(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7093340号
(P7093340)

(45)発行日　令和4年6月29日(2022.6.29)

(24)登録日　令和4年6月21日(2022.6.21)

(51)国際特許分類

Ｇ０６Ｑ　30/06　(2012.01)	Ｇ０６Ｑ	30/06	３５０
Ｇ０６Ｆ　21/62　(2013.01)	Ｇ０６Ｆ	21/62	

ＦＩ

請求項の数　17　（全20頁）

(21)出願番号　特願2019-502658(P2019-502658)
(86)(22)出願日　平成29年7月21日(2017.7.21)
(65)公表番号　特表2019-523493(P2019-523493A)
(43)公表日　令和1年8月22日(2019.8.22)
(86)国際出願番号　PCT/IB2017/054426
(87)国際公開番号　WO2018/020373
(87)国際公開日　平成30年2月1日(2018.2.1)
審査請求日　令和2年7月13日(2020.7.13)
(31)優先権主張番号　1613106.2
(32)優先日　平成28年7月29日(2016.7.29)
(33)優先権主張国・地域又は機関
英国(GB)
(31)優先権主張番号　1613107.0
(32)優先日　平成28年7月29日(2016.7.29)
最終頁に続く

(73)特許権者　318001991
エヌチェーン ホールディングス リミテッド
ＮＣＨＡＩＮ ＨＯＬＤＩＮＧＳ ＬＩＭＩＴＥＤ
アンティグア・バーブーダ、 セントジョンズ、 ４４ チャーチ ストリート、 フィッツジェラルド ハウス
Ｆｉｔｚｇｅｒａｌｄ Ｈｏｕｓｅ， ４４ Ｃｈｕｒｃｈ Ｓｔｒｅｅｔ， Ｓｔ． Ｊｏｈｎ’ｓ， Ａｎｔｉｇｕａ ａｎｄ Ｂａｒｂｕｄａ （ＡＧ）
(74)代理人　100107766
弁理士　伊東 忠重
(74)代理人　100070150
最終頁に続く

(54)【発明の名称】　ブロックチェーンにより実現される方法及びシステム

(57)【特許請求の範囲】
【請求項１】
インターネット対応リソースへのアクセス及び／又は利用を制御する方法であって、
ｉ）前記インターネット対応リソースへのアクセス及び／又は利用に関するスマートコントラクトを表すトークンと、ｉｉ）前記インターネット対応リソースのユーザから前記リソースのコントローラ及び／又は第三者に値を転送するための少なくとも１つの出力とを含む第１のブロックチェーントランザクションを生成するステップと、
前記リソースのユーザに関連する公開鍵を前記インターネット対応リソースに通信するステップであって、ストレージリソースへの前記公開鍵の記憶に応答して、第２のブロックチェーントランザクションが前記リソースの前記コントローラにより生成され、前記リソースのユーザに関連する前記公開鍵へのアクセスを得るために前記第２のブロックチェーントランザクションをアンロックするためにエスクローエージェントに属する公開鍵が要求される、ステップと、
秘密鍵を用いて暗号化されたメッセージ又は他のデータを前記リソースに通信するステップと、
前記リソースのユーザに関連する前記公開鍵を用いた前記メッセージ又は他のデータの解読の成功に応じて、前記インターネット対応リソースへのアクセス及び／又は利用を許可又は防止するステップと、
メモリから前記リソースのユーザに関連する前記公開鍵を削除し、第３のブロックチェーントランザクションを自動的に生成し、及び前記第３のブロックチェーントランザクシ

ョンをブロックチェーンネットワークに提出することにより、前記インターネット対応リソースへの更なるアクセス及び／又は利用を防止するステップであって、前記第３のブロックチェーントランザクションは、前記リソースへトークンを送信する出力を含み、前記トークンは、前記リソースのユーザに関連する公開鍵又は前記公開鍵のハッシュを表すか又は含む、ステップと、
を含む方法。
【請求項２】
前記第三者は、エスクローエージェントであり、及び／又は、
前記スマートコントラクトは、前記リソースへのアクセス又は利用のための合意に関する詳細又は条件を含み、及び／又は、
前記値の転送は、通貨額などの資金の支払いである、請求項１記載の方法。
【請求項３】
前記第１のブロックチェーントランザクションは、前記リソースのユーザに関連する公開鍵を表すトークンを含むリディームスクリプトを有する出力を含む、請求項１又は２記載の方法。
【請求項４】
前記公開鍵を表すトークンから前記公開鍵にアクセス又は取得し、それをメモリに格納するステップを含む、請求項３記載の方法。
【請求項５】
前記第１のブロックチェーントランザクションは、前記リソースのコントローラによって生成され、修正のために前記リソースのユーザに送信される、請求項１乃至４何れか一項記載の方法。
【請求項６】
前記リソースのユーザは、少なくとも１つの出力を前記第１のブロックチェーントランザクションに加えることによって前記第１のブロックチェーントランザクションを修正する、請求項５記載の方法。
【請求項７】
前記第１のブロックチェーントランザクションをブロックチェーンネットワークに送信するステップを含む、請求項１乃至６何れか一項記載の方法。
【請求項８】
前記暗号化されたメッセージは、好ましくは、携帯又はポータブル計算デバイスを用いて、前記リソースのユーザによって前記インターネット対応リソースに送信される、請求項１乃至７何れか一項記載の方法。
【請求項９】
前記第２のブロックチェーントランザクションのトークンによって表される公開鍵に基づき、メモリから前記ユーザの公開鍵の以前に格納されているバージョンを削除するステップを含む、請求項１記載の方法。
【請求項１０】
前記第２のブロックチェーントランザクションの出力を使う入力を含む第３のブロックチェーントランザクションを作成することによって、前記第２のブロックチェーントランザクションのトークンをトークン化解除するステップを含む、請求項１乃至９何れか一項記載の方法。
【請求項１１】
ブロックチェーンネットワークへの前記第１、第２及び／又は第３のブロックチェーントランザクションの送信は自動化され、好ましくは、前記送信の時間は、各ブロックチェーントランザクション内に備えられた指示又は設定に依存する、請求項１乃至１０何れか一項記載の方法。
【請求項１２】
前記第１のブロックチェーントランザクションは、
前記リソースのコントローラにデポジットの支払いを転送するための出力、及び／又は、

