

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6971019号
(P6971019)

(45) 発行日 令和3年11月24日(2021.11.24)

(24) 登録日 令和3年11月4日(2021.11.4)

(51) Int.Cl. F I
G 0 6 Q 2 0 / 4 0 (2012.01) G 0 6 Q 2 0 / 4 0 3 0 0

請求項の数 20 (全 54 頁)

(21) 出願番号	特願2016-187625 (P2016-187625)	(73) 特許権者	397052181
(22) 出願日	平成28年9月26日 (2016. 9. 26)		GMOインターネット株式会社
(65) 公開番号	特開2018-55203 (P2018-55203A)		東京都渋谷区桜丘町26番1号
(43) 公開日	平成30年4月5日 (2018. 4. 5)	(74) 代理人	110000877
審査請求日	令和1年9月6日 (2019. 9. 6)		龍華国際特許業務法人
		(72) 発明者	松浦 岳登
			東京都渋谷区桜丘町26番1号 GMOインターネット株式会社内
		(72) 発明者	ニコラス ジェームズ ミルズ
			東京都渋谷区桜丘町26番1号 GMOインターネット株式会社内
		審査官	山内 裕史

最終頁に続く

(54) 【発明の名称】 データ管理システム、情報処理装置、プログラム、及び、データ管理方法

(57) 【特許請求の範囲】

【請求項1】

ユーザが有する一の権利の変動に関するトランザクション情報を、前記一の権利の変動に関する分散型台帳を管理する分散型台帳管理システムに送信する場合に、前記トランザクション情報の少なくとも一部が前記ユーザの秘密鍵を用いて暗号化された暗号化データを、前記一の権利を一意に特定する権利識別情報又は前記権利識別情報を示す情報に対応付けて、前記分散型台帳管理システムに送信するトランザクション情報送信部と、

前記ユーザから、前記一の権利に対する指示を受け付ける入力部と、

前記指示の実行による前記一の権利の変動の有無を判定する権利変動判定部と、

を備え、

前記トランザクション情報は、

前記変動における前記一の権利の1以上の承継先を示す承継先情報と、

前記一の権利の直前の変動に関する、直前のトランザクション情報の符号化データと、

前記一の権利の変動の内容を示す内容情報を格納する内容情報格納部に格納される前記内容情報の符号化データ、又は、前記内容情報格納部に格納された前記内容情報の符号化データと、

を含み、

前記分散型台帳管理システムは、P2Pネットワークを構成する複数のノードを有し、

前記複数のノードのそれぞれは、前記分散型台帳を格納し、

前記分散型台帳は、複数のブロックを含み、

前記複数のブロックのそれぞれは、
 前記一の権利の1以上の変動に関する1以上のトランザクション情報と、
 直前のブロックの符号化データと、
 を含み、
 前記トランザクション情報送信部は、
 前記権利変動判定部が、前記指示の実行により前記一の権利に変動が生じると判定した
 場合において、前記一の権利は移転せず、前記一の権利の内容に変更が生じるときに、
 承継先として前記ユーザを指定する前記承継先情報を含む前記トランザクション情報を
 、前記分散型台帳管理システムに送信する、
 データ管理システム。

10

【請求項2】

ユーザが有する一の権利の変動に関するトランザクション情報を、前記一の権利の変動
 に関する分散型台帳を管理する分散型台帳管理システムに送信する場合に、前記トランザ
 クション情報の少なくとも一部が前記ユーザの秘密鍵を用いて暗号化された暗号化デー
 タを、前記一の権利を一意に特定する権利識別情報又は前記権利識別情報を示す情報に対応
 付けて、前記分散型台帳管理システムに送信するトランザクション情報送信部、
 を備え、

前記トランザクション情報は、
 前記変動における前記一の権利の1以上の承継先を示す承継先情報と、
 前記一の権利の直前の変動に関する、直前のトランザクション情報の符号化データと、
 前記一の権利の変動の内容を示す内容情報を格納する内容情報格納部に格納される前記
 内容情報の符号化データ、又は、前記内容情報格納部に格納された前記内容情報の符号化
 データと、

20

を含み、
 前記分散型台帳管理システムは、P2Pネットワークを構成する複数のノードを有し、
 前記複数のノードのそれぞれは、前記分散型台帳を格納し、
 前記分散型台帳は、複数のブロックを含み、

前記複数のブロックのそれぞれは、
 前記一の権利の1以上の変動に関する1以上のトランザクション情報と、
 直前のブロックの符号化データと、
 を含み、

30

前記一の権利の変動は、前記一の権利の内容又は客体の変更（仮想通貨の残高の変更を
 除く。）を含み、

前記一の権利は、(a)物権、準物権、債権、契約上の地位、及び、デジタルデータの
 アクセス権又はパーミッション、(b)有体物又は無体物の、使用又は利用、収益及び処
 分の少なくとも1つに関する権利、並びに(c)知的財産権、知的財産に関する実施権又
 は利用権、及び、著作権の少なくとも1つである、

データ管理システム。

【請求項3】

前記一の権利は、(a)物権、準物権、債権及び契約上の地位、(b)有体物又は無体
 物の処分に関する権利、並びに、(c)知的財産権、知的財産に関する実施権又は利用権
 及び著作権の少なくとも1つである、

40

請求項2に記載のデータ管理システム。

【請求項4】

前記一の権利の目的物に、前記ユーザを識別するために用いられるユーザ識別情報、及
 び、前記目的物に対する命令を送信する命令送信部をさらに備える、

請求項1から請求項3までの何れか一項に記載のデータ管理システム。

【請求項5】

ユーザが有する一の権利の変動に関するトランザクション情報を、前記一の権利の変動
 に関する分散型台帳を管理する分散型台帳管理システムに送信する場合に、前記トランザ

50

クシヨクン情報の少なくとも一部が前記ユーザの秘密鍵を用いて暗号化された暗号化データを、前記一の権利を一意に特定する権利識別情報又は前記権利識別情報を示す情報に対応付けて、前記分散型台帳管理システムに送信するトランザクシヨクン情報送信部と、

前記一の権利の目的物に、前記ユーザを識別するために用いられるユーザ識別情報、及び、前記目的物に対する命令を送信する命令送信部と、

を備え、

前記目的物は、通信機能を有する有体物であり、

前記トランザクシヨクン情報は、

前記変動における前記一の権利の1以上の承継先を示す承継先情報と、

前記一の権利の直前の変動に関する、直前のトランザクシヨクン情報の符号化データと、

前記一の権利の変動の内容を示す内容情報を格納する内容情報格納部に格納される前記内容情報の符号化データ、又は、前記内容情報格納部に格納された前記内容情報の符号化データと、

を含み、

前記分散型台帳管理システムは、P2Pネットワークを構成する複数のノードを有し、

前記複数のノードのそれぞれは、前記分散型台帳を格納し、

前記分散型台帳は、複数のブロックを含み、

前記複数のブロックのそれぞれは、

前記一の権利の1以上の変動に関する1以上のトランザクシヨクン情報と、

直前のブロックの符号化データと、

を含む、

データ管理システム。

【請求項6】

前記目的物は、

前記目的物の機能に関する制限の実施又は解除を制御する制限制御部と、

前記目的物に関する1以上の権利の権利識別情報又は前記権利識別情報を示す情報を格納する権利識別情報格納部と、

前記命令送信部が送信した前記ユーザ識別情報及び前記命令を受信する命令受信部と、

前記分散型台帳管理システムに、前記命令に関連する権利の前記権利識別情報又は前記権利識別情報を示す情報を送信し、前記命令に関連する権利の現在の権利者を示す情報の抽出を要求する要求送信部と、

前記分散型台帳管理システムから、前記要求送信部が送信した前記要求に対する応答を受信する応答受信部と、

前記命令受信部が受信した前記命令を実行する命令実行部と、

を備え、

前記制限制御部は、前記ユーザ識別情報が、前記応答に含まれている場合に、前記制限を解除することを決定し、

前記命令実行部は、前記制限制御部が前記制限を解除することを決定した場合に、前記命令を実行する、

請求項4又は請求項5に記載のデータ管理システム。

【請求項7】

前記目的物は、

前記目的物の機能に関する制限の実施又は解除を制御する制限制御部と、

前記目的物に関する1以上の権利の権利識別情報又は前記権利識別情報を示す情報を格納する権利識別情報格納部と、

前記命令送信部が送信した前記ユーザ識別情報及び前記命令を受信する命令受信部と、

前記分散型台帳管理システムに、前記権利識別情報格納部に格納された前記権利識別情報又は前記権利識別情報を示す情報の少なくとも一部、及び、前記ユーザ識別情報を送信し、前記ユーザが前記命令に関連する権利を有するか否かの判定を要求する要求送信部と

、

10

20

30

40

50

前記分散型台帳管理システムから、前記要求送信部が送信した前記要求に対する応答を受信する応答受信部と、

前記命令受信部が受信した前記命令を実行する命令実行部と、
を備え、

前記制限制御部は、前記応答が、前記ユーザが前記命令に関連する権利を有することを示す場合に、前記制限を解除することを決定し、

前記命令実行部は、前記制限制御部が前記制限を解除することを決定した場合に、前記命令を実行する、

請求項 4 又は請求項 5 に記載のデータ管理システム。

【請求項 8】

前記目的物は、

前記目的物の機能に関する制限の実施又は解除を制御する制限制御部と、

前記目的物に関する 1 以上の権利の権利識別情報又は前記権利識別情報を示す情報を格納する権利識別情報格納部と、

前記命令送信部が送信した前記ユーザ識別情報及び前記命令を受信する命令受信部と、

前記分散型台帳管理システムに、前記ユーザ識別情報を送信し、前記ユーザが有する 1 以上の権利の権利識別情報又は前記権利識別情報を示す情報の抽出を要求する要求送信部と、

前記分散型台帳管理システムから、前記要求送信部が送信した前記要求に対する応答を受信する応答受信部と、

前記命令受信部が受信した前記命令を実行する命令実行部と、
を備え、

前記制限制御部は、前記応答に含まれる前記権利識別情報又は前記権利識別情報を示す情報が、前記権利識別情報格納部に格納された前記権利識別情報又は前記権利識別情報を示す情報の中に含まれている場合に、前記制限を解除することを決定し、

前記命令実行部は、前記制限制御部が前記制限を解除することを決定した場合に、前記命令を実行する、

請求項 4 又は請求項 5 に記載のデータ管理システム。

【請求項 9】

前記ユーザから、前記一の権利に対する指示を受け付ける入力部と、

前記指示の実行による前記一の権利の変動の有無を判定する権利変動判定部と、

前記権利変動判定部が、前記指示の実行により前記一の権利に変動が生じると判定した場合に、当該変動の内容を示す内容情報を生成又は更新する内容情報更新部と、

をさらに備え、

前記トランザクション情報送信部は、前記権利変動判定部が、前記指示の実行により前記一の権利に変動が生じると判定した場合に、前記内容情報の符号化データを含む前記トランザクション情報を、前記分散型台帳管理システムに送信する、

請求項 2 から請求項 8 までの何れか一項に記載のデータ管理システム。

【請求項 10】

前記内容情報へのアクセスを制限するアクセス制限部をさらに備える、

請求項 9 に記載のデータ管理システム。

【請求項 11】

前記トランザクション情報送信部は、

前記権利変動判定部が、前記指示の実行により前記一の権利に変動が生じると判定した場合において、前記一の権利は移転せず、前記一の権利の内容に変更が生じるときに、

承継先として前記ユーザを指定する前記承継先情報を含む前記トランザクション情報を、前記分散型台帳管理システムに送信する、

請求項 9 又は請求項 10 に記載のデータ管理システム。

【請求項 12】

前記分散型台帳管理システムに対して、

10

20

30

40

50

前記ユーザを識別するために用いられるユーザ識別情報を送信し、
 前記ユーザが有する 1 以上の権利の権利識別情報又は前記権利識別情報を示す情報の抽出、又は、前記ユーザが前記一の権利を有するか否かの判定を要求する、
 要求送信部をさらに備える、
 請求項 1 から請求項 3 までの何れか一項に記載のデータ管理システム。

【請求項 1 3】

前記トランザクション情報は、ブロックチェーン技術を利用した暗号通貨のトランザクション情報であり、
 前記権利識別情報は、前記暗号通貨を一意に特定する通貨識別情報であり、
 前記ユーザの前記暗号通貨の保有量は、前記ユーザの前記一の権利の持分に応じて決定される、
 請求項 1 から請求項 1 2 までの何れか一項に記載のデータ管理システム。

【請求項 1 4】

前記トランザクション情報は、前記暗号通貨の全発行量を定義する情報をさらに含む、
 請求項 1 3 に記載のデータ管理システム。

【請求項 1 5】

前記分散型台帳管理システムとの間で、通信回線を介して情報を送受するよう構成された情報処理装置をさらに備え、

前記情報処理装置は、

前記分散型台帳管理システムに対して、(i) 特定のユーザが有する権利を示す情報の抽出、(i i) 特定の権利を有する者を示す情報の抽出、又は、(i i i) 前記特定のユーザが前記特定の権利を有するか否かの判定を要求する要求送信部、

を有し、

前記分散型台帳管理システムは、1 以上の権利の変動に関する 1 以上の分散型台帳を管理し、

前記 1 以上のトランザクション情報の少なくとも 1 つは、

当該トランザクション情報により表現される変動における、当該トランザクション情報により表現される権利の 1 以上の承継先を示す承継先情報と、

当該トランザクション情報により表現される権利の直前の変動に関する、直前のトランザクション情報の符号化データと、

当該トランザクション情報により表現される権利を一意に特定する権利識別情報又は前記権利識別情報を示す情報と、

当該トランザクション情報の少なくとも一部が前記ユーザの秘密鍵で暗号化された暗号化データと、

を含む、

請求項 1 から請求項 1 4 までの何れか一項に記載のデータ管理システム。

【請求項 1 6】

前記内容情報格納部をさらに備え、

前記内容情報格納部は、前記分散型台帳管理システムとは別のデータベースシステムであり、

前記内容情報格納部は、前記内容情報と、前記内容情報の前記符号化データとを対応付けて格納する、

請求項 1 から請求項 1 5 までの何れか一項に記載のデータ管理システム。

【請求項 1 7】

コンピュータを、請求項 1 から請求項 1 6 までの何れか一項に記載のデータ管理システムとして機能させるためのプログラム。

【請求項 1 8】

コンピュータが、ユーザが有する一の権利の変動に関するトランザクション情報を、前記一の権利の変動に関する分散型台帳を管理する分散型台帳管理システムに送信する場合に、前記コンピュータが、前記トランザクション情報の少なくとも一部が前記ユーザの秘

10

20

30

40

50

密鍵を用いて暗号化された暗号化データを、前記一の権利を一意に特定する権利識別情報又は前記権利識別情報を示す情報に対応付けて、前記一の権利の変動に関する分散型台帳を管理する分散型台帳管理システムに送信するトランザクション情報送信段階と、

前記コンピュータが、前記ユーザから、前記一の権利に対する指示を受け付ける入力段階と、

前記コンピュータが、前記指示の実行による前記一の権利の変動の有無を判定する権利変動判定段階と、

を有し、

前記トランザクション情報は、

前記変動における前記一の権利の1以上の承継先を示す承継先情報と、

前記一の権利の直前の変動に関する、直前のトランザクション情報の符号化データと、

前記一の権利の変動の内容を示す内容情報を格納する内容情報格納部に格納される前記内容情報の符号化データ、又は、前記内容情報格納部に格納された前記内容情報の符号化データと、

を含み、

前記分散型台帳管理システムは、P2Pネットワークを構成する複数のノードを有し、

前記複数のノードのそれぞれは、前記分散型台帳を格納し、

前記分散型台帳は、時系列に連続する複数のブロックを含み、

前記複数のブロックのそれぞれは、

前記一の権利の1以上の変動に関する1以上のトランザクション情報と、

直前のブロックの符号化データと、

を含み、

前記トランザクション情報送信段階は、

前記権利変動判定段階において、前記指示の実行により前記一の権利に変動が生じると判定された場合において、前記一の権利は移転せず、前記一の権利の内容に変更が生じるときに、前記コンピュータが、承継先として前記ユーザを指定する前記承継先情報を含む前記トランザクション情報を、前記分散型台帳管理システムに送信する段階、

を含む、

データ管理方法。

【請求項19】

コンピュータが、ユーザが有する一の権利の変動に関するトランザクション情報を、前記一の権利の変動に関する分散型台帳を管理する分散型台帳管理システムに送信する場合に、前記コンピュータが、前記トランザクション情報の少なくとも一部が前記ユーザの秘密鍵を用いて暗号化された暗号化データを、前記一の権利を一意に特定する権利識別情報又は前記権利識別情報を示す情報に対応付けて、前記一の権利の変動に関する分散型台帳を管理する分散型台帳管理システムに送信するトランザクション情報送信段階、

を有し、

前記トランザクション情報は、

前記変動における前記一の権利の1以上の承継先を示す承継先情報と、

前記一の権利の直前の変動に関する、直前のトランザクション情報の符号化データと、

前記一の権利の変動の内容を示す内容情報を格納する内容情報格納部に格納される前記内容情報の符号化データ、又は、前記内容情報格納部に格納された前記内容情報の符号化データと、

を含み、

前記分散型台帳管理システムは、P2Pネットワークを構成する複数のノードを有し、

前記複数のノードのそれぞれは、前記分散型台帳を格納し、

前記分散型台帳は、時系列に連続する複数のブロックを含み、

前記複数のブロックのそれぞれは、

前記一の権利の1以上の変動に関する1以上のトランザクション情報と、

直前のブロックの符号化データと、

10

20

30

40

50

を含み、

前記一の権利の変動は、前記一の権利の内容又は客体の変更（仮想通貨の残高の変更を除く。）を含み、

前記一の権利は、（ a ）物権、準物権、債権、契約上の地位、及び、デジタルデータのアクセス権又はパーミッション、（ b ）有体物又は無体物の、使用又は利用、収益及び処分の少なくとも1つに関する権利、並びに（ c ）知的財産権、知的財産に関する実施権又は利用権、及び、著作権の少なくとも1つである、

データ管理方法。

【請求項 20】

コンピュータが、ユーザが有する一の権利の変動に関するトランザクション情報を、前記一の権利の変動に関する分散型台帳を管理する分散型台帳管理システムに送信する場合に、前記コンピュータが、前記トランザクション情報の少なくとも一部が前記ユーザの秘密鍵を用いて暗号化された暗号化データを、前記一の権利を一意に特定する権利識別情報又は前記権利識別情報を示す情報に対応付けて、前記一の権利の変動に関する分散型台帳を管理する分散型台帳管理システムに送信するトランザクション情報送信段階と、

前記一の権利の目的物に、前記ユーザを識別するために用いられるユーザ識別情報、及び、前記目的物に対する命令を送信する命令送信段階と、

を有し、

前記目的物は、通信機能を有する有体物であり、

前記トランザクション情報は、

前記変動における前記一の権利の1以上の承継先を示す承継先情報と、

前記一の権利の直前の変動に関する、直前のトランザクション情報の符号化データと、

前記一の権利の変動の内容を示す内容情報を格納する内容情報格納部に格納される前記内容情報の符号化データ、又は、前記内容情報格納部に格納された前記内容情報の符号化データと、

を含み、

前記分散型台帳管理システムは、P2Pネットワークを構成する複数のノードを有し、

前記複数のノードのそれぞれは、前記分散型台帳を格納し、

前記分散型台帳は、時系列に連続する複数のブロックを含み、

前記複数のブロックのそれぞれは、

前記一の権利の1以上の変動に関する1以上のトランザクション情報と、

直前のブロックの符号化データと、

を含む、

データ管理方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、データ管理システム、プログラム、データ管理方法、情報処理装置、データ構造に関する。

【背景技術】

【0002】

デジタルコンテンツを利用しているユーザが機器を買い替えた場合に、新端末が、端末管理サーバから、旧端末から新端末に機器変更されたことの移転証明を取得することで、コンテンツを使用する権利の引き継ぎを認証するシステムが知られている（例えば、特許文献1を参照されたい）。

（先行技術文献）

（特許文献）

（特許文献1）特開2016-081134号公報

【発明の概要】

【発明が解決しようとする課題】

10

20

30

40

50

【 0 0 0 3 】

しかしながら、クライアント・サーバ・システムのような集中管理型のシステムを利用して権利を管理する場合、サーバに格納されたデータの信憑性を保証することが難しい。

【 課題を解決するための手段 】

【 0 0 0 4 】

本発明の第 1 の態様においては、データ管理システムが提供される。上記のデータ管理システムは、ユーザが有する一の権利の変動に関するトランザクション情報を、一の権利の変動に関する分散型台帳を管理する分散型台帳管理システムに送信する場合に、トランザクション情報の少なくとも一部がユーザの秘密鍵を用いて暗号化された暗号化データを、一の権利を一意に特定する権利識別情報又は権利識別情報を示す情報に対応付けて、分散型台帳管理システムに送信するトランザクション情報送信部を備える。上記のデータ管理システムにおいて、トランザクション情報は、変動における一の権利の 1 以上の承継先を示す承継先情報と、一の権利の直前の変動に関する、直前のトランザクション情報の符号化データと、一の権利の変動の内容を示す内容情報を格納する内容情報格納部に格納される内容情報の符号化データ、又は、内容情報格納部に格納された内容情報の符号化データとを含む。上記のデータ管理システムにおいて、分散型台帳管理システムは、P2Pネットワークを構成する複数のノードを有する。上記のデータ管理システムにおいて、複数のノードのそれぞれは、分散型台帳を格納する。上記のデータ管理システムにおいて、分散型台帳は、複数のブロックを含む。上記のデータ管理システムにおいて、複数のブロックのそれぞれは、一の権利の 1 以上の変動に関する 1 以上のトランザクション情報と、直前のブロックの符号化データとを含む。

10

20

【 0 0 0 5 】

上記のデータ管理システムは、ユーザから、一の権利に対する指示を受け付ける入力部を備えてよい。上記のデータ管理システムは、指示の実行による一の権利の変動の有無を判定する権利変動判定部を備えてよい。上記のデータ管理システムは、権利変動判定部が、指示の実行により一の権利に変動が生じると判定した場合に、当該変動の内容を示す内容情報を生成又は更新する内容情報更新部を備えてよい。上記のデータ管理システムは、トランザクション情報送信部は、権利変動判定部が、指示の実行により一の権利に変動が生じると判定した場合に、内容情報の符号化データを含むトランザクション情報を、分散型台帳管理システムに送信してよい。

30

【 0 0 0 6 】

上記のデータ管理システムは、内容情報へのアクセスを制限するアクセス制限部を備えてよい。上記のデータ管理システムにおいて、トランザクション情報送信部は、権利変動判定部が、指示の実行により一の権利に変動が生じると判定した場合において、一の権利は移転せず、一の権利の内容に変更が生じるときに、承継先としてユーザを指定する承継先情報を含むトランザクション情報を、分散型台帳管理システムに送信してよい。上記のデータ管理システムにおいて、トランザクション情報は、ブロックチェーン技術を利用した暗号通貨のトランザクション情報であってよい。上記のデータ管理システムにおいて、権利識別情報は、暗号通貨を一意に特定する通貨識別情報であってよい。上記のデータ管理システムにおいて、ユーザの暗号通貨の保有量は、ユーザの一の権利の持分に依りて決定されてよい。上記のデータ管理システムにおいて、トランザクション情報は、暗号通貨の全発行量を定義する情報をさらに含んでよい。上記のデータ管理システムは、一の権利の目的物に、ユーザを識別するために用いられるユーザ識別情報、及び、目的物に対する命令を送信する命令送信部を備えてよい。

