(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7472781号
(P7472781)

(45)発行日　令和6年4月23日(2024.4.23)

(24)登録日　令和6年4月15日(2024.4.15)

(51)国際特許分類
Ｇ０６Ｆ　21/64　(2013.01)

ＦＩ
Ｇ０６Ｆ　21/64

請求項の数　9　（全15頁）

(21)出願番号　特願2020-216399(P2020-216399)
(22)出願日　令和2年12月25日(2020.12.25)
(65)公開番号　特開2022-101967(P2022-101967A)
(43)公開日　令和4年7月7日(2022.7.7)
審査請求日　令和5年1月11日(2023.1.11)

(73)特許権者　000004260
株式会社デンソー
愛知県刈谷市昭和町１丁目１番地
(74)代理人
矢作 和行
(74)代理人　100121991
弁理士　野々部 泰平
(74)代理人　100145595
弁理士　久保 貴則
(72)発明者　徐 ▲シン▼
愛知県刈谷市昭和町１丁目１番地 株式会社デンソー内
審査官　吉田 歩

最終頁に続く

(54)【発明の名称】　データ保存装置、データ保存方法、およびデータ保存プログラム

(57)【特許請求の範囲】
【請求項１】
移動体（Ａ）に搭載され、ノーマルワールド（ＮＷ）および前記ノーマルワールドからのアクセスが制限されるセキュアワールド（ＳＷ）を規定し、前記移動体にて取得される取得データを、ブロックチェーン（ＢＣ）を用いて保存するデータ保存装置であって、
前記ブロックチェーンに連結する新規ブロックを、少なくとも直前のブロックから生成されたブロックハッシュ値に基づいて生成するブロック生成部（１４０）と、
特定の更新タイミングごとに前記ブロックチェーンの最後に連結された最終ブロックに基づく最終ブロックハッシュ値を前記セキュアワールドのストレージ領域（ＴＳ）に保存することで、前回の前記更新タイミングにて保存した前記最終ブロックハッシュ値を更新する保存処理部（１５０）と、
少なくとも前記更新タイミングごとに、前記取得データと前記最終ブロックハッシュ値とに基づくハッシュ値であるデータハッシュ値を生成するデータハッシュ生成部（１２０）と、
を備えるデータ保存装置。
【請求項２】
前記移動体に搭載された３つ以上の他の情報処理装置に対して、前記ブロックチェーンに前記新規ブロックを連結してよいか否かを検証させるための検証情報を送信する送信部（１６０）をさらに備え、
前記ブロック生成部は、３つ以上の前記情報処理装置にて前記新規ブロックの連結につ

いて多数決合意が取れたと判断した場合に、前記新規ブロックを前記ブロックチェーンへ連結する請求項１に記載のデータ保存装置。
【請求項３】
前記保存処理部は、前記移動体における駆動源の停止タイミングにて、前記最終ブロックハッシュ値の更新を実行する請求項１または請求項２に記載のデータ保存装置。
【請求項４】
前記データハッシュ生成部は、予め設定された鍵情報を、さらに前記データハッシュ値の生成に利用する請求項１から請求項３のいずれか１項に記載のデータ保存装置。
【請求項５】
移動体（Ａ）に搭載され、ノーマルワールド（ＮＷ）および前記ノーマルワールドからのアクセスが制限されるセキュアワールド（ＳＷ）を規定し、前記移動体にて取得される取得データを、ブロックチェーン（ＢＣ）を用いて保存するために、プロセッサ（１０２）により実行されるデータ保存方法であって、
前記ブロックチェーンに連結する新規ブロックを、少なくとも直前のブロックから生成されたブロックハッシュ値に基づいて生成するブロック生成プロセス（Ｓ１４０，Ｓ１５０）と、
特定の更新タイミングごとに、前記ブロックチェーンの最後に連結された最終ブロックに基づく最終ブロックハッシュ値を前記セキュアワールドのストレージ領域（ＴＳ）に保存することで、前回の前記更新タイミングにて保存した前記最終ブロックハッシュ値を更新する保存処理プロセス（Ｓ２１０，Ｓ２２０，Ｓ２３０）と、
少なくとも前記更新タイミングごとに、前記取得データと前記最終ブロックハッシュ値とに基づくハッシュ値であるデータハッシュ値を生成するデータハッシュ生成プロセス（Ｓ１２０，Ｓ２５５）と、
を含むデータ保存方法。
【請求項６】
前記移動体に搭載された３つ以上の他の情報処理装置に対して、前記ブロックチェーンに前記新規ブロックを連結してよいか否かを検証させるための検証情報を送信する送信プロセス（Ｓ１６０，Ｓ２６０）をさらに含み、
前記ブロック生成プロセスでは、３つ以上の前記情報処理装置にて前記新規ブロックの連結について多数決合意が取れたと判断した場合に、前記新規ブロックを前記ブロックチェーンへ連結する請求項５に記載のデータ保存方法。
【請求項７】
前記保存処理プロセスでは、前記移動体における駆動源の停止タイミングにて、前記最終ブロックハッシュ値の更新を実行する請求項５または請求項６に記載のデータ保存方法。
【請求項８】
前記データハッシュ生成プロセスでは、予め設定された鍵情報を、さらに前記データハッシュ値の生成に利用する請求項５から請求項７のいずれか１項に記載のデータ保存方法。
【請求項９】
移動体（Ａ）に搭載され、ノーマルワールド（ＮＷ）および前記ノーマルワールドからのアクセスが制限されるセキュアワールド（ＳＷ）を規定し、前記移動体にて取得される取得データを、ブロックチェーン（ＢＣ）を用いて保存するために、プロセッサ（１０２）に実行させる命令を含むデータ保存プログラムであって、
前記命令は、
前記ブロックチェーンに連結させる新規ブロックを、少なくとも直前のブロックから生成されたブロックハッシュ値に基づいて生成させるブロック生成プロセス（Ｓ１４０，Ｓ１５０）と、
特定の更新タイミングごとに、前記ブロックチェーンの最後に連結された最終ブロックに基づく最終ブロックハッシュ値を前記セキュアワールドのストレージ領域（ＴＳ）に保存することで、前回の前記更新タイミングにて保存した前記最終ブロックハッシュ値を更新させる保存処理プロセス（Ｓ２１０，Ｓ２２０，Ｓ２３０）と、

