(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号

特表2023-536027
(P2023-536027A)

(43)公表日　令和5年8月23日(2023.8.23)

(51)Int.Cl.			F I		テーマコード(参考)
G06F	21/62	(2013.01)	G06F	21/62	
H04L	9/32	(2006.01)	H04L	9/32	200Z
G06F	21/60	(2013.01)	G06F	21/60	320

審査請求 未請求　予備審査請求 未請求　(全 23 頁)

(21)出願番号　特願2022-545124(P2022-545124)
(86)(22)出願日　令和2年11月16日(2020.11.16)
(85)翻訳文提出日　令和4年8月25日(2022.8.25)
(86)国際出願番号　PCT/EP2020/082248
(87)国際公開番号　WO2022/022844
(87)国際公開日　令和4年2月3日(2022.2.3)
(31)優先権主張番号　P.434845
(32)優先日　令和2年7月29日(2020.7.29)
(33)優先権主張国・地域又は機関
ポーランド(PL)

(71)出願人　522294420
ディセラ　エスペー・ゾオ
ＤＩＣＥＬＬＡ　ＳＰ．　Ｚ　Ｏ．Ｏ．
ポーランド　クラクフ　ウリツァ・ポドレ　６０
ｕｌ．　Ｐｏｄｏｌｅ　６０　Ｋｒａｋｏｗ　Ｐｏｌａｎｄ
(74)代理人　110000567
弁理士法人サトー
(72)発明者　ミシュタル　クシシュトフ
ポーランド　クラクフ　ウリツァ・デプスキエゴ　７４／４
(72)発明者　クビツァーミシュタル　アレクサンドラ
ポーランド　クラクフ　ウリツァ・デプスキエゴ　７４／４

最終頁に続く

(54)【発明の名称】データ、特にバイオテクノロジー・ラボラトリのデータをセキュアにするための方法およびシステム

(57)【要約】
本発明は、中央サーバと、２つ又はそれ以上のサブシステムとを備えるシステム中で実現された、ブロックチェーン・テクノロジーを使用してデータをセキュアにするための方法であって、２つ又はそれ以上のサブシステムの各々は、情報データを記憶するための第１のブロックチェーン・データベースと、アクセス・データを記憶するための第２のブロックチェーン・データベースとを備え、第１のデータベースへのアクセスを有するユーザは、対応する許可の情報を用いて別のユーザのデジタル鍵を第２のデータベースに追加することによって、前記別のユーザが、ユーザによってオーサリングされたデータを第１のデータベースから読み取ることを可能にするか又は禁止することが可能である方法に関係する。本発明はまた、中央サーバと、各々が専用のサブサーバによって制御される、２つ又はそれ以上のサブシステムとを備えるデータをセキュアにするためのシステムに関する。
【選択図】図５

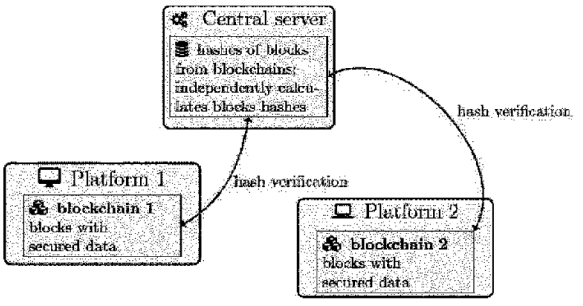

Fig. 5

【特許請求の範囲】
【請求項１】
中央サーバと、各々が専用のサブサーバによって制御される、２つまたはそれ以上のサブシステムとを備えるシステム中で実現された、ブロックチェーン・テクノロジーを使用して、データ、特にバイオテクノロジー・ラボラトリのデータをセキュアにするための方法であって、前記２つまたはそれ以上のサブシステムの各々は、
－　情報データ、特にバイオテクノロジー・ラボラトリのデータを記憶するための第１のブロックチェーン・データベースであって、前記第１のブロックチェーン・データベース中のトランザクションが、第１の特定の情報をトランザクションとして扱うことと、オーサーのデジタル鍵を用いて前記第１の特定の情報のオーサーによって前記トランザクションのデジタル署名を作成することと、第１の新しいブロックにトランザクションを結合することと、前記第１のデータベース中の前のブロックのハッシュを用いて前記第１の新しいブロックを暗号化することと、前記第１のデータベースに前記第１の新しいブロックを記憶することとを含む、ブロックチェーン・ルールに従ってコミットされる、第１のブロックチェーン・データベースと、
－　前記第１のデータベースへのアクセスを有するユーザのデジタル鍵と、各そのようなユーザの前記デジタル鍵に関連付けられたこのユーザによって前記第１のデータベースからデータを読み取るかまたは前記第１のデータベースにデータを書き込むための許可に関する情報とを含む、アクセス・データを記憶するための第２のブロックチェーン・データベースであって、そこにおいて、第２のデータベース情報が、第２の特定の情報をトランザクションとして扱うことと、オーサーのデジタル鍵を用いて前記第２の特定の情報のオーサーによって前記トランザクションのデジタル署名を作成することと、第２の新しいブロックにトランザクションを結合することと、前記第２のデータベース中の前のブロックのハッシュを用いて前記第２の新しいブロックを暗号化することと、前記第２のデータベースに前記第２の新しいブロックを記憶することとを含む、ブロックチェーン・ルールに従って記憶される、第２のブロックチェーン・データベースと
を備え、
－　前記第１のデータベースへのアクセスを有するあらゆる認可されたユーザは、対応する許可の情報を用いて別のユーザの前記デジタル鍵を前記第２のデータベースに追加することによって、前記別のユーザが、前記認可されたユーザによってオーサリングされたデータを前記第１のデータベースから読み取ることを可能にすることが可能であり、
－　前記第１のデータベースへのアクセスを有するあらゆる認可されたユーザは、対応する許可の情報を用いて別のユーザの前記デジタル鍵を前記第２のデータベースに追加することによって、前記別のユーザが、前記認可されたユーザによってオーサリングされたデータを前記第１のデータベースから読み取ることを禁止することが可能であり、
－　前記第１のデータベースへのアクセスを有するあらゆる認可されたユーザが、前記認可されたユーザによってオーサリングされた前記第１のデータベース中のデータへのアクセスに関する前に付与された権利を別のユーザから撤回することが可能であり、
データをセキュアにするための前記方法が、
－　好ましくは、ハッシュのみおよび随意にタイムスタンプを収集することによって、前記２つまたはそれ以上のサブシステム中のブロックチェーン・データベースから前記ハッシュおよび随意にタイムスタンプを収集することと、
－　偽のハッシュを回避するために前記サブサーバの秘密鍵を使用して、前記中央サーバと前記サブサーバとの間で新しいトランザクションを交換し、ハッシュの互換性を単独で検証することと
による、前記２つまたはそれ以上のサブシステム中のブロックチェーン・データベースの互換性および不変性の前記中央サーバによる検証を含む、
方法。
【請求項２】
ＳＨＡ－３が、前記第１のブロックチェーン・データベースおよび／または前記第２のブ

ロックチェーン・データベース中のブロック・ハッシュの算出のためのハッシュ関数として使用される、請求項１に記載の方法。
【請求項３】
４０９６ビットの鍵サイズをもつＲＳＡアルゴリズムが、前記トランザクションのデジタル署名を、前記第１のブロックチェーン・データベースおよび／または前記第２のブロックチェーン・データベース中のそれのオーサーのデジタル鍵を用いて作成するために使用される、請求項１または２に記載の方法。
【請求項４】
前記システムが、追加としてタイムスタンプ・サーバを備え、前記タイムスタンプ・サーバが、前記第１のブロックチェーン・データベースおよび／または前記第２のブロックチェーン・データベースに、特に前記第１のブロックチェーン・データベースおよび／または前記第２のブロックチェーン・データベース中のトランザクションおよび／またはブロックにタイムスタンプを提供する、請求項１から３のいずれか一項に記載の方法。
【請求項５】
前記第２のデータベースが、Ｋ個の先行するブロックのハッシュおよび最新の要約ブロックのハッシュを含んでいる、要約ブロックを備え、要約ブロックが、ユーザ特権の更新された情報を含んでいる、請求項１から４のいずれか一項に記載の方法。
【請求項６】
前記中央サーバが、前記要約ブロックを監視する、請求項５に記載の方法。
【請求項７】
前記中央サーバが、前記サブサーバと周期的に通信し、特に、各々が専用のサブサーバによって制御される、前記２つまたはそれ以上のサブシステムの各々中のブロックチェーン・データベースが、前記中央サーバによって周期的に検証される、請求項１から６のいずれか一項に記載の方法。
【請求項８】
インターネット・アクセスなしにラボラトリ・サーバまたは中央コンピュータ上で走る、請求項１から７のいずれか一項に記載の方法。
【請求項９】
前記第１のブロックチェーン・データベースおよび前記第２のブロックチェーン・データベースが、前記情報データ、特にバイオテクノロジー・ラボラトリのデータと、前記第１のデータベースへのアクセスを有するユーザのデジタル鍵、および各そのようなユーザの前記デジタル鍵に関連付けられたこのユーザによって前記第１のデータベースからデータを読み取るかまたは前記第１のデータベースにデータを書き込むための許可に関する情報を含む、前記アクセス・データの両方を記憶するための同一のブロックチェーン・データベースである、請求項１から８のいずれか一項に記載の方法。
【請求項１０】
前記第１のデータベースに記憶された前記データが、移植のためのドナー登録、バイオストレージまたは臨床試験に関する、請求項１から９のいずれか一項に記載の方法。
【請求項１１】
中央サーバと、各々が専用のサブサーバによって制御される、２つまたはそれ以上のサブシステムとを備える、データ、特にバイオテクノロジー・ラボラトリのデータをセキュアにするためのシステムであって、前記２つまたはそれ以上のサブシステムの各々が、情報データ、特にバイオテクノロジー・ラボラトリのデータを記憶するための第１のブロックチェーン・データベースと、前記第１のデータベースへのアクセスを有するユーザのデジタル鍵と、各そのようなユーザの前記デジタル鍵に関連付けられたこのユーザによって前記第１のデータベースからデータを読み取るかまたは前記第１のデータベースにデータを書き込むための許可に関する情報とを含む、アクセス・データを記憶するための第２のブロックチェーン・データベースとを備え、前記システムが、請求項１から１０のいずれか一項に記載の方法を実行するために構成およびプログラムされた、システム。
【発明の詳細な説明】