40

【 0 0 0 7 】

上記のデータ管理システムにおいて、目的物は、目的物の機能に関する制限の実施又は解除を制御する制限制御部を備えてよい。目的物は、目的物に関する 1 以上の権利の権利識別情報又は権利識別情報を示す情報を格納する権利識別情報格納部を備えてよい。目的物は、命令送信部が送信したユーザ識別情報及び命令を受信する命令受信部を備えてよい。目的物は、分散型台帳管理システムに、命令に関連する権利の権利識別情報又は権利識

50

別情報を示す情報を送信し、命令に関連する権利の現在の権利者を示す情報の抽出を要求する要求送信部を備えてよい。目的物は、分散型台帳管理システムから、要求送信部が送信した要求に対する応答を受信する応答受信部を備えてよい。目的物は、命令受信部が受信した命令を実行する命令実行部を備えてよい。上記のデータ管理システムにおいて、制限制御部は、ユーザ識別情報が、応答に含まれている場合に、制限を解除することを決定してよい。上記のデータ管理システムにおいて、命令実行部は、制限制御部が制限を解除することを決定した場合に、命令を実行してよい。

【 0 0 0 8 】

上記のデータ管理システムにおいて、目的物は、目的物の機能に関する制限の実施又は解除を制御する制限制御部を備えてよい。目的物は、目的物に関する1以上の権利の権利識別情報又は権利識別情報を示す情報を格納する権利識別情報格納部を備えてよい。命令送信部が送信したユーザ識別情報及び命令を受信する命令受信部を備えてよい。目的物は、分散型台帳管理システムに、権利識別情報格納部に格納された権利識別情報又は権利識別情報を示す情報の少なくとも一部、及び、ユーザ識別情報を送信し、ユーザが命令に関連する権利を有するか否かの判定を要求する要求送信部を備えてよい。目的物は、分散型台帳管理システムから、要求送信部が送信した要求に対する応答を受信する応答受信部を備えてよい。目的物は、命令受信部が受信した命令を実行する命令実行部を備えてよい。上記のデータ管理システムにおいて、制限制御部は、応答が、ユーザが命令に関連する権利を有することを示す場合に、制限を解除することを決定してよい。上記のデータ管理システムにおいて、命令実行部は、制限制御部が制限を解除することを決定した場合に、命令を実行してよい。

【 0 0 0 9 】

上記のデータ管理システムにおいて、目的物は、目的物の機能に関する制限の実施又は解除を制御する制限制御部を備えてよい。目的物は、目的物に関する1以上の権利の権利識別情報又は権利識別情報を示す情報を格納する権利識別情報格納部を備えてよい。目的物は、命令送信部が送信したユーザ識別情報及び命令を受信する命令受信部を備えてよい。目的物は、分散型台帳管理システムに、ユーザ識別情報を送信し、ユーザが有する1以上の権利の権利識別情報又は権利識別情報を示す情報の抽出を要求する要求送信部を備えてよい。目的物は、分散型台帳管理システムから、要求送信部が送信した要求に対する応答を受信する応答受信部を備えてよい。目的物は、命令受信部が受信した命令を実行する命令実行部を備えてよい。上記のデータ管理システムにおいて、制限制御部は、応答に含まれる権利識別情報又は権利識別情報を示す情報が、権利識別情報格納部に格納された権利識別情報又は権利識別情報を示す情報の中に含まれている場合に、制限を解除することを決定してよい。上記のデータ管理システムにおいて、命令実行部は、制限制御部が制限を解除することを決定した場合に、命令を実行してよい。

【 0 0 1 0 】

上記のデータ管理システムは、分散型台帳管理システムに対して、ユーザを識別するために用いられるユーザ識別情報を送信し、ユーザが有する1以上の権利の権利識別情報又は権利識別情報を示す情報の抽出、又は、ユーザが一の権利を有するか否かの判定を要求する要求送信部を備えてよい。上記のデータ管理システムにおいて、一の権利は、(i) 物権、準物権、債権若しくは契約上の地位、又は、(i i) デジタルデータのアクセス権若しくはパーミッションであってよい。上記のデータ管理システムにおいて、一の権利は、有体物又は無体物の、使用又は利用、収益及び処分 of の少なくとも1つに関する権利であってよい。上記のデータ管理システムにおいて、一の権利は、知的財産権、知的財産に関する実施権若しくは利用権、又は、出版権であってよい。

【 0 0 1 1 】

本発明の第2の態様においては、コンピュータを、上記の権利管理システムとして機能させるためのプログラムが提供される。上記のプログラムを格納する非一時的コンピュータ可読媒体が提供されてもよい。

【 0 0 1 2 】

10

20

30

40

50

本発明の第3の態様においては、少なくとも、1以上の権利の変動に関する1以上の分散型台帳を管理する分散型台帳管理システムとの間で、通信回線を介して情報を送受するよう構成された情報処理装置が提供される。上記の情報処理装置は、分散型台帳管理システムに対して、(i)特定のユーザが有する権利を示す情報の抽出、(ii)特定の権利を有する者を示す情報の抽出、又は、(iii)特定のユーザが特定の権利を有するか否かの判定を要求する要求送信部を備える。上記の情報処理装置において、分散型台帳管理システムは、P2Pネットワークを構成する複数のノードを有する。上記の情報処理装置において、複数のノードのそれぞれは、分散型台帳を格納する。上記の情報処理装置において、分散型台帳は、時系列に連続する複数のブロックを含む。上記の情報処理装置において、複数のブロックのそれぞれは、1以上の権利の1以上の変動に関する1以上のトランザクション情報と、直前のブロックの符号化データとを含む。上記の情報処理装置において、1以上のトランザクション情報の少なくとも1つは、当該トランザクション情報により表現される変動における、当該トランザクション情報により表現される権利の1以上の承継先を示す承継先情報と、当該トランザクション情報により表現される権利の直前の変動に関する、直前のトランザクション情報の符号化データと、当該トランザクション情報により表現される権利を一意に特定する権利識別情報又は権利識別情報を示す情報と、当該トランザクション情報の少なくとも一部をユーザの秘密鍵で暗号した暗号化データとを含む。

10

【0013】

本発明の第4の態様においては、コンピュータを、上記の情報処理装置として機能させるためのプログラムが提供される。上記のプログラムを格納する非一時的コンピュータ可読媒体が提供されてもよい。

20

【0014】

本発明の第5の態様においては、データ管理方法が提供される。上記のデータ管理方法は、ユーザが有する一の権利の変動に関するトランザクション情報を、一の権利の変動に関する分散型台帳を管理する分散型台帳管理システムに送信する場合に、トランザクション情報の少なくとも一部がユーザの秘密鍵を用いて暗号化された暗号化データを、一の権利を一意に特定する権利識別情報又は権利識別情報を示す情報に対応付けて、一の権利の変動に関する分散型台帳を管理する分散型台帳管理システムに送信するトランザクション情報送信段階を有する。上記のデータ管理方法において、トランザクション情報は、変動における一の権利の1以上の承継先を示す承継先情報と、一の権利の直前の変動に関する、直前のトランザクション情報の符号化データと、一の権利の変動の内容を示す内容情報を格納する内容情報格納部に格納される内容情報の符号化データ、又は、内容情報格納部に格納された内容情報の符号化データとを含む。上記のデータ管理方法において、分散型台帳管理システムは、P2Pネットワークを構成する複数のノードを有する。上記のデータ管理方法において、複数のノードのそれぞれは、分散型台帳を格納する。上記のデータ管理方法において、分散型台帳は、時系列に連続する複数のブロックを含む。上記のデータ管理方法において、複数のブロックのそれぞれは、一の権利の1以上の変動に関する1以上のトランザクション情報と、直前のブロックの符号化データとを含む。

30

【0015】

本発明の第6の態様においては、複数のブロックを含むデータ構造が提供される。上記のデータ構造において、複数のブロックのそれぞれは、ユーザが有する一の権利の1以上の変動に関する1以上のトランザクション情報を示すデータと、直前のブロックの符号化データとを含む。上記のデータ構造において、1以上のトランザクション情報を示すデータの少なくとも1つは、当該トランザクション情報により表現される一の権利の変動に関する一の権利の1以上の承継先を示す承継先データと、一の権利の直前の変動に関する直前のトランザクション情報の符号化データと、一の権利を一意に特定する権利識別情報又は権利識別情報を示すデータと、一の権利の変動の内容を示す内容情報を格納する内容情報格納部に格納される内容情報の符号化データ、又は、内容情報格納部に格納された内容情報の符号化データと、当該トランザクション情報の少なくとも一部をユーザの秘密鍵で

40

50

暗号した暗号化データとを含む。

【0016】

本発明の第7の態様においては、時系列に連続する複数のブロックを構成する第1トランザクション情報のデータ構造が提供される。上記のデータ構造は、第1トランザクション情報により表現される権利の変動における、権利の1以上の承継先を示すデータを含む。上記のデータ構造は、権利の直前の変動に関する第2トランザクション情報の符号化データを含む。上記のデータ構造は、権利を一意に特定する権利識別情報又は権利識別情報を示すデータを含む。上記のデータ構造は、権利の変動の内容を示す内容情報を格納する内容情報格納部に格納される内容情報の符号化データ、又は、内容情報格納部に格納された内容情報の符号化データを含む。上記のデータ構造は、第1トランザクション情報の少なくとも一部を、権利を有する者の秘密鍵で暗号した暗号化データを含む。

10

【0017】

なお、上記の発明の概要は、本発明の必要な特徴の全てを列挙したものではない。また、これらの特徴群のサブコンビネーションもまた、発明となりうる。

【図面の簡単な説明】

【0018】

【図1】権利管理システム100のシステム構成の一例を概略的に示す。

【図2】ノード112の内部構成一例を概略的に示す。

【図3】ブロックチェーン300のデータ構造の一例を概略的に示す。

【図4】ブロックヘッダ310のデータ構造の一例を概略的に示す。

20

【図5】トランザクションデータ500のデータ構造の一例を概略的に示す。

【図6】ユーザ端末120の内部構成の一例を概略的に示す。

【図7】データテーブル700の一例を概略的に示す。

【図8】データテーブル800の一例を概略的に示す。

【図9】権利管理システム900のシステム構成の一例を概略的に示す。

【図10】ユーザ端末920の内部構成の一例を概略的に示す。

【図11】目的物930の内部構成の一例を概略的に示す。

【図12】権利管理システム900における情報処理の一例を概略的に示す。

【図13】権利管理システム900における情報処理の一例を概略的に示す。

【図14】権利管理システム900における情報処理の一例を概略的に示す。

30

【図15】エスクローシステム2100のシステム構成の一例を概略的に示す。

【図16】データテーブル2200の一例を概略的に示す。

【図17】コントラクトオブジェクト2300の一例を概略的に示す。

【発明を実施するための形態】

【0019】

以下、発明の実施の形態を通じて本発明を説明するが、以下の実施形態は特許請求の範囲にかかる発明を限定するものではない。また、実施形態の中で説明されている特徴の組み合わせの全てが発明の解決手段に必須であるとは限らない。なお、図面において、同一または類似の部分には同一の参照番号を付して、重複する説明を省く場合がある。

【0020】

40

[権利管理システム100の概要]

図1は、権利管理システム100のシステム構成の一例を概略的に示す。本実施形態において、権利管理システム100は、ビットコインなどの暗号通貨(cryptocurrency; 仮想通貨と称される場合もある。)の取引にも使用されているブロックチェーン技術を利用して、1以上の権利のそれぞれの変動履歴を管理する。1以上の権利のそれぞれは、一の権利の一例であってよい。

【0021】

権利の変動としては、権利の発生又は取得、権利の変更、及び、権利の消滅を例示することができる。権利の発生又は取得としては、承継取得と、原始取得とを例示することができる。承継取得としては、移転的承継と、設権的承継とを例示することができる。移転

50

的承継としては、特定承継と、包括承継又は一般承継とを例示することができる。権利の変更としては、権利の内容の変更、権利の客体の変更などを例示することができる。

【 0 0 2 2 】

上記の権利は、(i) 物権、準物権、債権若しくは契約上の地位、又は、(i i) デジタルデータのアクセス権若しくはパーミッションであってよい。準物権としては、知的財産権を例示することができる。アクセス権又はパーミッションとしては、読み込みの許否、書き込みの許否、実行の許否などを例示することができる。アクセス権又はパーミッションの他の例としては、閲覧の許否、保存の許否、送信の許否、出力の許否、複製の許否などを例示することができる。出力としては、プリンタ出力、音声出力、画像出力などを例示することができる。

10

【 0 0 2 3 】

上記の権利は、有体物の使用若しくは利用、収益及び処分の少なくとも1つに関する権利、又は、無体物の使用若しくは利用、収益及び処分の少なくとも1つに関する権利であってよい。無体物としては、デジタルデータ、IPアドレス、知的財産などを例示することができる。上記のデジタルデータは、ゲーム内又は仮想空間内におけるアイテムであってもよい。上記の権利は、知的財産権、知的財産に関する実施権若しくは利用権、又は、著作権であってよい。知的財産権としては、産業財産権、著作権(著作隣接権、著作人格権を含む。)、商品化権、回路配置利用権、育成者権、営業秘密、商品等表示、商品形態、トレードドレス、原産地表示、地理的表示、商号権、肖像権、ドメインネームなどを例示することができる。

20

【 0 0 2 4 】

暗号通貨においては、暗号通貨の取引(トランザクションと称される場合がある。)の履歴をブロックチェーンとして記録し、P2Pネットワークに参加する複数のノードの間で当該ブロックチェーンを共有することにより、上記取引の正当性を担保している。ブロックチェーンは、時系列に連続する複数のブロックがチェーン状に繋がったデータであり、各ブロックは、一定期間におけるトランザクションのデータ(トランザクションデータと称する場合がある。)を含む。ブロックチェーン技術によれば、複数のブロックが過去の情報を保持した状態で追加されていくので、履歴の改竄が非常に困難になる。

【 0 0 2 5 】

本実施形態によれば、1以上の権利のそれぞれの変動履歴に関する情報が、ブロックチェーンとして、P2Pネットワーク上に記憶される。つまり、権利の変動が発生するたびにトランザクションが生成される。そして、複数のトランザクションが1つのブロックにまとめられ、当該ブロックが既存のブロックチェーンに追加される。

30

【 0 0 2 6 】

各ブロックは、例えば、複数のトランザクションが当該ブロックにまとめられた時間(ブロックロック時間と称する場合がある。)に関する情報を含む。これにより、時系列に連続する複数のブロックを含むブロックチェーンが生成される。また、各ブロックは、直前のブロックの符号化データを含む。符号化データは、ハッシュ値であってよい。

【 0 0 2 7 】

ブロックチェーンに記録されている情報は改竄が難しく、信憑性が高いので、当該情報を利用して、現在の権利者を証明するサービス、権利又はデジタルデータの存在を証明するサービス、デジタルデータが正当な権原又は権限を有する者により作成されたことを証明するサービス、デジタルデータが改竄されていないことを証明するサービスなどを提供することができる。

40

【 0 0 2 8 】

本実施形態においては、説明を簡単にする目的で、権利管理システム100を用いて、1以上の権利のそれぞれの正当な権利者に関する情報を管理するサービスを提供する場合について説明する。しかしながら、権利管理システム100により提供されるサービスは本実施形態に限定されない。他の実施形態において、権利管理システム100は、上記の権利又はデジタルデータの存在証明サービスなどの他、物品又はデジタルデータの遠隔操

50

作サービス、レンタルサービス若しくはシェアリングサービス、エスクローサービスなどを提供することができる。また、権利によっては、行政庁が管理する登記簿への登記を要求される場合も考えられるが、実際の登記手続については説明を省略する。

【 0 0 2 9 】

[権利管理システム 1 0 0 のシステム構成]

本実施形態において、権利管理システム 1 0 0 は、分散型台帳管理システム 1 1 0 と、ユーザ端末 1 2 0 とを備える。本実施形態において、分散型台帳管理システム 1 1 0 は、例えば、複数のノード 1 1 2 と、ピア・ツー・ピア・ネットワーク 1 1 4 とを有する。本実施形態において、分散型台帳管理システム 1 1 0 及びユーザ端末 1 2 0 は、通信ネットワーク 1 0 を介して互いに情報を送受することができる。

10

【 0 0 3 0 】

権利管理システム 1 0 0 は、データ管理システムの一例であってよい。ユーザ端末 1 2 0 は、データ管理システム又は情報処理装置の一例であってよい。

【 0 0 3 1 】

本実施形態において、通信ネットワーク 1 0 は、分散型台帳管理システム 1 1 0 及びユーザ端末 1 2 0 の間で情報を伝送する。通信ネットワーク 1 0 は、有線通信の伝送路であってもよく、無線通信の伝送路であってもよく、無線通信の伝送路及び有線通信の伝送路の組み合わせであってもよい。通信ネットワーク 1 0 は、無線パケット通信網、インターネット、P2Pネットワーク、専用回線、VPNなどを含んでもよい。通信ネットワーク 1 0 は、(i) 携帯電話回線網などの移動体通信網を含んでもよく、(i i) 無線MAN (例えば、WiMAX (登録商標) である。)、無線LAN (例えば、WiFi (登録商標) である。)、Bluetooth (登録商標)、Zigbee (登録商標)、NFC (Near Field Communication) などの無線通信網を含んでもよい。

20

【 0 0 3 2 】

本実施形態において、目的物 3 0 は、ユーザ A が有する権利の目的、又は、ユーザ A の行為の対象となる。目的物 3 0 には、複数の権利が設定されてもよい。目的物 3 0 は、有体物であってもよく、無体物であってもよい。目的物 3 0 は、デジタルデータであってもよい。デジタルデータとしては、データベース、データベースに含まれる各レコード、アプリケーションソフトウェアの電子ファイル (例えば、ワードファイル、エクセルファイル、テキストデータ、音楽データ、写真データ、動画データ、電子ゲームのセーブデータなどである。)、電子ゲームのアイテム、及び、これらの符号化データ (例えば、ハッシュ値である。) などを例示することができる。

30

【 0 0 3 3 】

目的物 3 0 は、通信機能を有し、分散型台帳管理システム 1 1 0 及びユーザ端末 1 2 0 の少なくとも一方と情報を送受してもよい。一実施形態によれば、目的物 3 0 は、ユーザ端末 1 2 0 から、目的物 3 0 を操作するための命令を受信する。目的物 3 0 は、分散型台帳管理システム 1 1 0 にアクセスして、ユーザ A が上記の命令を実行するための権原又は権限を有しているかを確認する。

【 0 0 3 4 】

他の実施形態によれば、目的物 3 0 は、コンピュータを有し、目的物 3 0 の状態をユーザ端末 1 2 0 に報告する。目的物 3 0 が植物、微生物、生物などである場合、目的物 3 0 の状態を監視する監視装置が、目的物 3 0 の状態をユーザ端末 1 2 0 に報告してもよい。目的物 3 0 又は上記の監視装置は、ユーザ端末 1 2 0 に対して、目的物 3 0 の状態に関するトランザクションを分散型台帳管理システム 1 1 0 に送信するよう要求してもよい。目的物 3 0 の状態としては、目的物 3 0 の使用状態、消耗状態又は劣化状態、生育状態などを例示することができる。目的物 3 0 の状態に関する情報は、目的物 3 0 の価値の増減に関する情報の一例であってよい。

40

【 0 0 3 5 】

一例として、目的物 3 0 が自動車である場合、目的物 3 0 は、例えば、ユーザ端末 1 2

50

0 から開錠命令を受信した場合、エンジン若しくはシステムを始動した場合、エンジン若しくはシステムを停止した場合、ユーザ端末 120 との通信を確立した場合、又は、ユーザ端末 120 との通信を終了する場合に、移動履歴、操作履歴、走行距離、バッテリー特性などに関する情報を、ユーザ端末 120 に送信する。これにより、例えば、目的物 30 を売却する場合に、目的物 30 の購入者は、目的物 30 の状態に関する信憑性の高い情報を取得することができる。

【0036】

本実施形態において、分散型台帳管理システム 110 は、1 以上の権利のそれぞれの変動履歴に関する情報を、ブロックチェーンとして格納する。分散型台帳管理システム 110 は、一般的なデータベースシステムに要求される機能を備えてよい。ブロックチェーンは、分散型台帳の一例であってよい。一実施形態において、分散型台帳管理システム 110 は、権利ごとにブロックチェーンを格納する。他の実施形態において、分散型台帳管理システム 110 は、目的物ごとにブロックチェーンを格納する。例えば、目的物に設定される権利が予め定められている場合、又は、権利管理システム 100 が管理する権利が予め定められている場合、分散型台帳管理システム 110 は、目的物ごとにブロックチェーンを格納することで、当該権利を管理することができる。

【0037】

より具体的には、権利管理システム 100 を利用して、物品の所有権を管理する場合、分散型台帳管理システム 110 は、物品ごとにブロックチェーンを格納してよい。これにより、所有権の変動履歴を管理することができる。また、権利管理システム 100 を利用して、物品のレンタル若しくはシェアリング、又は、デジタルデータの貸与（例えば、電子ゲームにおけるアイテムの付与である。）に関するサービスを提供する場合、分散型台帳管理システム 110 は、物品又はデジタルデータごとにブロックチェーンを格納してよい。これにより、貸借権、使用権、アクセス権などの変動履歴を管理することができる。

【0038】

本実施形態において、複数のノード 112 のそれぞれは、ブロックチェーンを格納する。複数のノード 112 のそれぞれは、分散型台帳管理システム 110 に参加する情報処理装置であればよく、その具体的な構成は特に限定されない。複数のノード 112 のそれぞれは、新たなブロックの承認処理（採掘処理と称される場合がある。）を実行するためのプログラムが導入されたコンピュータであってよい。一実施形態において、任意のノード 112 が、分散型台帳管理システム 110 に自由に参加することができる。他の実施形態において、分散型台帳管理システム 110 には、許可されたノード 112 のみが参加することができる。

【0039】

複数のノード 112 のそれぞれは、ユーザ端末 120 からのトランザクションデータを受信する。複数のノード 112 のそれぞれは、各ノードが受信した複数のトランザクションデータを含む新たなブロックの承認処理を実行する。新たなブロックの承認処理は、一定の時間間隔で実行されてよい。承認処理は、例えば、いずれかのノードが、予め定められた条件を満たす解を発見する処理である。承認処理は、上記の方法に限定されない。承認処理は、ブロックチェーン技術又は類似の技術において知られている手法又は将来的に新たに開発される手法に従って実施されてよい。1 台のノード 112 が新たなブロックを承認すると、当該ブロックがブロックチェーンに追加され、当該ブロックを含むブロックチェーンが他のノード 112 に共有される。

【0040】

一実施形態において、複数のノード 112 のそれぞれは、ユーザ端末 120 からの要求に応じて、当該要求に合致する 1 以上のトランザクションデータを抽出し、抽出されたトランザクションデータをユーザ端末 120 に送信してもよい。他の実施形態において、複数のノード 112 のそれぞれは、ユーザ端末 120 からの要求に応じて、当該要求に合致する 1 以上のトランザクションデータを抽出し、抽出されたトランザクションデータを利用して、当該要求に応じた処理を実行してもよい。複数のノード 112 のそれぞれは、上

10

20

30

40

50

記の処理の結果を、ユーザ端末120に送信してよい。

【0041】

本実施形態において、ピア・ツー・ピア・ネットワーク114は、複数のノード112の間で情報を伝送する。ピア・ツー・ピア・ネットワーク114は、有線通信の伝送路であってもよく、無線通信の伝送路であってもよく、無線通信の伝送路及び有線通信の伝送路の組み合わせであってもよい。ピア・ツー・ピア・ネットワーク114は、無線通信網、インターネット及び専用回線の少なくとも1つ、又は、それらの組み合わせを含んでよい。無線通信の方式は、移動体通信方式であってもよく、近距離無線通信方式であってもよい。近距離無線としては、無線MAN、無線LAN、Bluetooth（登録商標）、Zigbee（登録商標）、NFCなどを例示することができる。