少なくとも前記更新タイミングごとに、前記取得データと前記最終ブロックハッシュ値とに基づくハッシュ値であるデータハッシュ値を生成させるデータハッシュ生成プロセス（Ｓ１２０，Ｓ２５５）と、
を含むデータ保存プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
この明細書における開示は、移動体にて取得されるデータを保存する技術に関する。
【背景技術】
【０００２】
非特許文献１には、車載ＥＣＵに対して暗号鍵を付与し、当該暗号鍵に基づいて正規ＥＣＵの認証を行う技術が開示されている。
【先行技術文献】
【非特許文献】
【０００３】
【文献】国際交通安全学会誌　Ｖｏｌ．４２，Ｎｏ．２，２０１７年１０月、３９頁～４７頁
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかし、車載ＥＣＵに暗号鍵を付与したとしても、当該暗号鍵が漏洩した場合、偽の車載ＥＣＵの取り付け等によるデータの改ざんが容易となる虞がある。非特許文献１には、こうした状況への対策について何ら開示されていない。
【０００５】
開示される目的は、データの改ざんを困難にすることが可能なデータ保存装置、データ保存方法、およびデータ保存プログラムを提供することである。
【課題を解決するための手段】
【０００６】
この明細書に開示された複数の態様は、それぞれの目的を達成するために、互いに異なる技術的手段を採用する。また、特許請求の範囲およびこの項に記載した括弧内の符号は、ひとつの態様として後述する実施形態に記載の具体的手段との対応関係を示す一例であって、技術的範囲を限定するものではない。
【０００７】
開示されたデータ保存装置のひとつは、移動体（Ａ）に搭載され、ノーマルワールド（ＮＷ）およびノーマルワールドからのアクセスが制限されるセキュアワールド（ＳＷ）を規定し、移動体にて取得される取得データを、ブロックチェーン（ＢＣ）を用いて保存するデータ保存装置であって、
ブロックチェーンに連結する新規ブロックを、少なくとも直前のブロックから生成されたブロックハッシュ値に基づいて生成するブロック生成部（１４０）と、
特定の更新タイミングごとにブロックチェーンの最後に連結された最終ブロックに基づく最終ブロックハッシュ値をセキュアワールドのストレージ領域（ＴＳ）に保存することで、前回の更新タイミングにて保存した最終ブロックハッシュ値を更新する保存処理部（１５０）と、
少なくとも更新タイミングごとに、取得データと最終ブロックハッシュ値とに基づくハッシュ値であるデータハッシュ値を生成するデータハッシュ生成部（１２０）と、
を備える。
【０００８】
開示されたデータ保存方法のひとつは、移動体（Ａ）に搭載され、ノーマルワールド（ＮＷ）およびノーマルワールドからのアクセスが制限されるセキュアワールド（ＳＷ）を規定し、移動体にて取得される取得データを、ブロックチェーン（ＢＣ）を用いて保存す

るために、プロセッサ（１０２）により実行されるデータ保存方法であって、
ブロックチェーンに連結する新規ブロックを、少なくとも直前のブロックから生成されたブロックハッシュ値に基づいて生成するブロック生成プロセス（Ｓ１４０，Ｓ１５０）と、
特定の更新タイミングごとに、ブロックチェーンの最後に連結された最終ブロックに基づく最終ブロックハッシュ値をセキュアワールドのストレージ領域（ＴＳ）に保存することで、前回の更新タイミングにて保存した最終ブロックハッシュ値を更新する保存処理プロセス（Ｓ２１０，Ｓ２２０，Ｓ２３０）と、
少なくとも更新タイミングごとに、取得データと最終ブロックハッシュ値とに基づくハッシュ値であるデータハッシュ値を生成するデータハッシュ生成プロセス（Ｓ１２０，Ｓ２５５）と、
を含む。

【０００９】

開示されたデータ保存プログラムのひとつは、移動体（Ａ）に搭載され、ノーマルワールド（ＮＷ）およびノーマルワールドからのアクセスが制限されるセキュアワールド（ＳＷ）を規定し、移動体にて取得される取得データを、ブロックチェーン（ＢＣ）を用いて保存するために、プロセッサ（１０２）に実行させる命令を含むデータ保存プログラムであって、
命令は、
ブロックチェーンに連結させる新規ブロックを、少なくとも直前のブロックから生成されたブロックハッシュ値に基づいて生成させるブロック生成プロセス（Ｓ１４０，Ｓ１５０）と、
特定の更新タイミングごとに、ブロックチェーンの最後に連結された最終ブロックに基づく最終ブロックハッシュ値をセキュアワールドのストレージ領域（ＴＳ）に保存することで、前回の更新タイミングにて保存した最終ブロックハッシュ値を更新させる保存処理プロセス（Ｓ２１０，Ｓ２２０，Ｓ２３０）と、
少なくとも更新タイミングごとに、取得データと最終ブロックハッシュ値とに基づくハッシュ値であるデータハッシュ値を生成させるデータハッシュ生成プロセス（Ｓ１２０，Ｓ２５５）と、
を含む。

【００１０】

これらの開示によれば、特定の更新タイミングごとに、ストレージ領域に保存された最終ブロックハッシュ値が更新される。偽のデータ保存装置の取り付け等によりデータが改ざんされた場合には、最終ブロックハッシュ値および新規データハッシュ値が本来のものと異なったものとなるため、これらの値の少なくとも一方に基づいて改ざんの有無を検証することが可能となり得る。さらに、これらの値は更新タイミングごとに変化するため、前回以前の更新タイミングにおけるこれらの値が漏洩したとしても、改ざんが検知され得る。以上により、データの改ざんを困難にすることが可能なデータ保存装置、データ保存方法、およびデータ保存プログラムが提供され得る。

【図面の簡単な説明】

【００１１】

【図１】車載ＥＣＵが有する機能の一例を示すブロック図である。
【図２】データ保存方法の一例を示す概念図である。
【図３】ブロックハッシュ値の更新方法の一例を示す概念図である。
【図４】データ保存方法のうち、ブロックチェーンの生成処理の一例を示すフローチャートである。
【図５】データ保存方法のうち、検証対象のＥＣＵにて実行される処理の一例を示すフローチャートである。
【図６】データ保存方法のうち、検証担当のＥＣＵにて実行される処理の一例を示すフローチャートである。