【技術分野】
【０００１】
本発明は、データ、特にバイオテクノロジー・ラボラトリのデータをセキュアにするための方法、およびこの方法を実装するためのシステムに関する。
【背景技術】
【０００２】
ブロックチェーン
２００８年に、Ｓａｔｏｓｈｉ　Ｎａｋａｍｏｔｏは、現在世界中で第１の暗号通貨と呼ばれる、ビットコインを記述する論文［５］を発行した。プレフィックス暗号通貨は、ワード暗号から導出される。ビットコインは、インターネットを介して匿名で現金が要らないトランザクションを実施する能力を提供する、完全で複雑なシステムである。ビットコインは、システムのユーザのうちの誰かによって管理され得る、分散型決済台帳に基づく。そのようなユーザは、管理に対する彼らの報酬が、新たにマイニングされた通貨であるので、マイナーと呼ばれる。マイナーは、トランザクションに関する情報を集め、それらが実施され得るかどうかを検証する。次いで、彼らは、決済台帳に記憶すべきトランザクションを選定する。この台帳は、ブロックチェーンとして知られている。使用される暗号アルゴリズムのおかげで、別のユーザとしてトランザクションを行うことは不可能である。その上、トランザクションがブロックチェーンに記憶された場合、誰もそれを変更または削除することができない。
【０００３】
すべてのビットコイン・トランザクションは、暗号化されずにブロックチェーンに記憶されるが、ブロックチェーンに暗号化されたデータを保持することも可能であることに留意されたい。
【０００４】
ビットコイン・テクノロジー
ブロックチェーンの数個の実装形態があり、我々は、よく知られているプリカーサー・ビットコインに焦点を当てる。詳細については、［２］を参照されたい。トランザクションを行うことを希望する売り手または支払人は、ブロックチェーンに彼らのアクションをサブミットしなければならない。ブロックチェーン・システムに接続された全員が、トランザクションに関する情報を受信する。受信者は、マイナーと呼ばれ、アルゴリズムによってアクションを検証するクライアントである。暗号化アルゴリズムによる検証は、２つの計算ステップを用いて実行される。マイナーは、算出能力を提供する。マイニングのためのソフトウェアは、無料で単純である。その上、証明書が必要とされず、よって、全員が彼らのコンピュータを用いて志願することができる。マイナーは、トランザクションのために使用され得るビットコインの存在を検証しなければならない。次いで、マイナーは、フォームをチェックし、トランザクションを受け付ける。マイナーが、ブロック全体を検証した場合、マイナーは、ビットコインを与えられる。ブロックは、トランザクションの検証プロセスに関する詳細な情報を有する。ブロックは、それが、固定数のマイナーによって検証された後、ブロックチェーンに記憶される。しかも、あらゆるブロック内に、タイムスタンプと、データ・ブロック中の（非）インタラプションをセキュアにする、ハッシュと呼ばれる数学的に生成された複素変数和とがある。ブロックのこれらの暗号化ハッシュは、先行するおよび現在のブロックに基づいて算出される。この固有で一意の和は、ブロックチェーンにブロックを結合するセキュリティ署名を構成する。ハッシュ・コードの不可逆性は、ブロックチェーンを不変にする。このようにして、我々はデジタル信頼を得る。アクションの分散型検証および履歴にそれらを保存することは、トランザクションを実施するために、銀行のようなメディエータ・エンティティを無用にする。
例：
１．ジョンが、アリスにビットコインを支払うことを望む。
２．ジョンのトランザクションが行われる。
３．トランザクションは、新しいブロックに結合される。

４．ブロックは、マイナーにブロードキャストされる。
５．マイナーは、トランザクションを検証し、受け付ける。
６．新しいブロックが、前のブロックのハッシュを用いて暗号化される。
７．新しいブロックは、ブロックチェーンの一部分になる。
８．アリスは、ビットコインを受け取る。
【０００５】
ブロックチェーン中の機密データ
分散型システムが、広く使用され得る。最も大きい利益は、サード・パーティの必要がないということである。前に見たように、分散型データは、セキュアにされ、かつ不変であり得る。今日では、たいていの組織は、彼らのサービスを最適化するために、我々のパーソナル・データを収集する。彼らは、我々のニーズを予測することおよび我々のデジタル・パーソナル画像を作成することを希望し、これにより、あらゆる態様のパーソナル情報は、今日の経済において価値があるリソースである。パーソナライズされたシステムには多くの利益があるが、我々のプライバシーについての問題が懸念される。しかも、現在、よりしばしば組織は、パーソナル機密データに対する制御をほとんど有しない。それが、この情報が、サード・パーティによって取り扱われるべきではない理由である。集中システムは、ハッカー攻撃ならびにフィッシングに対して脆弱である。ソリューションは、ユーザが、ユーザの情報を所有し、その情報を提供する役目を果たすことである。
【０００６】
我々は、［８］によって提案されたブロックチェーン・ストレージ・ソリューションを適用することによって、これを行うことができる。著者は、ブロックチェーンおよびオフブロックチェーン・ストレージの利点を有するパーソナル・データ管理システムを提案した。これは、数個の主要な態様、すなわち、データ所有権、データ透明度可聴性およびきめの細かいアクセス制御を必要とする。提案されたプラットフォームは、自分のパーソナル情報を所有および制御するユーザと、サービスとを区別する。あらゆるユーザは、コロケートされたデータと、それが組織によってどのようにアクセスされるかとに関する情報を有する。サービスは、ユーザのデータにアクセスするために彼らから許可を委任した。しかも、データの所有者は、サービスに対してデータへのアクセスを否定するために、許可のセットへの変更を行うことが可能である。このソリューションは、モバイル・アプリのものと同様である。それは、アクセス制御ポリシーがブロックチェーンに記憶されるので、ユーザ・インターフェースに影響を及ぼさない。ユーザのみが、ブロックチェーンの変更を行うことが可能である（図１）。
【０００７】
ヘルス・ケアにおけるブロックチェーン・アプリケーションに関するいくつかのアイデアが、［２］において見られ得る。
【０００８】
ラボラトリ
医薬品製造品質管理基準（ＧＭＰ：Ｇｏｏｄ　Ｍａｎｕｆａｃｔｕｒｉｎｇ　Ｐｒａｃｔｉｃｅ）および医薬品安全試験実施基準（ＧＬＰ：Ｇｏｏｄ　Ｌａｂｏｒａｔｏｒｙ　Ｐｒａｃｔｉｃｅ）ラボラトリにおいて得られた結果は、信頼できなければならない。部分的な結果の修正は、最終結果の失敗をもたらすことがある。それが、ラボ記録が、正確におよび偽造なしに収集されなければならない理由である。あらゆる記録のオーサーを覚えていることも重要である。オーサーシップは、疑う余地がないものでなければならず、これは、誰も、別のユーザに代わって記録を作成することができない、およびどのユーザも、自身の記録のうちのいずれかの自身のオーサーシップを否定することができないことを意味する。その上、文書は不変でなければならず、それにより、どの記憶されたデータも修正または削除され得ない。これらの要件は、ユーザに厳密な記録を保持させ、これは、客観的にラボラトリの信頼性を増加させる。
【０００９】
この問題を解決することは、発明者が、バイオテクノロジー・ラボラトリの従業員および

