求項 16】

前記コロニーサーバが前記管理対象データに関する要求に応じて取得又は生成した管理対象データを先頭から所定のサイズまでのデータを含む部分データと、前記所定のサイズ+1以降のデータを含む本体データとに分割して、前記部分データを前記センターサーバに送信するステップは、

前記管理対象データを先頭から所定のサイズまでのデータに代えて、前記管理対象データの任意の一部分から所定のサイズのデータを前記部分データとし、

前記所定のサイズ+1以降のデータに代えて、前記管理対象データの任意の一部分以外の残余部分のデータを前記本体データとするように分割する、

請求項 9 から 15 のいずれか 1 項に記載のデータ管理方法。

10

【請求項 17】

コロニーサーバ装置であって、

端末から管理対象データに関する要求を受け取る手段と、

前記管理対象データに関する要求に応じて取得又は生成した管理対象データを先頭から所定のサイズまでのデータを含む部分データと、前記所定のサイズ+1以降のデータを含む本体データとに分割して、前記部分データをセンターサーバ装置に送信する分割送信手段と、

前記センターサーバ装置から、前記部分データを少なくとも含む暗号化したデータである暗号化キーを識別するためのハッシュ値を受け取り、前記本体データに関連付けて前記ハッシュ値を記憶する本体データ管理手段と

20

を含み、

前記コロニーサーバ装置は、前記センターサーバ装置から、前記本体データに関連付けて記憶された前記ハッシュ値とは一致しない新たなハッシュ値を、所定の間隔で受信し、

前記コロニーサーバ装置は、前記本体データに関連付けて記憶された前記ハッシュ値を、前記所定の間隔で、前記新たなハッシュ値に更新し、

前記コロニーサーバ装置は、前記暗号化キーと共に記憶された前記ハッシュ値が更新された場合には、前記センターサーバ装置に前記新たなハッシュ値を用いて前記暗号化キーを識別させるために、前記新たなハッシュ値を含む、管理対象データに関する取引要求を前記センターサーバ装置に送信し、

前記部分データは、前記暗号化キーから復元され、

30

前記管理対象データは、前記部分データと前記本体データとを結合することで復元される、

コロニーサーバ装置。

【請求項 18】

前記分割送信手段は、前記管理対象データを先頭から所定のサイズまでのデータに代えて、前記管理対象データの任意の一部分から所定のサイズのデータを前記部分データとし、

前記所定のサイズ+1以降のデータに代えて、前記管理対象データの任意の一部分以外の残余部分のデータを前記本体データとするように分割する、

請求項 17 に記載のコロニーサーバ装置。

【請求項 19】

40

センターサーバ装置であって、

コロニーサーバ装置から、管理対象データの先頭から所定のサイズまでのデータを含む部分データを受け取る手段と、

前記部分データを少なくとも含む暗号化したデータである暗号化キーを生成し、前記暗号化キーと共に該暗号化キーを識別するためのハッシュ値を記憶する部分データ管理手段と、

前記暗号化キーと共に記憶された前記ハッシュ値を前記コロニーサーバ装置に送信するハッシュ通知手段と

を含み、

前記ハッシュ通知手段は、前記暗号化キーと共に記憶された前記ハッシュ値を、所定の

50

間隔で、前記ハッシュ値とは一致しない新たなハッシュ値に更新して、前記新たなハッシュ値を前記コロニーサーバ装置に送信し、

前記センターサーバ装置は、前記暗号化キーと共に記憶された前記ハッシュ値が更新された場合には、前記コロニーサーバ装置からの前記新たなハッシュ値を含む、管理対象データに関する要求に応じて、前記新たなハッシュ値を用いて前記暗号化キーを識別し、

前記部分データは、前記暗号化キーから復元され、

前記管理対象データは、前記部分データと、前記管理対象データの先頭から前記所定のサイズ+1以降のデータを含む本体データとを結合することで復元される、センターサーバ装置。

【請求項 20】

前記部分データは、前記管理対象データを先頭から所定のサイズまでのデータに代えて、前記管理対象データの任意の一部分から所定のサイズのデータを含み、

前記本体データは、前記所定のサイズ+1以降のデータに代えて、前記管理対象データの前記任意の一部分以外の残余部分のデータを含む、

請求項 19 に記載のセンターサーバ装置。

【請求項 21】

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 17 又は 18 に記載のコロニーサーバ装置の各手段として機能されるプログラム。

【請求項 22】

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 19 又は 20 に記載のセンターサーバ装置の各手段として機能させるプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、インターネット等のネットワークを介して機密情報、電子為替、付記電文、暗号資産、仮想通貨、電子通貨、有価証券等のデータ（以下、「管理対象データ」という）を、クラウドを構成する複数のサーバで安全に保存し、利用者が使用する情報処理端末からの要求に応じて、当該端末に管理対象データを適宜取得させることを可能にするためのシステム、方法、装置及びプログラムに関する。

【0002】

具体的には、本発明は、利用者のスマートフォン、コンピュータ等の情報処理端末とインターネット等のネットワークを介して接続されたサーバ（以下、「コロニーサーバ」という）が、利用者の情報処理端末からアップロードされた管理対象データを、先頭から所定のサイズまでのデータを含む部分データと、それ以降のデータを含む本体データとに分割して、コロニーサーバとクローズドネットワークを介して接続されたサーバ（以下、「センターサーバ」という）に部分データを送信し、センターサーバは受信した部分データを暗号化して、ブロックチェーンの1ブロックとして記憶し、部分データのハッシュ値を所定の間隔で更新するとともに、本体データのハッシュ値を部分データのものと同じ値に更新することで、高度なセキュリティを実現しつつ、管理対象データを安全に流通させることを可能にする技術に関する。

【背景技術】

【0003】

例えば、金融商品等の取引は、従来、金融機関や政府などの信頼できる中央集権機関を経由して実施されてきたが、近年、利用者間の P2P（Peer to Peer）によって直接的な取引に代替する技術として、ブロックチェーンを用いた分散台帳技術がある。

【0004】

分散台帳技術は、主に、分散台帳システムへの参加者間の取引において、中央集権機関ではなく（任意ないしは特定の）参加者による合意形成や承認によって取引を確定させることができる。また、分散台帳技術は、複数のトランザクションをブロックとしてまとめ、数珠つなぎにブロックチェーンと呼ばれる分散台帳に記録し、連続するブロックにハッ

10

20

30

40

50

シュ計算を施すことにより、改ざんを実質不可能にすることができる。さらに、分散台帳技術は、参加者全員が同一の台帳データを共有することにより、参加者全員での取引の確認を可能とする。

【0005】

以上のような特徴から、ブロックチェーン等の分散台帳技術は、信頼できるデータの管理及び共有や、契約に基づく取引の執行及び管理を行う仕組みとして、金融分野やIoT（Internet of Thing）等の幅広い分野での応用が検討されている。その1つの応用例として、ビットコイン等の暗号資産の取引には、既にブロックチェーン等の分散台帳技術が実装されている。暗号資産は、仮想通貨とも呼ばれている。

【0006】

スマートフォン等の情報処理端末を用いて、ネットワーク経由によるオンラインで、利用者が暗号資産（仮想通貨、種々の金融商品等）を売買する電子商取引では、その取引記録をブロックチェーン上に記録することができる。例えば、特開2019-106639号公報（特許文献1）には、上記のような電子商取引をブロックチェーン上で行うことが可能な電子商取引装置等が記載されており、ブロックチェーン上では、当事者間の信頼関係や第三者への信頼が存在しなくても、取引記録の改竄困難性などから、コンテンツの持ち逃げ等を防ぐことができる。

【先行技術文献】

【特許文献】

【0007】

【文献】特開2019-106639号公報

【発明の概要】

【発明が解決しようとする課題】

【0008】

上記のように、暗号資産の電子商取引は、ブロックチェーンを用いることで実現することができるが、ブロックチェーンでは、取引の公正性が、当該ブロックチェーンを構成する各ノードによって保証されるため、取引の内容が基本的に公開されるという性質が有るため、悪意のある者がブロックチェーンのシステム的な脆弱性を探することは可能である。そして、脆弱性が見つかった場合に、その脆弱性を突いて不正アクセス等で意図しない第三者に暗号資産を流出させることは現実に起こり得るため、ブロックチェーンのセキュリティ対策が十分であるとはいえない。

【0009】

また、ブロックチェーン上に記録される取引の公正性を保証するためには、コンピュータによって、ブロックチェーンにおける複数のブロックの各々が正しい記録であることを検証する検証作業が必要になる。例えば、ビットコインで採用されているプルーフオブワーク（POW）という仕組みでは、ブロックチェーンに新たなブロックを追加するために、ナンス（nonce）と呼ばれる値を総当たり式に変化させて、所定の条件を満たすハッシュ値（例えば、一定回数の「0」の連続から始まるハッシュ値）を算出するのに、コンピュータの膨大な計算が必要となり、その計算ために大量の電力が消費されることになる。

【0010】

これらの課題を解決するために、本発明では、機密情報、電子為替、付記電文、暗号資産、仮想通貨、電子通貨、有価証券等の管理対象データをクラウド上で安全に保存し、オンラインで適宜利用者に配布するために、端末と、コロニーサーバと、センターサーバとを少なくとも備えるデータ管理システムを提供する。本発明に係るデータ管理システムにおいて、コロニーサーバが端末から受信した管理対象データを先頭から所定のサイズまでのデータを含む部分データを記憶し、センターサーバが所定のサイズ+1以降のデータを含む本体データを記憶することで、管理対象データを部分データと本体データとに分散させて管理するだけでなく、不正アクセス等によってコロニーサーバから本体データが流出したとしても、そもそも本体データは、管理対象データの一部のデータでしかなく、本体データのみでは無価値なものであり、本体データのみからは、管理対象データを復元する

10

20

30

40

50

ことができない。このように、本発明では、たとえコロニーサーバから本体データが不正に流出したとしても、実質的な被害を受けることのない堅牢なセキュリティを実現したデータ管理システム、方法、装置及びプログラム（以下、単に「データ管理システム等」ともいう）を提供する。

【0011】

また、本発明では、センターサーバは受信した部分データを暗号化して、ブロックチェーンの1ブロックとして記憶し、部分データのハッシュ値を所定の間隔で更新するとともに、コロニーサーバにおける本体データのハッシュ値を部分データのハッシュ値と同じ値に更新させることで、不正アクセス等によってコロニーサーバから本体データが流出した場合であっても、当該本体データと対となる部分データを含む暗号化キーを特定しようとしても、暗号化キーのハッシュ値は所定の間隔で更新されるため、不正に流出した本体データに含まれるハッシュ値に一致するハッシュ値を含む暗号化キーは存在しなくなり、不正に流出した本体データから管理対象データを復元することを不可能にするデータ管理システム等を提供する。

10

【0012】

さらに、本発明では、センターサーバは、管理対象データの全体ではなく一部のデータである部分データのみをブロックチェーン上に記憶することができるため、比較的小さな記憶領域でブロックチェーンを管理することができ、センターサーバを政府や銀行等の信頼できる機関で運用することで、ブロックチェーンの公正性を保証する計算作業を簡略化もしくは省略することができるデータ管理システム等を提供する。

20

【課題を解決するための手段】

【0013】

本発明に係るデータ管理システムの1つの実施形態として、
前記データ管理システムは、
端末と、
前記端末と第1のネットワークを介して接続されたコロニーサーバと、
前記コロニーサーバと第2のネットワークを介して接続されたセンターサーバと
を少なくとも備え、
前記端末は、管理対象データに関する要求を前記コロニーサーバに送信し、
前記コロニーサーバは、前記管理対象データに関する要求に応じて取得又は生成した管理対象データを、先頭から所定のサイズまでのデータを含む部分データと、前記所定のサイズ+1以降のデータを含む本体データとに分割して、前記部分データを前記センターサーバに送信する分割送信部と、
前記センターサーバからハッシュ値を受け取り、前記本体データに関連付けて前記ハッシュ値を記憶する本体データ管理部と、
前記ハッシュ値を更新するハッシュ更新部と
を含み、
前記センターサーバは、前記部分データを少なくとも含む暗号化したデータである暗号化キーを生成し、前記暗号化キーと共に該暗号化キーを識別するための前記ハッシュ値を記憶する部分データ管理部と、
前記暗号化キーと共に記憶された前記ハッシュ値を前記コロニーサーバに送信するハッシュ通知部と、
前記ハッシュ値を用いて前記暗号化キーを識別して取得する暗号化キー取得部と
を含み、
前記ハッシュ通知部は、前記暗号化キーと共に記憶された前記ハッシュ値を、所定の間隔で、前記本体データに関連付けて記憶された前記ハッシュ値とは一致しない新たなハッシュ値に更新して、前記新たなハッシュ値を前記コロニーサーバに送信し、
前記ハッシュ更新部は、前記新たなハッシュ値を受け取り、前記本体データに関連付けて記憶された前記ハッシュ値を前記新たなハッシュ値に更新し、
前記暗号化キー取得部は、前記暗号化キーと共に記憶された前記ハッシュ値が更新され

30

40

50

た場合には、前記コロニーサーバからの前記新たなハッシュ値を含む、管理対象データに関する要求に応じて、前記新たなハッシュ値を用いて前記暗号化キーを識別して取得し、前記部分データは、前記暗号化キーから復元され、前記管理対象データは、前記部分データと前記本体データとを結合することで復元されることを特徴とする。

【0014】

本発明に係るデータ管理システムの好ましい実施形態として、前記部分データ管理部は、前記部分データの他に、前記管理対象データのファイル名及び時間の少なくとも一方を含めて、暗号化を行い、前記暗号化キーは、前記部分データの他に、前記ファイル名及び前記時間の少なくとも一方を含むことを特徴とする。

10

【0015】

本発明に係るデータ管理システムの好ましい実施形態として、前記管理対象データに関する要求は、前記端末においてアップロードされた、前記管理対象に対応する管理対象データを含むことを特徴とする。

【0016】

本発明に係るデータ管理システムの好ましい実施形態として、前記管理対象データに関する要求は、前記コロニーサーバにおいて前記管理対象に対応する管理対象データを生成させる要求であることを特徴とする。

【0017】

本発明に係るデータ管理システムの好ましい実施形態として、前記所定のサイズは、前記管理対象データの先頭から30バイト以下であることを特徴とする。

20

【0018】

本発明に係るデータ管理システムの好ましい実施形態として、前記所定の間隔は、24時間以下の間隔であることを特徴とする。

【0019】

本発明に係るデータ管理システムの好ましい実施形態として、前記第1のネットワークはインターネットであり、前記第2のネットワークはクロースドネットワークであることを特徴とする。

30

【0020】

本発明に係るデータ管理システムの好ましい実施形態として、前記コロニーサーバの分割送信部は、前記管理対象データを先頭から所定のサイズまでのデータに代えて、前記管理対象データの任意の一部分から所定のサイズのデータを前記部分データとし、

前記所定のサイズ+1以降のデータに代えて、前記管理対象データの任意の一部分以外の残余部分のデータを前記本体データとするように分割することを特徴とする。

【0021】

本発明に係るデータ管理方法の1つの実施形態として、前記データ管理方法は、端末と、前記端末と第1のネットワークを介して接続されたコロニーサーバと、前記コロニーサーバと第2のネットワークを介して接続されたセンターサーバとを少なくとも備えたデータ管理システムによって実行されるデータ管理方法において、前記端末が管理対象データに関する要求を前記コロニーサーバに送信するステップと、前記コロニーサーバが前記管理対象データに関する要求に応じて取得又は生成した管理対象データを先頭から所定のサイズまでのデータを含む部分データと、前記所定のサイズ+1以降のデータを含む本体データとに分割して、前記部分データを前記センターサーバに送信するステップと、

40

前記センターサーバが、前記部分データを少なくとも含む暗号化したデータである暗号化キーを生成するステップと、

50

前記センターサーバが、前記暗号化キーと共に該暗号化キーを識別するためのハッシュ値を記憶するステップと、

前記センターサーバが、前記ハッシュ値を前記コロニーサーバに送信するステップと、
前記コロニーサーバが、前記本体データに関連付けて前記ハッシュ値を記憶するステップと
を含み、

