(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7469715号
(P7469715)

(45)発行日　令和6年4月17日(2024.4.17)

(24)登録日　令和6年4月9日(2024.4.9)

(51)国際特許分類
Ｇ０６Ｑ　50/06　(2024.01)

ＦＩ
Ｇ０６Ｑ　50/06

請求項の数　9　（全31頁）

(21)出願番号　特願2022-574893(P2022-574893)
(86)(22)出願日　令和3年1月13日(2021.1.13)
(86)国際出願番号　PCT/JP2021/000742
(87)国際公開番号　WO2022/153375
(87)国際公開日　令和4年7月21日(2022.7.21)
審査請求日　令和5年2月9日(2023.2.9)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　110002918
弁理士法人扶桑国際特許事務所
(72)発明者　宮前 剛
神奈川県川崎市中原区上小田中４丁目１番１号 富士通株式会社内
(72)発明者　小櫻 文彦
神奈川県川崎市中原区上小田中４丁目１番１号 富士通株式会社内
審査官　池田 聡史

最終頁に続く

(54)【発明の名称】　データ格納方法、データ格納プログラム、および情報処理装置

(57)【特許請求の範囲】
【請求項１】
コンピュータが、
生産者が生産した取引資源の生産実績を示す第１のデータと、消費者が消費した前記取引資源の消費実績を示す第２のデータとを取得し、
前記消費者の前記消費実績分の前記取引資源の供給元として前記生産者の前記生産実績分の前記取引資源を割り当てることについての前記第１のデータと前記第２のデータとの整合性の条件が満たされることを証明する証明情報を生成し、
前記証明情報を含み、前記第１のデータおよび前記第２のデータの総データサイズよりもデータサイズが小さい第３のデータを生成し、
前記生産者が生産した前記取引資源の供給権の取引履歴が格納されたブロックチェーンに、前記第３のデータを含む、前記取引資源が前記消費者によって消費されたことを示すトランザクションレコードを格納する、
データ格納方法。
【請求項２】
前記トランザクションレコードの格納では、第１のコンピュータが前記トランザクションレコードを生成し、前記第１のコンピュータは生成した前記トランザクションレコードを、前記ブロックチェーンを格納している第２のコンピュータに送信し、前記第２のコンピュータは、前記証明情報に基づいて、前記第１のデータと前記第２のデータとの整合性の条件が満たされることを検証し、正しく検査できた場合に前記トランザクションレコー

ドを前記ブロックチェーンに格納する、
請求項１記載のデータ格納方法。
【請求項３】
前記証明情報の生成では、所定の資源供給期間内の単位期間ごとに、前記第１のデータに示される前記生産実績と、前記第２のデータに示される前記消費実績とを比較し、前記単位期間それぞれについて消費量分の生産量があるという条件が満たされることを証明する前記証明情報を生成する、
請求項１または２に記載のデータ格納方法。
【請求項４】
前記証明情報の生成では、前記第２のデータに示される前記消費実績の総量についてのコミットメント関数の値を計算し、前記第１のデータと前記第２のデータとの整合性の条件が満たされることに加え、前記コミットメント関数の値が正しいことを証明する前記証明情報を生成する。
請求項１ないし３のいずれかに記載のデータ格納方法。
【請求項５】
前記ブロックチェーン上での前記取引資源を供給する権利の取引情報をＵＴＸＯ（Unspent Transaction Output）方式で管理し、前記生産者の生産期間と単位時間当たりの生産量とにより、前記ＵＴＸＯ方式におけるインプットとアウトプットの対象となる前記取引資源を特定する、
請求項１ないし４のいずれかに記載のデータ格納方法。
【請求項６】
前記第１のデータは、前記生産実績についての前記生産者の第１の電子署名を含み、前記第２のデータは、前記消費実績についての前記消費者の第２の電子署名を含み、
前記証明情報の生成では、前記第１のデータと前記第２のデータとの整合性の条件が満たされることに加え、前記生産者の前記第１の電子署名と前記消費者の前記第２の電子署名とが正当であることを証明する前記証明情報をする、
請求項１ないし５のいずれかに記載のデータ格納方法。
【請求項７】
前記トランザクションレコードの格納では、前記ブロックチェーンにおいて前記取引資源を供給する権利を有する者の署名を含む前記トランザクションレコードを前記ブロックチェーンに格納する、
請求項１ないし６のいずれかに記載のデータ格納方法。
【請求項８】
コンピュータに、
生産者が生産した取引資源の生産実績を示す第１のデータと、消費者が消費した前記取引資源の消費実績を示す第２のデータとを取得し、
前記消費者の前記消費実績分の前記取引資源の供給元として前記生産者の前記生産実績分の前記取引資源を割り当てることについての前記第１のデータと前記第２のデータとの整合性の条件が満たされることを証明する証明情報を生成し、
前記証明情報を含み、前記第１のデータおよび前記第２のデータの総データサイズよりもデータサイズが小さい第３のデータを生成し、
前記生産者が生産した前記取引資源の供給権の取引履歴が格納されたブロックチェーンに、前記第３のデータを含む、前記取引資源が前記消費者によって消費されたことを示すトランザクションレコードを格納する、
処理を実行させるデータ格納プログラム。
【請求項９】
生産者が生産した取引資源の生産実績を示す第１のデータと、消費者が消費した前記取引資源の消費実績を示す第２のデータとを記憶する記憶部と、
前記消費者の前記消費実績分の前記取引資源の供給元として前記生産者の前記生産実績分の前記取引資源を割り当てることについての前記第１のデータと前記第２のデータとの

整合性の条件が満たされることを証明する証明情報を生成し、前記証明情報を含み、前記第１のデータおよび前記第２のデータの総データサイズよりもデータサイズが小さい第３のデータを生成し、前記生産者が生産した前記取引資源の供給権の取引履歴が格納されたブロックチェーンに、前記第３のデータを含む、前記取引資源が前記消費者によって消費されたことを示すトランザクションレコードを格納する処理部と、
を有する情報処理装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データ格納方法、データ格納プログラム、および情報処理装置に関する。
【背景技術】
【０００２】
多数のユーザが参加する取引に関するデータは、何らかの手段によって台帳で管理される。台帳を中央集権型のプラットフォームで管理すると、そのプラットフォームの維持管理を行う第三者機関が本当に信頼できるか否かを証明し続けなければならない。特にプラットフォームが成長して管理者の責任や権限が増大した場合や、管理者を含めたプラットフォームのユーザの間の利害関係が複雑化してしまうと、その証明は非常に困難になる。
【０００３】
近年では、信頼できる第三者機関を置かずに、非中央集権的な台帳管理が可能なブロックチェーンによる台帳管理が提案されている。ブロックチェーンは、ネットワークを構成する複数のノードが同一のデータベースを保持する分散型台帳技術の１つである。ブロックチェーンでは、ネットワーク上のトランザクション群がブロックとしてまとめて処理され、ハッシュ関数によって各ブロックがリンクされている。ブロックチェーンにおいて記録されたブロックのデータは、後続のすべてのブロックを変更しない限り遡及的に変更することはできず、ブロックチェーンを用いた台帳管理のプラットフォームは改変に対する安全性が高い。
【０００４】
ブロックチェーンは、取引履歴がオープンであり、取引履歴の改ざんが困難なことから、暗号資産の台帳管理などの様々な分野で利用されている。ブロックチェーンを利用した技術の一例として、環境に貢献する電力を、環境に貢献する方法で消費することを促し、再生可能エネルギーの導入・普及の促進を図る電力取引システムが提案されている。
【先行技術文献】
【特許文献】
【０００５】
【文献】特開２０２０－１０７２０２号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
ブロックチェーンでは台帳を分散管理するため、サーバで一括して管理するデータベースと比較してストレージコストが高くなる。この問題は、取り扱うデータ量が大きくなったときに顕著となる。例えば電力などの資源取引において実際に消費した資源を生産者から購入する場合、購入対象期間内の生産実績と消費実績とを照合することとなる。資源の生産実績や消費実績のデータは逐次生成されるため、これらのデータを含めてブロックチェーンで管理しようとするとブロックチェーンで管理するデータ量が肥大化し、ストレージコストの増大を招く。
【０００７】
１つの側面では、本発明は、ブロックチェーンで取り扱うデータ量を削減することを目的とする。
【課題を解決するための手段】
【０００８】

１つの案では、コンピュータによるデータ格納方法が提供される。
コンピュータは、生産者が生産した取引資源の生産実績を示す第１のデータと、消費者が消費した取引資源の消費実績を示す第２のデータとを取得する。次にコンピュータは、消費者の消費実績分の取引資源の供給元として生産者の生産実績分の取引資源を割り当てることについての第１のデータと第２のデータとの整合性の条件が満たされることを証明する証明情報を生成する。さらにコンピュータは、証明情報を含み、第１のデータおよび第２のデータの総データサイズよりもデータサイズが小さい第３のデータを生成する。そしてコンピュータは、生産者が生産した取引資源の供給権の取引履歴が格納されたブロックチェーンに、第３のデータを含む、取引資源が消費者によって消費されたことを示すトランザクションレコードを格納する。

【発明の効果】

【０００９】

１態様によれば、ブロックチェーンで取り扱うデータ量を削減することができる。
本発明の上記および他の目的、特徴および利点は本発明の例として好ましい実施の形態を表す添付の図面と関連した以下の説明により明らかになるであろう。