診断法と協働することを必要とした。実生活の問題をアルゴリズム技術手法に変換することは、多大な時間を必要とした。

【００１０】

ラボ従業員についての数個の主要な態様、すなわち、

－　制限およびアクセス・ルールを伴う、倉庫への一定のアクセス、

－　プロセスを改善するための、生産を処理するルール、

－　ラボ結果を集めるルール。取得されたデータのオーサーシップ、

－　偽造および変造を回避するための、毎日の作業を報告するルール、

－　クライアントとのコミュニケーション

があった。

すべてのこれらの態様は、ラボ・ワークフローに著しい影響を及ぼす。

【００１１】

ブロックチェーン・テクノロジーは、アカウンティングおよびバンキングにおいて広く使用されているが、それらの分野においてだけではない。日常生活の多くの異なる領域においてこのテクノロジーを適応させる多くのプロジェクトがある。ヘルス・ケアの広く理解されている領域においてブロックチェーン・テクノロジーを使用することによる、我々のプロジェクトは、それらの１つである。

【００１２】

バイオテクノロジー・ラボにおける文書のための要件は、記録が紙上に保持されているとき、強化され得ない。しかしながら、ラボ記録のための関連する要件は、ブロックチェーンの主要な特徴によって満たされる。本特許出願は、それによって、データがブロックチェーンに記憶され、新たに追加されたトランザクションの正当性がチェックされる、ブロックチェーン・テクノロジーを使用してバイオテクノロジー・ラボラトリのデータをセキュアにするための革新的な方法およびシステムを提案する。

【００１３】

「Ｍｏｂｉｌｅ ｈｅａｌｔｈ ｍａｎａｇｅｍｅｎｔ ｄａｔａｂａｓｅ，ｔａｒｇｅｔｅｄ ｅｄｕｃａｔｉｏｎａｌ ａｓｓｉｓｔａｎｃｅ（ｔｅａ）ｅｎｇｉｎｅ，ｓｅｌｅｃｔｉｖｅ ｈｅａｌｔｈ ｃａｒｅ ｄａｔａ ｓｈａｒｉｎｇ，ｆａｍｉｌｙ ｔｒｅｅ ｇｒａｐｈｉｃａｌ ｕｓｅｒ ｉｎｔｅｒｆａｃｅ，ａｎｄ ｈｅａｌｔｈ ｊｏｕｒｎａｌ ｓｏｃｉａｌ ｎｅｔｗｏｒｋ ｗａｌｌ ｆｅｅｄ，ｃｏｍｐｕｔｅｒ－ｉｍｐｌｅｍｅｎｔｅｄ ｓｙｓｔｅｍ，ｍｅｔｈｏｄ ａｎｄ ｃｏｍｐｕｔｅｒ ｐｒｏｇｒａｍ ｐｒｏｄｕｃｔ」と題する米国特許出願公開第２０１７０３６４６３７（Ａ１）号は、電子コンピューティング・デバイス上の第１の人の健康情報をキャプチャおよび表示するシステム、方法およびコンピュータ・プログラム製品であって、そこにおいて、電子コンピューティング・デバイスは、１つまたは複数のコンピュータ・プロセッサと、１つまたは複数のメモリ・デバイスとを含むことができ、コンピュータ実装方法は、たとえば、ａ）第１のクライアント・コンピューティング・デバイス上の第１の人ユーザに関するデータを電子的に受信することであって、ここで、第１の人ユーザは、各々が１つまたは複数のコンピューティング・デバイスを有する、１人もしくは複数の家族ユーザ、またはユーザが、パーソナル健康データ記録をその人と共有することを望み得るユーザを有し、第１の人ユーザに関するデータは、第１の人に関する任意の識別データ、任意の入力された健康関係データ、または任意のキャプチャされた健康関係データを含むことができ、任意の健康関係データ、アプリケーション・プログラミング・インターフェース（ＡＰＩ）アクセス可能データ、あるいはたとえば、電子医療記録（ＥＭＲ）、スキャンされたデータ、検知されたデータ、または光学文字認識（ＯＣＲ）キャプチャされたデータなど、他の健康記録を含むことができる、第１の人ユーザに関するデータを電子的に受信することと、ｂ）１人または複数の第２の人ユーザに関するデータを受信することであって、ここで、少なくとも１人の第２の人ユーザは、第１の人がその人と接続されることを望む任意の他の人ユーザ、家族、保護者、友人、個人、またはケア提供者を含むことができ、第２の人ユーザに関するデータは、任意の識別データ、任意

の入力された健康関係データ、または第２の人ユーザに関する任意のキャプチャされた健康関係データを含むことができる、１人または複数の第２の人ユーザに関するデータを受信することと、ｃ）第１の人ユーザに関するデータの少なくとも一部分を第２の人ユーザに電子的に共有することとを含むことができる、システム、方法およびコンピュータ・プログラム製品を開示する。様々な他の実施形態は、健康雑誌、対象が絞られた教育コンテンツ、対話型家系図、選択可能な共有、エスカレートされたアラーティング、通知、および共同デジタル・ファイル・キャビネットなど、様々な特徴を含むことができる。この明細書は、データがどのように記憶されるかの技術的詳細ではなく、モバイル・アプリケーションに焦点を当てている。特に、この明細書は、中央サーバと、各々が専用のサブサーバによって制御される、２つまたはそれ以上のブロックチェーン・サブシステムとを備え、そこにおいて、中央サーバが、前記２つまたはそれ以上のサブシステム中のブロックチェーン・データベースの互換性および不変性を検証する、システムを開示または示唆しない。

【発明の概要】

【発明が解決しようとする課題】

【００１４】

これにより、本発明の目的は、ブロックチェーン・テクノロジーを使用して、データ、特にバイオテクノロジー・ラボラトリのデータをセキュアにし、（各個のデータが、それのオーサーを有するので）データの安全性および信頼性を提供し、同時にデータ・アクセスおよび制御の管理しやすい方式をユーザに提供するための方法およびシステムを提供することである。その上、本発明は、法律の関連する規定に完全に準拠するシステムおよび方法を提供する。

【課題を解決するための手段】

【００１５】

本発明によれば、中央サーバと、各々が専用のサブサーバによって制御される、２つまたはそれ以上のサブシステムとを備えるシステム中で実現された、ブロックチェーン・テクノロジーを使用して、データ、特にバイオテクノロジー・ラボラトリのデータをセキュアにするための方法であって、２つまたはそれ以上のサブシステムの各々は、

－　情報データ、特にバイオテクノロジー・ラボラトリのデータを記憶するための第１のブロックチェーン・データベースであって、第１のブロックチェーン・データベース中のトランザクションが、第１の特定の情報をトランザクションとして扱うことと、オーサーのデジタル鍵を用いて前記第１の特定の情報のオーサーによってトランザクションのデジタル署名を作成することと、第１の新しいブロックにトランザクションを結合することと、第１のデータベース中の前のブロックのハッシュを用いて第１の新しいブロックを暗号化することと、第１のデータベースに第１の新しいブロックを記憶することとを含む、ブロックチェーン・ルールに従ってコミットされる、第１のブロックチェーン・データベースと、

－　第１のデータベースへのアクセスを有するユーザのデジタル鍵と、各そのようなユーザのデジタル鍵に関連付けられたこのユーザによって第１のデータベースからデータを読み取るかまたは第１のデータベースにデータを書き込むための許可に関する情報とを含む、アクセス・データを記憶するための第２のブロックチェーン・データベースであって、そこにおいて、第２のデータベース情報が、第２の特定の情報をトランザクションとして扱うことと、オーサーのデジタル鍵を用いて前記第２の特定の情報のオーサーによってトランザクションのデジタル署名を作成することと、第２の新しいブロックにトランザクションを結合することと、第２のデータベース中の前のブロックのハッシュを用いて第２の新しいブロックを暗号化することと、第２のデータベースに第２の新しいブロックを記憶することとを含む、ブロックチェーン・ルールに従って記憶される、第２のブロックチェーン・データベースと