前記センターサーバは、前記暗号化キーと共に記憶された前記ハッシュ値を、所定の間隔で、前記本体データに関連付けて記憶された前記ハッシュ値とは一致しない新たなハッシュ値に更新して、前記新たなハッシュ値を前記コロニーサーバに送信し、

前記コロニーサーバは、前記本体データに関連付けて記憶された前記ハッシュ値を、前記新たなハッシュ値に更新し、

前記センターサーバは、前記暗号化キーと共に記憶された前記ハッシュ値が更新された場合には、前記コロニーサーバからの前記新たなハッシュ値を含む、管理対象データに関する要求に応じて、前記新たなハッシュ値を用いて前記暗号化キーを識別して取得し、

前記部分データは、前記暗号化キーから復元され、

前記管理対象データは、前記部分データと前記本体データとを結合することで復元されることを特徴とする。

【0022】

本発明に係るデータ管理方法の好ましい実施形態として、

前記センターサーバは、前記暗号化キーを生成するステップにおいて、前記部分データの他に、前記管理対象データのファイル名及び時間の少なくとも一方を含めて、暗号化を行い、

前記暗号化キーは、前記部分データの他に、前記ファイル名及び前記時間の少なくとも一方を含むことを特徴とする。

【0023】

本発明に係るデータ管理方法の好ましい実施形態として、

前記管理対象データに関する要求は、前記端末においてアップロードされた、前記管理対象に対応する管理対象データを含むことを特徴とする。

【0024】

本発明に係るデータ管理方法の好ましい実施形態として、

前記管理対象データに関する要求は、前記コロニーサーバにおいて前記管理対象に対応する管理対象データを生成させる要求であることを特徴とする。

【0025】

本発明に係るデータ管理方法の好ましい実施形態として、

前記所定のサイズは、前記管理対象データの先頭から30バイト以下であることを特徴とする。

【0026】

本発明に係るデータ管理方法の好ましい実施形態として、

前記所定の間隔は、24時間以下の間隔であることを特徴とする。

【0027】

本発明に係るデータ管理方法の好ましい実施形態として、

前記第1のネットワークはインターネットであり、前記第2のネットワークはクローズドネットワークであることを特徴とする。

【0028】

本発明に係るデータ管理方法の好ましい実施形態として、

前記コロニーサーバが前記管理対象データに関する要求に応じて取得又は生成した管理対象データを先頭から所定のサイズまでのデータを含む部分データと、前記所定のサイズ+1以降のデータを含む本体データとに分割して、前記部分データを前記センターサーバに送信するステップは、

前記管理対象データを先頭から所定のサイズまでのデータに代えて、前記管理対象デー

10

20

30

40

50

タの任意の一部分から所定のサイズのデータを前記部分データとし、

前記所定のサイズ+1以降のデータに代えて、前記管理対象データの任意の一部分以外の残余部分のデータを前記本体データとするように分割することを特徴とする。

【0029】

本発明に係るコロニーサーバ装置の1つの実施形態として、前記コロニーサーバ装置は、端末から管理対象データに関する要求を受け取る手段と、

前記管理対象データに関する要求に応じて取得又は生成した管理対象データを先頭から所定のサイズまでのデータを含む部分データと、前記所定のサイズ+1以降のデータを含む本体データとに分割して、前記部分データをセンターサーバ装置に送信する分割送信手段と、

前記センターサーバ装置から、前記部分データを少なくとも含む暗号化したデータである暗号化キーを識別するためのハッシュ値を受け取り、前記本体データに関連付けて前記ハッシュ値を記憶する本体データ管理手段と

を含み、

前記コロニーサーバ装置は、前記センターサーバ装置から、前記本体データに関連付けて記憶された前記ハッシュ値とは一致しない新たなハッシュ値を、所定の間隔で受信し、

前記コロニーサーバ装置は、前記本体データに関連付けて記憶された前記ハッシュ値を、前記所定の間隔で、前記新たなハッシュ値に更新し、

前記コロニーサーバ装置は、前記暗号化キーと共に記憶された前記ハッシュ値が更新された場合には、前記センターサーバ装置に前記新たなハッシュ値を用いて前記暗号化キーを識別させるために、前記新たなハッシュ値を含む、管理対象データに関する要求を前記センターサーバ装置に送信し、

前記部分データは、前記暗号化キーから復元され、

前記管理対象データは、前記部分データと前記本体データとを結合することで復元されることを特徴とする。

【0030】

本発明に係るコロニーサーバ装置の好ましい実施形態として、

前記分割送信手段は、前記管理対象データを先頭から所定のサイズまでのデータに代えて、前記管理対象データの任意の一部分から所定のサイズのデータを前記部分データとし、

前記所定のサイズ+1以降のデータに代えて、前記管理対象データの任意の一部分以外の残余部分のデータを前記本体データとするように分割することを特徴とする。

【0031】

本発明に係るセンターサーバ装置の1つの実施形態として、前記センターサーバ装置は、センターサーバ装置であって、

コロニーサーバ装置から、管理対象データの先頭から所定のサイズまでのデータを含む部分データを受け取る手段と、

前記部分データを少なくとも含む暗号化したデータである暗号化キーを生成し、前記暗号化キーと共に該暗号化キーを識別するためのハッシュ値を記憶する部分データ管理手段と、

前記暗号化キーと共に記憶された前記ハッシュ値を前記コロニーサーバ装置に送信するハッシュ通知手段と

を含み、

前記ハッシュ通知手段は、前記暗号化キーと共に記憶された前記ハッシュ値を、所定の間隔で、前記ハッシュ値とは一致しない新たなハッシュ値に更新して、前記新たなハッシュ値を前記コロニーサーバ装置に送信し、

前記センターサーバ装置は、前記暗号化キーと共に記憶された前記ハッシュ値が更新された場合には、前記コロニーサーバ装置からの前記新たなハッシュ値を含む、管理対象データに関する要求に応じて、前記新たなハッシュ値を用いて前記暗号化キーを識別し、

前記部分データは、前記暗号化キーから復元され、

前記管理対象データは、前記部分データと、前記管理対象データの先頭から前記所定の

10

20

30

40

50

サイズ+1以降のデータを含む本体データとを結合することで復元されることを特徴とする。

【0032】

本発明に係るセンターサーバ装置の好ましい実施形態として、

前記部分データは、前記管理対象データを先頭から所定のサイズまでのデータに代えて、前記管理対象データの任意の一部分から所定のサイズのデータを含み、

前記本体データは、前記所定のサイズ+1以降のデータに代えて、前記管理対象データの任意の一部分以外の残余部分のデータを含むことを特徴とする。

【0033】

本発明に係るプログラムの1つの実施形態として、前記プログラムは、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コロニーサーバ装置の各手段として機能されることを特徴とする。

【0034】

本発明に係るプログラムの1つの実施形態として、前記プログラムは、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センターサーバ装置の各手段として機能されることを特徴とする。

【発明の効果】

【0035】

本発明に係るデータ管理システム、方法、装置及びプログラムは、コロニーサーバが端末から受信した管理対象データを先頭から所定のサイズまでのデータを含む部分データを記憶し、センターサーバが所定のサイズ+1以降のデータを含む本体データを記憶することで、管理対象データを分散させて管理するだけでなく、不正アクセス等によってコロニーサーバから本体データが流出したとしても、そもそも本体データは、管理対象データの一部のデータでしかなく、本体データのみでは無価値なものであることから、不正アクセスに対して堅牢なセキュリティを実現することができる。

【0036】

また、本発明に係るデータ管理システム等は、センターサーバの管理下にあるブロックチェーンにおける1ブロックに暗号化キーとして記憶した部分データのハッシュ値を、所定の間隔で更新するとともに、コロニーサーバにおける本体データのハッシュ値を部分データのハッシュ値と同じ値に更新させることで、不正アクセス等によってコロニーサーバから本体データが流出した場合であっても、不正に流出した本体データと対となる部分データを含む暗号化キーのハッシュ値は所定の間隔で更新されるため、当該本体データのハッシュ値に一致するハッシュ値を含む暗号化キーは存在しなくなり、不正に流出した本体データを解析しても、管理対象データを復元するために必要な暗号化キーにたどり着くことは困難となり、管理対象データを復元することは実質的に不可能にすることができる。

【0037】

さらに、本発明に係るデータ管理システム等は、センターサーバは、管理対象データの全体ではなく一部のデータである部分データのみをブロックチェーン上に記憶することができるため、比較的小さな記憶領域でブロックチェーンを管理することができる。これにより、センターサーバでブロックチェーンに新たなブロックを形成する際等に、ハッシュ値の計算等は比較的小さな情報に基づいて行えることになるから、コンピュータにおける計算量を大幅に減らすことが期待できる。そして、センターサーバを政府や銀行等の信頼できる機関で運用することで、ブロックチェーンの公正性を保証する検証作業を簡略化もしくは省略することができ、コンピュータを用いた膨大な計算及びそれに伴う電力の消費を抑えることができる。

【図面の簡単な説明】

【0038】

【図1】本発明の一実施形態に係るデータ管理システムの構成を示す概略構成図（システム構成図）である。

【図2】本発明の一実施形態に係るサーバ及び情報処理端末のハードウェア構成の一例を

10

20

30

40

50

示す概略構成図（ブロック図）である。

【図 3】本発明の一実施形態に係るセンターサーバ及びコロニーサーバの概略構成図（ブロック図）である。

【図 4】センターサーバ及びコロニーサーバのデータ処理の手順の一例を示す図である。

【図 5】コロニーサーバからセンターサーバへの管理対象データの登録処理の概要を示す図である。

【図 6】センターサーバで管理されるブロックチェーンの基本的な構成の概要を示す概略図である。

【図 7】管理対象データをセンターサーバに登録する処理の流れを示すシーケンス図である。

【図 8】センターサーバから管理対象データを取得する処理の流れを示すシーケンス図である。

【図 9】管理対象データを同じコロニーサーバに接続された端末間で譲渡する処理の流れを示すシーケンス図である。

【図 10】管理対象データを異なるコロニーサーバに接続された端末間で譲渡する処理の流れを示すシーケンス図である。

【図 11】管理対象データを異なるコロニーサーバに接続された端末間で譲渡する処理の流れを示すシーケンス図である。

【図 12】銀行間の金融商品の取引に本発明に係るデータ管理システムを適用した例を示す図である。

【図 13】イベント参加者への特典付与に本発明に係るデータ管理システムを適用した例を示す図である。

【図 14】管理対象データを暗号化キーと本体データとに分割する処理の流れを示すデータ管理システム全体としてのフローチャートである。

【図 15】センターサーバからアクセス可能なブロックチェーンにおける 1 ブロックと、コロニーサーバからアクセス可能な本体データとの関係を示す図である。

【図 16】コロニーサーバにおいて独立して記憶される本体データの概要を示す図である。

【図 17】センターサーバにおいてブロックチェーンに新たに暗号化キーを含むブロックを接続する処理の流れを示すフローチャートである。

【図 18】センターサーバの管理下にあるブロックチェーンの構成を示す図である。

【図 19】センターサーバのデータベースに記憶される各種情報の概要を示す図である。

【図 20】コロニーサーバのデータベースに記憶される情報の概要を示す図である。

【図 21】ブロックチェーンにおいて改ざんを検出した際の各ブロックの凍結及び修復の処理の概要を示す図である。

【図 22】ブロックチェーンを監視して改ざんを検出した際の処理の流れを示すフローチャートである。

【図 23】ブロックチェーンにおけるブロックを凍結する処理の流れを示すフローチャートである。

【図 24】ブロックチェーンを修復する処理の流れを示すフローチャートである。

【発明を実施するための形態】

【0039】

以下に図面を参照して、本発明の一実施形態について説明する。なお、実施の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適宜実施することができる。

【0040】

図 1 は、本発明の一実施形態に係るデータ管理システムの構成を示すシステム構成図である。データ管理システムは、例示的に、センターサーバ 10 と、コロニーサーバ 20 と、情報処理端末 30 とを含む。情報処理端末 30 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、携帯電話等のインターネットに接続可能な端末である

10

20

30

40

50

。本発明に係るデータ管理システムは、有価物、機密情報、電子為替、付記電文等の電子的なデータを管理対象とする。ここでは、管理対象となる電子的なデータを管理対象データと呼ぶ。管理対象データは、本発明に係るデータ管理システムにおけるセンターサーバ10、コロニーサーバ20、及び情報処理端末30の各記憶手段に記憶可能であり、必要に応じて送受信可能なデータである。なお、管理対象データは、本発明に係るデータ管理システムにおいて、電子的なデータとして取り扱い可能なデータであればどのような内容のデータでも良い。また、有価物とは、金銭上の価値があるものであり、例えば、暗号資産、仮想通貨、電子通貨、有価証券、機密情報等である。センターサーバ10とコロニーサーバ20とは、ネットワークN1を介して接続される。ネットワークN1は、例えば、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る。コロニーサーバ20と情報処理端末30とは、ネットワークN2を介して接続される。ネットワークN2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る。ネットワークN1及びN2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かオープンネットワークかを選択することができる。

【0041】

情報処理端末30は、例えば、インターネット等であるネットワークN2を介してコロニーサーバ20にアクセスすることは可能であるが、センターサーバ10とはクローズドネットワークであるネットワークN1を介して接続されていないため、直接的にアクセスすることはできない。センターサーバ10にアクセスすることができるのは、ネットワークN2を介して接続されたコロニーサーバ20のみである。図1に示す実施形態では、センターサーバ10は、1台であるが複数台設けてもよい。

【0042】

図2は、本発明の一実施形態に係るサーバ及び情報処理端末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、センターサーバ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、コロニーサーバ20及び情報処理端末30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】

センターサーバ10は、例示的に、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】

CPU 11は、メモリ12に記録されているプログラム、又は、記憶部27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。CPU 11は、例えば、サーバ装置を本発明のセンターサーバ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、センターサーバ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。本発明のその他のサーバ、情報処理端末についても同様である。

【0045】

メモリ12には、CPU 11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。CPU 11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、センターサーバ10の管理者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、センターサーバ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、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)
等の半導体メモリで構成され、各種データを記憶する。

【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N1を介して、コロニーサーバ20との間で相互に通信を行う。

10

【0050】

なお、センターサーバ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、暗号資産取引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、画像データ等の各種のデータは、必要に応じて記憶部17にインストールされ
る。

【0051】

次に、コロニーサーバ20のハードウェアの構成について説明する。コロニーサーバ2
0は、図2に示すように、例示的に、CPU21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、上述のセンターサーバ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。情報処理端末3
0についても同様である。なお、情報処理端末30を、携帯型の装置として構成する場合
には、情報処理端末30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。

20

【0052】

図3を参照してデータ管理システムを構成するセンターサーバ10及びコロニーサーバ
20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センターサーバ
及びコロニーサーバのブロック図である。センターサーバ10は、センターサーバ側のデ
ータ管理のためのプログラムが実行された場合、CPU11において、部分データ管理部
111と、ハッシュ通知部112と、暗号化キー取得部113が機能する。また、記憶部
17の一部の記憶領域には、コロニー情報記憶部171と、ユーザ情報記憶部172と、
暗号化キー記憶部173とが設定される。コロニー情報記憶部171、ユーザ情報記憶部
172及び暗号化キー記憶部173に記憶される情報の詳細は後述する。

30

【0053】

センターサーバ10の部分データ管理部111は、コロニーサーバ20から送信させる
管理対象データの一部のデータである部分データを暗号化し、暗号化した部分データを暗
号化キーとして記憶したブロックを生成して、ブロックをブロックチェーンに追加するこ
とができる。また、部分データ管理部111は、部分データの他に、管理対象データのフ
ァイル名及び時間の少なくとも一方を含めて、暗号化を行ってもよく、暗号化キーには、
部分データの他に、そのファイル名及び時間の少なくとも一方を含めてもよい。

