

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7573592号
(P7573592)

(45)発行日 令和6年10月25日(2024.10.25)

(24)登録日 令和6年10月17日(2024.10.17)

(51)国際特許分類 F I
G 0 6 Q 50/10 (2012.01) G 0 6 Q 50/10
G 0 6 Q 10/02 (2012.01) G 0 6 Q 10/02

請求項の数 12 (全67頁)

(21)出願番号	特願2022-501918(P2022-501918)	(73)特許権者	514136668 パナソニック インテレクチュアル プロ パティ コーポレーション オブ アメリカ Panasonic Intellec tual Property Corpo ration of America アメリカ合衆国 9 0 5 0 4 カリフォル ニア州, トーランス, スイート 4 5 0 , ウエスト 1 9 0 ストリート 2 0 5 0
(86)(22)出願日	令和3年2月17日(2021.2.17)	(74)代理人	100109210 弁理士 新居 広守
(86)国際出願番号	PCT/JP2021/005827	(74)代理人	100137235 弁理士 寺谷 英作
(87)国際公開番号	WO2021/166928	(74)代理人	100131417 弁理士 道坂 伸一
(87)国際公開日	令和3年8月26日(2021.8.26)		
審査請求日	令和5年11月30日(2023.11.30)		
(31)優先権主張番号	62/979,645		
(32)優先日	令和2年2月21日(2020.2.21)		
(33)優先権主張国・地域又は機関	米国(US)		

最終頁に続く

(54)【発明の名称】 制御方法、制御装置、及び、プログラム

(57)【特許請求の範囲】

【請求項 1】

第1分散台帳を保有している第1ノードと、それぞれ第2分散台帳を保有している複数の第2ノードとを含むシステムにおける前記第1ノードの制御方法であって、

前記複数の第2ノードのそれぞれへの第1トランザクションデータの送信処理を実行し、前記送信処理において前記第1ノードと通信することができた第2ノードの数をカウントし、

カウントした前記数が所定数より多い場合、前記第1トランザクションデータを前記第1分散台帳に格納し、カウントした前記数が前記所定数以下の場合、前記第1トランザクションデータを前記第1分散台帳に格納しない

制御方法。

【請求項 2】

前記格納では、カウントした前記数が所定数より多い場合、前記第1トランザクションデータを含む第1ブロックを生成し、カウントした前記数が前記所定数以下の場合、前記第1ブロックを生成しない

請求項 1 に記載の制御方法。

【請求項 3】

前記第1トランザクションデータは、第1契約に関する契約情報を含む

請求項 1 または 2 に記載の制御方法。

【請求項 4】

10

20

前記第 1 ノードは、前記第 1 分散台帳で第 1 ブロックチェーンを管理し、
前記送信処理において前記第 1 ノードと通信することができた複数の第 2 ノードとの間で、コンセンサスアルゴリズムを実行し、生成した前記第 1 ブロックを前記第 1 ブロックチェーンに格納する
請求項 2 を引用する請求項 3 に記載の制御方法。

【請求項 5】

さらに、
前記第 1 ブロックチェーンに格納された前記第 1 トランザクションデータに含まれる前記第 1 契約に係る処理を実行する
請求項 4 に記載の制御方法。

10

【請求項 6】

カウントした前記数が前記所定数以下の場合、前記カウントを継続しながら所定の条件を満たすまで 1 以上のタイミングで前記送信処理を再実行する
請求項 1 から 5 のいずれか 1 項に記載の制御方法。

【請求項 7】

前記所定の条件は、カウントした前記数が前記所定数より多いこと、または、前記カウントを開始してから所定時間経過することであり、
前記カウントを開始してから前記所定時間経過することを満たすことで前記送信処理の再実行を停止した場合、前記第 1 トランザクションデータを削除する
請求項 6 に記載の制御方法。

20

【請求項 8】

前記システムは、複数の移動体をシェアリングするサービスに用いられ、
前記サービスのサービス対象は、前記複数の移動体であり、
前記第 1 契約は、第 1 の移動体の利用予約であり、
前記第 1 トランザクションデータは、ユーザが前記第 1 ノードを介して前記第 1 の移動体の利用予約を行うための予約トランザクションデータであり、前記ユーザの ID と、前記ユーザが前記第 1 の移動体を利用する時間帯を示す情報と、予約番号とを含む、
請求項 4 または 5 に記載の制御方法。

【請求項 9】

さらに、
前記第 1 ノードが、前記ユーザから前記第 1 の移動体の利用を開始するための要求として前記第 1 の移動体の解錠要求を受信し、
前記第 1 ノードが、前記解錠要求に対応する前記予約トランザクションデータが前記第 1 ブロックチェーンに格納されているか確認し、
前記予約トランザクションデータが格納されている場合、前記時間帯に前記第 1 の移動体を解錠することを前記ユーザに許可する
請求項 8 に記載の制御方法。

30

【請求項 10】

さらに、
前記ユーザに前記第 1 の移動体を貸し出したことを示す貸出トランザクションデータであって、前記ユーザの ID と、前記予約番号と、前記ユーザに前記第 1 の移動体を貸し出した時刻のタイムスタンプとを含む貸出トランザクションデータを取得し、
前記貸出トランザクションデータを含む第 2 ブロックを、前記第 1 ブロックチェーンに格納し、
前記ユーザが前記第 1 の移動体を返却したことを示す返却トランザクションデータであって、前記ユーザの ID と、前記予約番号と、前記ユーザが前記第 1 の移動体を返却した時刻のタイムスタンプとを含む返却トランザクションデータを取得し、
前記返却トランザクションデータを含む第 3 ブロックを、前記第 1 ブロックチェーンに格納し、

40

前記予約トランザクションデータに含まれる前記ユーザの ID に対して、前記第 1 の移

50

動体の利用料金の徴収を実行する

請求項 9 に記載の制御方法。

【請求項 1 1】

第 1 分散台帳を保有している制御装置と、それぞれ第 2 分散台帳を保有している複数の他の制御装置とを備えるシステムにおける制御装置であって、

プロセッサと、

メモリと、を備え、

前記プロセッサは、前記複数の他の制御装置のそれぞれへの第 1 トランザクションデータの送信処理を実行し、

前記プロセッサは、前記送信処理において前記制御装置と通信することができた他の制御装置の数をカウントし、

前記プロセッサは、カウントした前記数が所定数より多い場合、前記第 1 トランザクションデータを前記第 1 分散台帳に格納し、カウントした前記数が前記所定数以下の場合、前記第 1 トランザクションデータを前記第 1 分散台帳に格納しない

制御装置。

【請求項 1 2】

第 1 分散台帳を保有している第 1 ノードと、それぞれ第 2 分散台帳を保有している複数の第 2 ノードとを含むシステムにおける前記第 1 ノードの制御方法をコンピュータに実行させるためのプログラムであって、

前記複数の第 2 ノードのそれぞれへの第 1 トランザクションデータの送信処理を実行し、

前記送信処理において前記第 1 ノードと通信することができた第 2 ノードの数をカウントし、

カウントした前記数が所定数より多い場合、前記第 1 トランザクションデータを前記第 1 分散台帳に格納し、カウントした前記数が前記所定数以下の場合、前記第 1 トランザクションデータを前記第 1 分散台帳に格納しないことを、

コンピュータに実行させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、制御方法、制御装置、及び、プログラムに関する。

【背景技術】

【0002】

例えば特許文献 1 には、車両端末とユーザ端末との間で送受信される利用予約に関する情報をブロックチェーンで適切に管理する技術が開示されている。

【先行技術文献】

【特許文献】

【0003】

【文献】特開 2019 - 153130 号公報

【発明の概要】

【発明が解決しようとする課題】

【0004】

しかしながら、物体の利用予約などの契約または取引の管理にブロックチェーンを用いる場合、特許文献 1 に開示されている技術では、フォークが発生したときのブロックチェーンの振る舞いを悪用して、物体を不正に利用することができてしまうという問題がある。

【0005】

本開示は、上述の事情を鑑みてなされたもので、ブロックチェーンを悪用したサービス対象の不正利用を抑制できる制御方法、制御装置、及び、プログラムを提供することを目的とする。

【課題を解決するための手段】

【0006】

10

20

30

40

50

本開示の一態様に係る制御方法は、第 1 分散台帳を保有している第 1 ノードと、それぞれ第 2 分散台帳を保有している複数の第 2 ノードとを含むシステムにおける前記第 1 ノードの制御方法であって、前記複数の第 2 ノードのそれぞれへの第 1 トランザクションデータの送信処理を実行し、前記送信処理において前記第 1 ノードと通信することができた第 2 ノードの数をカウントし、カウントした前記数が所定数より多い場合、前記第 1 トランザクションデータを前記第 1 分散台帳に格納し、カウントした前記数が前記所定数以下の場合、前記第 1 トランザクションデータを前記第 1 分散台帳に格納しない。

【0007】

なお、これらの包括的または具体的な態様は、システム、方法、集積回路、コンピュータプログラムまたはコンピュータで読み取り可能な CD-ROM などの記録媒体で実現されてもよく、システム、方法、集積回路、コンピュータプログラム及び記録媒体の任意な組み合わせで実現されてもよい。

10

【発明の効果】

【0008】

本開示によれば、ブロックチェーンを悪用したサービス対象の不正利用を抑制できる。

【図面の簡単な説明】

【0009】

【図 1】図 1 は、不正利用を行う方法の手順を説明するための図である。

【図 2 A】図 2 A は、図 1 に示すステップ 1 が行われる場面の一例を示す図である。

【図 2 B】図 2 B は、図 1 に示すステップ 2、3 が行われる場面の一例を示す図である。

20

【図 2 C】図 2 C は、図 1 に示すステップ 4 が行われる場面の一例を示す図である。

【図 2 D】図 2 D は、図 1 に示すステップ 5 が行われる場面の一例を示す図である。

【図 2 E】図 2 E は、図 1 に示すステップ 6 が行われる場面の一例を示す図である。

【図 2 F】図 2 F は、図 1 に示すステップ 6 の後に行われる場面の一例を示す図である。

【図 3 A】図 3 A は、フォークが発生したときのブロックチェーンの振る舞いを説明するための図である。

【図 3 B】図 3 B は、フォークが発生したときのブロックチェーンの振る舞いを説明するための図である。

【図 3 C】図 3 C は、フォークが発生したときのブロックチェーンの振る舞いを説明するための図である。

30

【図 4】図 4 は、実施の形態に係るシステムの構成の一例を示す図である。

【図 5 A】図 5 A は、実施の形態に係るシステムの構成の他の一例を示す図である。

【図 5 B】図 5 B は、実施の形態に係るシステムの構成の他の一例を示す図である。

【図 5 C】図 5 C は、実施の形態に係るシステムの構成の他の一例を示す図である。

【図 6】図 6 は、実施の形態に係る移動体装置の構成の一例を示す図である。

【図 7】図 7 は、実施の形態に係る端末の構成の一例を示す図である。

【図 8】図 8 は、比較例の第 1 例に係るシステムの正常処理の動作概要を示すフローチャートである。

【図 9 A】図 9 A は、図 8 のステップ S 1 の動作により台帳 A 及び台帳 B に格納されるブロックチェーンのブロックを概念的に示す図である。

40

【図 9 B】図 9 B は、図 8 のステップ S 3 の動作により台帳 A 及び台帳 B に格納されるブロックチェーンのブロックを概念的に示す図である。

【図 9 C】図 9 C は、図 8 のステップ S 5 の動作により台帳 A 及び台帳 B に格納されるブロックチェーンのブロックを概念的に説明するための図である。

【図 10】図 10 は、比較例の第 1 例に係るシステムの予約処理を示すシーケンス図である。

【図 11】図 11 は、比較例の第 1 例に係るシステムの貸出処理を示すシーケンス図である。

【図 12】図 12 は、比較例の第 1 例に係るシステムの返却処理を示すシーケンス図である。

50

【図 1 3】図 1 3 は、比較例に係るシステムの料金算定処理の詳細を説明するためのフローチャートである。

【図 1 4】図 1 4 は、比較例の第 2 例に係るシステムの正常処理の動作概要を示すフローチャートである。

【図 1 5 A】図 1 5 A は、図 1 4 のステップ S 1 A の動作により台帳 A に格納されるブロックチェーンのブロックを概念的に示す図である。

【図 1 5 B】図 1 5 B は、図 1 4 のステップ S 3 A の動作により台帳 A に格納されるブロックチェーンのブロックを概念的に示す図である。

【図 1 5 C】図 1 5 C は、図 1 4 のステップ S 5 A の動作により台帳 A に格納されるブロックチェーンのブロックを概念的に示す図である。

10

【図 1 6】図 1 6 は、図 1 4 のステップ S 6 A の動作により台帳 A 及び台帳 B に格納されるブロックチェーンのブロックを概念的に説明するための図である。

【図 1 7】図 1 7 は、図 1 4 のステップ S 6 A の動作により台帳 A 及び台帳 B に格納されるブロックチェーンのブロックを概念的に説明するための図である。

【図 1 8】図 1 8 は、比較例の第 2 例に係るシステムの予約処理を示すシーケンス図である。

【図 1 9】図 1 9 は、比較例の第 2 例に係るシステムの貸出処理を示すシーケンス図である。

【図 2 0】図 2 0 は、比較例の第 2 例に係るシステムの返却処理を示すシーケンス図である。

20

【図 2 1】図 2 1 は、比較例の第 2 例に係る移動体装置 A の通信復帰時に行われるシステムの処理を示すシーケンス図である。

【図 2 2】図 2 2 は、比較例に係るシステムのブロック連結処理を説明するためのフローチャートである。

【図 2 3】図 2 3 は、比較例の第 3 例に係るシステムの不正処理の動作概要を示すフローチャートである。

【図 2 4 A】図 2 4 A は、図 2 3 のステップ S 1 0 の動作により台帳 A に格納されるブロックチェーンのブロックを概念的に示す図である。

【図 2 4 B】図 2 4 B は、図 2 3 のステップ S 1 1 の動作により台帳 A に格納されるブロックチェーンのブロックを概念的に示す図である。

30

【図 2 4 C】図 2 4 C は、図 2 3 のステップ S 1 2 の動作により台帳 A に格納されるブロックチェーンのブロックを概念的に示す図である。

【図 2 5】図 2 5 は、図 2 3 のステップ S 1 3 の動作により台帳 A 及び台帳 B に格納されるブロックチェーンのブロックを概念的に説明するための図である。

【図 2 6】図 2 6 は、図 2 3 のステップ S 1 3 の動作により台帳 A 及び台帳 B に格納されるブロックチェーンのブロックを概念的に説明するための図である。

【図 2 7】図 2 7 は、図 2 3 のステップ S 1 4 の動作により台帳 A 及び台帳 B に格納されるブロックチェーンのブロックを概念的に示す図である。

【図 2 8】図 2 8 は、比較例の第 3 例に係るシステムのローカル予約を行う場合の処理を示すシーケンス図である。

40

【図 2 9】図 2 9 は、比較例の第 3 例に係るシステムの競合予約を行う場合の処理を示すシーケンス図である。

【図 3 0】図 3 0 は、比較例の第 3 例に係るシステムのローカル貸出の処理を示すシーケンス図である。

【図 3 1】図 3 1 は、比較例の第 3 例に係る移動体装置 A の通信復帰時に行われるシステムの処理を示すシーケンス図である。

【図 3 2】図 3 2 は、比較例の第 3 例に係るシステムの返却処理を示すシーケンス図である。

【図 3 3】図 3 3 は、比較例の第 4 例に係るシステムの不正処理の動作概要を示すフローチャートである。

50

【図 3 4 A】図 3 4 A は、図 3 3 のステップ S 1 0 の動作により台帳 A に格納されるブロックチェーンのブロックを概念的に示す図である。

【図 3 4 B】図 3 4 B は、図 3 3 のステップ S 1 1 の動作により台帳 A に格納されるブロックチェーンのブロックを概念的に示す図である。

【図 3 4 C】図 3 4 C は、図 3 3 のステップ S 1 2 の動作により台帳 A に格納されるブロックチェーンのブロックを概念的に示す図である。

【図 3 4 D】図 3 4 D は、図 3 3 のステップ S 1 3 A の動作により台帳 A に格納されるブロックチェーンのブロックを概念的に示す図である。

【図 3 5】図 3 5 は、図 3 3 のステップ S 1 4 A の動作により台帳 A 及び台帳 B に格納されるブロックチェーンのブロックを概念的に説明するための図である。

10

【図 3 6】図 3 6 は、図 3 3 のステップ S 1 4 A の動作により台帳 A 及び台帳 B に格納されるブロックチェーンのブロックを概念的に説明するための図である。

【図 3 7】図 3 7 は、比較例の第 4 例に係るシステムのローカル返却の処理を示すシーケンス図である。

【図 3 8】図 3 8 は、比較例の第 4 例に係る移動体装置 A の通信復帰時に行われるシステムの処理を示すシーケンス図である。

【図 3 9】図 3 9 は、実施の形態に係るシステムのローカル予約不可の処理を示すシーケンス図である。

【図 4 0】図 4 0 は、実施の形態に係るブロック格納対象決定処理を示すフローチャートである。

20

【図 4 1】図 4 1 は、実施の形態に係るシステムのローカル貸出の処理を示すシーケンス図である。

【発明を実施するための形態】

【0010】

(本開示の一態様を得るに至った経緯)

上述したように特許文献 1 には、車両端末とユーザ端末との間で送受信される利用予約に関する情報をブロックチェーンで適切に管理する技術が開示されている。

【0011】

しかしながら、特許文献 1 に開示されている技術では、ブロックチェーンの仕組みを悪用して不正利用できる。以下、例を挙げて説明する。

30

【0012】

図 1 は、不正利用を行う方法の手順を説明するための図である。図 2 A ~ 図 2 F は、図 1 に示す手順が行われる場面の一例を示す図である。図 1 には、複数のバイクをシェアリングするサービスにおけるバイク A に対する利用予約を行い、バイク A を不正利用する場合の手順が示されている。なお、矢印は現在時刻を示す。また、複数のバイクはそれぞれ、ブロックチェーンで予約が管理された台帳を持っているとしている。図 2 A は図 1 に示すステップ 1 が行われる場面の一例を示す図であり、図 2 B は図 1 に示すステップ 2、3 が行われる場面の一例を示す図である。図 2 C は図 1 に示すステップ 4 が行われる場面の一例を示す図であり、図 2 D は図 1 に示すステップ 5 が行われる場面の一例を示す図である。図 2 E は図 1 に示すステップ 6 が行われる場面の一例を示す図であり、図 2 F は図 1 に示すステップ 6 の後に行われるステップ 7 の場面の一例を示す図である。

40

【0013】

不正利用を企てるユーザは、図 2 A に示すように、ステップ 1 において例えば 12 : 00 ~ 12 : 15 の間の 15 分だけ、バイク A を利用する第 1 予約を行う。すると、バイク A の台帳 A は他のバイクの台帳 B、C と通信可能 (オンライン) な状態であるので、図 1 のステップ 1 に示すように、黒色で示される第 1 予約 Tx が、すべての台帳 (台帳 A、B 及び C) に格納される。この結果、バイク A を解錠して、ユーザは、12 : 00 ~ 12 : 15 の間の 15 分だけ利用できる。

【0014】

次に、不正利用を企てるユーザは、図 2 B に示すように、ステップ 2 及び 3 において、

50

バイク A の台帳 A を他のバイクの台帳 B、C と通信不可な（オフライン）状態にする。続いて、不正利用を企てるユーザは、例えば 16 : 00 ~ 16 : 15 の間の 15 分だけ、バイク A を利用する第 2 予約を、他のバイクの台帳 B、C に対して行う。すると、バイク A の台帳 A はオフライン状態であるので、図 1 のステップ 3 に示すように黒色で示される第 2 予約 Tx が、オンライン状態の台帳 B 及び C のみに格納される。

【0015】

次に、不正利用を企てるユーザは、図 2 C に示すように、ステップ 4 において、例えば 12 : 15 ~ 16 : 15 の間、バイク A を利用する不正予約をバイク A の台帳 A に対して行う。すると、バイク A の台帳 A は他のバイクの台帳 B、C と通信不可な（オフライン）状態であるので、図 1 のステップ 4 に示すように、ハッチングで示される不正予約 Tx が、バイク A の台帳 A のみに格納される。この結果、12 : 15 にはバイク A が解錠されるので、図 2 D に示すステップ 5 に示すように、そのユーザは、12 : 15 ~ 16 : 15 の間、オフライン状態のままバイク A を不正利用することができる。この場合、図 1 のステップ 5 に示すように、黒色で示される第 2 予約 Tx が、オンライン状態の台帳 B 及び C のみに格納される。

10

【0016】

次に、そのユーザは、図 2 E に示すように、ステップ 6 において、16 : 00 ~ 16 : 15 の間に、バイク A の台帳 A を他のバイクの台帳 B、C と通信可能な（オンライン）状態に復帰させる。すると、詳細は後述するが、台帳 A、B、C のブロックチェーンでフォークが発生し、図 1 のステップ 6 に示すように台帳 A のブロックチェーンでは、台帳 B、C のブロックチェーンと同じように、第 2 予約 Tx が格納されることになる。そして、不正予約 Tx が第 2 予約 Tx の後に格納されることになる。

20

【0017】

ここで、ステップ 6 においてバイク A の台帳 A がオンライン状態に復帰すると、不正予約 Tx は、第 2 予約 Tx より後に台帳 A、B、C に格納されるというように、フォークが発生したときのブロックチェーンの振る舞いについて説明する。

【0018】

図 3 A ~ 図 3 C は、フォークが発生したときのブロックチェーンの振る舞いを説明するための図である。図 3 A ~ 図 3 C には、移動体 A の台帳 A と移動体 B の台帳 B とに格納されるトランザクションデータが概念的に示されている。Tx は、トランザクションデータを示す。移動体 A は、例えばバイク A であってもよい。

30

【0019】

まず、図 3 A の左側に示すように、移動体 A の台帳 A と移動体 B の台帳 B とが他の移動体（不図示）と通信可能な（オンライン）状態である場合、台帳 A 及び台帳 B には、同じ Tx 1 を含むブロック 1 と、当該ブロック 1 に連結されて Tx 2 を含むブロック 2 が格納される。Tx 2 は、例えば、上記の第 1 予約 Tx に該当させてもよい。

【0020】

このように、台帳 A 及び台帳 B では、Tx 2 を含むブロック 2 が生成されると、前回生成されたブロック 1 に連結される。台帳 A 及び台帳 B では、同一のブロックチェーンが構成されている。

40

【0021】

次に、図 3 A の右側に示すように、移動体 A の台帳 A が他の移動体と通信断絶の（オフライン）状態になっている場合、台帳 A 及び台帳 B には、異なる Tx を含むブロックが格納される。図 3 A の右側に示す例では、台帳 A には、当該ブロック 2 に連結される Tx を含むブロック が格納されている一方で、台帳 B には、当該ブロック 2 に連結される Tx 3 を含むブロック 3 と当該ブロック 3 に連結される Tx 4 を含むブロック 4 とが格納されている。Tx 3 は、例えば、上記の第 2 予約 Tx に該当させ、Tx は、例えば、上記の不正予約 Tx に該当させてもよい。

【0022】

このように、台帳 A がオフライン状態になると、台帳 A 及び台帳 B の通信が断絶される

50

ので、台帳 A 及び台帳 B は独自にブロックチェーンを更新することになる。

【 0 0 2 3 】

次に、図 3 B の左側に示すように、移動体 A の台帳 A が他の移動体との通信可能な状態に復帰（オフライン復帰）させると、台帳 A 及び台帳 B は、異なるブロックチェーンを共有し合う。図 3 B の左側に示す例における台帳 A 及び台帳 B では、当該ブロック 2 に連結されるブロックが分岐し、当該ブロック 2 に T x を含むブロック が連結され、かつ、当該ブロック 2 に T x 3 を含むブロック 3 と T x 4 を含むブロック 4 とが連結される。以下、ブロックに分岐して連結されるブロックチェーンのうち最も長いブロックチェーンを主鎖と称し、それ以外のブロックチェーンを側鎖と称する。図 3 B の左側に示す例では、T x 3 を含むブロック 3 と T x 4 を含むブロック 4 とがブロック 2 の主鎖に該当し、T x を含むブロック がブロック 2 の側鎖に該当する。

10

【 0 0 2 4 】

このように、台帳 A が再びオンライン状態になると、ブロック 2 に連結されるブロックチェーンが分岐し、フォークが発生する。

【 0 0 2 5 】

次に、図 3 B の右側に示すように、ブロック 2 の側鎖である T x を含むブロック が削除され、フォークが解消されている。このとき、ブロック に含まれていた T x は削除されず、各移動体に搭載されている移動体装置のトランザクションプールに保存される。図 3 B の右側に示す例では、移動体装置 A と移動体装置 B のトランザクションプールに T x が保存される。

20

【 0 0 2 6 】

次に、図 3 C に示すように、台帳 A 及び台帳 B では、新たなブロックを生成するタイミングで、T x が含まれて格納される。図 3 C に示す例では、台帳 A 及び台帳 B には、同じ T x を含むブロック 5 が、当該ブロック 4 に連結されて格納される。

【 0 0 2 7 】

このようにして、台帳 A 及び台帳 B では、フォークが解消されて、同じブロックチェーンを持つようになる。以下、図 2 F に戻って説明を続ける。

【 0 0 2 8 】

最後に、不正利用を企てたユーザは、図 2 F に示すように、ステップ 7 において、バイク A を返却する。その後、料金徴収アルゴリズムが実行されて、バイク A の利用料金が徴収される。しかし、第 1 予約分と第 2 予約分のみが料金徴収され、1 2 : 1 5 ~ 1 6 : 1 5 の間の利用分すなわち不正利用分の料金については徴収されない。

30

【 0 0 2 9 】

これは、ステップ 6 においてバイク A の台帳 A がオンライン状態に復帰すると、不正予約 T x は、第 2 予約 T x より後に台帳 A、B、C に格納され、さらに第 2 予約 T x の予約時間帯と不正予約 T x の予約時間帯とはブッキングしているからである。また、料金徴収アルゴリズムは、ブッキングしている予約（つまり、競合予約）であり後の予約である不正予約に対する料金徴収はされない。このようにして、そのユーザは、料金を支払わずにバイク A を 4 時間利用できることになる。

【 0 0 3 0 】

以上のように、物体の利用予約などの管理にブロックチェーンを用いる場合、フォークが発生したときのブロックチェーンの振る舞いを悪用して、物体を不正に利用することができてしまうという問題がある。

40

【 0 0 3 1 】

それに対して、本開示の一態様に係る制御方法は、第 1 分散台帳を保有している第 1 ノードと、それぞれ第 2 分散台帳を保有している複数の第 2 ノードとを含み、サービス対象の利用に用いられるシステムにおける前記第 1 ノードの制御方法であって、前記複数の第 2 ノードのそれぞれへの第 1 トランザクションデータの送信処理を実行し、前記送信処理において前記第 1 ノードと通信することができた第 2 ノードの数をカウントし、カウントした前記数が所定数より多い場合、前記第 1 トランザクションデータを前記第 1 分散台帳

50

に格納し、カウントした前記数が前記所定数以下の場合、前記第1トランザクションデータを前記第1分散台帳に格納しない。

【0032】

これによれば、第1ノードは所定数を越えた数の他の移動体装置である第2ノードと通信できなければ、例えば移動体を利用するための予約トランザクションデータを第1分散台帳に格納しない。これにより、第1ノードを第2ノードと通信不可の状態にさせて、第1分散台帳だけに第1トランザクションデータを格納させるといったサービス対象の不正利用に繋がる処理を抑制することができる。よって、分散台帳を悪用したサービス対象の不正利用を抑制できる。

【0033】

また、例えば、前記格納では、カウントした前記数が所定数より多い場合、前記第1トランザクションデータを含む第1ブロックを生成し、カウントした前記数が前記所定数以下の場合、前記第1ブロックを生成しなくてもよい。