10

【0042】

本実施形態において、ユーザ端末120は、ユーザAが利用する情報処理装置である。ユーザ端末120は、通信ネットワーク10を介して分散型台帳管理システム110との間で情報を送受することができる情報処理装置であればよく、その具体的な構成は特に限定されない。ユーザ端末120は、パーソナルコンピュータ、携帯電話又はスマートフォン、携帯端末（PDA、タブレット、ノートブック・コンピュータ又はラップトップ・コンピュータなどを例示することができる。）、無線端末などであってよい。

【0043】

本実施形態において、ユーザ端末120は、ユーザAの秘密鍵122を格納する。ユーザ端末120は、ユーザAの秘密鍵122を利用して、ユーザAが有する1又は複数の権利のそれぞれの変動に関する1以上のトランザクションを生成する。ユーザ端末120は、生成されたトランザクションを、複数のノード112の少なくとも一部に送信する。一実施形態において、ユーザ端末120は、生成されたトランザクションを、複数のノード112のうちいずれか1つに送信する。ユーザ端末120からトランザクションを受信したノード112は、ピア・ツー・ピア・ネットワーク114によって、他の全てのノード112に当該トランザクションを転送する。他の実施形態において、ユーザ端末120は、生成されたトランザクションを、複数のノード112にブロードキャストしてもよい。

20

【0044】

[権利管理システム100の各部のハードウェア構成]

30

【0045】

権利管理システム100の各部は、ハードウェアにより実現されてもよく、ソフトウェアにより実現されてもよく、ハードウェア及びソフトウェアにより実現されてもよい。権利管理システム100の各部は、単一のサーバによって実現されてもよく、複数のサーバによって実現されてもよい。

【0046】

権利管理システム100の各部は、一般的な構成の情報処理装置において、権利管理システム100の各部の動作を規定したソフトウェア又はプログラムを起動することにより実現されてよい。上記の情報処理装置は、CPU等のプロセッサ、ROM、RAM、通信インターフェースなどを有するデータ処理装置と、キーボード、タッチパネル、カメラ、マイク、各種センサ、GPS受信機などの入力装置と、表示装置、スピーカ、振動装置などの出力装置と、メモリ、HDDなどの記憶装置とを備えてよい。権利管理システム100は、その一部に、仮想サーバ又はクラウドシステムを含んでもよい。

40

【0047】

上記の情報処理装置において、上記のデータ処理装置又は記憶装置は、上記のソフトウェア又はプログラムを記憶してよい。上記のソフトウェア又はプログラムは、プロセッサによって実行されることにより、上記の情報処理装置に、当該ソフトウェア又はプログラムによって規定された動作を実行させる。上記のソフトウェア又はプログラムは、非一時的なコンピュータ可読記憶媒体に格納されていてもよい。

【0048】

50

[権利管理システム 100 による権利管理の概要]

< データの登録 >

権利管理システム 100 は、例えば下記の手順により、ユーザ A が有する権利の変動に関する情報を、分散型台帳管理システム 110 に登録する。まず、目的物 30 を目的とする権利を有するユーザ A が、ユーザ端末 120 上で、当該権利の変動を生じさせ得る操作を実行する。権利の変動を生じさせ得る操作としては、ユーザ端末 120 上で動作するアプリケーションソフトウェアに関する操作、インターネット上のアプリケーションサーバにより提供されるサービスを利用するための操作などを例示することができる。

【 0049 】

例えば、ユーザ A が、ユーザ端末 120 を操作してオンラインゲームを実行する場合、まず、ユーザ A のアカウントが作成される。このとき、アカウントを利用する権利が発生又は移転する。その後、ゲームの進行に従って、アイテムの入手、キャラクター又はアイテムのレベルアップなどのイベントが発生する。例えば、ユーザ A が電子ゲーム内でアイテムを入手すると、当該アイテムを利用する権利が発生又は移転する。また、電子ゲーム内でキャラクター又はアイテムがレベルアップすると、アカウント又はアイテムを利用する権利の内容に変更が生じる。アカウント又はアイテムを利用する権利は、一の権利の一例であってよい。

10

【 0050 】

ユーザの操作によりユーザ A の権利に変動が生じる場合、ユーザ端末 120 は、ユーザ端末 120 に格納された秘密鍵 122 を利用して、当該権利の変動に関するトランザクションデータを生成する。次に、ユーザ端末 120 は、生成されたトランザクションデータを、通信ネットワーク 10 を介して、分散型台帳管理システム 110 に送信する。分散型台帳管理システム 110 は、ユーザ端末 120 から受け取ったトランザクションデータを適切なタイミングでブロック化して、新たなブロックチェーンを生成する。これにより、ユーザ A は、自己の権利の変動に関する情報を分散型台帳管理システム 110 に登録することができる。

20

【 0051 】

< データの抽出 >

ユーザ A は、ユーザ端末 120 を操作して、分散型台帳管理システム 110 に格納された情報にアクセスすることができる。例えば、ユーザ端末 120 は、ユーザ A の指示に基づいて、特定の条件に合致するデータを抽出するための要求、特定の条件の成否を判定するための要求などを、分散型台帳管理システム 110 に送信する。分散型台帳管理システム 110 は、ユーザ端末 120 からの要求を受信し、当該要求に応じた処理を実行する。これにより、ユーザ A は、特定の権利の変動履歴を閲覧したり、自己の有する権利を確認したりすることができる。

30

【 0052 】

[権利管理システム 100 による権利管理の具体例 1]

一実施形態において、ユーザ A が、目的物 30 (例えば、ユーザ A が所有する自動車である。) をユーザ B に譲渡する場合、ユーザ A は、ユーザ端末 120 に、目的物 30 の所有権をユーザ A からユーザ B に移転させるための処理を実行させるべく、ユーザ端末 120 を操作する。上記の処理が開始されると、ユーザ端末 120 は、目的物 30 の所有権の移転に関するトランザクションデータを生成して、例えば、複数のノード 112 のうちのいずれか 1 つに、当該トランザクションデータを送信する。これにより、目的物 30 の所有権がユーザ B に移転したことを示すトランザクションデータが、分散型台帳管理システム 110 に登録される。目的物 30 の所有権は、一の権利の一例であってよい。

40

【 0053 】

[権利管理システム 100 による権利管理の具体例 2]

他の実施形態において、ユーザ A が、目的物 30 をユーザ B に貸し出す場合、ユーザ A は、ユーザ端末 120 に、目的物 30 に賃借権又は使用権を設定するための処理を実行させるべく、ユーザ端末 120 を操作する。上記の処理が開始されると、ユーザ端末 120

50

は、(i) 新たに賃借権若しくは使用権を発生させるための処理、又は、(i i) 既存の賃借権若しくは使用権の権利者及び内容を変更するための処理を実行する。ユーザ端末 120 は、例えば、上記の処理に対応するトランザクションデータを生成して、複数のノード 112 のうちのいずれか 1 つに、当該トランザクションデータを送信する。これにより、目的物 30 の賃借権又は使用権がユーザ B に移転したことを示すトランザクションデータが、分散型台帳管理システム 110 に登録される。目的物 30 に設定される賃借権若しくは使用権は、一の権利の一例であってよい。

【 0054 】

新たに賃借権を発生させるための処理において、ユーザ端末 120 は、例えば、発行用のトランザクションデータを生成して、複数のノード 112 のうちのいずれか 1 つに、当該トランザクションデータを送信する。新たに発生する賃借権の内容としては、(i) 賃借権の存続期間、(i i) 賃借権の譲渡又は賃借物の転貸を許すことを定めた特約の有無などを例示することができる。

10

【 0055 】

発行用のトランザクションデータは、例えば、当該トランザクションが発行用であることを示す情報と、発行条件に関する情報と、当該トランザクションにより表現される権利に関する情報と、当該権利の承継人に関する情報とを含む。発行条件に関する情報としては、発行するアセットの単位数を指定する情報、発行されるアセットの量のスケールを指定する情報 (*divisibility* と称される場合がある。)、アセットの量の上限値を指定する情報などを例示することができる。なお、アセットの量は、暗号通貨の枚数に相当し、本実施形態において、アセットの量は、例えば、権利の持分を表す。また、初回発行時のアセットの量を、発行条件で指定したアセットの量の上限值に設定することで、発行後に流通するアセットの量が増加することを防止し、流通するアセットの量を一定に保つことができる。

20

【 0056 】

権利に関する情報としては、各権利を一意に特定する情報 (権利識別情報と称する場合がある。) 又は権利識別情報を示す情報、各権利の内容に関する情報などを例示することができる。権利識別情報としては、(i) 目的物の識別情報、(i i) 目的物の識別情報と、権利の種類又は名称を示す情報との組み合わせなどを例示することができる。目的物の識別情報としては、(i) 目的物の製造番号、識別番号又は MAC アドレス、(i i) これらと、製造者又は販売者の識別情報との組み合わせなどを例示することができる。権利識別情報を示す情報としては、権利識別情報の符号化データ (例えば、ハッシュ値である。) などを例示することができる。なお、権利識別情報又は権利識別情報を示す情報を、権利 ID と称する場合がある。

30

【 0057 】

既存の賃借権の権利者及び内容を変更するための処理において、ユーザ端末 120 は、例えば、移転用のトランザクションデータを生成して、複数のノード 112 のうちのいずれか 1 つに、当該トランザクションデータを送信する。ユーザ端末 120 は、権利者及び内容の変更に関する移転用のトランザクションデータを生成してもよく、権利者の変更に関する移転用のトランザクションデータと、権利の内容の変更に関する移転用のトランザクションデータとを生成してもよい。権利者に変更がなく、権利の内容にのみ変更がある場合、ユーザ端末 120 は、承継人として現在の権利者を指定する移転用のトランザクションを生成してよい。

40

【 0058 】

移転用のトランザクションデータは、例えば、当該トランザクションが移転用であることを示す情報と、当該トランザクションにより表現される権利に関する情報と、当該権利の承継人に関する情報と、当該トランザクションにより承継される持分に関する情報とを含む。権利に関する情報としては、権利 ID、権利の内容に関する情報などを例示することができる。

【 0059 】

50

図2は、ノード112の内部構成一例を概略的に示す。本実施形態において、ノード112は、通信制御部210と、ブロックチェーン生成部220と、格納部230と、要求処理部240とを備える。格納部230は、例えば、ブロックチェーン格納部232と、公開鍵格納部234とを含む。

【0060】

本実施形態において、通信制御部210は、他のノード112との間の通信、及び、ユーザ端末120との間の通信の少なくとも一方を制御する。目的物30が通信機能を有する場合、通信制御部210は、目的物30との間の通信を制御してもよい。通信制御部210は、外部の機器に情報を送信する送信部として機能してもよく、外部の機器からの情報を受信する受信部として機能してもよい。通信制御部210は、通信インターフェースであってよい。通信制御部210は、複数の種類の通信方式に対応していてもよい。

10

【0061】

通信制御部210は、例えば、他のノード112、ユーザ端末120又は目的物30からの要求を受信して、当該要求を要求処理部240に転送する。通信制御部210は、当該要求に対する応答として、要求処理部240における処理の実行結果を、上記の要求の送信元に送信してよい。通信制御部210は、例えば、ユーザ端末120からのトランザクションデータを受信して、当該トランザクションデータをブロックチェーン生成部220に転送する。通信制御部210は、例えば、ユーザ端末120から、秘密鍵122に対応する公開鍵を受信して、公開鍵格納部234に格納する。上記の公開鍵は、ユーザ端末120からのトランザクションデータに含まれていてもよい。

20

【0062】

ブロックチェーン生成部220は、ユーザ端末120からのトランザクションデータを取得し、ブロックチェーンを生成する。例えば、ブロックチェーン生成部220は、予め定められた期間が経過するごとに、当該期間に取得した1又は複数のトランザクションデータをブロック化して新たなブロックを生成する。上記の予め定められた期間は、厳密に定められた期間であってもよく、凡その期間であってもよい。上記の予め定められた期間内にトランザクションデータが取得されなかった場合、ブロックチェーン生成部220は、新たなブロックを生成してもよく、新たなブロックを生成しなくてもよい。

【0063】

ブロック化の手順は特に限定されるものではないが、例えば、下記の手順で実行される。ブロックチェーン生成部220は、まず、直前のブロックがブロックチェーンに追加された後、予め定められた期間に取得された1又は複数のトランザクションデータを特定する。上記の予め定められた期間にトランザクションデータが取得されなかった場合には、1又は複数のトランザクションデータを特定する工程が省略されてもよい。

30

【0064】

次に、ブロックチェーン生成部220は、ブロックチェーン格納部232に格納されている現在のブロックチェーンにアクセスして、直前のブロックのデータを抽出する。次に、ユーザ端末120は、抽出された直前のブロックをハッシュ化する。ハッシュ化は、符号化の一例であってよい。その後、ブロックチェーン生成部220は、ノンス(nonce; number used once)と呼ばれる数値データを含むヘッダと、直前のブロックのハッシュ値と、予め定められた期間に取得された1又は複数のトランザクションデータとを一纏めにして、新たなブロックを生成する。

40

【0065】

上記の予め定められた期間にトランザクションデータが取得されなかった場合、ブロックチェーン生成部220は、例えば、ノンスを含むヘッダと、直前のブロックのハッシュ値とを一纏めにして、新たなブロックを生成する。新たなブロックに含まれるノンスは、直前のブロックに含まれるノンスと異なる値を有してよい。

【0066】

ブロックチェーン生成部220は、新たなブロックを生成した後、当該ブロックの承認処理を実行する。承認処理の手順は特に限定されるものではないが、例えば、下記の手順

50

で実行される。ブロックチェーン生成部 220 は、まず、新たなブロックをハッシュ化する。ブロックチェーン生成部 220 は、新たなブロックのハッシュ値と、予め定められたターゲットの値とを比較する。新たなブロックのハッシュ値が、予め定められたターゲットの値よりも小さい場合、当該ブロックを承認する。一方、新たなブロックのハッシュ値が、予め定められたターゲットの値よりも大きい場合、新たなブロックに含まれるノンスの値を変更して、上記の処理を繰り返す。ターゲットは、採掘難易度 (d i f f i c u l t y) の算出元となるデータであり、ターゲットが小さいほど、採掘難易度が大きいことを示す。

【 0 0 6 7 】

新たなブロックが承認されると、ブロックチェーン生成部 220 は、当該ブロックを既存のブロックチェーンに追加して、新たなブロックチェーンを生成する。ブロックチェーン生成部 220 は、新たなブロックチェーンをブロックチェーン格納部 232 に格納する。また、ブロックチェーン生成部 220 は、新たなブロックチェーンを他のノード 112 に送信し、他のノード 112 との間で最新のブロックチェーンを共有する。

10

【 0 0 6 8 】

一実施形態において、ブロックチェーン生成部 220 は、権利ごとにブロックチェーンを生成する。例えば、目的物 30 の所有権に関するトランザクションデータと、目的物 30 に設定された賃借権に関するトランザクションデータとを、それぞれ別のブロックチェーンを用いて管理する。他の実施形態において、ブロックチェーン生成部 220 は、目的物ごとにブロックチェーンを生成する。例えば、目的物 30 の所有権に関するトランザクションデータと、目的物 30 に設定された賃借権に関するトランザクションデータとを、同一のブロックチェーンを用いて管理する。

20

【 0 0 6 9 】

本実施形態において、格納部 230 は、様々な情報を格納する。ブロックチェーン格納部 232 は、例えば、ブロックチェーン生成部 220 が生成したブロックチェーンを格納する。公開鍵格納部 234 は、例えば、ユーザ端末 120 の秘密鍵 122 に対応する公開鍵を格納する。格納部 230 は、その他の情報を格納してもよい。

【 0 0 7 0 】

本実施形態において、要求処理部 240 は、分散型台帳管理システム 110 に対する様々な要求を処理する。要求処理部 240 は、処理の結果を、当該要求に対する応答として、当該要求の送信元に送信する。分散型台帳管理システム 110 に対する要求としては、特定の条件に合致するデータを抽出するための要求、特定の条件の成否を判定するための要求などを例示することができる。

30

【 0 0 7 1 】

一実施形態において、要求処理部 240 は、ユーザ端末 120 又は目的物 30 から、権利 ID と、当該権利 ID により特定される権利の権利者の識別情報を抽出するための要求とを受け取る。この場合、要求処理部 240 は、例えば、ブロックチェーン格納部 232 を参照して、上記の権利に関するブロックチェーンにアクセスし、当該権利の権利者の識別情報を抽出する。その後、要求処理部 240 は、抽出された情報を、当該要求に対する応答として、当該要求の送信元に送信する。

40

【 0 0 7 2 】

他の実施形態において、要求処理部 240 は、ユーザ端末 120 又は目的物 30 から、権利 ID と、ユーザ A の識別情報と、ユーザ A が当該権利 ID により特定される権利の権利者であるか否かを判定するための要求とを受け取る。この場合、要求処理部 240 は、例えば、ブロックチェーン格納部 232 を参照して、上記の権利に関するブロックチェーンにアクセスし、当該権利の権利者の識別情報を抽出する。次に、要求処理部 240 は、抽出された権利者の識別情報が、ユーザ A の識別情報と合致するか否かを判定することで、ユーザ A が、当該権利の権利者であるか否かを判定する。その後、要求処理部 240 は、判定結果を示す情報を、当該要求に対する応答として、当該要求の送信元に送信する。

【 0 0 7 3 】

50

他の実施形態において、要求処理部 240 は、ユーザ端末 120 又は目的物 30 から、ユーザ A の識別情報と、ユーザ A が有する権利の権利 ID を抽出するための要求とを受け取る。この場合、要求処理部 240 は、例えば、ブロックチェーン格納部 232 を参照して、ブロックチェーン格納部 232 に格納された 1 又は複数のブロックチェーンにアクセスし、各ブロックチェーンに対応する権利の現在の権利者の識別情報を抽出する。次に、要求処理部 240 は、抽出された権利者の識別情報が、ユーザ A の識別情報と合致するかどうかを判定することで、ユーザ A が、各ブロックチェーンに対応する権利の現在の権利者であるかどうかを判定する。その後、要求処理部 240 は、ユーザ A が現在の権利者であると判定された権利の権利 ID を、当該要求に対する応答として、当該要求の送信元に送信する。

10

【0074】

図 3 ~ 図 5 を用いて、ブロックチェーン格納部 232 に格納されるデータのデータ構造の一例について説明する。図 3 は、ブロックチェーン 300 のデータ構造の一例を概略的に示す。ブロックチェーン 300 は、時系列に連続する複数のブロックを含む。図 3 においては、説明を簡単にする目的で、ブロックチェーン 300 を構成する複数のブロックのうち、ブロック B_i と、ブロック B_i 用の直前のブロックであるブロック B_{i-1} とを示す (i は 2 以上の正の整数である)。本実施形態において、複数のブロックのそれぞれは、ブロックヘッダ 310 と、1 又は複数のトランザクションデータ 320 とを含む。1 又は複数のトランザクションデータ 320 のそれぞれは、一の権利の変動に関するトランザクション情報の一例であってよい。

20

【0075】

本実施形態において、単一のブロックの中に、複数の権利に関するトランザクションデータが含まれる場合について説明した。しかしながら、ブロックのデータ構造は本実施形態に限定されない。他の実施形態によれば、単一のブロックは、単一の権利に関するトランザクションデータを含み、他の権利に関するトランザクションデータを含まない。

【0076】

本実施形態において、単一のブロックの中に、複数のトランザクションデータが含まれる場合について説明した。しかしながら、ブロックのデータ構造は本実施形態に限定されない。他の実施形態によれば、単一のブロックの中には、単一のトランザクションデータが含まれる。さらに他の実施形態によれば、単一のブロックの中に、トランザクションデータが含まれなくてもよい。トランザクションデータが生成されるタイミングと、ブロックが生成されるタイミングとの関係によっては、トランザクションデータが含まれないブロックが生成され得る。

30

【0077】

図 4 に示すとおり、本実施形態において、ブロックヘッダ 310 は、ブロック B_i (現在のブロックと称する場合がある。) のブロックバージョン 410 と、ブロック B_{i-1} (直前のブロックと称する場合がある。) のブロックヘッダのハッシュ値 412 と、ブロック B_i のトランザクションデータのマークル・ルートのハッシュ値 414 と、ブロック B_i のブロックロック時間 416 と、ブロック B_i のブロックロック時における採掘処理のターゲット 418 と、ブロック B_i の採掘処理で算出されたノンス 420 とを含む。

40

【0078】

本実施形態において、ブロックバージョン 410 は、ブロック化のルール、プロトコル又はアルゴリズムのバージョンを示す。ブロックロック時間 416 は、ブロック B_i が承認された時刻を示す。ブロック B_i が承認された時刻は、ブロック B_i に含まれる 1 以上のトランザクションデータがブロック化された時間の一例であってよい。ターゲット 418 は、ブロック B_i の承認処理におけるターゲットを示す。ハッシュ値は、符号化データの一例であってよく、ハッシュ化は、符号化の一例であってよい。

【0079】

図 5 は、権利の変動に関するトランザクションデータ 500 のデータ構造の一例を概略的に示す。本実施形態において、トランザクションデータ 500 は、バージョン 502 と

50

、入力数 5 0 4 と、1 又は複数の入力 5 0 6 と、出力数 5 0 8 と、1 又は複数の出力 5 1 0 と、ブロックロック時間 5 1 2 とを有する。本実施形態において、バージョン 5 0 2 は、トランザクションデータ 5 0 0 のフォーマット又はプロトコルを定めたルールのバージョンを示す。入力数 5 0 4 は、入力 5 0 6 の数を示す。出力数 5 0 8 は、出力 5 1 0 の数を示す。ブロックロック時間 5 1 2 は、トランザクションデータ 5 0 0 を含むブロックが承認された時刻を示す。

【 0 0 8 0 】

本実施形態において、1 又は複数の入力 5 0 6 のそれぞれは、例えば、直前のトランザクションデータのハッシュ値 5 2 2 と、直前の出力インデックス 5 2 4 と、署名スクリプト 5 2 8 のサイズ 5 2 6 と、署名スクリプト 5 2 8 と、シーケンス終端記号 5 3 4 とを含む。署名スクリプト 5 2 8 は、トランザクションデータ 5 0 0 の署名値 5 3 0 と、現在の権利者の秘密鍵に対応する公開鍵 5 3 2 とを含んでもよい。

10

【 0 0 8 1 】

トランザクションデータ 5 0 0 の署名値 5 3 0 は、トランザクションデータ 5 0 0 の少なくとも一部を、現在の権利者（被承継人と称される場合がある。）の秘密鍵で暗号化した暗号化データであってよい。トランザクションデータ 5 0 0 の一部又は全体を現在の権利者の秘密鍵により暗号化して署名値 5 3 0 を生成する方法は、公知の暗号通貨におけるトランザクションを生成する手法、又は、将来的に開発された暗号通貨におけるトランザクションを生成する手法を採用してよい。

【 0 0 8 2 】

本実施形態において、1 又は複数の出力 5 1 0 のそれぞれは、例えば、承継される持分 5 4 2 と、公開鍵検証スクリプト 5 4 6 のサイズ 5 4 4 と、公開鍵検証スクリプト 5 4 6 とを含む。公開鍵検証スクリプト 5 4 6 は、承継人の公開鍵のハッシュ値 5 4 8 と、トランザクションデータの種類に関する情報 5 5 0 と、権利に関する情報 5 5 2 とを含んでもよい。