40

【0054】

ハッシュ通知部112は、所定の間隔で暗号化キーを記憶したブロックのブロックハッ
シュ値を、当該ブロックハッシュ値とは異なるハッシュ値に更新して、更新されたブロッ
クハッシュ値を新たなハッシュ値としてコロニーサーバに送信することができる。所定の
間隔は、24時間以下の間隔とすることができ、例えば、1時間、6時間、12時間、2
4時間等を指定することができる。また、所定の間隔は、24時間を超える時間を指定す
ることもできる。

50

【0055】

暗号化キー取得部113は、コロニーサーバ20からの要求（管理対象データに関する要求）に含まれるハッシュ値に基づいて、暗号化キー記憶部173に記憶された暗号化キーを識別して、当該暗号化キーを取得することができる。例えば、暗号化キー取得部113は、所定の間隔で、暗号化キーと共に暗号化キー記憶部173に記憶されたハッシュ値が更新された場合には、コロニーサーバ20からの新たなハッシュ値を含む、管理対象データに関する要求に応じて、当該新たなハッシュ値を用いて暗号化キー記憶部173から所望の暗号化キーを識別し、当該暗号化キーを取得することができる。

【0056】

コロニーサーバ20は、コロニーサーバ側のデータ管理のためのプログラムが実行された場合、CPU21において、分割送信部211と、本体データ管理部212と、ハッシュ更新部213とが機能する。また、記憶部27の一部の記憶領域には、ハッシュ情報記憶部271と、本体データ記憶部272とが設定される。ハッシュ情報記憶部271及び本体データ記憶部272に記憶される情報の詳細は後述する。

10

【0057】

コロニーサーバ20の分割送信部211は、情報処理端末30からの管理対象データに関する要求に応じて取得又は生成した管理対象データを先頭から所定のサイズまでのデータを含む部分データと、所定のサイズ+1以降のデータを含む本体データとに分割して、部分データをセンターサーバ10に送信することができる。ここで、所定のサイズは、例えば、管理対象データの先頭から30バイト以下とすることができる。所定のサイズは、これに限定されるものではなく、適宜設定することができる。

20

【0058】

また、分割送信部211は、管理対象データを先頭から所定のサイズまでのデータに代えて、管理対象データの任意の一部分から所定のサイズのデータを部分データとし、先頭から所定のサイズ+1以降のデータに代えて、管理対象データの任意の一部分（つまり、部分データ）以外の残余部分のデータを本体データとするように分割することもできる。

【0059】

本体データ管理部212は、センターサーバ10からブロックハッシュ値を受け取り、本体データに関連付けてブロックハッシュ値を本体データのハッシュ値としてハッシュ情報記憶部271に記憶することができる。また、本体データ管理部212は、情報処理端末30からコロニーサーバ20にアップロードされる管理対象データの本体データを本体データ記憶部272に記憶することができる。

30

【0060】

ハッシュ更新部213は、センターサーバ10のハッシュ通知部112から通知される新たなハッシュ値を受け取り、当該新たなハッシュ値で本体データに関連付けて記憶されたハッシュ値を更新することができる。新たなハッシュ値は、本体データに関連付けて既に記憶されているハッシュ値とは異なるハッシュ値である。

【0061】

図4は、センターサーバ及びコロニーサーバのデータ処理の手順の一例を示す。はじめに、コロニーサーバ20において、利用者の情報処理端末30から管理対象データのアップロード（もしくは、コロニーサーバ20において管理対象データの生成）を行い（ステップ1）、管理対象データを圧縮して（ステップ2）、管理対象データに相当する圧縮データの0と1のビット列を、MIME（Multipurpose Internet Mail Extensions）に基づいて、16進数のテキストデータに置き換える（ステップ3）。図4に示す一例では、管理対象データを圧縮しているが、これに限定されるものではなく、管理対象データを圧縮しなくてもよい。MIMEは、インターネットの電子メールの規格を拡張して、さまざまな形式を扱えるようにした規格である。

40

【0062】

次に、コロニーサーバ20において、例えば、管理対象データに相当する16進数テキストデータの先頭30バイトを部分データとして切り取り（カットし）（ステップ4）、

50

31バイト以降のデータを本体データとしてデータベース（例えば、本体データ記憶部272）に登録（記憶）する（ステップ5）。

【0063】

そして、部分データ（先頭30バイトのデータ）は、コロニーサーバ20から管理対象データの登録ファイル名と共に、センターサーバ10に送信される。センターサーバ10では、部分データ（先頭30バイトのデータ）と管理対象データのファイル名を受信して（ステップ6）、それらに基づいて管理対象データの一部である部分データの暗号化を行う（ステップ7）。例えば、部分データを暗号化して暗号化キー（DBED（Data Binary Encrypted Data）ともいう）を生成する。暗号化キー（DBED）をブロックチェーン（又はブロックチェーンデータツリー（Block chain data tree））の1ブロックとして追加（登録）して（ステップ8）、ブロックチェーンハッシュ（Block chain hash）を生成、すなわち、ブロックチェーンに追加されたブロックのブロックハッシュ値を計算する（ステップ9）。最後に、センターサーバ10からコロニーサーバ20にブロックハッシュ値を送信して、コロニーサーバ20において、バイナリラージオブジェクト（BLOB）として、バイナリデータであるブロックハッシュ値をデータベース（例えば、ハッシュ情報記憶部271）に登録する（ステップ10）。

【0064】

図5は、コロニーサーバからセンターサーバへの管理対象データの登録処理の概要を示す。利用者X（ユーザX）は、情報処理端末30Xを用いて、ネットワークN1を介して、コロニーサーバ20にログインして管理対象データをコロニーサーバ20にアップロードする。コロニーサーバ20にアップロードされた管理対象データは、上述のとおり、MIME（例えばMIME64）に基づいて、例えば、ABCDEFG2345678等のように文字列化され、管理対象データを示すファイル名と共に次の処理に渡される。コロニーサーバ20において、文字列化された管理対象データを先頭から所定のサイズまでの部分データ（例えば、ABC）と、所定のサイズ+1以降の本体データ（例えば、DEFG2345678）とに分割して、部分データはファイル名と共に、ネットワークN2を介した暗号化通信により、センターサーバ10に送信される。図4及び5に示す例では、文字列化された管理対象データの先頭から所定のサイズまでのデータを部分データとし、それ以降のデータを本体データとしているが、これに限定されるものではなく、部分データは、管理対象データを先頭から所定のサイズまでのデータに代えて、管理対象データの任意の一部分から所定のサイズのデータを含み、本体データは、所定のサイズ+1以降のデータに代えて、管理対象データの任意の一部分以外の残余部分のデータを含むこともできる。

【0065】

このように、本発明の一実施形態に係るデータ管理システムは、コロニーサーバ20が情報処理端末30から受信した管理対象データを先頭から所定のサイズまでのデータを含む部分データを記憶し、センターサーバ10が所定のサイズ+1以降のデータを含む本体データを記憶することで、管理対象データを分散させて管理するだけでなく、不正アクセス等によってコロニーサーバ20から本体データが流出したとしても、そもそも本体データは、管理対象データの一部のデータでしかなく、本体データのみでは無価値なものであることから、不正アクセスに対して堅牢なセキュリティを実現することができる。

【0066】

また、本発明の一実施形態に係るデータ管理システムは、センターサーバ10は、管理対象データの全体ではなく一部のデータである部分データのみをブロックチェーン上に記憶することができるため、比較的小さな記憶領域でブロックチェーンを管理することができる。これにより、センターサーバ10でブロックチェーンに新たなブロックを形成する際等に、ハッシュ値の計算等は比較的小さな情報に基づいて行えることになるから、センターサーバ10等のコンピュータにおける計算量を大幅に減らすことが期待できる。そして、センターサーバ10を政府や銀行等の信頼できる機関で運用することで、ブロックチェーンの公正性を保証する検証作業を簡略化もしくは省略することができ、コンピュータを用いた膨大な計算及びそれに伴う電力の消費を抑えることができる。

【0067】

図6は、センターサーバで管理されるブロックチェーンの基本的な構成の概要を示す。ブロックチェーン100の1つのブロック101Aは、互いに異なる2つのブロックハッシュ値（Block Chain Hash(1)とBlock Chain Hash(2)、例えば、0xaa708c8c, 0x038b67cf）と、管理対象データの部分データを暗号化した暗号化キー（例えば、ddyymsUGIURA100）とを含む。一方のブロックハッシュ値（Block Chain Hash(1)）は、前のブロックのブロックハッシュ値と同じハッシュ値であり、ハッシュ値が同じであることに基づいてブロック101Aは前のブロックと結合される。同様に、他方のブロックハッシュ値（Block Chain Hash(2)）は、先のブロックハッシュ値と同じハッシュ値であり、ハッシュ値が同じであることに基づいて、ブロック101Aは先のブロックとも結合される。

10

【0068】

図7は、管理対象データをセンターサーバに登録する処理の流れを示すシーケンス図である。利用者は情報処理端末30を用いて、例えばインターネットを介してコロニーサーバ20にログイン（サインイン）してアクセスし（ステップS101）、コロニーサーバ20は、利用者の情報処理端末30を用いたログインが成功した場合に、ログイン成功（OK）の応答を情報処理端末30に送信する（ステップS102）。そして、利用者は、情報処理端末30上で、管理対象データのアップロード又は管理対象データの生成リクエストを選択して（ステップS103）、コロニーサーバ20に管理対象データをアップロードする、又は管理対象データの生成リクエストを送信する（ステップS104）。コロニーサーバ20では、アップロード又は生成された管理対象データを、上述したとおり、圧縮、文字列化等の暗号化処理を行い、例えば、先頭から30バイトまでの部分データと31バイト以降の本体データとに分割して、先頭30バイトの部分データをセンターサーバ10に送信する（ステップS106）。

20

【0069】

センターサーバ10において、ブロックチェーンに追加するため1つのブロックを生成し（ステップS107）、先頭30バイトの部分データの他に少なくとも管理対象データに関連する時間（例えば、アップロード日時、作成日時等）及び管理対象データに対応するファイル名の少なくとも一方を含めて暗号化を行い、部分データの他にファイル名及び時間（アップロード日時、作成日時等）の少なくとも一方を含む暗号化キーを生成する（ステップS108）。本実施例では、暗号化の際に、部分データの他に、時間、ファイル名を用いているが、これに限定されるものではなく、その他の文字列、データ等（例えば、利用者のログインID、パスワード）を用いることもできる。暗号化キーを復号化することで、暗号化キーに含まれる部分データを復元（抽出）することができる。

30

【0070】

センターサーバ10は、生成したブロックに暗号化キーを含めて、ブロックチェーンに当該ブロックを追加し（ステップS109）、追加されたブロックのブロックハッシュ値をコロニーサーバ20に送信する（ステップS110）。コロニーサーバ20において、受信したブロックハッシュ値を本体データとともにデータベース（本体データ記憶部272）に記憶して、部分データが欠落した管理対象データ（すなわち、本体データ）を生成する（ステップS111）。最後に、コロニーサーバ20は、管理対象データの生成が完了した場合に、完了通知を情報処理端末30に送信する（ステップS112）。

40

【0071】

図8は、センターサーバから管理対象データを取得する処理の流れを示すシーケンス図である。利用者は情報処理端末30を用いて、例えばインターネットを介してコロニーサーバ20にログイン（サインイン）してアクセスし（ステップS201）、コロニーサーバ20は、利用者の情報処理端末30を用いたログインが成功した場合に、ログイン成功（OK）の応答を情報処理端末30に送信する（ステップS202）とともに、管理対象データ等の目録を送信する（ステップS203）。

【0072】

50

利用者は、情報処理端末30の画面上に表示される管理対象データ等の目録から、所望の管理対象データの取得のために必要な項目を選択して（ステップS204）、情報処理端末30は、利用者が選択した項目とともに、管理対象データの取得のリクエストをコロニーサーバ20に送信する（ステップS205）。コロニーサーバ20において、情報処理端末30からのリクエストに基づいて、データベースからリクエストされた管理対象データ（に対応する本体データ）を特定して検証を行う（ステップS206）。検証の結果、問題なければ、管理対象データの31バイト以降のデータである本体データを情報処理端末30に送信する（ステップS207）とともに、本体データに関連付けて記憶されているブロックハッシュ値に基づいて、本体データに対応する部分データをセンターサーバ10にリクエストする（ステップS208）。

10

【0073】

センターサーバ10は、リクエストに応じて、ブロックチェーンのブロックを検証し（ステップS209）、暗号化キーから管理対象データの先頭から30バイトのデータである部分データを復元（復号）して、コロニーサーバ20に送信する（ステップS210）。コロニーサーバ20は受信した部分データを情報処理端末30に送信し（ステップS211）、情報処理端末30において、受信した部分データを本体データに結合して、管理対象データを生成する（ステップS212）。

【0074】

図9は、管理対象データを同じコロニーサーバに接続された端末間で譲渡する処理の流れを示すシーケンス図である。同じコロニーサーバ20に接続された情報処理端末30Xの利用者Xから情報処理端末30Yの利用者Yに管理対象データを譲渡する場合、利用者Xは情報処理端末30Xを用いて、例えばインターネットを介してコロニーサーバ20にログイン（サインイン）してアクセスし（ステップS301）、コロニーサーバ20は、利用者の情報処理端末30Xを用いたログインが成功した場合に、ログイン成功（OK）の応答を情報処理端末30Xに送信する（ステップS302）とともに、管理対象データ等の目録を送信する（ステップS303）。

20

【0075】

利用者Xは、情報処理端末30Xの画面上に表示される管理対象データ等の目録から、管理対象データの譲渡のために必要な項目を選択して（ステップS304）、譲渡先である利用者YのユーザIDを入力する（ステップS305）とともに、譲渡のリクエストをコロニーサーバ20に送信する（ステップS306）。

30

【0076】

コロニーサーバ20は、譲渡先のユーザIDを検証し（ステップS307）、問題なければ、ダウンロードURLを生成し（ステップS308）、譲渡先の利用者Yのメールアドレスをセンターサーバ10にリクエストして（ステップS309）、応答（OK）とともにメールアドレスを取得する（ステップS310）。コロニーサーバ20は、取得したメールアドレス宛（情報処理端末30Y）にダウンロードURLを電子メールで通知する（ステップS311）。

【0077】

譲渡先の利用者Yは、情報処理端末30Yにおいて電子メールを確認し、ダウンロードURLを用いてコロニーサーバ20にログインして、管理対象データの本体データである31バイト以降のデータをダウンロードする（ステップS312）。コロニーサーバ20は、本体データがダウンロードされると、当該本体データのブロックハッシュ値をセンターサーバ10に送信する（ステップS313）。センターサーバ10は、受信したハッシュ値に一致するハッシュ値を有するブロックをブロックチェーンから特定し、ブロックに含まれる管理対象データを検証する（ステップS314）。センターサーバ10は、検証結果が正しい場合に、管理対象データの先頭30バイトである部分データをコロニーサーバ20に送信し（ステップS315）、コロニーサーバ20は受信した部分データを情報処理端末30Yに送信する（ステップS316）。最後に、情報処理端末30Yにおいて、受信した部分データを本体データに結合して、管理対象データを復元（生成）する（ス

40

50

テップ S 3 1 7)。

【0078】

図 1 0 及び図 1 1 は、管理対象データを異なるコロニーサーバに接続された端末間で譲渡する処理の流れを示すシーケンス図であり、図 1 0 及び図 1 1 にシーケンス図を合わせて、コロニーサーバ 2 0 A (コロニ A) に接続された情報処理端末 3 0 X からコロニーサーバ 2 0 B (コロニ B) に接続された情報処理端末 3 0 Y への管理対象データを譲渡する処理の流れを示す。

【0079】

まず、図 1 0 を参照すると、利用者 X は情報処理端末 3 0 X を用いて、例えばインターネットを介してコロニーサーバ 2 0 A にログイン (サインイン) してアクセスし (ステップ S 4 0 1)、コロニーサーバ 2 0 は、利用者の情報処理端末 3 0 X を用いたログインが成功した場合に、ログイン成功 (OK) の応答 (失敗した場合には、ログイン失敗 (NG) の応答) を情報処理端末 3 0 X に送信する (ステップ S 4 0 2) とともに、管理対象データ等の目録を送信する (ステップ S 4 0 3)。