エスクローエージェントに支払いを転送するための出力
を含む、請求項１乃至１１何れか一項記載の方法。
【請求項１３】
前記公開鍵又はその場所への参照をストレージリソースに格納するステップであって、好ましくは、前記ストレージリソースは、分散ハッシュテーブル又は前記リソースによってアクセス可能であるか、関連して備えられるメモリである、格納するステップ、及び／又は、
前記メモリのリソースから前記公開鍵を削除し、ブロックチェーントランザクションのリディームスクリプトを利用して、他のブロックチェーントランザクションのトークン化された出力を使うことによって、前記インターネット対応リソースへの更なるアクセス及び／又は利用を防止するステップ、
を更に含む、請求項１乃至１２何れか一項記載の方法。
【請求項１４】
前記インターネット対応リソースは、ＩｏＴデバイスである、請求項１乃至１３何れか一項記載の方法。
【請求項１５】
請求項１乃至１４何れか一項記載の方法を実行するよう構成されるコンピュータにより実現されるシステム。
【請求項１６】
当該システムは、
好ましくはＩｏＴデバイス又は装置であるインターネット対応リソースと、
ブロックチェーンと、
好ましくはポータブル又は携帯計算デバイスである、リソースのユーザに関連付けされ、前記ユーザに関連付けされた暗号化鍵を格納するよう構成されるインターネット対応クライアントデバイスと、
を含む、請求項１５記載のシステム。
【請求項１７】
前記インターネット対応リソースは、ブロックチェーントランザクションを生成し、前記ブロックチェーントランザクションをブロックチェーンネットワークに提供するよう構成される、請求項１５又は１６記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に分散型台帳技術（ブロックチェーン関連技術を含む）に関し、特にデバイス、システム、サービス又は電子／デジタルリソースなどのリソースへのアクセスを制御する際におけるブロックチェーンの利用に関する。本発明は特に、インターネット対応デバイスへのアクセスを提供及び／又は禁止する際の利用に適している。それはまた、例えば、レンタルの状況など、リソースへの一時的なアクセスが所望される状況における利用に適している。本発明の態様はまた、インターネット・オブ・シングズ（ＩｏＴ）に関する。本発明は、ＩｏＴデバイスを制御するのに適するものであってもよい。
【背景技術】
【０００２】
本文書では、このコンテクストにおいて現在最も広く知られている用語であるため、参照の便宜及び容易のため、“ブロックチェーン”という用語を利用する。当該用語は、コンセンサスベースブロックチェーン、オルトチェーン、サイドチェーン及びトランザクションチェーン技術、パーミッション型及び非パーミッション型台帳、共有台帳及びこれらの変形を含む全ての形態の電子的コンピュータベース分散型台帳を含むようここでは利用される。
【０００３】
ブロックチェーンは、トランザクションから構成されるブロックから構成されるコンピュ

ータベースの非中央化された分散システムとして実現される電子台帳である。各トランザクションは、少なくとも１つの入力と少なくとも１つの出力とを含む。各ブロックは、それの開始以来ブロックチェーンに書き込まれてきた全てのトランザクションの永続的で修正不可なレコードを作成するために一緒にチェーン化されたブロックの前のブロックのハッシュを含む。トランザクションは、トランザクションの出力がどのようにして誰によってアクセス可能であるかを特定する入力及び出力に埋め込まれたスクリプトとして知られる小さなプログラムを含む。ビットコインプラットフォーム上では、これらのスクリプトはスタックベーススクリプト言語を用いて記述される。

【０００４】

トランザクションがブロックチェーンに書き込まれるために、それは、ｉ）トランザクションを受信した最初のノードによって検証され、トランザクションが検証された場合、ノードはそれをネットワークにおける他のノードに中継し、ｉｉ）マイナーによって構築された新たなブロックに追加され、ｉｉｉ）マイニング、すなわち、過去のトランザクションの公開台帳に追加される必要がある。

【０００５】

ブロックチェーン技術の最も広く知られているアプリケーションは、他のブロックチェーン実現形態が提案及び開発されてきたが、ビットコイン台帳である。ビットコインは便宜及び説明の目的のためにここでは参照されうるが、本発明はビットコインブロックチェーンによる利用に限定されず、他のブロックチェーン実現形態が本発明の範囲内に属することが留意されるべきである。

【０００６】

ブロックチェーン技術は、仮想通貨の実現形態の利用について最も広く知られている。しかしながら、より最近では、デジタル起業家は、ビットコインが基づいている暗号化セキュリティシステムの利用と、ブロックチェーンに格納可能なデータの利用との双方を用いて新たなシステムを実現することを始めている。

【０００７】

現在の興味及び研究の１つのエリアは、“スマートコントラクト”の実現のためのブロックチェーンの利用である。これらは、契約又は合意の条項の実行を自動化するよう設計されたコンピュータプログラムである。自然言語で記述される従来の契約と異なって、スマートコントラクトは、結果を生じさせるために入力を処理可能なルールを含み、これらの結果に応じてアクションを実行させることが可能なマシーン実行可能なプログラムである。

【０００８】

ブロックチェーン関連の興味の他のエリアは、ブロックチェーンを介し実世界のエンティティを表現及び転送するための“トークン”（又は“カラードトークン”）の利用である。潜在的に機密又は秘密のアイテムは、区別可能な意味又は値を有さないトークンによって表現できる。従って、トークンは、実世界アイテムが参照されることを可能にする識別子として機能する。

【０００９】

本発明はまた、リソースへのアクセスを制御するためのブロックチェーンにより実現される機構の利用に関する。このリソースは、“インターネット・オブ・シングズ（ＩｏＴ）”デバイスとすることができる。ＩｏＴは、Ｗｉｋｉｐｅｄｉａによって、“物理デバイス、車両、建物及びエレクトロニクス、ソフトウェア、センサと共に埋め込まれた他のアイテムのネットワークと、これらのオブジェクトがデータを収集及び交換することを可能にするネットワーク接続であり、・・・ＩｏＴは、オブジェクトが既存のネットワークインフラストラクチャを介し遠隔的に検知及び制御されることを可能にする”として説明されている。

【００１０】

本発明は、添付した請求項に規定される。

【００１１】

本発明は、方法及び／又はシステムを提供しうる。それは制御方法／システムであっても

よい。それは、コンピュータにより実現される方法／システムであってもよい。それは、ブロックチェーンにより実現される方法／システムであってもよい。それは、ブロックチェーントランザクションを利用するよう構成されうる。それは、ブロックチェーンプロトコルを利用するよう構成されうる。本発明は、リソースへのアクセス又は利用の制御を実現するよう構成されうる。従って、本発明は、リソースの一時的な制御を提供するよう構成されうる。それは、リソースへのアクセス／利用を許可及び／又は拒絶するよう構成されうる。

【００１２】

リソースは、インターネット対応リソースであってもよい。それは、インターネット・オブ・シングズ（ＩｏＴ）リソースであってもよい。それは１つ以上のデバイスであってもよい。それは、車両、建物又は機械であってもよい。インターネット対応リソースは、リソースプロバイダによって提供、所有、管理されてもよい。

【００１３】

本発明は、検証又は認証方法／システムを提供しうる。本発明は、少なくとも１つの暗号化鍵の利用に関するものであってもよい。これは、公開／秘密鍵ペアであってもよい。暗号化鍵は、共有秘密を利用して生成されうる。

【００１４】

本発明は、リソースの状態又は機能をロック／アンロック、可能又は不可、実行又はシャットダウン、若しくは操作するよう構成されうる。本発明は、ユーザによるリソースへの一時的なアクセス／利用を制御するよう構成されうる。本発明は、レンタル又は貸出処理を実現するよう構成されうる。当該処理の少なくとも一部は、契約において実現、規定及び／又は説明されうる。これは、コンピュータにより実行可能なスマートコントラクトであってもよい。

【００１５】

本発明は、インターネット対応リソースへのアクセス及び／又は利用を制御する方法であって、第１のブロックチェーントランザクション（ＴｘＢ）を生成するステップを含む方法を含んでもよい。当該ステップは、リソースのコントローラによって実行されてもよい。ＴｘＢは、リソースのユーザに関連する公開鍵を表すトークンを含むリディームスクリプトを含む出力を含む不完全な形式で生成されうる。（リソースのユーザは、コントローラに以前に提供された公開鍵を有してもよい。）コントローラは、修正及び／又は記入のためリソースのユーザに不完全なトランザクションＴｘＢを送信してもよい。

【００１６】

リソースは、コントローラからの受信に応答して、第１のトランザクション（ＴｘＢ）を修正又は記入してもよい。

【００１７】

第１のトランザクション（ＴｘＢ）は、
ｉ）インターネット対応リソースへのアクセス及び／又は利用に関するスマートコントラクトを表すトークン、及び／又は、
ｉｉ）インターネット対応リソースのユーザからリソースのコントローラ及び／又は第三者に値を転送するための少なくとも１つの出力とを含んでもよい。