【0034】

このため、所定数を越えた第2ノードと通信できなければ、取得した第1トランザクションデータを含むブロックを生成できない。これにより、第1ノードを第2ノードと通信不可の状態にさせて、第1分散台帳だけに第1トランザクションデータを含むブロックを格納させるといったサービス対象の不正利用に繋がる処理を抑制することができる。よって、ブロックチェーンを悪用したサービス対象の不正利用を抑制できる。

【0035】

また、例えば、前記第1トランザクションは、前記サービス対象の利用を行う第1契約に関する契約情報を含んでもよい。

【0036】

このため、第1ノードを第2ノードと通信不可の状態にさせて、第1分散台帳だけに第1契約に関する契約情報を含む第1トランザクションデータを格納させるといったサービス対象の不正利用に繋がる処理を抑制することができる。

【0037】

また、例えば、前記第1ノードは、前記第1分散台帳で第1ブロックチェーンを管理し、前記送信処理において前記第1ノードと通信することができた複数の第2ノードとの間で、コンセンサスアルゴリズムを実行し、生成した前記第1ブロックを前記第1ブロックチェーンに格納してもよい。

【0038】

また、例えば、さらに、前記第1ブロックチェーンに格納された前記第1トランザクションデータに含まれる前記第1契約を履行してもよい。

【0039】

つまり、第1ブロックチェーンに格納されていないトランザクションデータに含まれる契約は履行されない。よって、分散台帳を悪用したサービス対象の不正利用を抑制できる。

【0040】

また、例えば、カウントした前記数が前記所定数以下の場合、前記カウントを継続しながら所定の条件を満たすまで1以上のタイミングで前記送信処理を再実行してもよい。

【0041】

このため、再実行の送信処理においてカウントした数が所定数より大きければ、第1トランザクションデータを第1分散台帳に格納することができる。よって、一時的な通信不良が原因で第1トランザクションデータが第1分散台帳に格納されない不具合を抑制することができる。

【0042】

また、例えば、前記所定の条件は、カウントした前記数が前記所定数より多いこと、または、前記カウントを開始してから所定時間経過することであり、前記カウントを開始してから前記所定時間経過することを満たすことで前記送信処理の再実行を停止した場合、前記第1トランザクションデータを削除してもよい。

10

20

30

40

50

【 0 0 4 3 】

このため、一時的な通信不良を排除してもカウントした数が所定数以下である場合の第1トランザクションデータを不正なトランザクションデータであると判定し、削除することができる。

【 0 0 4 4 】

また、例えば、前記システムは、複数の移動体をシェアリングするサービスに用いられ、前記サービス対象は、前記複数の移動体であり、前記第1契約は、第1の移動体の利用予約であり、前記第1トランザクションデータは、ユーザが前記第1ノードを介して前記第1の移動体の利用予約を行うための予約トランザクションデータであり、前記ユーザのIDと、前記ユーザが前記第1の移動体を利用する時間帯を示す情報と、予約番号とを含んでもよい。

10

【 0 0 4 5 】

また、例えば、さらに、前記第1ノードが、前記ユーザから前記第1の移動体の利用を開始するための要求として前記第1の移動体の解錠要求を受信し、前記第1ノードが、前記解錠要求に対応する前記予約トランザクションデータが前記第1ブロックチェーンに格納されているか確認し、前記予約トランザクションデータが格納されている場合、前記時間帯に前記第1の移動体を解錠することを前記ユーザに許可してもよい。

【 0 0 4 6 】

これによれば、第1ノードを第2ノードと通信不可の状態にさせて、第1分散台帳だけに予約トランザクションデータを含むブロックを格納させることを抑制できる。このため、第1ノードを第2ノードと通信不可の状態にさせることで行った予約で第1の移動体の解錠をユーザに許可することを抑制できる。

20

【 0 0 4 7 】

また、例えば、さらに、前記ユーザに前記第1の移動体を貸し出したことを示す貸出トランザクションデータであって、前記ユーザのIDと、前記予約番号と、前記ユーザに前記第1の移動体を貸し出した時刻のタイムスタンプとを含む貸出トランザクションデータを取得し、前記貸出トランザクションデータを含む第2ブロックを、前記第1ブロックチェーンに格納し、前記ユーザが前記第1の移動体を返却したことを示す返却トランザクションデータであって、前記ユーザのIDと、前記予約番号と、前記ユーザが前記第1の移動体を返却した時刻のタイムスタンプとを含む返却トランザクションデータを取得し、前記返却トランザクションデータを含む第3ブロックを、前記第1ブロックチェーンに格納し、前記予約トランザクションデータに含まれる前記ユーザのIDに対して、前記第1の移動体の利用料金の徴収を実行してもよい。

30

【 0 0 4 8 】

本開示の一態様に係る制御装置は、第1分散台帳を保有している制御装置と、それぞれ第2分散台帳を保有している複数の他の制御装置とを備え、サービス対象の利用に用いられるシステムにおける制御装置であって、プロセッサと、メモリと、を備え、前記プロセッサは、前記複数の他の制御装置のそれぞれへの第1トランザクションデータの送信処理を実行し、前記プロセッサは、前記送信処理において前記制御装置と通信することができた他の制御装置の数をカウントし、前記プロセッサは、カウントした前記数が所定数より多い場合、前記第1トランザクションデータを前記第1分散台帳に格納し、カウントした前記数が前記所定数以下の場合、前記第1トランザクションデータを前記第1分散台帳に格納しない。

40

【 0 0 4 9 】

本開示の一態様に係るプログラムは、第1分散台帳を保有している第1ノードと、それぞれ第2分散台帳を保有している複数の第2ノードとを含み、サービス対象の利用に用いられるシステムにおける前記第1ノードの制御方法をコンピュータに実行させるためのプログラムであって、前記複数の第2ノードのそれぞれへの第1トランザクションデータの送信処理を実行し、前記送信処理において前記第1ノードと通信することができた第2ノードの数をカウントし、カウントした前記数が所定数より多い場合、前記第1トランザク

50

ションデータを前記第1分散台帳に格納し、カウントした前記数が前記所定数以下の場合、前記第1トランザクションデータを前記第1分散台帳に格納しないことを、コンピュータに実行させるためのプログラムである。

【0050】

以下、図面を参照しながら、実施の形態について説明する。なお、以下で説明する実施の形態は、いずれも本開示の一具体例を示すものである。つまり、以下の実施の形態で示される数値、形状、材料、構成要素、構成要素の配置及び接続形態、ステップ、ステップの順序などは、一例であり、本開示を限定する主旨ではない。また、以下の実施の形態における構成要素のうち、最上位概念を示す独立請求項に記載されていない構成要素は、本開示の課題を達成するために必ずしも必要ではないが、より好ましい形態を構成する構成要素として説明される。

10

【0051】

(実施の形態)

まず、本開示に係るシステム構成について説明する。システムは、第1分散台帳で第1ブロックチェーンを管理する第1ノードと、それぞれ第2分散台帳で第2ブロックチェーンを管理する複数の第2ノードとを含み、サービス対象の利用に用いられる。システムは、例えば、複数の移動体をシェアリングするサービスに用いられてもよく、この場合のサービス対象は、複数の移動体である。本実施の形態では、システムは、端末(または移動体)を介してユーザから特定の移動体の利用予約を受け付けて、受け付けた利用予約に応じて特定の移動体をユーザに貸し出す。システムは、受け付けた利用予約での予約時間帯において、端末(または移動体)を介してユーザから、予約されている特定の移動体に対する貸出要求を受け付けると、ユーザへの特定の移動体の貸出を許可する。具体的には、システムは、ユーザから特定の移動体の解錠要求を受け付けると、事前に為されている利用予約を確認し、確認結果に応じて予約時間帯に特定の移動体を解錠することをユーザに許可する。

20

【0052】

なお、シェアリングするサービスにおける移動体は、例えば、自転車、バイク、自動車、船舶、飛行体などを含む。

【0053】

図4は、実施の形態に係るシステムの構成の一例を示す図である。

30

【0054】

システム1は、図4に示すように、例えば、移動体10A~10Cと、端末11A~11Cとを備える。この例では、移動体10A~10Cのそれぞれは、同じ内容のデータを共有するための分散台帳を保有している。これらの分散台帳では、例えば、同じ構成のブロックチェーンが共有されている。

【0055】

移動体10A~10Cと、端末11A~11Cとは、ネットワークで接続されている。ネットワークは、例えば、インターネット、携帯電話のキャリアネットワークなどであるが、どのような通信回線またはネットワークから構成されてもよい。

【0056】

なお、以下では、移動体10A~10Cのそれぞれを移動体10とも称するが、移動体10A~10Cを移動体A~移動体Cと称する場合もある。また、端末11A~11Cのそれぞれを端末11とも称するが、端末11A~11Cを端末A~端末Cと称する場合もある。また、移動体10A~10Cがそれぞれ備える分散台帳を台帳A~台帳Cと称する場合もある。

40

【0057】

なお、ブロックチェーンを格納する分散台帳を管理するシステムは、パブリック型、プライベート型及びコンソーシアム型のいずれの形態であってもよい。

【0058】

図5Aは、実施の形態に係るシステムの構成の他の一例を示す図である。

50

【 0 0 5 9 】

図 5 A では、例えば、移動体 1 0 A、1 0 B と、端末 1 1 A、1 1 B と、管理サーバ 2 0 とが示されている。この例では、移動体 1 0 A、1 0 B と、管理サーバ 2 0 とのそれぞれは、同じ内容のデータを共有するための分散台帳を保有している。これらの分散台帳では、例えば、同じ構成のブロックチェーンが共有されている。

【 0 0 6 0 】

移動体 1 0 A、1 0 B と、端末 1 1 A、1 1 B と、管理サーバ 2 0 とは、ネットワークで接続されている。ネットワークは、例えば、インターネット、携帯電話のキャリアネットワークなどであるが、どのような通信回線またはネットワークから構成されてもよい。

【 0 0 6 1 】

図 5 B は、実施の形態に係るシステムの構成の他の一例を示す図である。

【 0 0 6 2 】

図 5 B では、例えば、移動体 1 0 A ~ 1 0 C と、端末 1 1 A ~ 1 1 C とが示されている。この例では、端末 1 1 A ~ 1 1 C のそれぞれは、同じ内容のデータを共有するための分散台帳を保有している。これらの分散台帳では、例えば、同じ構成のブロックチェーンが共有されている。

【 0 0 6 3 】

移動体 1 0 A ~ 1 0 C と、端末 1 1 A ~ 1 1 C とは、ネットワークで接続されている。ネットワークは、例えば、インターネット、携帯電話のキャリアネットワークなどであるが、どのような通信回線またはネットワークから構成されてもよい。

【 0 0 6 4 】

図 5 C は、実施の形態に係るシステムの構成の他の一例を示す図である。

【 0 0 6 5 】

図 5 C では、例えば、移動体 1 0 A ~ 1 0 C と、端末 1 1 A ~ 1 1 C とが示されている。この例では、移動体 1 0 A ~ 1 0 C と、端末 1 1 A ~ 1 1 C とのそれぞれは、同じ内容のデータを共有するための分散台帳を保有している。これらの分散台帳では、例えば、同じ構成のブロックチェーンが共有されている。

【 0 0 6 6 】

移動体 1 0 A ~ 1 0 C と、端末 1 1 A ~ 1 1 C とは、ネットワークで接続されている。ネットワークは、例えば、インターネット、携帯電話のキャリアネットワークなどであるが、どのような通信回線またはネットワークから構成されてもよい。

【 0 0 6 7 】

以下では、図 4 のシステムにおける各構成について説明する。なお、図 5 A ~ 図 5 C のシステムの構成については、図 4 のシステムと比較して分散台帳を保有する装置または端末が異なるだけであり、同様に適用可能である。

【 0 0 6 8 】

まず、移動体 1 0 A ~ 1 0 C に設けられている移動体装置について説明する。なお、以下では、移動体 1 0 A ~ 1 0 C に設けられている移動体装置を、それぞれ移動体装置 A ~ 移動体装置 C と称する場合もある。

【 0 0 6 9 】

[移動体装置 1 0 0]

移動体装置 1 0 0 は、分散台帳でブロックチェーンを管理するノードの一例である。なお、ノードは制御装置と言い換えることができる。

【 0 0 7 0 】

移動体装置 1 0 0 は、移動体 1 0 に搭載されている情報処理装置であり、分散台帳を保有している。移動体装置 1 0 0 は、スマートフォン及びタブレットなどの携帯端末であってもよい。

【 0 0 7 1 】

図 6 は、実施の形態に係る移動体装置 1 0 0 の構成の一例を示す図である。

【 0 0 7 2 】

10

20

30

40

50

本実施の形態に係る移動体装置 100 は、入力部 101 と、トランザクションデータ生成部 102 と、トランザクションデータ検証部 103 と、ブロック生成部 104 と、同期部 105 と、スマートコントラクト実行部 106 と、ブロックチェーン管理部 107 と、分散台帳記憶部 108 と、状態記憶部 109 と、不正検知部 110 と、通信部 111 と、表示部 112 とを備える。

【0073】

<入力部 101>

入力部 101 は、ユーザからの入力を受け付ける。入力部 101 は、受け付けた情報入力を、表示部 112 に表示したり、トランザクションデータ生成部 102 に送信したり、通信部 111 に送信したりする。例えば、入力部 101 は、返却を示す情報入力をユーザから受け付けてもよい。

10

【0074】

<トランザクションデータ生成部 102>

トランザクションデータ生成部 102 は、トランザクションデータを生成する。

【0075】

本実施の形態では、トランザクションデータ生成部 102 は、ユーザに移動体 10 を貸し出したことを示す貸出トランザクションデータを生成する。具体的には、トランザクションデータ生成部 102 は、ユーザへの移動体 10 の貸出が行われた場合、ユーザに移動体 10 を貸し出したことを示す貸出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 102 は、例えば、ユーザからの解錠要求を受け付けて移動体の解錠が行われた場合、貸出トランザクションデータを生成する。貸出トランザクションデータは、ユーザ ID と、利用予約を識別するための予約番号（予約 ID）と、ユーザに移動体 10 を貸し出した時刻のタイムスタンプとを含む。

20

【0076】

また、トランザクションデータ生成部 102 は、ユーザが移動体 10 を返却したことを示す返却トランザクションデータを生成する。具体的には、トランザクションデータ生成部 102 は、ユーザにより移動体 10 の返却が行われた場合、ユーザが移動体 10 を返却したことを示す返却トランザクションデータを生成する。ユーザにより移動体 10 の返却が行われたことは、入力部 101 が返却を示す情報入力をユーザから受け付けることで判断されてもよいし、端末 11 を介して返却を示す情報入力をユーザから受け付ける（つまり、端末 11 から情報入力を通信部 111 が受信する）ことで判断されてもよいし、ユーザにより移動体 10 に対して施錠が行われたことで判断されてもよいし、予め定められている移動体 10 の返却施設において移動体の返却が受け付けられたときに返却施設から送信される通知を通信部 111 が受信することで判断されてもよい。返却トランザクションデータは、ユーザ ID と、予約番号（予約 ID）と、ユーザが移動体 10 を返却した時刻のタイムスタンプとを含む。

30

【0077】

なお、予約トランザクションデータは、端末 11A によって生成されるが、移動体装置 100 がユーザから利用予約を受け付ける場合には、トランザクションデータ生成部 102 は、利用予約を行うための予約トランザクションデータを生成してもよい。具体的には、トランザクションデータ生成部 102 は、ユーザから利用予約のための入力が入力部 101 に行われた場合、利用予約を示す予約情報を含む予約トランザクションデータを生成する。予約情報は、ユーザ ID と、利用予約を識別するための予約番号（予約 ID）と、ユーザに貸し出す予定の移動体装置 100 を識別するための装置 ID と、予約時間帯とを含む。

40

【0078】

<トランザクションデータ検証部 103>

トランザクションデータ検証部 103 は、通信部 111 がトランザクションデータを受信したとき検証アルゴリズムを実行し、そのトランザクションデータの正当性を検証する。そして、トランザクションデータ検証部 103 は、正当性が検証されたトランザクシ

50

ンデータを状態記憶部 109 のトランザクションプールの領域に格納する。状態記憶部 109 に格納された正当性が検証されたトランザクションデータは、通信部 111 によって、次に生成するブロックに格納すべきトランザクションデータの情報として、他の移動体装置 100 に送信される。

【0079】

例えば、トランザクションデータ検証部 103 は、通信部 111 が受信したトランザクションデータに、正しい方法で生成された電子署名が付与されているかなどを検証する。ここで、通信部 111 が受信するトランザクションデータは、予約トランザクションデータ、貸出トランザクションデータ、及び、返却トランザクションデータのいずれかである。つまり、トランザクションデータ検証部 103 は、予約トランザクションデータ、貸出トランザクションデータ、及び、返却トランザクションデータの正当性を検証する。

10

【0080】

なお、トランザクションデータ検証部 103 は、トランザクションデータがトランザクションデータ生成部 102 により生成される場合には、トランザクションデータの正当性の検証を行わなくてもよい。

【0081】

<ブロック生成部 104 >

ブロック生成部 104 は、トランザクションデータ検証部 103 により正当性が検証されたトランザクションデータを含むブロックを生成する。ブロック生成部 104 は、状態記憶部 109 に記憶されている検証済みの複数のトランザクションデータの中から所定の数のトランザクションデータを含むブロックを生成する。ブロック生成部 104 は、複数のトランザクションデータのうちのまだブロック生成の対象となっていない複数のトランザクションデータの中から、ブロック生成の対象とする複数のブロックを選択する。ブロック生成部 104 は、既にブロック生成の対象となった複数のトランザクションデータを状態記憶部 109 から削除してもよい。

20

【0082】

なお、移動体装置 100 のブロック生成部 104 で生成されるブロックと、他の移動体装置 100 のブロック生成部 104 で生成されるブロックとは異なってもよい。これは、各移動体装置 100 の通信状態によって状態記憶部 109 に格納されている検証済みのトランザクションデータが移動体装置 100 毎に異なっていたり、ブロック生成部 104 におけるブロック生成の判断基準が異なっていたりするためである。

30

【0083】

なお、ブロック生成の判断基準（ブロックに格納すべきトランザクションデータに関するルール）は、各移動体装置 100 が保持していてもよい。ブロック生成部 104 は、ブロック生成部 104 を備える移動体装置 100 が保持しているブロック生成の判断基準に基づいて、状態記憶部 109 に格納されている検証済みの複数のトランザクションデータから、複数のトランザクションデータを選択し、選択した複数のトランザクションデータを含むブロックを生成する。

【0084】

<同期部 105 >

同期部 105 は、他の移動体装置 100 との間で、ブロック生成部 104 において生成されたブロックの同期を行う。

40

【0085】

本実施の形態では、同期部 105 は、他の移動体装置 100 に、通信部 111 を介してブロック生成部 104 において生成されたブロックを送信する。そして、同期部 105 は、送信したブロックについて、他の移動体装置 100 との間で共同でコンセンサスアルゴリズムを実行する。コンセンサスアルゴリズムには、P B F T (Practical Byzantine Fault Tolerance) とよばれるコンセンサスアルゴリズムを用いてもよいし、その他の公知のコンセンサスアルゴリズムを用いてもよい。公知のコンセンサスアルゴリズムとしては、例えば P O W (Proof Of Work) または P O S (Proof Of Stake) などがある。なお

50

、P B F Tを用いる場合、同期部105は、まず、他の移動体装置100のそれぞれからトランザクションデータの検証が成功したか否かを示す報告を受け取り、当該報告の数が所定の数を超えたか否かを判定する。そして、同期部105は、当該報告の数が所定の数を超えたとき、コンセンサスアルゴリズムによってトランザクションデータの正当性が検証された場合であると判定してもよい。このように、同期部105は、他の移動体装置100のそれぞれから通知された報告に基づき、トランザクションデータが正当なトランザクションデータであること（つまり正当性）を合意し、ブロックの正当性を合意する。

【0086】

また、同期部105は、合意済みのブロックを分散台帳記憶部108に記憶されている分散台帳で管理されている第1ブロックチェーンに連結する。

10

【0087】

<スマートコントラクト実行部106>

スマートコントラクト実行部106は、分散台帳記憶部108の分散台帳に格納されたトランザクションデータに含まれるコントラクトコードなどを実行することで、スマートコントラクトを動作させる。

【0088】

《予約SC》

本実施の形態では、スマートコントラクト実行部106は、予約スマートコントラクトを動作させることで、サービス対象である移動体の利用予約を行う予約処理を行わせてもよい。スマートコントラクト実行部106は、分散台帳記憶部108に記憶される分散台帳内のブロックチェーンに予約トランザクションデータを含むブロックが追加された場合、予約処理を行わせてもよい。

20

【0089】

《料金徴収SC》

本実施の形態では、スマートコントラクト実行部106は、料金徴収スマートコントラクトを動作させることで、料金算定処理を行わせてもよい。スマートコントラクト実行部106は、分散台帳記憶部108に記憶される分散台帳内のブロックチェーンに返却トランザクションデータを含むブロックが追加された場合、料金算定処理を行わせる。なお、料金算定処理は、後述するブロックチェーン管理部107により行われる処理と同じである。

30

【0090】

《不正検知SC》

また、本実施の形態では、スマートコントラクト実行部106は、不正検知スマートコントラクトを動作させることで、不正検知処理を行わせてもよい。スマートコントラクト実行部106は、分散台帳記憶部108の第1ブロックチェーンに予約トランザクションデータを含むブロックが追加された場合、不正検知処理を行わせる。なお、不正検知処理は、後述する不正検知部110により行われる処理と同じである。

【0091】

《不正リスト生成SC》

また、本実施の形態では、スマートコントラクト実行部106は、不正リスト生成スマートコントラクトを動作させることで、不正リスト生成処理を行わせてもよい。スマートコントラクト実行部106は、分散台帳記憶部108に記憶される分散台帳内のブロックチェーンに不正トランザクションデータまたは不正検知トランザクションデータを含むブロックが追加された場合、不正検知処理において不正であると判定された不正なトランザクションデータ、又は、当該不正なトランザクションデータを識別するトランザクションデータIDを不正リストに追加する処理を行わせる。

40

【0092】

ここで、不正検知トランザクションデータは、不正検知処理によって不正なトランザクションデータが検知された場合に生成されるトランザクションデータであって、不正リスト生成処理を実行させるためのトランザクションデータである。不正リストは、不正であ

50

ると判定された不正なトランザクションデータのトランザクションデータIDの他に、当該不正なトランザクションデータの契約（例えば利用予約）を行ったユーザのユーザID、不正なトランザクションデータが生成された時刻などを含んでいてもよい。不正リストは、状態情報記憶部109に記憶されてもよいし、外部の装置が備えるメモリに記憶されてもよい。これにより、ユーザは、例えば、端末11を操作することで、不正なトランザクションデータであると判定されたトランザクションデータを検索することができる。

【0093】

このように、スマートコントラクト実行部106は、スマートコントラクトを動作させることで、利用料金の徴収、不正な予約の検知、不正リストの生成などを分散台帳によって管理することができる。なお、料金徴収スマートコントラクト、不正検知スマートコントラクト、及び、不正リスト生成スマートコントラクトは、例えば、ユーザにより端末11のアプリケーションにより生成され、これらのスマートコントラクトを含むブロックが予めブロックチェーンに格納されているものとする。

【0094】

<ブロックチェーン管理部107>

ブロックチェーン管理部107は、分散台帳記憶部108に記憶される分散台帳（以下、第1分散台帳と称する）で管理されているブロックチェーン（以下、第1ブロックチェーンと称する）を管理する。

【0095】

《主鎖・側鎖》

本実施の形態では、ブロックチェーン管理部107は、通信部111を介して他の移動体装置100が保有する分散台帳（以下、第2分散台帳と称する）で管理されているブロックチェーン（以下、第2ブロックチェーンと称する）を取得し、分散台帳記憶部108の第1分散台帳で管理されている第1ブロックチェーンと、取得した第2ブロックチェーンとを比較する。ブロックチェーン管理部107は、比較によって、第1ブロックチェーンを構成している複数のブロックと、第2ブロックチェーンを構成している複数のブロックとが同じであるか否かを判定する。ブロックチェーン管理部107は、第1ブロックチェーンを構成している複数のブロックと、第2ブロックチェーンを構成している複数のブロックとが同じでない場合、第1ブロックチェーンに含まれ、かつ、第2ブロックチェーンに含まれていない1以上の第1差異ブロックの数と、第2ブロックチェーンに含まれ、かつ、第1ブロックチェーンに含まれていない1以上の第2差異ブロックの数とのどちらが多いか（長い）かを判定する。つまり、ブロックチェーン管理部107は、1以上の第1差異ブロックの数と、1以上の第2差異ブロックの数とを比較することで、どちらが主鎖ブロックであるか、及び、どちらが側鎖ブロックであるかを決定する。なお、この決定は、第1ブロックチェーン及び第2ブロックチェーンの比較の結果、第1ブロックチェーンが1以上の第1差異ブロックを有し、かつ、第2ブロックチェーンが1以上の第2差異ブロックを有する場合に行われる。

【0096】

ブロックチェーン管理部107は、1以上の第1差異ブロック及び1以上の第2差異ブロックのうち多い方（長い方）を、第1ブロックチェーン及び第2ブロックチェーンで互いに共通する1以上の共通ブロックの後に追加する。そして、ブロックチェーン管理部107は、さらに、追加した多い方の後に1以上の第1差異ブロック及び1以上の第2差異ブロックのうち少ない方（短い方）に含まれる1以上のトランザクションデータを含む1以上のブロックを追加する。つまり、ブロックチェーン管理部107は、1以上の第1差異ブロック及び1以上の第2差異ブロックのうち多い方を主鎖ブロックとして決定し、1以上の第1差異ブロック及び1以上の第2差異ブロックのうち少ない方を側鎖ブロックとして決定する。そして、ブロックチェーン管理部107は、1以上の共通ブロックの後に、主鎖ブロック、側鎖ブロックに含まれる1以上のトランザクションデータから生成される追加ブロックの順で、主鎖ブロック及び追加ブロックを追加する。

【0097】

10

20

30

40

50

このようにして、ブロックチェーン管理部 107 は、分散台帳記憶部 108 の第 1 分散台帳で管理されている第 1 ブロックチェーンを更新する。つまり、ブロックチェーン管理部 107 は、第 1 ブロックチェーンと、他の移動体装置 100 が保有する第 2 分散台帳で管理されている第 2 ブロックチェーンとを比較して、これらのブロックチェーンの構成が異なる場合には、構成が互いに同じになるように第 1 ブロックチェーンを更新する。

【0098】

なお、ブロックチェーン管理部 107 は、第 1 ブロックチェーン及び第 2 ブロックチェーンの比較の結果、第 1 ブロックチェーンが 1 以上の第 1 差異ブロックを有していない場合、第 1 ブロックチェーンに 1 以上の第 2 差異ブロックを追加することで第 1 ブロックチェーンを更新する。

10

【0099】

ここで、1 以上の第 1 差異ブロックは、例えば、移動体装置 100 が他の移動体装置 100 と通信できない状態で第 1 ブロックチェーンに追加されることで生じた、第 2 ブロックチェーンには含まれていないブロックである。なお、1 以上の第 1 差異ブロックの数は、複数の他の移動体装置 100 が互いに通信可能な状態である場合、1 以上の第 2 差異ブロックの数よりも少ない可能性が高い。これは、第 2 ブロックチェーンは、第 1 ブロックチェーンを管理している移動体装置 100 よりも多い台数の複数の他の移動体装置 100 のそれぞれが保有する第 2 分散台帳で同期されて管理されているからであり、複数の他の移動体装置 100 において 1 台の移動体装置 100 よりもブロックを生成する機会が多く発生すると考えられるからである。このため、他の移動体装置 100 との間で通信できない 1 台の移動体装置 100 で生じた 1 以上の第 1 差異ブロックは、主鎖ブロックよりも側鎖ブロックとなる可能性が高い。