【図７】第２実施形態の車載ＥＣＵが有する機能の一例を示すブロック図である。
【図８】第２実施形態のデータ保存方法のうち、検証対象のＥＣＵにて実行される処理の一例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】
【００１２】
（第１実施形態）
第１実施形態のデータ保存装置について、図１～図６を参照しながら説明する。第１実施形態のデータ保存装置は、移動体の一例である車両Ａに搭載された電子制御装置である車載ＥＣＵ１００によって提供される。車載ＥＣＵ１００は、車両Ａにて取得される取得データ、特に車両Ａの操作履歴データＨＤを保存する。
【００１３】
車載ＥＣＵ１００は、車両Ａに複数台、例えば４台以上搭載されている情報処理装置である。複数の車載ＥＣＵ１００は、Ｅｔｈｅｒｎｅｔ（登録商標）等の通信規格に従う車載ネットワークを介して互いに通信可能である。車載ＥＣＵ１００は、それぞれ、後述する取得データの保存および検証以外の処理機能を実行可能である。例えば、車載ＥＣＵ１００は、自動運転機能、高度運転支援機能、周辺監視機能等を実行可能であってよい。また、車載ＥＣＵ１００の１つは、車両制御ＥＣＵ２０（後述）によって提供されてもよい。車載ＥＣＵ１００は、車載センサ１０および車両制御ＥＣＵ２０と車載ネットワークを介して接続されている。
【００１４】
車載センサ１０は、車両Ａに搭載される種々の検出構成である。車載センサ１０には、ドライバによる車両Ａの操作を検出可能なセンサが含まれる。例えば、車載センサ１０には、アクセルペダルの踏み込み量を検出するアクセルペダルセンサ、ブレーキペダルの踏み込み量を検出するブレーキペダルセンサ、ステアリングハンドルの操作量を検出するステアセンサ等が含まれる。各車載センサ１０は、検出したデータを少なくとも１つの車載ＥＣＵ１００に提供可能である。なお、車載センサ１０は、検出データを収集する他のＥＣＵを介して、間接的に車載ＥＣＵ１００に検出データを提供してもよい。
【００１５】
車載ＥＣＵ１００は、車両Ａに搭載された複数の電子制御装置である。車載ＥＣＵ１００のうち少なくとも１つは、上述の車載センサ１０からの取得データおよびブロックチェーンＢＣを保存するデータ保存装置である。他の車載ＥＣＵ１００は、ブロックチェーンＢＣを保存し、当該ブロックチェーンＢＣの信憑性を検証する。以下において、前者の車載ＥＣＵ１００を、「検証対象のＥＣＵ」、後者の車載ＥＣＵ１００を「検証担当のＥＣＵ」と表記する場合がある。
【００１６】
車載ＥＣＵ１００は、メモリ１０１、プロセッサ１０２、入出力インターフェース、およびこれらを接続するバス等を備えたコンピュータを主体として含む構成である。プロセッサ１０２は、演算処理のためのハードウェアである。プロセッサ１０２は、例えばＣＰＵ（Central Processing Unit）、ＧＰＵ（Graphics Processing Unit）およびＲＩＳＣ（Reduced Instruction Set Computer）－ＣＰＵ等のうち、少なくとも一種類をコアとして含む。
【００１７】
車載ＥＣＵ１００は、ノーマルワールドＮＷおよびセキュアワールドＳＷという少なくとも二つの異なる処理領域をシステム内に規定する。ノーマルワールドＮＷおよびセキュアワールドＳＷは、ハードウェア上で物理的に分離されていてもよく、またはハードウェアおよびソフトウェアの連携によって仮想的に分離されていてもよい。車載ＥＣＵ１００は、コンテキストスイッチ等の機能を利用し、アプリケーションの実行に必要なリソースを、ノーマルワールドＮＷおよびセキュアワールドＳＷに時間的に分離させている。
【００１８】
ノーマルワールドＮＷは、オペレーションシステムおよびアプリケーションを実行させ

る通常の領域である。ノーマルワールドＮＷには、データ保存のためのストレージ領域（Untrusted Storage）として、ノーマルストレージＵＳが設けられている。

【００１９】

セキュアワールドＳＷは、ノーマルワールドＮＷから隔離された領域である。セキュアワールドＳＷでは、セキュリティを要求される処理のためのセキュアなオペレーションシステムおよびアプリケーションが実行される。ノーマルワールドＮＷからセキュアワールドＳＷへのアクセスは、プロセッサ１０２の機能によって制限されている。そのため、ノーマルワールドＮＷからは、セキュアワールドＳＷの存在が認識不可能となり、セキュアワールドＳＷにて実行される処理およびセキュアワールドＳＷに保存された情報等の安全性が確保される。セキュアワールドＳＷには、データ保存のためのストレージ領域（Trusted Storage）として、セキュアストレージＴＳが設けられている。セキュアストレージＴＳの容量は、ノーマルストレージＵＳの容量よりも少なくされてよい。または、セキュアストレージＴＳの容量は、ノーマルストレージＵＳの容量と同等以上であってもよい。

【００２０】

メモリ１０１は、コンピュータにより読み取り可能なプログラムおよびデータ等を非一時的に格納または記憶する、例えば半導体メモリ、磁気媒体および光学媒体等のうち、少なくとも一種類の非遷移的実体的記憶媒体（non-transitory tangible storage medium）である。メモリ１０１は、後述のデータ保存プログラム等、プロセッサ１０２によって実行される種々のプログラムを格納している。

【００２１】

プロセッサ１０２は、メモリ１０１に格納されたデータ保存プログラムに含まれる複数の命令を、実行する。これにより車載ＥＣＵ１００は、データ保存のための機能部を、複数構築する。このように車載ＥＣＵ１００では、メモリ１０１に格納されたデータ保存プログラムが複数の命令をプロセッサ１０２に実行させることで、複数の機能部が構築される。具体的に、車載ＥＣＵ１００には、図１に示すように、データブロック作成部１１０、データハッシュ生成部１２０、ブロックハッシュ生成部１３０、ブロック生成部１４０、ハッシュ保存処理部１５０および送信処理部１６０が構築される。加えて、車載ＥＣＵ１００には、図１に示すようにブロックハッシュ保存処理部１７０、検証実行部１８０およびブロック保存処理部１９０等が構築される。

【００２２】

以上の機能部のうち、データブロック作成部１１０、データハッシュ生成部１２０、ブロックハッシュ生成部１３０、ブロック生成部１４０、ハッシュ保存処理部１５０および送信処理部１６０は、検証対象のＥＣＵにて構築される機能部である。また、ブロックハッシュ保存処理部１７０、検証実行部１８０およびブロック保存処理部１９０は、検証担当のＥＣＵにて構築される機能部である。図１においては、それぞれを異なる車載ＥＣＵ１００の機能として記載しているが、各車載ＥＣＵ１００は、検証対象および検証担当を兼任することも可能である。

【００２３】

データブロック作成部１１０は、車載センサ１０にて検出された検出データを、ドライバの操作履歴データＨＤとして取得し、データブロックを作成する。なお、以下においてデータブロックをトランザクションと表記する場合がある。トランザクションは、規定サイズの操作履歴データＨＤをひとまとめに格納する単位である。データブロック作成部１１０は、車両Ａの駆動源の起動中に定期的にトランザクションを作成する。データブロック作成部１１０は、作成したトランザクションを、後述のブロックチェーンＢＣに連結されるブロックＢＬと紐づけた状態でノーマルストレージＵＳに保存する。データブロック作成部１１０は、作成したトランザクションをデータハッシュ生成部１２０およびブロック生成部１４０に提供する。

【００２４】

データブロック作成部１１０は、車両Ａの駆動源が停止したと判断すると、トランザクションの作成を中止する。データブロック作成部１１０は、車両Ａの駆動源が起動したと

判断すると、トランザクションの作成を再開する。以下において、新たに生成されるトランザクションを、特に「新規トランザクション」と表記する場合がある。なお、ここで駆動源起動直後とは、駆動源が起動した後で車載ＥＣＵ１００の信憑性が確保される前のタイミングである。また、駆動源起動直後とは、駆動源が起動した後で初めてデータブロックを生成するタイミングであるということもできる。このタイミングは、「第２タイミング」の一例である。