【００１８】

それはまた、リソースのユーザに関連する公開鍵をインターネット対応リソースに通信するステップを含んでもよい。公開鍵は、暗号化鍵であってもよい。それは、公開／秘密鍵ペアの一部を構成してもよい。

【００１９】

それはまた、秘密鍵を用いて暗号化されたメッセージ又は他の形式のデータをリソースに通信するステップを含んでもよい。これは、暗号化鍵であってもよい。それは、公開／秘密鍵ペアの一部を構成してもよい。

【００２０】

それはまた、公開鍵を用いたメッセージの解読の成功に応じて、インターネット対応リソ

ースへのアクセス及び／又は利用を許可又は防止するステップを含んでもよい。
【００２１】
第三者は、エスクローエージェントであってもよい。スマートコントラクトは、リソースへのアクセス又は利用のための合意に関する詳細又は条件を含んでもよい。値の転送は、通貨額などの資金の支払いであってもよい。通貨は、例えば、ビットコインなどの仮想通貨であってもよい。
【００２２】
第１のブロックチェーントランザクションは、リソースのユーザに関連する公開鍵を表すトークンを含むリディームスクリプトを有する出力を含んでもよい。
【００２３】
当該方法は更に、トークンから公開鍵にアクセス又は取得し、それをメモリに格納するステップを含んでもよい。当該ステップは、インターネット対応リソースによって実行されてもよい。鍵はＩｏＴデバイス内又は接続されたメモリに格納されてもよい。
【００２４】
リソースのユーザは、ソースから第１のトランザクションを受信してもよい。それは、部分的に記入された形式で受信されてもよい。それは、リソースコントローラから受信されてもよい。リソースのユーザは、１つ以上の入力及び／又は１つ以上の出力を挿入することによって、第１のトランザクションを修正してもよい。
【００２５】
第１のトランザクションは、リソースのコントローラによって生成され、修正のためにリソースのユーザに何れかによって送信されてもよい。リソースのユーザは、少なくとも１つの出力を第１のトランザクションに加えることによって第１のブロックチェーントランザクションを修正してもよい。リソースのユーザは、それが、
・ブロックチェーン上の他の（以前の）トランザクションから仮想通貨の一部を使う入力、及び／又は、
・第三者に仮想通貨の一部を転送する出力、好ましくは、当該出力はまたトークン化された契約（すなわち、契約を表すトークン）を転送する、及び／又は、
・リソースのコントローラに仮想通貨の一部を転送する出力、及び／又は、
・リソースのユーザにおつりとして仮想通貨の一部を戻す出力
を含むように、第１のトランザクションを修正してもよい。
【００２６】
当該方法は、第１のトランザクションをブロックチェーンネットワークに送信するステップを含んでもよい。
【００２７】
暗号化されたメッセージは、リソースのユーザによってインターネット対応リソースに送信されてもよい。それは、スマートフォンなどの携帯又はポータブル計算デバイスを利用してユーザによって送信されてもよい。ａｐｐが、この目的のためにユーザの（クライアント）デバイスにインストールされてもよい。
【００２８】
当該方法はまた、ブロックチェーンネットワークに第２のトランザクションを送信するステップを含み、第２のトランザクションは、リソースにトークンを送信する出力を含み、トークンは、リソースのユーザに関連する公開鍵又は公開鍵のハッシュを表すか、又は含んでもよい。当該方法はまた、第２のトランザクションのトークンによって表される公開鍵に基づき、メモリからユーザの公開鍵の以前に格納されているバージョンを削除するステップを含んでもよい。これは、トークンによって提供される鍵の格納されているバージョンを検索することによって実現されうる。当該方法はまた、第２のトランザクションの出力を使う入力を含む第３のトランザクションを作成することによって、第２のトランザクションのトークンをトークン化解除するステップを含んでもよい。
【００２９】
ブロックチェーンネットワークへの第１、第２及び／又は第３のトランザクションの送信

は自動化されてもよい。送信の時間は、各トランザクション内に備えられた指示又は設定に依存してもよい。これは、ＣＬＴＶ指示若しくは機構、又は機能的に実質的に等価である他の機構であってもよい。

【００３０】

第１のブロックチェーントランザクションは、リソースのコントローラにデポジットの支払いを転送するための出力を含んでもよい。さらに又はあるいは、それは、エスクローエージェントに支払いを転送するための出力を含んでもよい。

【００３１】

当該方法はまた、公開鍵又はその場所への参照をストレージリソースに格納するステップを含んでもよい。ストレージリソースは、分散ハッシュテーブル又はリソースによってアクセス可能であるか、関連して備えられるメモリであってもよい。

【００３２】

当該方法はまた、メモリのリソースから公開鍵を削除し、及び／又は、ブロックチェーントランザクションのリディームスクリプトを利用して、他のブロックチェーントランザクションのトークン化された出力を使うことによって、インターネット対応リソースへの更なるアクセス及び／又は利用を防止するステップを含んでもよい。

【００３３】

本発明は、インターネット対応リソースへのアクセス及び／又は利用を制御する方法を提供しうる。当該方法は、メモリに格納されている公開鍵に対応する秘密鍵の提供によって、インターネット対応リソースへのアクセス及び／又は利用を許可するステップを含みうる。公開鍵は、リソース内、リソース上又はリソースに接続されるメモリに格納されてもよい。さらに又はあるいは、それは、インターネット対応リソースから遠隔である又は別の場所に格納されてもよい。

【００３４】

さらに又はあるいは、当該方法は、メモリから公開鍵を削除することによって、インターネット対応リソースへのアクセス及び／又は利用を防止するステップを含んでもよい。

【００３５】

さらに又はあるいは、アクセス及び／又は利用を防止するステップは、第２のブロックチェーントランザクションのリディームスクリプト（ｒｅｄｅｅｍ　ｓｃｒｉｐｔ）を利用して、第１のブロックチェーントランザクションのトークン化（ｔｏｋｅｎｉｓｅｄ）された出力を使うことを含んでもよい。

【００３６】

本発明はまた、上述した方法の何れかの実施例を実行するよう構成されるコンピュータにより実現されるシステムを提供する。

【００３７】

本発明は、命令、フラグ、コード、オペコード又はコンピュータコードの一部（便宜上、“タイムロック機構”として参照する）を利用して、ブロックチェーンネットワークにトランザクションをブロードキャストし、及び／又はトランザクションの出力が利用可能な日付及び／又は時間を指定するステップを含んでもよい。これは、例えば、ビットコインＣｈｅｃｋＬｏｃｋＴｉｍｅＶｅｒｉｆｙ（ＣＬＴＶ）処理又は機能的に類似又は等価な機構を利用して実現されてもよい。さらに及び／又はあるいは、タイムロック機構は、適切に構成された計算エージェントを利用して実現されてもよい。トランザクションは、第１、第２及び／又は第３のトランザクションであってもよい。タイムロック機構は、トランザクションをブロックチェーンネットワークにブロードキャストするか、あるいは、例えば、リソースへのアクセス又は制御が許可、拒絶、変更又は取消される時間などの特定の時間に出力を使うのに利用可能である。タイムロック機構は、リソースユーザ、リソースプロバイダ又は第三者によって指定されてもよい。

本発明によるシステムは、

好ましくはＩｏＴデバイス又は装置であってもよいインターネット対応リソース、

ブロックチェーン、及び／又は、

ユーザに関連付けされ、ユーザに関連付けされた暗号化鍵を格納するよう構成されるインターネット対応デバイスを含んでもよい。（クライアント）デバイスは、ポータブル又は携帯計算デバイスであってもよい。