【0080】

利用者 X は、情報処理端末 3 0 X の画面上に表示される管理対象データ等の目録から、管理対象データの譲渡のために必要な項目を選択して (ステップ S 4 0 4)、譲渡先である利用者 Y のユーザ ID と、コロニーサーバ 2 0 B の ID を指定する (ステップ S 4 0 5) とともに、譲渡のリクエストをコロニーサーバ 2 0 A に送信する (ステップ S 4 0 6)。コロニーサーバ 2 0 A は、リクエストされた管理対象データの本体データを特定し、本体データのブロックハッシュ値と譲渡先の利用者 Y のユーザ ID とを含むリクエストをセンターサーバ 1 0 に送信する (ステップ S 4 0 7)。

【0081】

センターサーバ 1 0 は、受信したユーザ ID 及びブロックハッシュ値を検証し (ステップ S 4 0 8)、検証の結果正しければ、その旨の応答 (OK) とともに譲渡先の利用者 Y のメールアドレスをコロニーサーバ 2 0 A に送信し (ステップ S 4 0 9)、コロニーサーバ 2 0 は、管理対象データの譲渡を行うか否かの最終確認を情報処理端末 3 0 X に送信する (ステップ S 4 1 0)。情報処理端末 3 0 X は、譲渡の実行を承認する旨の応答 (OK) とともに最終的な譲渡のリクエストをコロニーサーバ 2 0 A に送信し (ステップ S 4 1 1)、コロニーサーバ 2 0 A は、リクエストをセンターサーバ 1 0 に送信する (ステップ S 4 1 2)。

【0082】

センターサーバ 1 0 は管理対象データの先頭 3 0 バイトを含む部分データをコロニーサーバ 2 0 B に送信する (ステップ S 4 1 3)。ここで、図 1 1 を参照すると、コロニーサーバ 2 0 B は、利用者 X からの管理対象データの譲渡がある旨の通知を、譲渡先の利用者 Y は情報処理端末 3 0 Y に通知する (ステップ S 4 1 4)。利用者 Y は、情報処理端末 3 0 Y の画面上に表示される通知等に応じて、情報処理端末 3 0 Y からログインしてコロニーサーバ 2 0 B にアクセスして (ステップ S 4 1 5)、情報処理端末 3 0 Y は、センターサーバ 1 0 から送られてきた管理対象データの先頭 3 0 バイトである部分データを受信する (ステップ S 4 1 6)。

【0083】

図 1 0 を再び参照すると、コロニーサーバ 2 0 A はリクエストをセンターサーバ 1 0 に送信した直後又は実質的には同時に、管理対象データの 3 1 バイト以降のデータである本体データをダウンロードするための URL を生成する (ステップ S 4 1 7)。図 1 1 を参照すると、ダウンロード URL を生成した (ステップ S 4 1 7) 後、コロニーサーバ 2 0 A は、ダウンロード URL を電子メールで、情報処理端末 3 0 Y に送信し (ステップ S 4 1 8)、譲渡先の利用者 Y は、情報処理端末 3 0 Y において電子メールを確認し、ダウンロード URL を用いてコロニーサーバ 2 0 A にログインして、管理対象データの本体データである 3 1 バイト以降のデータをダウンロードする (ステップ S 4 1 9)。最後に、情報処理端末 3 0 Y において、受信した部分データを本体データに結合して、管理対象デー

10

20

30

40

50

タを復元する（ステップ S 4 2 0）。

【 0 0 8 4 】

図 1 2 は、銀行間の金融商品の取引に本発明に係るデータ管理システムを適用した例を示す図である。本発明のシステムは、例えば地方銀行 A から地方銀行 B への送金について、中央銀行（例えば、日本銀行）内の任意の複数の承認者による認証を簡便に行うことができる。複数の承認者で認証を行うことで、なりすましによる送金等を未然に防止することができる。銀行 A から銀行 B への送金（例えば、管理対象データとして電子通貨の送信）は、図 7 に示した、管理対象データをセンターサーバに登録する処理、図 1 0 及び図 1 1 に示した、管理対象データを異なるコロニーサーバに接続された端末間で譲渡する処理に基づいて実現することができる。

10

【 0 0 8 5 】

銀行 A の担当者（送信者）は、銀行 A サーバ（コロニーサーバ A）に接続された端末を用いて、インターネット等の公衆回線を介して、銀行 A サーバにログインしてアクセスし、銀行 A サーバは、銀行 A の担当者の端末を用いたログインが成功した場合に、ログイン成功（OK）の応答を当該端末に送信する。そして、銀行 A の担当者は、端末上で、管理対象データの一例である電子通貨のアップロード又は電子通貨の生成リクエストを選択して、銀行 A サーバに電子通貨をアップロードする、又は電子通貨の生成リクエストを送信する。銀行 A サーバでは、アップロード又は生成された電子通貨を、圧縮、文字列化等の暗号化処理を行い、例えば、先頭から 3 0 バイトまでの部分データと 3 1 バイト以降の本体データとに分割して、先頭 3 0 バイトの部分データを、専用回線（クローズドネットワーク）を介して中央銀行サーバ（センターサーバ）に送信する（ステップ 1）。

20

【 0 0 8 6 】

中央銀行サーバにおいて、先頭 3 0 バイトの部分データをブロックチェーンに追加するため 1 つのブロックを生成し、先頭 3 0 バイトの部分データの他に少なくとも管理対象データである電子通貨に関連する時間（例えば、アップロード日時、作成日時等）及び管理対象データである電子通貨に対応するファイル名の少なくとも一方を含めて暗号化を行い、部分データの他にファイル名及び時間（アップロード日時、作成日時等）の少なくとも一方を含む暗号化キーを生成する。中央銀行サーバは、生成したブロックに暗号化キーを含めて、ブロックチェーンに当該ブロックを追加し、追加されたブロックのブロックハッシュ値（図 1 2 中の「+ h a s h」）を銀行 A サーバに送信する（ステップ 2）。ブロックハッシュ値は、中央銀行サーバにおいて所定の間隔で更新され、銀行 A サーバに送信される。

30

【 0 0 8 7 】

銀行 A サーバにおいて、受信したブロックハッシュ値を本体データとともにデータベースに記憶して、部分データが欠落した電子通貨（すなわち、本体データ）を生成する。最後に、銀行 A サーバは、電子通貨の登録（生成）が完了した場合に、完了通知を銀行 A の担当者の端末に送信する。管理対象データである電子通貨は中央銀行サーバ登録時に、当該サーバ内のブロックチェーンへ永続的に管理登録されるため、送金リクエストは後日などの別タイミングとしても問題ない。

【 0 0 8 8 】

ここで、管理対象データである電子通貨の部分データ（例えば、先頭 3 0 バイト）を含む暗号化キーは、電子通貨の本体データ（例えば、先頭 3 1 バイト以降のデータ）を復元するための情報（以下、「復元情報」ともいう）である。つまり、復元情報（先頭 3 0 バイトを含む暗号化キーに相当）は、所定のバイトのデータ列であるとする、このデータを任意の人数分に分割して割符として使用することができる。復元情報である部分データを、任意の人数分に分割することを、ここでは割符化と呼ぶ。

40

【 0 0 8 9 】

割符化のアルゴリズム（処理手順）は、例えば、復元情報から 3 名分の割符を生成する場合に、まず、2 つのランダムな所定のバイトのデータ列を割符として生成する。次に、2 つの割符のデータ列を 2 進化し、最後に、2 進化された 2 つの割符のデータ列の総和の

50

下位1ビットが復元情報となるように、3つ目の割符のデータ列を生成する。例えば、3つの割符（割符1、割符2及び割符3）のデータ列が下記のような場合、各割符のデータ列の第1列目は、1，0，1なので、総和は10（2進数）となり、下位1ビットは0であり、第2列目は、1，1，1なので、総和は11となり、下位1ビットは1となる。

割符1	1	1	1	0	0	0	0	1	0	0	0	0	1	0	1	1	0	1	1	0	0	0	0	1
割符2	0	1	0	0	1	0	1	0	1	0	0	0	0	0	0	1	0	1	0	0	1	0	1	1
割符3	1	1	0	0	1	0	1	0	1	1	1	0	1	0	0	0	0	1	0	0	1	0	0	1

以上のような方法で、3つの割符を合わせることで、電子通貨を復元するための下記のような復元情報（暗号化キー）を生成することができる。

復元情報	0	1	1	0	0	0	0	1	0	1	1	0	0	0	1	0	0	1	1	0	0	0	1	0	1
------	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

このように、復元情報（暗号化キー）を割符として分割して管理することで、例えば、銀行Aから銀行Bへの送金について、中央銀行内において複数の承認者にそれぞれ割符を持たせ、それらの割符を用いることで、金融取引の認証を簡便に行うことができる。また、複数の承認者になりすまして、違法に金融取引を実行することも事実上不可能である。

【0090】

銀行Aサーバに接続された銀行Aの担当者（送信者）の端末から、銀行Bサーバに接続された銀行Bの担当者（受信者）の端末に管理対象データの一例である電子通貨を譲渡（送金）する場合、銀行Aの担当者（送信者）は、端末を用いて、例えばインターネット等の公衆回線を介して銀行Aサーバにログイン（サインイン）してアクセスし、銀行Aサーバは、銀行Aの担当者（送信者）の端末を用いたログインが成功した場合に、ログイン成功（OK）の応答を当該端末に送信するとともに、電子通貨等の目録を送信する。

20

【0091】

銀行Aの担当者（送信者）は、端末の画面上に表示される電子通貨等の目録から、電子通貨の譲渡のために必要な項目を選択して、送金先である銀行Bサーバ（コロニーサーバB）のアドレス等の識別情報（ID）と、担当者（受信者）のユーザIDを入力するとともに、送信のリクエストを銀行Aサーバに送信する。

【0092】

銀行Aサーバは、リクエストされた電子通貨の本体データを特定し、本体データのブロックハッシュ値と送金先の銀行Bの担当者のユーザIDとを含むリクエストを中央銀行サーバに送信する。中央銀行サーバは、受信したユーザID及びブロックハッシュ値を検証し、検証の結果正しければ、その旨の応答（OK）とともに送金先の銀行Bの担当者のメールアドレスを銀行Aサーバに送信し、銀行Aサーバは、電子通貨の送金を行うか否かの最終確認を銀行Aの担当者の端末に送信する。

30

【0093】

銀行Aの担当者は、送金の実行を承認する場合に、端末から承認する旨の応答を行うとともに最終的な送金のリクエストを銀行Aサーバに送信し、銀行Aサーバは、電子通貨の送金先の受信者のユーザIDを検証し、問題なければ、ダウンロードURLを生成し、送金先の銀行Bの担当者（受信者）のメールアドレスを中央銀行サーバにリクエストして、応答（OK）とともにメールアドレスを取得する。銀行Aサーバは、取得したメールアドレス宛（銀行Bの担当者の端末宛）にダウンロードURLを電子メールで通知する（ステップ3）。また、このとき、中央銀行サーバは電子通貨の先頭30バイトを含む部分データを銀行Bサーバに送信する。銀行Bサーバは、銀行Aの担当者からの電子通貨の送金がある旨の通知を、送金先の銀行Bの担当者の端末に通知する。

40

【0094】

銀行Bの担当者（受信者）は、端末において電子メールを確認し、ダウンロードURLを用いて、インターネット等の公衆回線を介して銀行Aサーバにログインして、ダウンロードを要求する（ステップ4）。銀行Aサーバは、要求に応じて、管理対象データである電子通貨の本体データ（31バイト以降のデータ）をダウンロード可能にし、銀行Bの担当者の端末は本体データをダウンロードすることができる（ステップ5）。

【0095】

50

また、銀行Bサーバは、銀行Aの担当者からの電子通貨の送金がある旨の通知を、送金先の担当者の端末に通知する。銀行Bの担当者は、端末から銀行Bサーバにアクセスし、銀行Bサーバは、中央銀行サーバから送られてきた電子通貨の先頭30バイトである部分データを含む暗号化キー（復元情報）を、専用回線を介して取得する（ステップ6）。銀行Bの担当者（受信者）の端末は、インターネット等の公衆回線を介して、暗号化キーをダウンロードすることができる（ステップ7）。そして、銀行Bの担当者の端末によって、暗号化キーに含まれる部分データと本体データとを結合することで、電子通貨が復元される。これにより、銀行Aから銀行Bへの送金が完了する。

【0096】

このように、銀行Bの担当者は、メール等の任意の通知を受け、コロニーサーバである銀行Bサーバへログインを行い、電子通貨の部分データを含む暗号化キーを取得することで、部分データが欠けている電子通貨を、完全な電子通貨へと復元（復号）を行うことができる。この際、銀行Bサーバでは復元処理を行わず、銀行Bの担当者の端末のWebブラウザ上で復元処理のリクエストを受け付け、端末において復元処理を実行することができる。本発明の一実施形態に係るデータ管理システムの本スキームにおいて、コロニーサーバ（銀行Bサーバ）上では、テンポラリーとしての実体は生成されないため、不正にアクセスされることはない。なお、各サーバ上ではごくわずかのキャッシュが残るため、取引工程に応じて適切なデータ抹消が行われるように構成することもできる。

【0097】

図13は、イベント参加者への特典付与に本発明に係るデータ管理システムを適用した例を示す図である。本発明のシステムは、予め決められた場所に行くことで、クーポン、ポイント等の特典が付与されるようなイベントにも、応用することができる。例えば、電車に乗車して予め決められた駅で降車することで、キャラクタのスタンプ等の特典を得ることができるスタンプラリーのようなイベントにも応用することができ、また、電車の車両の混雑度に応じて、乗客を混雑している車両から空いている車両に誘導し、実際に混んでいる車両から空いている車両に移動した乗客に特典を付与する仕組みにも応用することができる。さらに、予め指定されたイベント会場に来場することで特典を付与し、イベント会場において指示された特定場所に行くことで、特典を付与するような仕組みにも本発明のシステムを応用することができる。

【0098】

例えば、特典に相当する電子データ（以下、「特典データ」という）を受け取る側のスマートフォン等の携帯端末において、マイク等で音を聞き取り、特定の音の周波数に応答して、特典付与のリクエストを携帯端末からコロニーサーバに送信して、特典データの取得を実行することができる。特定の場所を識別できるのであれば、マイク等で音を聞き取る代わりに、携帯端末のGPS情報でもよい。

【0099】

また、電車の混雑緩和に応用した例として、乗車中に、電車内に流れる案内音声等の特定の音（音の周波数）に応じて、乗客の携帯端末に特典データを取得させるように、携帯端末に通知して特典データの取得を促すことができる。このような特典付与の仕組みにより、電車において混雑している車両から、空いている車両に乗客を移動させるために、空いている車両の車内で、特典データの取得を可能とする案内音声等の特定の音を流すようにすることで、乗客の移動を促すことができる。

【0100】

また、イベント会場の特定の場所で、特典データの取得を可能とする案内音声、広告等の特定の音を流すことで、イベント参加者を移動させることもできる。本システムをイベントに応用した場合、図13を参照して説明すると、イベント運営者（送信者）は、イベント運営サーバA（コロニーサーバA）に接続された端末を用いて、インターネット等の公衆回線を介して、イベント運営サーバAにログインしてアクセスし、イベント運営サーバAは、イベント運営者の端末を用いたログインが成功した場合に、ログイン成功（OK）の応答を当該端末に送信する。そして、イベント運営者は、端末上で、管理対象データ

の一例である特典データのアップロード又は特典データの生成リクエストを選択して、イベント運営サーバAに特典データをアップロードする、又は特典データの生成リクエストを送信する。イベント運営サーバAでは、アップロード又は生成された特典データを、圧縮、文字列化等の暗号化処理を行い、例えば、先頭から30バイトまでの部分データと31バイト以降の本体データとに分割して、先頭30バイトの部分データを、専用回線（クロードネットワーク）を介してセンターサーバに送信する（ステップ1）。