【図面の簡単な説明】

【００１０】

【図１】第１の実施の形態に係るデータ格納方法の一例を示す図である。
【図２】電力取引システムの構成の一例を示す図である。
【図３】ノードのハードウェアの一例を示す図である。
【図４】各ノードの機能の一例を示すブロック図である。
【図５】電力供給権の取引の概要を示す図である。
【図６】電力供給権の取引の一例を示す図である。
【図７】電力供給権の取引の第１の例を示す図である。
【図８】電力供給権の取引の第２の例を示す図である。
【図９】電源供給権トランザクションレコードのデータ構造の一例を示す図である。
【図１０】スマートメータレコードと電力マッチングレコードとに含まれる情報の一例を示す図である。
【図１１】電力マッチングの一例を示す図である。
【図１２】取引対象の電力の総電力供給期間開始前の処理手順の一例を示すシーケンス図である。
【図１３】取引対象の電力の総電力供給期間開始後の処理手順の一例を示すシーケンス図である。
【図１４】非化石証書の発行と検証の処理手順の一例を示すシーケンス図である。

【発明を実施するための形態】

【００１１】

以下、本実施の形態について図面を参照して説明する。なお各実施の形態は、矛盾のない範囲で複数の実施の形態を組み合わせて実施することができる。

〔第１の実施の形態〕

まず第１の実施の形態について説明する。第１の実施の形態は、資源の供給権の取引をブロックチェーンで管理し、資源の生産実績と消費実績とをブロックチェーン外で管理することで、ブロックチェーンで取り扱うデータ量を削減するためのデータ格納方法である。

【００１２】

図１は、第１の実施の形態に係るデータ格納方法の一例を示す図である。図１にはブロックチェーンシステム４と、ブロックチェーンシステム４外の情報処理装置１０とが示されている。

【００１３】

ブロックチェーンシステム４は、例えば複数のコンピュータを含み、複数のコンピュータはＰ２Ｐ（Peer to Peer）で接続されている。ブロックチェーンシステム４に含まれるコンピュータは、ノードと呼ぶこともある。ブロックチェーンシステム４では、複数のノ

ードにブロックチェーン５が分散格納される。
【００１４】
ブロックチェーン５には、生産者１，２で生産され消費者３によって消費される取引資源についての供給権の取引台帳が格納される。取引資源は、例えば電力などのエネルギー資源である。取引資源には、例えば生物体の持つエネルギーを利用したバイオ燃料も含まれる。ブロックチェーン５には、取引資源の供給権が譲渡された場合に、その譲渡取引を示すトランザクションレコード５ａ，５ｂが登録される。
【００１５】
生産者１，２は、自身が有する生産設備で生産する取引資源の供給権を有する。そして生産者１，２は、取引資源の供給権を第三者に譲渡することができる。
例えば生産者１，２が取引資源の供給権を譲渡すると、その取引内容を示すトランザクションレコード５ａがブロックチェーン５に登録される。トランザクションレコード５ａには、ＩＤ「Ａ」の生産者１とＩＤ「Ｂ」の生産者２とが、取引資源をＩＤ「Ｄ」の仲介者に譲渡したことが示されている。
【００１６】
情報処理装置１０は、例えば記憶部１１と処理部１２とを有するコンピュータである。情報処理装置１０は、例えば所定の処理手順が記述されたデータ格納プログラムを実行することにより、第１の実施の形態に係るデータ格納方法を実施することができる。記憶部１１は、例えば情報処理装置１０が有するメモリ、またはストレージ装置である。処理部１２は、例えば情報処理装置１０が有するプロセッサ、または演算回路である。
【００１７】
情報処理装置１０は、例えば生産者１，２が生産する取引資源の供給権を有する仲介者（ＩＤ［Ｄ］）が有する装置である。仲介者「Ｄ」は、生産者１，２が取引資源を生産した後、消費者３（ＩＤ［Ｃ］）にその取引資源の供給権に基づく供給契約を結ぶことができる。この供給契約を履行するには、生産者１，２による取引資源の生産実績が、消費者３による消費実績以上であることが前提となる。
【００１８】
そこで情報処理装置１０の処理部１２は、生産者１，２が生産した取引資源の生産実績を示す第１のデータ６と、消費者３が消費した取引資源の消費実績を示す第２のデータ７とを取得する。例えば処理部１２は、生産者１，２それぞれの生産設備に取り付けられた計測器で計測された生産量の時系列変化を示すデータを、第１のデータ６として取得する。例えば処理部１２は、消費者３の消費設備に取り付けられた計測器で計測された消費量の時系列変化を示すデータを、第２のデータ７として取得する。処理部１２は、取得した第１のデータ６と第２のデータ７とを記憶部１１に格納する。
【００１９】
処理部１２は、消費者３の消費実績分の取引資源の供給元として生産者１，２の生産実績分の取引資源を割り当てることについての第１のデータ６と第２のデータ７との整合性の条件が満たされることを証明する証明情報８ｂを生成する。証明情報８ｂは、例えばゼロ知識証明の値である。ゼロ知識証明としては、例えば非対話ゼロ知識証明が用いられる。
【００２０】
例えば処理部１２は、所定の資源供給期間内の単位期間ごとに、第１のデータ６に示される生産実績と、第２のデータ７に示される消費実績とを比較する。処理部１２は、単位期間それぞれについて消費量分の生産量があるという条件が満たされることを証明する証明情報８ｂを生成する。
【００２１】
また処理部１２は、第２のデータ７に示される消費実績の総量（総消費実績）についてのコミットメント関数の値８ａを計算してもよい。この場合、処理部１２は、第１のデータ６と第２のデータ７との整合性の条件が満たされることに加え、コミットメント関数の値８ａが正しいことを証明する証明情報８ｂを生成する。
【００２２】

さらに処理部１２は、証明情報８ｂを含み、第１のデータ６および第２のデータ７の総データサイズよりもデータサイズが小さい第３のデータ８を生成する。なお、処理部１２は、証明情報８ｂにおいてコミットメント関数の値８ａが正しいことを証明した場合、第３のデータ８にコミットメント関数の値８ａを含める。

【００２３】

処理部１２は、生産者１，２が生産した取引資源の供給権の取引履歴が格納されたブロックチェーン５に、第３のデータ８を含む、取引資源が消費者によって消費されたことを示すトランザクションレコード５ｂを格納する。例えば処理部１２は、トランザクションレコード５ｂをブロックチェーンシステム４に送信する。ブロックチェーンシステム４では、トランザクションレコード５ｂの正当性を検証する。例えばブロックチェーンシステム４内の１つのノードが、証明情報８ｂに基づいて、第１のデータ６と第２のデータ７との整合性の条件が満たされることを検証する。そのノードは、正当な場合にトランザクションレコード５ｂを含むブロックをブロックチェーン５に追加する。

【００２４】

このように生産実績と消費実績との管理がブロックチェーンシステム４外で行われ、ブロックチェーンには生産実績と消費実績を集約することで生成された第３のデータが格納されている。これにより、ブロックチェーン５のデータ量を削減することができる。なお生産実績と消費実績との整合性がとれていることは証明情報８ｂによって証明される。そのため、ブロックチェーンシステム４では証明情報８ｂを検証することで、ブロックチェーンシステム４内で第１のデータ６および第２のデータ７を管理することなく、生産実績と消費実績との整合性がとれていることを検証できる。証明情報８ｂがゼロ知識証明の値であれば、ブロックチェーンシステム４のノードは、適用されたゼロ知識証明の検証処理を実施することで、証明情報８ｂの正当性を検証できる。

【００２５】

生産実績と消費実績とをブロックチェーンシステム４外で管理すれば、生産者の生産実績および消費者の消費実績を秘匿状態とすることも可能となる。すなわち、生産実績と消費実績とをブロックチェーンシステム４内に管理すると、生産実績と消費実績は公開情報とならざるを得ない。それに対し、生産実績と消費実績とをブロックチェーンシステム４外で管理していれば、生産実績と消費実績とを取り扱う情報処理装置１０などにおいて生産実績と消費実績を非公開の情報として管理することができる。その結果、生産者および消費者のプライバシーが保護される。

【００２６】

またブロックチェーンシステム４では、例えばブロックチェーン５上での取引資源を供給する権利の取引情報をＵＴＸＯ（Unspent Transaction Output）方式で管理することができる。この場合、ブロックチェーンシステム４内のノードは、生産者１，２の生産期間と単位時間当たりの生産量とにより、ＵＴＸＯ方式におけるインプットとアウトプットの対象となる取引資源を特定する。このように生産期間と生産量との２次元の情報で取引対象となる取引資源を特定することで、電力のように生産期間と消費期間とが一致することが求められるような取引資源の供給権の取引にＵＴＸＯ方式を適用することが可能となる。そしてＵＴＸＯ方式を利用することにより、同じ取引資源が複数の相手に譲渡されること（ダブルカウント）を抑止できる。

【００２７】

なお生産者１，２および消費者３の正当性は、電子署名技術を用いて証明することができる。例えば情報処理装置１０の処理部１２は、生産実績についての生産者１，２の第１の電子署名を含む第１のデータ６を取得すると共に、消費実績についての消費者３の第２の電子署名を含む第２のデータ７を取得する。そして処理部１２は、生産実績と消費実績との整合性の条件が満たされることに加え、生産者１，２の第１の電子署名と消費者３の第２の電子署名とが正当であることを証明する証明情報８ｂを生成する。

【００２８】

これにより第１のデータ６が、ブロックチェーン５に示される供給権についての生産者

の生産実績であることが保証される。また消費者３が誰であるのかについても証明情報８ｂによって証明される。消費者３を証明できることは、例えば非化石エネルギーを用いて生産された取引資源を消費したことを消費者３が証明する場合に有用となる。

【００２９】

なお生産者１，２が生産した取引資源を譲渡できるのは、その取引資源の供給権を有する者（例えばＩＤ「Ｄ」の仲介者）である。そこで情報処理装置１０の処理部１２は、例えばブロックチェーン５において取引資源を供給する権利を有する者の電子署名を含むトランザクションレコード５ｂをブロックチェーン５に格納する。これにより、ブロックチェーンシステム４において、取引資源を供給する権利を有する者の意思による譲渡取引のトランザクションレコード５ｂであることを確認できる。