【００３８】

クライアントデバイスは、スマートフォン、タブレットコンピュータ又はラップトップであってもよい。クライアントデバイスは、公開及び／又は秘密暗号化鍵を生成するよう構成されてもよい。それは、秘密の値を利用してこれを実行してもよい。クライアントデバイスは、“ａｐｐ”などのソフトウェアを実行するよう構成されてもよい。ａｐｐは、リソースとやりとりして通信するよう構成されてもよい。それは、セキュアな方法で暗号化鍵を格納するよう構成されてもよい。それは、鍵を利用してメッセージを暗号化するよう構成されてもよい。それは、暗号化されたメッセージをリソースに通信するよう構成されてもよい。これは、無線通信チャネル及び／又はプロトコルを介し実現されてもよい。ａｐｐは、サーバ上に備えられた他のソフトウェアリソースと通信するよう構成されてもよい。サーバは、リソースプロバイダによって又はために運営されてもよい。サーバはウェブサイトを運営してもよい。ウェブサイトは、ユーザがインターネット対応リソースを制御、アクセス及び／又は利用する関心を登録することを可能にしてもよい。サーバサイドのソフトウェアは、スマートコントラクトを生成するよう構成されてもよい。スマートコントラクトは、インターネット対応リソースへのアクセス／利用に関する条項及び／又は条件を含んでもよい。

【００３９】

インターネット対応リソースは、ブロックチェーントランザクションを生成し、トランザクションをブロックチェーンネットワークに提供するよう構成されてもよい。

【００４０】

本発明の一態様又は実施例に関して説明される何れかの特徴は、本発明の他の何れかの態様又は実施例に等しく適用可能であってもよい。当該方法に関して説明される何れかの特徴はまた、システムに適用されてもよいし、その反対であってもよい。

【００４１】

本発明は、レンタルのシナリオに関する以下の例示的な実施例において実質的に説明されるような方法及び／又はシステムを提供しうる。

【００４２】

本発明の上記及び他の態様は、ここに説明される実施例から明らかであり、参照して解明されるであろう。本発明の実施例は、添付した図面を参照して例示的に説明される。

【図面の簡単な説明】

【００４３】

【図１ａ】本発明の例示的な実施例によるシステムを示す。

【図１ｂ】実施例によるシステムを利用して自動車の貸出に関連するステップを示すフローチャートを提供する。

【図２】本発明の実施例を実現するのに利用されうる複数のトランザクションと各自の入力／出力とを示す。

【図３ａ】インターネット対応自動車へのアクセスを可能にするのに利用される第１のブロックチェーントランザクションを示す。

【図３ｂ】インターネット対応自動車へのアクセスを可能にするのに利用される第１のブロックチェーントランザクションを示す。

【図４】自動車へのアクセスを削除するのに利用される第２のブロックチェーントランザクションを示す。

【図５】自動車へのアクセスを制御するのに利用される第３のブロックチェーントランザクションを示す。

【図６】具体例の自動車貸出処理に利用される仮想通貨の量をトークン化解除するのに利用される第４のブロックチェーントランザクションを示す。

【発明を実施するための形態】

【００４４】
本発明は、リソースへの一時的なアクセスを提供、終了及び制御する機構を提供する。効果的には、それは、ブロックチェーンプロトコルを利用して、インターネットへのアクセスを有するユーザがリソースとやりとりすることを可能にする。これは、何れのタイプのリソースとすることも可能であるが、本例では、リソースはインターネット対応レンタカーである。当該方法は、ブロックチェーンプロトコルと共に利用可能な全範囲のトランザクションの可能性、すなわち、通常（例えば、ビットコイン）のトランザクション、スマートコントラクト及び“カラードコイン”（トークン化された）トランザクションを利用する。
【００４５】
説明のみの目的のため、本発明が車両レンタルサービスに利用される具体例を提供する。自動車レンタルサービスは、数時間から数ヶ月までの範囲の特定の期間において車両をレンタルすることに関する広範なサービスを含む。これらのサービスはしばしば、オンライン予約及びスマートフォンアプリケーションを通じてウェブサイトを介し提供される。高速インターネットアクセスと結びついたスマートフォン技術の急速な普及による顧客の嗜好の変化は、産業の成長の要因であるキーファクタの１つである。しかしながら、自動車レンタル処理の当該具体例は限定的であることを意図していないことが留意されるべきである。本発明は、あるタイプのリソースへの一時的なアクセスが制御される必要がある他のコンテクスト及びアプリケーションにおいて等しく利益を有する。ここで説明される基礎となるインフラストラクチャは、永続的なレコードが所望され、２つ以上の主体が何れかのタイプのアクセス関連の合意、例えば、居住用財産の貸出のための契約などを実現することを所望する各種トランザクションについて利用可能である。
【００４６】
本発明は、ユーザがやりとりするのに極めて便利である改良されたアクセス解決策を提供する。それは、ユーザ（例えば、借り手）がアクセスを実施又は終了するため、所定の位置に物理的に行くことを必要としない。例えば、従来のレンタル状況では、借り手は自動車又は財産の鍵を収集し、又は契約などに署名するため、レンタルオフィスに行く必要があった。本発明は、スマートフォンなどの計算デバイスが自動車／家の鍵などのアクセス機構として機能することを可能にするため、この問題を回避する。さらに、ソフトウェアアプリケーションの本発明の内蔵は、検索能力を提供し、ユーザが詳細を登録することを可能にする。
【００４７】
本発明の１つの重要な側面は、それがブロックチェーンネットワークにブロックチェーントランザクションをブロードキャストし、及び／又は出力が指定された時間に使用可能になるための機構を利用可能であることである。例えば、ビットコインＣｈｅｃｋＬｏｃｋＴｉｍｅＶｅｒｉｆｙ（ＣＬＴＶ）機構は、トランザクションにおいて利用可能である。本発明に関して、これはそれが契約の実行を自動化するのに利用可能であるため、効果的でありうる。例えば、それは、リソースへのアクセス又は利用がいつ付与、変更又は拒絶可能であるかを制御するのに利用可能である。
【００４８】
リソースはインターネット・オブ・シングズ（ＩｏＴ）デバイスを利用して、リソース関連機能などの可能な機能の範囲を実行することに留意することが重要である。ユーザの暗号化鍵（ＰｕｂＫｅｙ）は、アクセスを付与するため、格納用のリソースに通信される。この鍵は、更なるアクセスを禁止するため、リソースのメモリから以降に削除される。ＩｏＴデバイスは、プログラマブル“ブロックチェーンＩＯＴデバイス（ＢＩＤ）”であり、すなわち、それは、ブロックチェーンネットワークをモニタ、やりとり及びそれに公開することが可能なインターネット対応デバイスである。本発明はまた通信プロトコルを含む。好適な実施例では、これはソフトウェアアプリケーション（ａｐｐ）を介したリソースとの通信を可能にする。
【００４９】

図１ａは、本発明の例示的な実施例によるシステム１００を実現するのに利用されるシステム１００を示す。しかしながら、当業者は、システム１００に対する変形が本発明の範囲内に依然として属する一方、可能であることを理解するであろう。

【００５０】

システム１００は、

・自動車をレンタルするのに顧客によって利用されるウェブサイトを運営するサーバ１０２

・ブロックチェーンＩｏＴデバイス（ＢＩＤ）１０６を含むＩｏＴデバイス１０４を有する自動車１１０

・ニアフィールド通信、Ｂｌｕｅｔｏｏｔｈ（登録商標）又は他の何れか適切であって、好ましくは無線伝送プロトコルを利用してＩｏＴデバイス１０４を介し自動車１１０にメッセージを送信するよう構成されるスマートフォン又はタブレット、ラップトップなどの他の計算デバイス１０８