20

【0100】

1 以上の第 1 差異ブロックは、契約に関する情報を含むトランザクションデータを含むブロックを有していてもよい。契約は、例えば移動体 10 の利用予約である。契約に関する情報を含むトランザクションデータは、例えば予約トランザクションデータ、返却完了トランザクションデータ、貸出トランザクションデータ、及び、返却トランザクションデータである。

【0101】

なお、ブロックチェーン管理部 107 は、第 2 ブロックチェーンの全てを取得しなくてもよく、一部を取得すればよい。例えば、ここでブロックチェーン管理部 107 に取得される第 2 ブロックチェーンの一部とは、前回の第 1 ブロックチェーンの更新が実行された後の最後のブロックより後のブロック以降の 1 以上のブロックである。

30

【0102】

《貸出処理》

また、ブロックチェーン管理部 107 は、移動体 10 をユーザに貸し出すための貸出処理を行ってもよい。この場合、ブロックチェーン管理部 107 は、通信部 111 が解錠要求を受信すると、分散台帳記憶部 108 に記憶されている第 1 分散台帳内の第 1 ブロックチェーンを参照することで、解錠要求に基づく予約が為されているか否かを確認する。具体的には、ブロックチェーン管理部 107 は、解錠要求に含まれる予約番号と同じ予約番号を含む予約トランザクションデータが第 1 ブロックチェーンに格納されているか否かを判定する。ブロックチェーン管理部 107 は、解錠要求に含まれる予約番号と同じ予約番号を含む予約トランザクションデータが第 1 ブロックチェーンに格納されている場合、解錠要求に基づく予約が為されていると判断し、移動体 10 に解錠指示する。解錠指示することで、ブロックチェーン管理部 107 は、移動体 10 の解錠をユーザに許可する。移動体 10 は、解錠指示を取得すると、解錠指示に基づいて、施錠を行っているアクチュエータを動作させ、移動体 10 の施錠を解除（解錠）する。

40

【0103】

解錠要求は、ユーザが利用予約において利用を予約した移動体装置 100 のロックを解除するための情報である。解錠要求は、利用予約を特定するために少なくとも予約番号を

50

含んでいけばよい。解錠要求は、さらに、利用予約したユーザを示すユーザID、利用予約の対象の移動体10の移動体ID、移動体10を予約した移動体装置100の装置ID、予約時間帯などを含んでいてもよい。

【0104】

なお、ブロックチェーン管理部107は、解錠要求を受信する代わりに、第1ブロックチェーンに格納されている利用予約の予約時間帯の開始時刻になった場合に、移動体装置100が設けられている移動体に解錠指示してもよい。

【0105】

《料金算定処理》

また、ブロックチェーン管理部107は、スマートコントラクト実行部106に実行されるスマートコントラクトの代わりに、料金算定処理を行ってもよい。ブロックチェーン管理部107は、前回の処理の実行から一定間隔が経過したこと、または、分散台帳記憶部108に記憶されている第1分散台帳内の第1ブロックチェーンに新たに連結されたブロックに返却トランザクションデータが含まれていることをトリガとして、料金算定処理を行う。ブロックチェーン管理部107は、分散台帳記憶部108の第1ブロックチェーンを検索し、互いに両立しない2以上の契約情報をそれぞれ含む2以上のトランザクションデータが、第1分散台帳で管理されている第1ブロックチェーンに含まれるか否かを判定する。互いに両立しない2以上の契約情報とは、具体的には、互いに両立しない2以上の予約情報である。互いに両立しない2以上の予約情報は、例えば、互いに同じ装置IDと、互いに一部の時間帯が重複している2以上の予約時間帯とを含む重複予約である。なお、この判定は、後述する不正検知部110における第1の不正判定と同じであるため、不正検知部110における第1の不正判定の判定結果がある場合には、この判定結果を用いてもよい。ブロックチェーン管理部107は、第1ブロックチェーンに互いに両立しない予約情報が含まれる場合、これらの2以上の予約情報を含む2以上のトランザクションデータのうち、第1ブロックチェーンに最初に追加された1つのトランザクションデータに含まれる契約情報が対応する契約を履行する。つまり、ブロックチェーン管理部107は、重複予約があったときには、重複予約の中で最先の利用予約に対して料金を算定し、算定した料金をユーザから徴収する料金徴収処理を実行する。換言すると、ブロックチェーン管理部107は、重複予約の中で最先の利用予約以外の利用予約に対しては、同一ユーザからの二重徴収を防ぐために、料金算定を行わず料金徴収処理を実行しない。

【0106】

なお、料金算定の対象となる利用予約は、第1ブロックチェーンに格納されている返却トランザクションデータに含まれる予約番号の利用予約であって、まだ料金の算定が行われていない利用予約である。つまり、既に料金の算定が行われた利用予約は、料金算定の対象から除外される。また、仮に返却トランザクションデータに含まれる予約番号に対応する利用予約が第1ブロックチェーンに格納されていない場合、返却トランザクションデータに対する料金算定は行われない。

【0107】

<分散台帳記憶部108>

分散台帳記憶部108は、第1ブロックチェーンで管理されている第1分散台帳を記憶している。本実施の形態では、第1分散台帳は、予約トランザクションデータ、貸出トランザクションデータ、及び、返却トランザクションデータを格納している。

【0108】

<状態記憶部109>

状態記憶部109は、分散台帳の最新版のデータを記憶している記憶部である。状態記憶部109に記憶されているデータは、コンピュータにより変更されたり、削除されたりすることが可能なデータである。状態記憶部109は、例えばスマートコントラクトを実行するための変数、関数などが格納されるオンメモリの領域とトランザクションデータを格納するトランザクションプールの領域とを含む。状態記憶部109は、トランザクションデータ検証部103により正当性が検証されたトランザクションデータを記憶してもよ

10

20

30

40

50

い。状態記憶部 109 は、通信部 111 を介して取得された第 2 ブロックチェーンを記憶してもよい。状態記憶部 109 は、第 2 ブロックチェーンのうちの 1 以上の第 2 差異ブロックを記憶してもよい。状態記憶部 109 は、分散台帳記憶部 108 に記憶されている第 1 ブロックチェーンを記憶してもよい。状態記憶部 109 は、分散台帳に格納される前のトランザクションデータを記憶してもよい。状態記憶部 109 は、トランザクションデータにより呼び出されたスマートコントラクトを記憶してもよい。また、状態記憶部 109 は、分散台帳に格納されているスマートコントラクトの変数を記憶していてもよい。状態記憶部 109 は、トランザクションデータ生成部 102 により生成されたトランザクションデータを記憶してもよい。状態記憶部 109 は、通信部 111 により受信されたトランザクションデータを記憶してもよい。

10

【0109】

状態記憶部 109 は、上述した各データを一時的に記憶してもよい。

【0110】**<不正検知部 110 >**

不正検知部 110 は、トランザクションデータ検証部 103 により検証済みのトランザクションデータが状態記憶部 109 のトランザクションプールの領域に格納されると、ブロック格納対象決定処理を行う。不正検知部 110 は、予め状態記憶部 109 のオンメモリの領域または分散台帳記憶部 108 の第 1 分散台帳に格納されているブロック格納対象決定アルゴリズムを実行することで、ブロック格納対象決定処理を行ってもよい。不正検知部 110 は、自身の移動体装置 100 と通信することができた他の移動体装置 100 の数をカウントし、カウントした数が所定数より多いか否かを判定する。不正検知部 110 は、カウントした数が所定数より多い場合にブロック生成を許可し、カウントした数が処置値以下の場合にブロック生成を許可しない。つまり、不正検知部 110 は、カウントした数が所定数より多い場合のみブロック生成を許可する不正検知処理を行う。

20

【0111】

なお、不正検知部 110 は、不正検知部 110 は、カウントした数が所定数より多い場合のみブロック生成を許可するとしたが、ブロック生成の許可に限らずに、第 1 分散台帳への格納を許可するとしてもよい。つまり、ブロックチェーンを用いてトランザクションデータの共有が各移動体装置 100 で行われていなくてもよく、分散台帳で行われていればよい。

30

【0112】

なお、不正検知部 110 は、複数の他の移動体装置 100 に、トランザクションデータの送信処理を実行し、当該送信処理においてエラーを発生させなかった他の移動体装置 100 を通信可能と判定してもよい。この場合、不正検知部 110 は、エラーを発生させなかった他の移動体装置 100 の数が所定数より多いことで、自身の移動体装置 100 と通信することができた他の移動体装置 100 の数が所定数より多いと判定すればよい。

【0113】

また、複数の他の移動体装置 100 は、トランザクションデータを受信すると、受信完了の通知を、トランザクションデータを送信した移動体装置 100 に返す。このことを利用して、不正検知部 110 は、トランザクションデータの送信処理を実行し、当該送信処理において受信完了の通知を送信した他の移動体装置を通信可能と判定してもよい。この場合、不正検知部 110 は、受信完了の通知を送信した他の移動体装置 100 の数が所定数より多いことで、自身の移動体装置 100 と通信することができた他の移動体装置 100 の数が所定数より多いと判定すればよい。

40

【0114】

なお、不正検知部 110 は、カウントした、自身の移動体装置 100 と通信することができた他の移動体装置 100 の数が所定数以下の場合、カウントを継続しながら所定の条件を満たすまで 1 以上のタイミングでトランザクションデータの送信処理を再実行してもよい。所定の条件は、カウントした数が所定数より多いこと、または、カウントを開始してから所定時間経過することである。つまり、不正検知部 110 は、カウント数が所定数

50

より大きくなったことを検知したとき、または、カウントを開始してから所定時間経過したときに、送信処理の再実行を停止する。不正検知部 110 は、カウント数が所定数より大きくなったことを検知することで送信処理の再実行を停止した場合、送信処理の対象であるトランザクションデータを含むブロックの生成を許可する。不正検知部 110 は、カウントを開始してから所定時間経過することを満たすことで送信処理の再実行を停止した場合、カウント数の条件を満たさないため、送信処理の対象であるトランザクションデータを削除する。

【0115】

このように、所定数を超えた他の移動体装置 100 と通信できなければ、送信処理において送信したトランザクションデータを含むブロックを生成させないので、移動体 100 の不正利用に繋がるようなトランザクションデータをブロックチェーンに格納させないようにできる。これにより、移動体 100 の不正利用に繋がる予約トランザクションデータがトランザクションプールに格納されていても、ブロックチェーンに格納されず、移動体 100 を利用させないようにすることができる。よって、料金算定アルゴリズムでは料金徴収がされない不正予約をそもそも行わせないようにできる。

10

【0116】

《その他》

また、不正検知部 110 は、通信部 111 が他の移動体装置 100 との間で通信できない状態から通信可能になった時のみに、不正検知処理を行ってもよい。また、不正検知部 110 は、通信部 111 が他の移動体装置 100 との間で通信できない状態から通信可能になった時であり、かつ、ブロックチェーン管理部 107 において第 1 ブロックチェーンと第 2 ブロックチェーンとの比較の結果、主鎖ブロックと側鎖ブロックが発生した時のみに、不正検知処理を行ってもよい。

20

【0117】

<通信部 111>

通信部 111 は、ネットワークを介して情報を他の移動体装置 100 または端末 11 に送信したり、他の移動体装置 100 または端末 11 から情報を受信したりする。通信部 111 は、ネットワークを介して他の移動体装置 100 または端末 11 との間で通信を行う。なお、この通信は、T L S (Transport Layer Security) によりなされてもよく、T L S 通信用の暗号鍵は通信部 111 で保持してもよい。

30

【0118】

本実施の形態では、通信部 111 は、端末 11 から予約トランザクションデータを受信する。また、通信部 111 は、端末 11 から解錠要求を受信する。また、通信部 111 は、他の移動体装置 100 から、他の移動体装置 100 において検証済みのトランザクションデータを受信する。通信部 111 は、他の移動体装置 100 との間で、共同でコンセンサスアルゴリズムを実行するために、ブロックの送受信を行う。

【0119】

<表示部 112>

表示部 112 は、入力部 101 が受け付けた情報入力を表示する。表示部 112 は、端末 11 から送信された情報を表示してもよい。表示部 112 は、移動体装置 100 の返却をユーザから受け付けるための表示 (U I : User Interface) を表示してもよい。

40

【0120】

続いて、端末 11 A ~ 11 C について説明する。なお、端末 11 A ~ 端末 11 C の構成は共通しているので、端末 11 と称して説明する。

【0121】

[端末 11]

端末 11 は、ユーザにより使用される端末の一例である。端末 11 は、例えばパーソナルコンピュータであってもよいし、スマートフォン及びタブレットなどの携帯端末であってもよい。

【0122】

50

図7は、実施の形態1に係る端末11の構成の一例を示す図である。

【0123】

本実施の形態に係る端末11は、入力部1101と、表示部1102と、通信部1103とを備える。

【0124】

<入力部1101>

入力部1101は、ユーザの操作による情報入力を受け付ける。入力部1101は、受け付けた情報入力を、表示部1102に表示したり、通信部1103に送信したりする。

【0125】

例えば、入力部1101は、利用予約を行うためのアプリケーションが導入されており、利用予約を行うための表示(UI)への入力を受け付ける。この表示(UI)は、表示部1102に表示される。入力部1101は、端末11を保有しているユーザの電子署名を受け付けて、受け付けた利用予約のための入力と電子署名とを含む予約トランザクションデータを生成する。

10

【0126】

また、入力部1101は、予約した移動体装置100に対して解錠要求のための表示(UI: User Interface)への入力を受け付ける。この表示(UI)は、表示部1102に表示される。入力部1101は、解錠要求のための入力を受け付けて、解錠要求を生成する。

【0127】

<表示部1102>

表示部1102は、入力部1101が受け付けた情報入力を表示する。表示部1102は、利用予約を行うための表示(UI)を表示する。また、表示部1102は、解錠要求のための表示(UI)を表示する。

20

【0128】

<通信部1103>

通信部1103は、ネットワークを介して情報を移動体装置100に送信したり、移動体装置100から情報を受信したりまたは通知されたりする。また、通信部1103は、ネットワークを介して、他の端末11に情報を送信したり、他の端末11からの情報を受信したりしてもよい。

30

【0129】

このように、通信部1103は、ネットワークを介して移動体装置100または他の端末11との間で通信を行う。なお、この通信は、T L Sによりなされてもよく、T L S通信の暗号鍵は通信部1103で保持してもよい。

【0130】

例えば、通信部1103は、予約トランザクションデータを移動体装置100へ送信する。また、通信部1103は、解錠要求を予約した移動体装置100へ送信する。

【0131】

[システムの動作等]

次に、以上のように構成されたシステムの動作について説明する。

40

【0132】

まず、比較例として、複数の移動体をシェアリングするサービスにおける移動体Aに対する処理を正常に行う正常処理について説明し、ブロックチェーンの仕組みを悪用して移動体Aを不正利用する場合の当該処理すなわち不正処理について説明する。その後、不正対策した本開示の当該処理について説明する。

【0133】

[比較例の第1例]

移動体Aが常にオンライン状態である場合の処理を比較例の第1例として説明する。

【0134】

図8は、比較例の第1例に係るシステムの正常処理の動作概要を示すフローチャートで

50

ある。図 8 には、移動体装置 A、B、C がオンライン状態で移動体 A に対する処理を正常に行う正常処理の動作の概要が示されている。図 9 A ~ 図 9 C は、移動体装置 A の台帳 A 及び移動体装置 B の台帳 B に格納されるブロックチェーンのブロックを概念的に説明するための図である。図 9 A は、図 8 のステップ S 1 の動作により台帳 A 及び台帳 B に格納されるブロックチェーンのブロックを概念的に示す図である。図 9 B は、図 8 のステップ S 3 の動作により台帳 A 及び台帳 B に格納されるブロックチェーンのブロックを概念的に示す図である。図 9 C は、図 8 のステップ S 5 の動作により台帳 A 及び台帳 B に格納されるブロックチェーンのブロックを概念的に示す図である。以下では、移動体 A を利用したいユーザが端末 A を用いて、移動体 A に搭載されている移動体装置 A に対して処理を行うとして説明する。

10

【 0 1 3 5 】

図 8 に示すように、まず、例えば端末 A は、移動体装置 A と通信し、移動体装置 A が搭載されている移動体 A の予約処理を行う (S 1)。より具体的には、端末 A は、移動体装置 A と通信し、移動体 A を利用予約するための予約トランザクションデータ $T r s v$ を生成して、移動体装置 A に送信する。この場合、例えば、図 9 A に示すように、移動体装置 A と移動体装置 B とが他の移動体装置と通信可能な (オンライン) 状態であるので、台帳 A 及び台帳 B には共に、移動体 A を利用予約するための予約トランザクションデータ $T r s v$ を含むブロックが格納される。

【 0 1 3 6 】

次に、例えば端末 A は、移動体装置 A と通信し、移動体 A の貸出処理を行う (S 3)。より具体的には、端末 A は、移動体装置 A と通信し、移動体 A を利用するため移動体 A の解錠要求を送信する。すると、移動体装置 A は、移動体 A を解錠させ、移動体 A が解錠されたことをトリガに移動体 A の貸出開始を示す貸出トランザクションデータ $T r n t$ を生成する。この場合、例えば、図 9 B に示すように、移動体装置 A と移動体装置 B とが他の移動体装置と通信可能な (オンライン) 状態であるので、台帳 A 及び台帳 B には共に、移動体 A の貸出開始を示す貸出トランザクションデータ $T r n t$ を含むブロックが格納される。

20

【 0 1 3 7 】

次に、例えば端末 A は、移動体装置 A と通信し、移動体 A の返却処理を行う (S 5)。より具体的には、端末 A を操作したユーザは、解錠された移動体 A を、利用予約した時間を利用して、その後返却する。移動体装置 A は、移動体 A が返却されると、移動体 A の返却完了を示す返却トランザクションデータ $T r t n$ を生成する。この場合、例えば、図 9 C に示すように、移動体装置 A と移動体装置 B とが他の移動体装置と通信可能な (オンライン) 状態であるので、台帳 A 及び台帳 B には共に、移動体 A の返却完了を示す返却トランザクションデータ $T r t n$ を含むブロックが格納される。

30

【 0 1 3 8 】

次に、移動体装置 A などでは、料金算定処理を行う (S 7)。より具体的には、移動体装置 A などでは、料金算定アルゴリズムが実行されて、ユーザが行った移動体 A の利用予約に対して移動体 A を利用した料金が徴収される。

【 0 1 3 9 】

続いて、図 8 に示すステップ S 1 ~ S 5 の処理詳細すなわち予約処理、貸出処理及び返却処理の詳細についてシーケンス図を用いて説明する。以下でも、移動体 A を利用したいユーザが端末 A を用いて、移動体 A に搭載されている移動体装置 A に対して移動体 A の予約処理、貸出処理及び返却処理を行うとして説明する。

40

【 0 1 4 0 】

[比較例の第 1 例に係る予約処理]

図 1 0 は、比較例の第 1 例に係るシステムの予約処理を示すシーケンス図である。

【 0 1 4 1 】

まず、端末 A は、移動体 A を利用したいユーザの操作に基づいて、移動体 A を利用予約するための予約トランザクションデータ $T r s v$ を生成する (S 1 0 1)。ここで、端末

50

Aすなわち端末11Aには、入力部1101としてアプリケーションが導入されており、アプリケーションがユーザの操作に基づいて予約トランザクションデータTrsvを生成してよい。

【0142】

次に、端末Aは、移動体Aの移動体装置Aと通信し、ステップS101で生成した予約トランザクションデータTrsvを移動体装置Aに送信する(S102)。

【0143】

次に、移動体装置Aは、ステップS102で送信された予約トランザクションデータTrsvを受信すると、他の移動体装置である移動体装置B、Cに予約トランザクションデータTrsvを転送する(S103)。これにより、移動体装置B、Cは、予約トランザクションデータTrsvを取得する。

10

【0144】

次に、移動体装置A、B、Cはそれぞれ、取得した予約トランザクションデータTrsvの正当性を含む検証を行う検証アルゴリズムを実行する(S104)。なお、予約トランザクションデータTrsvの検証が成功しなかった場合、予約処理を終了することになる。

【0145】

次に、移動体装置A、B、Cはそれぞれ、ステップS104で実行された検証アルゴリズムにより検証済みの予約トランザクションデータTrsvをトランザクションプールに格納する(S105)。より具体的には、移動体装置Aは、検証済みの予約トランザクションデータTrsvをトランザクションプールaに格納し、移動体装置Bは、検証済みの予約トランザクションデータTrsvをトランザクションプールbに格納する。移動体装置Cは、検証済みの予約トランザクションデータTrsvをトランザクションプールcに格納する。

20

【0146】

次に、移動体装置A、B、Cは互いに、通信可能な状態であるので、次に生成するブロックに格納すべきトランザクションデータの情報をやりとりする(S106)。図10に示す例では、移動体装置A、B、Cは、次に生成するブロックに格納すべきトランザクションデータに、検証済みの予約トランザクションデータTrsvがあることを確認する。

【0147】

次に、移動体装置A、B、Cはそれぞれ、検証済みの予約トランザクションデータTrsvを含むブロックBlc(Trsv)を生成する(S107)。

30

【0148】

次に、移動体装置A、B、Cはそれぞれ、他の移動体装置に、ステップS107で生成したブロックBlc(Trsv)を送信する(S108)。これにより、移動体装置A、B、Cはそれぞれ、他の移動体装置に、ブロックBlc(Trsv)に含まれる予約トランザクションデータTrsvの正当性の検証が成功したことの報告を通知することができる。

【0149】

次に、移動体装置A、B、Cは、共同でコンセンサスアルゴリズムを実行する(S109)。具体的には、移動体装置A、B、Cはそれぞれ、ステップS108で通知された報告に基づき、予約トランザクションデータTrsvが正当なトランザクションデータであること(つまり正当性)を合意し、ブロックBlc(Trsv)の正当性を合意する。図10に示す例では、ブロックBlc(Trsv)に含まれる予約トランザクションデータTrsvが正当なトランザクションデータであること(つまり正当性)が合意され、ブロックBlc(Trsv)の正当性も合意される。なお、ステップS107及びステップS108の処理は、ステップS109でコンセンサスアルゴリズムを実行する際に行われてもよい。

40

【0150】

次に、移動体装置A、B、Cはそれぞれ、ステップS109で合意済みのブロックBl

50

c (T r s v) を分散台帳内のブロックチェーンに連結する (S 1 1 0)。より具体的には、移動体装置 A は、合意済みのブロック B l c (T r s v) を台帳 A 内のブロックチェーンに連結し、移動体装置 B は、合意済みのブロック B l c (T r s v) を台帳 B 内のブロックチェーンに連結する。移動体装置 C は、合意済みのブロック B l c (T r s v) を台帳 C 内のブロックチェーンに連結する。

【 0 1 5 1 】

これにより、図 9 A に示すように、台帳 A、台帳 B 及び台帳 C には共に、移動体 A を利用予約するための予約トランザクションデータ T r s v を含むブロックが格納される。

【 0 1 5 2 】

[比較例の第 1 例に係る貸出処理]

図 1 1 は、比較例の第 1 例に係るシステムの貸出処理を示すシーケンス図である。

【 0 1 5 3 】

まず、端末 A は、移動体 A を利用したいユーザの操作に基づいて、移動体 A の解錠要求を移動体装置 A に送信する (S 3 0 1)。ここで、端末 A すなわち端末 1 1 A には、入力部 1 1 0 1 としてアプリケーションが導入されており、アプリケーションがユーザの操作に基づいて移動体 A の解錠要求を生成して送信してもよい。移動体 A の解錠要求には、ユーザの予約 ID など、対応する移動体 A への予約を識別できる情報が含まれている。

【 0 1 5 4 】

次に、移動体装置 A は、ステップ S 3 0 1 で送信された解錠要求を受信すると、台帳 A のブロックチェーンに解錠要求に対応する予約があるかを確認する (S 3 0 2)。ここで、移動体装置 A は、台帳 A のブロックチェーンに、予約トランザクションデータ T r s v があるか否かを確認することで、解錠要求に対応する予約があるかを確認してもよい。図 1 0 に示す例では、台帳 A のブロックチェーンに、予約トランザクションデータ T r s v が含まれているため、移動体装置 A は台帳 A のブロックチェーンに解錠要求に対応する予約があることを確認できる。

【 0 1 5 5 】

次に、移動体装置 A は、移動体 A のロックを解除する (S 3 0 3)。ここで、移動体装置 A は、移動体 A のロックを管理する機器に対して、解除指示をすることで、移動体 A のロックを解除してもよいし、直接移動体 A のロックを解除してもよい。

【 0 1 5 6 】

次に、移動体装置 A は、移動体 A のロックが解除されたことをトリガに、移動体 A の貸出開始を示す貸出トランザクションデータ T r n t を生成する (S 3 0 4)。貸出トランザクションデータ T r n t には、移動体 A を利用するユーザ ID とともに貸出開始時刻とが含まれる。貸出開始時刻は、例えばロックが解除された時刻である。

【 0 1 5 7 】

次に、移動体装置 A は、他の移動体装置である移動体装置 B、C に貸出トランザクションデータ T r n t を転送する (S 3 0 5)。これにより、移動体装置 B、C は、貸出トランザクションデータ T r n t を取得する。

【 0 1 5 8 】

次に、移動体装置 A、B、C はそれぞれ、貸出トランザクションデータ T r n t の正当性を含む検証を行う検証アルゴリズムを実行する (S 3 0 6)。

【 0 1 5 9 】

次に、移動体装置 A、B、C はそれぞれ、ステップ S 3 0 6 で実行された検証アルゴリズムにより検証済みの貸出トランザクションデータ T r n t をトランザクションプールに格納する (S 3 0 7)。より具体的には、移動体装置 A は、検証済みの貸出トランザクションデータ T r n t をトランザクションプール a に格納し、移動体装置 B は、検証済みの貸出トランザクションデータ T r n t をトランザクションプール b に格納する。移動体装置 C は、検証済みの貸出トランザクションデータ T r n t をトランザクションプール c に格納する。

【 0 1 6 0 】

10

20

30

40

50

次に、移動体装置 A、B、C は互いに、通信可能な状態であるので、次に生成するブロックに格納すべきトランザクションデータの情報をやりとりする (S 3 0 8)。図 1 1 に示す例では、移動体装置 A、B、C は、次に生成するブロックに格納すべきトランザクションデータに、検証済みの貸出トランザクションデータ $T r n t$ があることを確認する。

【0 1 6 1】

次に、移動体装置 A、B、C はそれぞれ、検証済みの貸出トランザクションデータ $T r n t$ を含むブロック $B l c (T r n t)$ を生成する (S 3 0 9)。

【0 1 6 2】

次に、移動体装置 A、B、C はそれぞれ、他の移動体装置に、ステップ S 3 0 9 で生成したブロック $B l c (T r n t)$ を送信する (S 3 1 0)。これにより、移動体装置 A、B、C はそれぞれ、他の移動体装置に、ブロック $B l c (T r n t)$ に含まれる貸出トランザクションデータ $T r n t$ の正当性の検証が成功したことの報告を通知することができる。

10

【0 1 6 3】

次に、移動体装置 A、B、C は、共同でコンセンサスアルゴリズムを実行する (S 3 1 1)。具体的には、移動体装置 A、B、C はそれぞれ、ステップ S 3 1 0 で通知された報告に基づき、貸出トランザクションデータ $T r n t$ が正当なトランザクションデータであること (つまり正当性) を合意し、ブロック $B l c (T r n t)$ の正当性を合意する。図 1 1 に示す例では、ブロック $B l c (T r n t)$ に含まれる貸出トランザクションデータ $T r n t$ が正当なトランザクションデータであること (つまり正当性) が合意され、ブロック $B l c (T r n t)$ の正当性も合意される。なお、ステップ S 3 0 9 及びステップ S 3 1 0 の処理は、ステップ S 3 1 1 でコンセンサスアルゴリズムを実行する際に行われてもよい。