【００２５】

データハッシュ生成部１２０は、作成されたトランザクションに基づくハッシュ値を、データハッシュ値として生成する。

【００２６】

具体的には、データハッシュ生成部１２０は、図２に示すように、セキュアストレージＴＳに保存されたブロックハッシュ値ＢＨ（ＢＨ＿１）と、トランザクションとを合成したものを、データハッシュ値に変換する。この処理は、トランザクションに対して電子署名を施す処理と解することができる。以下において、新たに生成されたデータハッシュ値を、特に「新規データハッシュ値」と表記する場合がある。データハッシュ生成部１２０は、データハッシュ値をブロック生成部１４０へと提供する。

【００２７】

ブロックハッシュ生成部１３０は、ブロックチェーンＢＣに連結された最後のブロックＢＬである最終ブロックに基づくハッシュ値を、ブロックハッシュ値ＢＨとして生成する。このブロックハッシュ値ＢＨが「最終ブロックハッシュ値」の一例である。図２に示す例では、最終ブロックは「ＢＬＯＣＫ３」、ブロックハッシュ値ＢＨは「ＢＨ＿３」である。ブロックハッシュ生成部１３０は、単にブロックをハッシュ関数にてブロックハッシュ値ＢＨに変換すればよい。ブロックハッシュ生成部１３０は、ブロックハッシュ値ＢＨをブロック生成部１４０および送信処理部１６０に提供する。

【００２８】

以上のデータハッシュ生成部１２０およびブロックハッシュ生成部１３０は、ハッシュ値の生成において、暗号学的ハッシュ関数を利用する。暗号学的ハッシュ関数は、違う入力から同一のハッシュ値を出力することがなく、且つ、出力されたハッシュ値から入力を推測することが実質不可能という特性を有している。例えば、ＳＨＡ－２のひとつであるＳＨＡ－２５６が、暗号学的ハッシュ関数として使用される。または、ＳＨＡ－１、ＳＨＡ－２５６以外のＳＨＡ－２およびＳＨＡ－３等の暗号学的ハッシュ関数が、必要とされる出力長（ビット数）に合わせて適宜使用されてよい。

【００２９】

ブロック生成部１４０は、データハッシュ生成部１２０から取得したデータハッシュ値と、ブロックハッシュ生成部１３０から取得したブロックハッシュ値ＢＨとの組み合わせによるブロックＢＬを生成する。また、ブロック生成部１４０は、生成されたブロックをブロックチェーンＢＣの最後に連結して保存する。

【００３０】

ここで、ブロック生成部１４０は、新規のブロックＢＬを連結する合意が形成された場合にのみ、以上の処理を実施する。詳記すると、ブロック生成部１４０は、まず検証担当のＥＣＵから送信された検証結果を取得する。例えば、ブロック生成部１４０は、３つ以上の他の車載ＥＣＵ１００にて実施された検証結果を取得する。検証結果には、車載ＥＣＵ１００の信憑性を承認するか否かを判断した判断情報が少なくとも含まれる。

【００３１】

そして、ブロック生成部１４０は、取得された検証結果に基づいて、過半数の検証担当のＥＣＵにてデータの信憑性が承認された場合に、新規ブロックＢＬを生成し、当該ブロックＢＬを連結する。図２に示す例では、ＤＨ＿Ｄ（データハッシュ値）と、ＢＨ＿３（ブロックハッシュ値）との組み合わせによるＢＬＯＣＫ４が、新規ブロックとしてＢＬＯＣＫ３の後に連結される。ブロック生成部１４０は、過半数の検証担当のＥＣＵにてデータの信憑性が承認されなかった場合には、ブロックＢＬの連結を中断する。

【００３２】
ハッシュ保存処理部１５０は、ブロックハッシュ値ＢＨを特定のタイミングでセキュアストレージＴＳに保存する。ハッシュ保存処理部１５０は、例えば、車両Ａの駆動源の停止タイミングを保存のタイミングとする。このとき、ハッシュ保存処理部１５０は、前回の停止タイミングにて保存されていたブロックハッシュ値ＢＨを、新たなブロックハッシュ値ＢＨで更新することになる。図３に示す例では、前回の停止タイミングでの最終ブロックであるＢＬＯＣＫ２から生成されたブロックハッシュ値であるＢＨ＿２が、今回の停止タイミングでの最終ブロックであるＢＬＯＣＫ４から生成されたブロックハッシュ値であるＢＨ＿４に更新される。ハッシュ保存処理部１５０は、例えば、車両制御ＥＣＵ２０から駆動源の停止を判断可能な信号（停止信号）を取得した場合に、停止タイミングであると判断する。停止信号は、駆動源が停止した状態を示す停止状態信号であってもよいし、駆動源の停止を指示する停止指示信号であってもよい。停止タイミングは、「更新タイミング」の一例である。
【００３３】
送信処理部１６０は、ブロックチェーンＢＣの生成または車載ＥＣＵ１００の検証において、他の車載ＥＣＵ１００への提供が必要な情報の送信処理を実行する。具体的には、送信処理部１６０は、トランザクションと、その時点でのブロックチェーンＢＣの最終ブロックから生成されたブロックハッシュ値ＢＨとを他の車載ＥＣＵ１００へと送信する。なお、以下において、この検証対象のＥＣＵにて生成されたブロックハッシュ値ＢＨを、対象ブロックハッシュ値と表記する場合がある。送信処理部１６０は、「送信部」の一例である。
【００３４】
ブロックハッシュ保存処理部１７０は、検証担当のＥＣＵにおいて、ブロックハッシュ値ＢＨを駆動源の停止タイミングでセキュアストレージＴＳに保存する。ブロックハッシュ保存処理部１７０は、自身のノーマルストレージＵＳに保存されたブロックチェーンＢＣの最終ブロックからブロックハッシュ値ＢＨを生成してもよいし、検証対象のＥＣＵからブロックハッシュ値ＢＨを取得してもよい。なお、ここでの「自身のノーマルストレージＵＳに保存されたブロックチェーンＢＣ」とは、検証対象のＥＣＵから分散されたブロックチェーンＢＣを意味する。
【００３５】
検証実行部１８０は、検証対象のＥＣＵの信憑性を検証し、承認するか否かの判断情報を生成する。検証実行部１８０は、検証対象から送信された新規トランザクションおよび対象ブロックハッシュ値を取得し、これらの情報と、自身が保存する情報とに基づいて検証を実行する。検証実行部１８０は、自身のセキュアストレージＴＳに保存されたブロックハッシュ値ＢＨである担当ブロックハッシュ値と、検証対象から取得した新規トランザクションとに基づくデータハッシュ値（担当データハッシュ値）を生成する。
【００３６】
一例として、検証実行部１８０は、自身の保存するブロックチェーンＢＣの最終ブロックから生成したブロックハッシュ値（担当ブロックハッシュ値）と、対象ブロックハッシュ値とが一致するか否かを判定する。一致すると判定すると、検証実行部１８０は、検証対象の信憑性を承認する旨の判断情報を生成する。一方で、一致しないと判定すると、検証実行部１８０は、検証対象の信憑性を承認しない旨の判断情報を生成する。検証実行部１８０は、生成した判断情報を、検証対象および検証担当のＥＣＵへと送信する。
【００３７】
ブロック保存処理部１９０は、他の検証担当のＥＣＵから送信された検証結果を取得する。ブロック保存処理部１９０は、過半数の検証担当のＥＣＵにてデータの信憑性が承認された場合に、検証対象のＥＣＵから取得したトランザクションと自身のセキュアストレージＴＳに保存されたブロックハッシュ値ＢＨとからデータハッシュ値を生成する。ブロック保存処理部１９０は、当該データハッシュ値と、自身のブロックチェーンＢＣにおける最終ブロックから生成されたブロックハッシュ値ＢＨとでブロックを生成し、ノーマル