を有する。

【００５１】

本例では、“ブロックチェーンＩＯＴデバイス（ＢＩＤ）”は、オフＢＩＤでセキュアに格納され、暗号化鍵を介しアクセスされる所定の指示を実行するようセットアップされた計算エージェントである。“オフＢＩＤ”によって、当該指示がＢＩＤ自体内には備えられず、他の何れかに格納され、必要に応じてアクセスされることを意味する。これらの指示は選択され、選択された１つ以上のタスクを実行するよう構成される。実行時、当該指示はＩＯＴデバイスの動作を制御及び影響を与えることが可能である。ＢＩＤは、ＩＯＴデバイス自体に配置されてもよく、それは、ＢＩＤがＩＯＴデバイスに備えられたメモリにインストールされることを意味する。しかしながら、他の実施例では、ＢＩＤはオフデバイスに配置され、デバイスとのインターネット接続を有してもよい。

【００５２】

ＩＯＴデバイスは、他のデバイス又はＤＨＴなどとセキュアに通信及びやりとりできるように、それ自体の暗号化鍵（ＩＰアドレスと共に）を有する。それの“オペレーティングシステム”は、（少なくとも、限定することなく）

・暗号化計算

・外部ソース（ＤＨＴなど）からの指示の抽出

・切り替えスイッチ（すなわち、物理的ＩＯＴデバイス上のように）などのシンプルなアクションの実行

のための埋め込み機能を備えたシンプルで汎用的なシステムである。

【００５３】

従って、ＩＯＴデバイスとそれに関連するＢＩＤの何れも自らのビルトインされた指示を含まず、それが何を実行するか、又はそれをどのように実行するかについて“知らない”。ＢＩＤは、他の何れかから指示をセキュアに抽出するための機構しか有さない。ＢＩＤは（以下は限定的でなく例示的である）、

・自らのマスタ秘密及び公開鍵ペアへのアクセス；それはまた自らの（導出可能な）ＢＴＣアドレスを有する

・データをＩＰアドレスに送信し、又はＩＰアドレスからデータを受信する能力

・秘密共有プロトコル計算－好適な実施例では、これらは機械コードに埋め込まれてもよい

・ブロックチェーンイベントの検索及び解釈

・それに付属された（本質的には単なるスイッチのセットである標準的なＡＰＩを介し）物理的デバイスの実行及び制御

のシンプルなアクションのセットのみを実行可能である。

【００５４】

ＢＩＤの入出力の通信は、鍵が共有された秘密を用いて作成されることを可能にするセキュリティ機構を利用して暗号化可能である。これは、

（ｉ）“ハッキング”からのより強力なセキュリティ

（ｉｉ）シンプルで汎用的なソフトウェアアップグレードプロトコル

（ｉｉｉ）デバイスアグノスチズム（ｄｅｖｉｃｅ　ａｇｎｏｓｔｉｃｉｓｍ）
を可能にする。
【００５５】
ここで、システム１００を利用した自動車レンタル処理の各種フェーズを、図２に示されるような（ビットコイン）トランザクションのチェーンを参照して説明する。レンタル処理は、
１．フェーズ１：レンタル合意が参加する主体間で設定される。
２．フェーズ２：リソースへのアクセスが許可される、すなわち、顧客がリソースを利用する。
３．フェーズ３：契約がある理由から終了した、例えば、契約の条項による時間で期限切れとなった、又はレンタカーの返却などの終了イベントが行われたなどのため、特定のリソースへのアクセスが取り除かれた、
という３つの“フェーズ”を用いて説明される。
【００５６】
フェーズ１：契約の設定
図１ｂ及び２を参照されたい。本例では、リソースプロバイダは自動車レンタル企業であり、リソースはインターネット対応コンピュータをボード上に有する車両である。顧客（本例では“ユーザ”又は“借り手”として参照されうる）は、貸出企業とのレンタルの合意に入力するための彼女の希望を通知するため、プロバイダのウェブサイトを介し彼女の注文の詳細を入力する。顧客は、貸出企業に彼／彼女の公開鍵を提供する。公開鍵は、当該分野において知られるような暗号化鍵ペアを一緒になって構成する対応する秘密鍵を有する。図１ｂのステップＳ１００を参照されたい。
【００５７】
これに応答して、自動車貸出企業は新たな契約を生成する。これは、機械実行可能な“スマートコントラクト”（以降、単に“契約”として参照される）である。スマートコントラクトは当該分野において知られている。自動車貸出企業は、図１ｂのステップＳ１０２において、公衆に利用可能な分散ハッシュテーブル（ＤＨＴ）にそれを公開することによって、契約を共有する。契約は、例えば、ピックアップ及び返却時間、モデル車両の詳細などの自動車貸出の条項を含む。顧客には契約の場所が通知され（又は、それのコピーが送信され）、これにより、顧客は当該条項及び条件を閲覧し、彼／彼女が進めることを所望するか決めることができる。本例では、自動車レンタルのコストは１０ビットコイン（ＢＴＣ）であると仮定する。
【００５８】
効果的には、ＤＨＴに関する契約の登録がまた、第三者が当該文書にアクセスし、紛争の場合には条項を確認することを可能にする。しかしながら、いくつかの実施例では、セキュリティ機構は、許可された個人又はグループに契約へのアクセスを制限するのに利用されてもよく、例えば、パスワード又は他の形態の認証が必要とされてもよい。
【００５９】
自動車貸出企業による提案されるトランザクションＴｘＢの生成
当該企業はまた、（ブロックチェーンネットワークでなく）顧客に送信されるブロックチェーントランザクション（ＴｘＢ）を生成する。図３ａの提案されるトランザクションＴｘＢを参照されたい。レンタルの合意が実現されるために、借り手は貸出企業によって準備されたトランザクションＴｘＢを記入する必要がある。提案されるトランザクションは、トークン（又は“カラードコイン”）を含む。ここでは、“トークン”又は“カラードコイン”という用語は互換的に利用される。当該技術において知られるように、トークンはあるメタデータを含むことによって“通常の”ブロックチェーントランザクションを介しデータを搬送するのに利用可能である。これは、ある固有の値（例えば、ビットコイン）を提供し、出力のロックスクリプトのメタデータ内にトークンを含む出力を含めることによって実現される。本ケースでは、Ｏｕｔｐｕｔ　０のスクリプトは、顧客の公開鍵のハッシュを含むメタデータを含む、トークン化されたコインは、レンタカーに属するブロックチェー

ンアドレスを用いて使うことができる。従って、自動車は、合意が実現されるとトークンを介し顧客の公開鍵にアクセス可能である。これは、図１ｂのステップ１０２に示される。
【００６０】
従って、提案されるＴｘＢは、借り手とのレンタル合意に入力するためのレンタル企業の意思の確認として機能し、また借り手の公開鍵に関して自動車が知るための方法を提供する。提案されるＴｘＢはまた、自動車にアドレス指定された出力（Ｏｕｔｐｕｔ　１）と彼女の公開鍵のハッシュとを含むトランザクションを借り手が閲覧することを可能にする。
【００６１】
提案されるトランザクションＴｘＢが借り手に送信されると、それは、１つの入力（Ｉ０）及び１つの出力（Ｏ０）を有する。入力は前のトランザクションの出力を使い（図２における破線のボックスに示されるような）、自動車レンタル企業のデジタルシグネチャによって署名される。
【００６２】
提案されるブロックチェーントランザクションＴｘＢの第１の入力（Ｉ０）は、入力及び出力がＴｘＢに追加されることを可能にするＳＩＧＨＡＳＨフラグＳＩＧＨＡＳＨ＿ＮＯＮＥ｜ＳＩＧＨＡＳＨ＿ＡＮＹＯＮＥＣＡＭＰＡＮＹを含む。ＳＩＧＨＡＳＨ＿ＮＯＮＥの利用は、誰もそれを変更できない点で入力をプロテクトする。しかしながら、借り手は出力を変更可能である。
【００６３】
当該出力Ｏ０のロックスクリプトは、借り手の公開鍵のハッシュを含む。ロックスクリプトは、以下を含む。
【００６４】
【表１】