【００３０】

〔第２の実施の形態〕

次に第２の実施の形態について説明する。第２の実施の形態は、電力取引の台帳をブロックチェーンで管理する場合におけるデータ量の削減に関するものである。

【００３１】

＜システム構成＞

図２は、電力取引システムの構成の一例を示す図である。ネットワーク２０には、ブロックチェーンシステム３０に含まれる複数のノード４００，４００ａ，・・・が接続されている。複数のノード４００，４００ａ，・・・は、互いにＰ２Ｐで通信接続されている。複数のノード４００，４００ａ，・・・が連係して動作することで、電力取引の台帳がブロックチェーンにより分散管理される。

【００３２】

電力取引は発電事業者４１ａ，４１ｂ，・・・、小売電気事業者４３ａ，４３ｂ，・・・、および電力消費者４２ａ，４２ｂ，・・・の間で行われる。電力取引の参加者であるユーザは、それぞれネットワーク２０に接続されたノード１００，１００ａ，・・・，２００，２００ａ，・・・，３００，３００ａ，・・・，４００，４００ａ，・・・を有する。ノード１００，１００ａ，・・・，２００，２００ａ，・・・，３００，３００ａ，・・・，４００，４００ａ，・・・は、電力を供給する権利の取引に用いるコンピュータである。

【００３３】

発電事業者４１ａは、物理発電設備５１ａを有する。物理発電設備５１ａは、石油、ガス、石炭などの化石燃料を用いた発電設備、または水力、太陽光、風力などの再生可能エネルギーを用いた発電設備である。物理発電設備５１ａは発電した電力を、電力供給網（変電・送電・配電のシステム）に供給する。物理発電設備５１ａにはスマートメータ５３ａが取り付けられており、発電した電力がスマートメータ５３ａにより計測される。スマートメータ５３ａは、ネットワーク２０に接続されている。スマートメータ５３ａが計測した電力は、発電事業者４１ａのノード２００によって読み出される。

【００３４】

同様に発電事業者４１ｂも、スマートメータ５３ｂが取り付けられた物理発電設備５１ｂを有する。スマートメータ５３ｂが計測した電力は、発電事業者４１ｂのノード２００ａによって読み出される。

【００３５】

電力消費者４２ａは、電力消費設備５２ａを有する。電力消費設備５２ａは、工場、住宅、オフィスなどの電力を用いた機器を有する設備である。電力消費設備５２ａは、電力供給網を介して電力の供給を受ける。電力消費設備５２ａにはスマートメータ５３ｃが取り付けられており、消費した電力がスマートメータ５３ｃにより計測される。スマートメータ５３ｃは、ネットワーク２０に接続されている。スマートメータ５３ｃが計測した電力は、電力消費者４２ａのノード３００によって読み出される。

【００３６】

同様に電力消費者４２ｂも、スマートメータ５３ｄが取り付けられた電力消費設備５２

ｂを有する。スマートメータ５３ｄが計測した電力は、電力消費者４２ｂのノード３００ａによって読み出される。

【００３７】

小売電気事業者４３ａ，４３ｂ，・・・は、ノード１００，１００ａ，・・・を用いて、例えば発電事業者４１ａ，４１ｂ，・・・から電力供給権を買い取り、その電力供給権の範囲内で電力消費者４２ａ，４２ｂ，・・・に電力を販売する。小売電気事業者４３ａ，４３ｂ，・・・間で電力供給権を取引することもできる。

【００３８】

電力供給権の取引は、ブロックチェーンによって台帳が管理される。例えば発電事業者４１ａが電力供給権を売却した場合、ノード２００が、電力供給権の取引内容を示すトランザクションレコード（電力供給権トランザクションレコード）を生成する。ノード２０ａは、生成した電力供給トランザクションレコードをブロックチェーンシステム３０のいずれかのノードに送信する。ブロックチェーンシステム３０によって電力供給トランザクションレコードの正当性が検証されると、その電力供給トランザクションレコードがブロックチェーンに登録される。

【００３９】

非化石価値検証者４４は、ノード５００により非化石証書の正当性を検証し、再生可能エネルギーで発電した電力を利用したことの認定を行う。非化石証書は、再生可能エネルギーで発電した電力の非化石価値を証書化したものである。非化石化証書は、再生可能エネルギーで発電された電力を供給した小売電気事業者４３ａのノード１００で発行される。発行された非化石証書は、該当する電力の供給を受けた電力消費者４２ａのノード３００に渡される。電力消費者４２ａは、非化石証書をノード３００からノード５００に送信する。するとノード５００は、非化石証書が正当であることを検証する。

【００４０】

図３は、ノードのハードウェアの一例を示す図である。図３には、代表的にノード１００のハードウェア構成を示している。

ノード１００は、プロセッサ１０１によって装置全体が制御されている。プロセッサ１０１には、バス１０９を介してメモリ１０２と複数の周辺機器が接続されている。プロセッサ１０１は、マルチプロセッサであってもよい。プロセッサ１０１は、例えばＣＰＵ（Central Processing Unit）、ＭＰＵ（Micro Processing Unit）、またはＤＳＰ（Digital Signal Processor）である。プロセッサ１０１がプログラムを実行することで実現する機能の少なくとも一部を、ＡＳＩＣ（Application Specific Integrated Circuit）、ＰＬＤ（Programmable Logic Device）などの電子回路で実現してもよい。

【００４１】

メモリ１０２は、ノード１００の主記憶装置として使用される。メモリ１０２には、プロセッサ１０１に実行させるＯＳ（Operating System）のプログラムやアプリケーションプログラムの少なくとも一部が一時的に格納される。また、メモリ１０２には、プロセッサ１０１による処理に利用する各種データが格納される。メモリ１０２としては、例えばＲＡＭ（Random Access Memory）などの揮発性の半導体記憶装置が使用される。

【００４２】

バス１０９に接続されている周辺機器としては、ストレージ装置１０３、ＧＰＵ（Graphics Processing Unit）１０４、入力インタフェース１０５、光学ドライブ装置１０６、機器接続インタフェース１０７およびネットワークインタフェース１０８がある。

【００４３】

ストレージ装置１０３は、内蔵した記録媒体に対して、電気的または磁気的にデータの書き込みおよび読み出しを行う。ストレージ装置１０３は、コンピュータの補助記憶装置として使用される。ストレージ装置１０３には、ＯＳのプログラム、アプリケーションプログラム、および各種データが格納される。なお、ストレージ装置１０３としては、例えばＨＤＤ（Hard Disk Drive）やＳＳＤ（Solid State Drive）を使用することができる。

【００４４】

ＧＰＵ１０４は画像処理を行う演算装置であり、グラフィックコントローラとも呼ばれる。ＧＰＵ１０４にはモニタ２１が接続されている。ＧＰＵ１０４は、プロセッサ１０１からの命令に従って、画像をモニタ２１の画面に表示させる。モニタ２１としては、有機ＥＬ（Electro Luminescence）を用いた表示装置や液晶表示装置などがある。

【００４５】

入力インタフェース１０５には、キーボード２２とマウス２３とが接続されている。入力インタフェース１０５は、キーボード２２やマウス２３から送られてくる信号をプロセッサ１０１に送信する。なお、マウス２３は、ポインティングデバイスの一例であり、他のポインティングデバイスを使用することもできる。他のポインティングデバイスとしては、タッチパネル、タブレット、タッチパッド、トラックボールなどがある。

【００４６】

光学ドライブ装置１０６は、レーザ光などを利用して、光ディスク２４に記録されたデータの読み取り、または光ディスク２４へのデータの書き込みを行う。光ディスク２４は、光の反射によって読み取り可能なようにデータが記録された可搬型の記録媒体である。光ディスク２４には、ＤＶＤ（Digital Versatile Disc）、ＤＶＤ－ＲＡＭ、ＣＤ－ＲＯＭ（Compact Disc Read Only Memory）、ＣＤ－Ｒ（Recordable）／ＲＷ（ReWritable）などがある。

【００４７】

機器接続インタフェース１０７は、ノード１００に周辺機器を接続するための通信インタフェースである。例えば機器接続インタフェース１０７には、メモリ装置２５やメモリリーダライタ２６を接続することができる。メモリ装置２５は、機器接続インタフェース１０７との通信機能を搭載した記録媒体である。メモリリーダライタ２６は、メモリカード２７へのデータの書き込み、またはメモリカード２７からのデータの読み出しを行う装置である。メモリカード２７は、カード型の記録媒体である。

【００４８】

ネットワークインタフェース１０８は、ネットワーク２０に接続されている。ネットワークインタフェース１０８は、ネットワーク２０を介して、他のコンピュータまたは通信機器との間でデータの送受信を行う。ネットワークインタフェース１０８は、例えばスイッチやルータなどの有線通信装置にケーブルで接続される有線通信インタフェースである。またネットワークインタフェース１０８は、基地局やアクセスポイントなどの無線通信装置に電波によって通信接続される無線通信インタフェースであってもよい。

【００４９】

ノード１００は、以上のようなハードウェアによって、第２の実施の形態の処理機能を実現することができる。図２に示した他のノード３１，３２，・・・，２００，３００，４００，５００，６００も、ノード１００と同様のハードウェアによって実現することができる。また第１の実施の形態に示した装置も、図３に示したノード１００と同様のハードウェアにより実現することができる。