20

【 0 0 8 3 】

本実施形態において、承継人の公開鍵のハッシュ値 5 4 8 は、トランザクションデータ 5 0 0 により表現される権利の変動における、当該権利の 1 以上の承継先を示す。上記の権利変動において権利者に変更がない場合、承継人の公開鍵のハッシュ値 5 4 8 は、被承継人の公開鍵のハッシュ値であってよい。トランザクションデータの種類に関する情報 5 5 0 は、トランザクションデータ 5 0 0 が発行用のトランザクションデータであるか、移転用のトランザクションデータであるかを示す情報であってよい。

30

【 0 0 8 4 】

権利に関する情報 5 5 2 としては、権利 ID、権利の内容に関する情報（内容情報と称する場合がある。）などを例示することができる。内容情報としては、（ i ）権利の客体又は目的物の特徴、仕様又は状態に関する情報、（ i i ）権利の客体又は目的物の変更に関する情報、（ i i i ）権利の制限に関する情報、（ i v ）権利行使の条件に関する情報などを例示することができる。

【 0 0 8 5 】

内容情報は、（ i ）変動後の権利の内容又は権利変動の内容（権利の内容又は権利変動の内容を、権利又は権利変動の内容と称する場合がある。）を示すデータであってもよく、（ i i ）権利又は権利変動の内容を記録したデータの U R I であってもよく、（ i i i ）権利又は権利変動の内容を記録したデータの符号化データであってもよい。権利又は権利変動の内容を記録したデータは、分散型台帳管理システム 1 1 0 とは別の第 2 データベースシステム（内容情報格納部の一例であってよい。）、又は、当該第 2 データベースシステムに含まれるレコード、若しくは、当該レコードの一部であってもよい。上記のレコードの一部は、キー・バリュ型データベースのバリュー値であってもよい。

40

【 0 0 8 6 】

本実施形態において、トランザクションデータ 5 0 0 は、ブロックチェーン 3 0 0 のブロック B_i を構成するトランザクションデータ 3 2 0 の一例であってよい。トランザクシ

50

ョンデータ500は、移転用（転送用と称される場合もある。）のトランザクションデータの一例であってもよい。トランザクションデータ500は、第1トランザクション情報の一例であってもよい。直前のトランザクションデータは、第2トランザクション情報の一例であってもよい。ハッシュ値は、符号化データの一例であってもよく、ハッシュ化は、符号化の一例であってもよい。署名値530は、トランザクションデータ500の少なくとも一部を、被承継人の秘密鍵で暗号した暗号化データの一例であってもよい。被承継人は、一の権利を有するユーザの一例であってもよい。被承継人の公開鍵532は、被承継人を識別する識別情報の一例であってもよい。承継人の公開鍵は、承継人を識別する識別情報の一例であってもよい。

【0087】

本実施形態においては、入力数504及び出力数508が1又は複数である場合について説明した。しかしながら、トランザクションデータ500は本実施形態に限定されない。他の実施形態において、トランザクションデータ500は、入力数504及び出力数508の少なくとも一方が0であってもよい。

【0088】

本実施形態においては、トランザクションデータ500が移転用のトランザクションデータである場合について説明した。しかしながら、トランザクションデータ500は本実施形態に限定されない。他の実施形態において、トランザクションデータ500は、発行用のトランザクションデータであってもよい。

【0089】

トランザクションデータ500が発行用のトランザクションデータである場合、トランザクションデータ500の入力506は、予め定められたルール又はプロトコルに従って、発行用のトランザクションデータであることを示すための特別なデータが入力されてよい。例えば、直前のトランザクションデータのハッシュ値522及び直前の出力インデックス524に、予め定められた特別なデータが入力される。また、トランザクションデータ500は、トランザクションデータ500により表現される権利の発行条件に関する情報を示すデータを更に含んでよい。発行条件に関する情報は、上述のとおりであってもよい。

【0090】

さらに他の実施形態において、トランザクションデータ500は、ブロックチェーン技術を利用した暗号通貨のトランザクション情報であってもよい。この場合、権利IDは、上記の暗号通貨を一意に特定する通貨識別情報であってもよい。暗号通貨の通貨識別情報として権利IDを用いることで、既存の暗号通貨のプラットフォームを利用して、又は、既存の暗号通貨のプラットフォームと同様の仕組みを利用して、当該権利IDにより識別される権利の変動の履歴を管理することができる。また、各ユーザの暗号通貨の保有量は、各ユーザが有する権利の持分に応じて決定されてよい。この場合、上記のアセットの量の上限值を指定する情報は、暗号通貨の全発行量を定義する情報の一例であってもよい。

【0091】

図5の実施形態においては、トランザクションデータ500が、残高に関する情報を格納する領域のみを有する場合について説明した。しかしながら、トランザクションデータ500は、本実施形態に限定されない。他の実施形態において、トランザクションデータ500は、ノード112のコンピュータにより実行されるプログラム（コードと称する場合がある。）を含んでもよい。

【0092】

この場合、トランザクションデータ500は、例えば、(i)図5に関連して説明したような、残高に関する情報を格納する領域に加えて、(ii)コードを格納する領域（コード格納領域と称する場合がある。）と、(iii)コードの実行に関するデータを格納する領域（データ格納領域と称する場合がある。）とを有する。トランザクションデータ500は、図5に関連して説明したような、残高に関する情報を格納する領域に代えて、(i)コードを格納する領域（コード格納領域と称する場合がある。）と、(ii)コー

10

20

30

40

50

ドの実行に関するデータを格納する領域（データ格納領域と称する場合がある。）とを有してもよい。

【0093】

コードの実行手順は、例えば、下記のとおりである。まず、ノード112が、他の端末（例えば、ユーザ端末120である。）から、ノード112に格納されているトランザクションデータ500に含まれるコードの実行を開始させるためのメッセージを受信する。ノード112が上記のメッセージを受信すると、ノード112のコンピュータは、コードを自動的に実行させる。ノード112のコンピュータは、上記のコードの実行結果を、トランザクションデータ500のデータ格納領域に格納してもよい。ノード112のコンピュータは、格納されたコードを特定するためのアドレスを発行してもよい。

10

【0094】

上記のコードとしては、(i)権利の承継元及び当該権利の承継先間の契約内容を示す情報（コントラクトと称される場合がある。）として、各種のコードを、分散型台帳管理システム110に登録するためのコード、(ii)コントラクトとして登録されたコードに対して命令を実行するためのコード、(iii)トランザクションを生成するためのコード、及び、これらの組み合わせを例示することができる。上記のコードは、スマートコントラクトコードであってもよい。

【0095】

例えば、エスクローサービスを実現する場合、トランザクションデータ500のコード格納領域には、(i)コンピュータに、エスクローサービス提供者によるエスクローサービスを具現化するコードを、分散型台帳管理システム110に登録するための処理を実行させるためのコード、(ii)コンピュータに、契約内容を記録する処理を実行させるためのコード、(iii)コンピュータに、目的物の所有権を、目的物の販売者から、エスクローサービス提供者に移転する処理を実行させるためのコード、(iv)コンピュータに、目的物の所有権を、エスクローサービス提供者から、目的物の購入者に移転する処理を実行させるためのコード、(v)コンピュータに、目的物の代金に相当する額の暗号通貨を、目的物の購入者から、エスクローサービス提供者に移転する処理を実行させるためのコード、(vi)コンピュータに、目的物の代金に相当する額の暗号通貨を、エスクローサービス提供者から、目的物の販売者に移転する処理を実行させるためのコードなどが格納される。

20

30

【0096】

上記の契約内容としては、契約を締結したことを示す情報、目的物の所有権を、当該目的物の購入者に、特定の金額で譲渡したことを示す情報などを例示することができる。上記の各コードが実行されることにより、各コードの目的に応じたトランザクションが生成されてよい。上記の各コードには、各コードを実行するための条件が定義されていてもよい。

【0097】

図5の実施形態においては、権利に関する情報552が、公開鍵検証スクリプト546の領域に格納されている場合について説明した。しかしながら、権利に関する情報552が格納される領域は、公開鍵検証スクリプト546に限定されない。権利に関する情報552は、トランザクションデータ500内の任意の領域に格納されてよい。例えば、権利に関する情報552は、上記のコードを格納する領域に格納される。

40

【0098】

図6は、ユーザ端末120の内部構成の一例を概略的に示す。本実施形態において、ユーザ端末120は、通信制御部610と、入出力部620と、トランザクションデータ生成部630と、格納部640と、要求生成部650とを備える。格納部640は、鍵情報格納部642と、トランザクションデータ格納部644とを有してよい。

【0099】

通信制御部610は、トランザクション情報送信部、命令送信部、又は、要求送信部の一例であってよい。入出力部620は、入力部の一例であってよい。トランザクションデ

50

ータ生成部 630 は、暗号化部、権利変動判定部、鍵生成部、又は、内容情報更新部の一例であってよい。格納部 640 は、内容情報格納部の一例であってよい。

【0100】

本実施形態において、通信制御部 610 は、分散型台帳管理システム 110 又は複数のノード 112 との間の通信を制御する。目的物 30 が通信機能を有する場合、通信制御部 610 は、目的物 30 との間の通信を制御してもよい。通信制御部 610 は、外部の機器に情報を送信する送信部として機能してもよく、外部の機器からの情報を受信する受信部として機能してもよい。通信制御部 610 は、通信インターフェースであってよい。通信制御部 610 は、複数の種類の通信方式に対応していてもよい。

【0101】

[トランザクションデータの送信]

本実施形態において、通信制御部 610 は、トランザクションデータ生成部 630 が生成したトランザクションデータを、分散型台帳管理システム 110 に送信する。トランザクションデータ生成部 630 は、例えば、特定の権利の変動を検出した場合に、当該権利の変動に関するトランザクションデータを生成する。

【0102】

一実施形態において、トランザクションデータは、当該トランザクションデータにより表現される権利の権利 ID を含む。他の実施形態において、トランザクションデータにはメタデータが付与されており、当該メタデータ中に、トランザクションデータにより表現される権利の権利 ID が含まれていてもよい。

【0103】

トランザクションデータは、少なくとも、(i) 特定の権利の変動における当該権利の 1 以上の承継先を示す承継先情報（例えば、図 5 のハッシュ値 548 である。）と、(ii) 上記の権利の直前の変動に関するトランザクションデータの符号化データ（例えば、図 5 のハッシュ値 522 である。）とを含む。上記のトランザクションデータは、上記の権利変動に関するトランザクションデータの少なくとも一部を現在の権利者の秘密鍵で暗号化したデータ（例えば、図 5 の署名値 530 である。）をさらに含んでよい。

【0104】

これにより、通信制御部 610 は、上記の権利変動に関するトランザクションデータを分散型台帳管理システム 110 に送信する場合に、上記の権利の権利 ID と、当該権利変動に関するトランザクションデータの少なくとも一部を現在の権利者の秘密鍵で暗号化したデータ（例えば、図 5 の署名値 530 である。）とを対応付けて、分散型台帳管理システム 110 に送信することができる。なお、権利管理システム 100 が暗号通貨を利用して特定の権利を表現する場合、上記の権利 ID は、当該暗号通貨の通貨識別情報であってよい。上記の暗号通貨は、ビットコイン 2.0 又は暗号通貨 2.0 のルール又はプロトコルに準じたプラットフォーム上で実現されてもよい。上記のプラットフォームとしては、カラードコイン (Colored Coins)、カウンターパーティ (Counterparty)、オムニ (Omni)、イーサリアム (Ethereum) などを例示することができる。

【0105】

上述のとおり、トランザクションデータは、内容情報（例えば、図 5 の権利に関する情報 552 である。）をさらに含み得る。トランザクションデータは、内容情報が符号化されたデータを含んでもよい。内容情報は、分散型台帳管理システム 110 とは別の第 2 データベースシステム（内容情報格納部の一例であってよい。）、又は、当該第 2 データベースシステムに含まれるレコード、若しくは、当該レコードの一部であってよい。

【0106】

例えば、プラットフォームとして、ビットコイン又はカラードコインが利用される場合において、上記の権利変動において権利者に変更がないとき、トランザクションデータの承継先情報には、権利の承継先として被承継人を指定する情報が記載されてもよい。これにより、ビットコインなどのように残高情報以外の情報を取り扱うことが予定されてい

10

20

30

40

50

いプラットフォームを利用して、権利変動を表現することができる。他の実施形態において、プラットフォームとして、イーサリアムなどのスマートコントラクトが利用されるには、トランザクションデータの適切な領域に、内容変動を示すコードが記載される。

【 0 1 0 7 】

そこで、分散型台帳管理システム 1 1 0 とは別に、内容情報を記録する第 2 データベースシステムが存在する場合において、権利管理システム 1 0 0 を利用することにより、第 2 データベースシステムに格納された内容情報の存在又は信憑性を保証することができる。例えば、第 2 データベースシステムに格納される内容情報が生成されたり、第 2 データベースシステムに格納された内容情報が更新されたりするたびに、生成又は更新された内容情報に対応する権利の変動に関するトランザクションデータが生成される。このとき、トランザクションデータの適切な領域に、第 2 データベースシステムに格納された内容情報の符号化データ（例えば、ハッシュ値である。）が記録されてよい。生成されたトランザクションデータは、分散型台帳管理システム 1 1 0 に送信される。

10

【 0 1 0 8 】

上記のトランザクションデータがブロックチェーンに組み込まれることで、当該トランザクションデータの存在又は信憑性が保証される。その結果、第 2 データベースシステムに格納された内容情報の存在又は信憑性も保証される。新たに生成された内容情報の第 2 データベースへの格納処理、又は、第 2 データベースシステムに格納された内容情報の更新処理と、トランザクションデータの生成処理又は送信処理との順番は、特に限定されるものではない。第 2 データベースシステムは、内容情報格納部の一例であってよい。第 2 データベースシステムは、ユーザ端末 1 2 0 に配されてもよく、分散型台帳管理システム 1 1 0 及びユーザ端末 1 2 0 とは異なる情報処理装置上に構築されてもよい。

20

【 0 1 0 9 】

一実施形態において、第 2 データベースシステムに格納された内容情報へのアクセスが制限されてもよい。例えば、格納されたデータの読み込み及び書出しの少なくとも一方が制限される。格納されたデータの閲覧、保存、送信、出力及び複製の少なくとも 1 つが制限されてもよい。上記のアクセス制限は、(i) 第 2 データベースシステムによって実行されてもよく、(i i) 分散型台帳管理システム 1 1 0 により実行されてもよく、(i i i) 第 2 データベースシステム、分散型台帳管理システム 1 1 0、ユーザ端末 1 2 0 及び目的物 3 0 の少なくとも 2 つの間に介在する情報処理システムにより実行されてもよく、(i v) ユーザ端末 1 2 0 により実行されてもよい。

30

【 0 1 1 0 】

[各種要求の送信]

本実施形態において、通信制御部 6 1 0 は、要求生成部 6 5 0 が生成した各種の要求を送信する。例えば、通信制御部 6 1 0 は、上記の要求を、分散型台帳管理システム 1 1 0 に送信する。通信制御部 6 1 0 は、ユーザに対する要求を入出力部 6 2 0 に送信して、当該要求を出力させてもよい。目的物 3 0 が通信機能を有する場合、通信制御部 6 1 0 は、目的物 3 0 に対して、各種の要求又は命令を送信してもよい。通信制御部 6 1 0 は、目的物 3 0 から送信された情報を受信してもよい。通信制御部 6 1 0 は、上記の要求又は命令の実行に必要な情報を、当該要求又は命令に対応付けて送信してもよい。通信制御部 6 1 0 は、要求に対する応答を受信してもよい。

40

【 0 1 1 1 】

本実施形態において、入出力部 6 2 0 は、ユーザ端末 1 2 0 への入力を受け付ける。入出力部 6 2 0 は、ユーザから、任意の権利に対する指示を受け付けてよい。上記の指示は、ユーザ端末 1 2 0 の操作に関する指示であってもよい。例えば、ユーザが、ユーザ端末 1 2 0 を利用してオンラインゲームをプレイしている場合、当該ゲーム内でアイテムを入手するための操作（例えば、入力ボタンを押下する操作である。）は、上記の指示に該当する。

【 0 1 1 2 】

本実施形態において、入出力部 6 2 0 は、ユーザ端末 1 2 0 から情報を出力する。入出

50

力部 620 としては、キーボード、ポインティングデバイス、タッチパネル、マイク、カメラ、センサ、GPS 受信機などの入力装置、又は、表示装置、スピーカ、振動装置などの出力装置を例示することができる。入出力部 620 は、ユーザ・インタフェースであってもよい。

【0113】

本実施形態において、トランザクションデータ生成部 630 は、トランザクションデータを生成する。トランザクションデータ生成部 630 は、生成されたトランザクションデータをトランザクションデータ格納部 644 に格納する。また、トランザクションデータ生成部 630 は、通信制御部 610 を介して、生成されたトランザクションデータを分散型台帳管理システム 110 に送信する。

10

【0114】

トランザクションデータ生成部 630 は、ユーザ A の秘密鍵 122 と、秘密鍵 122 に対応する公開鍵とを生成してよい。トランザクションデータ生成部 630 は、上記の秘密鍵 122 及び公開鍵を鍵情報格納部 642 に格納してもよい。

【0115】

トランザクションデータの生成方法は特に限定されるものではないが、トランザクションデータ生成部 630 は、例えば、下記の手順により、現在の権利者がユーザ A である権利 R の i 番目の変動 V_i に関する移転用のトランザクションデータ T_i を生成する (i は 2 以上の正の整数である)。なお、変動 V_i において権利 R は移転せず、権利 R の内容に変更が生じる場合には、承継先として被承継人を指定する承継先情報を含むトランザクションデータ T_i を生成してよい。また、発行用のトランザクションデータ T_1 も、同様の手順により生成することができる。

20

【0116】

まず、トランザクションデータ生成部 630 は、少なくとも、(i) 変動 V_i における権利 R の 1 以上の承継先を示す承継先情報と、($i-1$) 権利 R の直前の変動 V_{i-1} に関するトランザクションデータ T_{i-1} の符号化データとを含む、仮のトランザクションデータを生成する。仮のトランザクションデータは、権利 ID を含んでもよい。仮のトランザクションデータは、変動 V_i において承継される権利 R の持分に関する情報を含んでもよい。仮のトランザクションデータは、変動 V_i における権利 R の内容の変更を示す内容情報を含んでもよい。上記の内容情報は、権利又は権利変動の内容を記録したデータの符号化データであってよい。

30

【0117】

仮のトランザクションデータは、トランザクションデータ T_i の署名スクリプト部分に、任意のデータを仮置きしたデータであってもよい。任意のデータは、ユーザ A の公開鍵のハッシュ値であってもよい。仮のトランザクションデータは、暗号化部による暗号化の対象となるトランザクションデータの少なくとも一部の一例であってよい。

【0118】

次に、トランザクションデータ生成部 630 は、仮のトランザクションデータの全体を、ユーザ A の秘密鍵 122 で暗号化して、トランザクションデータ T_i の署名値を生成する。その後、トランザクションデータ生成部 630 は、生成されたトランザクションデータ T_i の署名値と、ユーザ A の公開鍵とを、トランザクションデータ T_i の適切な領域に配置して、最終的なトランザクションデータ T_i を生成する。

40

【0119】

本実施形態において、トランザクションデータ生成部 630 は、権利 R の変動 V_i を検出した場合に、当該変動 V_i に関するトランザクションデータ T_i を生成する。一実施形態において、トランザクションデータ生成部 630 は、入出力部 620 がユーザからの指示を受け付けた場合に、当該指示の実行による権利変動の有無を判定する。他の実施形態において、トランザクションデータ生成部 630 は、通信制御部 610 が目的物 30 からの要求を受信した場合に、当該要求の実行による権利変動の有無を判定してもよい。トランザクションデータ生成部 630 は、目的物 30 からの要求に応じて、トランザクシ

50

データ T_i を生成してもよい。

【 0 1 2 0 】

トランザクションデータ生成部 6 3 0 は、上記の指示の実行により権利変動 V_i が生じると判定した場合に、当該変動 V_i に関するトランザクションデータ T_i を生成する。この場合において、トランザクションデータ T_i が、権利又は権利変動の内容を記録したデータの URI 又は符号化データを含む場合、トランザクションデータ生成部 6 3 0 は、分散型台帳管理システム 1 1 0 とは別の第 2 データベースシステムにアクセスして、上記の権利又は権利変動の内容を記録したデータを生成又は更新してよい。

【 0 1 2 1 】

トランザクションデータ生成部 6 3 0 は、入出力部 6 2 0 がユーザから指示を受け付けるたびに、当該指示の実行による権利変動の有無を判定してもよい。上記の指示は、特定の権利を変動させることを主目的とする処理又は操作に関する指示であってもよく、上記の指示は、特定の権利を変動させることを主目的としない処理又は操作に関する指示であってもよい。

10

【 0 1 2 2 】

格納部 6 4 0 は、様々な情報を格納する。鍵情報格納部 6 4 2 は、ユーザ A の秘密鍵 1 2 2 を格納する。鍵情報格納部 6 4 2 は、秘密鍵 1 2 2 に対応する公開鍵を格納してもよい。鍵情報格納部 6 4 2 は、複数のユーザのそれぞれの秘密鍵及び公開鍵を格納してもよい。トランザクションデータ格納部 6 4 4 は、トランザクションデータ生成部 6 3 0 が生成したトランザクションデータを格納する。格納部 6 4 0 は、その他の情報を格納しても

20

【 0 1 2 3 】

要求生成部 6 5 0 は、各種の要求を生成する。要求生成部 6 5 0 は、分散型台帳管理システム 1 1 0 に対する要求を生成してよい。例えば、要求生成部 6 5 0 は、分散型台帳管理システム 1 1 0 に対して、(i) 特定のユーザが有する権利を示す情報の抽出、(i i) 特定の権利を有する者を示す情報の抽出、又は、(i i i) 特定のユーザが特定の権利を有するか否かの判定を要求するデータを生成する。要求生成部 6 5 0 は、目的物 3 0 に対する要求を生成してもよく、ユーザ A に対する要求を生成してもよい。

【 0 1 2 4 】

要求生成部 6 5 0 は、上記の要求と対応付けて、特定のユーザを識別するために用いられるユーザ識別情報を、分散型台帳管理システム 1 1 0 に送信してよい。ユーザ識別情報は、当該ユーザの秘密鍵に対応する公開鍵又は当該公開鍵の符号化データであってもよい。ユーザ識別情報は、当該ユーザが利用するユーザ端末を識別するために用いられる端末識別情報であってもよい。要求生成部 6 5 0 は、上記の要求と対応付けて、特定の権利の権利 ID を、分散型台帳管理システム 1 1 0 に送信してよい。

30

【 0 1 2 5 】

図 7 は、データテーブル 7 0 0 の一例を概略的に示す。データテーブル 7 0 0 は、分散型台帳管理システム 1 1 0 にブロックチェーンとして格納されている情報を表形式で表現した場合の一実施形態を示す。本実施形態において、データテーブル 7 0 0 は、トランザクション ID 7 0 2 と、承継元のユーザ ID 7 0 4 と、承継先のユーザ ID 7 0 6 と、権利 ID 7 0 8 と、持分情報 7 1 0 と、内容情報 7 1 2 とを含む。

40

【 0 1 2 6 】

トランザクション ID 7 0 2 には、各トランザクションデータを識別する識別情報が記録される。被承継人のユーザ ID 7 0 4 には、各トランザクションデータに対応する権利変動における承継元のユーザのユーザ識別情報が記録される。承継人のユーザ ID 7 0 6 には、各トランザクションデータに対応する権利変動における承継先のユーザのユーザ識別情報が記録される。ユーザ識別情報としては、ユーザの名称、ユーザのアカウント名、ユーザのアドレス、ユーザの秘密鍵などを例示することができる。権利 ID 7 0 8 には、各トランザクションデータにより表現される権利の権利 ID が記録される。権利 ID は、権利の目的物を識別するための情報であってもよく、権利の目的物及び当該権利の種類を