OP_HASH160 <hash160(redeem script)> OP_EQUAL

ＴｘＢの出力O_0をアンロックするため、以下のリディームスクリプトが必要とされる。

【００６５】
【表２】

OP_1 <metadata hash (renter’s public key)> <car’s public key> OP_2 OP_CHECKMULTISIG

スクリプトにおけるこのメタデータは、セットアップ処理が完了したとき、自動車が借り手の公開鍵にアクセスすることを可能にする“カラードコイン”を含む。
【００６６】
<u>自動車貸出企業によるトランザクションＴｘＢ’の生成</u>
自動車貸出企業がＤＨＴに契約文書を送信すると、それはまた、借り手の公開鍵のハッシュを含む新たな文書を生成し、それをＤＨＴと共有する。ＴｘＢ’は、それに添付されたカラードコインを有する出力を含むブロックチェーントランザクションである。図５を参照されたい。カラードコインは、借り手の公開鍵の場所をエスクローエージェントに通知するのに利用される。これは、後述されるように、レンタル処理の終了フェーズについて必要とされる。ＴｘＢ’のリディームスクリプトは、
【００６７】

【表３】

OP_1 <metadata of hash (renter's public key)> <escrow's public key> OP_2 OP_CHECKMULTISIG.

として与えられる。

【００６８】

従って、エスクローの公開鍵は、ＴｘＢ’をアンロックし、借り手の公開鍵へのアクセスを取得するのに必要とされる。

【００６９】

顧客によるＴｘＢの記入

顧客が自動車レンタルに進むことを所望した場合、彼は前のトランザクション（ＴｘＡ）から彼女が所有するビットコイン（又は他のデジタル通貨）を使う。図１ｂ及び図２のステップ１０４を参照されたい。前の出力のコインの価値は１５ＢＴＣであり、車両レンタルのコストは１０ＢＴＣであると仮定する。

【００７０】

このとき、借り手は、借り手によって署名された入力（Ｉ１）を加えることによって提案されるＴｘＢに記入する。Ｉｎｐｕｔ　１は、ＴｘＡから１５ＢＴＣを使う（図１ｂのステップ１０４を参照されたい）。借り手はまた、

（ｉ）マルチシグネチャアドレスへの９ＢＴＣの固有の価値を有する１つのトークン化されたコイン－Ｏｕｔｐｕｔ　１

（ｉｉ）企業へのデポジットとしての１ＢＴＣ－Ｏｕｔｐｕｔ　２

（ｉｉｉ）彼女への５ＢＴＣの返却－Ｏｕｔｐｕｔ　３

を支払う３つの出力をトランザクションＴｘＢに加える。

【００７１】

図３ｂにおいて、記入されたバージョンのＴｘＢが示される。ＴｘＡが自動車レンタルのコストと同じ値の出力を有していた場合、顧客に返却されるおつりの必要はないことに留意されたい。

【００７２】

契約がＤＨＴに登録されると、関連するＵＲＩ及びハッシュ数がスクリプトにおけるメタデータ内のカラードコインを用いて表現できる。これは、トランザクションが契約に関連付けされることを可能にし、セキュリティ許可がそれを許可した場合、契約が参照及びアクセスされることを可能にする。

【００７３】

ＴｘＢのＯｕｔｐｕｔ　１のリディームスクリプトは、

【００７４】

【表４】

OP_2 <metadata contract> <renter's public key> <company's public key> <escrow's public key> OP_4 OP_CHECKMULTISIG

である。

【００７５】

トランザクションＴｘＢのアノテートされた具体例を提供する図３ｂにおいて、ＴｘＢの出力Ｏ０及び出力Ｏ１の異なる２つのリディームスクリプトが示される。

【００７６】

“借り手の公開鍵”は、自動車を借りている顧客の公開鍵である。“自動車の公開鍵”は、貸し出し中の自動車の公開鍵である。“企業の公開鍵”は、自動車レンタルを実施している企業の公開鍵である。“エスクローの公開鍵”は、エスクローエージェントの公開鍵である。

【００７７】

契約を表すトークンは、借り手のシグネチャ、企業のシグネチャ及びエスクローエージェントのシグネチャを含む２オブ３（２－ｏｆ－３）マルチシグネチャアドレスである。マルチシグネチャトランザクションは、資金が転送されるため、複数のシグネチャを必要とする。本シナリオでは、２オブ３マルチシグネチャ機構は、借り手が潜在的な署名者として指定された第三者仲介者（エスクローエージェント）及びレンタル企業にトランザクションへの資金を提供することを可能にするため、有用である。トランザクションがスムースに進行すると、顧客とレンタル企業との双方がトランザクションを署名し、資金がレンタル企業に転送される。何か間違いがある場合、彼らは顧客にリファンドするためのトランザクションに署名できる。彼らが同意できなかった場合、エスクローエージェントは、それを受けるべき主体に第２のシグネチャを提供する。

【００７８】

ＴｘＢが顧客によって記入されると、それはブロックチェーンネットワークに送信される。これは、顧客が契約における条項に同意し、自動車レンタルに進むことを所望していることを示す。ＣＬＴＶ機構は、トランザクションのブロードキャストの時間及び／又は出力が利用可能な時間を指定するのに利用可能である。

【００７９】

フェーズ２：アクセスが可能とされる

図１ｂのステップ１０６において、ＩｏＴデバイス１０４は、ＴｘＢのＯｕｔｐｕｔ　０からのカラードコインを利用して、ＤＨＴからの借り手の公開鍵にアクセスする。公開鍵の場所は、メッセージを介し自動車に利用可能とされてもよい。メッセージは、公開鍵がＤＨＴにおいてどこに配置されているかを示すハッシュを含んでもよい。ＩｏＴデバイス１０４は、その後、自動車にアクセスすることが許可された個人に対応する公開鍵のそれのデータベースに公開鍵を加えることができる。従って、ここで自動車は顧客の公開鍵を知ることになる。対象とする実現形態に応じて、鍵はＩｏＴデバイスに備えられたメモリに格納されてもよいし、あるいは、別の場所にオフデバイスに格納され、その後、必要に応じてデバイスによってアクセスされてもよい。図１ｂのステップ１０６を参照されたい。

【００８０】

しかしながら、本発明の他の実施例では、借り手の公開鍵は他の何れか適切な方法でＩｏＴデバイスに通信可能であり、本例において説明された方法を介する必要はない。

【００８１】

顧客は、自動車レンタル企業に以前に提供された公開鍵に対応する秘密鍵を含むスマートフォン１０８を有する。スマートフォンは、自動車レンタル企業のサーバからダウンロード及びインストールされたアプリケーション（ａｐｐ）を実行するよう構成されてもよい。ａｐｐは、顧客が自動車レンタル企業及び／又は自動車とやりとりすることを可能にする機能を提供してもよい。スマートフォン１０８は、ＩｏＴデバイス１０４にメッセージ（“アンロックドア”）を通信する。メッセージは、秘密鍵を用いて暗号化され、対応する公開鍵によってのみ解読可能である。図１ｂのステップＳ１０８を参照されたい。