【0101】

センターサーバにおいて、先頭30バイトの部分データをブロックチェーンに追加するため1つのブロックを生成し、先頭30バイトの部分データの他に少なくとも管理対象データである特典データに関連する時間（例えば、アップロード日時、作成日時等）及び管理対象データである特典データに対応するファイル名の少なくとも一方を含めて暗号化を行い、部分データの他にファイル名及び時間（アップロード日時、作成日時等）の少なくとも一方を含む暗号化キーを生成する。センターサーバは、生成したブロックに暗号化キーを含めて、ブロックチェーンに当該ブロックを追加し、追加されたブロックのブロックハッシュ値（図13中の「+Hash」）をイベント運営サーバAに送信する（ステップ2）。ブロックハッシュ値は、センターサーバにおいて所定の間隔で更新され、イベント運営サーバAに送信される。

【0102】

イベント運営サーバAにおいて、受信したブロックハッシュ値を本体データとともにデータベースに記憶して、部分データが欠落した特典データ（すなわち、本体データ）を生成する。最後に、イベント運営サーバAは、特典データの登録（生成）が完了した場合に、完了通知をイベント運営者の端末に送信する。特典データはセンターサーバ登録時に、当該サーバ内のブロックチェーンへ永続的に管理登録されるため、特典付与のリクエストは後日などの別タイミングとしても問題ない。

【0103】

イベント運営サーバAに接続されたイベント運営者の端末から、イベント運営サーバB（コロニーサーバB）に接続されたイベント参加者（受信者）の端末に特典データを譲渡する（特典を付与する）場合、イベント参加者の携帯端末が、予め決められた場所に移動したことに起因して、すなわち、予め決められた場所に移動したことをトリガーとして、特典付与のために特典データの本体データ及び部分データを含む暗号化キーを、各サーバ（イベント運営サーバA及びB）に要求することができる（ステップ3からステップ7）。

【0104】

イベントの一例として、電車に乗って決められた駅に設置されたスタンプを集めるといったスタンプラリーの例を挙げる。イベント参加者が、電車に乗車して予め決められた駅で降車することで、キャラクタの電子的なスタンプやポイント等の特典を得ることができるように、降車駅の位置情報と実質的に一致する位置に、イベント参加者の携帯端末が移動したこと、又は、降車駅で流れる音声案内当の音の特定の周波数を携帯端末のマイク等で集音したことをトリガーとして、特典付与のリクエストを各サーバ（イベント運営サーバA及びB）に送信することができる。

【0105】

また、このようなイベントに限らず、同様の方法で、電車の混雑緩和にも応用することができる。例えば、電車において混雑している車両から、混雑していない車両に移動することを乗客に促すために、イベント運営サーバA（又はイベント運営サーバB）は、特定の車両（混雑していない車両）に移動することで、特典が付与される旨の通知を乗客の携帯端末に通知することができる。混雑していない車両の車内では、特典データの取得を可能とする案内音声等の音の特定の周波数を流し、乗客が混雑していない車両に移動すると、当該特定の周波数をその乗客の携帯端末のマイク等で集音したことをトリガーとして、特典付与のリクエストを各サーバに送信することができる（イベント運営サーバA及びB）。

【0106】

イベント参加者への特典付与の流れの各ステップ（ステップ３からステップ７）は、図１３に示されるように、イベント参加者が指定された場所（例えば、イベント会場）に移動して、イベント参加者の携帯端末のGPS等の位置情報がその場所を示したことをトリガーとして、又は指定された場所でスピーカ等から流れる音を携帯端末のマイク等で集音し、集音した音の特定の周波数をトリガーとして、特典データの本体データを要求する（ステップ３）。イベント運営サーバＡは、特典データの送信先のイベント参加者（受信者）のユーザＩＤを検証し、問題なければ、ダウンロードＵＲＬを生成し、送信先のイベント参加者（受信者）のメールアドレスをセンターサーバにリクエストして、応答（ＯＫ）とともにメールアドレスを取得する。イベント運営サーバＡは、取得したメールアドレス宛（イベント参加者の端末宛）にダウンロードＵＲＬを電子メールで通知する（ステップ４）。また、このとき、センターサーバは特典データの先頭３０バイトを含む部分データをイベント運営サーバＢに送信する。イベント運営サーバＢは、イベント運営者からの特典付与がある旨の通知を、送信先のイベント参加者の携帯端末に通知する。

【０１０７】

イベント参加者（受信者）は、携帯端末において電子メールを確認し、ダウンロードＵＲＬを用いて、インターネット等の公衆回線を介してイベント運営サーバＡにログインして、ダウンロードを要求する（ステップ５）。イベント運営サーバＡは、要求に応じて、管理対象データである特典データの本体データ（３１バイト以降のデータ）をダウンロード可能にし、イベント参加者の携帯端末は本体データをダウンロードすることができる（ステップ６）。

【０１０８】

また、イベント運営サーバＢは、イベント運営者からの特典付与がある旨の通知を、送信先のイベント参加者の携帯端末に通知する。イベント参加者は、携帯端末からイベント運営サーバＢにアクセスし、イベント運営サーバＢは、センターサーバから送られてきた特典データの先頭３０バイトである部分データを含む暗号化キー（復元情報）を、専用回線を介して取得する（ステップ８）。イベント参加者の携帯端末は、インターネット等の公衆回線を介して、暗号化キーをダウンロードすることができる（ステップ９）。そして、イベント参加者の携帯端末によって、暗号化キーに含まれる部分データと本体データとを結合することで、特典データが復元されることで、イベント参加者に特典付与が行われる。これにより、イベント運営者からイベントへの特典付与が完了する。

【０１０９】

このように、イベント参加者は、メール等の任意の通知を受け、コロニーサーバであるイベント運営サーバＢへログインを行い、特典データの部分データを含む暗号化キーを取得することで、部分データが欠けている特典データを、完全な特典データへと復元（復号）を行うことができる。この際、イベント運営サーバＢでは復元処理を行わず、イベント参加者のWebブラウザ上で復元処理のリクエストを受け付け、携帯端末において復元処理を実行することができる。本発明の一実施形態に係るデータ管理システムの本スキームにおいて、コロニーサーバ（イベント運営サーバＢ）上では、テンポラリとしての実体は生成されないため、不正にアクセスされることはない。なお、各サーバ上ではごくわずかのキャッシュが残るため、取引工程に応じて適切なデータ抹消が行われるように構成することもできる。

【０１１０】

図１３に示した１つの実施例では、イベント参加者への特典付与に、図１０及び図１１に示したセンターサーバに接続された２つのコロニーサーバを用いた管理対象データの譲渡（他コロニーの場合）の方法を応用しているが、これに限定されるものではなく、図９に示したセンターサーバに接続された１つのコロニーサーバを用いた管理対象データの譲渡（自コロニーの場合）の方法を応用してもよい。

【０１１１】

また、本発明のデータ管理システムは、図１２及び図１３に示した実施例に限定されるものではなく、音楽、映画、書籍等の著作物の電子データの転送にも使用することができ

、映画や音楽配信のプラットフォームとして応用することができる。

【0112】

本発明は、図1に示した一実施形態に係るデータ管理システムにおいて、上述したとおり、コロニーサーバ20と情報処理端末30との間の通信は、インターネット等のオープンなネットワークが利用される。一方で、携帯電話などの無線局の急速な増加や無線通信の高速化に伴い、周波数の需要が増大しており、携帯電話等の通信量は更に増大となることが予想される。このため、電波の割当てや周波数の再編を行い、周波数の逼迫状況を緩和し、新たな周波数需要に的確に対応することが求められている。1つの対応策となり得る第5世代移動通信システム(5G)は、超高速、低遅延、多数接続等がシステム要件とされ、その実現に向けた研究開発が世界各国で進められている。特に、従来の移動通信システムと異なり、IoTの基盤となることが期待されており、膨大な数の端末が基地局に接続されるとともに、多種多様なサービスが提供されることが見込まれている。

10

【0113】

このような状況下において、本発明は、第5世代移動通信システム(5G)に基づいた通信を行う場合に、携帯電話等での電波(周波数)の有効利用に寄与することができる。例えば、図12及び図13に示した実施例のように、本発明のデータ管理システムは、管理対象データを部分データと本体データとに分割して、部分データを暗号化した暗号化キーをセンターサーバで管理し、本体データをコロニーサーバで管理する。コロニーサーバと情報処理端末との通信は、5Gを利用したインターネット回線を介して行うことができるが、部分データを含む暗号化キーは、そもそも僅かなサイズ(例えば、管理対象データの先頭30バイト)となので、通信回線をひっぱくするものでなく、通信回線をひっぱくする可能性がある大きなサイズの本体データは、転送先の情報処理端末への送信が急ぎでない場合には、通信回線が空いているときに、自動的に、コロニーサーバから本体データをダウンロードするようにしてもよい。これにより、本発明は電波(周波数)の有効理由に寄与することができる。

20

【0114】

図14は、管理対象データを暗号化キーと本体データとに分割する処理の流れを示すデータ管理システム全体としてのフローチャートである。機密情報、電子為替、付記電文、暗号資産、仮想通貨、電子通貨、有価証券等の電子的なデータを扱う場合に、情報処理端末30は、当該電子的なデータを管理対象データとしてコロニーサーバ20にアップロードして(ステップS501)、コロニーサーバ20において管理対象データの暗号化を行う(ステップS502)。例えば、AES暗号化(AES-256-CBC)を用いることができる。また、管理対象データの暗号化については、図4及び図5に示すように圧縮、MIMEを用いた方法でもよく、その他の暗号化方法でもよい。

30

【0115】

コロニーサーバ20は、暗号化した管理対象データを、所定のサイズの部分データと、当該部分データ以外の残りのデータを含む本体データとに分離する(ステップS503)。例えば、部分データを暗号化した管理対象データの先頭から30バイトまでのデータとし、本体データを31バイト以降から最後までまでのデータとすることができるが、これに限定されるものではない。

40

【0116】

センターサーバ10側では、部分データ(例えば、先頭30バイトのデータ)を保存するためのブロックチェーンの1ブロックを生成し(ステップS504)、部分データを含む暗号化キーを生成し(ステップS505)、生成された現在のブロックハッシュ値をコロニーサーバ20に通知する(ステップS506)。コロニーサーバ20側では、データベース(ハッシュ情報記憶部271)にハッシュ値を格納する(ステップS507)。データ管理システムで生成される部分データを含むブロックチェーン及び本体データの詳細は、図15から図16に示す。

【0117】

図15は、センターサーバからアクセス可能なブロックチェーンにおける1ブロックと

50

、コロニーサーバからアクセス可能な本体データとの関係を示す。また、図16は、コロニーサーバにおいて独立して記憶される本体データの概要を示す。ブロックチェーン100の概要は、図6に示したが、図15においてより具体的に示すと、センターサーバ10のデータベース（暗号化キー記憶部173）に記憶されるブロックチェーン100の1つのブロック101Aには、例えば、少なくとも前のブロックのハッシュ値102Aと、現在のブロックのハッシュ値104Aと、暗号化キー105Aとを含む。ハッシュ値102A及び104Aは、例えば64バイトのデータとすることができる。現在のブロックのハッシュ値104Aは、センターサーバ10によって、所定の間隔で新たなハッシュ値に更新される。暗号化キー105は、更新されることなく固定されたデータである。暗号化キー105は、例えば、管理対象データのファイル名と、取引又はファイル作成等の日時と、先頭から30バイトのデータとを含み、それらを暗号化したデータである。なお、ブロック101Aには、ブロック101Aを識別するための情報として4バイトのファイルIDを含めることができる。

10

【0118】

図15及び図16を参照すると、コロニーサーバ20のデータベース（本体データ記憶部272）には、データブロック群200が格納される。データブロック群200に含まれる複数のデータブロック201Aから201Dは、ブロックチェーンを構成するものではなく互いに独立して記憶される。

【0119】

1つのデータブロック201Aには、例えば、少なくとも現在のブロックのハッシュ値204Aと、本体データ205Aとを含む。ハッシュ値204Aは、例えば64バイトのデータとすることができる。本体データ205Aは、例えば、管理対象データの31バイト以降のデータであり、必要に応じて、管理対象データのファイル名、利用者のユーザIDを適宜含めることができる。なお、データブロック201Aには、データブロック201Aを識別するための情報として4バイトのファイルIDを含めることができる。

20

【0120】

センターサーバ10は、現在のブロックのハッシュ値104Aを所定の間隔で更新して、コロニーサーバ20に通知する。所定の間隔は、24時間以下で1時間、2時間、3時間、4時間、5時間、6時間の間隔としても良いし、24時間よりも大きい間隔にしてもよい。コロニーサーバ20は、センターサーバ10からの通知を受け取り、ハッシュ値104Aと同じ値に、ハッシュ値204Aに更新することで、あたかも、ブロックチェーンにおいて暗号化キー105Aを含むブロックのハッシュ値104Aと、本体データ205Aを含むハッシュ値204Aとがリンクして更新しているように動作する。このような動作を本発明においては、代謝とも表現する。つまり、ハッシュ値104Aとハッシュ値204Aとが、所定の間隔で更新することを、リンクしながら代謝ともいう。

30

【0121】

このように、本発明に係るデータ管理システムは、管理対象データを部分データと本体データとに分けて管理し、センターサーバ10の管理下にあるブロックチェーン100における1ブロックに暗号化キーとして記憶した部分データに対応するハッシュ値を、所定の間隔で更新するとともに、コロニーサーバ20における本体データに対応するハッシュ値を、部分データに対応するハッシュ値と同じ値に更新させること（つまり、リンクしながら代謝させること）で、不正アクセス等によってコロニーサーバ20から本体データが流出した場合であっても、不正に流出した本体データと対となる部分データを含む暗号化キーのハッシュ値は所定の間隔で更新されるため、当該本体データのハッシュ値に一致するハッシュ値を含む暗号化キーは存在しなくなり、不正に流出した本体データを解析しても、管理対象データを復元するために必要な暗号化キーにたどり着くことは困難となり、管理対象データを復元することは実質的に不可能にすることができる。

40

【0122】

本発明の一実施形態に係るデータ管理システムは、機密情報、電子為替、付記電文、暗号資産、仮想通貨、電子通貨、有価証券等の電子データを管理対象データとすることがで

50

き、取り扱う電子データの内容には実質的な制限がない。本発明に係るデータ管理システムにおける送信側では、送信するデータは種類及びサイズに可能な限り制限が無く、センターサーバで管理するデータは可能な限り少容量であり、また、送信するデータは本体データ（一部欠落させたデータ）と部分データ（欠落部分）とに分割され、それぞれ別のネットワークを利用して送受信され、インターネット等の公衆回線を介して送受信中のデータは本体データ（部分データを除いた管理対象データ）であり、本体データをハッキングされても、一部欠落させたデータであるから実害はないといった特徴を有する。一方、本発明に係るデータ管理システムにおける受信側では、受信する部分データを含む暗号化キーは可能な限り少容量であり、受信予定の本体データを事前にダウンロードすることができ、本体データとは別のネットワークを介して受信した暗号化キーを用いて本体データから管理対象データを端末で復元することができるため、送受信中の本体データ又は部分データを含む暗号化キーを、別々にハッキングされても実害はないといった特徴を有する。

10

【0123】

図17は、センターサーバにおいてブロックチェーンに新たに暗号化キーを含むブロックを接続する処理の流れを示すフローチャートである。図17に示すフローチャートは、例えば、図7に示したように、情報処理端末30からコロニーサーバ20を介してセンターサーバ10に管理対象データの1つのである電子通貨データを登録する際の処理の流れに対応する。