20

【0 1 6 4】

次に、移動体装置 A、B、C はそれぞれ、ステップ S 3 1 1 で合意済みのブロック $B l c (T r n t)$ を分散台帳内のブロックチェーンに連結する (S 3 1 2)。より具体的には、移動体装置 A は、合意済みのブロック $B l c (T r n t)$ を台帳 A 内のブロックチェーンに連結し、移動体装置 B は、合意済みのブロック $B l c (T r n t)$ を台帳 B 内のブロックチェーンに連結する。移動体装置 C は、合意済みのブロック $B l c (T r n t)$ を台帳 C 内のブロックチェーンに連結する。

30

【0 1 6 5】

これにより、図 9 B に示すように、台帳 A、台帳 B 及び台帳 C には共に、貸出トランザクションデータ $T r n t$ を含むブロックが格納され、移動体 A が貸出開始されたことが記録されることになる。

【0 1 6 6】

[比較例の第 1 例に係る返却処理]

図 1 2 は、比較例の第 1 例に係るシステムの返却処理を示すシーケンス図である。

【0 1 6 7】

まず、移動体 A を利用したユーザにより移動体 A が返却されると、移動体装置 A は、移動体 A が返却されたことを確認する (S 5 0 1)。ここで、例えば、ユーザ A は、移動体 A を所定の返却施設に置いたり、移動体 A を所定の位置に置いて移動体装置 A の UI の返却ボタンを押したりすることで、移動体 A を返却できる。ユーザ A は、端末 A に表示される UI の返却ボタンを押して移動体 A を返却してもよい。移動体装置 A は、所定の返却施設または端末 A により移動体 A が返却された旨のメッセージが入力されることで、移動体 A が返却されたことを確認してもよいし、移動体装置 A の UI の返却ボタンが押されたことで、移動体 A が返却されたことを確認してもよい。

40

【0 1 6 8】

次に、移動体装置 A は、移動体 A が返却されたことを確認したことをトリガに、移動体 A の返却完了を示す返却トランザクションデータ $T r t n$ を生成する (S 5 0 2)。返却トランザクションデータ $T r t n$ には、移動体 A を利用するユーザ ID と返却時刻と移動

50

体 A を利用したときの予約 ID とが含まれる。返却時刻は、例えば、移動体 A が返却されたことを移動体装置 A が確認した時刻である。なお、返却トランザクションデータ $T r t n$ に、予約 ID に含める場合に限られず、ユーザの移動体 A の利用料金を算定できる情報を含んでいればよい。

【 0 1 6 9 】

次に、移動体装置 A は、他の移動体装置である移動体装置 B、C に返却トランザクションデータ $T r t n$ を転送する (S 5 0 3)。これにより、移動体装置 B、C は、返却トランザクションデータ $T r t n$ を取得する。

【 0 1 7 0 】

次に、移動体装置 A、B、C はそれぞれ、取得した返却トランザクションデータ $T r t n$ の正当性を含む検証を行う検証アルゴリズムを実行する (S 5 0 4)。 10

【 0 1 7 1 】

次に、移動体装置 A、B、C はそれぞれ、ステップ S 5 0 4 で実行された検証アルゴリズムにより検証済みの返却トランザクションデータ $T r t n$ をトランザクションプールに格納する (S 5 0 5)。より具体的には、移動体装置 A は、検証済みの返却トランザクションデータ $T r t n$ をトランザクションプール a に格納し、移動体装置 B は、検証済みの返却トランザクションデータ $T r t n$ をトランザクションプール b に格納する。移動体装置 C は、検証済みの返却トランザクションデータ $T r t n$ をトランザクションプール c に格納する。なお、図示していないが、移動体装置 A、B、C は互いに、通信可能な状態であるので、次に生成するブロックに格納すべきトランザクションデータの情報をやりとり 20

【 0 1 7 2 】

次に、移動体装置 A、B、C はそれぞれ、検証済みの返却トランザクションデータ $T r t n$ を含むブロック $B l c (T r t n)$ を生成する (S 5 0 6)。

【 0 1 7 3 】

次に、移動体装置 A、B、C はそれぞれ、他の移動体装置に、ステップ S 5 0 6 で生成したブロック $B l c (T r t n)$ を送信する (S 5 0 7)。これにより、移動体装置 A、B、C はそれぞれ、他の移動体装置に、ブロック $B l c (T r t n)$ に含まれる返却トランザクションデータ $T r t n$ の正当性の検証が成功したことの報告を通知することができる。 30

【 0 1 7 4 】

次に、移動体装置 A、B、C は、共同でコンセンサスアルゴリズムを実行する (S 5 0 8)。具体的には、移動体装置 A、B、C はそれぞれ、ステップ S 5 0 7 で通知された報告に基づき、返却トランザクションデータ $T r t n$ が正当なトランザクションデータであること (つまり正当性) を合意し、ブロック $B l c (T r t n)$ の正当性を合意する。図 1 2 に示す例では、ブロック $B l c (T r t n)$ に含まれる返却トランザクションデータ $T r t n$ が正当なトランザクションデータであること (つまり正当性) が合意され、ブロック $B l c (T r t n)$ の正当性も合意される。なお、ステップ S 5 0 6 及びステップ S 5 0 7 の処理は、ステップ S 5 0 8 でコンセンサスアルゴリズムを実行する際に行われてもよい。 40

【 0 1 7 5 】

次に、移動体装置 A、B、C はそれぞれ、ステップ S 5 0 8 で合意済みのブロック $B l c (T r t n)$ を分散台帳内のブロックチェーンに連結する (S 5 0 9)。より具体的には、移動体装置 A は、合意済みのブロック $B l c (T r t n)$ を台帳 A 内のブロックチェーンに連結し、移動体装置 B は、合意済みのブロック $B l c (T r t n)$ を台帳 B 内のブロックチェーンに連結する。移動体装置 C は、合意済みのブロック $B l c (T r t n)$ を台帳 C 内のブロックチェーンに連結する。これにより、図 9 C に示すように、台帳 A、台帳 B 及び台帳 C には共に、返却トランザクションデータ $T r t n$ を含むブロックが格納さ 50

れ、移動体 A の返却完了が記録されることになる。

【 0 1 7 6 】

次に、移動体装置 A、B、C はそれぞれ、ブロックチェーンに格納された予約情報をチェックする (S 5 1 0)。より具体的には、移動体装置 A、B、C はそれぞれ、返却トランザクションデータ $T r t n$ を含むブロックが自身の台帳内のブロックチェーンに連結されることで、予約スマートコントラクトを実行させて、ブロックチェーンに格納された予約情報として予約トランザクションデータ $T r s v$ があることを確認する。

【 0 1 7 7 】

次に、移動体装置 A、B、C はそれぞれ、料金算定アルゴリズムを実行する (S 5 1 1)。図 1 2 に示す例では、移動体 A を利用した料金の徴収が実行される。ここで、料金算定アルゴリズムは予約スマートコントラクトに含まれるとしてもよいし、料金徴収スマートコントラクトに含まれるとしてもよい。移動体装置 A、B、C はそれぞれ、料金徴収スマートコントラクトまたは予約スマートコントラクトを実行させて、予約トランザクションデータ $T r s v$ に含まれる移動体 A の利用予約に対して、料金を徴収する処理を行わせてもよい。なお、料金算定アルゴリズムの実行を、図 1 2 に示す例では返却処理の一部として説明したが、これに限らない。図 8 に示す料金算定処理で行われてもよい。

【 0 1 7 8 】

[比較例に係る料金算定処理]

続いて、図 8 に示すステップ S 7 の料金算定処理の詳細についてフローチャートを用いて説明する。

【 0 1 7 9 】

図 1 3 は、比較例に係るシステムの料金算定処理の詳細を説明するためのフローチャートである。以下では、代表して移動体装置 A で当該処理が行われる場合について説明する。

【 0 1 8 0 】

図 8 に示すステップ S 7 において、まず、移動体装置 A は、料金徴収のトリガがあるかを確認する (S 7 1)。このトリガは、一定間隔が経過したことでよいし、台帳 A のブロックチェーンに新たに連結されたブロックに返却トランザクションデータ $T r t n$ が含まれていることであってもよい。

【 0 1 8 1 】

ステップ S 7 1 において、トリガがあったときには (S 7 1 で Y e s)、移動体装置 A は、台帳 A のブロックチェーン内を検索する (S 7 2)。なお、ステップ S 7 1 において、トリガがないときには (S 7 1 で N o)、移動体装置 A は、ステップ S 7 1 に戻る。

【 0 1 8 2 】

次に、移動体装置 A は、台帳 A のブロックチェーン内に他にも予約 (つまり重複予約) があるかどうかを確認する (S 7 3)。

【 0 1 8 3 】

ステップ S 7 3 において、重複予約があったときには (S 7 3 で Y e s)、予約すなわち返却トランザクションデータ $T r t n$ に含まれる予約 ID が重複予約の中で最先かどうかを確認する (S 7 4)。なお、ステップ S 7 3 において、重複予約がないときには (S 7 3 で N o)、ステップ S 7 5 に進む。

【 0 1 8 4 】

ステップ S 7 4 において、重複予約の中で最先であったときには (S 7 4 で Y e s)、移動体装置 A は、料金算定アルゴリズムを実行する (S 7 5)。これにより、予約すなわち返却トランザクションデータ $T r t n$ に含まれる移動体 A の利用予約を示す予約 ID に対する料金が算定される。なお、ステップ S 7 4 において、重複予約の中で最先でないときには (S 7 4 で N o)、料金算定処理を終了する。

【 0 1 8 5 】

次に、移動体装置 A は、料金徴収処理を実行する (S 7 6)。これにより、ユーザが行った移動体 A の利用予約を示す予約 ID に対して移動体 A を利用した料金が徴収される。予約トランザクションデータ $T r s v$ に含まれる移動体 A の利用予約に対して、料金を徴

10

20

30

40

50

収する処理を行わせてもよい。

【0186】

[比較例の第2例]

比較例の第1例では、移動体Aがオンライン状態である場合に、複数の移動体をシェアリングするサービスにおける移動体Aに対する予約処理、貸出処理及び返却処理を正常に行う場合について説明した。続いて、比較例の第2例として、移動体装置Aがオフライン状態である場合に、移動体Aに対する予約処理、貸出処理及び返却処理を正常に行い、その後、移動体装置Aがオンライン状態に復帰する場合に行われる処理について説明する。

【0187】

図14は、比較例の第2例に係るシステムの正常処理の動作概要を示すフローチャートである。図14には、移動体装置Aがオフライン状態である一方で、移動体装置B、Cとがオンライン状態である場合の移動体Aに対する予約処理、貸出処理及び返却処理を正常に行う正常処理の動作の概要が示されている。図15A～図17は、移動体装置Aの台帳A及び移動体装置Bの台帳Bに格納されるブロックチェーンを概念的に説明するための図である。図15Aは、図14のステップS1Aの動作により台帳Aに格納されるブロックチェーンのブロックを概念的に示す図である。図15Bは、図14のステップS3Aの動作により台帳Aに格納されるブロックチェーンのブロックを概念的に示す図である。図15Cは、図14のステップS5Aの動作により台帳Aに格納されるブロックチェーンのブロックを概念的に示す図である。図16及び図17は、図14のステップS6Aの動作により台帳A及び台帳Bに格納されるブロックチェーンのブロックを概念的に説明するための図である。以下では、移動体Aを利用したいユーザが端末Aを用いて、移動体Aに搭載されている移動体装置Aに対して処理を行うとして説明する。

10

20

【0188】

図14に示すように、まず、例えば端末Aは、他の移動体装置B、Cと通信可能でない(オフライン)状態の移動体装置Aと通信し、オフライン状態の移動体装置Aが搭載されている移動体Aの予約処理を行う(S1A)。つまり、端末Aは、オフライン状態の移動体装置Aに対して移動体Aをローカル予約する予約処理を行う。より具体的には、端末Aは、移動体装置Aと通信し、移動体Aを利用予約するための予約トランザクションデータTrsvを生成して、移動体装置Aに送信する。この場合、例えば、図15Aに示すように、移動体装置Aは移動体装置Bと通信可能でない(オフライン)状態であるので、台帳Aのみに、移動体Aを利用予約するための予約トランザクションデータTrsvを含むブロックが格納される。

30

【0189】

次に、例えば端末Aは、オフライン状態の移動体装置Aと通信し、移動体Aの貸出処理を行う(S3A)。つまり、端末Aは、オフライン状態の移動体装置Aに対して移動体Aをローカル貸出する貸出処理を行う。より具体的には、端末Aは、移動体装置Aと通信し、移動体Aを利用するため移動体Aの解錠要求を送信することができる。すると、移動体装置Aは、移動体Aを解錠させ、移動体Aが解錠されて移動体Aの貸出開始を示す貸出トランザクションデータTrntを生成する。この場合、例えば、図15Bに示すように、移動体装置Aはオフライン状態であるので、台帳Aのみに、移動体Aの貸出開始を示す貸出トランザクションデータTrntを含むブロックが格納される。

40

【0190】

次に、例えば端末Aは、オフライン状態の移動体装置Aと通信し、移動体Aの返却処理を行う(S5A)。つまり、端末Aは、オフライン状態の移動体装置Aに対して移動体Aをローカル返却する返却処理を行う。より具体的には、端末Aを操作したユーザは、解錠された移動体Aを、利用予約した時間利用して、その後返却する。移動体装置Aは、移動体Aが返却されると、移動体Aの返却完了を示す返却トランザクションデータTrtnを生成する。この場合、例えば、図15Cに示すように、移動体装置Aはオフライン状態であるので、台帳Aのみに、移動体Aの返却完了を示す返却トランザクションデータTrtnを含むブロックが格納される。

50

【 0 1 9 1 】

その後、移動体装置 A がオンライン状態に復帰するとする。すると、移動体装置 A がオンライン状態に復帰した時に、システムにおいて復帰時処理が行われる (S 6 A)。より具体的には、ステップ S 1 A ~ ステップ S 5 A では、上述したように、移動体装置 A が移動体装置 B と通信不可の (オフライン) 状態になっている。このため、図 1 6 の (a) に示すように、移動体装置 A がオンライン状態に復帰した時点では、台帳 A 及び台帳 B のブロックチェーンには、異なるブロックが連結されている。次いで、移動体装置 A がオンライン状態に復帰すると、図 1 6 の (b) に示すように、移動体装置 A の台帳 A 及び移動体装置 B の台帳 B には、異なるブロックチェーンを共有し合うことになりフォークが発生する。ここで、オフライン状態の移動体装置 A の台帳 A のブロックチェーンに連結されたブロックが側鎖ブロックに該当し、オンライン状態の移動体装置 B の台帳 B のブロックチェーンに連結されたブロックが主鎖ブロックに該当する。このため、図 1 7 の (a) 及び (b) に示すように、移動体装置 A の台帳 A 及び移動体装置 B の台帳 B では、側鎖ブロックが削除され、側鎖ブロックに含まれるトランザクションデータがトランザクションプールに保存されることで、フォークが解消される。なお、図 1 7 の (b) では、予約トランザクションデータ $T r s v$ と貸出トランザクションデータ $T r n t$ と返却トランザクションデータ $T r t n$ とがトランザクションプールに保存されている。その後、図 1 7 の (c) に示すように、移動体装置 A の台帳 A 及び移動体装置 B の台帳 B のブロックチェーンでは、新たなブロックを生成するタイミングで、トランザクションプールに保存されたトランザクションデータを含むブロックが生成されて連結される。

10

20

【 0 1 9 2 】

次に、移動体装置 A などでは、料金算定処理を行う (S 7)。ステップ S 7 の料金算定処理は、上述した通りであるので説明を省略する。

【 0 1 9 3 】

続いて、図 1 4 に示すステップ S 1 A の予約処理、ステップ S 3 A の貸出処理及び S 5 A の返却処理の詳細すなわちローカル予約、ローカル貸出及びローカル返却の詳細処理についてシーケンス図を用いて説明する。また、図 1 4 に示すステップ S 6 A の移動体装置 A の通信復帰時の処理の詳細についてもシーケンス図を用いて説明する。以下、移動体 A を利用したいユーザが端末 A を用いて、移動体 A に搭載されている移動体装置 A に対して移動体 A の予約処理、貸出処理及び返却処理を行うとして説明する。

30

【 0 1 9 4 】

[比較例の第 2 例に係る予約処理]

図 1 8 は、比較例の第 2 例に係るシステムの予約処理すなわちローカル予約の処理を示すシーケンス図である。図 1 0 と同様の要素には同一の符号を付しており、詳細な説明は省略する。

【 0 1 9 5 】

まず、端末 A は、移動体 A を利用したいユーザの操作に基づいて、移動体 A を利用予約するための予約トランザクションデータ $T r s v$ を生成し (S 1 0 1)、生成した予約トランザクションデータ $T r s v$ を移動体装置 A に送信する (S 1 0 2)。

【 0 1 9 6 】

次に、移動体装置 A は、ステップ S 1 0 2 で送信された予約トランザクションデータ $T r s v$ を受信すると、他の移動体装置である移動体装置 B、C に予約トランザクションデータ $T r s v$ を転送することを試みるが、失敗する (S 1 0 3 A)。移動体装置 A はオフライン状態であるため、移動体装置 B、C に予約トランザクションデータ $T r s v$ を転送できないからである。このため、移動体装置 B、C は、予約トランザクションデータ $T r s v$ を取得しない。

40

【 0 1 9 7 】

次に、移動体装置 A は、取得した予約トランザクションデータ $T r s v$ の正当性を含む検証を行う検証アルゴリズムを実行する (S 1 0 4)。なお、予約トランザクションデータ $T r s v$ の検証が成功しなかった場合、予約処理を終了することになる。

50

【 0 1 9 8 】

次に、移動体装置 A は、ステップ S 1 0 4 で実行された検証アルゴリズムにより検証済みの予約トランザクションデータ T r s v をトランザクションプール a に格納する (S 1 0 5)。

【 0 1 9 9 】

次に、移動体装置 A は、検証済みの予約トランザクションデータ T r s v を含むブロック B l c (T r s v) を生成する (S 1 0 7)。なお、移動体装置 A は、オフライン状態であるので移動体装置 B、C とは、次に生成するブロックに格納すべきトランザクションデータの情報をやりとりしないで、ブロック B l c (T r s v) を生成する。

【 0 2 0 0 】

次に、移動体装置 A は、他の移動体装置である移動体装置 B、C に、ステップ S 1 0 7 で生成したブロック B l c (T r s v) を送信することを試みるが、失敗する (S 1 0 8 A)。移動体装置 A はオフライン状態であるため、移動体装置 B、C にブロック B l c (T r s v) を送信できないからである。

【 0 2 0 1 】

次に、移動体装置 A は、単独でコンセンサスアルゴリズムを実行する (S 1 0 9 A)。具体的には、移動体装置 A は、予約トランザクションデータ T r s v が正当なトランザクションデータであること (つまり正当性) を単独で合意し、ブロック B l c (T r s v) の正当性を単独で合意する。図 1 8 に示す例では、移動体装置 A は、ブロック B l c (T r s v) に含まれる予約トランザクションデータ T r s v が正当なトランザクションデータであること (つまり正当性) を合意することで、ブロック B l c (T r s v) の正当性も合意する。なお、ステップ S 1 0 7 の処理は、ステップ S 1 0 9 A で単独でコンセンサスアルゴリズムを実行する際に行われてもよい。

【 0 2 0 2 】

次に、移動体装置 A は、ステップ S 1 0 9 A で合意済みのブロック B l c (T r s v) を台帳 A 内のブロックチェーンに連結する (S 1 1 0)。

【 0 2 0 3 】

これにより、図 1 5 A に示すように、台帳 A のみに、移動体 A を利用予約するための予約トランザクションデータ T r s v を含むブロックが格納され、予約が確定されることになる。このように、オフライン状態の台帳 A のみで自己完結して予約が確定されることを以下ではローカル予約と称する。

【 0 2 0 4 】

[比較例の第 2 例に係る貸出処理]

図 1 9 は、比較例の第 2 例に係るシステムの貸出処理すなわちローカル貸出の処理を示すシーケンス図である。図 1 1 と同様の要素には同一の符号を付しており、詳細な説明は省略する。

【 0 2 0 5 】

まず、端末 A は、移動体 A を利用したいユーザの操作に基づいて、移動体 A の解錠要求を移動体装置 A に送信する (S 3 0 1)。

【 0 2 0 6 】

次に、移動体装置 A は、ステップ S 3 0 1 で送信された解錠要求を受信すると、台帳 A のブロックチェーンに解錠要求に対応する予約があるかを確認し (S 3 0 2)、移動体 A のロックを解除する (S 3 0 3)。

【 0 2 0 7 】

次に、移動体装置 A は、移動体 A のロックが解除されたことをトリガに、移動体 A の貸出開始を示す貸出トランザクションデータ T r n t を生成する (S 3 0 4)。

【 0 2 0 8 】

次に、移動体装置 A は、他の移動体装置である移動体装置 B、C に貸出トランザクションデータ T r n t を転送することを試みるが、失敗する (S 3 0 5 A)。移動体装置 A はオフライン状態であるため、移動体装置 B、C に貸出トランザクションデータ T r n t を

10

20

30

40

50

転送できないからである。このため、移動体装置 B、C は、貸出トランザクションデータ `Trnt` を取得しない。

【0209】

次に、移動体装置 A は、貸出トランザクションデータ `Trnt` の正当性を含む検証を行う検証アルゴリズムを実行する (S306)。

【0210】

次に、移動体装置 A は、ステップ S306 で実行された検証アルゴリズムにより検証済みの貸出トランザクションデータ `Trnt` をトランザクションプール a に格納する (S307)。

【0211】

次に、移動体装置 A はそれぞれ、検証済みの貸出トランザクションデータ `Trnt` を含むブロック `Blc(Trnt)` を生成する (S309)。なお、移動体装置 A は、オフライン状態であるので移動体装置 B、C とは、次に生成するブロックに格納すべきトランザクションデータの情報をやりとりしないで、ブロック `Blc(Trnt)` を生成する。

【0212】

次に、移動体装置 A は、他の移動体装置である移動体装置 B、C に、ステップ S309 で生成したブロック `Blc(Trnt)` を送信することを試みるが、失敗する (S310A)。移動体装置 A はオフライン状態であるため、移動体装置 B、C にブロック `Blc(Trnt)` を送信できないからである。

【0213】

次に、移動体装置 A は、単独でコンセンサスアルゴリズムを実行する (S311A)。具体的には、移動体装置 A は、貸出トランザクションデータ `Trnt` が正当なトランザクションデータであること (つまり正当性) を単独で合意し、ブロック `Blc(Trnt)` の正当性を単独で合意する。図 19 に示す例では、移動体装置 A は、ブロック `Blc(Trnt)` に含まれる貸出トランザクションデータ `Trnt` が正当なトランザクションデータであること (つまり正当性) を合意することで、ブロック `Blc(Trnt)` の正当性も合意する。なお、ステップ S309 の処理は、ステップ S311 でコンセンサスアルゴリズムを実行する際に行われてもよい。

【0214】

次に、移動体装置 A は、ステップ S311A で合意済みのブロック `Blc(Trnt)` を台帳 A 内のブロックチェーンに連結する (S312)。

【0215】

これにより、図 15B に示すように、台帳 A のみに、貸出トランザクションデータ `Trnt` を含むブロックが格納され、移動体 A が貸出開始されたことが記録されることになる。このように、オフライン状態の台帳 A のみで自己完結して移動体 A が貸出開始されたことが記録されることを以下ではローカル貸出と称する。

【0216】

[比較例の第 2 例に係る返却処理]

図 20 は、比較例の第 2 例に係るシステムの返却処理を示すシーケンス図である。図 12 と同様の要素には同一の符号を付しており、詳細な説明は省略する。

【0217】

まず、移動体 A を利用したユーザにより移動体 A が返却されると、移動体装置 A は、移動体 A が返却されたことを確認する (S501)。

【0218】

次に、移動体装置 A は、移動体 A が返却されたことを確認したことをトリガに、移動体 A の返却完了を示す返却トランザクションデータ `Trtn` を生成する (S502)。

【0219】

次に、移動体装置 A は、他の移動体装置である移動体装置 B、C に返却トランザクションデータ `Trtn` を転送することを試みるが、失敗する (S503A)。移動体装置 A はオフライン状態であるため、移動体装置 B、C に返却トランザクションデータ `Trtn` を

10

20

30

40

50

転送できないからである。このため、移動体装置 B、C は、返却トランザクションデータ `Trtn` を取得しない。

【0220】

次に、移動体装置 A は、取得した返却トランザクションデータ `Trtn` の正当性を含む検証を行う検証アルゴリズムを実行する (S504)。

【0221】

次に、移動体装置 A は、ステップ S504 で実行された検証アルゴリズムにより検証済みの返却トランザクションデータ `Trtn` をトランザクションプール a に格納する (S505)。

【0222】

次に、移動体装置 A は、検証済みの返却トランザクションデータ `Trtn` を含むブロック `Blc(Trtn)` を生成する (S506)。なお、移動体装置 A は、オフライン状態であるので移動体装置 B、C とは、次に生成するブロックに格納すべきトランザクションデータの情報をやりとりしないで、ブロック `Blc(Trtn)` を生成する。

【0223】

次に、移動体装置 A は、他の移動体装置である移動体装置 B、C に、ステップ S506 で生成したブロック `Blc(Trtn)` を送信することを試みるが、失敗する (S507A)。移動体装置 A はオフライン状態であるため、移動体装置 B、C にブロック `Blc(Trtn)` を送信できないからである。

【0224】

次に、移動体装置 A は、単独でコンセンサスアルゴリズムを実行する (S508A)。具体的には、移動体装置 A は、返却トランザクションデータ `Trtn` が正当なトランザクションデータであること (つまり正当性) を単独で合意し、ブロック `Blc(Trtn)` の正当性を単独で合意する。図 20 に示す例では、移動体装置 A は、ブロック `Blc(Trtn)` に含まれる返却トランザクションデータ `Trtn` が正当なトランザクションデータであること (つまり正当性) を合意することで、ブロック `Blc(Trtn)` の正当性も合意する。なお、ステップ S506 の処理は、ステップ S508A でコンセンサスアルゴリズムを実行する際に行われてもよい。

【0225】

次に、移動体装置 A は、ステップ S508A で合意済みのブロック `Blc(Trtn)` を台帳 A 内のブロックチェーンに連結する (S509)。これにより、図 15C に示すように、台帳 A のみに、返却トランザクションデータ `Trtn` を含むブロックが格納され、移動体 A の返却完了が記録されることになる。このように、オフライン状態の台帳 A のみで自己完結して移動体 A の返却完了が記録されることを以下ではローカル返却と称する。

【0226】

次に、移動体装置 A は、ブロックチェーンに格納された予約情報をチェックする (S510)。より具体的には、移動体装置 A、B、C はそれぞれ、返却トランザクションデータ `Trtn` が自身の台帳内のブロックチェーンに連結されることで、予約スマートコントラクトを実行させて、ブロックチェーンに格納された予約情報として予約トランザクションデータ `Trsv` があることを確認する。

【0227】

そして、移動体装置 A は、料金算定アルゴリズムを実行する (S511)。

【0228】

[比較例の第 2 例に係る移動体装置 A の通信復帰時の処理]

続いて、図 14 に示すステップ S6A の移動体装置 A の通信復帰時の処理の詳細について説明する。

【0229】

図 21 は、比較例の第 2 例に係る移動体装置 A の通信復帰時に行われるシステムの処理を示すシーケンス図である。

【0230】

10

20

30

40

50

まず、移動体装置 A は、他の移動体装置である移動体装置 B、C と通信可能（オンライン状態）に復帰したとする（S 6 0 1）。移動体装置 A は、移動体 A に搭載されているので、移動体 A の所在位置によってはオフライン状態となったり、オンライン状態になったりし得る。

【0 2 3 1】

すると、移動体装置 A は、他の移動体装置である移動体装置 B、C に、信号を送信する（S 6 0 2）。信号は、移動体装置 A がオンライン状態になったことを通知できるなんらかの信号であればよい。