ストレージＵＳのブロックチェーンＢＣに連結して保存する。これにより、ブロック保存処理部１９０は、検証対象のＥＣＵから分散されたブロックチェーンＢＣを保持可能である。

【００３８】

なお、ブロック保存処理部１９０は、当該新規ブロックＢＬを、検証対象のＥＣＵから取得してもよい。ブロック保存処理部１９０は、過半数の検証担当のＥＣＵにてデータの信憑性が承認されなかった場合には、ブロックＢＬの連結を中断する。

【００３９】

次に、機能ブロックの共同により、車載ＥＣＵ１００が実行するデータ保存方法のフローを、図４～５に従って以下に説明する。なお、後述するフローにおいて「Ｓ」とは、プログラムに含まれた複数命令によって実行される、フローの複数ステップを意味する。

【００４０】

まず、データ保存処理のうち、検証対象のＥＣＵが取得したデータに基づいてブロックチェーンＢＣを生成する処理について図４を参照して説明する。まず、Ｓ１１０にて、データブロック作成部１１０が、取得したデータに基づくトランザクションを生成する。次に、Ｓ１２０では、データハッシュ生成部１２０が、トランザクションに基づいてデータハッシュ値を生成する。

【００４１】

続くＳ１３０では、ブロックハッシュ生成部１３０が、最終ブロックに基づいてブロックハッシュ値ＢＨを生成する。さらに、Ｓ１４０では、送信処理部１６０が、最終ブロックのブロックハッシュ値ＢＨと新規トランザクションとを検証担当のＥＣＵに送信する。そして、Ｓ１５０では、ブロック生成部１４０が、新規ブロックＢＬの連結について多数決合意が形成されたか否かを判定する。合意が形成されたと判定すると、本フローがＳ１６０へと移行する。Ｓ１６０では、ブロック生成部１４０が、新規ブロックＢＬを生成してブロックチェーンＢＣに連結する。Ｓ１６０の処理の後、本フローはＳ１１０へと戻る。

【００４２】

一方で、Ｓ１５０にて合意が形成されなかったと判定されると、本フローがＳ１７０へと移行する。Ｓ１７０では、ブロック生成部１４０が、新規ブロックＢＬの生成を中止し、本フローが終了する。

【００４３】

次に、データ保存処理のうち、データの信憑性を検証する処理について図５に従って説明する。まず、Ｓ２１０では、ブロックハッシュ生成部１３０が、車両Ａの駆動源が停止したか否かを判定する。停止していないと判定した場合、停止したと判定するまで待機する。一方で停止したと判定した場合には、Ｓ２２０にて、ブロックハッシュ生成部１３０が、最終ブロックからブロックハッシュ値ＢＨを生成する。次に、Ｓ２３０にて、ハッシュ保存処理部１５０が、生成したブロックハッシュ値ＢＨをセキュアストレージＴＳに保存し、前回保存されたブロックハッシュ値ＢＨを更新する。

【００４４】

続くＳ２４０では、データハッシュ生成部１２０が、車両Ａの駆動源が起動したか否かを判定する。起動していないと判定した場合、起動したと判定するまで待機する。一方で起動したと判定した場合には、Ｓ２５０にて、データブロック作成部１１０が新規トランザクションを作成する。続くＳ２５５にて、データハッシュ生成部１２０が、セキュアストレージＴＳに保存されたブロックハッシュ値ＢＨと新規トランザクションとに基づく新規データハッシュ値を生成する。さらに、Ｓ２６０では、送信処理部１６０が、生成した新規トランザクションおよび最終ブロックのブロックハッシュ値ＢＨを、検証担当のＥＣＵへと送信する。

【００４５】

そして、Ｓ２７０では、ブロック生成部１４０が、各車載ＥＣＵからの判断情報に基づき多数決合意が形成されたか否かを判定する。多数決合意が形成されたと判定した場合、Ｓ２８０にて、ブロック生成部１４０が、新規ブロックＢＬを生成してブロックチェーン

ＢＣに追加する。なお、Ｓ２８０の処理を実行した後は、図４に示すブロックチェーン生成処理を開始すればよい。一方で、Ｓ２７０にて多数決合意が形成されなかったと判定した場合、Ｓ２９０にて、ブロック生成部１４０は、新規ブロックＢＬの生成を中止する。

【００４６】

次に、データ保存処理のうち、検証担当のＥＣＵにて実行される処理について図６に従って説明する。図６に示す処理は、車載ＥＣＵ１００の起動中に実行される。

【００４７】

まず、Ｓ３１０では、ブロック保存処理部１９０が、車両Ａの駆動源が停止したか否かを判定する。停止していないと判定した場合、停止したと判定するまで待機する。一方で停止したと判定した場合には、Ｓ３２０にて、ブロックハッシュ保存処理部１７０が、検証対象のＥＣＵから分散されたブロックチェーンＢＣの最終ブロックからブロックハッシュ値ＢＨを生成する。次に、Ｓ３３０にて、ブロックハッシュ保存処理部１７０が、生成したブロックハッシュ値ＢＨをセキュアストレージＴＳに保存し、前回保存されたブロックハッシュ値を更新する。

【００４８】

続くＳ３４０では、検証実行部１８０が、車両Ａの駆動源が起動したか否かを判定する。起動していないと判定した場合、起動したと判定するまで待機する。一方で起動したと判定した場合には、Ｓ３５０にて、検証実行部１８０が、検証対象のＥＣＵから新規トランザクションおよびデータハッシュ値を取得する。

【００４９】

そして、Ｓ３６０では、検証実行部１８０が、検証対象のＥＣＵを承認するか否かを判定する。承認すると判定すると、Ｓ３６１にて、検証実行部１８０が、新たなブロックＢＬの追加を承認する旨の判断情報を他の車載ＥＣＵ１００へと送信する。

【００５０】

一方で、Ｓ３６０にてデータハッシュ値が一致しないと判定すると、Ｓ３６２にて、検証実行部１８０が、新たなブロックＢＬの追加を非承認する旨の判断情報を他の車載ＥＣＵ１００へと送信する。続くＳ３７０、Ｓ３８０、Ｓ３９０の処理は、図５におけるＳ２７０、Ｓ２８０、Ｓ２９０の処理と同等である。Ｓ３７０、Ｓ３８０、Ｓ３９０の処理は、ブロック保存処理部１９０により実行される。