50

識別するための情報であってもよい。持分情報 710 には、各トランザクションデータに対応する権利変動において承継される権利の持分に関する情報が記録される。内容情報 712 には、権利又は権利変動の内容を示す情報が記録される。内容情報 712 には、権利又は権利変動の内容を記録したデータの U R I 又は符号化データが記録されてもよい。

【0127】

権利管理システム 100 が、暗号通貨を利用して特定の権利を表現する場合、被承継人のユーザ ID 704 は当該暗号通貨の From アドレスに対応する。同様に、承継人のユーザ ID 706 は当該暗号通貨の To アドレスに対応し、権利 ID 708 は当該暗号通貨の通貨識別情報（例えば、暗号化通貨の名称又は当該暗号化通貨のプラットフォームの名称である。）に対応し、持分情報 710 は当該暗号通貨の枚数に対応する。

10

【0128】

図 8 は、データテーブル 800 の一例を概略的に示す。データテーブル 800 は、分散型台帳管理システム 110 とは別のデータベースシステムであって、内容情報を記録する第 2 データベースシステムに格納されるデータの一例を示す。この場合、データテーブル 700 の内容情報 712 には、例えば、内容情報を記録したデータの U R I、又は、当該内容情報の符号化データが記録される。本実施形態において、データテーブル 800 は、内容情報 804 と、内容情報 804 を符号化して得られた符号化データ 802 とを対応付けて格納する。符号化データ 802 は、例えば、内容情報 804 のハッシュ値である。符号化データ 802 は、内容情報 804 及び他の情報を含むデータのハッシュ値であってもよい。上記の他の情報としては、タイムスタンプ、IP アドレスなどを例示することができる。この場合、符号化後のデータの使いまわしを防止することができる。

20

【0129】

データテーブル 700 及びデータテーブル 800 を利用することで、データテーブル 800 に格納された内容情報 804 が改竄されていないことを実用上十分な精度で保証することができる。例えば、データテーブル 700 の内容情報 712 に、内容情報を記録したデータの符号化データが記録されている場合において、データテーブル 700 の内容情報 712 に記録された符号化データと、データテーブル 800 の符号化データ 802 に記録された符号化データとが一致すれば、データテーブル 800 に格納された内容情報 804 が改竄されていないと判断できる。なお、他の実施形態において、データテーブル 800 は、内容情報 804 と、内容情報 804 に関連する権利を識別するための権利 ID とを対応付けて格納してもよい。

30

【0130】

図 16 及び図 17 を用いて、分散型台帳管理システム 110 にブロックチェーンとして格納されている情報の他の例について説明する。図 16 は、データテーブル 2200 の一例を概略的に示す。データテーブル 2200 は、分散型台帳管理システム 110 にブロックチェーンとして格納されている情報を表形式で表現した一実施形態を示す。図 17 は、コントラクトオブジェクト 2300 の一例を概略的に示す。コントラクトオブジェクト 2300 は、データテーブル 2200 において、トランザクション ID が T_1 であるレコードに格納されたコードの一例である。コントラクトオブジェクト 2300 は、所有権を移転させるための命令と、権利の内容変動を記録するための命令とを含む。

40

【0131】

本実施形態において、データテーブル 2200 は、図 7 に関連して説明した処理と同様の処理を、いわゆるスマートコントラクトの技術を利用して実現した場合におけるデータテーブルの一例である。本実施形態において、データテーブル 2200 は、トランザクション ID 2202 と、操作アカウント 2204 と、ブロックチェーンに登録された実行対象のコード 2206 と、コードの呼出内容 2208 とを含む。データテーブル 2200 は、備考欄 2210 を有してもよい。

【0132】

トランザクション ID 2202 には、各トランザクションデータを識別する識別情報が格納される。操作アカウント 2204 には、各トランザクションデータに対応する権利変

50

動を発生させたユーザを識別する識別情報が格納される。実行対象のコード 2206 には、例えば、ブロックチェーンに格納されたコードのうち、各トランザクションで実行対象となるコードのアドレスが記録される。コードの呼出内容 2208 には、各トランザクションにおける実行対象のコードが保持する関数のうち、実行対象となる関数と、当該関数の引数とが記録される。実行対象のコード 2206 及びコードの呼出内容 2208 は、コード格納領域の一例であってよい。備考欄 2210 には、例えば、コードの簡単な説明が格納される。

【0133】

[権利管理システム 900 のシステム構成]

図 9 は、権利管理システム 900 のシステム構成の一例を概略的に示す。権利管理システム 900 によれば、キーレスエントリーシステム、レンタル又はシェアリングシステム、遠隔操作システム、エスクローシステム、決済システム、マッチングシステム、オークションシステム、オンラインゲームシステム、アップデートプログラムの配布システムなどを実現することができる。

【0134】

本実施形態において、権利管理システム 900 は、ユーザ端末 920 を備える。権利管理システム 900 は、分散型台帳管理システム 110 をさらに備えてよい。権利管理システム 900 は、目的物 930 をさらに備えてよい。権利管理システム 900 は、権利管理サーバ 940 をさらに備えてよい。本実施形態において、権利管理サーバ 940 は、内容情報格納部 942 と、情報管理部 944 とを有する。権利管理システム 900 は、データ管理システム 20 20 の一例であってよい。ユーザ端末 920 は、データ管理システム又は情報処理装置の一例であってよい。権利管理サーバ 940 又は内容情報格納部 942 は、第 2 データベースシステム 20 の一例であってよい。権利管理サーバ 940 又は情報管理部 944 は、内容情報更新部の一例であってよい。

【0135】

説明を簡単にすることを目的として、本実施形態においては、権利管理サーバ 940 が内容情報格納部 942 を備える場合について説明する。しかしながら、内容情報格納部 942 は本実施形態に限定されない。他の実施形態において、内容情報格納部 942 は、権利管理サーバ 940 の外部に配され、権利管理サーバ 940 との間で情報を送受することができるデータベースシステム 30 30 であってよい。

【0136】

本実施形態において、ユーザ端末 920 は、目的物 930 に対する命令を生成し、当該命令を目的物 930 に送信する点で、ユーザ端末 120 と相違する。ユーザ端末 920 は、近距離無線通信又は有線通信により、上記の命令を、目的物 930 に直接送信してよい。上記の相違点以外の点に関し、ユーザ端末 920 は、ユーザ端末 120 と同様の構成を有してよい。

【0137】

本実施形態において、目的物 930 は、通信機能を有し、分散型台帳管理システム 110、ユーザ端末 920 及び権利管理サーバ 940 との間で情報を送受する点で、目的物 30 と相違する。目的物 930 は、通信ネットワーク 10 を介して、分散型台帳管理システム 110、ユーザ端末 920 及び権利管理サーバ 940 との間で情報を送受してよい。目的物 930 は、近距離無線通信又は有線通信により、ユーザ端末 920 との間で情報を送受してもよい。目的物 930 は、権利管理サーバ 940 を介して、分散型台帳管理システム 110 及びユーザ端末 920 との間で情報を送受してもよい。

【0138】

目的物 930 は、ユーザ端末 920 からの命令を受信し、分散型台帳管理システム 110 に格納されたブロックチェーンに基づいて当該命令の実行の可否を判断する点で、目的物 30 と相違する。上記の相違点以外の点に関し、目的物 930 は、目的物 30 と同様の構成を有してよい。本実施形態において、目的物 930 は、分散型台帳管理システム 110 などにおける情報処理において目的物 930 のコンピュータを特定又は識別するための

10

20

30

40

50

秘密鍵 932 を格納していてもよい。なお、目的物 930 のコンピュータを特定したり又は識別したりする必要がない場合、目的物 930 は、秘密鍵 932 を格納していなくてもよい。

【0139】

例えば、目的物 930 のコンピュータは、秘密鍵 932 を用いて、目的物 930 に関する権利変動を示すトランザクションデータを作成し、当該トランザクションデータを分散型台帳管理システム 110 に登録する。例えば、分散型台帳管理システム 110 に格納されたトランザクションデータに、秘密鍵 932 により暗号化された署名値が含まれている場合、分散型台帳管理システム 110 は、当該トランザクションデータが目的物 930 のコンピュータにより生成されたことを特定できる。これにより、分散型台帳管理システム 110 は、秘密鍵 932 を用いて、目的物 930 のコンピュータを特定したり又は識別したりすることができる。

10

【0140】

[権利管理システム 900 による権利管理の概要]

本実施形態において、分散型台帳管理システム 110 は、目的物 930 に関する権利の変動履歴をブロックチェーンとして格納する。目的物 930 に関する権利の変動履歴は、ブロックチェーン中に、1 又は複数のトランザクションデータとして格納される。本実施形態において、ブロックチェーン中には、例えば、(i) 目的物 930 の現在の所有権者がユーザ A であることを示すトランザクションデータ、(i i) 目的物 930 のコンピュータに、目的物 930 に関する権利の変動履歴を示すデータにアクセスできる権利が設定されていることを示すトランザクションデータが含まれている。目的物 930 に関する権利の変動履歴を示すデータにアクセスできる権利としては、当該データへのアクセス権限（例えば、当該データそのものへのアクセス権限、又は、権利管理サーバ 940、内容情報格納部 942 若しくは分散型台帳管理システム 110 へのアクセス権限である。）、目的物 930 の所有権などを例示することができる。

20

【0141】

理解を容易にすることを目的として、本実施形態においては、(i) ユーザ A が、目的物 930 の現在の所有権者であり、(i i) 目的物 930 のコンピュータが、目的物 930 の所有権の変動履歴に関するデータにアクセスする権利を有し、(i i i) ユーザ A が、ユーザ端末 920 を利用して目的物 930 を操作する場合を例として、権利管理システム 900 について説明する。目的物 930 の所有権は、目的物 930 に関する権利の一例であってよい。

30

【0142】

この場合において、一実施形態によれば、分散型台帳管理システム 110 に格納されたブロックチェーン中には、目的物 930 の所有権に対応する暗号通貨を 2 枚発行するためのトランザクションと、1 枚の暗号通貨の所有権又は使用権をユーザ A に移転するためのトランザクションと、もう 1 枚の暗号通貨の所有権又は使用権を目的物 930 のコンピュータに移転するためのトランザクションとが含まれる。これにより、秘密鍵 122 を有するユーザ A と、秘密鍵 932 を有する目的物 930 のコンピュータとの両方に対して、目的物 930 の所有権の変動履歴に関するデータを、内容情報格納部 942 若しくは分散型台帳管理システム 110 に書き込んだり、当該データを、内容情報格納部 942 若しくは分散型台帳管理システム 110 から読み取ったりする権限を付与することができる。

40

【0143】

目的物 930 の所有権に対応する暗号通貨は、例えば、暗号通貨の発行時に、当該暗号通貨の名称として、目的物 930 の所有権を示す識別記号を含む文字列を設定することで生成することができる。なお、上記の暗号通貨の発行枚数は 3 枚以上であってもよい。また、各暗号通貨に割り当てられた所有権の持分比率は、等しくてもよく、等しくなくてもよい。

【0144】

他の実施形態によれば、目的物 930 の所有権に対応する第 1 暗号通貨を 1 枚発行する

50

ためのトランザクションと、第1暗号通貨の所有権又は使用権をユーザAに移転するためのトランザクションと、目的物930の所有権の変動履歴を示すデータにアクセスする権利に対応する第2暗号通貨を発行するためのトランザクションと、第2暗号通貨の所有権又は使用権を目的物930のコンピュータに移転するためのトランザクションとが含まれる。これにより、秘密鍵122を有するユーザAに対して、目的物930の所有権の変動履歴に関するデータを、内容情報格納部942若しくは分散型台帳管理システム110に書き込んだり、当該データを、内容情報格納部942若しくは分散型台帳管理システム110から読み取ったりする権限を付与することができる。一方、秘密鍵932を有する目的物930のコンピュータに対しては、目的物930の所有権の変動履歴に関するデータを、内容情報格納部942若しくは分散型台帳管理システム110から読み取る権限を付与することができる。

10

【0145】

第1暗号通貨は、例えば、第1暗号通貨の発行時に、当該暗号通貨の名称として、目的物930の所有権を示す識別記号を含む文字列を設定することで生成することができる。第2暗号通貨は、例えば、第2暗号通貨の発行時に、当該暗号通貨の名称として、目的物930の所有権を示す識別記号と、アクセス権限を示す記号とを含む文字列を設定することで生成することができる。アクセス権限としては、書込権限、読取権限、実行権限及びこれらの組み合わせを例示することができる。なお、第1暗号通貨の発行枚数は2枚以上であってもよく、第2暗号通貨の発行枚数は2枚以上であってもよい。また、各暗号通貨に割り当てられた権利の持分比率は、等しくてもよく、等しくなくてもよい。

20

【0146】

本実施形態において、目的物930の現在の所有権者であるユーザAは、ユーザ端末920を操作して、目的物930を操作する為の処理を実行する。ユーザ端末920は、ユーザAからの入力に応じて、目的物930に対する命令を生成する。また、ユーザ端末920は、目的物930に対する命令と、ユーザAのユーザ識別情報とを目的物930に送信する。

【0147】

目的物930を操作する為の処理としては、(i)目的物930の機能を制限するための処理、(ii)目的物930に設定された機能制限を解除するための処理、(iii)目的物930のコンピュータにプログラム(例えば、アップデートプログラムである。)をインストールするための処理、(iv)目的物930のコンピュータに特定のプログラム又は命令を実行させるための処理などを例示することができる。目的物930の機能を制限する手段としては、目的物930に設けられた施錠装置の施錠、ロック機能又はアクセス制限機能の有効化などを例示することができる。目的物930の機能制限を解除する手段としては、目的物930に設けられた施錠装置の開錠、ロック機能又はアクセス制限機能の無効化などを例示することができる。

30

【0148】

本実施形態において、目的物930は、ユーザ端末920からの命令を受け取ると、分散型台帳管理システム110にアクセスして、ユーザAが当該命令を実行する権原又は権限を有するか否かを判定する。上記の判定処理は、分散型台帳管理システム110において実行されてもよい。目的物930は、ユーザAが当該命令を実行する権原又は権限を有すると判断した場合、ユーザ端末920からの命令を実行する。一方、目的物930は、ユーザAが当該命令を実行する権原又は権限を有しないと判断した場合、ユーザ端末920からの命令を破棄する。

40

【0149】

上記の判定処理の具体的な方法は特に制限されるものではないが、例えば、下記の手順により実行される。一実施形態によれば、目的物930のコンピュータは、権利管理サーバ940又は分散型台帳管理システム110にアクセスして、目的物930の現在の所有権者に関する情報を要求する。権利管理サーバ940又は分散型台帳管理システム110は、まず、目的物930のコンピュータが、目的物930の現在の所有権者に関する情報

50

にアクセスする権限を有するか否かを判定する。権利管理サーバ940又は分散型台帳管理システム110は、目的物930のコンピュータがアクセス権限を有すると判断した場合、目的物930の現在の所有者に関する情報を、目的物930のコンピュータに送信する。目的物930のコンピュータは、ユーザ端末920から受信したユーザ識別情報と、権利管理サーバ940又は分散型台帳管理システム110から取得した目的物930の現在の所有者に関する情報とを比較して、ユーザAが上記の命令の実行権限を有するか否かを判定する。一方、権利管理サーバ940又は分散型台帳管理システム110は、目的物930のコンピュータがアクセス権限を有しないと判断した場合、上記の要求を破棄する。

【0150】

他の実施形態によれば、目的物930のコンピュータは、権利管理サーバ940又は分散型台帳管理システム110にアクセスして、ユーザAが命令を実行する権原又は権限を有するか否かに関する判定を要求する。例えば、目的物930のコンピュータは、上記の要求とともに、ユーザ端末920から受信したユーザ識別情報を、権利管理サーバ940又は分散型台帳管理システム110に送信する。権利管理サーバ940又は分散型台帳管理システム110は、まず、目的物930のコンピュータが、目的物930の現在の所有者に関する情報にアクセスする権限を有するか否かを判定する。権利管理サーバ940又は分散型台帳管理システム110は、目的物930のコンピュータがアクセス権限を有すると判断した場合、目的物930のコンピュータから受信したユーザ識別情報と、分散型台帳管理システム110に登録された目的物930の現在の所有者に関する情報とを比較して、ユーザAが上記の命令の実行権限を有するか否かを判定する。一方、権利管理サーバ940又は分散型台帳管理システム110は、目的物930のコンピュータがアクセス権限を有しないと判断した場合、上記の要求を破棄する。

【0151】

本実施形態において、内容情報格納部942は、権利変動の内容を示す内容情報を格納する。内容情報格納部942は、内容情報と、当該内容情報の符号化データとを対応付けて格納してよい。内容情報格納部942は、データテーブル800を格納してもよい。

【0152】

本実施形態において、情報管理部944は、権利管理システム900において利用される各種の情報を管理する。本実施形態において、情報管理部944は、内容情報を生成又は更新することにより、内容情報格納部942に格納された内容情報を管理する。情報管理部944は、内容情報格納部942及び分散型台帳管理システム110の少なくとも一方にアクセスするためのインターフェースであってもよい。

【0153】

一実施形態において、情報管理部944は、権利又は権利の内容の変動に関する情報を管理する。例えば、情報管理部944は、ユーザAがユーザ端末920を操作した結果、権利又は権利の内容に変動を生じさせる処理が実行された場合に、ユーザ端末920から、(i)当該変動に関する内容情報と、(ii)当該変動に関する内容情報の符号化データを含んだトランザクションデータとを受信する。

【0154】

情報管理部944は、受信した内容情報を、内容情報格納部942に格納する。情報管理部944は、受信した内容情報の符号化データを生成して、当該内容情報と、当該内容情報の符号化データとを対応付けて格納してよい。一方、情報管理部944は、受信した内容情報を符号化して得られた符号化データと、受信したトランザクションに含まれる内容情報の符号化データとを比較する。両者が一致する場合、情報管理部944は、受信したトランザクションデータを、分散型台帳管理システム110に登録する。

【0155】

本実施形態によれば、内容情報格納部942に格納されている内容情報が、内容情報格納部942に格納された時点から改竄されていないことを、実用的に十分な精度で保証することができる。また、遅くとも、上記のトランザクションデータを含むブロックが生成

10

20

30

40

50

された時刻には、内容情報が登録されていたことを、実用的に十分な精度で保証することができる。

【 0 1 5 6 】

目的物 9 3 0 のコンピュータは、例えば、下記の手順により、内容情報格納部 9 4 2 に格納されている内容情報の改竄の有無を判定する。まず、目的物 9 3 0 のコンピュータは、権利管理サーバ 9 4 0 にアクセスして、改竄の有無の判定対象となる内容情報を要求する。例えば、目的物 9 3 0 のコンピュータは、権利管理サーバ 9 4 0 に目的物 9 3 0 を示す権利 ID 又は目的物 9 3 0 の特定の権利を示す権利 ID を送信して、当該権利 ID に対応付けられた内容情報を要求する。権利管理サーバ 9 4 0 は、目的物 9 3 0 のコンピュータからの要求を受信すると、分散型台帳管理システム 1 1 0 にアクセスして、目的物 9 3 0 のコンピュータから取得した権利 ID に対応するトランザクションデータに含まれる符号化データを取得する。権利管理サーバ 9 4 0 は、内容情報格納部 9 4 2 にアクセスして、分散型台帳管理システム 1 1 0 から取得した符号化データに対応する内容情報を取得する。権利管理サーバ 9 4 0 は、内容情報格納部 9 4 2 から取得した内容情報を、目的物 9 3 0 のコンピュータに送信する。これにより、目的物 9 3 0 のコンピュータは、内容情報格納部 9 4 2 から、判定対象となる内容情報を取得する。

10

【 0 1 5 7 】

次に、目的物 9 3 0 のコンピュータは、内容情報格納部 9 4 2 から取得した内容情報を符号化する。目的物 9 3 0 のコンピュータは、分散型台帳管理システム 1 1 0 にアクセスして、内容情報格納部 9 4 2 から取得した内容情報の符号化データが、分散型台帳管理システム 1 1 0 に、目的物 9 3 0 のコンピュータから取得した権利 ID と対応付けられて登録されているか否かを判定する。例えば、目的物 9 3 0 のコンピュータは、内容情報格納部 9 4 2 から取得した内容情報の符号化データが、分散型台帳管理システム 1 1 0 に権利 ID と対応付けられて登録されている最新の符号化データと一致するか否かを判定する。内容情報格納部 9 4 2 から取得した内容情報の符号化データが分散型台帳管理システム 1 1 0 に登録されている場合、目的物 9 3 0 のコンピュータは、内容情報が改竄されていないと判定する。一方、上記の符号化データが分散型台帳管理システム 1 1 0 に登録されていない場合、目的物 9 3 0 のコンピュータは、内容情報が改竄されていると判定する。

20

【 0 1 5 8 】

また、本実施形態によれば、内容情報そのものが分散型台帳管理システム 1 1 0 に登録されるのではなく、内容情報の符号化データが分散型台帳管理システム 1 1 0 に登録される。これにより、第三者が分散型台帳管理システム 1 1 0 に登録された情報にアクセスしたとしても、内容情報そのものの漏えいを防止することができる。

30

【 0 1 5 9 】

他の実施形態において、情報管理部 9 4 4 は、内容情報として、目的物 9 3 0 を遠隔操作するためのコードを管理する。目的物 9 3 0 の遠隔操作としては、(i) 目的物 9 3 0 の機能を制限するための処理、(i i) 目的物 9 3 0 に設定された機能制限を解除するための処理、(i i i) 目的物 9 3 0 のコンピュータにプログラム (例えば、アップデートプログラムである。) をインストールするための処理、(i v) 目的物 9 3 0 のコンピュータに特定のプログラム又は命令を実行させるための処理などを例示することができる。

40

【 0 1 6 0 】

例えば、目的物 9 3 0 に関する権利 R の被承継人たるユーザ A と、権利 R の承継人との間で、権利 R の承継に関する契約が成立した場合、ユーザ A は、ユーザ端末 9 2 0 を操作して、契約内容を登録するための処理を実行する。この場合において、情報管理部 9 4 4 は、ユーザ端末 9 2 0 から、(i) 契約内容を登録するためのコードと、(i i) 上記のコードの符号化データを含むトランザクションデータを受信する。契約内容を登録するためのコードは、目的物 9 3 0 を遠隔操作するためのコードを含んでもよい。

【 0 1 6 1 】

情報管理部 9 4 4 は、受信したコードを、内容情報格納部 9 4 2 に格納する。情報管理部 9 4 4 は、受信したコードの符号化データを生成して、当該コードと、当該コードの符

50

号化データとを対応付けて格納してよい。また、情報管理部 9 4 4 は、受信したトランザクションデータを、分散型台帳管理システム 1 1 0 に登録する。上記のトランザクションデータは、上記のコードの符号化データを含んでいてもよい。

【 0 1 6 2 】

その後、目的物 9 3 0 のコンピュータは、情報管理部 9 4 4 にアクセスして、目的物 9 3 0 に対して送信されたデータの有無を問い合わせる。目的物 9 3 0 のコンピュータが、情報管理部 9 4 4 にアクセスするタイミングとしては、(i) 目的物 9 3 0 のコンピュータが、ユーザ端末 9 2 0 から、何らかの命令を受信した場合、(i i) 目的物 9 3 0 のコンピュータが、情報管理部 9 4 4 から、目的物 9 3 0 に関連する権利に関する内容情報が生成又は更新されたことを示す情報を受信した場合、(i i i) 予め定められた時刻が到達した場合、(i v) 前回のアクセスから、予め定められた時間が経過した場合などを例示することができる。