を備え、

－　第１のデータベースへのアクセスを有するあらゆる認可されたユーザは、対応する許

可の情報を用いて別のユーザのデジタル鍵を前記第２のデータベースに追加することによって、前記別のユーザが、前記認可されたユーザによってオーサリングされたデータを第１のデータベースから読み取ることを可能にすることが可能であり、
－　第１のデータベースへのアクセスを有するあらゆる認可されたユーザは、対応する許可の情報を用いて別のユーザのデジタル鍵を前記第２のデータベースに追加することによって、前記別のユーザが、前記認可されたユーザによってオーサリングされたデータを第１のデータベースから読み取ることを禁止することが可能であり、
－　第１のデータベースへのアクセスを有するあらゆる認可されたユーザが、前記認可されたユーザによってオーサリングされた第１のデータベース中のデータへのアクセスに関する前に付与された権利を別のユーザから撤回することが可能であり、
データをセキュアにするための前記方法が、
－　好ましくは、ハッシュのみおよび随意にタイムスタンプを収集することによって、前記２つまたはそれ以上のサブシステム中のブロックチェーン・データベースから前記ハッシュおよび随意にタイムスタンプを収集することと、
－　偽のハッシュを回避するためにサブサーバの秘密鍵を使用して、中央サーバとサブサーバとの間で新しいトランザクションを交換し、ハッシュの互換性を単独で検証することと
による、前記２つまたはそれ以上のサブシステム中のブロックチェーン・データベースの互換性および不変性の中央サーバによる検証を含む、
方法。

【００１６】
好ましくは、ＳＨＡ－３が、第１のブロックチェーン・データベースおよび／または第２のブロックチェーン・データベース中のブロック・ハッシュの算出のためのハッシュ関数として使用される。

【００１７】
好ましくは、４０９６ビットの鍵サイズをもつＲＳＡアルゴリズムが、トランザクションのデジタル署名を、第１のブロックチェーン・データベースおよび／または第２のブロックチェーン・データベース中のそれのオーサーのデジタル鍵を用いて作成するために使用される。

【００１８】
好ましくは、システムが、追加としてタイムスタンプ・サーバを備え、タイムスタンプ・サーバが、第１のブロックチェーン・データベースおよび／または第２のブロックチェーン・データベースに、特に第１のブロックチェーン・データベースおよび／または第２のブロックチェーン・データベース中のトランザクションおよび／またはブロックにタイムスタンプを提供する。

【００１９】
好ましくは、第２のデータベースが、Ｋ個の先行するブロックのハッシュおよび最新の要約ブロックのハッシュを含んでいる、要約ブロックを備え、要約ブロックが、ユーザ特権の更新された情報を含んでいる。

【００２０】
そのような場合、中央サーバが、要約ブロックを監視する。

【００２１】
好ましくは、中央サーバが、サブサーバと周期的に通信し、特に、各々が専用のサブサーバによって制御される、２つまたはそれ以上のサブシステムの各々中のブロックチェーン・データベースが、中央サーバによって周期的に検証される。

【００２２】
本発明的方法は、インターネット・アクセスなしにラボラトリ・サーバまたは中央コンピュータ上で走り得る。

【００２３】
好ましくは、前記第１のブロックチェーン・データベースおよび前記第２のブロックチェ

ーン・データベースが、情報データ、特にバイオテクノロジー・ラボラトリのデータと、第１のデータベースへのアクセスを有するユーザのデジタル鍵、および各そのようなユーザのデジタル鍵に関連付けられたこのユーザによって第１のデータベースからデータを読み取るかまたは第１のデータベースにデータを書き込むための許可に関する情報を含む、アクセス・データの両方を記憶するための同一のブロックチェーン・データベースである。

【００２４】

好ましくは、第１のデータベースに記憶されたデータが、移植のためのドナー登録、バイオストレージまたは臨床試験に関する。

【００２５】

本発明によれば、中央サーバと、各々が専用のサブサーバによって制御される、２つまたはそれ以上のサブシステムとを備える、データ、特にバイオテクノロジー・ラボラトリのデータをセキュアにするためのシステムであって、２つまたはそれ以上のサブシステムの各々が、情報データ、特にバイオテクノロジー・ラボラトリのデータを記憶するための第１のブロックチェーン・データベースと、第１のデータベースへのアクセスを有するユーザのデジタル鍵と、各そのようなユーザのデジタル鍵に関連付けられたこのユーザによって第１のデータベースからデータを読み取るかまたは第１のデータベースにデータを書き込むための許可に関する情報とを含む、アクセス・データを記憶するための第２のブロックチェーン・データベースとを備え、前記システムが、上述の発明的方法を実行するために構成およびプログラムされた、システム。

【００２６】

既存のブロックチェーン適合システムは、広範囲にわたり、分散されている。概して、そのようなシステムでは、マイナーのすべては、ブロックチェーン・データベースの一部分または全体を保有し、検証を実施する。トランザクションのこれらの分散型コピーは、ブロックチェーンのほとんどすべてのノードが、変造される必要があるので、十分な量の計算能力（「ハッキング・フォース」）を編成することは実際問題として不可能であるので、それらをハッキング攻撃または偽造に対して免疫があるようにする。

【００２７】

ラボラトリ・シナリオでは、トランザクションを検証するためにその量の計算能力を達成することは不可能である。しかし、その必要はない。ラボラトリ結果は、迷惑な攻撃の標的にはそれほど含まれない。結果が、資格がない人によって変造または破損されることを防ぐ必要がある。データの変更を追跡する必要がある。ラボラトリ・コンピュータは、たいてい、インターネットへのアクセスをもたない閉じられたネットワーク中にあり、それらは、公共サービスのようにオープンではない。

【００２８】

分散型ブロックチェーンにおけるのと同様の保護のレベルを達成するために、我々は、半分散型システムを製作することによって、分散化をシミュレートすることができる。このアイデアは、それらのそれぞれのブロックチェーン・サブシステムにおいて定期的なブロックチェーン保守を実施する、１つまたは複数のサブサーバと、ブロックチェーン・サブシステムのためのガードである、中央サーバとを必要とする。中央サーバは、ブロックチェーン・サブシステムからのハッシュおよびタイムスタンプ（のみ）を含んでいる。その上、固定間隔において、中央サーバは、サブサーバを、それらのブロックチェーンを計算することによって検証する。このシナリオでは、中央サーバは、ブロックチェーン全体を保有することをシミュレートする、追加のマイナーとして働く。

【００２９】

上記で説明された半分散型アプローチは、

－　完全分散型ブロックチェーンに比較してより少ない計算能力、

－　コンパクト・ネットワークのアイデアによる、追加の機器なしでのラボラトリの多様性に対する容易な適合の可能性、

－　中央サーバによって保有されるブロックチェーンのソフト・コピー、

－　それぞれのブロックチェーン・サブシステムにそれら自体のそれぞれのデータのみを保有するサブサーバの各々、
を含む、数個の利点を有する。
偽造攻撃の場合、少なくとも２つのサーバが、ハッキングされなければならない。システムは、インターネット・アクセスをもたない閉じられたネットワークにおいて実装され得、走ることができる。
【００３０】
本発明の好ましい実施形態が、添付の図面を参照しながらより詳細なやり方で以下で提示される。
【図面の簡単な説明】
【００３１】
【図１】上記のグラントアクセス・データ・ブロックチェーンの簡略化されたスキーマを提示する図である。
【図２】ブロック中のハッシュリンキングおよびＲＳＡ署名を示す図である。
【図３】提案されるラボラトリ・ブロックチェーン・プラットフォーム使用を提示する図であり、プラットフォームは、署名され、セキュアにされたトランザクションを検証および記憶し、追加のラボサポーティング・アルゴリズムは、ブロックチェーン・データに基づいてユーザのために分析を実施し、警報が、必要なときに送られる、図である。
【図４】Ｋ個の前のブロックのハッシュと最新の要約－ブロックのハッシュとを含んでいる、要約ブロックを示す図であり、要約ブロックは、ユーザ特権の更新された情報を含んでおり、要約－ブロックは、チェックポイント・ブロックであり、ブロックチェーンの「末尾」を算出する必要がない、図である。
【図５】２つまたはそれ以上のブロックチェーン・システムを制御し、すべてのブロックのハッシュおよびタイムスタンプを記憶し、ブロックチェーンが破損しているかどうかを周期的に検証する、中央サーバを提示する図である。
【発明を実施するための形態】
【００３２】
本発明の好ましい実施形態が、以下で詳細に説明される。例は、例示の働きのみをし、本発明の範囲を限定しない。
【００３３】
ブロックチェーン・アプリケーション
ビットコイン［５］の著者は、コインを生産し、トランザクションを検証する中央当局があり得ることを述べた。それは、当局が、あらゆるトランザクションに関する無限の知識を有するという問題を提起する。この問題は、非常に巧妙なやり方で解決され得る。これに対するソリューションを解説することを試みる前に、ＧＭＰおよびＧＬＰラボラトリのためにブロックチェーンにおいて定義するトランザクションに焦点を当てる。我々は、あらゆるデータ情報が、変更されず、それのオーサーを有することを希望する。我々のプラットフォームでは、単一の情報のトランザクションは、ビットコイン・システム中のコインを表す。
【００３４】
ユーザＡが何らかのトピックに関するノートを作成したシナリオを検討する。我々のシステムは、そのノートのオーサーシップ、ならびにユーザＡがそのノートのどの部分も否定することができないという事実を覚えている必要がある。それが、ユーザが、自身のデジタル署名によってノートを証明する理由である。異なるＢユーザは、ノートが欠陥を有し、よって彼が補正を行うことを希望することを述べた。彼は、これを行うことができるが、明らかなやり方においてではない。ユーザＢは、ノートをとり、そのノートからの算出されたハッシュ・コードを追加し、ノートに補正を追加する。自身のデジタル署名を追加した後、彼は、情報をサブミットする。このようにして、あらゆるユーザは、どの部分がＡのものであり、どの部分がＢのものであるかを検証することができる。我々は、本発明による、ビットコイン、暗号コインおよびデータ・ノートの間の互換性を認める。Ｂによ