【００５１】

なお、上述のＳ１４０，Ｓ１５０が「ブロック生成プロセス」、Ｓ２１０，Ｓ２２０，Ｓ２３０が「保存処理プロセス」、Ｓ１２０，Ｓ２５５が「データハッシュ生成プロセス」、Ｓ１６０，Ｓ２６０が「送信プロセス」の一例である。

【００５２】

以上の第１実施形態によれば、特定の更新タイミングごとに、ストレージ領域に保存された最終ブロックハッシュ値が更新される。偽の車載ＥＣＵの取り付け等によりデータが改ざんされた場合には、最終ブロックハッシュ値および新規データハッシュ値が本来のものと異なったものとなるため、これらの値の少なくとも一方に基づいて改ざんの有無を検証することが可能となり得る。さらに、これらの値は更新タイミングごとに変化するため、前回以前の更新タイミングにおけるこれらの値が漏洩したとしても、改ざんが検知され得る。以上により、データの改ざんを困難にすることが可能となり得る。

【００５３】

また、第１実施形態によれば、３つ以上の他の車載ＥＣＵ１００に対して新規データおよび新規データハッシュ値が検証情報として送信される。そして、３つ以上の他の車載ＥＣＵ１００にて多数決合意が取れたと判断された場合に、新規データハッシュ値およびブロックハッシュ値ＢＨに基づく新規ブロックＢＬが生成され、ブロックチェーンＢＣに連結される。これによれば、３つ以上の他の車載ＥＣＵ１００における多数決合意にて信憑性が判断されるので、２つ以下の他の車載ＥＣＵ１００にて信憑性を判断する場合に比べて、信憑性確保の確実性が大きくなる。

【００５４】

加えて、第１実施形態によれば、車両Ａの駆動源の停止タイミングにて、セキュアストレージＴＳに保存されている最終ブロックハッシュ値が更新される。故に、偽の車載ＥＣＵを取り付けられる可能性が比較的高い車両Ａの停止期間に入るタイミングにて最終ブロックハッシュ値が更新され得る。したがって、偽の車載ＥＣＵ１００による改ざんがより確実に困難になり得る。

【００５５】

（第２実施形態）

第２実施形態では、第１実施形態における車載ＥＣＵ１００の変形例について説明する。図７および図８において第１実施形態の図面中と同一符号を付した構成要素は、同様の構成要素であり、同様の作用効果を奏するものである。

【００５６】

第２実施形態のデータハッシュ生成部１２０は、新規データハッシュ値の生成に、ブロックハッシュ値ＢＨに加えて予め設定された鍵情報を利用する。鍵情報は、例えば、車載ＥＣＵ１００ごとに固有に付与された識別情報であるＭＡＣアドレスＭＡとされる。ＭＡＣアドレスＭＡは、ノーマルストレージＵＳに保存されている。または、鍵情報は、車載ＥＣＵ１００の製造時に予め設定された任意の鍵値であってもよい。データハッシュ生成部１２０は、新規トランザクション、ブロックハッシュ値ＢＨおよびＭＡＣアドレスＭＡを合成してハッシュ関数に入力することで、新規データハッシュ値を得る。データハッシュ生成部１２０は、駆動源の起動が判定されて新規トランザクションを生成した後に、以上の処理を実行する（Ｓ２５６）。

【００５７】

第２実施形態の車載ＥＣＵ１００によれば、予め設定された鍵情報が、さらに新規データハッシュ値の生成に利用される。故に、偽の車載ＥＣＵによる偽の新規データハッシュ値の生成がより困難になり得る。したがって、偽の車載ＥＣＵによる改ざんを一層確実に判別し得る。

【００５８】

（他の実施形態）

この明細書における開示は、例示された実施形態に制限されない。開示は、例示された実施形態と、それらに基づく当業者による変形態様を包含する。例えば、開示は、実施形態において示された部品および／または要素の組み合わせに限定されない。開示は、多様な組み合わせによって実施可能である。開示は、実施形態に追加可能な追加的な部分をもつことができる。開示は、実施形態の部品および／または要素が省略されたものを包含する。開示は、ひとつの実施形態と他の実施形態との間における部品および／または要素の置き換え、または組み合わせを包含する。開示される技術的範囲は、実施形態の記載に限定されない。開示されるいくつかの技術的範囲は、特許請求の範囲の記載によって示され、さらに特許請求の範囲の記載と均等の意味および範囲内での全ての変更を含むものと解されるべきである。

【００５９】

上述の実施形態において、車載ＥＣＵ１００は、ドライバの操作履歴データＨＤを取得データとして保存するとしたが、操作履歴データＨＤ以外のデータを保存してもよい。例えば、車載ＥＣＵ１００は、車両Ａの走行距離、走行経路および走行挙動等を保存してもよい。

【００６０】

上述の実施形態において、ハッシュ保存処理部１５０は、駆動源の停止を判断できる停止信号を取得した場合に、停止タイミングであると判断するとした。これに代えて、ハッシュ保存処理部１５０は、停止信号の取得から所定の時間経過した場合に停止タイミングであると判断してもよい。または、ハッシュ保存処理部１５０は、停止信号を取得し且つ車両Ａの電源スイッチ（イグニッションスイッチ等）がオフである場合に、停止タイミングであると判断してもよい。

【００６１】

上述の実施形態において、車載ＥＣＵ１００は、車両Ａの駆動源の停止タイミングにてセキュアストレージＴＳのブロックハッシュ値ＢＨを更新するとした。これに代えて、車載ＥＣＵ１００は、一定時間ごとにブロックハッシュ値ＢＨの更新を実行してもよい。または、車載ＥＣＵ１００は、新規ブロックを生成するたびにブロックハッシュ値ＢＨを更新してもよい。また、車載ＥＣＵ１００は、車両Ａのシフト位置がパーキングレンジにセットされたタイミングにてブロックハッシュ値ＢＨを更新してもよく、サーバから指示信号を受けたタイミングにてブロックハッシュ値ＢＨを更新してもよい。

【００６２】

上述の実施形態において、検証対象のＥＣＵは、３つ以上の検証担当のＥＣＵに対して新規トランザクションおよび新規データハッシュ値を送信するとした。これに代えて、検証対象のＥＣＵは、２つ以下の検証担当のＥＣＵに新規トランザクションおよび新規データハッシュ値を送信してもよい。この場合、検証対象のＥＣＵの承認は、多数決合意以外の手法で行われればよい。

【００６３】

上述の実施形態において、車載ＥＣＵ１００がデータ保存処理を実行するとした。これに代えて、車両Ａ以外の移動体に搭載されたデータ保存装置がデータ保存処理を実行してもよい。移動体には、船舶、飛行機、鉄道車両等が含まれる。