10

【 0 1 6 3 】

この場合において、上記の問い合わせには、符号化後のデータの使いまわしを防止するための情報を、秘密鍵 9 3 2 を利用して符号化又は暗号化したデータが含まれてよい。符号化後のデータの使いまわしを防止するための情報としては、タイムスタンプ、IP アドレスなどを例示することができる。目的物の秘密鍵 9 3 2 を利用することにより、情報管理部 9 4 4 にアクセスしている目的物 9 3 0 の正当性を保証することができる。

【 0 1 6 4 】

情報管理部 9 4 4 は、目的物 9 3 0 からの問い合わせを受信すると、目的物 9 3 0 による分散型台帳管理システム 1 1 0 に登録されたデータへのアクセスの許否を判定する。目的物 9 3 0 のコンピュータが、分散型台帳管理システム 1 1 0 に登録されたデータにアクセスする権限を有する場合、情報管理部 9 4 4 は、分散型台帳管理システム 1 1 0 にアクセスして、分散型台帳管理システム 1 1 0 に登録されたデータを取得し、目的物 9 3 0 に送信する。一方、目的物 9 3 0 のコンピュータが、分散型台帳管理システム 1 1 0 に登録されたデータにアクセスする権限を有しない場合、情報管理部 9 4 4 は、分散型台帳管理システム 1 1 0 へのアクセスが拒否されたことを示す情報を、目的物 9 3 0 に送信する。

20

【 0 1 6 5 】

さらに他の実施形態において、情報管理部 9 4 4 は、内容情報として、目的物 9 3 0 を遠隔操作するためのコードの代わりに、ユーザ端末 9 2 0 から目的物 9 3 0 に送信するデータを管理してよい。上記のデータの具体的な管理方法は、目的物 9 3 0 を遠隔操作するためのコードの管理方法と同様であってよい。

30

【 0 1 6 6 】

本実施形態において、情報管理部 9 4 4 が、(i) 内容情報格納部 9 4 2 に格納される内容情報を管理したり、(i i) ユーザ端末 9 2 0 又は目的物 9 3 0 と、分散型台帳管理システム 1 1 0 との間の通信を中継したりする場合について説明した。しかしながら、情報管理部 9 4 4 は本実施形態に限定されない。他の実施形態において、情報管理部 9 4 4 は、権利管理サーバ 9 4 0 により提供される各種のサービスを管理してもよい。

【 0 1 6 7 】

例えば、権利管理サーバ 9 4 0 は、遠隔操作サービス、情報配信サービス、マッチングサービス、オークションサービス、レンタルサービス又はシェアリングサービス、オンラインゲームサービス、エスクローサービス、決済サービスなどを提供する。情報管理部 9 4 4 は、上記のサービスにおけるユーザ・インタフェース、ユーザに提供する情報、ユーザ情報などを管理することにより、上記のサービスを管理する。

40

【 0 1 6 8 】

本実施形態においては、各ユーザの秘密鍵は各ユーザのユーザ端末に格納されており、各ユーザのユーザ端末が、トランザクションデータを生成する場合について説明した。しかしながら、権利管理システム 9 0 0 は本実施形態に限定されない。他の実施形態において、例えば、情報管理部 9 4 4 が、各ユーザの秘密鍵を管理してもよい。この場合、情報管理部 9 4 4 が、各ユーザの秘密鍵を利用して、トランザクションデータを生成してもよ

50

い。例えば、情報管理部 9 4 4 は、ユーザ A のユーザ端末 9 2 0 から内容情報を受信すると、ユーザ A の秘密鍵を利用して、当該内容情報の符号化データを含むトランザクションデータを生成してよい。情報管理部 9 4 4 は、生成されたトランザクションデータを分散型台帳管理システム 1 1 0 に登録してよい。

【 0 1 6 9 】

図 1 0 は、ユーザ端末 9 2 0 の内部構成の一例を概略的に示す。本実施形態において、ユーザ端末 9 2 0 は、通信制御部 6 1 0 と、入出力部 6 2 0 と、トランザクションデータ生成部 6 3 0 と、格納部 6 4 0 と、要求生成部 6 5 0 と、命令生成部 1 0 7 0 とを備える。格納部 6 4 0 は、例えば、鍵情報格納部 6 4 2 と、トランザクションデータ格納部 6 4 4 とを有する。通信制御部 6 1 0 は、命令送信部の一例であってよい。ユーザ端末 9 2 0 は、命令生成部 1 0 7 0 を備える点を除いて、ユーザ端末 1 2 0 と同様の構成を有してよい。そこで、上記の相違点以外の構成については説明を省略する。

10

【 0 1 7 0 】

命令生成部 1 0 7 0 は、目的物 9 3 0 に対する命令を生成する。目的物 9 3 0 に対する命令としては、目的物 9 3 0 を遠隔操作するためのコード、契約内容を登録するためのコードなどを例示することができる。命令生成部 1 0 7 0 は、生成された命令を、通信制御部 6 1 0 を介して目的物 9 3 0 に送信してよい。命令生成部 1 0 7 0 は、生成された命令と、ユーザ A のユーザ識別情報とを対応付けて、目的物 9 3 0 に送信してもよい。上記の命令としては、目的物 9 3 0 の機能に関する制限を実施するための命令、目的物 9 3 0 の機能に関する制限を解除するための命令、目的物 9 3 0 の状態に関する情報を報告させるための命令などを例示することができる。

20

【 0 1 7 1 】

命令生成部 1 0 7 0 は、例えば、生成された命令を、トランザクションデータ生成部 6 3 0 に送信する。一実施形態において、トランザクションデータ生成部 6 3 0 は、命令生成部 1 0 7 0 が生成した命令を含むトランザクションデータを生成する。他の実施形態において、トランザクションデータ生成部 6 3 0 は、命令生成部 1 0 7 0 が生成した命令の符号化データを含むトランザクションデータを生成する。トランザクションデータ生成部 6 3 0 により生成されたトランザクションデータは、目的物 9 3 0 に直接送信されてもよく、権利管理サーバ 9 4 0 を介して目的物 9 3 0 に送信されてもよい。

【 0 1 7 2 】

図 1 1 は、目的物 9 3 0 の内部構成の一例を概略的に示す。本実施形態において、目的物 9 3 0 は、入出力部 1 1 1 0 と、制御部 1 1 2 0 と、格納部 1 1 3 0 とを備える。制御部 1 1 2 0 は、例えば、通信制御部 1 1 2 2 と、要求生成部 1 1 2 4 と、機能制御部 1 1 2 6 と、実行部 1 1 2 8 とを有する。格納部 1 1 3 0 は、例えば、権利識別情報格納部 1 1 3 2 と、解除条件格納部 1 1 3 4 とを有する。通信制御部 1 1 2 2 は、要求送信部、応答受信部又は命令受信部の一例であってよい。機能制御部 1 1 2 6 は、制限制御部の一例であってよい。実行部 1 1 2 8 は、命令実行部の一例であってよい。

30

【 0 1 7 3 】

本実施形態において、入出力部 1 1 1 0 は、目的物 9 3 0 への入力を受け付ける。入出力部 1 1 1 0 は、ユーザからの指示を受け付けてもよい。上記の指示は、目的物 9 3 0 の操作に関する指示であってもよい。本実施形態において、入出力部 1 1 1 0 は、目的物 9 3 0 から情報を出力する。入出力部 1 1 1 0 としては、キーボード、ポインティングデバイス、タッチパネル、マイク、カメラ、センサ、GPS 受信機などの入力装置、又は、表示装置、スピーカ、振動装置、ビーコン発信装置などの出力装置を例示することができる。入出力部 1 1 1 0 は、ユーザ・インタフェースであってもよい。

40

【 0 1 7 4 】

本実施形態において、制御部 1 1 2 0 は、目的物 9 3 0 を制御する。本実施形態において、通信制御部 1 1 2 2 は、ユーザ端末 9 2 0 との間の通信を制御する。通信制御部 1 1 2 2 は、権利管理サーバ 9 4 0 との間の通信を制御してもよく、分散型台帳管理システム 1 1 0 又は複数のノード 1 1 2 との間の通信を制御してもよい。通信制御部 1 1 2 2 は、

50

外部の機器に情報を送信する送信部として機能してもよく、外部の機器からの情報を受信する受信部として機能してもよい。通信制御部 1 1 2 2 は、通信インターフェースであってもよい。通信制御部 1 1 2 2 は、複数の種類の通信方式に対応していてもよい。通信制御部 1 1 2 2 は、移動体通信、無線 M A N、無線 L A N、B l u e t o o t h (登録商標)、Z i g b e e (登録商標)、及び、N F Cの中から選ばれる 2 つ以上の種類の通信方式に対応してもよい。

【 0 1 7 5 】

本実施形態において、通信制御部 1 1 2 2 は、ユーザ端末 9 2 0 から、目的物 9 3 0 に対する命令を取得する。通信制御部 1 1 2 2 は、ユーザ端末 9 2 0 から、目的物 9 3 0 に対する命令と、ユーザ A のユーザ識別情報とを取得してもよい。通信制御部 1 1 2 2 は、
10
上記の命令又は情報を、権利管理サーバ 9 4 0 を介して取得してもよい。通信制御部 1 1 2 2 は、ユーザ端末 9 2 0 又は権利管理サーバ 9 4 0 から受け取った情報を要求生成部 1 1 2 4 に転送してよい。

【 0 1 7 6 】

本実施形態において、通信制御部 1 1 2 2 は、他の情報処理装置に対する各種の要求を、当該他の情報処理装置に送信する。他の情報処理装置としては、分散型台帳管理システム 1 1 0、権利管理サーバ 9 4 0 などを例示することができる。通信制御部 1 1 2 2 は、要求生成部 1 1 2 4 が生成した要求を、権利管理サーバ 9 4 0 又は分散型台帳管理システム 1 1 0 に送信してよい。通信制御部 1 1 2 2 は、上記の要求又は命令の実行に必要な情報を、当該要求又は命令に対応付けて送信してもよい。通信制御部 1 1 2 2 は、権利管理
20
サーバ 9 4 0 又は分散型台帳管理システム 1 1 0 から、上記の要求に対する応答を受信してよい。通信制御部 1 1 2 2 は、上記の応答を機能制御部 1 1 2 6 に転送してよい。

【 0 1 7 7 】

本実施形態において、要求生成部 1 1 2 4 は、各種の要求を生成する。要求生成部 1 1 2 4 は、権利管理サーバ 9 4 0 又は分散型台帳管理システム 1 1 0 に対する要求を生成してよい。例えば、通信制御部 1 1 2 2 が目的物 9 3 0 に対する命令を受信した場合、要求生成部 1 1 2 4 は、権利管理サーバ 9 4 0 又は分散型台帳管理システム 1 1 0 にアクセスして、ユーザ A が当該命令を実行する権原又は権限を有するか否かを判定するための要求を生成する。要求生成部 1 1 2 4 は、生成された要求を、通信制御部 1 1 2 2 を介して、
30
権利管理サーバ 9 4 0 又は分散型台帳管理システム 1 1 0 に送信してよい。

【 0 1 7 8 】

第 1 の実施形態において、要求生成部 1 1 2 4 は、上記の命令に関連する権利の現在の権利者のユーザ識別情報の抽出を要求するためのデータを生成する。要求生成部 1 1 2 4 は、生成されたデータと、上記の命令に関連する権利の権利 I D とを、権利管理サーバ 9 4 0 又は分散型台帳管理システム 1 1 0 に送信してよい。

【 0 1 7 9 】

第 2 の実施形態において、要求生成部 1 1 2 4 は、ユーザ A が上記の命令に関連する権利を有するか否かの判定を要求するためのデータを生成する。要求生成部 1 1 2 4 は、生成された要求と、ユーザ A のユーザ識別情報と、上記の命令に関連する権利の権利 I D とを、分散型台帳管理システム 1 1 0 に送信してよい。上記の命令に関連する権利は、権利
40
識別情報格納部 1 1 3 2 に格納された権利の少なくとも一部の一例であってよい。

【 0 1 8 0 】

第 3 の実施形態において、要求生成部 1 1 2 4 は、ユーザ A が有する 1 以上の権利の権利 I D の抽出を要求するためのデータを生成する。要求生成部 1 1 2 4 は、生成されたデータと、ユーザ A のユーザ識別情報とを、権利管理サーバ 9 4 0 又は分散型台帳管理システム 1 1 0 に送信してよい。

【 0 1 8 1 】

本実施形態において、機能制御部 1 1 2 6 は、目的物 9 3 0 の機能を制御する。機能制御部 1 1 2 6 は、目的物 9 3 0 の機能に関する制限の実施又は解除を制御してよい。例えば、機能制御部 1 1 2 6 は、要求生成部 1 1 2 4 が生成した要求に対する、権利管理サー
50

バ 9 4 0 又は分散型台帳管理システム 1 1 0 からの応答に基づいて、ユーザ A が、目的物 9 3 0 に対する命令を実行する権原又は権限を有するか否かを判定する。ユーザ A が、目的物 9 3 0 に対する命令を実行する権原又は権限を有すると判定された場合、機能制御部 1 1 2 6 は、目的物 9 3 0 の機能に関する制限を解除することを決定し、命令実行部 1 1 2 8 に上記の命令を実行させる。

【 0 1 8 2 】

一方、ユーザ A が、目的物 9 3 0 に対する命令を実行する権原又は権限を有しないと判定された場合、機能制御部 1 1 2 6 は、目的物 9 3 0 の機能に関する制限を実施する又は当該制限を解除しないことを決定し、上記の命令を破棄する。機能制御部 1 1 2 6 は、上記の命令を破棄する代わりに、当該命令を処理しないことにしてもよい。また、このとき、機能制御部 1 1 2 6 は、ユーザ A が上記の命令を実行するための権原又は権限を有していないことを示す情報を、通信制御部 1 1 2 2 を介してユーザ端末 9 2 0 に送信してよい。機能制御部 1 1 2 6 は、ユーザ A が上記の命令を実行するための権原又は権限を有していないことを示す情報を、入出力部 1 1 1 0 に出力してもよい。

10

【 0 1 8 3 】

第 1 の実施形態において、機能制御部 1 1 2 6 は、分散型台帳管理システム 1 1 0 による抽出結果と、ユーザ A のユーザ識別情報とを比較することで、ユーザ A が当該命令を実行する権原又は権限を有するか否かを判定してよい。例えば、分散型台帳管理システム 1 1 0 による抽出結果が、ユーザ A のユーザ識別情報と合致する場合、機能制御部 1 1 2 6 は、ユーザ A が当該命令を実行する権原又は権限を有すると判定する。

20

【 0 1 8 4 】

第 2 の実施形態において、機能制御部 1 1 2 6 は、権利管理サーバ 9 4 0 又は分散型台帳管理システム 1 1 0 による判定結果に基づいて、ユーザ A が当該命令を実行する権原又は権限を有するか否かを判定してよい。例えば、権利管理サーバ 9 4 0 又は分散型台帳管理システム 1 1 0 による判定結果が、ユーザ A が上記の命令に関連する権利を有することを示す場合、機能制御部 1 1 2 6 は、ユーザ A が当該命令を実行する権原又は権限を有すると判定する。

【 0 1 8 5 】

第 3 の実施形態において、機能制御部 1 1 2 6 は、権利管理サーバ 9 4 0 又は分散型台帳管理システム 1 1 0 による抽出結果と、上記の命令に関連する権利の権利 ID とを比較することで、ユーザ A が当該命令を実行する権原又は権限を有するか否かを判定してよい。例えば、権利管理サーバ 9 4 0 又は分散型台帳管理システム 1 1 0 による抽出結果に含まれる権利 ID が、権利識別情報格納部 1 1 3 2 に格納されている権利 ID (特に、上記の命令に関連する権利の権利 ID である。) の中に含まれている場合、機能制御部 1 1 2 6 は、ユーザ A が当該命令を実行する権原又は権限を有すると判定する。

30

【 0 1 8 6 】

さらに他の実施形態において、機能制御部 1 1 2 6 は、解除条件格納部 1 1 3 4 を参照して、上記の命令に関連する権利を行使するための条件 (解除条件と称する場合がある。) の有無を判定する。上記の命令に関連する権利について解除条件が設定されておらず、ユーザ A が当該命令を実行する権原又は権限を有する場合、機能制御部 1 1 2 6 は、目的物 9 3 0 の機能に関する制限を解除することを決定し、命令実行部 1 1 2 8 に上記の命令を実行させる。

40

【 0 1 8 7 】

一方、上記の命令に関連する権利について解除条件が設定されている場合、機能制御部 1 1 2 6 は、権利管理サーバ 9 4 0 又は分散型台帳管理システム 1 1 0 にアクセスして、上記の命令に関連する権利の解除条件の充足性を判定するための情報を取得する。例えば、機能制御部 1 1 2 6 は、上記の命令に関連する権利の内容情報、目的物 9 3 0 に設定されている他の権利の権利 ID 及び内容情報などを取得する。機能制御部 1 1 2 6 は、権利管理サーバ 9 4 0 又は分散型台帳管理システム 1 1 0 から取得した情報に基づいて、解除条件が満たされているか否かを判定する。

50

【 0 1 8 8 】

解除条件が満たされており、ユーザ A が当該命令を実行する権原又は権限を有する場合、機能制御部 1 1 2 6 は、目的物 9 3 0 の機能に関する制限を解除することを決定し、命令実行部 1 1 2 8 に上記の命令を実行させる。一方、解除条件が満たされていない場合、機能制御部 1 1 2 6 は、目的物 9 3 0 の機能に関する制限を実施する又は当該制限を解除しないことを決定し、上記の命令を破棄する。この場合、機能制御部 1 1 2 6 は、解除条件が満たされていないことを示す情報を、ユーザ端末 9 2 0 に送信したり、入出力部 1 1 1 0 に出力したりしてよい。

【 0 1 8 9 】

実行部 1 1 2 8 は、通信制御部 1 1 2 2 が受信した、目的物 9 3 0 に対する命令を実行する。実行部 1 1 2 8 は、機能制御部 1 1 2 6 が目的物 9 3 0 の機能に関する制限を解除することを決定した場合に、上記の命令を実行してよい。

10

【 0 1 9 0 】

格納部 1 1 3 0 は、各種の情報を格納する。権利識別情報格納部 1 1 3 2 は、目的物 9 3 0 に設定されている権利の権利 ID を格納する。権利識別情報格納部 1 1 3 2 は、目的物 9 3 0 に設定されている権利の権利 ID を、目的物 9 3 0 の機能若しくは処理、又は、目的物 9 3 0 に対する命令と対応付けて格納してもよい。解除条件格納部 1 1 3 4 は、目的物 9 3 0 の機能に関する制限を解除するための解除条件を格納する。格納部 1 1 3 0 は、その他の情報を格納してもよい。

【 0 1 9 1 】

20

図 1 2 は、権利管理システム 9 0 0 における情報処理の一例を概略的に示す。図 1 2 を用いて、権利管理システム 9 0 0 におけるトランザクションデータの登録処理の一実施形態について説明する。なお、本実施形態において、内容情報格納部 9 4 2 は、ユーザ A が有する 1 以上の権利のそれぞれの内容情報を格納している。本実施形態よれば、まず、ステップ 1 2 0 2 (ステップを S と省略して記載する場合がある。)において、ユーザ端末 9 2 0 の入出力部 6 2 0 が、ユーザ A からの入力を受け付ける。上記の入力は、ユーザ端末 9 2 0 の操作に関する指示であってよい。

【 0 1 9 2 】

上記の指示により、ユーザ A が有する権利 R に i 番目の変動 V_i が生じる場合、S 1 2 0 4 において、トランザクションデータ生成部 6 3 0 は、変動 V_i に関する移転用のトランザクションデータ T_i を生成する (i は 2 以上の正の整数である)。例えば、トランザクションデータ生成部 6 3 0 は、トランザクションデータ T_i を生成する工程において、権利 R 又は権利変動 V_i の内容を示す内容情報を生成する。また、生成された内容情報を符号化して、内容情報の符号化データ (例えば、ハッシュ値である。)を生成する。トランザクションデータ生成部 6 3 0 は、上記の内容情報の符号化データをトランザクションデータ T_i の適切な位置に配置する。これにより、内容情報の符号化データを含むトランザクションデータ T_i が生成される。

30

【 0 1 9 3 】

トランザクションデータ生成部 6 3 0 は、トランザクションデータ T_i を生成する工程において、権利 R の変動 V_i に関するトランザクションデータ T_i の少なくとも一部を、ユーザ A の秘密鍵 1 2 2 で暗号化することによりトランザクションデータ T_i の署名値を生成し、当該署名値をトランザクションデータ T_i の適切な領域に配置してよい。これにより、トランザクションデータ T_i が、権利 R の権利者であるユーザ A により生成されたことを保証することができる。

40

【 0 1 9 4 】

その後、トランザクションデータ生成部 6 3 0 は、生成されたトランザクションデータ T_i を、分散型台帳管理システム 1 1 0 に参加する複数のノード 1 1 2 のうちの 1 つに送信する。本実施形態において、トランザクションデータ生成部 6 3 0 は、トランザクションデータ T_i を、権利管理サーバ 9 4 0 を介して、分散型台帳管理システム 1 1 0 に参加するノード 1 1 2 に送信する。より具体的には、トランザクションデータ生成部 6 3 0 は

50

、内情情報と、トランザクションデータ T_i とを、一旦、権利管理サーバ940に送信する。

【0195】

このとき、トランザクションデータ生成部630は、署名値を含むトランザクションデータ T_i を、権利Rの権利IDと対応付けて送信してよい。一実施形態によれば、トランザクションデータ生成部630は、上記の署名値及び上記の権利IDを含むトランザクションデータ T_i を送信する。他の実施形態によれば、トランザクションデータ生成部630は、上記の署名値を含むトランザクションデータ T_i に、上記の権利IDを含むメタデータを付与したデータを送信する。

【0196】

なお、変動 V_i において、権利Rは移転せず、権利Rの内容に変更が生じる場合、トランザクションデータ生成部630は、承継先として被承継人(ユーザAである。)を指定する承継先情報を含むトランザクションデータ T_i を生成してよい。また、目的物930に新たな権利を設定する場合、トランザクションデータ生成部630は、発行用のトランザクションデータ T_i (i は1である。)を生成してよい。

【0197】

S1212において、権利管理サーバ940の情報管理部944が、ユーザ端末920から、内容情報及びトランザクションデータ T_i を受信する。情報管理部944は、ユーザ端末920から受信したデータの正当性を確認する。例えば、情報管理部944は、ユーザ端末920から受信した内容情報を符号化して、内容情報の符号化データを生成する。情報管理部944は、(i)ユーザ端末920から受信した内容情報の符号化データと、(ii)ユーザ端末920から受信したトランザクションデータ T_i に含まれる符号化データとを比較する。両者が一致する場合、情報管理部944は、ユーザ端末920から受信したデータは正当なデータであると判定する。

【0198】

上記のデータの正当性が確認された場合、S1214において、情報管理部944が、内容情報格納部942に格納された内容情報を更新する。また、S1216において、情報管理部944は、ユーザ端末920から受信したトランザクションデータ T_i を、分散型台帳管理システム110に転送する。これにより、トランザクションデータ T_i が、権利管理サーバ940を介して、ユーザ端末920から分散型台帳管理システム110に送信される。内容情報の更新は、トランザクションデータの転送前であってもよく、トランザクションデータの転送後であってもよい。