【００５０】

ノード１００は、例えばコンピュータ読み取り可能な記録媒体に記録されたプログラムを実行することにより、第２の実施の形態の処理機能を実現する。ノード１００に実行させる処理内容を記述したプログラムは、様々な記録媒体に記録しておくことができる。例えば、ノード１００に実行させるプログラムをストレージ装置１０３に格納しておくことができる。プロセッサ１０１は、ストレージ装置１０３内のプログラムの少なくとも一部をメモリ１０２にロードし、プログラムを実行する。またノード１００に実行させるプログラムを、光ディスク２４、メモリ装置２５、メモリカード２７などの可搬型記録媒体に記録しておくこともできる。可搬型記録媒体に格納されたプログラムは、例えばプロセッサ１０１からの制御により、ストレージ装置１０３にインストールされた後、実行可能となる。またプロセッサ１０１が、可搬型記録媒体から直接プログラムを読み出して実行することもできる。

【００５１】

＜電力供給権の取引に求められる技術要件＞

図２，図３に示した構成のシステムにより、電力供給権の取引が実施される。ここで電力供給権の取引を行うシステムに求められる技術的な要件について説明する。

【００５２】

［非中央集権性］

最初の要件は、非中央集権的なシステムであることである。すなわち信頼できる第三者機関を置かない前提で、トランザクションシステムを正しく運用できることが求められる。

【００５３】

［トレーサビリティ］

２つ目の要件は、トレーサビリティを有することである。物理発電設備５１ａ，５１ｂは、例えば家庭のソーラー光発電設備のように再生可能エネルギーを用いた発電設備の場合がある。再生可能エネルギーで発電された電力に基づく電力供給権は、例えば小売電気事業者４３ａ，４３ｂに譲渡され、その電力供給権に基づいて電力消費者４２ａ，４２ｂに電力が供給される。電力消費者４２ａ，４２ｂである企業は、太陽光、水力、地熱などの非化石電源により発電された電力を購入して消費すると、ＣＳＲ（Corporate Social Responsibility）の観点で高く評価される。従って電力消費者４２ａ，４２ｂは、非化石電源により発電された電力を購入した際には、それを証明する情報（非化石価書）の取得を希望する場合がある。非化石電力の消費者が非化石価値の検証者から非化石価値の獲得を認められるためには、いつどの物理発電設備によって発電された電力に基づく非化石価値であるかを証明できることが重要となる。そのために、電力供給権の取引の履歴を正しく追跡できることが要求される。

【００５４】

［ダブルカウント防止］

３つ目の要件は、電力供給権のダブルカウントが防止されていることである。電力の取引におけるダブルカウントは、１つの物理発電設備においてある期間に発電される電力供給権が、異なる２つの相手に譲渡されることである。これは各物理発電設備の各時刻の発電実績が、複数の異なる発電実績として悪用されてしまうことを防止するために重要となる。

【００５５】

［スケーラビリティー］

４つ目の要件は、高いスケーラビリティーを有することである。個人の家屋への小規模の太陽光発電システムの導入が一般化し、１００万件規模の小規模発電事業者が存在する。これらの小規模発電事業者で発電した電力供給権を取引するには、１００万件以上のリアルタイムに近い（３０分単位の）非化石電力についての需給マッチングを管理できるトランザクション性能が求められる。

【００５６】

［ストレージコスト］

５つ目の要件はストレージコストを低く抑えることである。電力は物理発電設備５１ａ，５１ｂによって生産され、電力消費設備５２ａ，５２ｂによって消費される。これらの設備による発電実績と電力消費実績とを正確に管理することが要求される。物理発電設備５１ａ，５１ｂに取り付けられているスマートメータ５３ａ，５３ｂは、３０分ごとに、過去３０分間に発電した電力量を含むスマートメータレコードを生成する。一方、電力消費設備５２ａ，５２ｂのスマートメータ５３ｃ，５３ｄは、３０分ごとに、過去３０分間に消費した電力量を含むスマートメータレコードを生成する。その結果、スマートメータレコードが大量に生成される。そのため長期間にわたって運用可能なシステムとするには、膨大な量のスマートメータレコードを管理するためのストレージコストを低く抑えることが重要となる。

【００５７】

［プライバシー］

６つ目の要件は、ユーザのプライバシーを保護できることである。プライバシー情報と

位置付けられるのは、例えば電力発電実績および電力消費実績のスマートメータのデータである。スマートメータのデータを電力取引の当事者以外のユーザには開示せずにすむことが求められる。

【００５８】

＜要件を満たすための技術の概要＞

第２の実施の形態では、以上の６つの要件を満たすために、ブロックチェーンを用いたシステムを提供する。ただし、ブロックチェーンを用いただけでは、電力供給権の取引に求められるすべての技術的要件を満たすことはできない。特に以下のような課題が存在する。

【００５９】

まず、ブロックチェーンは通常のデータベースと比較してストレージコストが高く、またデータの整合性を検証するための処理が遅い。さらに、ブロックチェーンはすべてのユーザ間でデータを共有するため、電力発電実績や電力消費実績をそのままの形でブロックチェーンに格納するとプライバシーが保たれない。

【００６０】

すなわちブロックチェーンは分散型で取引の台帳を管理可能な技術であり、ブロックチェーンを利用することで非中央集権型のシステムを構築できる。ただしブロックチェーンは、トランザクション数が多くなりすぎると迅速に処理できなくなるというスケーラビリティー問題が存在する。そのため、多数の物理発電設備または電力消費設備によって３０分ごとに生成される膨大なスマートメータレコードすべてをトランザクションとしてブロックチェーンに格納することは困難である。

【００６１】

そこで第２の実施の形態のシステムでは、膨大なスマートメータレコードをブロックチェーンに格納するのではなく、スマートメータレコードを集約することでサイズダウンした電力マッチングレコードをブロックチェーンに格納する。これにより、ブロックチェーンに格納するデータサイズを抑えることができ、スケーラビリティー問題を解決できる。

【００６２】

電力マッチングレコードは、ある物理発電設備により発電された電力に対応するスマートメータレコードとその電力を消費した消費設備のスマートメータレコードとを集約することにより生成されるものである。電力マッチングレコードには、「消費設備ＩＤ」「総電力供給期間」「総電力量コミットメント」「ゼロ知識証明」「仮想発電設備による電子署名」が含まれるが、集約元の複数のスマートメータレコードのデータの総量よりもデータサイズが小さい。そのため、電力マッチングレコードであれば、ブロックチェーンに格納しても、ブロックチェーンで取り扱うデータ量の増大が抑止される。

【００６３】

しかも第２の実施の形態のシステムでは、ブロックチェーンに格納された電力マッチングレコードに「総電力量コミットメント」と「ゼロ知識証明」を含めることにより、発電実績と電力消費実績との整合性がとれていることをゼロ知識証明によって証明する。これにより、例えば発電量の総量及び消費量の総量が一致しているか否かの検証を、それぞれのスマートメータレコードに含まれる発電実績および電力消費実績を秘匿したまま実行することが可能となる。

【００６４】

このように、第２の実施の形態に係る電力取引システムによれば、サイズダウンした電力マッチングレコードがブロックチェーンに格納される。これにより、ブロックチェーンのスケーラビリティー問題を解決するとともに、ゼロ知識証明技術によって、発電実績および電力消費実績を秘匿したまま、電力取引の正当性の検証を可能とする電力取引ブロックチェーンシステムを提供することができる。

【００６５】

なお、物理発電設備のスマートメータレコードと消費設備のスマートメータレコードとをマージしたデータを圧縮すればデータサイズを小さくすることができる。そのためデー

タ圧縮技術を用いればブロックチェーンの容量の削減は可能である。しかし、ブロックチェーンに登録されたデータは公開情報となる。そのため、圧縮されたデータを伸張することで、スマートメータレコードの内容も第三者に見られてしまう。従って、プライバシー保護の要件を満たしつつブロックチェーンのデータサイズを削減するには、スマートメータレコードをブロックチェーン外で管理し、電力マッチングレコードのみをブロックチェーンに登録するのが適切である。

【００６６】

電力供給権の取引は、発電事業者４１ａ，４１ｂ，・・・、電力消費者４２ａ，４２ｂ，・・・、および小売電気事業者４３ａ，４３ｂ，・・・の間で行われる。このうち小売電気事業者４３ａ，４３ｂ，・・・は、電力供給権の取引においては、仮想発電設備の運用者として取り扱うことができる。また発電事業者４１ａ，４１ｂ，・・・それぞれは、複数の物理発電設備を運用する可能性がある。同様に電力消費者４２ａ，４２ｂ，・・・は、複数の電力消費設備を運用する可能性がある。

【００６７】

このように電力供給権を取引するユーザと物理発電設備または電力消費設備とは、１対１には対応しない。そして、実際の電力の供給と消費は、仮想発電設備を介して、物理発電設備と電力消費設備との間で行われる。そのため、発電実績と電力消費実績を考慮した取引を行うには、仮想発電設備、物理発電設備、電力消費設備それぞれを識別することが求められる。そこで仮想発電設備、物理発電設備、電力消費設備それぞれには予め一意の識別子（電力設備ＩＤ）が付与され、電力設備ＩＤを用いて電力供給権の取引、発電実績、電力消費実績が管理される。このときシステム上は、仮想発電設備、物理発電設備、電力消費設備それぞれが、電力供給権の取引主体として取り扱われる。以下、仮想発電設備、物理発電設備、および電力消費設備を総称して、電力設備と呼ぶ。

【００６８】

＜電力供給権の取引のためのノードの機能＞

次にブロックチェーンを利用して電力供給権を取引するために各ノードが有する機能について説明する。

【００６９】

図４は、各ノードの機能の一例を示すブロック図である。発電事業者４１ａのノード２００は、スマートメータレコード提供部２１０とトランザクション生成部２２０とを有する。