って行われた補正機構は、同じ暗号コインを２回費やす場合と同様である。折り畳み署名を検証するシステムは、ビットコイン・シナリオと同様にこの問題を解決することがわかる。

【００３５】

異なる態様は、情報を作成する必要が起こったときである。コインは、特定の正規化されたやり方で作られ得る。我々のプラットフォームに記憶された情報は、あらゆる認可されたユーザのために利用可能であるべきである。それが、我々が、ユーザのための許可アクセスを表す第２のタイプのコインを必要とする理由である。それが、あらゆる認可されたラボラトリ・ユーザが、自身の同僚のデジタル鍵を追加する能力を有し、彼がブロックチェーン中の遷移を行うことを可能にする理由である。あらゆる認可されたユーザと同様に、それは、同様に、特定のユーザがシステムにアクセスするのを否定することができる。要約すれば、ビットコイン・システムでは、誰から誰にコインが送られるかに関する情報が記憶される。本発明的プラットフォームに、我々は、

－　許可情報をもつユーザ・デジタル鍵。我々は、ユーザがトランザクションに署名することを可能にされるかどうかを追跡する、

－　データ情報。我々は、ラボラトリ・データのオーサーシップを追跡し、このソリューションは一般的であり、そのため、任意のタイプのラボ・データが記憶され得る、

ということに関する情報を記憶する。

【００３６】

それゆえ、本発明的ソリューションでは、データおよび証明の両方が、ブロックチェーン・データベースに収集される。この観点から、本発明的システムは、２つの部分から構成されると見なされ得る。

【００３７】

技術詳細

プログラミング言語およびライブラリ。我々は、我々が（任意のテクノロジーにおいて）任意のシステムのためにアプリケーションを作成することができるように、特定の暗号化パッケージおよびプログラミング言語Ｐｙｔｈｏｎ３を選定する。パイソン・アプリは、Ｃ言語のアプリほど効率的ではないが、それらは、よりポータブルである。Ｐｙｔｈｏｎはまた、サイバーセキュリティをもって作業する専門のプログラマーの間で評価される。プロトタイプでは、我々は、ＳＨＡ－３実装されたハッシュ関数のために、ジャンゴ・フレームワークおよび暗号パイソン・パッケージを使用した。それは、単純で効果的なプログラミングを可能にし、急速に広がっている。これらのアルゴリズムは、我々のニーズに対して十分である。

【００３８】

ブロック・ハッシュ関数。ブロックチェーンの基本的で不可欠な成分は、十分に定義されたハッシュ関数である。米国標準技術局（ＮＩＳＴ）は、２つの文献［１］および［３］を発行し、ここで、３つのハッシュ関数、すなわち、ＳＨＡ－１、ＳＨＡ－２およびＳＨＡ－３のみを認定した。

【００３９】

ＳＨＡ－３は、他の２つとは技術的にまったく異なる。ＳＨＡ－１およびＳＨＡ－２は、共通した数学的機構に基づく。２０１７年に、グーグルは、ＳＨＡ－１が、突破され、セキュリティのために使用されるべきではないことを発表した［７］。ＳＨＡ－１およびＳＨＡ－２と比較して、我々は、新しくてバグがないアルゴリズムとしてＳＨＡ－３を選定した。

【００４０】

ユーザ・デジタル署名。ブロックチェーンを作成する際の次の重要なステップは、デジタル署名およびそれの検証のためのアルゴリズムである。ここで、主要なソリューションは、非対称一方向暗号化関数である。米国標準技術局（ＮＩＳＴ）は、［４］において、デジタル署名を使用した３つの暗号化アルゴリズム、すなわち、ＲＳＡ、ＤＳＡおよびＥＣＤＳＡを定義した。

【００４１】
暗号化権威のＢｒｕｃｅ　Ｓｃｈｎｅｉｅｒによって提案された楕円曲線に関する論争［６］により、我々は、４０９６ビットの鍵サイズをもつＲＳＡアルゴリズムを選定した。
【００４２】
ブロック実装形態の詳細。将来の問題を回避するために、我々は、鍵のあらかじめ定義されたセットをもつ辞書の形態でブロックを設計した。それらのオブジェクトは、容易にシリアライズされ、ＪＳＯＮフォーマットにデシリアライズされ得る。
リスティング１．１は、辞書ブロックのための７つの鍵を示す。
ｃｌａｓｓ　ＢｌｏｃｋＦｉｅｌｄ（Ｅｎｕｍ）：
ＢＬＯＣＫ＿ＴＹＰＥ　＝　０
ＴＩＭＥＳＴＡＭＰ　＝　１
ＡＵＴＨＯＲ　＝　２
ＳＩＧＮＡＴＵＲＥ　＝　３
ＯＢＪＥＣＴ　＝　４
ＰＲＥＶＩＯＵＳ＿ＨＡＳＨ　＝　５
ＮＯＮＣＥ　＝　６
リスティング１．１。ブロック・オブジェクト中のすべてのパラメータを記述するＥｎｕｍ。
我々はまた、リスティング１．２において示される５つのタイプのブロックを定義した。
ｃｌａｓｓ　ＢｌｏｃｋＴｙｐｅ（Ｅｎｕｍ）：
ＧＥＮＥＳＩＳ　＝　０
ＩＮＳＥＲＴ＿ＢＬＯＣＫ　＝　１
ＵＰＤＡＴＥ＿ＢＬＯＣＫ　＝　２
ＩＮＳＥＲＴ＿ＫＥＹ　＝　３
ＲＥＶＯＫＥ＿ＫＥＹ　＝　４
リスティング１．２。チェーン中の可能なタイプのブロックを記述するＥｎｕｍ。
【００４３】
ジェネシス・ブロックは、チェーン中の第１のものである。ブロックチェーンにはただ１つのジェネシス・ブロックがあり得る。それは、システム・アドミニストレータ鍵を含んでおり、それは、拒否され得ない。公開鍵は、ソフトウェアを管理する管理者によって制御され、ラボラトリ従業員の手中にない。
【００４４】
プラットフォーム
我々は、ブロックチェーン・テクノロジー・プロトタイプの実装の作業を終わらせ、その上、我々は、我々の理論的分析によって与えられる目的に適合するやり方で、ブロックチェーン・テクノロジーの非従来型修正を行った。我々は、我々のシステムによって節約された時間リソースを検証した。著しい改善があった。システムは、時間がかかり、リソースを消費する問題に効果的であった。設計されたプラットフォームは、ラボラトリ条件で検証された。我々は、設計されたソリューションが、ラボラトリ・ワークフロー（図３）に影響を及ぼしたことがわかった。
【００４５】
我々は、使用事例のあらゆる態様における、ならびに我々のシステムの性能における有効性を確認した。ブロックチェーン機構による処理時間およびメモリ使用量は、計算量的に厳しくなかった。
【００４６】
少ないカスタマイゼーションをもつ我々が設計したテンプレート・プラットフォームは、ラボラトリにおいて広く望まれる利益を提供する。下記は、提案されるブロックチェーン・システムに由来する利点のリストである。
１．データが、無認可の変更に対してセキュアにされる。
２．データのブロックチェーン・セキュリティが、それらをオーセンティックおよびレピ