【0199】

S1222において、分散型台帳管理システム110に参加する複数のノード112のうちの一つが、権利管理サーバ940から、トランザクションデータ T_i を受信する。権利管理サーバ940からトランザクションデータ T_i を受信したノード112は、他のノード112に、トランザクションデータ T_i を転送する。複数のノード112のそれぞれは、トランザクションデータ T_i と、予め定められた期間に受信した他のトランザクションデータとを一纏めにして、新たなブロックを生成する。

【0200】

次に、複数のノード112のそれぞれは、新たなブロックの承認処理を実行する。1台のノード112によって新たなブロックが承認されると、当該ノードのブロックチェーン生成部220が、当該ブロックを既存のブロックチェーンに追加して、新たなブロックチェーンを生成する。S1224において、複数のノード112の間で、新たなブロックチェーンが共有される。これにより、トランザクションデータの登録処理が完了する。

【0201】

図13は、権利管理システム900における情報処理の一例を概略的に示す。図13を用いて、権利管理システム900における目的物930の遠隔操作処理の第1の実施形態について説明する。本実施形態によれば、まず、S1302において、ユーザ端末920の入出力部620が、ユーザAからの入力を受け付ける。上記の入力は、目的物930の

10

20

30

40

50

操作に関する指示であってよい。上記の操作は、目的物 9 3 0 のロックを解除するための操作であってもよい。

【 0 2 0 2 】

S 1 3 0 4 において、命令生成部 1 0 7 0 が、上記の指示に対応する目的物 9 3 0 に対する命令を生成し、当該命令を目的物 9 3 0 に送信する。一実施形態において、命令生成部 1 0 7 0 は、通信ネットワーク 1 0 を介して、当該命令を目的物 9 3 0 に送信する。命令生成部 1 0 7 0 は、当該命令を、権利管理サーバ 9 4 0 を介して、目的物 9 3 0 に送信してもよい。他の実施形態によれば、命令生成部 1 0 7 0 は、当該命令を、近距離無線通信により、P 2 P で目的物 9 3 0 に送信する。

【 0 2 0 3 】

S 1 3 1 2 において、目的物 9 3 0 の通信制御部 1 1 2 2 が、ユーザ端末 9 2 0 からの命令を受信して、当該命令を要求生成部 1 1 2 4 に転送する。要求生成部 1 1 2 4 は、上記の命令に関連する権利の現在の権利者のユーザ識別情報の抽出を要求するためのデータを生成する。要求生成部 1 1 2 4 は、生成されたデータと、上記の命令に関連する権利の権利 ID とを、分散型台帳管理システム 1 1 0 に送信する。なお、分散型台帳管理システム 1 1 0 と、ユーザ端末 9 2 0 及び目的物 9 3 0 との間に、権利管理サーバ 9 4 0 が介在している場合、要求生成部 1 1 2 4 は、生成されたデータと、上記の命令に関連する権利の権利 ID とを、権利管理サーバ 9 4 0 に送信してもよい。

【 0 2 0 4 】

S 1 3 1 4 において、分散型台帳管理システム 1 1 0 が、目的物 9 3 0 からの要求を受信する。分散型台帳管理システム 1 1 0 は、目的物 9 3 0 から受け取った 1 又は複数の権利 ID で示される権利のそれぞれを表現するブロックチェーンにアクセスする。その後、分散型台帳管理システム 1 1 0 は、目的物 9 3 0 から受け取った 1 又は複数の権利 ID で示される権利のそれぞれについて、現在の権利者のユーザ識別情報を抽出する。分散型台帳管理システム 1 1 0 は、目的物 9 3 0 からの要求に対する応答として、ブロックチェーンから抽出された情報を、目的物 9 3 0 に送信する。

【 0 2 0 5 】

分散型台帳管理システム 1 1 0 と、ユーザ端末 9 2 0 及び目的物 9 3 0 との間に、権利管理サーバ 9 4 0 が介在している場合、例えば、権利管理サーバ 9 4 0 が、分散型台帳管理システム 1 1 0 にアクセスして、目的物 9 3 0 からの要求に応じた情報をブロックチェーンから抽出する。また、権利管理サーバ 9 4 0 は、目的物 9 3 0 からの要求に対する応答として、ブロックチェーンから抽出された情報を、目的物 9 3 0 に送信する。

【 0 2 0 6 】

S 1 3 1 6 において、目的物 9 3 0 の通信制御部 1 1 2 2 が、権利管理サーバ 9 4 0 又は分散型台帳管理システム 1 1 0 からの応答を受信して、当該応答を機能制御部 1 1 2 6 に転送する。機能制御部 1 1 2 6 は、権利管理サーバ 9 4 0 又は分散型台帳管理システム 1 1 0 から受信した抽出結果と、ユーザ端末 9 2 0 から受信したユーザ A のユーザ識別情報とに基づいて、ユーザ A が目的物 9 3 0 に対する命令を実行する権原又は権限を有するか否かを判定する。

【 0 2 0 7 】

ユーザ A が、目的物 9 3 0 に対する命令を実行する権原又は権限を有すると判定された場合、機能制御部 1 1 2 6 は、命令実行部 1 1 2 8 に上記の命令に対応する処理を実行させる。命令実行部 1 1 2 8 による処理が完了すると、目的物 9 3 0 の遠隔操作処理が完了する。一方、ユーザ A が、目的物 9 3 0 に対する命令を実行する権原又は権限を有しないと判定された場合、機能制御部 1 1 2 6 は、上記の命令を破棄する。その結果、上記の命令は実行されることなく、目的物 9 3 0 の遠隔操作処理が終了する。

【 0 2 0 8 】

図 1 4 は、権利管理システム 9 0 0 における情報処理の一例を概略的に示す。図 1 4 を用いて、権利管理システム 9 0 0 における目的物 9 3 0 の遠隔操作処理の第 2 の実施形態について説明する。図 1 4 に記載された実施形態は、S 1 3 1 2 及び S 1 3 1 4 の代わり

10

20

30

40

50

に、S 1 4 1 2 及び S 1 4 1 4 が実行される点で、図 1 3 に記載された実施形態と相違する。上記の相違点以外の点については、図 1 3 に記載された実施形態と同様の構成を有してよい。

【 0 2 0 9 】

本実施形態によれば、S 1 4 1 2 において、目的物 9 3 0 の通信制御部 1 1 2 2 が、ユーザ端末 9 2 0 からの命令を受信して、当該命令を要求生成部 1 1 2 4 に転送する。要求生成部 1 1 2 4 は、ユーザ A が上記の命令に関連する権利を有するか否かの判定を要求するためのデータを生成する。要求生成部 1 1 2 4 は、生成された要求と、ユーザ A のユーザ識別情報と、上記の命令に関連する権利の権利 ID とを、分散型台帳管理システム 1 1 0 に送信する。

10

【 0 2 1 0 】

S 1 4 1 4 において、分散型台帳管理システム 1 1 0 が、目的物 9 3 0 からの要求を受信する。分散型台帳管理システム 1 1 0 は、目的物 9 3 0 から受け取った 1 又は複数の権利 ID で示される権利のそれぞれを表現するブロックチェーンにアクセスする。その後、分散型台帳管理システム 1 1 0 は、目的物 9 3 0 から受け取った 1 又は複数の権利 ID で示される権利のそれぞれについて、現在の権利者のユーザ識別情報を抽出する。

【 0 2 1 1 】

分散型台帳管理システム 1 1 0 は、上記の抽出の結果と、ユーザ端末 9 2 0 から受信したユーザ A のユーザ識別情報とに基づいて、ユーザ A が、目的物 9 3 0 に対する命令を実行する権原又は権限を有するか否かを判定する。分散型台帳管理システム 1 1 0 は、目的物 9 3 0 からの要求に対する応答として、上記の判定の結果を、目的物 9 3 0 に送信する。また、S 1 3 1 6 において、機能制御部 1 1 2 6 は、分散型台帳管理システム 1 1 0 から受信した判定結果に基づいて、ユーザ A が、目的物 9 3 0 に対する命令を実行する権原又は権限を有するか否かを判定する。

20

【 0 2 1 2 】

本実施形態において、目的物 9 3 0 が、権利管理サーバ 9 4 0 を介することなく、分散型台帳管理システム 1 1 0 に要求などを送信する場合について説明した。しかしながら、権利管理システム 9 0 0 における情報処理は本実施形態に限定されない。他の実施形態において、分散型台帳管理システム 1 1 0 と、ユーザ端末 9 2 0 及び目的物 9 3 0 との間に、権利管理サーバ 9 4 0 が介在してもよい。

30

【 0 2 1 3 】

図 1 5 は、権利管理システム 9 0 0 を利用したエスクローシステム 2 1 0 0 の一例を概略的に示す。本実施形態において、エスクローシステム 2 1 0 0 は、クライアント端末 2 2 を利用するユーザ A と、クライアント端末 2 4 を利用するユーザ B とに対して、エスクローサービスを提供する。クライアント端末 2 2 及びクライアント端末 2 4 のそれぞれは、ユーザ端末 1 2 0 又はユーザ端末 9 2 0 と同様の構成を有してよい。

【 0 2 1 4 】

本実施形態において、クライアント端末 2 2 は、ユーザ A の秘密鍵 1 2 2 を格納している。クライアント端末 2 4 は、ユーザ B の秘密鍵 2 1 2 2 を格納している。また、権利管理サーバ 9 4 0 は、エスクローサービスを管理するサービス提供者としての秘密鍵 2 1 2 4 を格納している。

40

【 0 2 1 5 】

[契約の締結]

本実施形態においては、まず、目的物 9 3 0 の所有権を有するユーザ A と、目的物 9 3 0 の購入を希望するユーザ B とが、権利管理サーバ 9 4 0 により提供されるマッチングサービス又はオークションサービスを利用して、目的物 9 3 0 の譲渡契約を締結する。これにより、権利管理サーバ 9 4 0 は、上記の譲渡契約に伴う権利の変動に関する情報を取得する。マッチングサービス又はオークションサービスは、例えば、情報管理部 9 4 4 における情報処理により実現される。情報管理部 9 4 4 は、目的物 9 3 0 に関する権利の被承継人と、当該権利の承継を希望する承継候補者とを仲介する仲介部を有してよい。

50

【 0 2 1 6 】

なお、譲渡契約の成立過程は、本実施形態に限定されない。他の実施形態において、ユーザ A 及びユーザ B は、権利管理サーバ 9 4 0 により提供されるサービスを利用することなく、譲渡契約を締結してもよい。この場合、ユーザ A 又はユーザ B がクライアント端末 2 2 又はクライアント端末 2 4 を操作して、契約内容に関する情報を権利管理サーバ 9 4 0 に送信する。契約内容に関する情報としては、取引の対象となる権利の権利 ID、取引相手のユーザ ID、金額などを例示することができる。クライアント端末 2 2 又はクライアント端末 2 4 は、契約内容を示すデータと、契約内容を示すデータの符号化データを含むトランザクションを、権利管理サーバ 9 4 0 に送信してもよい。

【 0 2 1 7 】

[目的物 9 3 0 の状態確認]

取引開始前に、ユーザ B が目的物 9 3 0 の状態確認を希望する場合がある。この場合、ユーザ A は、目的物 9 3 0 の状態を示す情報（ステータス情報と称する場合がある。）を、ユーザ B に送信する。ステータス情報は、目的物 9 3 0 が譲渡契約の条件を満足することを確認できる情報であればよく、その詳細については特に限定されない。一実施形態によれば、クライアント端末 2 2 は、目的物 9 3 0 の外観の画像を含むステータス情報を、クライアント端末 2 4 に送信する。他の実施形態によれば、クライアント端末 2 2 は、近距離無線通信又は有線通信により、目的物 9 3 0 に配されたコンピュータから、目的物 9 3 0 のステータス情報を取得する。例えば、目的物 9 3 0 が自動車である場合、クライアント端末 2 2 は、目的物 9 3 0 のコンピュータにアクセスして、目的物 9 3 0 の走行距離に関する情報を取得する。クライアント端末 2 2 は、目的物 9 3 0 から取得したステータス情報をクライアント端末 2 4 に送信する。

【 0 2 1 8 】

ステータス情報は、電子メールプログラム、メッセージプログラムなどを利用してクライアント端末 2 4 に送信されてもよく、権利管理サーバ 9 4 0 を介して、クライアント端末 2 4 に送信されてもよい。ステータス情報は、権利管理サーバ 9 4 0 により提供されるサービスを利用してクライアント端末 2 4 に送信されてもよい。

【 0 2 1 9 】

ユーザ A が、権利管理サーバ 9 4 0 により提供されるサービスを利用する場合、ユーザ A は、例えば下記の手順により、ステータス情報をクライアント端末 2 4 に送信する。ユーザ A は、まず、クライアント端末 2 2 を操作して、目的物 9 3 0 の状態を報告させるための命令を、目的物 9 3 0 に送信する。これにより、クライアント端末 2 2 がステータス情報を取得することができる。次に、ユーザ A は、権利管理サーバ 9 4 0 により提供されるファイル共有サービスを利用して、ステータス情報を、クライアント端末 2 2 から権利管理サーバ 9 4 0 にアップロードする。

【 0 2 2 0 】

次に、ユーザ A は、クライアント端末 2 2 を操作して、ステータス情報の読み込みに関するアクセス権を発行するためのトランザクションを生成する。クライアント端末 2 2 は、上記のトランザクションを権利管理サーバ 9 4 0 に送信する。また、ユーザ A は、クライアント端末 2 2 を操作して、ステータス情報の読み込みに関するアクセス権をユーザ B に移転することを示すトランザクションを生成する。クライアント端末 2 2 は、上記のトランザクションを権利管理サーバ 9 4 0 に送信する。このとき、クライアント端末 2 2 は、上記のアクセス権に関する内容情報を権利管理サーバ 9 4 0 に送信してもよい。なお、後述の他の権利についても、上記のアクセス権と同様にして、トランザクション及び内容情報が権利管理サーバ 9 4 0 に送信されてよい。

【 0 2 2 1 】

権利管理サーバ 9 4 0 は、上記の 2 つのトランザクションを分散型台帳管理システム 1 1 0 に転送する。これにより、ユーザ B がステータス情報にアクセスできるようになる。このとき、権利管理サーバ 9 4 0 は、上記のアクセス権に関する内容情報を内容情報格納部 9 4 2 に格納してもよい。なお、後述の他の権利についても、上記のアクセス権と同様

10

20

30

40

50

にして、内容情報が内容情報格納部 9 4 2 に格納されてもよい。また、情報管理部 9 4 4 は、ステータス情報の U R I を、クライアント端末 2 4 に送信する。これにより、ユーザ B は、ステータス情報にアクセスして、当該情報を閲覧することができる。上記の 2 つのトランザクションには、ステータス情報のハッシュ値が格納されていてもよい。これにより、ステータス情報の信憑性が担保される。これらのサービスは、情報管理部 9 4 4 における情報処理により実現されてよい。

【 0 2 2 2 】

[エスクローサービスの開始]

ユーザ B がステータス情報を確認した上で、目的物 9 3 0 の所有権の移転を希望する場合、ユーザ B は、クライアント端末 2 4 を操作して、権利管理サーバ 9 4 0 に、エスクローサービスの提供開始を要求する。権利管理サーバ 9 4 0 は、クライアント端末 2 4 からの要求を受信して、当該要求に応じて、エスクローサービスに関する処理を開始する。エスクローサービスに関する処理は、情報管理部 9 4 4 における情報処理により実現されてよい。情報管理部 9 4 4 は、エスクローサービスに関する処理を実行するエスクローサービス提供部を有してよい。

10

【 0 2 2 3 】

例えば、情報管理部 9 4 4 は、クライアント端末 2 4 から、エスクローサービスの開始を要求することを示す情報を取得すると、クライアント端末 2 4 に対して、代金の供託処理を実行することを要求する。クライアント端末 2 4 は、情報管理部 9 4 4 からの要求を受信すると、例えば、クライアント端末 2 4 の表示装置にユーザ B に対して代金の供託を促す画面を表示させる。ユーザ B が、権利管理サーバ 9 4 0 により提供される代金供託サービスを利用する場合、クライアント端末 2 4 は、表示装置に代金供託サービス用のユーザ・インタフェースを表示させてよい。目的物 9 3 0 の代金は、ビットコインなどの暗号通貨を利用して供託されてもよい。例えば、ユーザ B は、秘密鍵 2 1 2 4 に対応するアドレスに代金を送金する。

20

【 0 2 2 4 】

供託金の金額は、目的物 9 3 0 の代金と同一であってもよく、目的物 9 3 0 の代金より少なくてもよく、目的物 9 3 0 の代金より多くてもよい。供託金の金額は、目的物 9 3 0 の代金と、暗号通貨の相場変動のリスクに応じた金額及びエスクローサービスの利用手数料に相当する金額の少なくとも一方との合計であってもよい。

30

【 0 2 2 5 】

[目的物 9 3 0 の配送]

情報管理部 9 4 4 は、ユーザ B が目的物 9 3 0 の代金を供託したことを示す情報を取得すると、クライアント端末 2 2 に対して、目的物 9 3 0 をユーザ B に配送することを要求する。例えば、情報管理部 9 4 4 は、クライアント端末 2 2 の表示装置に、ユーザ A に対して目的物 9 3 0 をユーザ B に配送することを促す画面を表示させる。情報管理部 9 4 4 は、ユーザ B が目的物 9 3 0 の代金を支払ったことを示す情報を、クライアント端末 2 4 から取得してもよく、代金決済サービスを提供する情報処理システムから取得してもよい。

40

【 0 2 2 6 】

ユーザ A は、配送前の準備として、(i) 目的物 9 3 0 の機能を制限する、(i i) 目的物 9 3 0 の所有権をサービス提供者に譲渡するなどの処理を実行してよい。例えば、ユーザ A は、目的物 9 3 0 の機能の一部又は全部に制限を課した状態で、目的物 9 3 0 を配送する。一実施形態において、上記の制限は、目的物 9 3 0 の所有権又は使用权を有する者でなければ解除することができないように設定される。この場合、ユーザ A は、クライアント端末 2 2 を操作して、予め定められた期間に限って、ユーザ B が目的物 9 3 0 の一部又は全部を使用する権利を発行するためのトランザクションを生成する。クライアント端末 2 2 は、上記のトランザクションを権利管理サーバ 9 4 0 に送信する。

【 0 2 2 7 】

例えば、ユーザ B がクライアント端末 2 4 を使用して目的物 9 3 0 にアクセスすると、

50

目的物 930 は、クライアント端末 24 からユーザ B を識別するための情報を取得する。また、目的物 930 は、権利管理サーバ 940 にアクセスして、ユーザ B が目的物 930 の使用权を有するか否かを確認する。これにより、目的物 930 の所有権がユーザ B に移転されていない状態であっても、ユーザ B が目的物 930 の動作を確認することができる。

【0228】

他の実施形態において、目的物 930 にユーザ B を識別するための情報を記録しておき、ユーザ B がクライアント端末 24 を使用して目的物 930 にアクセスした場合に、ユーザ B の認証処理を実行してもよい。なお、ユーザ A は、ユーザ B による動作確認に必要な機能については制限を課すことなく、目的物 930 を配送してもよい。

10

【0229】

ユーザ A は、目的物 930 を配送した後、クライアント端末 22 を操作して、配送手続が完了したことを示す情報を権利管理サーバ 940 に送信する。また、ユーザ A は、クライアント端末 22 を操作して、目的物 930 の所有権をサービス提供者に譲渡するためのトランザクションを生成する。クライアント端末 22 は、一定期間が経過しても代金が精算されない場合には、目的物 930 の所有権をユーザ A に戻すようなコードを含むトランザクションを生成してもよい。クライアント端末 22 は、上記のトランザクションを権利管理サーバ 940 に送信する。

【0230】

[目的物 930 の動作確認]

ユーザ B は、目的物 930 を受領すると、目的物 930 の状態及び動作を確認する。ユーザ B が目的物 930 を操作した場合、目的物 930 のコンピュータは、目的物 930 の操作履歴を示すトランザクションを生成し、当該トランザクションを権利管理サーバ 940 に送信させるための命令を、クライアント端末 24 に送信してよい。クライアント端末 24 は、目的物 930 のコンピュータから上記の命令を受信すると、目的物 930 の操作履歴を示すトランザクションを生成して、当該トランザクションを権利管理サーバ 940 に送信する。なお、目的物 930 のコンピュータが、目的物 930 を識別するための秘密鍵（図示していない。例えば、秘密鍵 932 である。）を有している場合、目的物 930 のコンピュータが、目的物 930 の操作履歴を示すトランザクションを生成して、当該トランザクションを権利管理サーバ 940 に送信してもよい。これにより、ユーザ B が目的物 930 を受領していないと虚偽の申告を行うことを抑制することができる。

20

30

【0231】

目的物 930 の状態が譲渡契約の内容に合致する場合、ユーザ B は、クライアント端末 24 を操作して、目的物 930 を受領したことを示す情報（受領確認情報と称する場合がある。）を、権利管理サーバ 940 に送信する。目的物 930 の状態が譲渡契約の内容に合致しない場合、ユーザ B は、クライアント端末 24 を操作して、目的物 930 の受領を拒否することを示す情報（受領拒否情報と称する場合がある。）を、権利管理サーバ 940 に送信する。

【0232】

[所有権の移転及び決済]

情報管理部 944 は、は、クライアント端末 24 から受領確認情報を受信したことに応じて、所有権の移転処理と、代金の支払処理とを実施する。所有権の移転処理及び代金の支払処理は、同時に実施されてよい。情報管理部 944 は、例えば、(i) 目的物 930 の所有権が、サービス提供者からユーザ B に移転することを示すトランザクションデータと、(ii) 目的物 930 の代金に相当する量の暗号通貨が、サービス提供者の供託用の口座アカウントからユーザ A の口座アカウントに移転することを示すトランザクションデータを生成して、分散型台帳管理システム 110 に登録する。

40

【0233】

情報管理部 944 は、エスクローサービスの利用手数料に相当する量の暗号通貨が、ユーザ A 及びユーザ B の少なくとも一方の口座アカウントから、サービス提供者の口座アカ

50

ウントに移転することを示すトランザクションデータを生成して、分散型台帳管理システム110に登録してもよい。供託金の残金が存在する場合、情報管理部944は、供託金の残金に相当する量の暗号通貨が、サービス提供者の供託用の口座アカウントからユーザBの口座アカウントに移転することを示すトランザクションデータを生成して、分散型台帳管理システム110に登録してよい。

【0234】

一方、情報管理部944は、クライアント端末24から受領拒否情報を受信したことに応じて、例えば、下記のとおり、所有権の移転処理と、代金の支払処理とを実施する。情報管理部944は、例えば、(i)目的物930の所有権が、サービス提供者からユーザAに移転することを示すトランザクションデータと、(ii)目的物930の代金に相当する量の暗号通貨が、サービス提供者の供託用の口座アカウントからユーザBの口座アカウントに移転することを示すトランザクションデータとを生成して、分散型台帳管理システム110に登録する。情報管理部944は、エスクローサービスの利用手数料に相当する量の暗号通貨が、ユーザA及びユーザBの少なくとも一方の口座アカウントから、サービス提供者の口座アカウントに移転することを示すトランザクションデータを生成して、分散型台帳管理システム110に登録してもよい。

10

【0235】

トランザクションがブロックチェーンに組み込まれるまで、ある程度の時間を要する。そこで、情報管理部944は、定期的には又は任意のタイミングで、分散型台帳管理システム110にアクセスして、上記のトランザクションのそれぞれが、対応するブロックチェーンに組み込まれたことを確認してよい。情報管理部944は、上記のトランザクションのそれぞれが、対応するブロックチェーンに組み込まれたことを確認した後、所有権の移転処理及び代金の支払処理が完了したことを、クライアント端末22及びクライアント端末24に通知してよい。