【００７０】

スマートメータレコード提供部２１０は、物理発電設備５１ａ（図２参照）に取り付けられたスマートメータ５３ａから、物理発電設備５１ａにおける発電量の時間遷移を示すスマートメータレコードを定期的に取得する。スマートメータレコード提供部２１０は、物理発電設備５１ａで発電した電力を販売する権利を有する小売電気事業者のノードに、取得したスマートメータレコードを送信する。

【００７１】

トランザクション生成部２２０は、発電事業者４１ａが電力供給権を小売電気事業者に売った場合に、取引内容を示す電力供給権トランザクションレコードを生成する。トランザクション生成部２２０は、生成した電力供給権トランザクションレコードを、ブロックチェーンシステム３０内のいずれかのノードに送信する。またトランザクション生成部２２０は、生成した電力供給権トランザクションレコードを、電力供給権の譲渡先の電力設備（例えば仮想発電設備）を運用するユーザ（例えば小売電気事業者）のノードへ送信する。

【００７２】

発電事業者４１ａ以外の発電事業者４１ｂ，・・・が有するノード２００ａ，・・・も、ノード２００と同様の機能を有する。

電力消費者４２ａのノード３００は、スマートメータレコード提供部３１０と非化石証書管理部３２０とを有する。

【００７３】
スマートメータレコード提供部３１０は、電力消費設備５２ａ（図２参照）に取り付けられたスマートメータ５３ｃから、電力消費設備５２ａにおける消費電力の時間遷移を示すスマートメータレコードを定期的に取得する。スマートメータレコード提供部３１０は、電力消費設備５２ａで消費した電力分の電力供給権を有する小売電気事業者から電力の共有を受ける契約を結んだ場合に、その小売電気事業者のノードに取得したスマートメータレコードを送信する。
【００７４】
非化石証書管理部３２０は、非化石エネルギーで発電された電力の販売する権利を購入した場合に、その電力の販売元から非化石証書を取得する。非化石証書管理部３２０は、取得した非化石証書をメモリまたはストレージ装置に格納する。そして非化石証書管理部３２０は、非化石エネルギーで発電された電力を消費したことを第三者（例えば非化石価値検証者４４）に非化石証書を送信する。
【００７５】
電力消費者４２ａ以外の電力消費者４２ｂ，・・・が有するノード３００ａ，・・・（図２参照）も、ノード３００と同様の機能を有する。
小売電気事業者４３ａのノード１００は、スマートメータレコード管理部１１０、マッチング部１２０、トランザクション生成部１３０、トランザクション記憶部１４０、および非化石証書発行部１５０を有する。
【００７６】
スマートメータレコード管理部１１０は、小売電気事業者４３ａが、電力供給権に基づく電力共有契約を締結したことを示す情報の入力に応じて、その電力供給権に対応する物理発電設備と電力供給先の電力消費設備とのスマートメータレコードとを取得する。スマートメータレコード管理部１１０は、取得したスマートメータレコードをメモリ１０２またはストレージ装置１０３に格納する。
【００７７】
マッチング部１２０は、電力供給契約の対象となる電力供給権に対応する物理発電設備の発電実績と電力消費設備の電力消費実績の整合性を検証する。整合性が確認できた場合、トランザクション生成部１３０に電力供給権トランザクションレコードの生成を指示する。
【００７８】
トランザクション生成部１３０は、取引された総電力量を示す総電力量コミットメントと、発電実績と電力消費実績との整合性がとれていることを証明するゼロ知識証明とを含む電力供給権トランザクションレコードを生成する。そしてトランザクション生成部１３０は、生成した電力供給権トランザクションレコードを、ブロックチェーンシステム３０内のいずれかのノードに送信する。またトランザクション生成部１３０は、電力供給権トランザクションレコードの生成に使用した情報をトランザクション記憶部１４０に格納する。さらにトランザクション生成部１３０は、電力供給権の譲渡先の電力設備（例えば他の仮想発電設備）を運用するユーザ（例えば他の小売電気事業者）のノードへ、生成した電力供給権トランザクションレコードを送信する。
【００７９】
トランザクション生成部１３０は、他のノードからそのノードが生成した電力供給権トランザクションレコードを受信した場合、受信した電力供給権トランザクションレコードをトランザクション記憶部１４０に格納する。
【００８０】
トランザクション記憶部１４０は、トランザクション生成部１３０が生成した電力供給権トランザクションレコードを記憶する。またトランザクション記憶部１４０は、他のノードからノード１００に送信された電力供給権トランザクションレコード（ノード１００に対応する仮想発電設備を電力供給権の譲渡先とする電力供給権トランザクションレコード）を記憶する。

【００８１】
非化石証書発行部１５０は、非化石エネルギーで発電された電力の電力供給権の販売先の電力消費者からの依頼に応じて、非化石証書を発行する。例えば非化石証書発行部１５０は、トランザクション記憶部１４０に格納されている電力供給権トランザクションレコードに基づいて非化石証書を生成する。そして非化石証書発行部１５０は、生成した非化石証書を、発行を依頼した電力消費者のノードへ送信する。
【００８２】
小売電気事業者４３ａ以外の小売電気事業者４３ｂ，・・・が有するノード１００ａ，・・・（図２参照）も、ノード１００と同様の機能を有する。
ブロックチェーンシステム３０を構成するノード４００は、スマートコントラクト４１０とブロックチェーンプラットフォーム４２０とを有する。
【００８３】
スマートコントラクト４１０は、ブロックチェーンを用いた取引契約を自動で実行する。例えばスマートコントラクト４１０は、電力供給権トランザクションレコードを受信すると、そのトランザクションレコードに示される取引内容に基づいて、予め設定されている取引の成約条件が満たされたか否かを検証する。そしてスマートコントラクト４１０は、取引の成約条件が満たされた場合、電力供給権トランザクションレコードのブロックチェーンプラットフォーム４２０への格納処理を行う。
【００８４】
ブロックチェーンプラットフォーム４２０は、ブロックチェーンシステム３０内の他のノード４００ａ，・・・と連係し、ブロックチェーンの仕組みを用いて電力供給権の取引の台帳を管理する。例えばブロックチェーンプラットフォーム４２０は、スマートコントラクト４１０から受信した電力供給権トランザクションレコードを含むブロックを、ブロックチェーンの新たなブロックとして追加する。ブロックチェーンプラットフォーム４２０は、ブロックチェーンにブロックを追加した場合、ブロックチェーンシステム３０を構成する他のノード４００ａ，・・・にブロックチェーンを送信し、ブロックチェーンを分散管理する。
【００８５】
ブロックチェーン記憶部４２１は、電力供給権の取引を示すブロックチェーンを記憶する。例えばブロックチェーン記憶部４２１には、スマートコントラクト４１０またはブロックチェーンシステム３０を構成する他のノード４００ａ，・・・で更新されたブロックチェーンが格納される。
【００８６】
ブロックチェーンシステム３０を構成するノード４００以外のノード４００ａ，・・・も、ノード４００と同様の構成を有する。
なお、図４に示した各要素間を接続する線は通信経路の一部を示すものであり、図示した通信経路以外の通信経路も設定可能である。例えばブロックチェーンシステム３０で管理しているブロックチェーンは公開情報であり、ブロックチェーンシステム３０外のいずれのノードからも参照可能である。また、図４に示した各ノード内の各要素の機能は、例えば、その要素に対応するプログラムモジュールをコンピュータに実行させることで実現することができる。
【００８７】
＜電力供給権の取引の概要＞
図５は、電力供給権の取引の概要を示す図である。図５に示すように、電力供給権の取引はブロックチェーン６０内で管理される。他方、発電実績と電力消費実績は、ブロックチェーン６０外で管理される。
【００８８】
前述の電力供給権に求められる要件のうち、非中央集権性はブロックチェーン６０を利用することにより達成できる。トレーサビリティおよびダブルカウント防止はブロックチェーン６０においてＵＴＸＯ（Unspent Transaction Output）方式を用いた電力供給権

管理を行うことで達成される。

【００８９】

ＵＴＸＯ方式は、あるユーザ（例えば小売電気事業者）の未使用トランザクションを合計することで、そのユーザの有する権利（例えば電力供給権）の総量を算出するものである。ＵＴＸＯ方式を採用すると、電力供給権の譲渡を表す電力供給権トランザクションレコードにおいて、譲渡元のユーザが有する電力供給権がインプットに設定される。その電力供給権トランザクションレコードのアウトプットに、譲渡する電力供給権が設定される。あるユーザがアウトプットで指定された電力供給権のうち、他の電力供給権トランザクションレコードのインプットとして使用されていない電力供給権が、そのユーザから他のユーザに移譲されていない（自身が保有している）電力供給権を表す。

【００９０】

ＵＴＸＯ方式においては、同じリソースを異なる複数の他者に譲渡することはできない。そのためＵＴＸＯ方式で電力供給権を取引することで、電力供給権の取引のダブルカウントの防止が可能となる。またＵＴＸＯ方式では、インプットとアウトプットの形式で電力供給権の譲渡人と譲受人とが電力供給権トランザクションレコードに示される。その結果、電力供給権の取引の履歴を正しく追跡できる（トレーサビリティの要件が満たされる）。

【００９１】

ストレージコストの要件は、スマートメータレコード７５ａ，７５ｂ，・・・，７６ａ，７６ｂ，・・・，７７ａ，７７ｂ，・・・を集約した電力マッチングレコード７８をブロックチェーン６０に登録することで達成される。スケーラビリティーの要件は、取引対象の電力供給権に対応する物理発電設備の発電実績と譲受人の電力消費設備の電力消費実績とのマッチングをブロックチェーン６０外で行うことで達成できる。