【００８２】

自動車１０４は、スマートフォンから暗号化されたメッセージを受信し、ステップ１０６において格納された公開鍵を用いてそれを解読しようとする。メッセージが所定の値又はコードを提供するよう解読不可である場合、検証は失敗であり、自動車はロックされたままである。あるいは、メッセージが以前に格納された公開鍵を用いて解読に成功した場合、検証は成功したとみなされ、車両はアンロックされる。このようにして、リソースへのアクセスは、暗号化鍵の利用に基づく許可又は拒絶される。

【００８３】

利用中、スマートフォンのａｐｐは、“ロック”、“アンロック”、“ライトの点灯”など、自動車への各種メッセージを送信するのに利用されてもよい。これらのメッセージのそれぞれは顧客の秘密鍵を用いて暗号化され、指定されたタスクが格納されている公開鍵による解読の成功後に実行される。

【００８４】

フェーズ３：アクセスが不可とされる

最後のフェーズでは、貸出期間が終了する。これは、契約において指定された期間が経過したため、あるいは、顧客がもはや車両を必要としないか、あるいは他の理由によるものであってもよい。従って、自動車への借り手の一時的なアクセスはここで取り消されるべきである。車両が返却されると（又はレンタル期間の終了が何れかの方法で企業によって認識される）、エスクローエージェントは、企業のシグネチャ及び借り手のシグネチャを利用することを含む新たなブロックチェーントランザクション（ＴｘＣ）を生成する。図１ｂのステップＳ１１２を参照されたい。ＴｘＣの目的は、９ＢＴＣの資金が自動車貸出企業に支払い可能となるように、カラードコインを“リリース”することである。トランザクション（ＴｘＣ）が図４に示される。

【００８５】

ＴｘＣは、図２に示されるような２つの入力を含む。第１の入力（Ｉ０）はＴｘＢからの出力Ｏ１を使う。第２の入力（Ｉ１）は、図５に示されるＴｘＢ’からの出力である。ＴｘＢ’は、自動車貸出企業によって、上述されるように生成された。

【００８６】

ブロックチェーンネットワークにＴｘＣをブロードキャストすると、自動車貸出企業は、ステップＳ１１４においてＩｏＴデバイス１０４にメッセージを送信する。当該メッセージは、貸出処理が完了したことを通知する。メッセージは、リディームスクリプト及び借り手の公開鍵のハッシュを含む。

【００８７】

その後、ステップＳ１１６において、ＩｏＴデバイス１０４は、自動車のメモリ（又はそれが格納された他の何れかの場所）から借り手の公開鍵を削除し、これは、自動車がスマートフォン１０８からのメッセージをもはや解読できないことを意味する。

【００８８】

ＢＩＤ１０６は、その後、ステップＳ１１８において、新たなブロックチェーントランザクションＴｘＤを生成し、ＴｘＣによって生成されたカラードコインをトークン化解除又は“通常”のビットコイン値に変換する。

【００８９】

トークン化解除は、トークンを含む入力と、トークンを含まない出力とを有する新たなトランザクションＴｘＤを作成することによって実行される。トークン化解除を実行するため、必要とされるシグネチャが、トークンを含むリディームスクリプトに加えてロックスクリプトに提示される。これは、

【００９０】

【表５】

HASH160 <hash of redeem script containing **token**> EQUAL　*(TxC の出力のためのロックスクリプト)*

<signature><redeem script containing **token**>　*(TxD によって TxC のロックスクリプトに提示される)*

HASH160 <hash of signature> CHECKSIG　*(TxD の出力:これはトークンを含まないことに留意されたい)*

として表現できる。

【００９１】

従って、トークンはＴｘＤによって削除された。

【００９２】

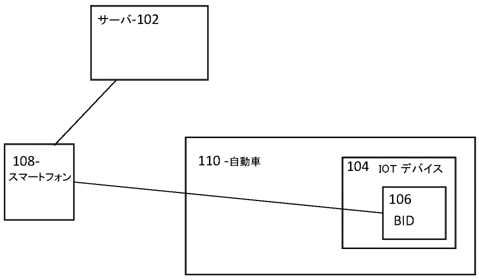
本発明の効果は、（限定することなく）

・それが設計によって本来的にセキュアである－ブロックチェーン（例えば、ビットコイ

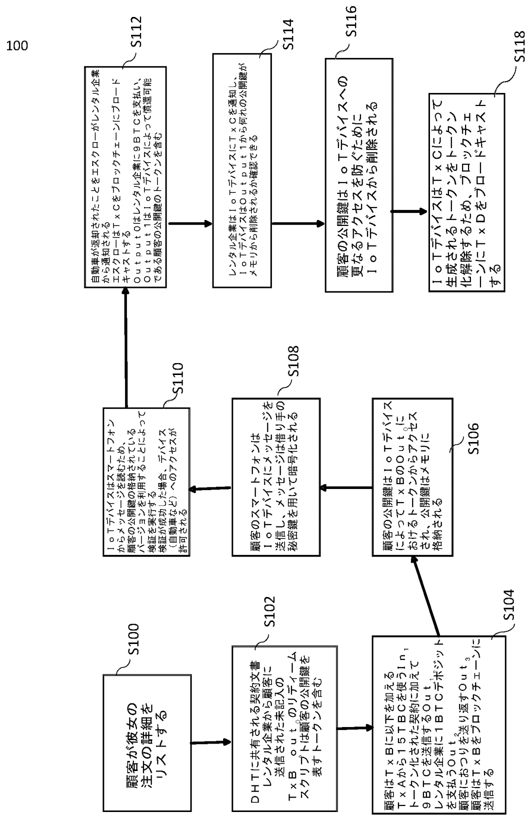
ン）プロトコルは信頼される主体を必要としない
・実施例がブロックチェーンプロトコルに基づくとき、それはＥＣＤＳＡを利用して所有権を証明し、ブロックチェーントランザクションにおいて重要な役割を演じる
・本発明はＣｈｅｃｋＬｏｃｋＴｉｍｅＶｅｒｉｆｙ（ＣＬＴＶ）オプション／設定を利用して、リソースへのアクセスが許可されるべき時間にトランザクションをブロードキャストすることができる
・分散化され、これにより、大規模な単一のポイントの不具合を回避し、攻撃に脆弱でない管理及び維持が容易であり、ビットコインネットワークが直接的に利用される
・安価で少額なトランザクション費用が通常はビットコインプロトコルの下で予想される
・ブロックチェーンはグローバル且つパブリックであり、インターネットへのアクセスを有する誰によってもいつでも利用可能である
・透過的であり、データがブロックチェーンに書き込まれると、誰でもそれを確認できる
・レコードが変更不可であり、データがブロックチェーンに書き込まれると、誰もそれを変更できない
・プライバシ及び匿名性が維持され、個人又は主体の特定のための情報が利用可能でないことを含む。
上述した実施例は本発明を限定するのでなく例示するものであり、当業者は添付した請求項によって規定される本発明の範囲から逸脱することなく他の多数の実施例を設計可能であることが留意されるべきである。請求項において、括弧内に配置された何れかの参照符号は請求項を限定するものとして解釈されものでない。“含む”などの単語は、何れかの請求項又は明細書全体に列記された以外の要素又はステップの存在を排除しない。本明細書では、“含む”は“含む又は構成される”を意味し、“含んでいる”は“含んでいる又は構成されている”を意味する。要素の単数形の参照は、当該要素の複数形の参照を排除せず、その反対も同様である。本発明は、複数の異なる要素を含むハードウェアによって、及び適切にプログラムされたコンピュータによって実現されてもよい。複数の手段を列挙した装置の請求項では、これらの手段のいくつかは単一のハードウェアによって実現されてもよい。特定の手段が互いに異なる従属形式の請求項に記載されるという単なる事実は、これらの手段の組み合わせが効果的に利用可能でないことを示すものでない。