【0124】

コロニーサーバ20は、情報処理端末30等から、管理対象データの登録や生成等、管理対象データへのアクセスがあると（ステップS601）、センターサーバ10にその旨を通知し（ステップS602）、センターサーバ10ではブロックチェーン100のブロックの検証が行われる（ステップS602）。センターサーバ10は、ブロックチェーン100における複数のブロックの各々について有効か無効かを示す有効フラグを各ブロックに関連付けて記憶する。ブロックチェーン100の現在のブロック（例えば、末尾のブロック）に対応する有効フラグをチェックして（ステップ、S604）、有効でない場合（ステップS604のNO）には、エラーメッセージ等の通知処理を実行する（ステップS612）。

20

【0125】

ブロックチェーン100の現在のブロック（末尾のブロック）に対応する有効フラグが有効を示す場合（例えば、ステップS604のYES）には、センターサーバ10において、ブロックチェーン100に新たに追加するためのブロックを生成する（ステップS605）。そして、センターサーバ10は、ブロックチェーン100に新たに生成したブロック（新ブロック）を接続するために、新ブロックに管理対象データの部分データ（例えば、先頭から30バイト）を格納する（ステップS606）。さらに、センターサーバ10は、いままで有効フラグが有効であったブロック（旧ブロック）の有効フラグを、無効を示す値に変更して（ステップS607）、ブロックチェーン100に新ブロックを追加する（ステップS608）。具体的には、ブロックチェーン100において、旧ブロックに新ブロックを接続する。

30

【0126】

その後、センターサーバ10は、管理対象データの部分データ（例えば、先頭30バイトのデータ）の追加が完了した旨とともに、新ブロックのブロックハッシュ値を、コロニーサーバ20に通知する（ステップS609）。コロニーサーバ20では、管理対象データの本体データ（例えば、31バイト以降のデータ）に対応するハッシュ値を、センターサーバ10から通知された新ブロックのハッシュ値に更新する（ステップS610）。コロニーサーバ20は、センターサーバ10への電子通貨の登録が成功したか否かをチェックし（ステップS610）、成功した場合（ステップS611のYES）には処理を終了し、失敗した場合（ステップS611のNO）にはエラーメッセージ等の通知処理を実行する（ステップS612）。

40

【0127】

50

図18は、センターサーバの管理下にあるブロックチェーンの構成を示す。ブロックチェーン100における1つのブロック101Aは、基本的には、図17に示す構成と同様であり、直前のブロックのハッシュ値102Aと、現在のブロックのハッシュ値104Aと、暗号化キー105Aとを含む。その他のブロック101B、101Cについても同様である。ブロック101A、101B及び101Cの各々には、ナンス103A、103B及び103Cが含まれ、例えば、プルーフオブワークと同様の手法により、次のブロックをつなげるためのハッシュ値の計算に用いることができる。センターサーバ10が1台の場合には、ブロックチェーンの検証を省略できるため、ナンスを使用する必要がないが、本発明の別の実施形態として、データ管理システムが複数のセンターサーバ10を備え、ブロックチェーン100が複数のセンターサーバ10の管理下にある場合には、各センターサーバ10において、ブロックチェーンの検証を行い、新たなブロックを追加するために、ナンスを使用することができる。

【0128】

ブロックチェーン100において、ブロック101Aとブロック101Bとは、ハッシュ値104Aとハッシュ値102Bとが同じ値であることで結合され、ブロック101Bとブロック101Cとは、ハッシュ値104Bとハッシュ値102Cとが同じ値であることで結合される。

【0129】

図19は、センターサーバのデータベースに記憶される各種情報の概要を示す。センターサーバ10のデータベースとして、例えば、図2に示すように、コロニー情報を記憶するためのコロニー情報記憶部171と、ユーザ情報を記憶するためのユーザ情報記憶部172と、図18に示したようなブロックチェーン100を記憶するための暗号化キー記憶部173とを備える。図19(a)に示すコロニー情報は、例えば、コロニー情報記憶部171に記憶される。コロニー情報としては、例えば、センターサーバ10に接続される1以上のコロニーサーバ20のコロニーサーバIDと、コロニーサーバ20に情報処理端末30からログインする利用者のユーザIDと、コロニーサーバID及びユーザIDが有効(TRUE)であるか、いずれか一方が無効(FALSE)であるかを示す有効フラグとを含む。例えば、センターサーバ10は、コロニー情報記憶部171に記憶されたコロニー情報を参照して、有効フラグに基づいて有効なコロニーサーバID及びユーザIDを特定することができる。

【0130】

図19(b)に示すユーザ情報は、例えば、ユーザ情報記憶部172に記憶される。ユーザ情報としては、例えば、本発明に係るデータ管理システムの利用者のユーザIDと、メールアドレスと、ユーザID及びメールアドレスが有効(TRUE)であるか、いずれか一方が無効(FALSE)であるかを示す有効フラグとを含む。例えば、センターサーバ10は、ユーザ情報記憶部172に記憶されたユーザ情報を参照して、有効フラグに基づいて有効なユーザID及びメールアドレスを特定することができる。なお、本実施形態では、コロニー情報記憶部171に記憶されるコロニー情報及びユーザ情報記憶部172に記憶されるユーザ情報は、暗号化キー記憶部173に記憶されるブロックチェーン100に関連するデータとは独立して、別のデータとして記憶される。

【0131】

図20は、コロニーサーバのデータベースに記憶される情報の概要を示す。コロニーサーバ20のデータベースとして、例えば、図3に示すように、ハッシュ情報を記憶するためのハッシュ情報記憶部271と、図16に示したような本体データのデータブロック群200を記憶するための本体データ記憶部272とを備える。図20に示すハッシュ情報は、例えば、ハッシュ情報記憶部271に記憶される。ハッシュ情報としては、例えば、ユーザIDと、本体データを保存するデータブロックのブロックハッシュ(例えば、64バイトのデータ)と、管理対象データの取引日時(年/月/日/時:分:秒(YYYY/MM/DD/HH:MM:SS))と、少なくともブロックハッシュ値が有効(TRUE)であるか、無効(FALSE)であるかを示す有効フラグとを含む。例えば、コロニーサーバ20は、ハッシ

10

20

30

40

50

ュ情報記憶部 271 に記憶されたハッシュ情報を参照して、有効フラグに基づいて有効なハッシュ値か否かを判断することができる。

【0132】

センターサーバ10には、ブロックチェーンの改ざんを監視するための監視ボットと、ブロックチェーンを修復するための修復ボットとを備えることができる。ボットとは、一定のタスクや処理を自動化するためのアプリケーションやプログラムのことである。図21は、例示的に、複数のブロック301Aから301Dが連結されたブロックチェーン300に対する、監視ボット及び修復ボットの処理の概要を示す。つまり、図21は、ブロックチェーンにおいて改ざんを検出した際の各ブロックの凍結及び修復の処理の概要を示す。図21にブロックチェーンの一例として示したブロックチェーン300は、図18に示したブロックチェーン100と基本的には同じ構造を有するブロックチェーンである。

10

【0133】

監視ボットは、センターサーバ10の管理下にあるブロックチェーン300の常時監視を行うことができる。例えば、監視ボットが、ブロックチェーン300において、ブロック301Bに改ざん（不正な改変等）を見つけた場合には、センターサーバ10又は監視ボットは、例えば、ブロック301Bに対応するフラグを無効にすることでブロック301Bを無効化するとともに、ブロック301B以降のブロック、つまり、ブロック301Bに連結されたブロック301C、ブロック301Cに連結されたブロック301Dも同様に無効化する。このようにブロックを無効化することを、ここではブロックを凍結するともいう。

20

【0134】

不正改ざんが見つかったことに応じて、不正改ざんブロック以降のブロックを凍結した後、修復ボットによって、ブロックチェーン300の修復処理が実行される。修復ボットは、センターサーバ10の管理下にあるブロックチェーン300とは独立して管理された帳簿データベース（図示せず）を参照して、正しい取引記録に基づいて、改ざんされたブロック301B以降のブロックを復元するために、ブロックの修正を行う。例えば、銀行等の金融機関において、センターサーバ10を運用する場合には、センターサーバ10とは、完全に独立したサーバの帳簿データベースによって管理対象データの取引記録が格納されている。この帳簿データベースを参照することで、センターサーバ10の管理下にあるブロックチェーン300を復元することができる。

30

【0135】

図21に示す修復処理の例では、修復ボットにより、帳簿データベースを参照して修復されたブロック302Bが生成され、ブロック301Aのハッシュ値を書き換えて、ブロック302Bのハッシュ値をブロック301Aのハッシュ値と同じにすることで、ブロック301Aに、ブロック302Bを結合する。同様に、ブロック302Cは、修復ボットにより、帳簿データベースを参照して修復されたブロックであり、ブロック302Cのハッシュ値をブロック302Bのハッシュ値と同じにすることで、ブロック302Bに、ブロック302Cを結合する。ブロック302Dについても同様である。

【0136】

修正ボットの修正中に、新しい取引があった場合、例えば、ブロック302Bが修正された後に、新たな取引があると、ブロック302Bとブロック302Cとの間に、新たなブロック303Aが挟み込まれる。つまり、ブロック302Bが修正された後に、新たな取引記録を格納するブロック303Aが生成されて、ブロック303Aのハッシュ値を、修正されたブロック302Bのハッシュ値と同じにすることで、ブロック302Bにブロック303Aが連結される。同様に、ブロック303Aにブロック302Cが連結され、ブロック302Cにブロック302Dが連結される。

40

【0137】

図22は、ブロックチェーンを監視して改ざんを検出した際の処理の流れを示すフローチャートである。監視ボットは、例えば、センターサーバ10に少なくとも一時的に常駐して、ブロックチェーン（例えば、ブロックチェーン100）を常時監視する処理を実行

50

する（ステップS701）。監視によってブロックチェーンにおけるブロックに改ざん（不正な改変等）が見つかったか否かをチェックし（ステップS702）、見つからない場合（ステップS702のNO）には、監視処理（ステップS701）を続行する。改ざんが見つかった場合（ステップS702のYES）には、図21に示したように、監視ボット又はセンターサーバ10が、不正に改ざんされたブロックを凍結する処理を実行する（ステップS703）。そして、ブロックチェーンの構成をチェックした（ステップS704）後、改ざんされたブロック以降に連結されたブロックも同様に凍結処理を実行する（ステップS705）。

【0138】

ブロックチェーンの改ざんブロックを凍結した後、センターサーバ10は、管理者にメールを送信し（ステップS706）、メール送信が成功したか否かをチェックし（ステップS707）、失敗した場合（ステップS707のNO）には、メールの送信を再度実行する（ステップS706）。メールの送信が成功した場合（ステップS707のYES）には、ブロックチェーンの凍結の影響がおよぶコロニーサーバ20の各々の管理者にメールを送信する（ステップS708）。

【0139】

各コロニーサーバ20の管理者へのメールの送信が成功したか否かをチェックし（ステップS709）、成功した場合（ステップS709のYES）には、処理を終了する。メール送信が失敗した場合（ステップS709のNO）には、センターサーバ10の管理者にメールを送信してその旨を連絡して（ステップS710）、メール送信が失敗したコロニーサーバの管理者へのメール送信をリトライする（ステップS708）。

【0140】

図23は、ブロックチェーンにおけるブロックを凍結する処理の流れを示すフローチャートである。図22に示すフローチャートとは別の実施形態である。利用者が手動でブロックチェーンのブロックに対応するデータを取得するか、又はボットの代謝処理（更新されたハッシュ値を通知する処理）等の際にブロックチェーンのブロックに対応するデータにアクセスする（ステップS801）。当該データに対応する保存されたファイルのハッシュ値を比較して（ステップS802）、改ざんされていないか否かをチェックする（ステップS803）。改ざんされていない場合（ステップS803のYES）には、正常に処理を終了し、改ざんされている場合（ステップS803のNO）には、センターサーバ10から利用者（及び管理者）のメールアドレスを取得し（ステップS804）、利用者及びコロニーサーバ管理者宛にメール送信を行い、メール送信が成功したか否かをチェックする（ステップS805）。メール送信が成功した場合（ステップS805のYES）には、該当するデータを凍結する（つまり、そのデータが無効であることを示すために、そのデータに関連する有効または無効を示すフラグをオフする）（ステップS806）。メール送信が失敗した場合（ステップS805のNO）には、再度メールの送信を行ってメールの送信状況をチェックする（ステップS805）。

【0141】

図24は、ブロックチェーンを修復する処理の流れを示すフローチャートである。ブロックチェーンの凍結処理後に、センターサーバ10において、コロニーサーバ20から管理対象データの部分データとともに新たにブロックを追加する指示を受け（ステップS901）、ブロックチェーンの末尾が凍結状態か否かをチェックする（ステップS902）。チェーンの末尾が凍結状態にない場合（ステップS902のNO）には、ステップS905に進む。ブロックチェーンの末尾が凍結状態にある場合（ステップS902のYES）には、ブロックチェーンを辿り凍結されていないブロックを探す（ステップS903）。凍結されていないブロックを見つけると、凍結されていないブロックに新たなブロックを連結することで、チェーンを分岐させる（ステップS904）。そして、コロニーサーバ20から受け取った部分データを含む暗号化キーを生成して（ステップS905）、暗号化キーを格納してブロックチェーンの生成を行う（ステップS906）。最後に、センターサーバ10は、図7に示す管理対象データの登録の処理と同様に、コロニーサーバ2

10

20

30

40

50

0 に生成したブロックのハッシュ値を通知する（ステップ S 9 0 7）

【産業上の利用可能性】

【0 1 4 2】

本発明に係るデータ管理システム等は、インターネット等のネットワークを介して暗号資産、仮想通貨、電子通貨、有価証券等の管理対象データを、クラウドを構成する複数のサーバで安全に保存し、利用者が使用する情報処理端末からの要求に応じて、当該端末に管理対象データを適宜取得させるような電子商取引などに利用可能である。

【符号の説明】

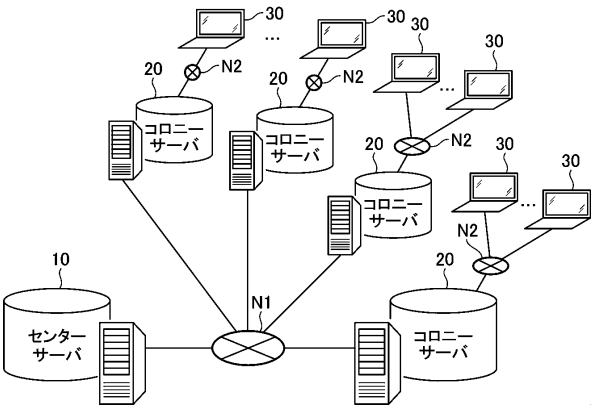
【0 1 4 3】

1 0	: センターサーバ	10
1 1	: C P U	
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	: コロニーサーバ	
2 0 A	: コロニーサーバ	20
2 0 B	: コロニーサーバ	
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	: 情報処理端末	30
3 0 X	: 情報処理端末	
3 0 Y	: 情報処理端末	
1 0 0	: ブロックチェーン	
1 0 1 A	: ブロック	
1 0 1 B	: ブロック	
1 0 1 C	: ブロック	
1 0 2 A	: ハッシュ値	
1 0 2 B	: ハッシュ値	
1 0 2 C	: ハッシュ値	
1 0 3 A	: ナンス	40
1 0 3 B	: ナンス	
1 0 4 A	: ハッシュ値	
1 0 4 B	: ハッシュ値	
1 0 5	: 暗号化キー	
1 0 5 A	: 暗号化キー	
1 1 1	: 部分データ管理部	
1 1 2	: ハッシュ通知部	
1 1 3	: 暗号化キー取得部	
1 7 1	: コロニー情報記憶部	
1 7 2	: ユーザ情報記憶部	50