【００９２】

さらにブロックチェーンシステム３０外の各ノードがスマートメータレコードを秘密に管理する。そしてブロックチェーンシステム３０外の各ノードは、コミットメントスキームを用いて総電力供給量を隠蔽するとともに、マッチング結果の正当性をゼロ知識証明７８ｂによって証明する。これによりプライバシーの保護が達成される。

【００９３】

図５には、物理発電設備Ａと物理発電設備Ｂの電力供給権を小売電気事業者が取得し、その小売電気事業者が電力消費設備Ｇを有する電力消費者へ、電力供給権を譲渡する場合の例が示されている。なおシステム上は、小売電気事業者が仮想発電設備Ｄを運用しているものとして扱われる。このような取引の概略を以下に示す。

【００９４】

ブロックチェーンシステム３０において、電力供給権を管理する台帳がブロックチェーン６０で生成される。電力供給管理は、多くの場合、一ヶ月といったまとまった期間で行われるためデータ量は膨大にはならない。従って、電力供給権の取引に関するすべての電力供給権トランザクションレコードをブロックチェーン６０上で管理する。

【００９５】

例えばブロック６１には、物理発電設備Ａを有する発電事業者が電力供給権７１を有し、物理発電設備Ｂを有する発電事業者が電力供給権７２を有することが記録されているものとする。電力供給権７１，７２には、物理発電設備で発電予定の電力と発電期間が設定されている。

【００９６】

仮想発電設備Ｄを有する小売電気事業者は、各発電事業者との間で電力供給権７１，７２の譲渡契約を結ぶ。この譲渡契約は、例えば電力供給権７１，７２に設定された発電期間の開始前に行われる。譲渡契約が結ばれると、発電事業者は自身の有するノードを用いて電力供給権７１，７２の譲渡内容を示す電力供給権トランザクションレコード７０ａ，７０ｂを生成する。そして各発電事業者のノードは、電力供給権トランザクションレコード７０ａ，７０ｂをブロックチェーンシステム３０内のノードに送信する。

【００９７】
ブロックチェーンシステム３０では、電力供給権トランザクションレコード７０ａ，７０ｂの内容が正当であることを確認後、電力供給権トランザクションレコード７０ａ，７０ｂを含む新たなブロック６２をブロックチェーン６０に登録する。ブロック６２には、２つの電力供給権７１，７２を包含する電力供給権７３を、仮想発電設備Ｄを運用する小売電気事業者が有していることが示される。またブロック６２には、前のブロック６１のハッシュ値が含まれる。これにより取引履歴の改ざんが抑止される。
【００９８】
なお、ブロックチェーンシステム３０では、発電実績のダブルカウントを防止するために、各物理発電設備の各時刻の電力供給権が複数の異なる電力消費設備に割り当てられることがないように、ＵＴＸＯ方式で電力供給権の取引を管理する。
【００９９】
次に仮想発電設備Ｄを運用する小売電気事業者は、電力消費設備Ｇを有する電力消費者との間で電力供給権７３に基づく電力の供給を結ぶ。電力供給権７１，７２に設定されていた発電期間が終了すると、仮想発電設備Ｄを運用する小売電気事業者は、自身の有するノードによりスマートメータレコード７５ａ，７５ｂ，・・・，７６ａ，７６ｂ，・・・，７７ａ，７７ｂ，・・・を収集する。以下仮想発電設備Ｄを運用するのは小売電気事業者４３ａ（図２参照）であり、その小売電気事業者４３ａはノード１００を用いて電力供給権の取引を行うものとする。
【０１００】
スマートメータレコード７５ａ，７５ｂ，・・・，７６ａ，７６ｂ，・・・，７７ａ，７７ｂ，・・・には、譲渡する電力供給権７３に示される発電期間分の一定時間（例えば３０分）間隔の発電および電力消費実績が示される。小売電気事業者４３ａのノード１００は、物理発電設備Ａと物理発電設備Ｂとのスマートメータレコード７５ａ，７５ｂ，・・・，７６ａ，７６ｂ，・・・に基づいて、取引の対象となる発電期間における一定時間間隔の発電量（発電実績）を算出する。またノード１００は、電力消費設備Ｇのスマートメータレコード７７ａ，７７ｂ，・・・に基づいて、取引の対象となる発電期間における一定時間間隔の電力消費量（電力消費実績）を算出する。
【０１０１】
次にノード１００は、電力発電実績と電力消費実績のマッチングが正しいことを示す電力マッチングレコード７８を生成し、ブロックチェーンシステム３０に送信する。電力マッチングレコード７８には、総電力供給量を隠蔽するために、総電力供給量についてのコミットメント（総電力量コミットメント７８ａ）が含まれる。また電力マッチングレコード７８には、譲渡された電力供給権７３に対応する物理発電設備Ａ，Ｂの発電実績と、譲渡先の電力消費設備Ｇの電力消費実績との整合性が採れていることを証明するゼロ知識証明７８ｂが含まれる。
【０１０２】
電力マッチングレコード７８を受信したブロックチェーンシステム３０は、電力マッチングレコード７８を含むブロック６３をブロックチェーン６０に登録する。この際、ブロックチェーンシステム３０は、電力消費者への電力供給権７３の譲渡に関する電力供給権トランザクションレコード７０ｃに示される電力消費設備Ｇへの電力供給権７４に対応するＵＴＸＯに、電力マッチングレコード７８を関連付ける。
【０１０３】
このように、３０分単位の大量のスマートメータレコードの代わりに、集約した電力マッチングレコード７８がブロックチェーン６０に記録される。これによりブロックチェーン６０のスケーラビリティーおよびストレージコストの問題が解決する。このとき、ブロックチェーン６０の内部データと外部データが整合性を持つことを、スマートメータレコードを開示せずに証明するために、ゼロ知識証明７８ｂが利用される。これにより発電事業者の発電実績や電力消費者の電力消費実績の秘匿状態が守られ、プライバシーの問題も解決される。

【０１０４】
なお、電力マッチングレコード７８をブロックチェーン６０に記録する際に、スマートコントラクト４１０がゼロ知識証明の検証を行う。そのため、不正な電力マッチングレコードがブロックチェーン６０上に記録されることを抑止することができる。
【０１０５】
＜電力供給権の取引へのＵＴＸＯ方の適用＞
次にＵＴＸＯ方式による電力供給権の取引について具体的に説明する。
図６は、電力供給権の取引の一例を示す図である。電力供給権７１～７４は、電力を供給する権利を有する発電期間と、その期間に発電する予定の電力とによって、供給できる電力が示される。横軸を時刻、縦軸を電力とするグラフで表すと、電力供給権７１～７４それぞれで供給可能な電力が矩形で表される。仮想発電設備Ｄで供給可能な電力は、物理発電設備Ａと物理発電設備Ｂとのそれぞれで供給可能な電力の合計となる。
【０１０６】
電力供給権７３の発電可能な電力の一部を、電力消費設備Ｇを運用する電力消費者に譲渡する場合、仮想発電設備Ｄで供給可能な電力を示す矩形の範囲内の電力が、電力供給権７４として電力消費設備Ｇに譲渡される。
【０１０７】
このようにブロックチェーンシステム３０では、取引対象の電力供給権が時刻と電力に基づいた二次元の情報で特定され、ＵＴＸＯ方式を利用して管理される。電力供給権の管理は、多くの場合、一ヶ月といったまとまった期間で行われる。そのため、データ量が膨大にはならない。従って、すべての電力供給権トランザクションレコードをブロックチェーン６０上で管理することが可能である。
【０１０８】
ＵＴＸＯ方式を採用しているため、ブロックチェーンシステム３０は同じリソース（期間とその期間内の電力とで表される矩形領域の電力）を複数の異なるユーザに譲渡することが許容されない。そのため、各物理発電設備の各時刻の電力供給が複数の異なる電力消費設備に割り当てられることがなくなり、発電実績のダブルカウントを防止することができる。ブロックチェーン６０において、電力消費設備Ｇの消費電力の分として譲渡された電力供給権７４を示す電力供給権トランザクションレコードには電力マッチングレコード７８が関連付けられる。
【０１０９】
＜発電実績と電力消費実績との電力供給権との関連付け＞
電力供給権トランザクションレコードは、電力供給権の譲渡が行われたことを示すトランザクションであり、実際の電力の供給ルートとは異なる。例えば仮想発電設備は電力を供給する権利を別の電力会社に転売することができる。この転売は、理論上、無限回数分繰り返すことができる。最終的に、ある仮想発電設備から電力消費設備への電力供給権を譲渡する電力供給トランザクションレコードの登録により譲渡の流れが終了する。
【０１１０】
従って、ＵＴＸＯの関係を示すグラフの末端は必ず電力消費設備となる。またそのグラフにおいて、電力消費設備の一つ手前は、最終的にその電力消費設備に対して電力供給した仮想発電設備となる。
【０１１１】
電力供給権トランザクションレコードは、電力供給権の譲渡を意味するため、原則として実際の発電時刻より前にブロックチェーンに記録される。しかし、発電実績と電力消費実績は、いずれもその時になってみないと分からない不確定な量である。従って電力消費設備への電力供給権の譲渡を示す電力供給権トランザクションレコードについては、権利の対象となる総電力供給期間の後にブロックチェーン６０に登録することができる。なお電力消費設備への電力供給権の譲渡を示す電力供給権トランザクションレコードを総電力供給期間の前に登録しておき、総電力供給期間の経過後に電力供給権の再譲渡を行うことで、事後的に電力供給権で消費された電力量の調整を行ってもよい。