20

【0236】

ユーザBは、所有権の移転処理が完了した後、クライアント端末24を操作して、制限を解除するための命令を、目的物930に送信する。目的物930は、分散型台帳管理システム110にアクセスして、ユーザBが上記の命令を実行するための権原又は権限を有しているかを確認する。その後、目的物930は、機能制限を解除するための処理を実行する。これにより、ユーザBは、目的物930を使用することができる。

30

【0237】

本実施形態においては、代金又は供託金の決済に、暗号通貨が利用される場合について説明した。しかしながら、決済手段は、本実施形態に限定されない。他の実施形態において、決済手段として、クレジット決済、現金決済、電子バリュー決済などが利用される。

【0238】

本実施形態においては、権利管理サーバ940が提供する各種のサービスを組み合わせ、エスクローサービスを実現する場合について説明した。しかしながら、権利管理サーバ940により提供されるエスクローサービスは本実施形態に限定されない。他の実施形態において、権利管理サーバ940は、供託サービスを利用せずにエスクローサービスを実現してもよい。

40

【0239】

また、権利管理サーバ940は、ステータス情報の通知、供託金又は代金の支払、商品の配送、所有権の移転などの順番を適宜変更して、エスクローサービスを実現してもよい。一実施形態において、ステータス情報の通知処理は、契約締結前になされてもよい。他の実施形態において、ステータス情報の閲覧処理に代わって、又は、ステータス情報の閲覧処理に加えて、動作確認処理を実施してもよい。動作確認処理は、受領確認処理を兼ねてよい。

【0240】

動作確認処理を実施する場合、例えば、ユーザAは、クライアント端末22を操作して、目的物930の使用権を発行する。目的物930の使用権には有効期限又は有効期間が

50

設定される。このとき、クライアント端末 2 2 は、ユーザ A の秘密鍵 1 2 2 を利用して、有効期限又は有効期間が設定された使用権を発行するためのトランザクションを生成し、権利管理サーバ 9 4 0 に送信する。また、ユーザ A は、クライアント端末 2 2 を操作して、上記の使用権をユーザ B に移転するためのトランザクションを生成し、権利管理サーバ 9 4 0 に送信する。権利管理サーバ 9 4 0 は、クライアント端末 2 2 からトランザクションを受信すると、当該トランザクションを分散型台帳管理システム 1 1 0 に転送する。

【 0 2 4 1 】

一方、ユーザ B は、目的物 9 3 0 を受領した後、クライアント端末 2 4 を操作して、目的物 9 3 0 に設定された機能制限を解除するための命令を、目的物 9 3 0 に送信する。目的物 9 3 0 のコンピュータは、権利管理サーバ 9 4 0 にアクセスして、ユーザ B が目的物 9 3 0 の使用権を有することを確認し、機能制限を解除するための処理を実行する。

10

【 0 2 4 2 】

ユーザ B は、目的物 9 3 0 の動作を確認した後、クライアント端末 2 4 を操作して、目的物 9 3 0 の動作確認が終了したことを示す情報（動作確認情報と称する場合がある。）を、権利管理サーバ 9 4 0 に送信する。権利管理サーバ 9 4 0 は、クライアント端末 2 4 から動作確認情報を受信したことに応じて、所有権の移転処理と、代金の支払処理とを実施する。

【 0 2 4 3 】

一方、目的物 9 3 0 が不良品である場合、ユーザ B は、クライアント端末 2 4 を操作して、目的物 9 3 0 が契約条件を満足しないことを示す情報（クレーム情報と称する場合がある。）を、権利管理サーバ 9 4 0 に送信する。クライアント端末 2 4 は、目的物 9 3 0 のステータス情報を取得して、当該ステータス情報を権利管理サーバ 9 4 0 に送信してもよい。権利管理サーバ 9 4 0 は、ユーザ B からのクレーム情報を、クライアント端末 2 2 に送信する。権利管理サーバ 9 4 0 は、クレーム情報及びステータス情報を、クライアント端末 2 2 に送信してもよい。

20

【 0 2 4 4 】

クレーム情報を受信したユーザ A が、契約の解除を決定した場合、ユーザ A は、クライアント端末 2 2 を操作して、契約の解除を示す情報を、権利管理サーバ 9 4 0 に送信する。権利管理サーバ 9 4 0 は、契約の解除を示す情報を受信すると、例えば、供託金をユーザ B に戻すためのトランザクションを生成して、分散型台帳管理システム 1 1 0 に送信する。権利管理サーバ 9 4 0 は、目的物 9 3 0 がユーザ A に返送され、クライアント端末 2 2 から受領確認情報を受信した後、供託金をユーザ B に戻すための処理を実行してもよい。

30

【 0 2 4 5 】

本実施形態によれば、万が一、ユーザ B が、使用権の期限内に動作確認処理を実施しなかった場合には、ユーザ B は目的物 9 3 0 の使用を継続することができなくなる。また、目的物 9 3 0 の所有権はユーザ A に属するので、ユーザ A は、目的物 9 3 0 を遠隔操作して、目的物 9 3 0 をロックすることもできる。

【 0 2 4 6 】

本実施形態においては、権利管理サーバ 9 4 0 が、図 5 に示されるようなトランザクションデータ 5 0 0 を利用して、エスクローサービスを実現する場合について説明した。しかしながら、トランザクションデータの形式は、本実施形態に限定されない。他の実施形態において、権利管理サーバ 9 4 0 は、コード格納領域にコードが格納されたトランザクションデータを利用して、エスクローサービスを実現してよい。

40

【 0 2 4 7 】

例えば、ユーザ A は、目的物 9 3 0 をユーザ B に配送した後、クライアント端末 2 2 を操作して、コード格納領域に、(i) 「ノード 1 1 2 のコンピュータに、サービス提供者が、ユーザ B から目的物 9 3 0 の代金に相当する額の供託金を受領したことを示す情報を受信したら、(a) 目的物 9 3 0 の所有権がユーザ A からサービス提供者に移転することを示すトランザクションデータを生成して、当該トランザクションデータを分散型台帳管

50

理システム 110 に送信するステップを実行させるためのコード」と、(ii)「ノード 112 のコンピュータに、ユーザ B が目的物 930 を受領したことを示す情報を受信したら、(a) 目的物 930 の所有権がサービス提供者からユーザ B に移転することを示すトランザクションデータと、(b) 目的物 930 の代金に相当する量の暗号通貨が、サービス提供者の供託用の口座アカウントからユーザ A の口座アカウントに移転することを示すトランザクションデータとを生成して、当該トランザクションデータを分散型台帳管理システム 110 に送信するステップを実行させるためのコード」とが格納されたトランザクションデータを生成する。上記のトランザクションデータは、各種の手数料を処理するためのトランザクションデータを生成するためのコードを含んでもよい。

【0248】

クライアント端末 22 は、生成されたトランザクションデータを権利管理サーバ 940 に送信する。権利管理サーバ 940 は、クライアント端末 22 から受信したトランザクションデータを、分散型台帳管理システム 110 に送信する。これにより、上述した実施形態と同様のエスクローサービスを実現することができる。

【0249】

以上、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施の形態に記載の範囲には限定されない。上記実施の形態に、多様な変更または改良を加えることが可能であることが当業者に明らかである。また、技術的に矛盾しない範囲において、特定の実施形態について説明した事項を、他の実施形態に適用することができる。その様な変更または改良を加えた形態も本発明の技術的範囲に含まれ得ることが、特許請求の範囲

【0250】

例えば、本願明細書には、下記のデータ管理システムに関する事項が記載されている。

[項目 A]

ユーザが有する一の権利の変動に関するトランザクション情報を、前記一の権利の変動に関する分散型台帳を管理する分散型台帳管理システムに送信する場合に、前記トランザクション情報の少なくとも一部が前記ユーザの秘密鍵を用いて暗号化された暗号化データを、前記一の権利を一意に特定する権利識別情報又は前記権利識別情報を示す情報に対応付けて、前記分散型台帳管理システムに送信するトランザクション情報送信部を備え、

前記トランザクション情報は、

前記変動における前記一の権利の 1 以上の承継先を示す承継先情報と、

前記一の権利の直前の変動に関する、直前のトランザクション情報の符号化データと、
を含み、

前記分散型台帳管理システムは、P2P ネットワークを構成する複数のノードを有し、

前記複数のノードのそれぞれは、前記分散型台帳を格納し、

前記分散型台帳は、複数のブロックを含み、

前記複数のブロックのそれぞれは、

前記一の権利の 1 以上の変動に関する 1 以上のトランザクション情報と、

直前のブロックの符号化データと、

を含む、

データ管理システム。

[項目 B]

エスクローサービス提供部をさらに備える、

項目 A に記載のデータ管理システム。

【0251】

特許請求の範囲、明細書、および図面中において示した装置、システム、プログラム、および方法における動作、手順、ステップ、および段階等の各処理の実行順序は、特段「より前に」、「先立って」等と明示しておらず、また、前の処理の出力を後の処理で用いるのでない限り、任意の順序で実現しうることに留意すべきである。特許請求の範囲、明細書、および図面中の動作フローに関して、便宜上「まず、」、「次に、」等を用いて説

10

20

30

40

50

明したとしても、この順で実施することが必須であることを意味するものではない。

【符号の説明】

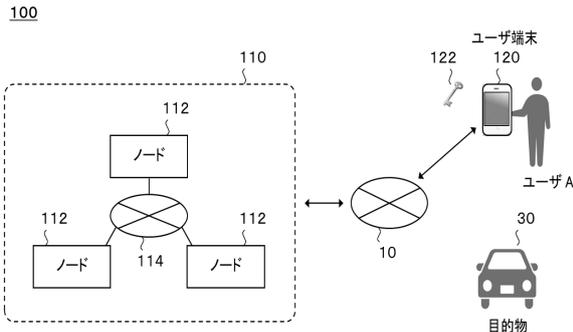
【0252】

10 通信ネットワーク、22 クライアント端末、24 クライアント端末、30
 目的物、100 権利管理システム、110 分散型台帳管理システム、112 ノード
 、114 ピア・ツー・ピア・ネットワーク、120 ユーザ端末、122 秘密鍵、2
 10 通信制御部、220 ブロックチェーン生成部、230 格納部、232 ブロッ
 クチェーン格納部、234 公開鍵格納部、240 要求処理部、300 ブロックチェ
 ーン、310 ブロックヘッダ、320 トランザクションデータ、410 ブロックバ
 ージョン、412 ハッシュ値、414 ハッシュ値、416 ブロックロック時間、4 10
 18 ターゲット、420 ノンス、500 トランザクションデータ、502 バージ
 ョン、504 入力数、506 入力、508 出力数、510 出力、512 ブロッ
 クロック時間、522 ハッシュ値、524 出力インデックス、526 サイズ、52
 8 署名スクリプト、530 署名値、532 公開鍵、534 シーケンス終端記号、
 542 持分、544 サイズ、546 公開鍵検証スクリプト、548 ハッシュ値、
 550 情報、552 情報、610 通信制御部、620 入出力部、630 トラン
 ザクションデータ生成部、640 格納部、642 鍵情報格納部、644 トランザク
 ションデータ格納部、650 要求生成部、700 データテーブル、702 トランザ
 クションID、704 ユーザID、706 ユーザID、708 権利ID、710
 持分情報、712 内容情報、800 データテーブル、802 符号化データ、804 20
 内容情報、900 権利管理システム、920 ユーザ端末、930 目的物、932
 秘密鍵、940 権利管理サーバ、942 内容情報格納部、944 情報管理部、1
 070 命令生成部、1110 入出力部、1120 制御部、1122 通信制御部、
 1124 要求生成部、1126 機能制御部、1128 実行部、1130 格納部、
 1132 権利識別情報格納部、1134 解除条件格納部、2100 エスクローシス
 テム、2122 秘密鍵、2124 秘密鍵、2200 データテーブル、2202 ト
 ランザクションID、2204 操作アカウント、2206 コード、2208 呼出内
 容、2210 備考欄、2300 コントラクトオブジェクト

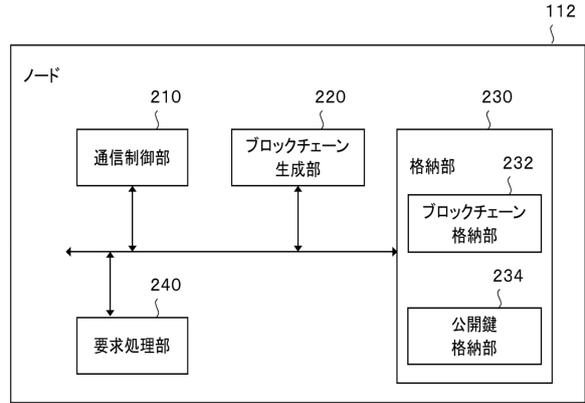
10

20

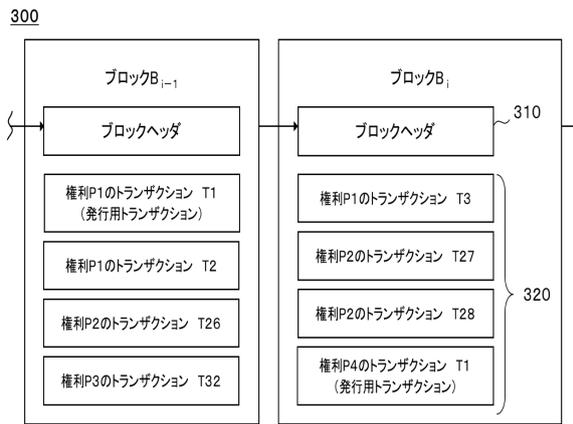
【図1】



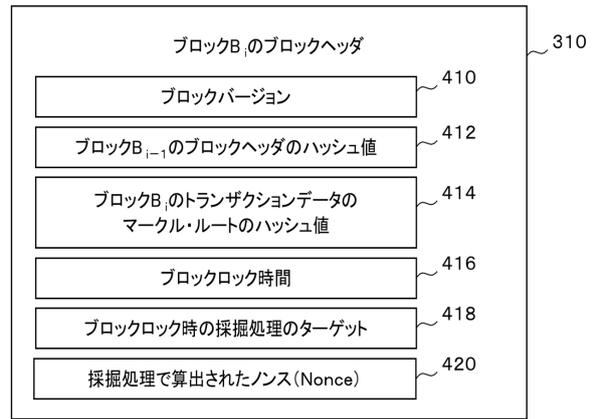
【図2】



【図3】



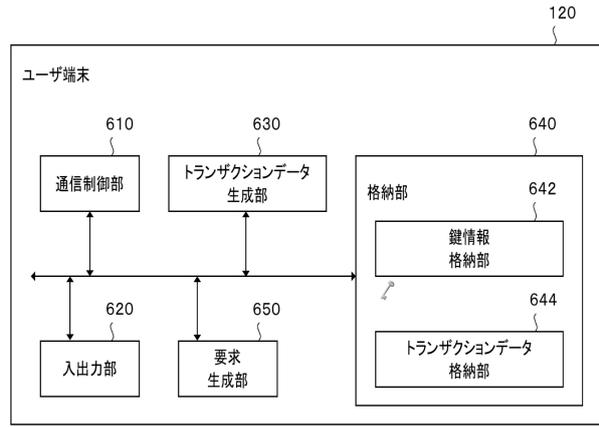
【図4】



【図5】



【図6】



【図7】

700

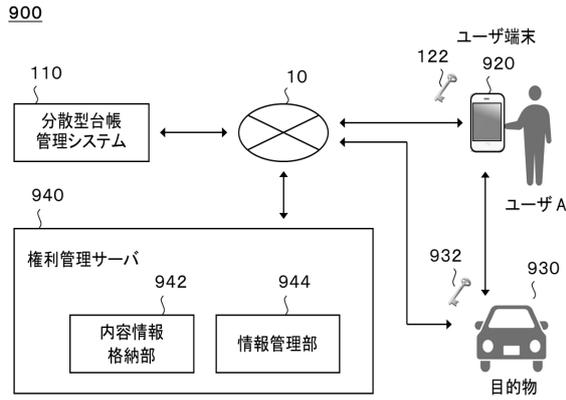
トランザクション ID	被承継人の ユーザID (Fromアドレス)	承継人の ユーザID (Toアドレス)	権利 ID (コイン名)	持分情報 (コイン数)	内容情報
T ₁	-	製造者 X	目的物20	1	原始取得
T ₂	製造者 X	販売者 Y	目的物20	1	移転
T ₃	販売者 Y	ユーザ A	目的物20	1	移転
T ₄	ユーザ A	ユーザ A	目的物20	1	内容変動
T ₅	ユーザ A	ユーザ B	目的物20	1	移転
T ₆	ユーザ B	ユーザ A	目的物20	1	移転
:	:	:	:	:	:

【図8】

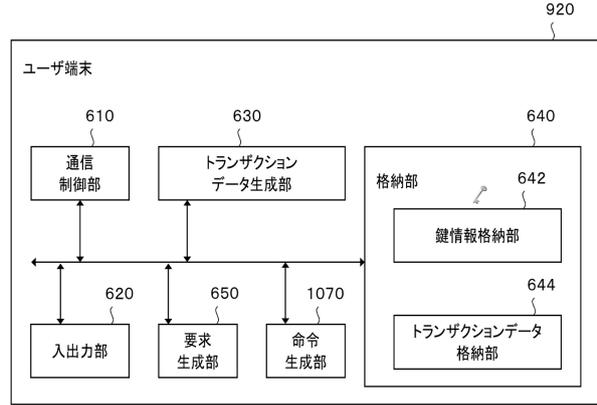
800

内容情報804の 符号化データ	内容情報
*****	権利者: 製造者X, 権利変動の内容: 目的物20の所有権の原始取得
*****	権利者: 販売者Y, 権利変動の内容: 目的物20の所有権の移転
*****	権利者: ユーザA, 権利変動の内容: 目的物20の所有権の移転
*****	権利者: ユーザA, 権利変動の内容: 目的物20の使用 (価値の増減) (走行距離***kmなど)
*****	権利者: ユーザB, 権利変動の内容: 目的物20の所有権の移転 (但し、処分権の行使は禁止する)
:	:

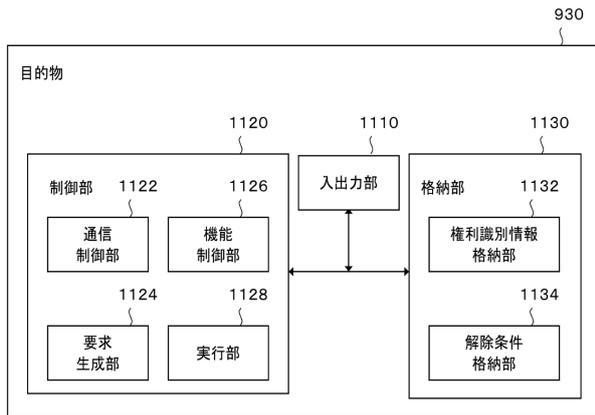
【図 9】



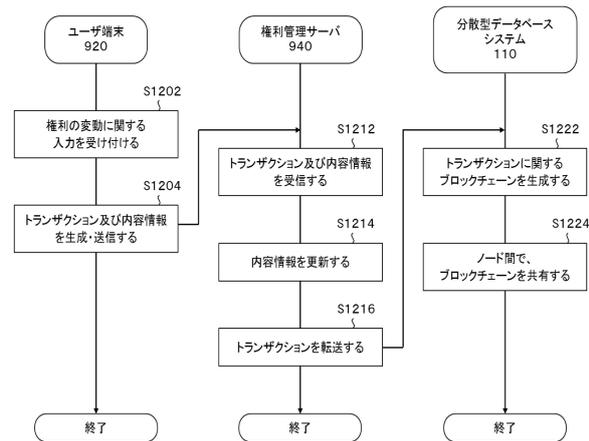
【図 10】



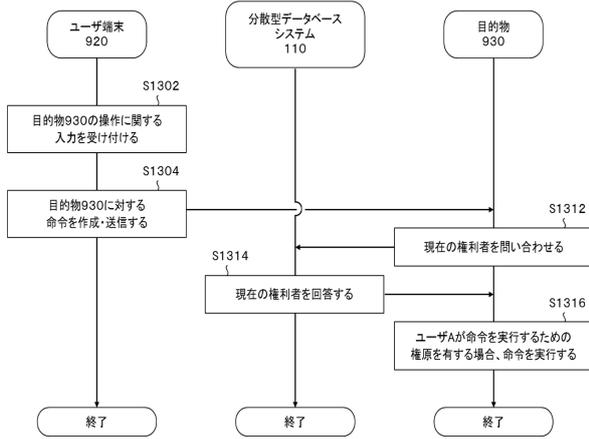
【図 11】



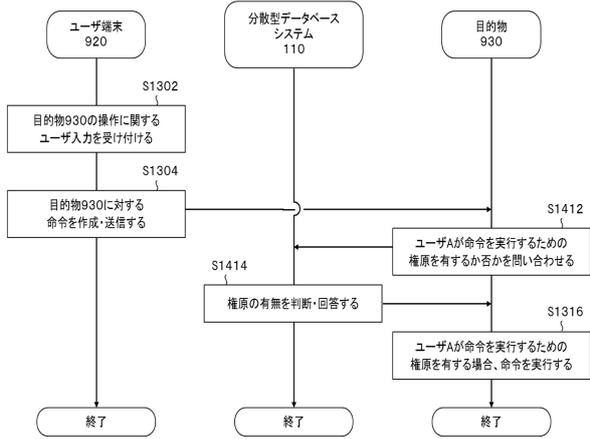
【図 12】



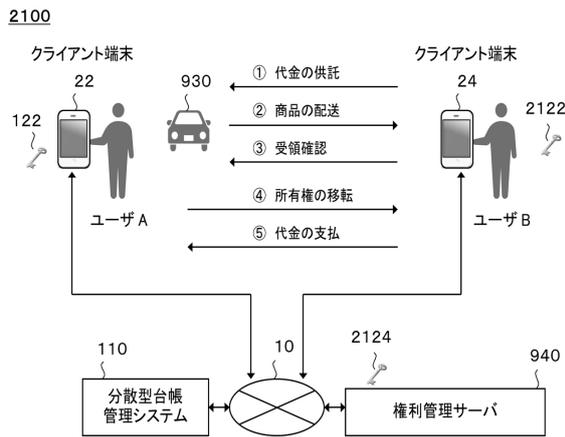
【図13】



【図14】



【図15】



【図16】

2200

トランザクション ID	操作アカウント	実行対象のコード	コードの呼出内容	備考欄
T ₁	製造者 X	-	new Object()	原始取得
T ₂	製造者 X	T1で生成されたコード	transfer (販売者Y)	移転
T ₃	販売者 Y	T1で生成されたコード	transfer (ユーザーA)	移転
T ₄	ユーザー A	T1で生成されたコード	write (dataHash)	内容変動
T ₅	ユーザー A	T1で生成されたコード	transfer (ユーザーB)	移転
T ₆	ユーザー B	T1で生成されたコード	transfer (ユーザーA)	移転
:	:	:	:	:

【 図 17 】

2300

```
contract Object {
    /** 現在の所有者 */
    address owner;
    /** 内容情報の符号化データ */
    string dataHash;

    function Object() {
        owner = msg.sender;
    }

    /** 所有権の移転 */
    function transfer(address toAddress) {
        if (msg.sender != owner) {
            return;
        }
        owner = toAddress;
    }

    /** 内容情報変更 */
    function write(string writeDataHash) {
        if (msg.sender != owner) {
            return;
        }
        dataHash = writeDataHash;
    }
}
```

フロントページの続き

(56)参考文献 特開2016-162431(JP,A)
米国特許出願公開第2016/0012424(US,A1)

(58)調査した分野(Int.Cl., DB名)
G06Q 10/00 - 99/00