【0 2 3 2】

次に、移動体装置 A、B、C は、各台帳内のブロックチェーンの異同判定を行う（S 6 0 3）。より具体的には、移動体装置 A は、台帳 A 内のブロックチェーンと他の移動体装置である移動体装置 B、C の台帳 B、C 内のブロックチェーンとの異同を判定する。移動体装置 B、C は、台帳 B、C 内のブロックチェーンと他の移動体装置である移動体装置 A の台帳 A 内のブロックチェーンとの異同を判定する。ここでは、図 1 6 の（a）に示す例のように、台帳 A と、台帳 B、C とのブロックチェーンには異なるブロックが連結されており、台帳 A 内のブロックチェーンと台帳 B、C 内のブロックチェーンとは異なる。このため、図 1 6 の（b）に示す例のように、移動体装置 A、B、C では、台帳 A、B、C において、異なるブロックチェーンを共有し合うのでフォークが発生する。

10

【0 2 3 3】

次に、移動体装置 A、B、C は、側鎖ブロックと主鎖ブロックとに該当するブロックについての情報を送信しあう（S 6 0 4、S 6 0 5）。本比較例では、一定時間オフライン状態であった移動体装置 A の台帳 A のブロックチェーンに連結されたブロックが側鎖ブロックに該当する。移動体装置 B、C の台帳 B、C のブロックチェーンに連結されたブロックは主鎖ブロックに該当することになる。

20

【0 2 3 4】

次に、移動体装置 A、B、C はそれぞれ、ステップ S 6 0 4 で得た側鎖ブロックのトランザクションデータ T p o l をトランザクションプールに格納する（S 6 0 6）。より具体的には、移動体装置 A は、台帳 A のブロックチェーンに連結された側鎖ブロックのトランザクションデータ T p o l のコピーをトランザクションプール a に格納する。移動体装置 B は、側鎖ブロックのトランザクションデータ T p o l をトランザクションプール b に格納し、移動体装置 C は、側鎖ブロックのトランザクションデータ T p o l をトランザクションプール c に格納する。

30

【0 2 3 5】

次に、移動体装置 A、B、C はそれぞれ、台帳 A、B、C のブロックチェーンと同一となるように更新する（S 6 0 7）。より具体的には、移動体装置 A は、台帳 A のブロックチェーンに連結されていた側鎖ブロックを削除し、主鎖ブロックを残すことで、台帳 B、C のブロックチェーンと同一となるように台帳 A のブロックチェーンを更新する。移動体装置 B は、台帳 B のブロックチェーンに連結されていた側鎖ブロックを削除し、主鎖ブロックを残すことで、台帳 A、C のブロックチェーンと同一となるように台帳 B のブロックチェーンを更新する。移動体装置 C は、台帳 C のブロックチェーンに連結されていた側鎖ブロックを削除し、主鎖ブロックを残すことで、台帳 A、B のブロックチェーンと同一となるように台帳 C のブロックチェーンを更新する。

40

【0 2 3 6】

次に、所定時間後のブロック生成タイミングにおいて、移動体装置 A、B、C はそれぞれ、トランザクションプールに格納しているトランザクションデータ T p o l を含むブロック B l c (T p o l) を生成する（S 6 1 4）。

【0 2 3 7】

次に、移動体装置 A、B、C はそれぞれ、他の移動体装置に、ステップ S 6 1 4 で生成したブロック B l c (T p o l) を送信する（S 6 1 5）。

【0 2 3 8】

50

次に、移動体装置 A、B、C は、共同でコンセンサスアルゴリズムを実行する (S 6 1 6)。具体的には、移動体装置 A、B、C はそれぞれ、トランザクションデータ T p o l が正当なトランザクションデータであること (つまり正当性) を合意し、ブロック B l c (T p o l) の正当性を合意する。図 2 1 に示す例では、ブロック B l c (T p o l) に含まれるトランザクションデータ T p o l が正当なトランザクションデータであること (つまり正当性) が合意され、ブロック B l c (T p o l) の正当性も合意される。なお、ステップ S 6 1 4 及びステップ S 6 1 5 の処理は、ステップ S 6 1 6 でコンセンサスアルゴリズムを実行する際に行われてもよい。

【0239】

次に、移動体装置 A、B、C はそれぞれ、ステップ S 6 1 6 で合意済みのブロック B l c (T p o l) を分散台帳内のブロックチェーンに連結する (S 6 1 7)。より具体的には、移動体装置 A は、合意済みのブロック B l c (T p o l) を台帳 A 内のブロックチェーンに連結し、移動体装置 B は、合意済みのブロック B l c (T p o l) を台帳 B 内のブロックチェーンに連結する。移動体装置 C は、合意済みのブロック B l c (T p o l) を台帳 C 内のブロックチェーンに連結する。これにより、図 1 7 の (c) に示すように、予約トランザクションデータ T r s v と貸出トランザクションデータ T r n t と返却トランザクションデータ T r t n とを含むブロックが格納され、移動体 A のローカル予約、ローカル貸出及びローカル返却が記録されることになる。

【0240】

次に、移動体装置 A は、ブロックチェーンに格納された予約情報をチェックする (S 6 2 0)。より具体的には、移動体装置 A、B、C はそれぞれ、返却トランザクションデータ T r t n を含むブロックが自身の台帳内のブロックチェーンに連結されることで、予約スマートコントラクトを実行させて、ブロックチェーンに格納された予約情報として予約トランザクションデータ T r s v があることを確認する。

【0241】

そして、移動体装置 A、B、C はそれぞれ、料金算定アルゴリズムを実行する (S 6 2 1)。なお、ステップ S 6 2 1 の処理は、上述したステップ S 5 1 1 の処理と同じであるので説明を省略する。

【0242】

[比較例に係るブロック連結処理]

続いて、ブロックチェーンに生成したブロックを連結するブロック連結処理の比較例について説明する。

【0243】

図 2 2 は、比較例に係るシステムのブロック連結処理を説明するためのフローチャートである。以下では、代表して移動体装置 A でブロック連結処理が行われる場合について説明する。

【0244】

まず、移動体装置 A は、トランザクションデータを取得または生成した場合 (S 1 0 0 1)、取得または生成したトランザクションデータの検証を行う検証アルゴリズムを実行する (S 1 0 0 2)。

【0245】

次に、移動体装置 A は、ステップ S 1 0 0 2 で実行された検証アルゴリズムにより検証済みのトランザクションデータをトランザクションプールに格納する (S 1 0 0 3)。

【0246】

次に、移動体装置 A は、台帳 A のブロックチェーンにブロックを連結するトリガの有るかを確認する (S 1 0 0 4)。ここでのトリガは、例えば数分間などの一定間隔が経過したことである。

【0247】

ステップ S 1 0 0 4 において、トリガがあったときには (S 1 0 0 4 で Y e s)、移動体装置 A は、他の移動体と通信可能かを確認する (S 1 0 0 5)。なお、ステップ S 1 0

10

20

30

40

50

04において、トリガがないときには(S1004でNo)、ステップS1001から処理を繰り返す。

【0248】

ステップS1005において、移動体装置Aは、他の移動体と通信可能でない場合すなわちオフライン状態である場合(S1005でNo)、移動体装置Aは、単独でコンセンサスアルゴリズムを実行する(S1006)。移動体装置Aは、取得または生成したトランザクションデータを含むブロックチェーンのブロックを生成し、コンセンサスアルゴリズムを実行することで合意形成を行う。なお、移動体装置Aは、取得または生成したトランザクションデータの正当性を検証し、当該トランザクションデータを含むブロックを生成してもよい。

10

【0249】

次に、移動体装置Aは、生成したブロックを、台帳Aのブロックチェーンに連結する(S1007)。

【0250】

一方、ステップS1005において、移動体装置Aは、他の移動体と通信可能である場合(S1005でYes)、移動体装置Aは、他の移動体と共同でコンセンサスアルゴリズムを実行する(S1008)。移動体装置A及び他の移動体のそれぞれは、当該トランザクションデータを含むブロックチェーンのブロックを生成し、コンセンサスアルゴリズムを実行することで生成したブロックに対する合意形成を行う。

【0251】

次に、移動体装置Aは、台帳Aのブロックチェーンと他の移動体の台帳内のブロックチェーンとが同じか否かを判定する(S1009)。

20

【0252】

ステップS1009において、同じ場合には(S1009でYes)、移動体装置Aは、台帳Aのブロックチェーンに合意済のブロックを連結する(S1010)。

【0253】

一方、ステップS1009において、同じでない場合には(S1009でNo)、側鎖となる方のブロックすなわち側鎖ブロックの当該トランザクションデータをトランザクションプールに格納する(S1011)。

【0254】

次に、移動体装置Aは、他の移動体の台帳内のブロックチェーンと同じになるように台帳Aのブロックチェーンを更新する(S1012)。

30

【0255】

次に、移動体装置Aは、ステップS1009で合意済のブロックを台帳Aのブロックチェーンに連結する(S1013)。

【0256】

[比較例の第3例]

続いて、ブロックチェーンの仕組みを悪用して移動体Aを不正利用する不正処理について説明する。比較例の第3例では、移動体装置Aがオフライン状態である場合に、移動体Aに対して不正な予約処理と正常な貸出処理を行い、その後、移動体装置Aをオンライン状態に復帰させて返却処理を行う場合について説明する。

40

【0257】

図23は、比較例の第3例に係るシステムの不正処理の動作概要を示すフローチャートである。図24A～図27は、移動体装置Aの台帳A及び移動体装置Bの台帳Bに格納されるブロックチェーンを概念的に説明するための図である。図24Aは、図23のステップS10の動作により台帳Aに格納されるブロックチェーンのブロックを概念的に示す図である。図24Bは、図23のステップS11の動作により台帳Aに格納されるブロックチェーンのブロックを概念的に示す図である。図24Cは、図23のステップS12の動作により台帳Aに格納されるブロックチェーンのブロックを概念的に示す図である。図25及び図26は、図23のステップS13の動作により台帳A及び台帳Bに格納されるブ

50

ロックチェーンのブロックを概念的に説明するための図である。図 2 7 は、図 2 3 のステップ S 1 4 の動作により台帳 A 及び台帳 B に格納されるブロックチェーンのブロックを概念的に示す図である。以下では、移動体 A を利用したいユーザが端末 A を用いて、移動体 A に搭載されている移動体装置 A に対して不正処理を行うとして説明する。

【 0 2 5 8 】

図 2 3 に示すように、まず、例えば端末 A は、オフライン状態の移動体装置 A に対して、当該移動体装置 A が搭載されている移動体 A の予約処理を行う (S 1 0)。ここでは、上述したように、端末 A は、オフライン状態の移動体装置 A に対して移動体 A をローカル予約する予約処理を行う。より具体的には、端末 A は、移動体装置 A と通信し、移動体 A を利用予約するための予約トランザクションデータ $T r s v A$ を生成して、移動体装置 A 10 に送信することができる。この場合、例えば、図 2 4 A に示すように、移動体装置 A はオフライン状態であるので、台帳 A のみに、移動体 A を利用予約するための予約トランザクションデータ $T r s v A$ を含むブロックが格納される。

【 0 2 5 9 】

次に、端末 A を用いたりユーザ個人のスマートフォンを用いたりなどなんらかの手段により、オンライン状態の移動体装置 B に対して、ステップ S 1 0 で行った移動体 A のローカル予約の時間帯が被るように移動体 A の予約処理を行う (S 1 1)。つまり、オンライン状態の移動体装置 B に対して移動体 A のローカル予約と競合するように移動体 A の競合予約処理を行う。本比較例では、ユーザは、端末 A を用いて、移動体 A を競合予約するための予約トランザクションデータ $T r s v B$ を生成して、オンライン状態の移動体装置 B 20 に対して送信する。この場合、例えば、図 2 4 B に示すように、移動体装置 B 等は、オフラインである移動体装置 A の台帳 A を除く台帳 B 等に、移動体 A を競合予約するための予約トランザクションデータ $T r s v B$ を含むブロックが格納される。

【 0 2 6 0 】

次に、例えば端末 A は、オフライン状態の移動体装置 A と通信し、移動体 A の貸出処理を行う (S 1 2)。つまり、上述したが、端末 A は、オフライン状態の移動体装置 A に対して移動体 A をローカル貸出する貸出処理を行う。より具体的には、端末 A は、移動体装置 A と通信し、移動体 A を利用するため移動体 A の解錠要求を送信することで、移動体装置 A に、移動体 A を解錠させ、移動体 A が解錠されたことをトリガに移動体 A の貸出開始を示す貸出トランザクションデータ $T r n t A$ を生成させる。この場合、例えば、図 2 4 30 C に示すように、移動体装置 A はオフライン状態であるので、台帳 A のみに、移動体 A の貸出開始を示す貸出トランザクションデータ $T r n t A$ を含むブロックが格納される。

【 0 2 6 1 】

次に、ユーザは移動体装置 A をオンライン状態に復帰させるとする。すると、移動体装置 A がオンライン状態に復帰した時に、システムにおいて復帰時処理が行われる (S 1 3)。

【 0 2 6 2 】

より具体的には、ステップ S 1 0 ~ ステップ S 1 2 では、上述したように、移動体装置 A がオフライン状態であるため、図 2 5 の (a) に示すように、移動体装置 A がオンライン状態に復帰した時点では、台帳 A 及び台帳 B のブロックチェーンには、異なるブロック 40 が連結されている。次いで、移動体装置 A がオンライン状態に復帰すると、図 2 5 の (b) に示すように、移動体装置 A の台帳 A 及び移動体装置 B の台帳 B には、異なるブロックチェーンを共有し合うことになりフォークが発生する。ここで、オフライン状態の移動体装置 A の台帳 A のブロックチェーンに連結されたブロックが側鎖ブロックに該当し、オンライン状態の移動体装置 B の台帳 B のブロックチェーンに連結されたブロックが主鎖ブロックに該当する。このため、図 2 6 の (a) 及び (b) に示すように、移動体装置 A の台帳 A 及び移動体装置 B の台帳 B では、側鎖ブロックが削除され、側鎖ブロックに含まれるトランザクションデータがトランザクションプールに保存されることで、フォークが解消される。なお、図 2 6 の (b) では、予約トランザクションデータ $T r s v A$ と貸出トランザクションデータ $T r n t A$ とがトランザクションプールに保存されている。その後、 50

図 26 の (c) に示すように、移動体装置 A の台帳 A 及び移動体装置 B の台帳 B のブロックチェーンでは、新たなブロックを生成するタイミングで、トランザクションプールに保存されたトランザクションデータを含むブロックが生成されて連結される。

【 0 2 6 3 】

次に、例えば端末 A は、オンライン状態の移動体装置 A と通信し、移動体 A の返却処理を行う (S 1 4)。より具体的には、端末 A を操作したユーザは、解錠された移動体 A を、利用予約した時間利用して、その後返却する。移動体装置 A は、移動体 A が返却されると、移動体 A の返却完了を示す返却トランザクションデータ $T r t n A$ を生成する。この場合、例えば、図 27 に示すように、移動体装置 A はオンライン状態であるので、台帳 A、B 等のすべてに、移動体 A の返却完了を示す返却トランザクションデータ $T r t n A$ を含むブロックが格納される。

10

【 0 2 6 4 】

次に、移動体装置 A などでは、料金算定処理を行う (S 1 5)。ステップ S 1 5 の料金算定処理は、ステップ S 7 の料金算定処理と同じ処理であるので説明を省略する。予約トランザクションデータ $T r s v A$ と予約トランザクションデータ $T r s v B$ とが競合しており、予約トランザクションデータ $T r s v A$ を含むブロックの方が、予約トランザクションデータ $T r s v B$ を含むブロックよりも時間的に後となる後ろに連結される。この結果、予約トランザクションデータ $T r s v A$ に対応する予約に対しての料金は徴収されないので、予約トランザクションデータ $T r s v A$ に対応する予約において移動体 A を利用した料金を払わないという不正が成立してしまう。

20

【 0 2 6 5 】

続いて、図 23 に示すステップ S 10 のローカル予約の処理、ステップ S 11 の競合予約の処理、及びステップ S 12 のローカル貸出の処理の詳細についてシーケンス図を用いて説明する。

【 0 2 6 6 】

[比較例の第 3 例に係る予約処理]

図 28 は、比較例の第 3 例に係るシステムのローカル予約を行う場合の処理を示すシーケンス図である。図 18 と同様の要素には同様の符号を付しており、詳細な説明は省略する。

【 0 2 6 7 】

まず、端末 A は、移動体 A を利用したいユーザの操作に基づいて、移動体 A を利用予約するための予約トランザクションデータ $T r s v A$ を生成し (S 101B)、生成した予約トランザクションデータ $T r s v A$ を移動体装置 A に送信する (S 102B)。

30

【 0 2 6 8 】

次に、移動体装置 A は、ステップ S 102B で送信された予約トランザクションデータ $T r s v A$ を受信すると、他の移動体装置である移動体装置 B、C に予約トランザクションデータ $T r s v A$ を転送することを試みるが、失敗する (S 103B)。移動体装置 A はオフライン状態であるため、移動体装置 B、C に予約トランザクションデータ $T r s v A$ を転送できないからである。

【 0 2 6 9 】

次に、移動体装置 A は、取得した予約トランザクションデータ $T r s v A$ の正当性を含む検証を行う検証アルゴリズムを実行する (S 104B)。

40

【 0 2 7 0 】

次に、移動体装置 A は、ステップ S 104B で実行された検証アルゴリズムにより検証済みの予約トランザクションデータ $T r s v A$ をトランザクションプール a に格納する (S 105B)。

【 0 2 7 1 】

次に、移動体装置 A は、検証済みの予約トランザクションデータ $T r s v A$ を含むブロック $B 1 c (T r s v A)$ を生成する (S 107B)。

【 0 2 7 2 】

50

次に、移動体装置 A は、他の移動体装置である移動体装置 B、C に、ステップ S 1 0 7 B で生成したブロック B 1 c (T r s v A) を送信することを試みるが、失敗する (S 1 0 8 B)。移動体装置 A はオフライン状態であるため、移動体装置 B、C にブロック B 1 c (T r s v A) を送信できないからである。

【 0 2 7 3 】

次に、移動体装置 A は、単独でコンセンサスアルゴリズムを実行する (S 1 0 9 B)。なお、ステップ S 1 0 7 B の処理は、ステップ S 1 0 9 B で単独でコンセンサスアルゴリズムを実行する際に行われてもよい。

【 0 2 7 4 】

次に、移動体装置 A は、ステップ S 1 0 9 B で合意済みのブロック B 1 c (T r s v A) を台帳 A 内のブロックチェーンに連結する (S 1 1 0 B)。

10

【 0 2 7 5 】

これにより、図 2 4 A に示すように、台帳 A のみに、移動体 A を利用予約するための予約トランザクションデータ T r s v A を含むブロックが格納され、ローカル予約が確定されることになる。

【 0 2 7 6 】

図 2 9 は、比較例の第 3 例に係るシステムの競合予約を行う場合の処理を示すシーケンス図である。

【 0 2 7 7 】

まず、ユーザは例えば端末 A を用いて、移動体 A を競合予約するための予約トランザクションデータ T r s v B を生成する (S 1 0 1 C)。

20

【 0 2 7 8 】

次に、ユーザは例えば端末 A を用いて、移動体装置 B に対して、ステップ S 1 0 1 C で生成した予約トランザクションデータ T r s v B を送信する (S 1 0 2 C)。

【 0 2 7 9 】

次に、移動体装置 B は、オンライン状態であるので、ステップ S 1 0 2 C で送信された予約トランザクションデータ T r s v B を受信すると、他の移動体装置である移動体装置 C に予約トランザクションデータ T r s v B を転送する (S 1 0 3 C)。これにより、移動体装置 A を除く移動体装置 C は、予約トランザクションデータ T r s v B を取得する。

【 0 2 8 0 】

30

次に、移動体装置 B、C はそれぞれ、取得した予約トランザクションデータ T r s v B の正当性を含む検証を行う検証アルゴリズムを実行する (S 1 0 4 C)。

【 0 2 8 1 】

次に、移動体装置 B、C はそれぞれ、ステップ S 1 0 4 C で実行された検証アルゴリズムにより検証済みの予約トランザクションデータ T r s v B をトランザクションプールに格納する (S 1 0 5 C)。より具体的には、移動体装置 B は、検証済みの予約トランザクションデータ T r s v B をトランザクションプール b に格納し、移動体装置 C は、検証済みの予約トランザクションデータ T r s v B をトランザクションプール c に格納する。

【 0 2 8 2 】

次に、移動体装置 B、C は互いに、通信可能な状態であるので、次に生成するブロックに格納すべきトランザクションデータの情報をやりとりする (S 1 0 6 C)。図 2 9 に示す例では、移動体装置 B、C は、次に生成するブロックに格納すべきトランザクションデータに、検証済みの予約トランザクションデータ T r s v B があることを確認する。

40

【 0 2 8 3 】

次に、移動体装置 B、C はそれぞれ、検証済みの予約トランザクションデータ T r s v B を含むブロック B 1 c (T r s v B) を生成する (S 1 0 7 C)。

【 0 2 8 4 】

次に、移動体装置 B、C はそれぞれ、移動体装置 A を除く他の移動体装置に、ステップ S 1 0 7 C で生成したブロック B 1 c (T r s v B) を送信する (S 1 0 8 C)。これにより、移動体装置 B、C はそれぞれ、移動体装置 A を除く他の移動体装置に、ブロック B

50

1 c (T r s v B) に含まれる予約トランザクションデータ T r s v B の正当性の検証が成功したことの報告を通知することができる。

【 0 2 8 5 】

次に、移動体装置 B、C は、共同でコンセンサスアルゴリズムを実行する (S 1 0 9 C)。具体的には、移動体装置 B、C はそれぞれ、ステップ S 1 0 8 C で通知された報告に基づき、予約トランザクションデータ T r s v B が正当なトランザクションデータであること (つまり正当性) を合意し、ブロック B 1 c (T r s v B) の正当性を合意する。なお、ステップ S 1 0 7 C 及びステップ S 1 0 8 C の処理は、ステップ S 1 0 9 C でコンセンサスアルゴリズムを実行する際に行われてもよい。

【 0 2 8 6 】

次に、移動体装置 B、C はそれぞれ、ステップ S 1 0 9 C で合意済みのブロック B 1 c (T r s v B) を分散台帳内のブロックチェーンに連結する (S 1 1 0 C)。より具体的には、移動体装置 B は、合意済みのブロック B 1 c (T r s v B) を台帳 B 内のブロックチェーンに連結し、移動体装置 C は、合意済みのブロック B 1 c (T r s v B) を台帳 C 内のブロックチェーンに連結する。

【 0 2 8 7 】

これにより、図 2 4 B に示すように、台帳 B 及び台帳 C には共に、予約トランザクションデータ T r s v B を含むブロックが格納される。

【 0 2 8 8 】

[比較例の第 3 例に係る貸出処理]

図 3 0 は、比較例の第 3 例に係るシステムのローカル貸出の処理を示すシーケンス図である。図 1 9 と同様の要素には同様の符号を付しており、詳細な説明は省略する。

【 0 2 8 9 】

まず、端末 A は、移動体 A を利用するユーザの操作に基づいて、移動体 A の解錠要求を移動体装置 A に送信する (S 3 0 1 B)。

【 0 2 9 0 】

次に、移動体装置 A は、ステップ S 3 0 1 B で送信された解錠要求を受信すると、台帳 A のブロックチェーンに解錠要求に対応する予約があるかを確認し (S 3 0 2 B)、移動体 A のロックを解除する (S 3 0 3 B)。

【 0 2 9 1 】

次に、移動体装置 A は、移動体 A のロックが解除されたことをトリガに、移動体 A の貸出開始を示す貸出トランザクションデータ T r n t A を生成する (S 3 0 4 B)。

【 0 2 9 2 】

次に、移動体装置 A は、他の移動体装置である移動体装置 B、C に貸出トランザクションデータ T r n t A を転送することを試みるが、失敗する (S 3 0 5 B)。移動体装置 A はオフライン状態であるため、移動体装置 B、C に貸出トランザクションデータ T r n t A を転送できないからである。

【 0 2 9 3 】

次に、移動体装置 A は、貸出トランザクションデータ T r n t A の正当性を含む検証を行う検証アルゴリズムを実行する (S 3 0 6 B)。

【 0 2 9 4 】

次に、移動体装置 A は、ステップ S 3 0 6 B で実行された検証アルゴリズムにより検証済みの貸出トランザクションデータ T r n t A をトランザクションプール a に格納する (S 3 0 7 B)。

【 0 2 9 5 】

次に、移動体装置 A はそれぞれ、検証済みの貸出トランザクションデータ T r n t A を含むブロック B 1 c (T r n t A) を生成する (S 3 0 9 B)。

【 0 2 9 6 】

次に、移動体装置 A は、他の移動体装置である移動体装置 B、C に、ステップ S 3 0 9 B で生成したブロック B 1 c (T r n t A) を送信することを試みるが、失敗する (S 3

10

20

30

40

50

10 B)。移動体装置 A はオフライン状態であるため、移動体装置 B、C にブロック B l c (T r n t A) を送信できないからである。

【0297】

次に、移動体装置 A は、単独でコンセンサスアルゴリズムを実行する (S 3 1 1 B)。具体的には、移動体装置 A は、貸出トランザクションデータ T r n t A が正当なトランザクションデータであること (つまり正当性) を単独で合意し、ブロック B l c (T r n t A) の正当性を単独で合意する。なお、ステップ S 3 0 9 B の処理は、ステップ S 3 1 1 B でコンセンサスアルゴリズムを実行する際に行われてもよい。

【0298】

次に、移動体装置 A は、ステップ S 3 1 1 B で合意済みのブロック B l c (T r n t A) を台帳 A 内のブロックチェーンに連結する (S 3 1 2 B)。 10

【0299】

これにより、図 2 4 C に示すように、台帳 A のみに、貸出トランザクションデータ T r n t A を含むブロックが格納され、移動体 A のローカル貸出が行われたことが記録される。

【0300】

[比較例の第 3 例に係る移動体装置 A の通信復帰時の処理]

続いて、図 2 3 に示すステップ S 1 3 の移動体装置 A の通信復帰時の処理の詳細について説明する。

【0301】

図 3 1 は、比較例の第 3 例に係る移動体装置 A の通信復帰時に行われるシステムの処理を示すシーケンス図である。図 2 1 と同様の要素には同様の符号を付しており、詳細な説明は省略する。 20

【0302】

まず、移動体装置 A は、他の移動体装置である移動体装置 B、C と通信可能 (オンライン状態) に復帰したとする (S 6 0 1 B)。

【0303】

すると、移動体装置 A は、他の移動体装置である移動体装置 B、C に、移動体装置 A がオンライン状態になったことを示す信号を送信する (S 6 0 2 B)。

【0304】

次に、移動体装置 A、B、C は、各台帳内のブロックチェーンの異同判定を行う (S 6 0 3 B)。より具体的には、移動体装置 A は、台帳 A 内のブロックチェーンと他の移動体装置である移動体装置 B、C の台帳 B、C 内のブロックチェーンとの異同を判定する。移動体装置 B、C は、台帳 B、C 内のブロックチェーンと他の移動体装置である移動体装置 A の台帳 A 内のブロックチェーンとの異同を判定する。ここでは、図 2 5 の (a) に示す例のように、台帳 A と、台帳 B、C とのブロックチェーンには異なるブロックが連結されており、台帳 A 内のブロックチェーンと台帳 B、C 内のブロックチェーンとは異なる。このため、図 2 5 の (b) に示す例のように、移動体装置 A、B、C では、台帳 A、B、C において、異なるブロックチェーンを共有し合うのでフォークが発生する。 30

【0305】

次に、移動体装置 A、B、C は、側鎖ブロックと主鎖ブロックとに該当するブロックについての情報を送信しあう (S 6 0 4 B、S 6 0 5 B)。本比較例では、一定時間オフライン状態であった移動体装置 A の台帳 A のブロックチェーンに連結されたブロックが側鎖ブロック B l c (T r s v A、T r n t A) に該当する。移動体装置 B、C の台帳 B、C のブロックチェーンに連結されたブロックは主鎖ブロック B l c (T r s v B) に該当する。 40