【００６４】

上述の実施形態において、ブロック生成部１４０は、データハッシュ値とブロックハッシュ値との組み合わせによるブロックＢＬを生成するとした。これに代えて、ブロック生成部１４０は、トランザクションとブロックハッシュ値の組み合わせによるブロックＢＬを生成してもよい。または、ブロック生成部１４０はトランザクション、データハッシュ値およびブロックハッシュ値の組み合わせによるブロックＢＬを生成してもよい。

【００６５】

上述の実施形態において、データハッシュ生成部１２０は、トランザクションが生成されるたびに、ブロックハッシュ値とトランザクションとを合成したものを、データハッシュ値に変換するとした。これに代えて、データハッシュ生成部１２０は、駆動源起動直後以外は、単にトランザクションをデータハッシュ値に変換し、駆動源起動直後には、ブロックハッシュ値とトランザクションとを合成したものをデータハッシュ値に変換する構成であってもよい。

【００６６】

上述の実施形態において、送信処理部１６０は、トランザクションとブロックハッシュ値を検証担当のＥＣＵに送信するとした。これに代えて、送信処理部１６０は、トランザクションと当該トランザクションから生成されたデータハッシュ値とを送信してもよい。

【００６７】

車載ＥＣＵ１００は、デジタル回路およびアナログ回路のうち少なくとも一方をプロセッサとして含んで構成される、専用のコンピュータであってもよい。ここで特にデジタル回路とは、例えば、ＡＳＩＣ（Application Specific Integrated Circuit）、ＦＰＧＡ（Field Programmable Gate Array）、ＳＯＣ（System on a Chip）、ＰＧＡ（Programmable Gate Array）、およびＣＰＬＤ（Complex Programmable Logic Device）等のうち、少なくとも一種類である。またこうしたデジタル回路は、プログラムを格納したメモリを、備えていてもよい。

【００６８】

車載ＥＣＵ１００は、１つのコンピュータ、またはデータ通信装置によってリンクされた一組のコンピュータ資源によって提供され得る。例えば、上述の実施形態における車載ＥＣＵ１００の提供する機能の一部は、他のＥＣＵによって実現されてもよい。

【符号の説明】

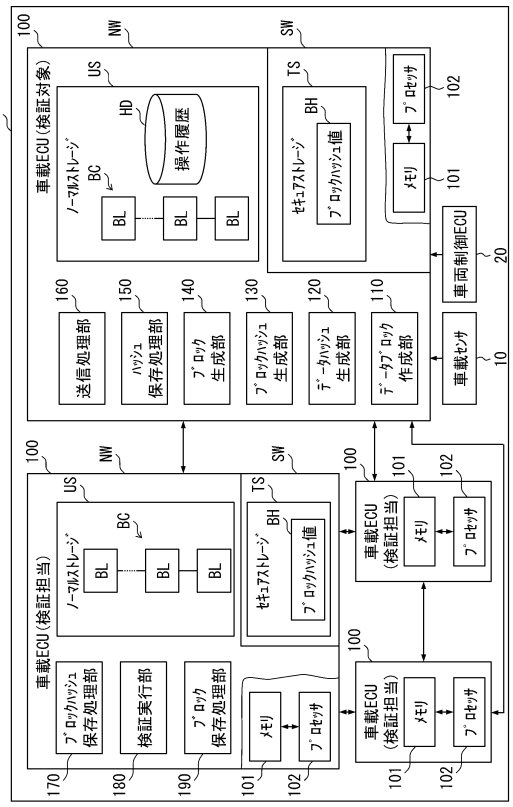
【００６９】

１００　車載ＥＣＵ（データ保存装置）、　１０２　プロセッサ、　１２０　データハッシュ生成部、　１４０　ブロック生成部、　１５０　ハッシュ保存処理部（保存処理部）

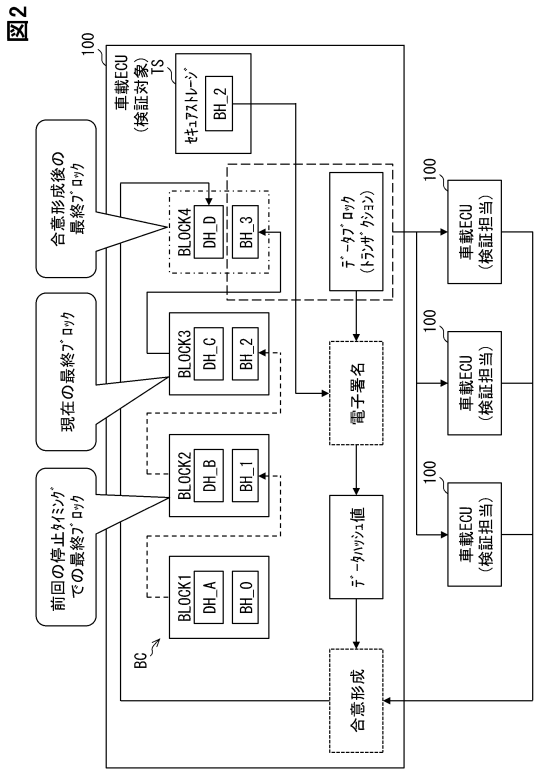
、　１６０　送信処理部（送信部）、　Ａ　車両（移動体）、　ＢＣ　ブロックチェーン、　ＮＷ　ノーマルワールド、　ＳＷ　セキュアワールド、　ＴＳ　セキュアストレージ（ストレージ領域）。