【０１１２】
電力消費設備へ電力供給権を譲渡する仮想発電設備を運用する小売電気事業者のノード１００は、取引された電力供給権の総電力供給期間の経過後、電力発電実績と電力消費実績のマッチング結果を意味する電力マッチングレコード７８を生成する。そしてノード１００は、生成した電力マッチングレコード７８を、電力消費設備への電力供給権の譲渡を示す電力供給権トランザクションレコードに関連付けて、ブロックチェーン６０に登録する。
【０１１３】
なお電力マッチングレコード７８にはゼロ知識証明７８ｂが含まれ、ゼロ知識証明７８ｂがスマートコントラクト４１０で検証される。これにより、電力マッチングレコード７８は適切な電力消費設備の適切なＵＴＸＯに対してしか関連付けることができない。
【０１１４】
なお図６の例では、電力供給権７１と電力供給権７２それぞれの一部の電力が電力供給権７４の電力となっている。ＵＴＸＯ方式の場合、電力供給権７１と電力供給権７２の一部を譲渡した場合、譲渡した後に残った電力の分の電力供給権は、自分自身へ譲渡する電力供給権トランザクションレコードによって譲渡元の権利として残される。
【０１１５】
＜電力供給権の取引例＞
以下、図７と図８を参照して、電力供給権の取引例について説明する。
図７は、電力供給権の取引の第１の例を示す図である。図７の例では物理発電設備Ａ，Ｂ，Ｃそれぞれから仮想発電設備Ｄへ電力供給権が譲渡されている。そして仮想発電設備Ｄが有する電力供給権に基づいて、電力消費設備Ｇへの電力供給契約が結ばれている。このとき物理発電設備Ａ，Ｂ，Ｃの発電実績が電力消費設備Ｇの電力消費実績を大きく上回っている。この場合、仮想発電設備Ｄから自分自身へ余剰分の電力供給権を譲渡（仮想通貨のおつりに相当）する電力供給権トランザクションレコードと、仮想発電設備Ｄから電力消費設備Ｇへの電力供給を示す電力供給権トランザクションレコードとが生成される。
【０１１６】
仮想発電設備Ｄから電力消費設備Ｇへの電力供給を示す電力供給権トランザクションレコードには電力マッチングレコード７９ａが付与される。そして電力マッチングレコード７９ａを含む電力供給権トランザクションレコードがブロックチェーン６０に登録される。
【０１１７】
図７では、電力供給権の取引における左側の設備がＵＴＸＯのインプットの対象であり、右側の設備がＵＴＸＯのアウトプットの対象である。発電後に電力供給権トランザクションレコードのアウトプットに対応する電力供給権を所有する仮想発電設備を運用する小売電気事業者のノードだけが、その電力供給権に対応する期間の電力マッチングを行うことができる。つまり、小売電気事業者のノードは、電力供給権トランザクションレコードのインプットで指定したＵＴＸＯの一部に対して電量マッチングを行う。そして小売電気事業者のノードは、その電力マッチングに関するデータセットを電力供給権トランザクションレコードのアウトプットフィールドに追加することができる。結果的に、該当する「ＵＴＸＯの一部」は電力マッチングにより消滅し、電力供給権はターミネートする（以後、誰にも譲渡できなくなる）。
【０１１８】
図８は、電力供給権の取引の第２の例を示す図である。図８の例では物理発電設備Ａ，Ｂ，Ｃそれぞれから仮想発電設備Ｑへ電力供給権が譲渡されている。さらに仮想発電設備Ｑから仮想発電設備Ｒへ電力供給権が譲渡されている。そして仮想発電設備Ｒが有する電力供給権に基づいて、電力消費設備Ｇへの電力供給契約が結ばれている。
【０１１９】
仮想発電設備Ｒから電力消費設備Ｇへ電力供給権を譲渡する電力供給権トランザクションレコードには電力マッチングレコード７９ｂが付与される。そして電力マッチングレコード７９ｂを含む電力供給権トランザクションレコードがブロックチェーン６０に登録さ

れる。なお電力消費設備Ｇへの電力供給を示す電力供給権トランザクションレコードはターミネートし、その後、該当する電力供給権を譲渡することはできなくなる。

【０１２０】

図８に示すように、複数の仮想発電設備を介して電力供給権が電力消費設備に譲渡される場合がある。物理発電設備と電力消費設備との間に介在する仮想発電設備の数は３以上の場合もあり得る。

【０１２１】

電力供給権を譲渡する側のノードは、電力供給権トランザクションレコードをブロックチェーンに書き出すと同時に、譲渡する相手のノードに電力供給権トランザクションレコードの内容を送信する。従って小売電気事業者のノードは、自身が譲渡先となる電力供給権トランザクションレコードのデータをすべてローカルで保持・管理している。

【０１２２】

＜電力供給トランザクションレコード＞

電源供給権トランザクションレコードのデータ構造は、インプットとアウトプットの種別に応じて異なる。例えば図７、図８では電力供給権の譲渡元の名称に隣接してインプットの種別が示されており、譲渡先の名称に隣接してアウトプットの種別が示されている。

【０１２３】

図９は、電源供給権トランザクションレコードのデータ構造の一例を示す図である。電力供給権トランザクションレコード８０のインプット８１の種別には、譲渡元電力設備自身の発電に基づく新規電力供給権のインプット（ｉ１）と譲渡に基づく電力供給権のインプット（ｉ２）がある。新規電力供給権は、物理発電設備を運用する発電事業者のノードが発行する電力供給権である。譲渡に基づく電力供給権は、仮想発電設備を運用する小売電気事業者のノードが発行する電力供給権である。インプット８１の種別ごとのインプット８１の内容は以下の通りである。

【０１２４】

［譲渡元電力設備自身の発電に基づく新規電力供給権のインプット（ｉ１）］

新規電力供給権の電源供給権トランザクションレコードには、譲渡元の物理発電設備ＩＤ、譲渡元の物理発電設備の発電に基づく電力供給権を表す矩形領域（発電期間×電力）、および譲渡元の物理発電設備による電子署名が含まれる。

【０１２５】

［譲渡に基づく電力供給権のインプット（ｉ２）］

譲渡に基づく電力供給権の電源供給権トランザクションレコードには、電力供給権を譲り受けた際の電力供給権トランザクションレコード、その電源供給権トランザクションレコード内の電力供給権のアウトプット番号、譲渡元の電力設備による電子署名が含まれる。

【０１２６】

電力供給権トランザクションレコード８０のアウトプット８２の種別には、電力消費設備以外（例えば仮想発電設備）に電力供給権を譲渡した場合のアウトプット（ｏ１）と、電力消費設備に電力供給権を譲渡した場合のアウトプット（ｏ２）とがある。電力消費設備に電力供給権を譲渡した場合とは、電力供給権がターミネートする場合である。アウトプット８２の種別ごとのアウトプット８２の内容は以下の通りである。

【０１２７】

［電力消費設備以外に電力供給権を譲渡した場合のアウトプット（ｏ１）］

電力消費設備以外に電力供給権を譲渡する電源供給権トランザクションレコードには、譲渡先電力設備ＩＤ、物理発電設備ＩＤ、および電力供給権を表す矩形領域（発電期間×電力）が含まれる。

【０１２８】

［電力消費設備に電力供給権を譲渡した場合のアウトプット（ｏ２）］

電力消費設備に電力供給権を譲渡する電源供給権トランザクションレコードには、電力消費設備ＩＤと電力マッチングレコードとが含まれる。電力マッチングレコードは、スマートメータレコードに基づいて生成される情報である。

【０１２９】
以上が、電力供給トランザクションレコードの内容である。
＜スマートコントラクト＞
ブロックチェーン６０に記録される電力供給トランザクションレコードの内容の正当性は、ブロックチェーンシステム３０におけるスマートコントラクト４１０によって保証される。例えば各電力供給権トランザクションレコードがＵＴＸＯ方式の原則（アウトプットをインプットの総量の範囲内で生成する）を守るようにスマートコントラクト４１０が制御する。これにより電力供給権のダブルカウントを防止することができる。以下にスマートコントラクトの検証内容を示す。
【０１３０】
［スマートコントラクトへの入力値］
・電力供給権トランザクションレコード
［スマートコントラクトの検証項目］
・電力供給権トランザクションレコードのインプットの電子署名の正当性の検証
・値の範囲の正当性の検証（以下の４項目の検証）
－認証機関の署名付きの譲渡先電力設備ＩＤがブロックチェーンに登録されていること。
－認証機関の署名付きの物理発電設備ＩＤがブロックチェーンに登録されていること。
－認証機関の署名付きの電力消費設備ＩＤがブロックチェーンに登録されていること（電力供給権のターミネートの場合のみ）。
－電力供給権を表す全ての矩形領域が正常な値の範囲に存在すること。
・電力供給権のダブルカウントが発生していないことの検証（以下の３項目の検証）。
－電力供給権トランザクションレコードのアウトプットで譲渡される電力供給権を表す各矩形領域が、電力供給権トランザクションレコードのインプットの電力供給権を表す全ての矩形領域の和集合の中に含まれること。
－異なる二つの電力供給権トランザクションレコードのアウトプットの電力供給権を表す矩形領域のペアのうち、重なるものが存在しないこと。
－各電力供給権トランザクションレコードのインプットの新規電力供給権と物理発電設備が同じでかつ矩形領域が重なる新規電力供給権が一つもブロックチェーン６０上に記録されていないこと（譲渡元が物理発電設備の場合のみ）。
・電力マッチングレコードのマッチング正当性証明の検証（電力供給権のターミネートの場合のみ）。
【０１３１】
以上がスマートコントラクト４１０における検証内容である。スマートコントラクト４１０がマッチング正当性証明を検証することで、発電実績や電力消費実績を示すスマートメータレコードの内容を秘匿したままでも、取引の正当性を保証することができる。
【０１３２】
＜電力マッチング＞
電力マッチングは、譲渡される電力供給権に対応する物理発電設備における総電力供給期間の発電実績と、譲渡先の電力消費者が運用する電力設備における総電力供給期間の電力消費実績の整合性を検証することである。発電実績と電力消費実績とは、スマートメータレコードに基づいて判断される。そして電力マッチングの結果が電力マッチングレコードに設定される。
【０１３３】
図１０は、スマートメータレコードと電力マッチングレコードとに含まれる情報の一例を示す図である。例えば物理発電設備に取り付けられたスマートメータ５３ａは、取り付け先の物理発電設備を識別する物理発電設備ＩＤ、発電期間、発電量、電子署名が含まれるスマートメータレコード７５ａ，７５ｂ，・・・を定期的に生成する。スマートメータレコード７５ａ，７５ｂ，・・・の生成周期は例えば３０分である。その場合、スマートメータレコード７５ａ，７５ｂ，・・・に示される発電期間の長さも３０分となる。発電量は、発電期間の間に発電された電力量である。電子署名は、スマートメータレコードの