【0306】

次に、移動体装置 A、B、C はそれぞれ、ステップ S 6 0 4 B で得た側鎖ブロックに含まれる予約トランザクションデータ T r s v A、貸出トランザクションデータ T r n t A を、トランザクションプールに格納する (S 6 0 6 B)。より具体的には、移動体装置 A は、台帳 A のブロックチェーンに連結された側鎖ブロックのトランザクションデータ T r 50

s v A、T r n t Aのコピーをトランザクションプール a に格納する。移動体装置 B は、側鎖ブロックのトランザクションデータ T r s v A、T r n t A をトランザクションプール b に格納し、移動体装置 C は、側鎖ブロックのトランザクションデータ T r s v A、T r n t A をトランザクションプール c に格納する。

【0307】

次に、移動体装置 A、B、C はそれぞれ、台帳 A、B、C のブロックチェーンと同一となるように更新する (S 6 0 7 B)。より具体的には、移動体装置 A は、台帳 A のブロックチェーンに連結されていた側鎖ブロックを削除し、主鎖ブロックを残すことで、台帳 B、C のブロックチェーンと同一となるように台帳 A のブロックチェーンを更新する。移動体装置 B は、台帳 B のブロックチェーンに連結されていた側鎖ブロックを削除し、主鎖ブロックを残すことで、台帳 A、C のブロックチェーンと同一となるように台帳 B のブロックチェーンを更新する。移動体装置 C は、台帳 C のブロックチェーンに連結されていた側鎖ブロックを削除し、主鎖ブロックを残すことで、台帳 A、B のブロックチェーンと同一となるように台帳 C のブロックチェーンを更新する。

10

【0308】

次に、所定時間後のブロック生成タイミングにおいて、移動体装置 A、B、C はそれぞれ、トランザクションプールに格納しているトランザクションデータ T r s v A、T r n t A を含むブロック B l c (T r s v A、T r n t A) を生成する (S 6 1 4 B)。

【0309】

次に、移動体装置 A、B、C はそれぞれ、他の移動体装置に、ステップ S 6 1 4 B で生成したブロック B l c (T r s v A、T r n t A) を送信する (S 6 1 5 B)。これにより、移動体装置 A、B、C はそれぞれ、他の移動体装置に、ブロック B l c (T r s v A、T r n t A) に含まれるトランザクションデータ T r s v A、T r n t A の正当性の検証が成功したことの報告を通知することができる。

20

【0310】

次に、移動体装置 A、B、C は、共同でコンセンサスアルゴリズムを実行する (S 6 1 6 B)。具体的には、移動体装置 A、B、C はそれぞれ、ステップ S 6 1 5 B で通知された報告に基づき、トランザクションデータ T r s v A、T r n t A が正当なトランザクションデータであること (つまり正当性) を合意し、ブロック B l c (T r s v A、T r n t A) の正当性を合意する。なお、ステップ S 6 1 4 B 及びステップ S 6 1 5 B の処理は、ステップ S 6 1 6 B でコンセンサスアルゴリズムを実行する際に行われてもよい。

30

【0311】

次に、移動体装置 A、B、C はそれぞれ、ステップ S 6 1 6 B で合意済みのブロック B l c (T r s v A、T r n t A) を分散台帳内のブロックチェーンに連結する (S 6 1 7 B)。より具体的には、移動体装置 A は、合意済みのブロック B l c (T r s v A、T r n t A) を台帳 A 内のブロックチェーンに連結し、移動体装置 B は、合意済みのブロック B l c (T r s v A、T r n t A) を台帳 B 内のブロックチェーンに連結する。移動体装置 C は、合意済みのブロック B l c (T r s v A、T r n t A) を台帳 C 内のブロックチェーンに連結する。これにより、図 2 6 の (c) に示すように、予約トランザクションデータ T r s v A と予約トランザクションデータ T r s v B と貸出トランザクションデータ T r n t A とを含むブロックが格納され、移動体 A のローカル予約、競合予約及びローカル貸出が記録されることになる。

40

【0312】

[比較例の第 3 例に係る返却処理]

続いて、図 2 3 に示すステップ S 1 4 の移動体装置 A の返却処理の詳細について説明する。

【0313】

図 3 2 は、比較例の第 3 例に係るシステムの返却処理を示すシーケンス図である。図 1 2 と同様の要素には同様の符号を付しており、詳細な説明は省略する。

【0314】

50

まず、移動体 A を利用したユーザにより移動体 A が返却されると、移動体装置 A は、移動体 A が返却されたことを確認する (S 5 0 1 B)。

【 0 3 1 5 】

次に、移動体装置 A は、移動体 A が返却されたことを確認したことをトリガに、移動体 A の返却完了を示す返却トランザクションデータ $T r t n A$ を生成する (S 5 0 2 B)。

【 0 3 1 6 】

次に、移動体装置 A は、他の移動体装置である移動体装置 B、C に返却トランザクションデータ $T r t n A$ を転送する (S 5 0 3 B)。これにより、移動体装置 B、C は、返却トランザクションデータ $T r t n A$ を取得する。

【 0 3 1 7 】

次に、移動体装置 A、B、C はそれぞれ、取得した返却トランザクションデータ $T r t n A$ の正当性を含む検証を行う検証アルゴリズムを実行する (S 5 0 4 B)。

【 0 3 1 8 】

次に、移動体装置 A、B、C はそれぞれ、ステップ S 5 0 4 B で実行された検証アルゴリズムにより検証済みの返却トランザクションデータ $T r t n A$ をトランザクションプールに格納する (S 5 0 5 B)。より具体的には、移動体装置 A は、検証済みの返却トランザクションデータ $T r t n A$ をトランザクションプール a に格納し、移動体装置 B は、検証済みの返却トランザクションデータ $T r t n A$ をトランザクションプール b に格納する。移動体装置 C は、検証済みの返却トランザクションデータ $T r t n A$ をトランザクションプール c に格納する。なお、図示していないが、移動体装置 A、B、C は互いに、通信可能な状態であるので、次に生成するブロックに格納すべきトランザクションデータの情報をやりとりする。図 3 2 に示す例では、移動体装置 A、B、C は、次に生成するブロックに格納すべきトランザクションデータに、検証済みの返却トランザクションデータ $T r t n A$ があることを確認する。

【 0 3 1 9 】

次に、移動体装置 A、B、C はそれぞれ、検証済みの返却トランザクションデータ $T r t n A$ を含むブロック $B l c (T r t n A)$ を生成する (S 5 0 6 B)。

【 0 3 2 0 】

次に、移動体装置 A、B、C はそれぞれ、他の移動体装置に、ステップ S 5 0 6 B で生成したブロック $B l c (T r t n A)$ を送信する (S 5 0 7 B)。これにより、移動体装置 A、B、C はそれぞれ、他の移動体装置に、ブロック $B l c (T r t n A)$ に含まれる返却トランザクションデータ $T r t n A$ の正当性の検証が成功したことの報告を通知することができる。

【 0 3 2 1 】

次に、移動体装置 A、B、C は、共同でコンセンサスアルゴリズムを実行する (S 5 0 8 B)。具体的には、移動体装置 A、B、C はそれぞれ、ステップ S 5 0 7 B で通知された報告に基づき、返却トランザクションデータ $T r t n A$ が正当なトランザクションデータであること (つまり正当性) を合意し、ブロック $B l c (T r t n A)$ の正当性を合意する。なお、ステップ S 5 0 6 B 及びステップ S 5 0 7 B の処理は、ステップ S 5 0 8 B でコンセンサスアルゴリズムを実行する際に行われてもよい。

【 0 3 2 2 】

次に、移動体装置 A、B、C はそれぞれ、ステップ S 5 0 8 B で合意済みのブロック $B l c (T r t n A)$ を分散台帳内のブロックチェーンに連結する (S 5 0 9 B)。より具体的には、移動体装置 A は、合意済みのブロック $B l c (T r t n A)$ を台帳 A 内のブロックチェーンに連結し、移動体装置 B は、合意済みのブロック $B l c (T r t n A)$ を台帳 B 内のブロックチェーンに連結する。移動体装置 C は、合意済みのブロック $B l c (T r t n A)$ を台帳 C 内のブロックチェーンに連結する。これにより、図 2 7 に示すように、台帳 A、台帳 B 及び台帳 C には共に、返却トランザクションデータ $T r t n A$ を含むブロックが格納され、移動体 A の返却完了が記録されることになる。

【 0 3 2 3 】

10

20

30

40

50

次に、移動体装置 A、B、C はそれぞれ、ブロックチェーンに格納された予約情報をチェックする (S 5 1 0 B)。より具体的には、移動体装置 A、B、C はそれぞれ、返却トランザクションデータ $T r t n A$ を含むブロックを含むブロックが自身の台帳内のブロックチェーンに連結されることで、予約スマートコントラクトを実行させて、ブロックチェーンに格納された予約情報として予約トランザクションデータ $T r s v$ があることを確認する。

【 0 3 2 4 】

次に、移動体装置 A、B、C はそれぞれ、料金算定アルゴリズムを実行する (S 5 1 1 B)。ここでは、例えば図 2 7 に示すように、予約トランザクションデータ $T r s v A$ と予約トランザクションデータ $T r s v B$ とが競合しており、予約トランザクションデータ $T r s v A$ を含むブロックの方が、予約トランザクションデータ $T r s v B$ を含むブロックよりも時間的に後となる後ろに連結されている。このため、料金算定アルゴリズムを実行されても、予約トランザクションデータ $T r s v A$ に対応する予約に対しての料金は徴収されず、予約トランザクションデータ $T r s v B$ に対応する予約に対しての料金のみが徴収されることになる。

10

【 0 3 2 5 】

このように、予約トランザクションデータ $T r s v A$ に対応する予約に対しての料金は徴収されないので、予約トランザクションデータ $T r s v A$ に対応する予約において移動体 A を利用した料金を払わないという不正が成立する。

【 0 3 2 6 】

[比較例の第 4 例]

比較例の第 3 例では、移動体装置 A をオンライン状態に復帰させてから返却処理を行う場合の不正処理について説明したが、これに限らない。移動体装置 A がオフライン状態である場合に、返却処理を行った後に移動体装置 A をオンライン状態に復帰させてもよい。この場合の不正処理を比較例の第 4 例として以下説明する。

20

【 0 3 2 7 】

図 3 3 は、比較例の第 4 例に係るシステムの不正処理の動作概要を示すフローチャートである。図 3 4 A ~ 図 3 6 は、移動体装置 A の台帳 A 及び移動体装置 B の台帳 B に格納されるブロックチェーンを概念的に説明するための図である。図 3 4 A は、図 3 3 のステップ S 1 0 の動作により台帳 A に格納されるブロックチェーンのブロックを概念的に示す図である。図 3 4 B は、図 3 3 のステップ S 1 1 の動作により台帳 A に格納されるブロックチェーンのブロックを概念的に示す図である。図 3 4 C は、図 3 3 のステップ S 1 2 の動作により台帳 A に格納されるブロックチェーンのブロックを概念的に示す図である。図 3 4 D は、図 3 3 のステップ S 1 3 A の動作により台帳 A に格納されるブロックチェーンのブロックを概念的に示す図である。図 3 5 及び図 3 6 は、図 3 3 のステップ S 1 4 A の動作により台帳 A 及び台帳 B に格納されるブロックチェーンのブロックを概念的に説明するための図である。以下でも、移動体 A を利用したいユーザが端末 A を用いて、移動体 A に搭載されている移動体装置 A に対して不正処理を行うとして説明する。

30

【 0 3 2 8 】

図 3 3 に示すステップ S 1 0 ~ ステップ S 1 2 は、図 2 3 で説明したステップ S 1 0 ~ ステップ S 1 2 と同じ処理であるので説明を省略する。また、図 3 4 A ~ 図 3 4 C は、図 2 4 A ~ 図 2 4 C と同一の図であるので説明を省略する。

40

【 0 3 2 9 】

次に、ステップ S 1 3 A において、例えば端末 A は、オフライン状態の移動体装置 A と通信し、移動体 A の返却処理を行う。つまり、端末 A は、オフライン状態の移動体装置 A に対して移動体 A をローカル返却する返却処理を行う。より具体的には、端末 A を操作したユーザは、解錠された移動体 A を、利用予約した時間利用して、その後返却する。移動体装置 A は、移動体 A が返却されると、移動体 A の返却完了を示す返却トランザクションデータ $T r t n A$ を生成する。この場合、例えば、図 3 4 D に示すように、移動体装置 A はオフライン状態であるので、台帳 A のみに、移動体 A の返却完了を示す返却トランザク

50

ションデータ $T r t n A$ を含むブロックが格納される。

【0330】

次に、ユーザは移動体装置 A をオンライン状態に復帰させるとする。すると、移動体装置 A がオンライン状態に復帰した時に、システムにおいて復帰時処理が行われる (S 1 4 A)。より具体的には、ステップ S 1 0 ~ ステップ S 1 3 A では、移動体装置 A がオフライン状態であるため、移動体装置 A がオンライン状態に復帰した時点では、例えば図 3 4 D に示すように、台帳 A 及び台帳 B のブロックチェーンには、異なるブロックが連結されている。次いで、移動体装置 A がオンライン状態に復帰すると、図 3 5 に示すように、移動体装置 A の台帳 A 及び移動体装置 B の台帳 B には、異なるブロックチェーンを共有し合うことになりフォークが発生する。ここで、オフライン状態の移動体装置 A の台帳 A のブロックチェーンに連結されたブロックの方が短いため側鎖ブロックに該当し、オンライン状態の移動体装置 B の台帳 B のブロックチェーンに連結されたブロックが長いので主鎖ブロックに該当する。このため、図 3 6 の (a) 及び (b) に示すように、移動体装置 A の台帳 A 及び移動体装置 B の台帳 B では、側鎖ブロックが削除され、側鎖ブロックに含まれるトランザクションデータがトランザクションプールに保存されることで、フォークが解消される。なお、図 3 6 の (b) では、予約トランザクションデータ $T r s v A$ と貸出トランザクションデータ $T r n t A$ と返却トランザクションデータ $T r t n A$ とがトランザクションプールに保存されている。その後、図 3 6 の (c) に示すように、移動体装置 A の台帳 A 及び移動体装置 B の台帳 B のブロックチェーンでは、新たなブロックを生成するタイミングで、トランザクションプールに保存されたトランザクションデータを含むブロックが生成されて連結される。

10

20

【0331】

次に、移動体装置 A などでは、料金算定処理を行う (S 1 5)。比較例の第 3 例と同様、予約トランザクションデータ $T r s v A$ と予約トランザクションデータ $T r s v B$ とが競合しており、予約トランザクションデータ $T r s v A$ を含むブロックの方が、予約トランザクションデータ $T r s v B$ を含むブロックよりも後ろに連結される。この結果、予約トランザクションデータ $T r s v A$ に対応する予約に対しての料金は徴収されないので、予約トランザクションデータ $T r s v A$ に対応する予約において移動体 A を利用した料金を払わないという不正が成立する。

【0332】

続いて、図 3 3 に示すステップ S 1 3 A のローカル返却の処理、ステップ S 1 4 A の移動体装置 A の通信復帰時の処理の詳細についてシーケンス図を用いて説明する。

30

【0333】

[比較例の第 4 例に係る返却処理]

図 3 7 は、比較例の第 4 例に係るシステムのローカル返却の処理を示すシーケンス図である。図 2 0 と同様の要素には同様の符号を付しており、詳細な説明は省略する。

【0334】

まず、移動体 A を利用したユーザにより移動体 A が返却されると、移動体装置 A は、移動体 A が返却されたことを確認する (S 5 0 1 C)。

【0335】

次に、移動体装置 A は、移動体 A が返却されたことを確認したことをトリガに、移動体 A の返却完了を示す返却トランザクションデータ $T r t n A$ を生成する (S 5 0 2 C)。

40

【0336】

次に、移動体装置 A は、他の移動体装置である移動体装置 B、C に返却トランザクションデータ $T r t n A$ を転送することを試みるが、失敗する (S 5 0 3 C)。移動体装置 A はオフライン状態であるため、移動体装置 B、C に返却トランザクションデータ $T r t n A$ を転送できないからである。

【0337】

次に、移動体装置 A は、取得した返却トランザクションデータ $T r t n A$ の正当性を含む検証を行う検証アルゴリズムを実行する (S 5 0 4 C)。

50

【0338】

次に、移動体装置Aは、ステップS504Cで実行された検証アルゴリズムにより検証済みの返却トランザクションデータTrtnAをトランザクションプールaに格納する(S505C)。

【0339】

次に、移動体装置Aは、検証済みの返却トランザクションデータTrtnAを含むブロックBlc(TrtnA)を生成する(S506C)。

【0340】

次に、移動体装置Aは、他の移動体装置である移動体装置B、Cに、ステップS506Cで生成したブロックBlc(TrtnA)を送信することを試みるが、失敗する(S507C)。移動体装置Aはオフライン状態であるため、移動体装置B、CにブロックBlc(TrtnA)を送信できないからである。

10

【0341】

次に、移動体装置Aは、単独でコンセンサスアルゴリズムを実行する(S508C)。具体的には、移動体装置Aは、返却トランザクションデータTrtnAが正当なトランザクションデータであること(つまり正当性)を単独で合意し、ブロックBlc(TrtnA)の正当性を単独で合意する。なお、ステップS506Cの処理は、ステップS508Cでコンセンサスアルゴリズムを実行する際に行われてもよい。

【0342】

次に、移動体装置Aは、ステップS508Cで合意済みのブロックBlc(TrtnA)を台帳A内のブロックチェーンに連結する(S509C)。これにより、図34Dに示すように、台帳Aのみに、返却トランザクションデータTrtnAを含むブロックが格納され、移動体Aのローカル返却が記録されることになる。

20

【0343】

次に、移動体装置Aは、ブロックチェーンに格納された予約情報をチェックする(S510C)。より具体的には、移動体装置A、B、Cはそれぞれ、返却トランザクションデータTrtnAが自身の台帳内のブロックチェーンに連結されることで、予約スマートコントラクトを実行させて、ブロックチェーンに格納された予約情報として予約トランザクションデータTrsvAがあることを確認する。

【0344】

そして、移動体装置Aはそれぞれ、料金算定アルゴリズムを実行する(S511C)。移動体装置Aはオフライン状態であるので、料金算定アルゴリズムにより、予約トランザクションデータTrsvAに対応する予約に対しての料金が算定されることになる。

30

【0345】

[比較例の第4例に係る移動体装置Aの通信復帰時の処理]

続いて、図33に示すステップS14Aの移動体装置Aの通信復帰時の処理の詳細について説明する。

【0346】

図38は、比較例の第4例に係る移動体装置Aの通信復帰時に行われるシステムの処理を示すシーケンス図である。図21と同様の要素には同様の符号を付しており、詳細な説明は省略する。

40

【0347】

まず、移動体装置Aは、他の移動体装置である移動体装置B、Cと通信可能(オンライン状態)に復帰したとする(S601C)。

【0348】

すると、移動体装置Aは、他の移動体装置である移動体装置B、Cに、移動体装置Aがオンライン状態になったことを示す信号を送信する(S602C)。

【0349】

次に、移動体装置A、B、Cは、各台帳内のブロックチェーンの異同判定を行う(S603C)。移動体装置Aの通信復帰の前では、例えば図34Dに示す例のように、台帳A

50

と、台帳B、Cとのブロックチェーンには異なるブロックが連結されているので、台帳A内のブロックチェーンと台帳B、C内のブロックチェーンとは異なる。このため、移動体装置Aの通信復帰時には、例えば図35に示す例のように、移動体装置A、B、Cの台帳A、B、Cでは、異なるブロックチェーンを共有し合うのでフォークが発生する。

【0350】

次に、移動体装置A、B、Cは、側鎖ブロックと主鎖ブロックとに該当するブロックについての情報を送信しあう(S604C、S605C)。本比較例では、一定時間オフライン状態であった移動体装置Aの台帳Aのブロックチェーンに連結されたブロックは側鎖ブロックBlc(TrsvA、TrntA、TrtnA)に該当する。一方、移動体装置B、Cの台帳B、Cのブロックチェーンに連結されたブロックは主鎖ブロックBlc(TrsvB)に該当することになる。

10

【0351】

次に、移動体装置A、B、Cはそれぞれ、ステップS604Cで得た側鎖ブロックのトランザクションデータTrsvA、TrntA、TrtnAをトランザクションプールに格納する(S606C)。

【0352】

次に、移動体装置A、B、Cはそれぞれ、台帳A、B、Cのブロックチェーンと同一となるように更新する(S607C)。より具体的には、移動体装置A、B、Cはそれぞれ、ブロックチェーンに連結されていた側鎖ブロックを削除し、主鎖ブロックを残すことで、台帳A、B、Cのブロックチェーンが同一となるように台帳Aのブロックチェーンを更新する。

20

【0353】

次に、所定時間後のブロック生成タイミングにおいて、移動体装置A、B、Cはそれぞれ、トランザクションプールに格納しているトランザクションデータTrsvA、TrntA、TrtnAを含むブロックBlc(TrsvA、TrntA、TrtnA)を生成する(S614C)。

【0354】

次に、移動体装置A、B、Cはそれぞれ、他の移動体装置に、ステップS614Cで生成したブロックBlc(TrsvA、TrntA、TrtnA)を送信する(S615C)。これにより、移動体装置A、B、Cはそれぞれ、他の移動体装置に、ブロックBlc(TrsvA、TrntA、TrtnA)に含まれるトランザクションデータTrsvA、TrntA、TrtnAの正当性の検証が成功したことの報告を通知することができる。

30

【0355】

次に、移動体装置A、B、Cは、共同でコンセンサスアルゴリズムを実行する(S616C)。具体的には、移動体装置A、B、Cはそれぞれ、ステップS615Cで通知された報告に基づき、トランザクションデータTrsvA、TrntA、TrtnAが正当なトランザクションデータであること(つまり正当性)を合意する。そして、ブロックBlc(TrsvA、TrntA、TrtnA)の正当性を合意する。なお、ステップS614C及びステップS615Cの処理は、ステップS616Cでコンセンサスアルゴリズムを実行する際に行われてもよい。

40

【0356】

次に、移動体装置A、B、Cはそれぞれ、ステップS616で合意済みのブロックBlc(TrsvA、TrntA、TrtnA)を分散台帳内のブロックチェーンに連結する(S617C)。より具体的には、移動体装置Aは、合意済みのブロックBlc(TrsvA、TrntA、TrtnA)を台帳A内のブロックチェーンに連結し、移動体装置Bは、合意済みのブロックBlc(TrsvA、TrntA、TrtnA)を台帳B内のブロックチェーンに連結する。移動体装置Cは、合意済みのブロックBlc(TrsvA、TrntA、TrtnA)を台帳C内のブロックチェーンに連結する。これにより、図36の(c)に示すように、予約トランザクションデータTrsvAと貸出トランザクションデータTrntAと返却トランザクションデータTrtnAとを含むブロックが格納さ

50

れ、移動体 A のローカル予約、ローカル貸出及びローカル返却が記録されることになる。

【 0 3 5 7 】

次に、移動体装置 A は、ブロックチェーンに格納された予約情報をチェックする (S 6 2 0 C) 。より具体的には、移動体装置 A 、 B 、 C はそれぞれ、返却トランザクションデータ $T r t n A$ を含むブロックが自身の台帳内のブロックチェーンに連結されることで、予約スマートコントラクトを実行させて、ブロックチェーンに格納された予約情報として予約トランザクションデータ $T r s v A$ と予約トランザクションデータ $T r s v B$ とがあることを確認する。

【 0 3 5 8 】

そして、移動体装置 A 、 B 、 C はそれぞれ、料金算定アルゴリズムを実行しない (S 6 2 1 C) 。より具体的には、移動体装置 A 、 B 、 C はそれぞれ、料金算定アルゴリズムを実行するが、予約トランザクションデータ $T r s v A$ に対応する予約に対しての料金は徴収されない。なお、ステップ S 6 2 1 C の処理は、上述したステップ S 5 1 1 B の処理と同じであるので説明を省略する。

10

【 0 3 5 9 】

ここでは、例えば図 3 6 の (c) に示すように、予約トランザクションデータ $T r s v A$ に対応する予約と予約トランザクションデータ $T r s v B$ とに対応する予約とが競合している。また、予約トランザクションデータ $T r s v A$ を含むブロックの方が、予約トランザクションデータ $T r s v B$ を含むブロックよりも後ろに連結されている。このため、料金算定アルゴリズムを実行されても、予約トランザクションデータ $T r s v A$ に対応する予約に対しての料金は徴収されず、予約トランザクションデータ $T r s v B$ に対応する予約に対しての料金のみが徴収されることになる。

20

【 0 3 6 0 】

このように、予約トランザクションデータ $T r s v A$ に対応する予約に対しての料金は徴収されないので、予約トランザクションデータ $T r s v A$ に対応する予約において移動体 A を利用した料金を払わないという不正が成立する。

【 0 3 6 1 】

[本実施の形態に係る不正対策後の処理]

続いて、不正処理の対策を行った本実施の形態に係る不正対策処理について説明する。

【 0 3 6 2 】

図 2 3 及び図 3 3 に示される不正処理では、ステップ S 1 1 で競合予約が行われることにより、ステップ S 1 0 で予約処理されたローカル予約に対する料金が徴収されなかった。このため、本実施の形態では、ステップ S 1 0 のローカル予約で生成された予約トランザクションデータを含むブロックを台帳に格納させないようにする。ローカル予約で生成された予約トランザクションデータを含むブロックが台帳に格納されなければ、予約が為されないためローカル予約による移動体 A の利用ができない。つまり、サービス対象である移動体 A の不正利用に繋がる処理を抑制することで、ブロックチェーンを悪用したサービス対象の不正利用を抑制させることができる。

30

【 0 3 6 3 】

以下では、ローカル予約について説明する。

40

【 0 3 6 4 】

図 3 9 は、実施の形態に係るシステムのローカル予約不可の処理を示すシーケンス図である。図 2 8 と同様の要素には同様の符号を付しており、詳細な説明は省略する。以下では、代表して移動体装置 A でローカル予約対策の処理が行われる場合について説明する。

【 0 3 6 5 】

まず、端末 A は、移動体 A を利用したいユーザの操作に基づいて、移動体 A を利用予約するための予約トランザクションデータ $T r s v A$ を生成し (S 1 0 1 D) 、生成した予約トランザクションデータ $T r s v A$ を移動体装置 A に送信する (S 1 0 2 D) 。

【 0 3 6 6 】

次に、移動体装置 A は、ステップ S 1 0 2 D で送信された予約トランザクションデータ

50

TrsvAを受信すると、他の移動体装置である移動体装置B、Cに予約トランザクションデータTrsvAを転送することを試みるが、失敗する(S103D)。移動体装置Aはオフライン状態であるため、移動体装置B、Cに予約トランザクションデータTrsvAを転送できないからである。

【0367】

次に、移動体装置Aは、取得した予約トランザクションデータTrsvAの正当性を含む検証を行う検証アルゴリズムを実行する(S104D)。

【0368】

次に、移動体装置Aは、予約トランザクションデータTrsvAに対してブロック格納対象決定アルゴリズムを実行することで、ブロック格納対象決定処理を行う(S105D)。このとき、移動体装置Aは、オフライン状態であるため、後述するブロック格納対象決定処理において、処理対象の予約トランザクションデータTrsvAがブロック格納対象でないと決定し、予約トランザクションデータTrsvAに付与されているフラグの値を、ブロック格納対象でないことを示す第2の値に設定する。なお、移動体装置Aは、オンライン状態であれば、ブロック格納対象決定処理において、処理対象の予約トランザクションデータTrsvAがブロック格納対象であると決定し、予約トランザクションデータTrsvAに付与されているフラグの値を、ブロック格納対象であることを示す第1の値に設定する。

10

【0369】

次に、移動体装置Aは、ステップS104Dで実行された検証アルゴリズムにより検証済みであり、かつ、フラグが立っていない(つまり、フラグの値が第2の値に設定されている)予約トランザクションデータTrsvAをトランザクションプールaに格納する(S106D)。