ュディエーションにする。
３．ブロックチェーンに記憶されたデータが、透過的である。
４．医薬品製造品質管理基準の法的規制、すなわち、米国連邦規制基準、タイトル１１、パート１１（ＧＭＰ　ＣＦＲ　２１パート１１）により、システムが、伝導する電子文書を可能にする。
５．システムが、バイオバンクのための法的要件に適合する。
６．システムは、医師のおよび歯科医の法律に従った組織および細胞調達の実現を助ける。
７．システムは、高度な医薬製品の生産に関する薬剤法律の法令を満たす。
８．システムは、生産ならびに（細胞、組織および器官を移植する）医学療法に関するＵＥ要件を満たす。
９．システムにおける追加のアルゴリズムが、ラボ・ワークフローを改善する統計値をアーカイブする。
１０．システムは、ラボラトリ・ストレージを安定的に管理する際に役立つ。
１１．システム内蔵分析アルゴリズムが、それらが需要検証、生産を列挙するので、従業員の時間を節約する。
【００４７】
システム安定性
著者は、［５］において、年代順にブロックをバインドする、タイムスタンプ・サーバ・アイデアを導入している。我々が提案するシステムでは、ただ１つのタイムスタンプ・サーバがある。サーバへのネットワークまたは物理的アクセスは、最低限に制限される。システムは、ラボラトリにおいて作成または編集されたデータ、ならびにこのデータをサブミットすることができるユーザの鍵をチェックする。タイムスタンプ・サーバは、年代順にトランザクションをソートする。新しいデータが追加されるとき、システムは、それの妥当性、たとえば、
－　ノートが以前に作られたかどうか、
－　ノートの編集されたコンテンツが、ブロックチェーン中の最後のものに対応するかどうか、
－　ユーザが、ノートを追加することを可能にされるかどうか。システムは、ユーザのデジタル鍵が、アクティブであり、コンテンツを追加することを許可されるどうかを検証する、
ということを検証する。
【００４８】
我々は、ブロックチェーンが破損しているかどうかを決定するために、安定性リストを作った。下記は、ブロックチェーンにブロックを挿入するときにシステムによって検証されるチェックリストである。
１．第１のブロックが、ジェネシス・ブロックではない。
２．２つ以上のブロックが、ジェネシス・ブロックである。
３．ジェネシス・ブロックのための前のハッシュ・フィールドが、予想されるものとは異なる。
４．ブロックの名前からのタイムスタンプが、ブロックのコンテンツに対応していない。
５．ブロックの前のハッシュ値が、それの前のブロックに適合しない。
６．ハッシュ・ストリングが、ゼロの固定長で始まらない。
７．ユーザ・デジタル鍵が、２回追加された。
８．ユーザ・デジタル鍵が、２回削除された。
９．ジェネシス鍵が削除された。
１０．デジタル鍵がないため、無認可のユーザによって追加されたブロック。
１１．デジタル鍵拒否のため、無認可のユーザによって追加されたブロック。
１２．ブロック中の必須のフィールドの欠如。
【００４９】

我々は、我々のシステムをハッキングすることを試みた。我々は、ブルートフォース攻撃を使用したが、幸運にも成功しなかった。我々が、我々のシステムを実行する際に選定した暗号化パッケージは、この種類の迷惑なハッキング・アクセスに専用である。その上、ハッシュ関数として使用されたＳＨＡ－３アルゴリズムは、最も安全で、最もセキュアで、最も効率的なハッシュ・アルゴリズムのうちの１つである。非量子コンピュータの場合、ＳＨＡ－３アルゴリズムは、次の２０～３０年の内に突破されないはずだ。

【００５０】

半分散型ブロックチェーン

ブロックチェーンを部分に分割する、またはあらゆるインスタンスにおいてブロックチェーン全体を保持する必要はない。それが、多くの別個のラボラトリをもつ大きい施設において、半分散型ブロックチェーンを導入することが有益である理由である。我々は、ブロック形態ラボラトリ・ブロックチェーンのハッシュのみを含んでおり、それらが破損しているかどうかを検証する１つの中央サーバを使用する。

－　マルチ・ラボラトリ・シナリオでは、ラボラトリにおける活動を検証する中央当局が必要である。

－　半分散型ブロックチェーンが、ラボラトリ・ユニットの間の透明度を増加させるために、マルチラボラトリ状況において欠かせないものである（図４）。

－　半分散型ブロックチェーン・シナリオでは、ただ１つの中央サーバがある。

－　中央サーバは、サブラボラトリにおけるブロックチェーンの互換性および不変性を検証し、サブラボラトリにおけるブロックチェーンの各々は、専用のサブサーバによって制御される。

－　中央サーバは、サブラボラトリのブロックチェーンからハッシュおよびタイムスタンプのみを収集する。

－　中央サーバおよびサブサーバは、新しいトランザクションを交換し、単独でハッシュの互換性を検証する。サブサーバの秘密鍵が、偽のハッシュを回避するために必要とされる。

－　サブサーバのブロックチェーン全体が、中央サーバによって周期的に検証される。

－　中央サーバは、（要約ブロックが使用される場合）要約ブロックを監視する。

－　中央サーバは、サブラボラトリと周期的に通信する。スケジュールが、管理者によって定義される（図５）。

【００５１】

プラットフォーム適合

以下の特徴は、随意であるが、本発明の有用な特徴であり、それらは、スーパーユーザ／管理者によってスケジュール・アルゴリズムとして使用され得、特定のラボラトリ状況に適合され得る。

－　単一のコンピュータが、追加の改善なしに、単純なブロックチェーンを含み、管理することができる。

－　ラボラトリ結果が、たいていエクセルの紙形態である。ユーザ・フレンドリーなインターフェースにより、本発明的プラットフォームは、ワークフローを増加させる。

－　メディア定常度。メディア・ファイルのハッシュのみが、ブロックチェーンに保持される。

－　ブロックチェーンは、半分散型であり得る。

－　ブロックチェーンは、インターネット・アクセスなしにラボラトリ・サーバまたは中央コンピュータ上で走り得る。

－　周期的に、ブロックチェーン全体が、算出され、非互換性についてチェックされる。

－　要約ブロック生成が、より小さい計算時間を達成するために、アクティベートされ得る。

－　サブラボラトリをもつ施設では、ブロックチェーンは、半分散させられる。中央サーバは、周期的に従属サブラボラトリのブロック形態ブロックチェーンのハッシュのみを収集および検証する、判定代行者である。

－　保守では、ブロックチェーン変更が可能にされない。
【００５２】
ジェネシス・ブロック
ジェネシス・ブロックの技術的詳細。
１．すべてのユーザ情報が、ブロックチェーン中にある。
２．ＵｓｅｒＤａｔａフィールドにおいて、ユーザのパスワードを用いて暗号化された秘密ユーザ鍵がある。
３．ただ１人のスーパーユーザ管理者がいる。
４．管理者のみが、ジェネシス・ブロックを作成することを許可される。
５．ブロックチェーンを開始するただ１つのジェネシス・ブロックがある。
【００５３】
ユーザ許可
ユーザの技術的詳細。
－　ジェネシス・ブロックが、ブロックチェーンを開始し、新しいユーザを作成するために必須である。
－　ユーザ許可および秘密鍵情報が、毎回チェックされる。
－無認可のアクセスをセキュアにするために、許可が、管理者およびジェネシス・ブロック・シナリオと同様にブロックチェーンに記憶される。
－　スーパーユーザのみが、新しい認可されたユーザを追加することができる。
－　スーパーユーザのみが、ユーザから許可を撤回することができる。
－　すべての実際のユーザ特権が、要約ブロックに記憶される。
【００５４】
要約－ブロック
特定の計算リサーチ・ユニットを除いて、いくつかのラボラトリではハイエンド・コンピュータの欠如があり得る。それが、我々が要約－ブロック・アイデアを導入した理由である。この単純な追加は、計算時間を短縮しながら、依然としてブロックチェーンの基礎を壊さないための完全なソリューションである。
１．要約－ブロックが、ブロックチェーンを短縮するショートカットブロックである。
２．要約－ブロックの目的は、新しいトランザクションのための計算時間を改善することである。
３．ブロック計算時間が、分析される。計算時間が臨界値を上回る場合、管理者は通知される。
４．スーパーユーザ管理者のみが、手動で要約－ブロックを強制することができる。
５．要約－ブロック生成条件。
－　新しいユーザが追加される。
－　ユーザ特権が変更される。
－　アルゴリズム制約。現在のブロック・サイズが大きすぎる。
－　計算時間が長すぎる。
－　保守制約。
６．要約－ブロック生成。
（ａ）ブロックチェーンが、Ｋ個のブロックに分割される。Ｋ個のブロックごとに、要約－ブロックがある。
（ｂ）ブロックチェーン全体が、要約－ブロックおよび残りの直近のブロックのみを使用することによって、破損について算出および検証される。
（ｃ）新しい要約－ブロックが、
－　前のブロック
－　前の要約－ブロック
－　（前の要約－ブロックから開始する）最近のブロック
のハッシュを含んでいる。
（ｄ）現在のブロックチェーンが、バックアップされ、最後のブロックとして要約－ブロ