【図面】

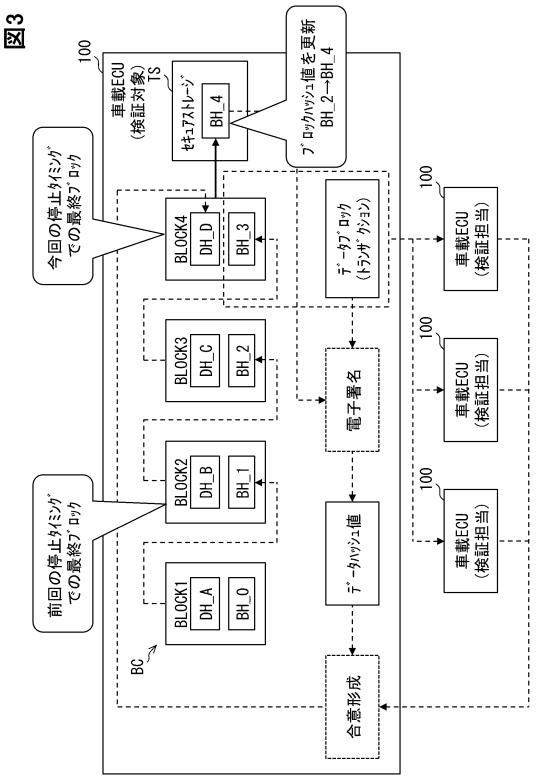
【図１】



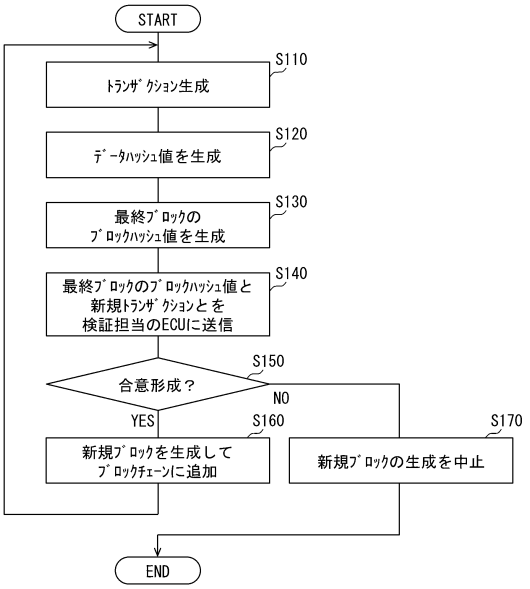
【図２】



【図３】

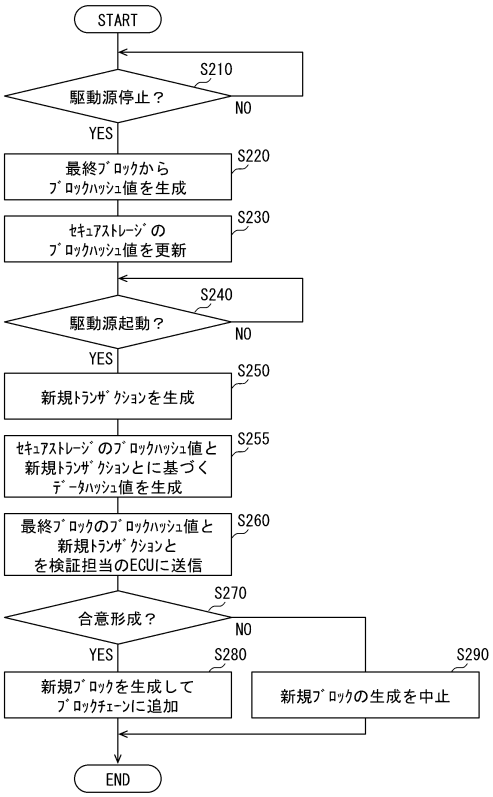


【図４】



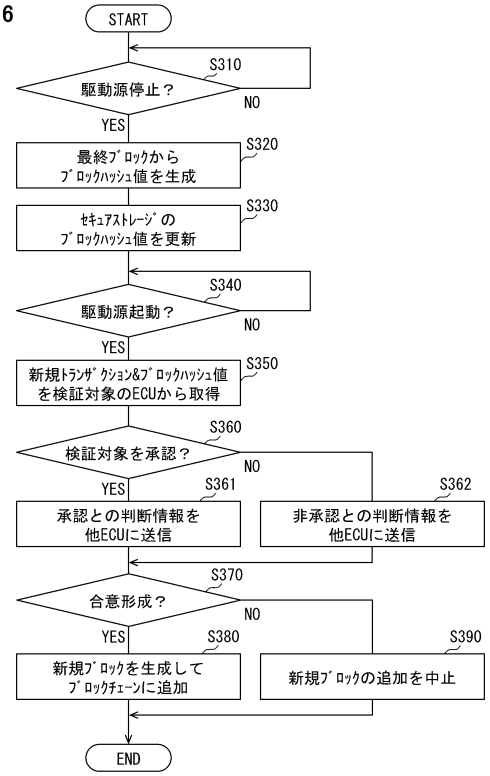
【図５】

図5



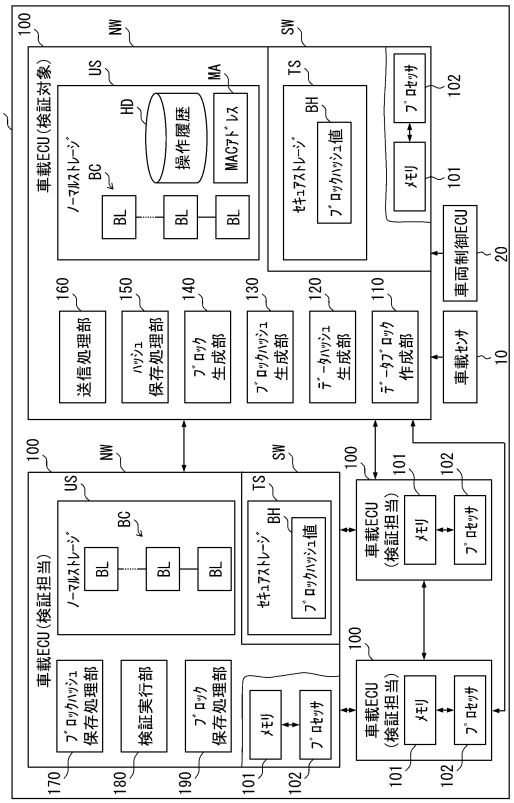
【図６】

図6



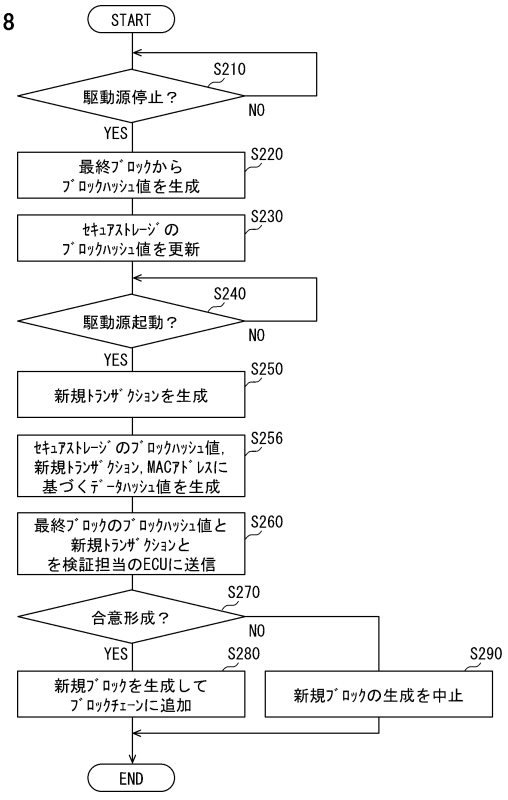
【図７】

図7



【図８】

図8



フロントページの続き

(56)参考文献 特表２０２０－５２５８７７（ＪＰ，Ａ）
特開２０１８－１３３７４４（ＪＰ，Ａ）
岡部 達哉 ほか，ブロックチェーン技術を用いた車両データ・製品トレーサビリティデータの改ざん防止，ＤＥＮＳＯ ＴＥＣＨＮＩＣＡＬ ＲＥＶＩＥＷ，日本，株式会社デンソー，2019年11月30日，２０１９，Ｖｏｌ．２４，ｐｐ．４２－５２，ＩＳＳＮ：１３４２－４１１４

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／６４