20

【0370】

次に、移動体装置Aは、ステップS104Dで実行された検証アルゴリズムにより検証済みであり、かつ、フラグが立っている(つまり、フラグの値が第1の値に設定されている)トランザクションデータを含むブロックBlcを生成する(S107D)。このとき、予約トランザクションデータTrsvAのフラグの値は第2の値に設定されているため、生成されるブロックBlcには、予約トランザクションデータTrsvAが含まれない。

【0371】

30

次に、移動体装置Aは、他の移動体装置である移動体装置B、Cに、ステップS107Bで生成したブロックBlc(TrsvA)を送信することを試みるが、失敗する(S108D)。移動体装置Aはオフライン状態であるため、移動体装置B、CにブロックBlc(TrsvA)を送信できないからである。

【0372】

次に、移動体装置Aは、単独でコンセンサスアルゴリズムを実行する(S109D)。なお、ステップS107Dの処理は、ステップS109Dで単独でコンセンサスアルゴリズムを実行する際に行われてもよい。

【0373】

次に、移動体装置Aは、ステップS109Dで合意済みのブロックBlc(TrsvA含まない)を台帳A内のブロックチェーンに連結する(S110D)。

40

【0374】

図40は、実施の形態に係るブロック格納対象決定処理を示すフローチャートである。図40に示す本実施の形態に係るブロック格納対象決定処理は、図39のステップS105Dにおいて実行される。以下では、移動体装置Aでブロック格納対象決定処理が行われる場合について説明する。

【0375】

本実施の形態では、図39のステップS105Dにおいて、まず、移動体装置Aは、ステップS102Dの予約トランザクションデータTrsvAの送信処理の結果、予約トランザクションデータTrsvAを所定数より多い他の移動体装置に送信できたか否かを判

50

定する (S 1 0 5 1 D)。

【 0 3 7 6 】

移動体装置 A は、予約トランザクションデータ T r s v A を所定数より多い他の移動体装置に送信できたと判定した場合 (S 1 0 5 1 D で Y e s)、処理対象の予約トランザクションデータ T r s v A がブロック格納対象であると決定し、予約トランザクションデータ T r s v A に付与されているフラグの値を、ブロック格納対象であることを示す第 1 の値に設定する (S 1 0 5 2 D)。なお、フラグの値は、初期値としてブロック格納対象でないことを示す第 2 の値が設定されているものとする。

【 0 3 7 7 】

移動体装置 A は、予約トランザクションデータ T r s v A を所定数より多い他の移動体装置に送信できなかったと判定した場合 (S 1 0 5 1 D で N o)、何もせずに処理を終了する。

10

【 0 3 7 8 】

なお、フラグの値は、初期値としてブロック格納対象でないことを示す第 2 の値が設定されているとしたが、第 2 の値が設定されていなくてもよい。この場合において、移動体装置 A は、予約トランザクションデータ T r s v A を所定数より多い他の移動体装置に送信できなかったと判定した場合 (S 1 0 5 1 D で N o)、処理対象の予約トランザクションデータ T r s v A がブロック格納対象でないと決定し、予約トランザクションデータ T r s v A に付与されているフラグの値を、ブロック格納対象でないことを示す第 2 の値に設定してもよい。

20

【 0 3 7 9 】

図 4 1 は、実施の形態に係るシステムのローカル貸出の処理を示すシーケンス図である。

【 0 3 8 0 】

まず、端末 A は、移動体 A を利用するユーザの操作に基づいて、移動体 A の解錠要求を移動体装置 A に送信する (S 3 0 1 D)。

【 0 3 8 1 】

次に、移動体装置 A は、ステップ S 1 0 1 D で送信された解錠要求を受信すると、台帳 A のブロックチェーンに解錠要求に対応する予約があるかを確認する (S 3 0 2 D)。

【 0 3 8 2 】

しかしながら、移動体装置 A の台帳 A 内のブロックチェーンには、予約トランザクションデータ T r s v A を含むブロックが連結されていないため、移動体 A のロックを解除が許可されない (S 3 0 3 D)。

30

【 0 3 8 3 】

このように、所定数を越えた他の移動体装置と通信できなければ、取得した予約トランザクションデータ T r s v A を含むブロックを生成できない。これにより、台帳 A のみに、移動体 A を利用予約するための予約トランザクションデータ T r s v A を含むブロックが格納されてローカル予約が確定されることを抑制することができる。また、これにより、オフライン状態とされた移動体装置 A に対する予約によって、移動体装置 A が搭載された移動体 A の貸出を抑制することができる。

【 0 3 8 4 】

[効果等]

以上のように、本実施の形態によれば、例えば移動体装置 A である第 1 ノードは、所定数を越えた数の他の移動体装置である第 2 ノードと通信できなければ、移動体 A を利用するための予約トランザクションデータを含むブロックを生成できない。これにより、第 1 ノードを第 2 ノードと通信不可の状態にさせても、台帳 A だけに予約トランザクションデータを含むブロックを格納させないので、移動体 A の貸出そのものを抑制できる。よって、シェアリングサービスにおける移動体の不正利用に繋がるような移動体の利用そのものをさせないようにすることができる。

40

【 0 3 8 5 】

なお、移動体 A は、上述したように、サービス対象の一例であり、移動体 A の利用予約

50

は、サービス対象の契約の一例である。所定数を越えた第2ノードと通信できなければ、取得した第1トランザクションデータを含むブロックを生成できない。これにより、第1ノードを第2ノードと通信不可の状態にさせて、第1分散台帳だけに第1トランザクションデータを含むブロックを格納させるといったサービス対象の不正利用に繋がる処理を抑制することができる。よって、ブロックチェーンを悪用したサービス対象の不正利用を抑制できる。

【0386】

[その他の実施の形態等]

以上のように、本開示について上記の実施の形態に基づいて説明してきたが、本開示は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本開示に含まれる。

10

【0387】

(1)上記の実施の形態では、サービス対象として、移動体を例に挙げて説明したがこれに限らない。サービス対象は、サービスが利用されないときには他のユーザが利用できないようにロックされていて、サービスを利用する際にロックが解除されるものであればよく、例えばホテルの部屋、電子ロッカーでもよい。また、契約は、例えば移動体10の利用予約に限らず、例えばホテルの部屋の利用予約、電子ロッカーの利用予約でもよい。

【0388】

(2)上記の実施の形態における各装置は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAMまたはハードディスクユニットには、コンピュータプログラムが記録されている。前記マイクロプロセッサが、前記コンピュータプログラムにしたがって動作することにより、各装置は、その機能を達成する。ここでコンピュータプログラムは、所定の機能を達成するために、コンピュータに対する指令を示す命令コードが複数個組み合わされて構成されたものである。

20

【0389】

(3)上記の実施の形態における各装置は、構成する構成要素の一部または全部は、1個のシステムLSI(Large Scale Integration:大規模集積回路)から構成されているとしてもよい。システムLSIは、複数の構成部を1個のチップ上に集積して製造された超多機能LSIであり、具体的には、マイクロプロセッサ、ROM、RAMなどを含んで構成されるコンピュータシステムである。前記RAMには、コンピュータプログラムが記録されている。前記マイクロプロセッサが、前記コンピュータプログラムにしたがって動作することにより、システムLSIは、その機能を達成する。

30

【0390】

また、上記の各装置を構成する構成要素の各部は、個別に1チップ化されていても良いし、一部またはすべてを含むように1チップ化されてもよい。

【0391】

また、ここでは、システムLSIとしたが、集積度の違いにより、IC、LSI、スーパーLSI、ウルトラLSIと呼称されることもある。また、集積回路化の手法はLSIに限るものではなく、専用回路または汎用プロセッサで実現してもよい。LSI製造後に、プログラムすることが可能なFPGA(Field Programmable Gate Array)や、LSI内部の回路セルの接続や設定を再構成可能なりコンフィギュラブル・プロセッサを利用しても良い。

40

【0392】

さらには、半導体技術の進歩または派生する別技術によりLSIに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適用等が可能性としてありえる。

【0393】

(4)上記の各装置を構成する構成要素の一部または全部は、各装置に脱着可能なICカードまたは単体のモジュールから構成されているとしてもよい。前記ICカードまたは

50

前記モジュールは、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ICカードまたは前記モジュールは、上記の超多機能LSIを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、前記ICカードまたは前記モジュールは、その機能を達成する。このICカードまたはこのモジュールは、耐タンパ性を有するとしてもよい。

【0394】

(5)本開示は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【0395】

また、本開示は、前記コンピュータプログラムまたは前記デジタル信号をコンピュータで読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD(Blu-ray(登録商標)Disc)、半導体メモリなどに記録したものとしてもよい。また、これらの記録媒体に記録されている前記デジタル信号であるとしてもよい。

【0396】

また、本開示は、前記コンピュータプログラムまたは前記デジタル信号を、電気通信回線、無線または有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

【0397】

また、本開示は、マイクロプロセッサとメモリを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記録しており、前記マイクロプロセッサは、前記コンピュータプログラムにしたがって動作するとしてもよい。

【0398】

また、前記プログラムまたは前記デジタル信号を前記記録媒体に記録して移送することにより、または前記プログラムまたは前記デジタル信号を、前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

【0399】

(6)上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【産業上の利用可能性】

【0400】

本開示は、制御方法、制御装置、及び、プログラムに利用でき、例えば自転車、自動二輪車などの移動体のシェアリングサービスなどでユーザが移動体利用のための契約を行う場合に、料金を払わない不正利用を抑制することができる制御方法、御方法、制御装置、及び、プログラムなどに利用可能である。

【符号の説明】

【0401】

1 システム

10、10A、10B、10C 移動体

11、11A、11B、11C 端末

20 管理サーバ

100 移動体装置

101、1101 入力部

102 トランザクションデータ生成部

103 トランザクションデータ検証部

104 ブロック生成部

105 同期部

106 スマートコントラクト実行部

107 ブロックチェーン管理部

108 分散台帳記憶部

10

20

30

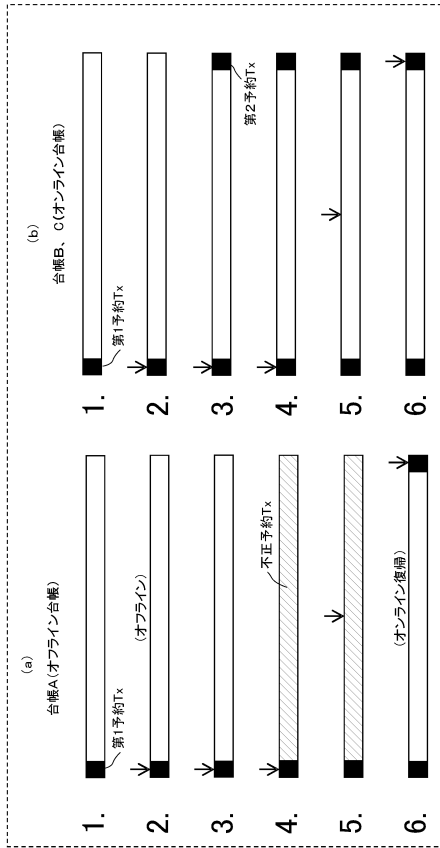
40

50

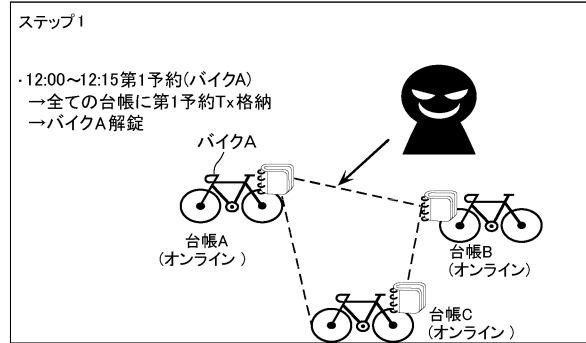
- 1 0 9 状態記憶部
- 1 1 0 不正検知部
- 1 1 1、1 1 0 3 通信部
- 1 1 2、1 1 0 2 表示部

【図面】

【図1】



【図2A】

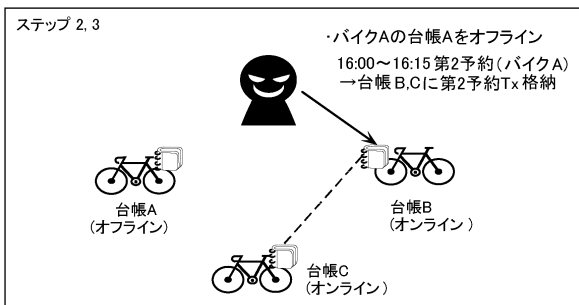


10

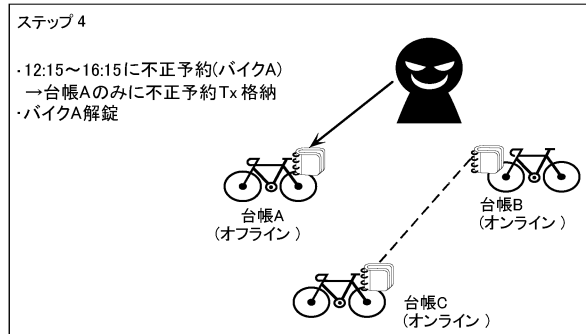
20

30

【図2B】



【図2C】



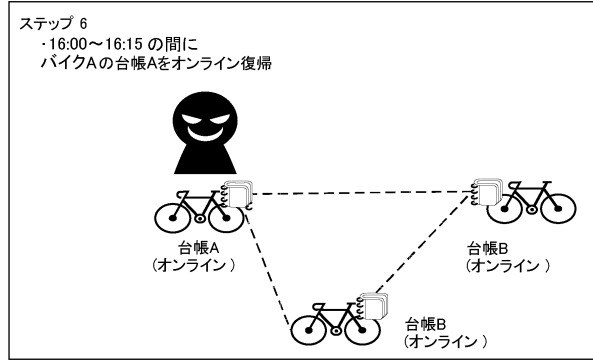
40

50

【図 2 D】

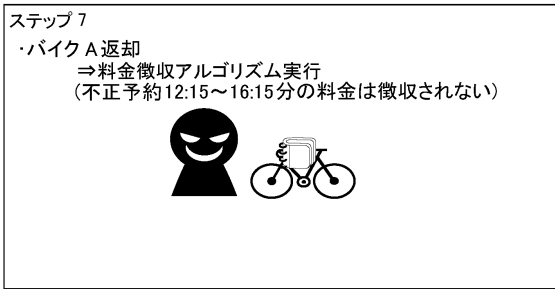


【図 2 E】

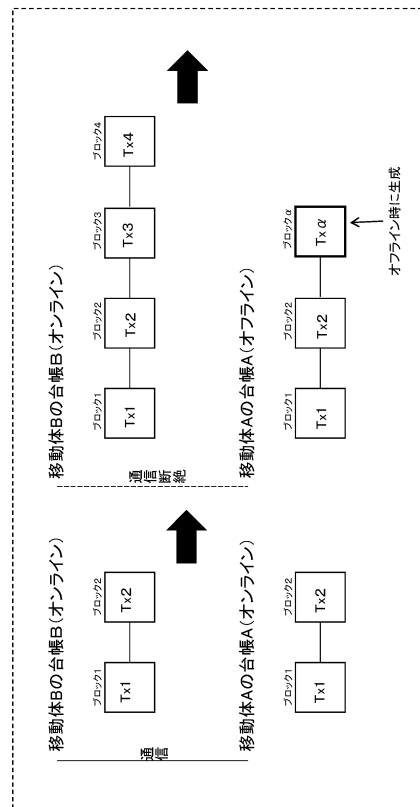


10

【図 2 F】



【図 3 A】



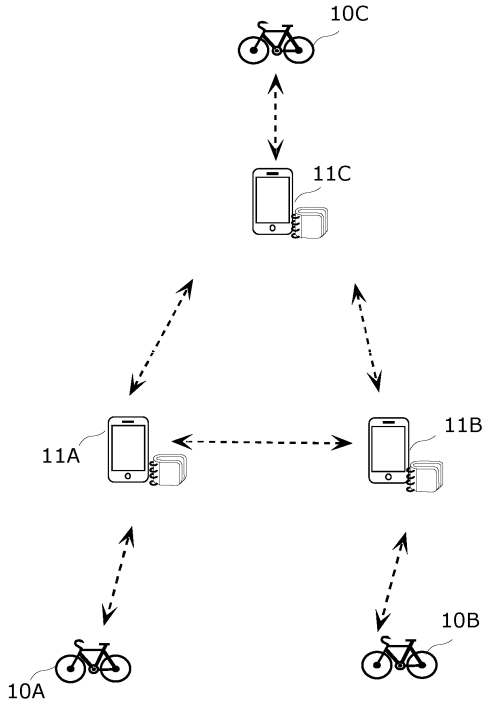
20

30

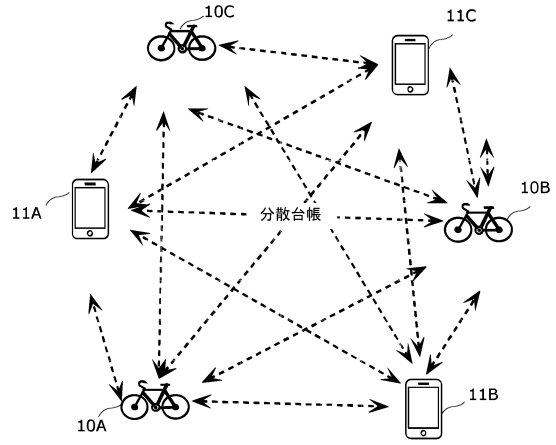
40

50

【図5B】



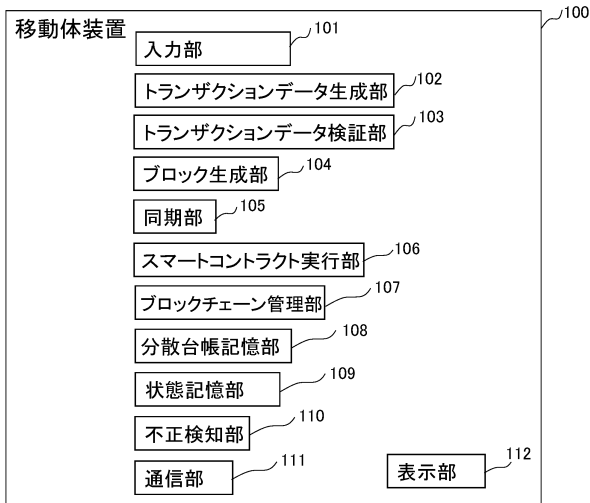
【図5C】



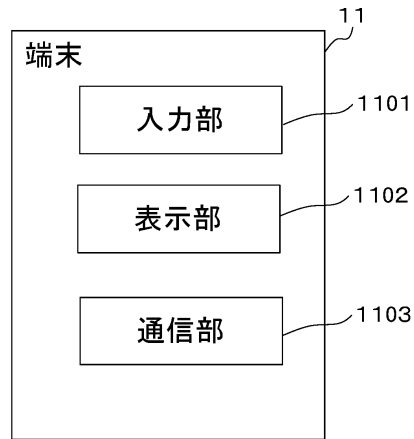
10

20

【図6】



【図7】

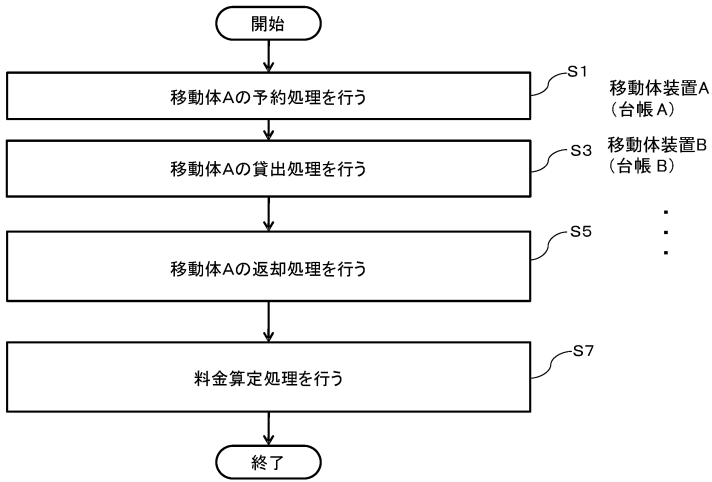


30

40

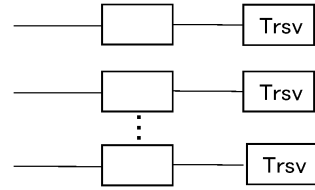
50

【 図 8 】



【 図 9 A 】

#1-1 (移動体Aの予約)

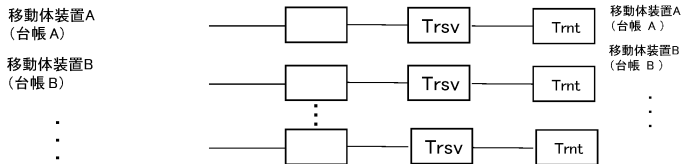


10

20

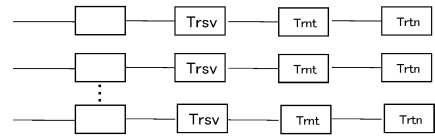
【 図 9 B 】

#1-2 (移動体Aの貸出)



【 図 9 C 】

#1-3 (移動体Aの返却)