ックと入れ替えられる。
（ｅ）古典的なブロックチェーン全体の検証が、スケジュールされる。
（ｆ）ジェネシス・ブロックは、同じままである。
【００５５】
上記で説明された（本発明的方法および本発明的システムを備える）プラットフォームは、バイオテクノロジー・ラボラトリに関係する選択された分野に適用された。そのようなアプリケーションの例が、以下で説明される。
【００５６】
移植のための電子ドナー登録
本発明的プラットフォームは、ラボラトリにおける組織提供患者を登録すること、および適切な文書の準備のためのウェブ・アプリケーションを配信するために適用された。システムは、組織ドナー登録のためのすべての必要なデータを完了することと、患者が提供することを可能にされ得るかどうかの決定を下すことと、実施されたテストおよびそれに関係する観測値を登録することとをも可能にする。システムのおかげで、チーム全体の作業を協調させることは容易である。
【００５７】
システムは、以下の３つのステップで動作させられる。
１．次のアプリケーション、すなわち、パーソナル・データ、収集されるべき組織のタイプ、または収集がそれにカバーされるべきリサーチ・プログラムと一緒のシステムへの患者の登録。
２．手順を続けるための承諾フォームのダウンロード可能な資格証明が、埋められ、これは、患者によって印刷および署名されなければならない。次いで、資格証明データの残りの要素が、埋められ、これは、特に、ラボラトリ・テストの結果および過去の病気を含む。このデータは検証され、患者が組織収集に対して可能にされるべきであるかどうかの決定が下される。
３．肯定的資格証明の場合、組織収集が実行される。ラボラトリにおける組織収集の後、収集データがシステムに入力され、それの番号が生成される。プロトコルを印刷し、協働エンティティのうちの１つに収集された組織を送る可能性がある。
【００５８】
バイオストレージ
本発明的プラットフォームは、薬剤製造業者の倉庫に貯蔵された材料、細胞静止薬ラボラトリ、ならびに薬局において準備された他のレセプション・ドラッグ、ＧＭＰおよびＧＬＰ規格の組織および細胞バンク・ラボラトリを管理するためのウェブ・アプリケーションを配信するために適用された。システムは、材料仕様を準備することによって、倉庫に貯蔵される各アイテムについて要件を定義することを可能にする。これのおかげで、アプリケーションは、倉庫に材料を放出する、貯蔵、送出、ならびになくなった材料を注文するプロセスにわたってステップバイステップでユーザを案内する。システムの固有の特徴は、中間材料の管理および文書化であり、これらは、ユーザのユニットにおいて開始材料から準備される。
【００５９】
システムは、以下の５つのステップで動作させられる。
１．倉庫に貯蔵される材料のリストを定義する。各々について、材料がそこから注文され得るサプライヤのリストを指定する。各材料について、品質仕様を開発し、そのような材料を獲得するためのテンプレートを記録する。
２．貯蔵のために材料を獲得する。サプライヤの記録および履歴を生成することによって、受け取った材料の互換性をそれの仕様とともに文書化する。ラベルを印刷し、放出された材料にそれを貼り、貯蔵エリア上の正しいロケーションにそれを置く。
３．在庫をチェックする。倉庫にある材料について警告リミットを設定すると、システムは、それらの有効期限が終わりに近づいている材料に関してユーザに通知する！ユーザが、短すぎる有効期限によって驚かされる前に、注文を生成する。

４．生産の準備をする！ユーザが、ユーザの製品／移植を生産する／処理するために必要とする材料のリストを定義する。ユーザが新しい注文の準備ができているかどうかをワンクリックでチェックする！
５．材料消費を管理する。倉庫に貯蔵された材料は、ユーザのビジネスの本質である特定の製品／移植に割り当てられ得る。これのおかげで、ユーザは、材料の使用について知り、容易に製品タイプ／移植に関するコスト、プロセスの持続時間、受け取った製品の量および従業員を分析する。

【００６０】

臨床試験

本発明的プラットフォームは、非商業的臨床試験においてＣＲＦ（症例報告書）を作成および管理するために使用されるウェブ・アプリケーションを配信するために適用された。アプリケーションは、スポンサー・リサーチ／ＣＲＯ（臨床リサーチ組織）、およびリサーチ・チームの両方のために設計される。調査（および／またはＣＲＯ）のスポンサーとして、ユーザは、新しい臨床試験のためのＣＲＦを迅速に作成し、ユーザは、臨床試験の進行を追跡し、モニタリング訪問を行うことが可能である。リサーチ・チームとして、ユーザは、治験参加者のＣＲＦに容易に記入することが可能である。

【００６１】

謝辞

この研究は、リサーチ・プロジェクト、すなわち、ブロックチェーン・テクノロジーに基づくバイオテクノロジーおよび診断ラボラトリにおける革新的なデータ・セキュリティ・システムの開発として、Ｍａｌｏｐｏｌｓｋａ　Ｒｅｇｉｏｎ　２０１４－２０２０についてＲｅｇｉｏｎａｌ　Ｏｐｅｒａｔｉｏｎａｌ　Ｐｒｏｇｒａｍｍｅによってサポートされた。契約番号：ＲＰＭＰ．０１．０２．０１－１２－０１８３／１８－００。

【００６２】

参考文献

１．Secure hash standard. Federal Information Processing Standard (FIPS)180-4(2012)
２．Angraal,S.、Krumholz,H.M.、Schulz,W.L.:Blockchain technology:applications in health care. Circulation:Cardiovascular Quality and Outcomes10(9)、e003800(2017)
３．Dworkin,M.J.:Sha-3 standard:Permutation-based hash and extendable-output functions. Federal Information Processing Standards (NIST FIPS)-202(2015)
４．Gallagher,P.:Digital signature standard (dss). Federal Information Processing Stan-dards Publications、volume FIPS 186-3ページ(2013)
５．Nakamoto,S.:Bitcoin:A peer-to-peer electronic cash system(2019)
６．Schneier,B.:The nsa is breaking most encryption on the internet blog post、september 2013
７．Stevens,M.、Bursztein,E.、Karpman,P.、Albertini,A.、Markov,Y.、Bianco,A.P.、Baisse,C.:Announcing the first shal collision. Google Security Blog (2017)
8.Zyskind,G.、Nathan,O.ら:Decentralizing privacy:Using blockchain to protect personal data. In:2015 IEEE Security and Privacy Workshops.180-184ページ.IEEE (2015)