【図面】

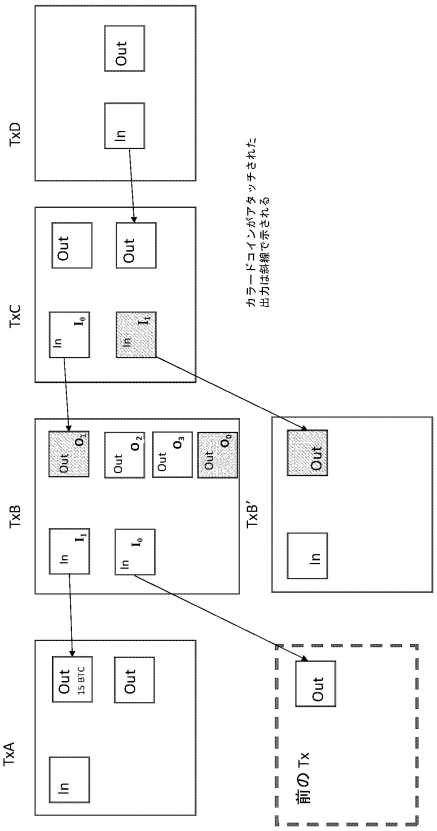
【図１ａ】


サーバ-102
108-
スマートフォン
110 -自動車
104 IOT デバイス
106
BID

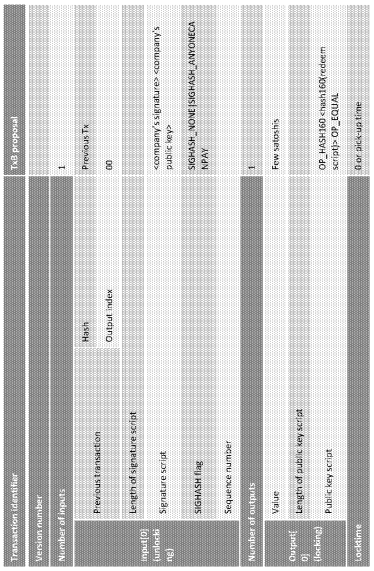
【図１ｂ】


100
S100
S102
S104
S106
S108
S110
S112
S114
S116
S118
顧客が彼女の注文の詳細をリストする

【図２】

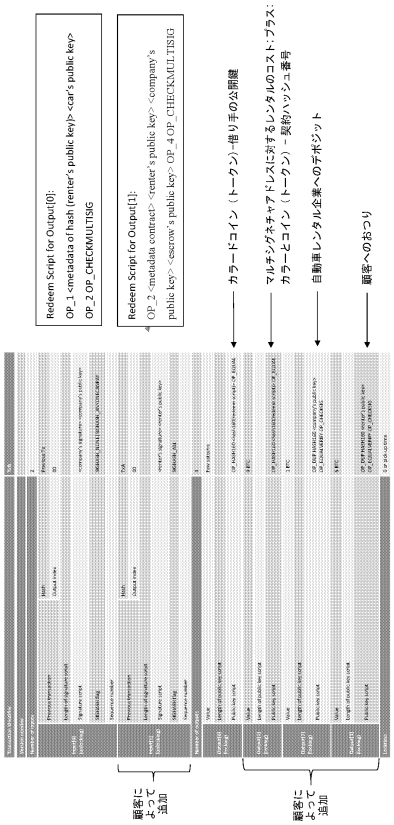


【図３ａ】



これはレンタル企業のセットアップフェーズ中にレンタル企業によって生成される提案されたトランザクションであり、顧客（借り手）に送信される。顧客は、その後、図３ｂに示される記入済みのトランザクションＴｘＢを生成するため、入力及び１つかの出力を加えることによって提案されたトランザクションを記入する。ＴｘＢの記入されたバージョンはブロックチェーンネットワークに送信される。

【図３ｂ】



【図４】

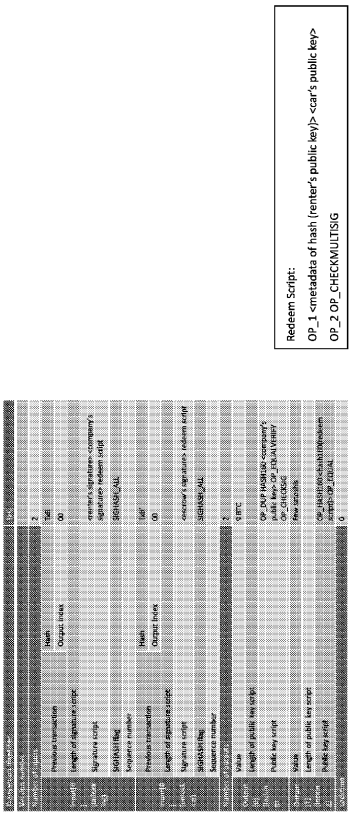


Fig. 4

【図５】

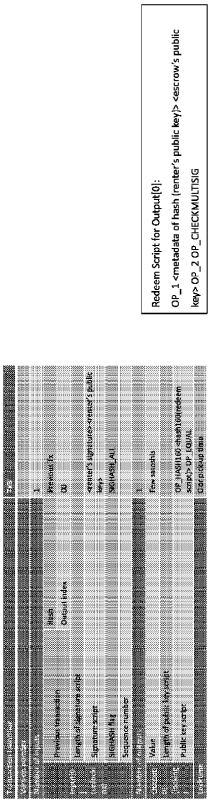


Fig. 5

【図６】

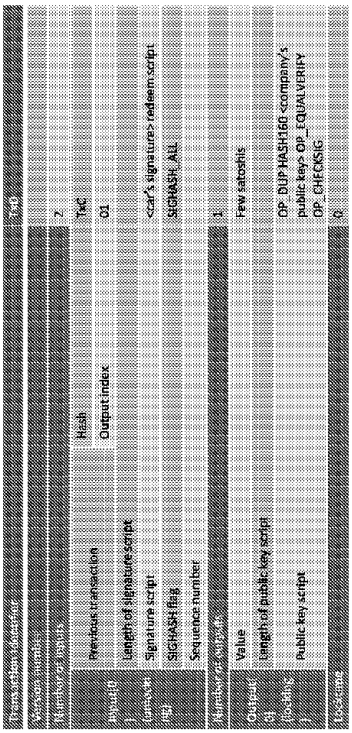


Fig. 6

フロントページの続き

(33)優先権主張国・地域又は機関
英国(GB)
弁理士　伊東 忠彦
(74)代理人　100091214
弁理士　大貫 進介
(72)発明者　ヴィンセント，ステファヌ
イギリス国 シーエフ１０ ２エイチエイチ カーディフ チャーチル ウェイ チャーチル ハウス ７ス フロア アーカート－ダイクス アンド ロード エルエルピー 内
審査官　永野 一郎
(56)参考文献　特許第５８７９４５１（ＪＰ，Ｂ１）
中国特許出願公開第１０５８０９０６２（ＣＮ，Ａ）
特開２０１２－０７９１０９（ＪＰ，Ａ）
米国特許出願公開第２０１６／００３５０５４（ＵＳ，Ａ１）
米国特許出願公開第２０１６／００９２９８８（ＵＳ，Ａ１）
米国特許出願公開第２０１６／０１６２８９７（ＵＳ，Ａ１）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　１０／００－９９／００
Ｇ０６Ｆ　２１／６２