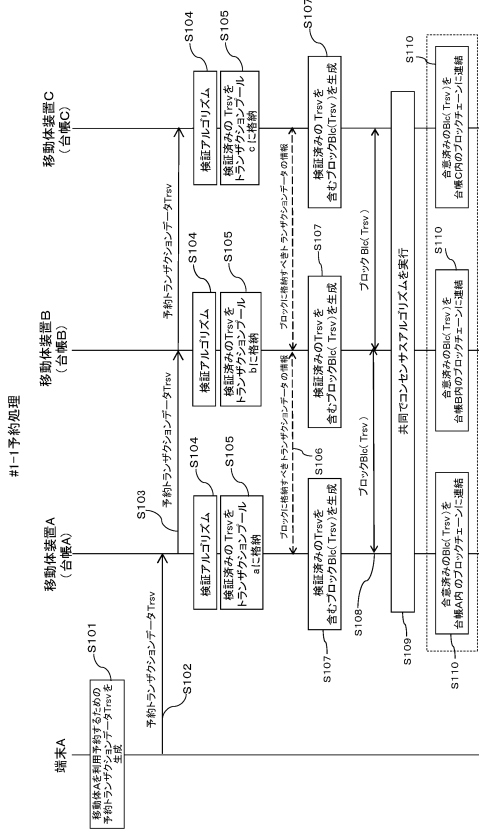


30

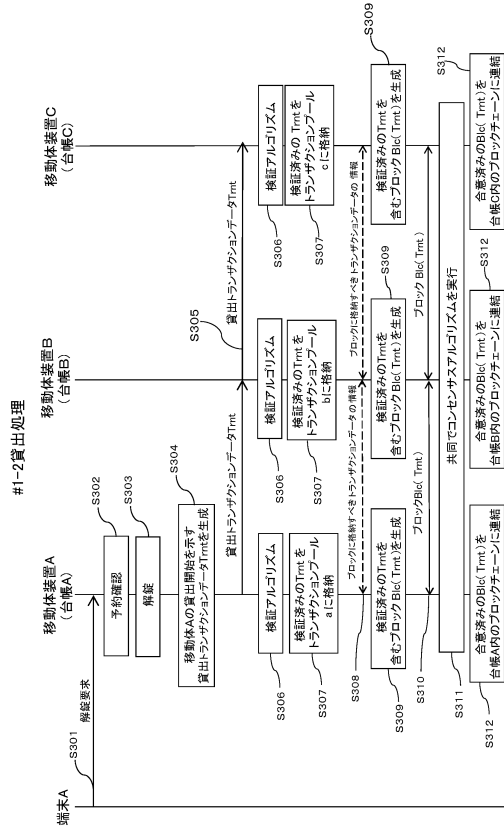
40

50

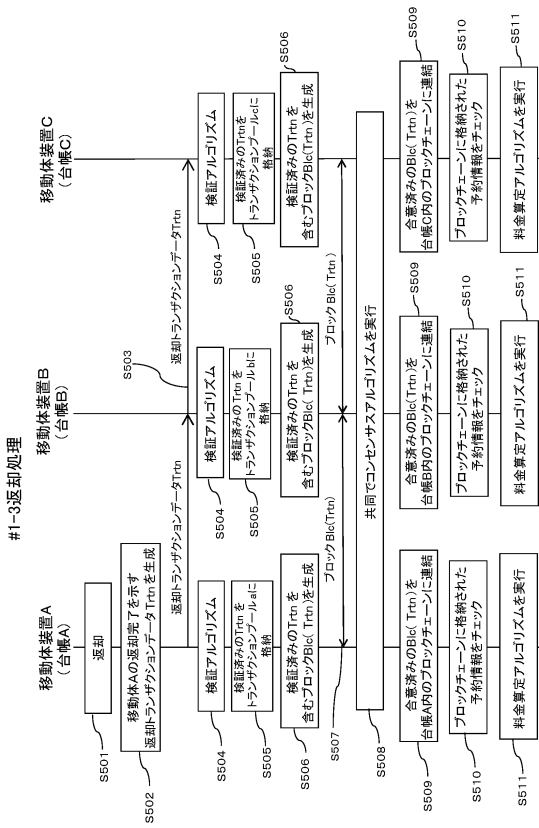
【図 1 0】



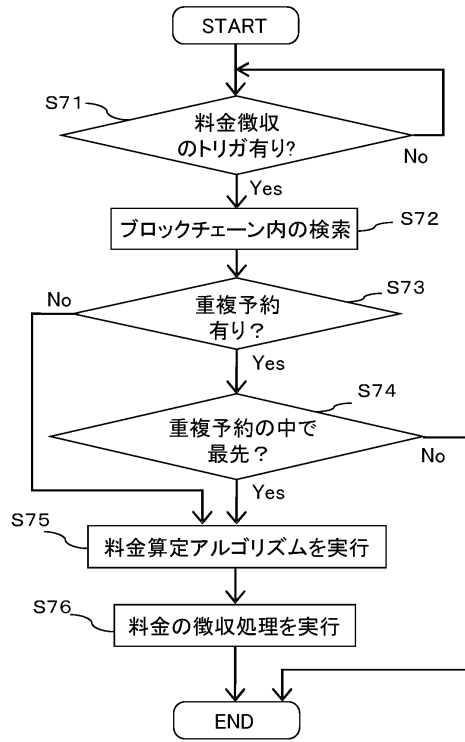
【図 1 1】



【図 1 2】



【図 1 3】



10

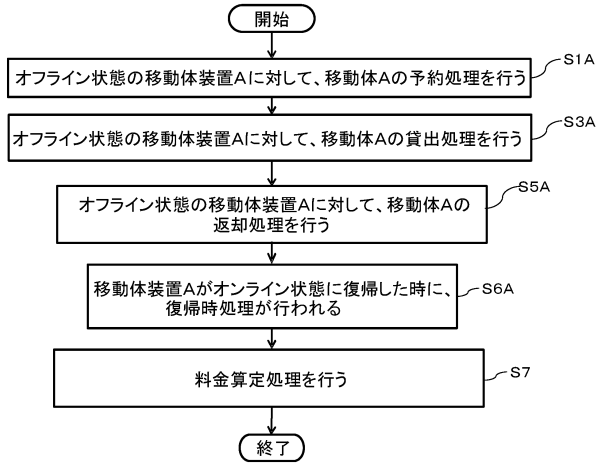
20

30

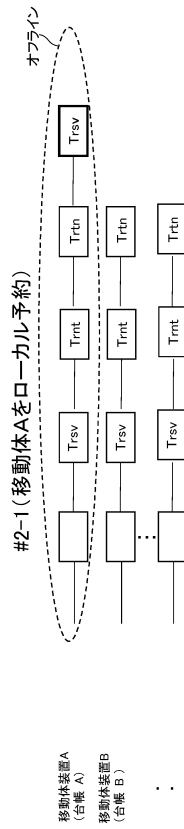
40

50

【図 1 4】



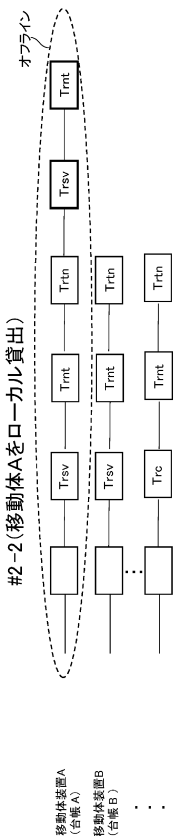
【図 1 5 A】



10

20

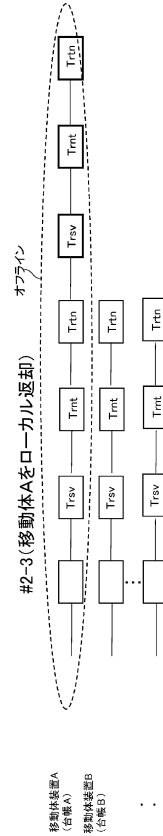
【図 1 5 B】



30

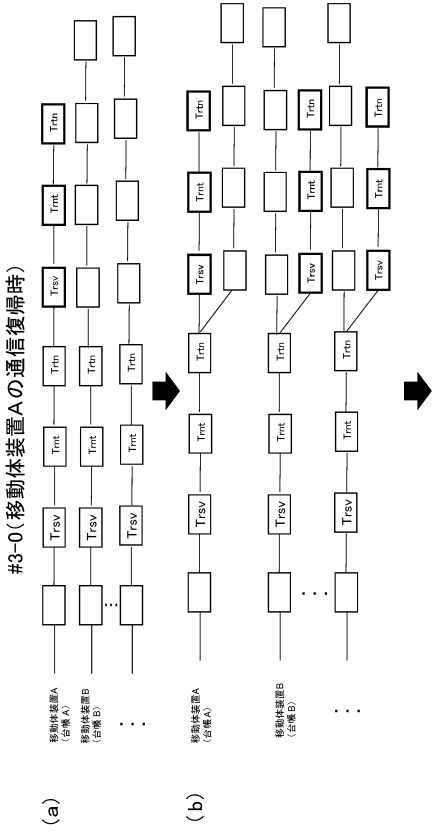
40

【図 1 5 C】

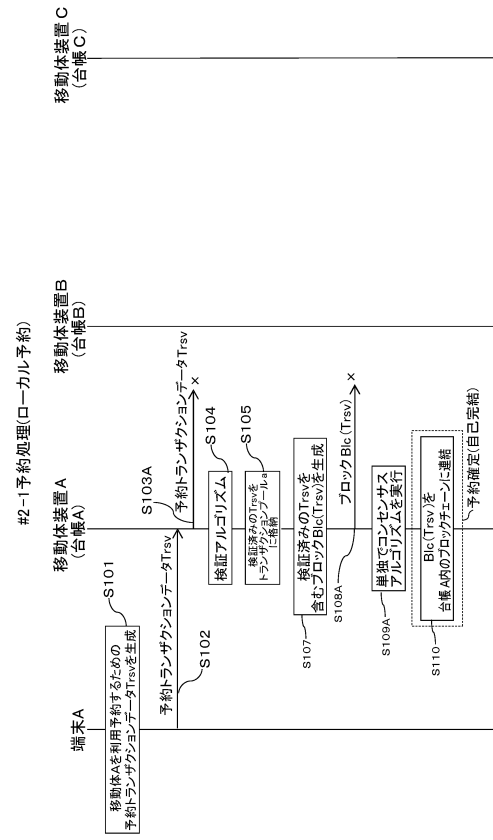


50

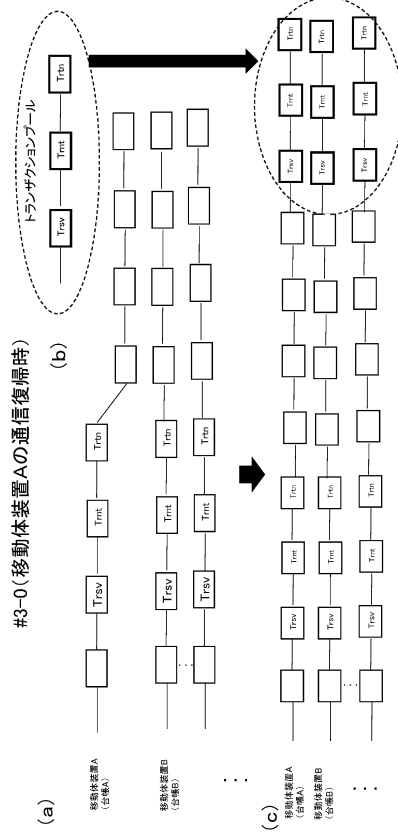
【図 16】



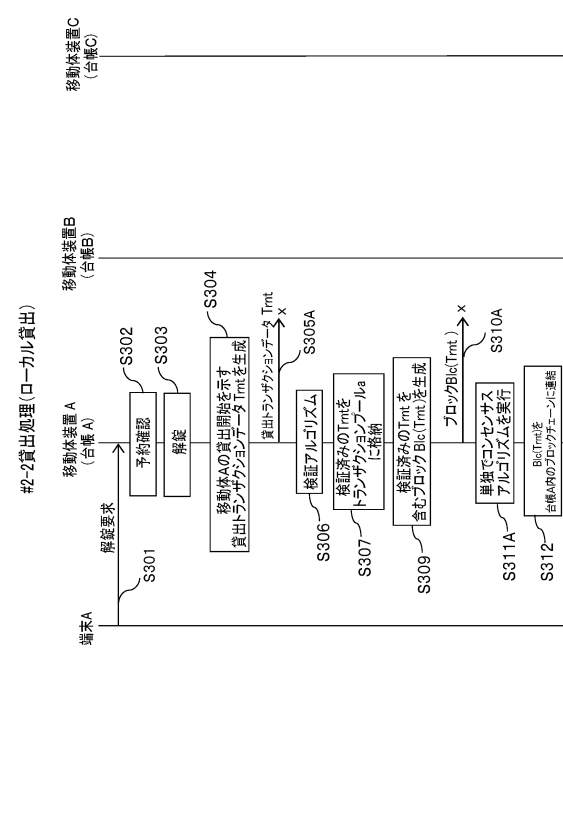
【図 18】



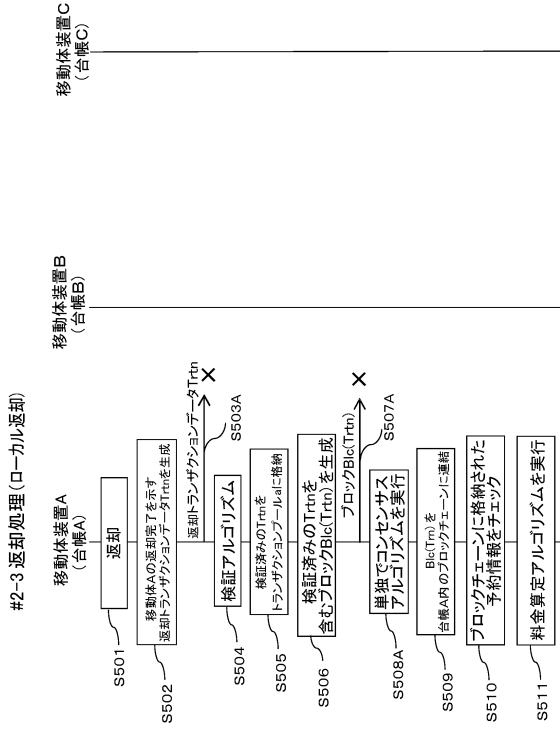
【図 17】



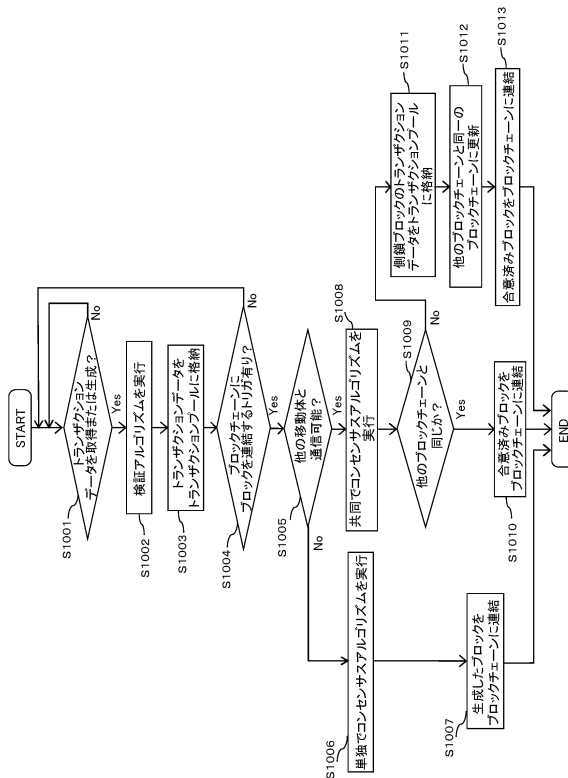
【図 19】



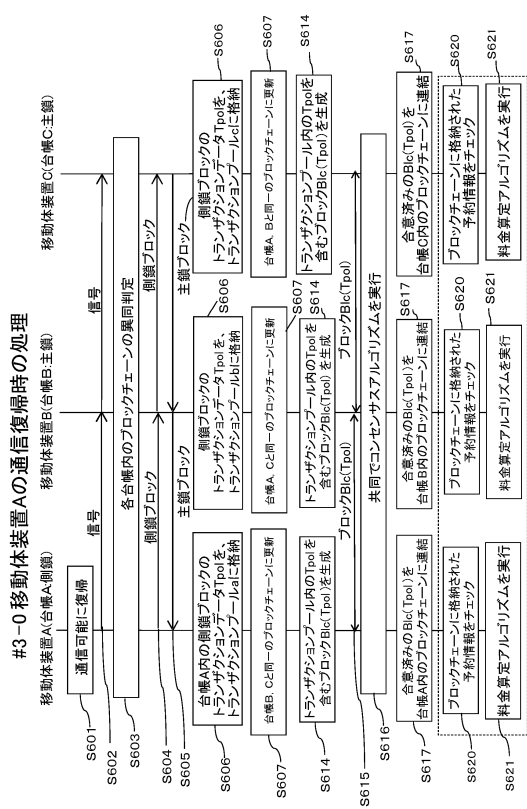
【図 2 0】



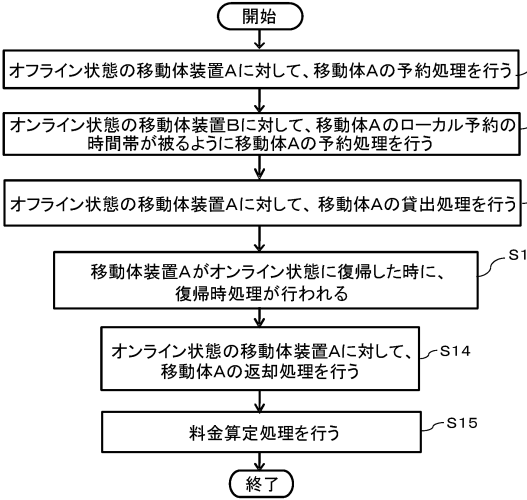
【図 2 2】



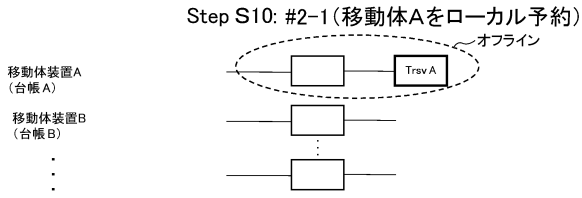
【図 2 1】



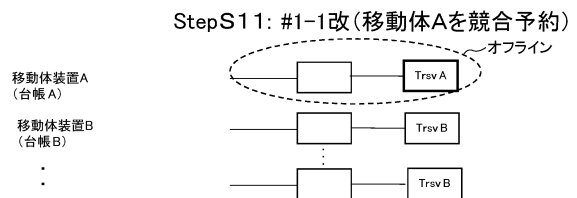
【図 2 3】



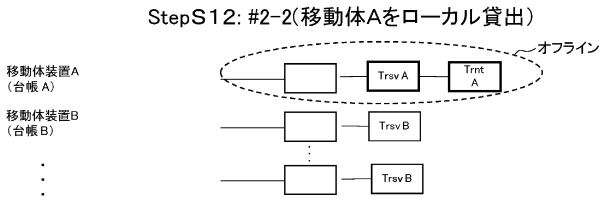
【図 2 4 A】



【図 2 4 B】

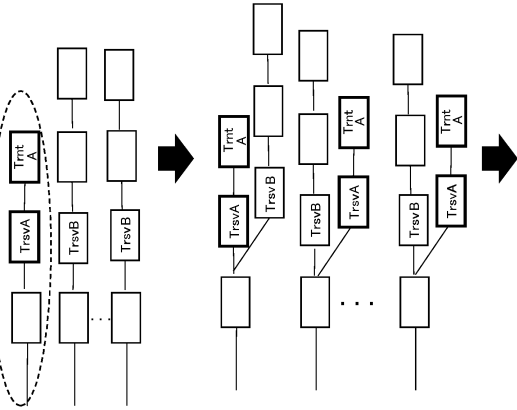


【図 2 4 C】



【図 2 5】

Step S13: #3-0(移動体装置Aの通信復帰時)



移動体装置A (台帳 A)
移動体装置B (台帳 B)
...

(a)

(b)

10

20

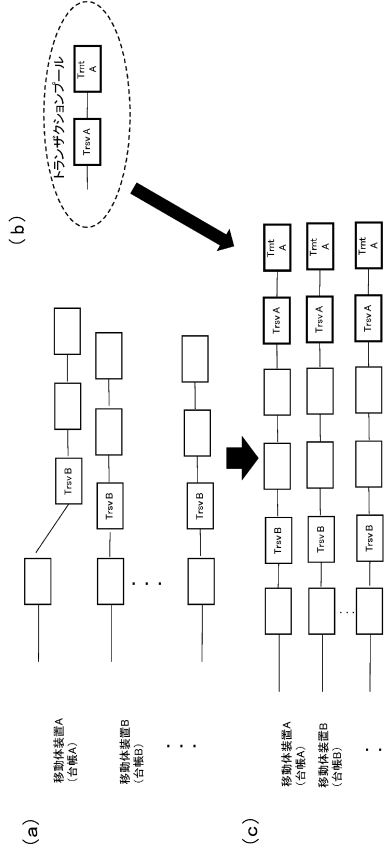
30

40

50

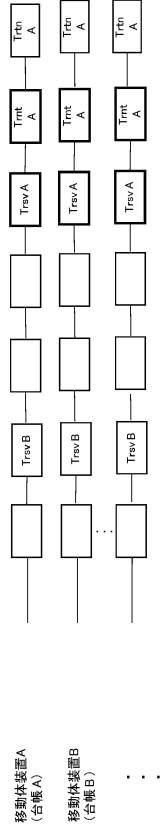
【図 26】

StepS13: #3-0 移動体装置Aの通信復帰時



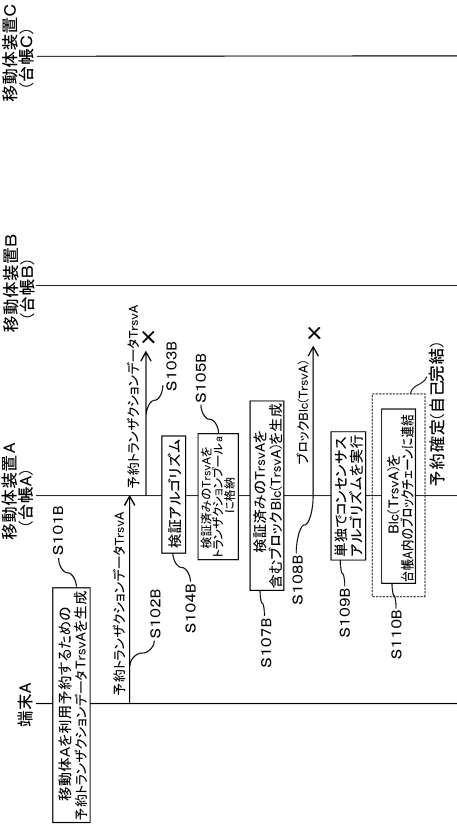
【図 27】

StepS14: #1-3 移動体Aを返却(オンライン)



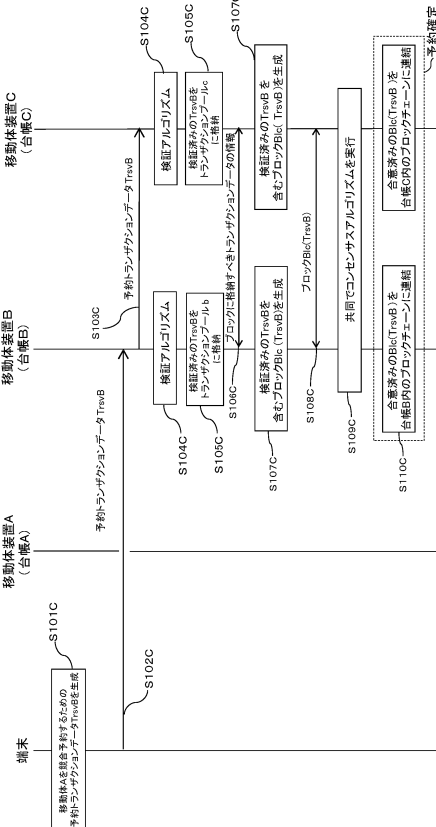
【図 28】

STEPS10#2-1ローカル予約

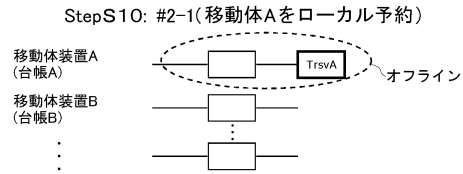


【図 29】

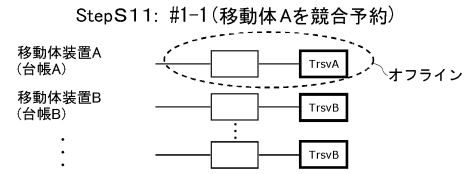
STEPS11: #1-1改 競合予約



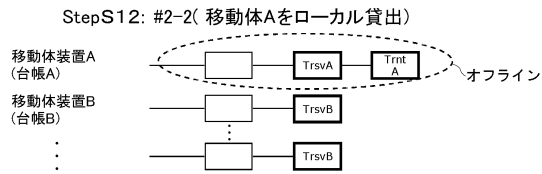
【図34A】



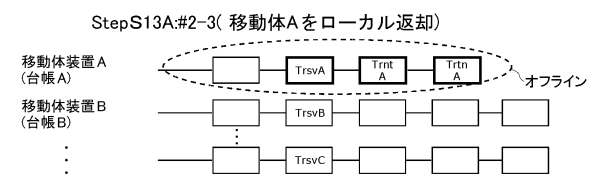
【図34B】



【図34C】

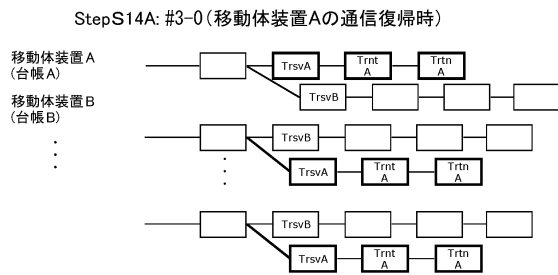


【図34D】

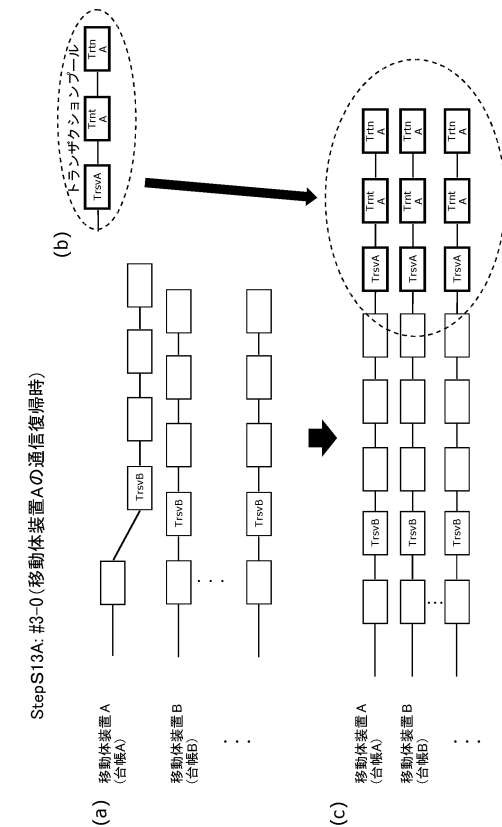


10

【図35】



【図36】



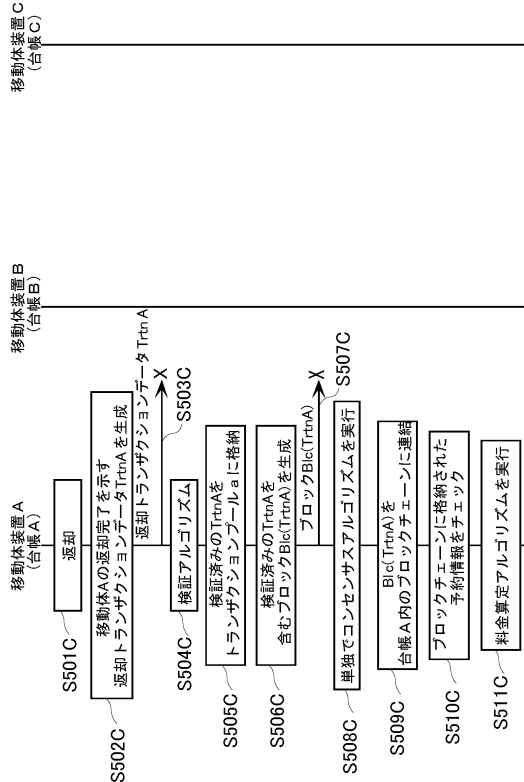
20

30

40

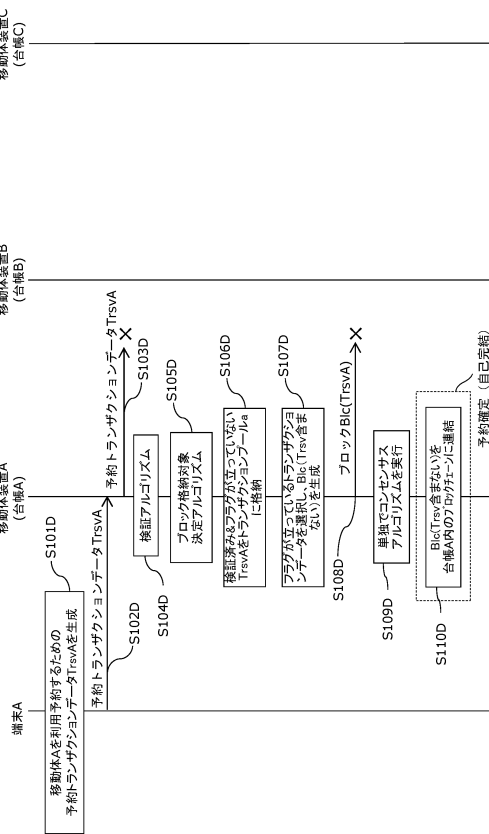
【図 37】

StepS13A: #2-3(移動体Aをローカル返却)



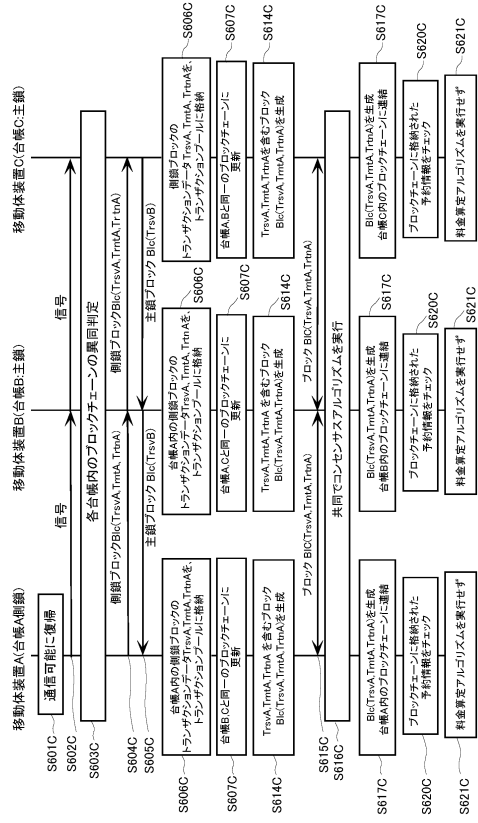
【図 39】

STEP1: #2-1' ローカル予約

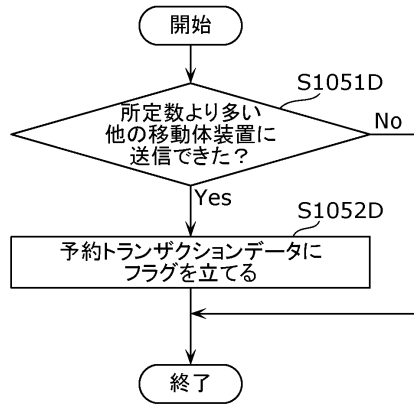


【図 38】

StepS14A: #3-0(移動体装置Aが通信復帰時の処理)

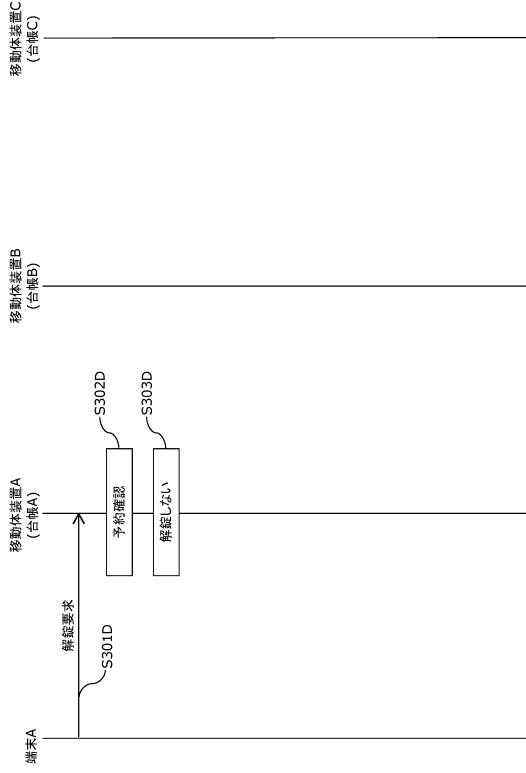


【図 40】



【 4 1 】

STEP3: #2-2' ローカル貸出



10

20

30

40

50

フロントページの続き

- (72)発明者 西田 直央
日本国大阪府門真市大字門真 1 0 0 6 番地 パナソニックホールディングス株式会社内
- (72)発明者 海上 勇二
日本国大阪府門真市大字門真 1 0 0 6 番地 パナソニックホールディングス株式会社内
- 審査官 貝塚 涼
- (56)参考文献 特開 2 0 1 9 - 1 5 3 1 3 0 (J P , A)
米国特許出願公開第 2 0 2 0 / 0 0 0 5 3 8 8 (U S , A 1)
特許第 6 4 6 9 9 2 0 (J P , B 1)
国際公開第 2 0 1 9 / 1 0 1 2 4 4 (W O , A 2)
特開 2 0 1 9 - 0 2 8 5 2 5 (J P , A)
- (58)調査した分野 (Int.Cl. , D B 名)
G 0 6 Q 1 0 / 0 0 - 9 9 / 0 0