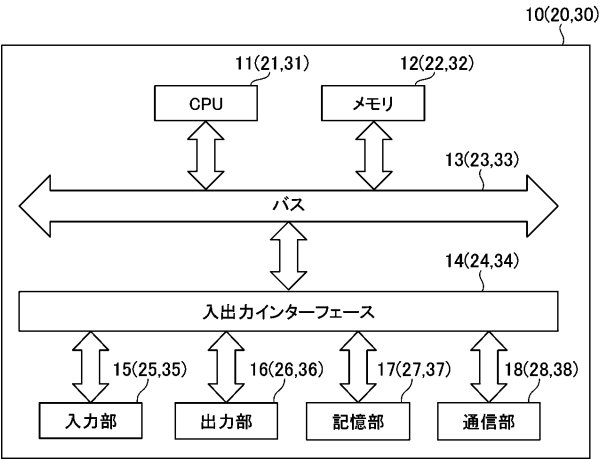
- 1 7 3 : 暗号化キー記憶部
- 2 0 0 : データブロック群
- 2 0 1 A : データブロック
- 2 0 4 A : ハッシュ値
- 2 0 5 A : 本体データ
- 2 1 1 : 分割送信部
- 2 1 2 : 本体データ管理部
- 2 1 3 : ハッシュ更新部
- 2 7 1 : ハッシュ情報記憶部
- 2 7 2 : 本体データ記憶部
- 3 0 0 : ブロックチェーン
- N 1 : ネットワーク
- N 2 : ネットワーク
- X : 利用者
- Y : 利用者