【図１】

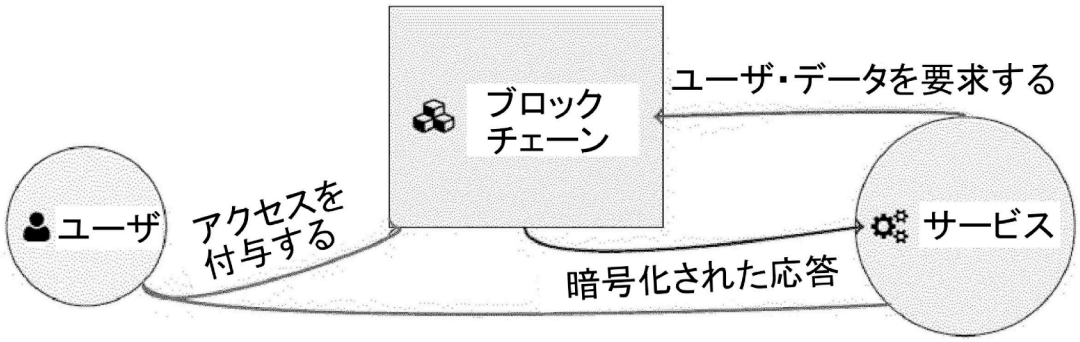

Fig. 1

【図２】

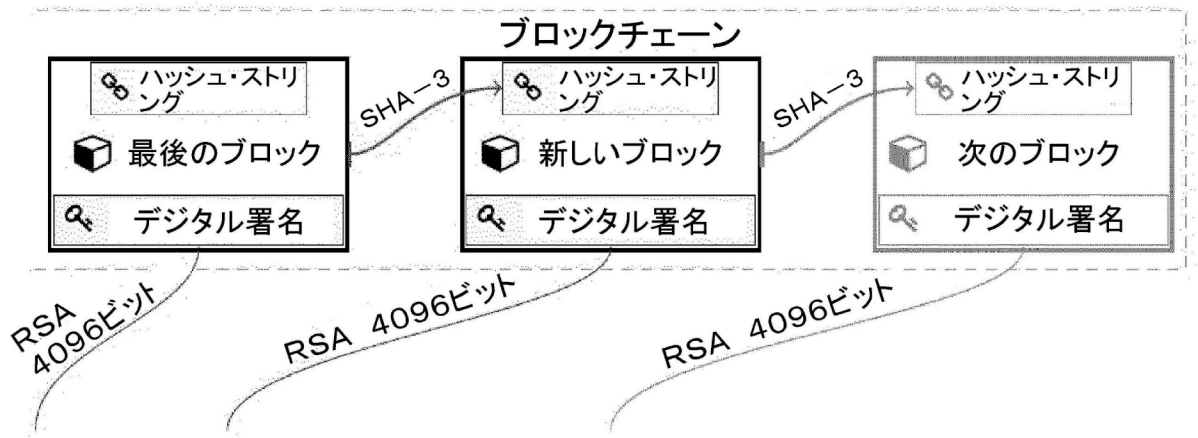

Fig. 2

【図３】

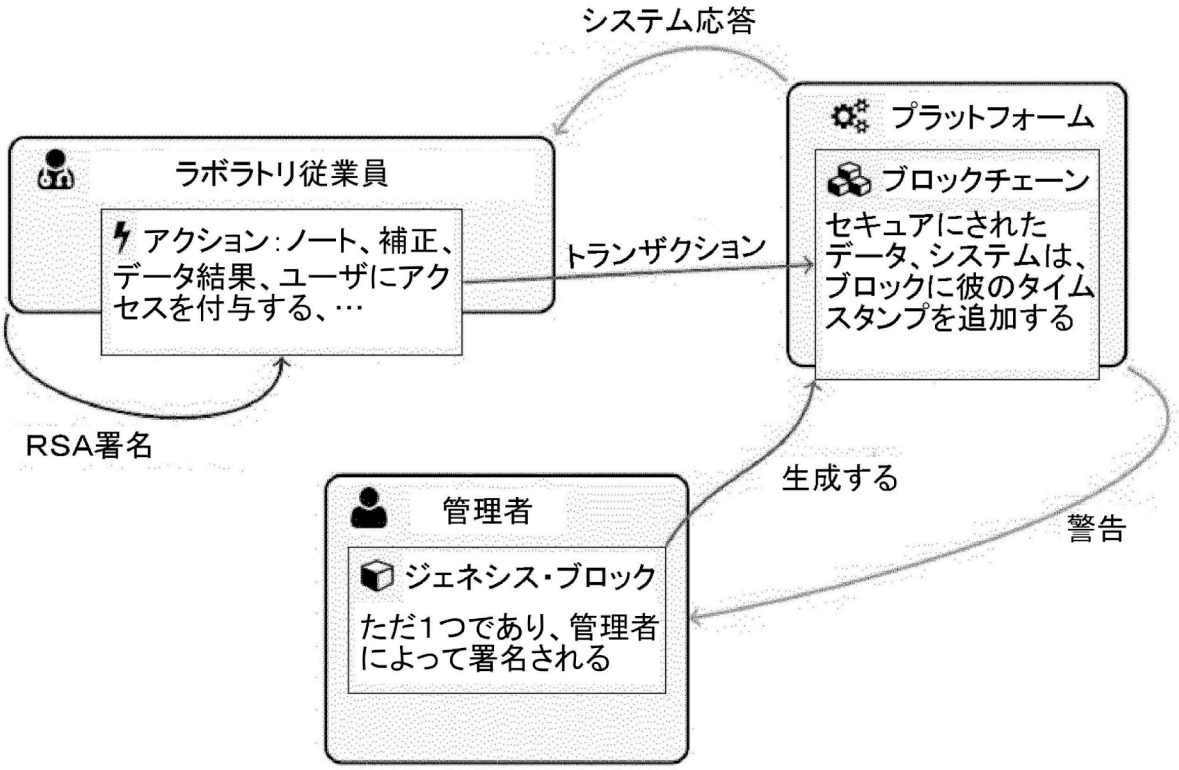

Fig. 3

【図４】

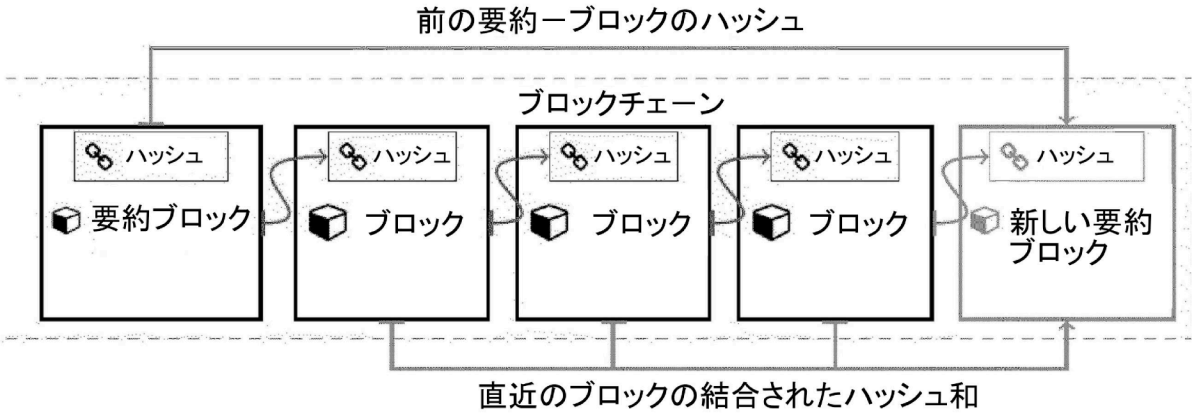

Fig. 4

【図５】

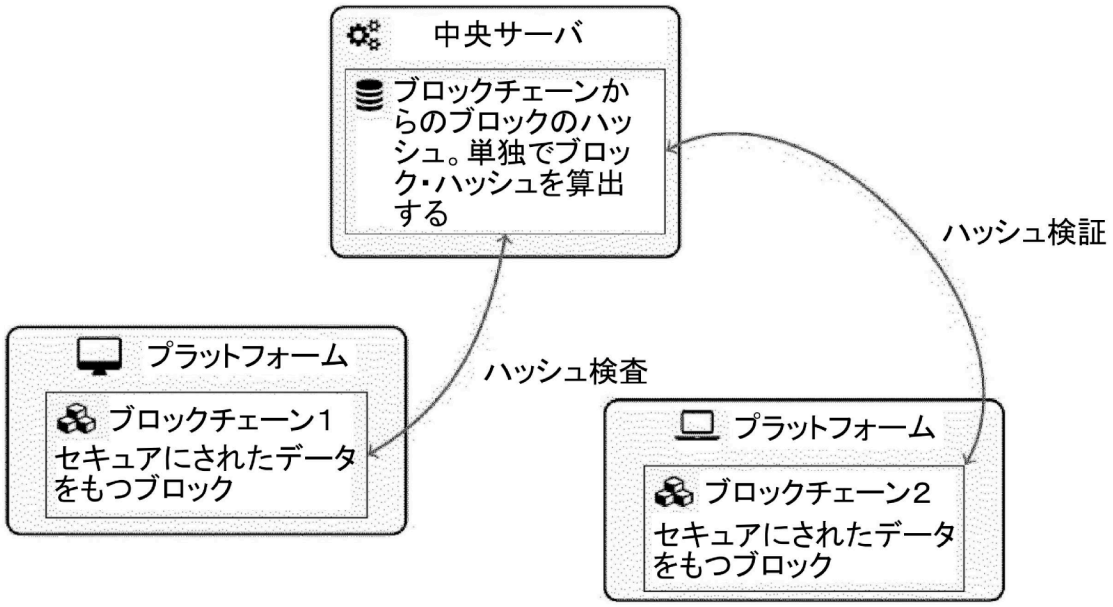
中央サーバ
ブロックチェーンからのブロックのハッシュ。単独でブロック・ハッシュを算出する
ハッシュ検証
ハッシュ検査
プラットフォーム
ブロックチェーン1
セキュアにされたデータをもつブロック
プラットフォーム
ブロックチェーン2
セキュアにされたデータをもつブロック

Fig. 5

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2020/082248

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L9/32
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, COMPENDEX, INSPEC, IBM-TDB, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2019/228560 A2 (ALIBABA GROUP HOLDING LTD [CN]) 5 December 2019 (2019-12-05) abstract figure 3 paragraph [0053] - paragraph [0075] -----	1-11
A	US 2019/294822 A1 (HENNEBERT CHRISTINE [FR]) 26 September 2019 (2019-09-26) abstract paragraph [0012] - paragraph [0023] figure 3 paragraph [0060] - paragraph [0100] -----	1-11

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 April 2021	22/04/2021

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Horn, Marc-Philipp

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2020/082248

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2019228560 A2	05-12-2019	CN 111183446 A	19-05-2020
		EP 3673446 A2	01-07-2020
		SG 11202002029V A	29-04-2020
		US 10880105 B1	29-12-2020
		WO 2019228560 A2	05-12-2019
US 2019294822 A1	26-09-2019	EP 3547202 A1	02-10-2019
		FR 3079323 A1	27-09-2019
		US 2019294822 A1	26-09-2019

フロントページの続き

(81)指定国・地域　AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,IT,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

(特許庁注：以下のものは登録商標)
１．ＰＹＴＨＯＮ

(72)発明者　スウザレツ　トマシュ
ポーランド　チェンストホヴァ　ウリツァ・オコルナ　８９ベ