【図面】

【図 1】



【図 2】



10

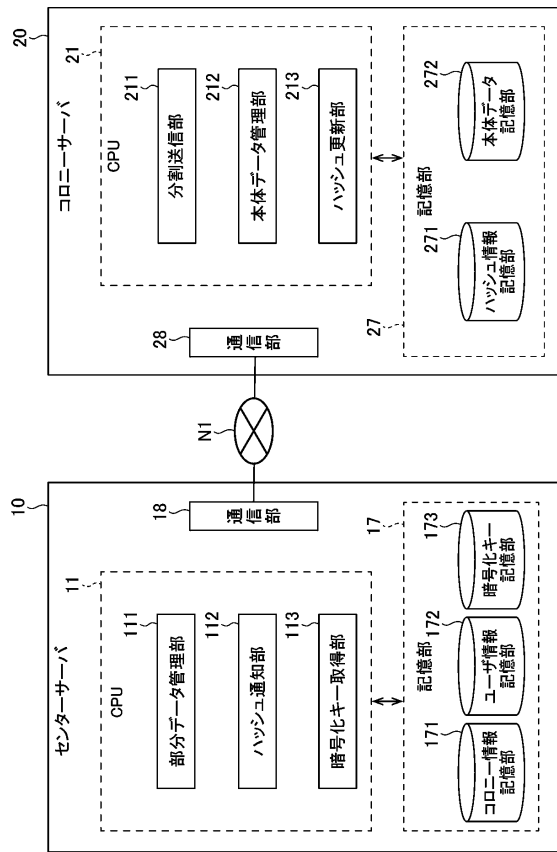
20

30

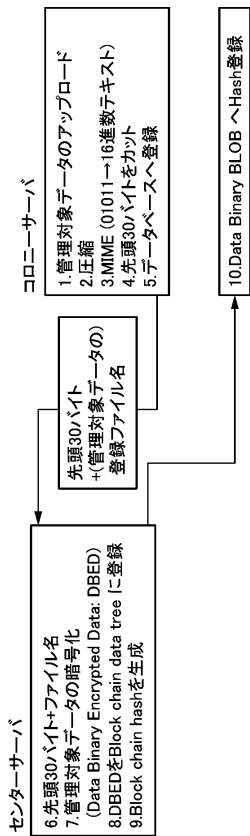
40

50

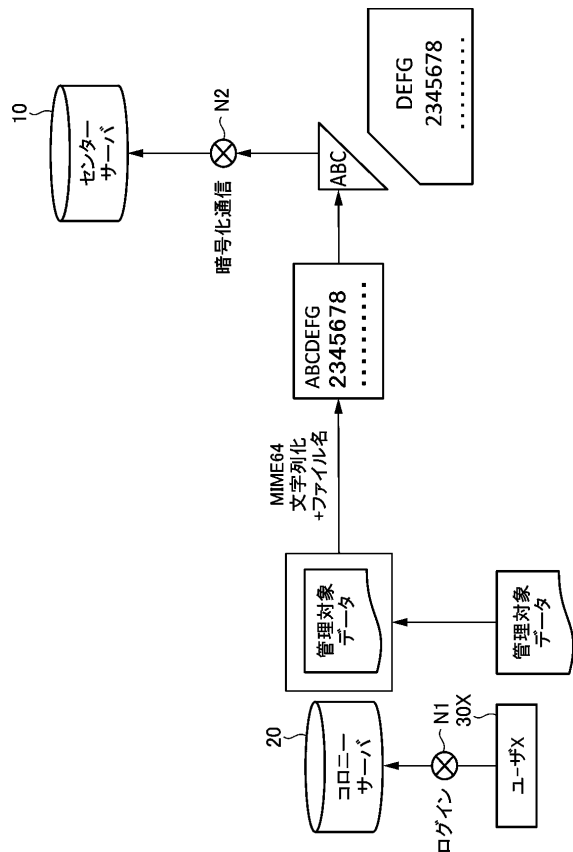
【図 3】



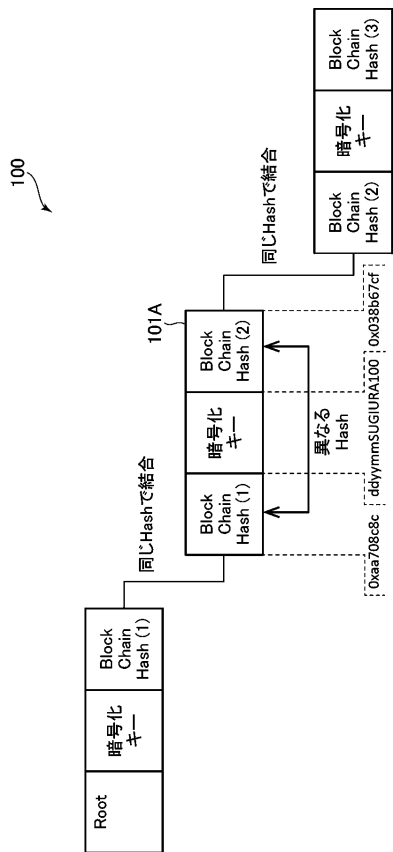
【図 4】



【図 5】



【図 6】



10

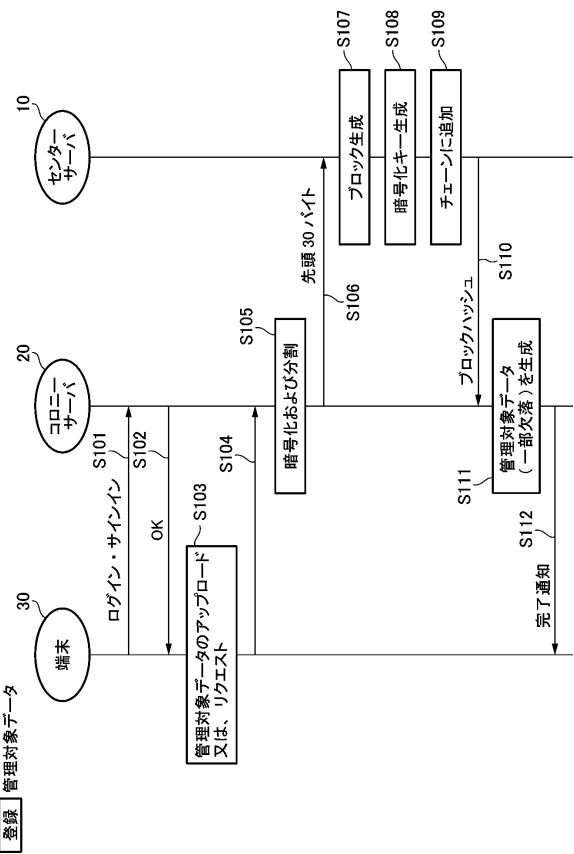
20

30

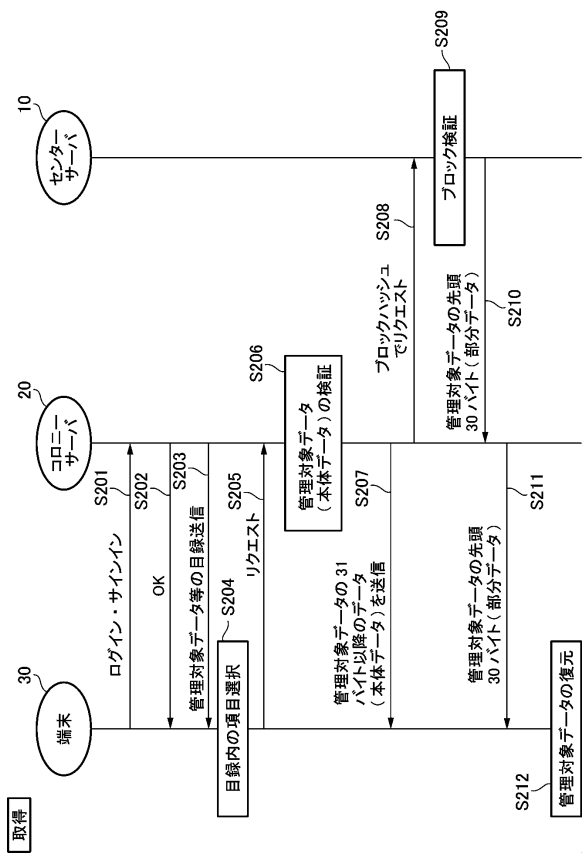
40

50

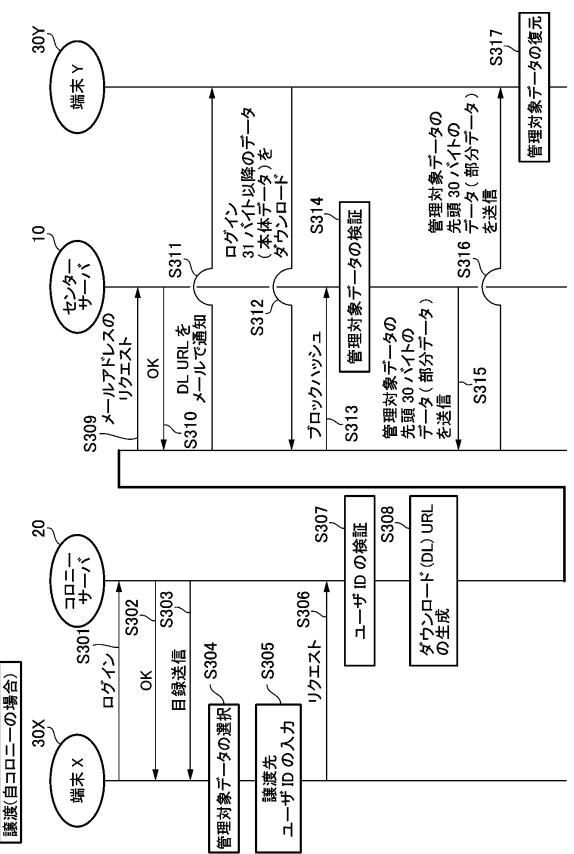
【図 7】



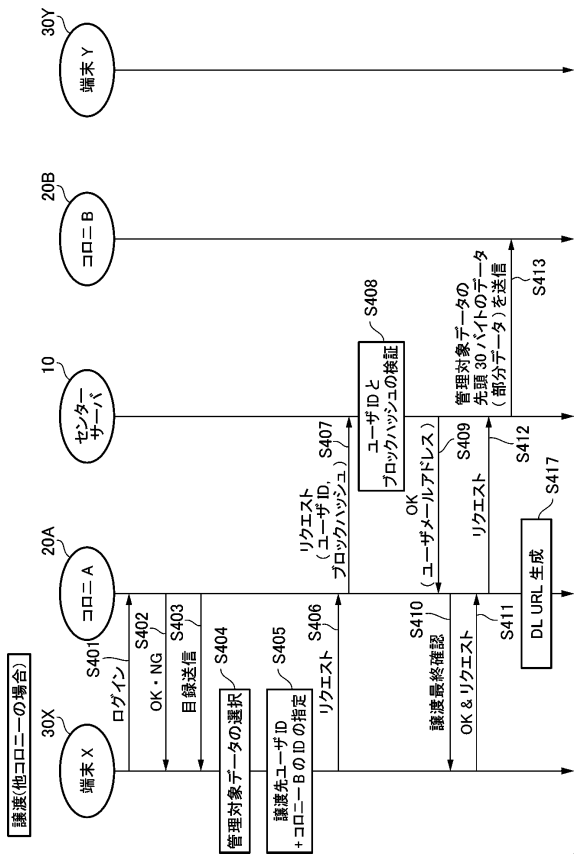
【図 8】



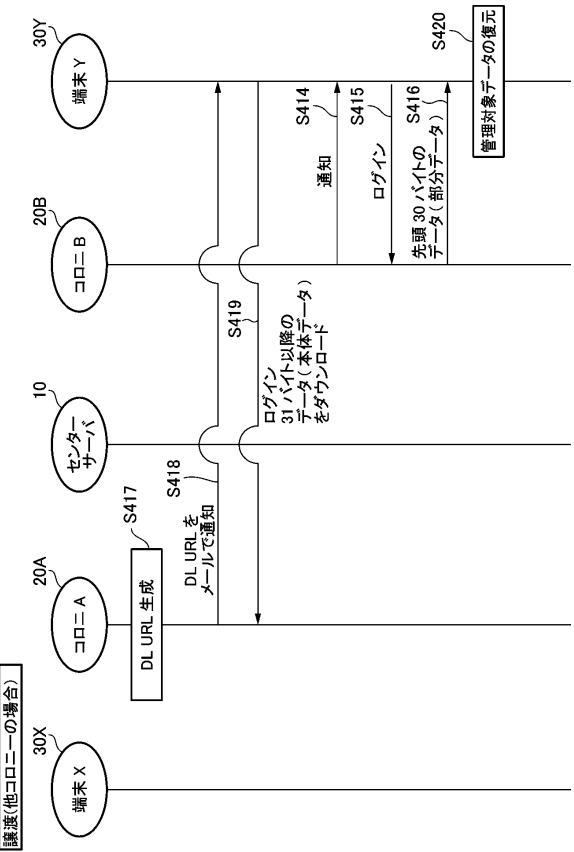
【図 9】



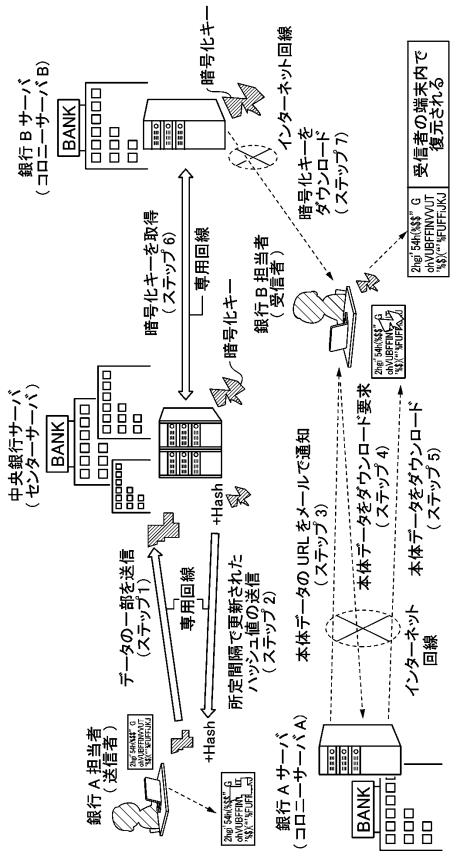
【図 10】



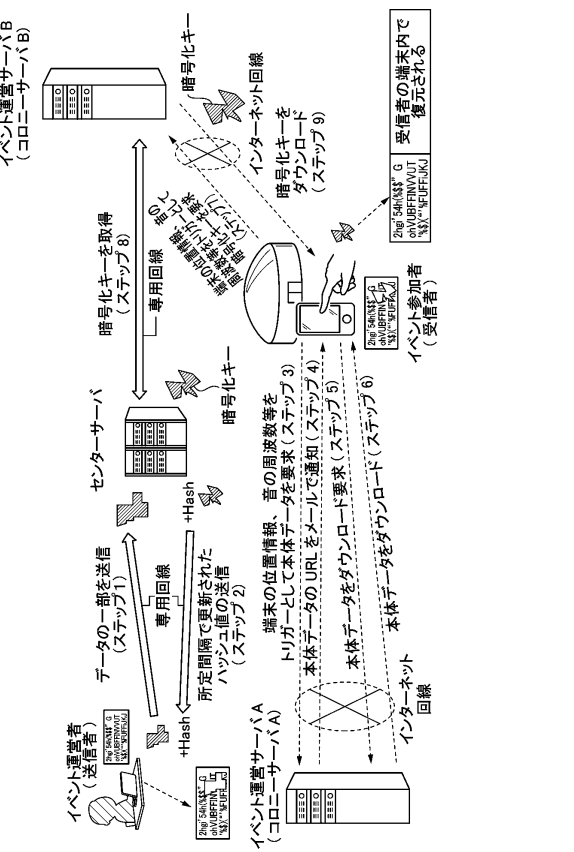
【図 1 1】



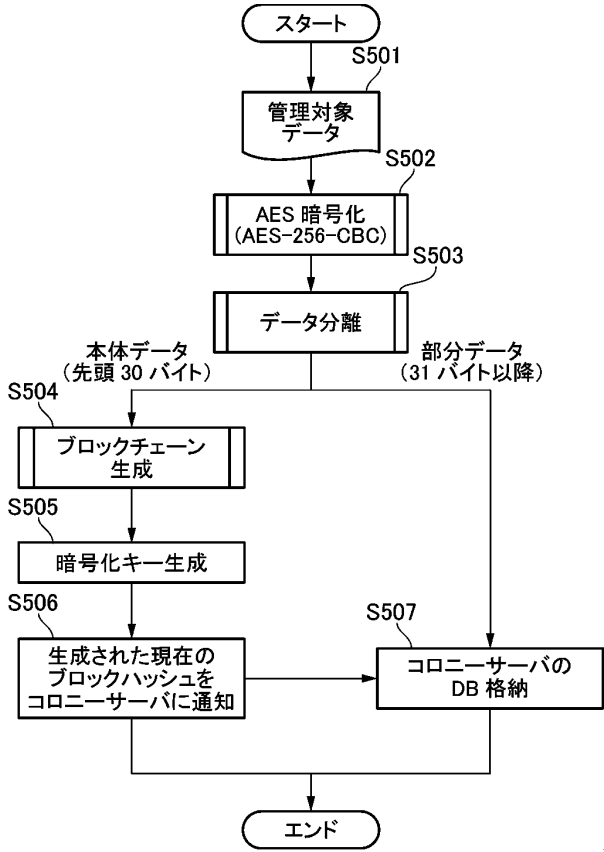
【図 1 2】



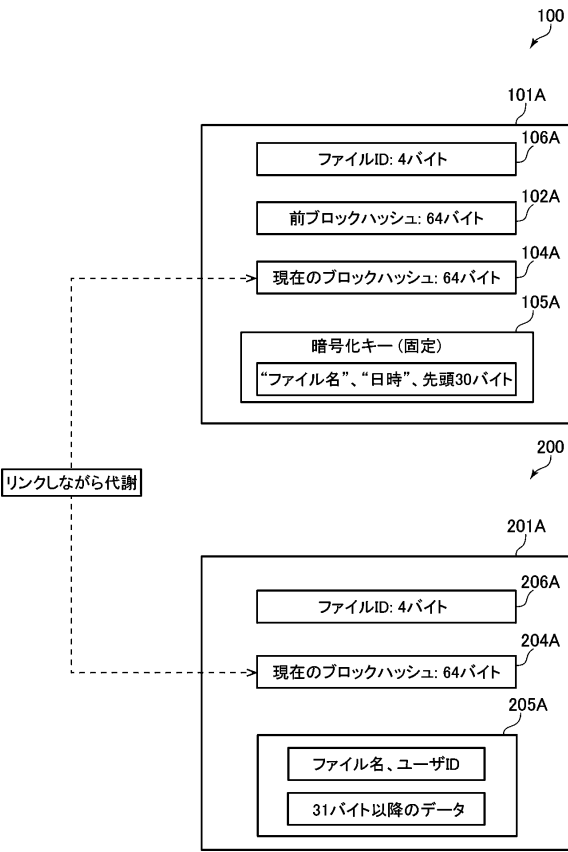
【図 1 3】



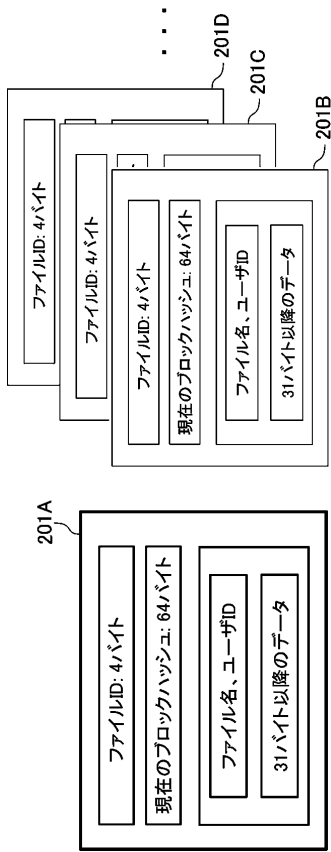
【図 1 4】



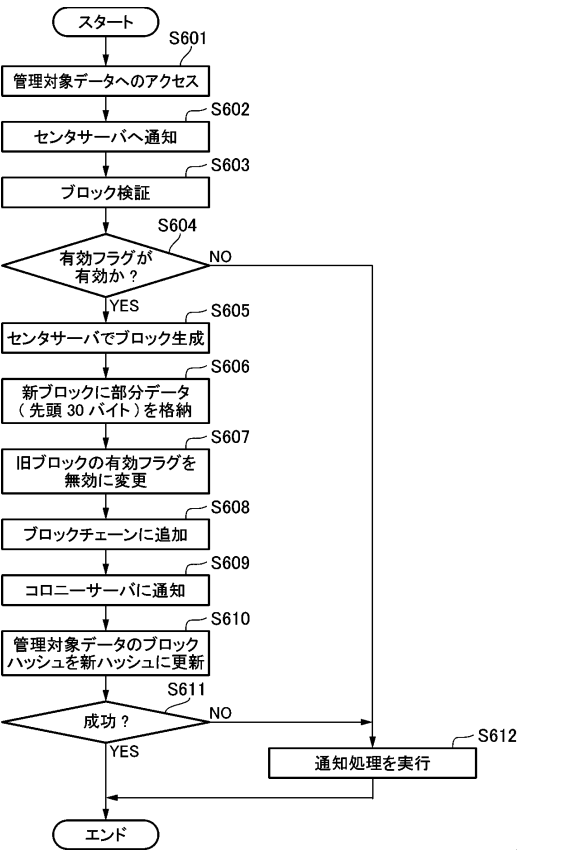
【図 15】



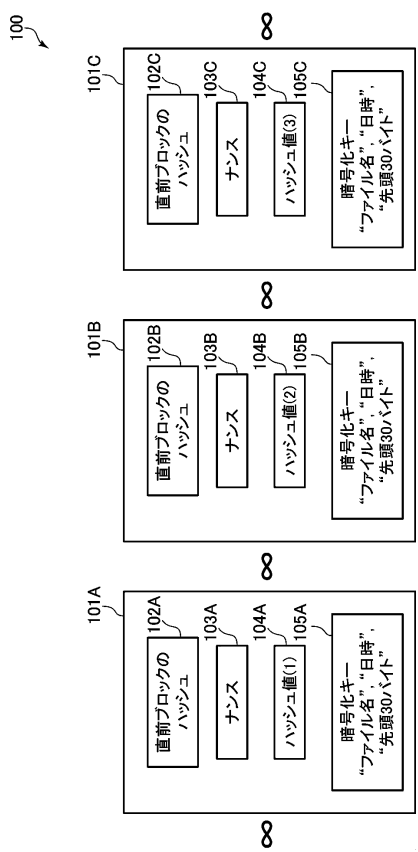
【図 16】



【図 17】



【図 18】



10

20

30

40

50

【図 19】

センターサーバブロックチェーンとは別のデータ

(a)

コロニーサーバID	ユーザID	有効フラグ(TRUE/FALSE)
AAAAAAAAAAAAA	XXXXXXXXXXXXXX	TRUE
BBBBBBBBBBBBB	YYYYYYYYYYYYYY	TRUE
CCCCCCCCCCCCC	ZZZZZZZZZZZZZZ	FALSE

(b)

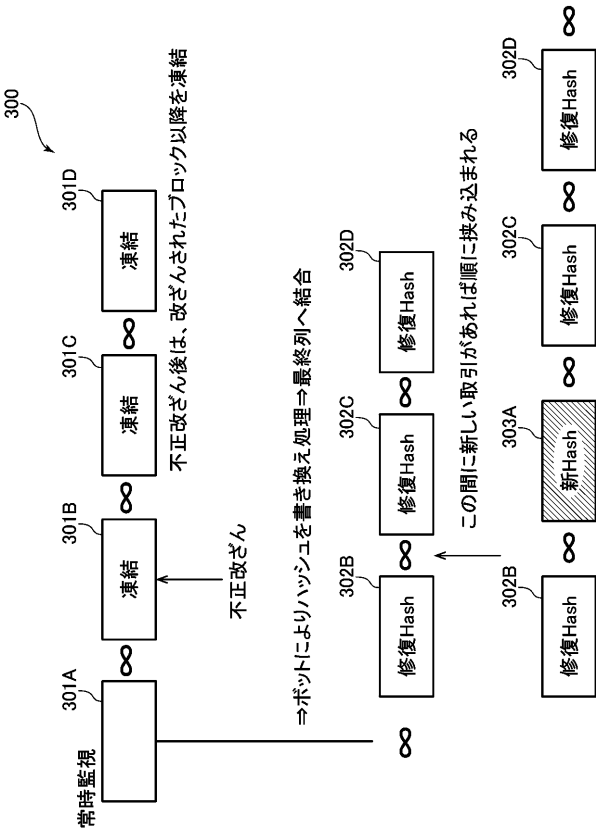
ユーザID	メールアドレス	有効フラグ(TRUE/FALSE)
XXXXXXXXXXXXXX	XXX@abc.co.jp	TRUE
YYYYYYYYYYYYYY	YY@abc.net	TRUE
ZZZZZZZZZZZZZZ	ZZ@ccc.ac.jp	FALSE

【図 20】

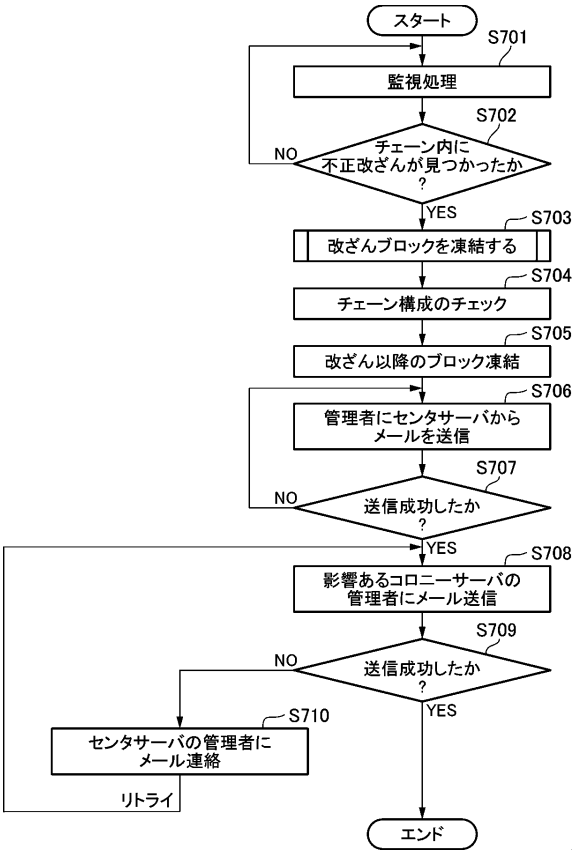
コロニーサーバ

ユーザID	所有ブロックハッシュ (64バイト)	取引日時 (YYYY/MM/DD HH:MM:SS)	有効フラグ(TRUE/FALSE)
XXXXXXXXXXXXXX	ハッシュ値(1)	20190511001125	TRUE
YYYYYYYYYYYYYY	ハッシュ値(2)	20190406002255	TRUE
ZZZZZZZZZZZZZZ	ハッシュ値(3)	20180115051645	FALSE

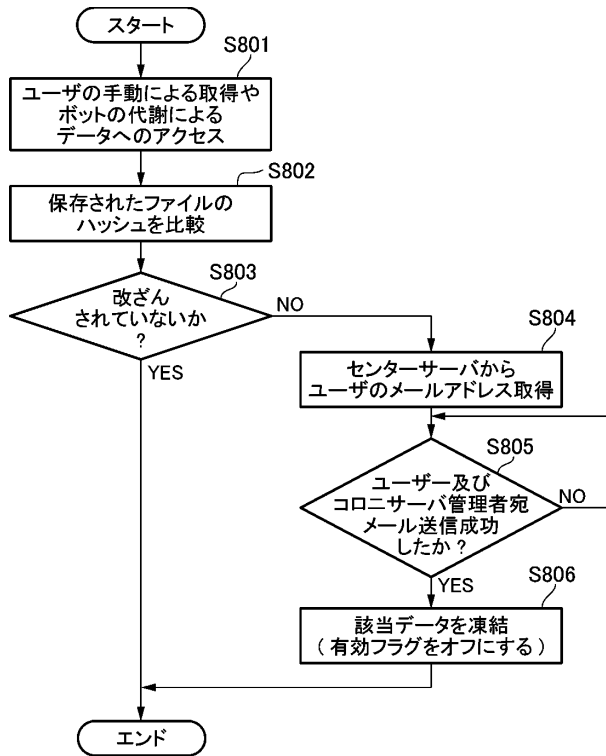
【図 21】



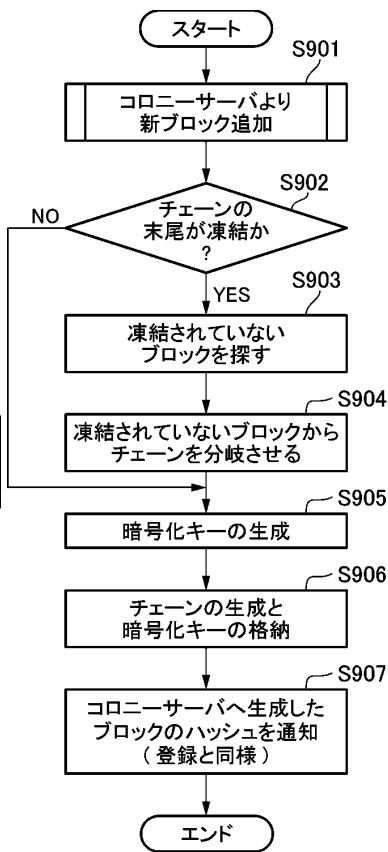
【図 22】



【図 2 3】



【図 2 4】



10

20

30

40

50

フロントページの続き

(74)代理人 100120525
弁理士 近藤 直樹

(74)代理人 100139712
弁理士 那須 威夫

(74)代理人 100176418
弁理士 工藤 嘉晃

(72)発明者 杉浦 伸一
愛知県名古屋市瑞穂区萩山町3丁目4番地

(72)発明者 中原 伸之
東京都世田谷区尾山台2丁目19番7号

(72)発明者 浅野 美香
愛知県名古屋市緑区大将ヶ根1丁目119番地

審査官 土谷 慎吾

(56)参考文献 特開2016-184917(JP, A)
特開2006-072952(JP, A)
特開2008-020964(JP, A)

(58)調査した分野 (Int.Cl., DB名)
H04L 9/32
G06F 21/62