内容に誤りがないことを示す物理発電設備の電子署名である。物理発電設備に取り付けられた他のスマートメータ５３ｂも、同様の内容のスマートメータレコード７６ａ，７６ｂ，・・・を生成する。

【０１３４】

電力消費設備に取り付けられたスマートメータ５３ｃは、取り付け先の電力消費設備を識別する電力消費設備ＩＤ、消費期間、消費量、および電子署名を含むスマートメータレコード７７ａ，７７ｂ，・・・を定期的に生成する。スマートメータレコード７７ａ，７７ｂ，・・・の生成周期は例えば３０分である。その場合、スマートメータレコード７７ａ，７７ｂ，・・・に示される消費期間の長さも３０分となる。消費量は、消費期間の間に消費した電力量である。電子署名は、スマートメータレコードの内容に誤りがないことを示す電力消費設備の電子署名である。

【０１３５】

ここでスマートメータ５３ａ，５３ｂ，５３ｃは信頼できるものとする。すなわちスマートメータ５３ａ，５３ｂ，５３ｃが電子署名を付与したスマートメータレコードに記録された発電量や電力消費量を含むすべてのデータは、信頼できるものとする。なお、電力設備ＩＤ（物理電力設備ＩＤおよび電力消費設備ＩＤを含む）は一定のビット幅を持つランダム値であり、仮名性（pseudonym）を持つものとする。

【０１３６】

物理発電設備のスマートメータレコード７５ａ，７５ｂ，・・・，７６ａ，７６ｂ，・・・と電力消費設備のスマートメータレコード７７ａ，７７ｂ，・・・とを集約することで、電力マッチングレコード７８が生成される。電力マッチングレコード７８には、電力消費設備ＩＤ、総電力供給期間、総電力量コミットメント、マッチング証明、および最終仮想発電設備による電子署名が含まれる。マッチング証明は、電力マッチングが正しく行われたことを証明する情報である。マッチング証明には、例えばゼロ知識証明が用いられる。

【０１３７】

電力マッチングレコード７８を生成するノードは、電力マッチングを行う。電力マッチングは、物理発電設備の発電実績と電力消費設備の電力消費実績とを照らし合わせ、電力消費実績に相当する電力が、取引の対象となっている電力供給権に対応する物理発電設備で発電できていることを確認する処理である。

【０１３８】

図１１は、電力マッチングの一例を示す図である。図１１には、総電力供給期間における物理発電設備Ａ，Ｂ，Ｃで発電した電力の電力供給権を電力消費設備Ｇに譲渡する場合の電力マッチングの例が示されている。２０２１年５月４日の６：００からの所定期間が総電力供給期間となっている。電力マッチングは、スマートメータレコードにおける発電期間単位（図１１の例では３０分）で行われる。

【０１３９】

例えば６：００から６：３０の期間の電力消費設備Ｇの電力消費実績（３０分間の消費電力）は６．８ｋｗである。同じ期間の物理発電設備Ａの発電実績は３．０ｋｗ、物理発電設備Ｂの発電実績は２．０ｋｗ、物理発電設備Ｃの発電実績は１．８ｋｗである。電力マッチングを行うノードは、物理発電設備の発電実績の合計が、電力消費設備の電力消費実績と等しいこと、または発電実績が電力消費実績以上であることを確認する。６：００から６：３０の期間の発電実績の合計が６．８ｋｗであり、電力消費設備Ｇの電力消費実績分の電力が物理発電設備で発電されている。

【０１４０】

６：３０から７：００の期間の電力消費設備Ｇの電力消費実績は９．９ｋｗである。同じ期間の物理発電設備Ａの発電実績は５．１ｋｗ、物理発電設備Ｂの発電実績は２．１ｋｗ、物理発電設備Ｃの発電実績は２．７ｋｗである。６：３０から７：００の期間の発電実績の合計が９．９ｋｗであり、電力消費設備Ｇの電力消費実績分の電力が物理発電設備で発電されている。

【０１４１】
７：００から７：３０の期間の電力消費設備Ｇの電力消費実績は７．７ｋｗである。同じ期間の物理発電設備Ａの発電実績は３．９ｋｗ、物理発電設備Ｂの発電実績は２．０ｋｗ、物理発電設備Ｃの発電実績は１．８ｋｗである。７：００から７：３０の期間の発電実績の合計が７．７ｋｗであり、電力消費設備Ｇの電力消費実績分の電力が物理発電設備で発電されている。
【０１４２】
総電力供給期間内の３０分単位のすべての期間について、電力消費設備Ｇの電力消費実績分の電力が物理発電設備で発電されていることが確認できたら、電力マッチングを行うノードは電力マッチングレコード７８を生成する。さらにそのノードは、生成した電力マッチングレコードをアウトプットに含む電力供給権トランザクションレコード８０を生成する。そして生成された電力供給権トランザクションレコード８０がブロックチェーン６０に登録される。
【０１４３】
このように、電力を販売する小売電気事業者のノードは、物理発電設備によって供給された電力と電力消費設備によって消費された電力を、３０分単位でマッチングさせる。ただし、２００万件分のスマートメータレコードをすべてブロックチェーン６０に記録することはできない。そのため小売電気事業者のノードは、電力マッチングごとに、関連する発電実績と電力消費実績とのスマートメータレコードを集約して電力マッチングレコードを生成し、電力マッチングレコードのみをブロックチェーン６０に記録する。このとき小売電気事業者のノードは、電力マッチングレコードに関連するすべてのデータをローカルのメモリまたはストレージ装置に保存する。
【０１４４】
次にマッチング正当性証明について詳細に説明する。小売電気事業者は、自身のノードを使用して、電力マッチングの正当性に関するゼロ知識証明を生成する。マッチング正当性証明の仕様は、以下の通りである。
【０１４５】
＜マッチング正当性証明＞
マッチング正当性証明は、公開入力値と秘匿入力値に基づいて、所定の命題が正しいことを証明する値である。公開入力値は以下の通りである。
【０１４６】
［公開入力値］
・物理発電設備ＩＤの集合
・電力消費設備ＩＤ
・物理発電設備と電力消費設備の電子署名の検証鍵
・総電力供給期間
・総電力量コミットメント
以上が公開入力値である。総電力量コミットメントは、コミットメントスキームに基づくコミットメント関数（$COMM_r(x)$）の関数値である。ｒはコミットメント乱数であり、ｘは総電力消費量である。コミットメント関数は、コミットメント乱数の値が異なれば異なる値を生成する。またある１つの総電力量コミットメントを生成するコミットメント乱数と総電力消費量との組み合わせは、１種類しか存在しない。
【０１４７】
秘匿入力値は以下の通りである。
［秘匿入力値］
・譲渡される電力供給権に対応するすべての物理発電設備の総電力供給期間内のすべてのスマートメータレコード（物理発電設備ＩＤ、発電期間、発電量、物理発電設備の電子署名を含む）
・電力供給権の譲渡先となる電力消費設備の総電力供給期間内のすべてのスマートメータレコード（電力消費設備ＩＤ、発電期間、電力消費量、電力消費設備の電子署名を含む）

・コミットメント乱数
以上が秘匿入力値である。マッチング正当性証明の命題は、以下のすべての命題を同時に満たすことである。
【０１４８】
［命題］
・すべての物理発電設備のすべてのスマートメータレコードの物理発電設備ＩＤが正しいこと。
・電力消費設備のすべてのスマートメータレコードの電力消費設備ＩＤが正しいこと。
・譲渡される電力供給権に対応するすべての物理発電設備について、物理発電設備から得られたスマートメータレコードの発電期間が総電力供給期間をカバーしていること。
・電力供給権の譲渡先となる電力消費設備のスマートメータレコードの消費期間が、総電力供給期間をカバーしていること。
・すべての物理発電設備のすべてのスマートメータレコードの電子署名が正しいこと。
・電力消費設備のすべてのスマートメータレコードの電子署名が正しいこと。
・総電力供給期間内の３０分単位のすべての単位期間について、電力消費設備のスマートメータレコードに示される発電量（発電実績）の和が、同じ単位期間の電力消費設備のスマートメータレコードに示される消費電力量（電力消費実績）と等しくなること。
・電力消費設備のすべてのスマートメータレコードの電力消費量の和をコミットメント関数の変数としたときのコミットメント関数の値が、総電力量コミットメントと等しくなること。すなわち電力消費設備のすべてのスマートメータレコードの電力消費量の和をΣとし、総電力量コミットメントをｃｍとしたとき、$COMM_e(\Sigma) = cm$となること。
【０１４９】
以上がマッチング正当性証明の命題である。物理発電設備ＩＤまたは電力消費設備ＩＤが正しいことは、例えば設備ＩＤを証明する認証機間から設備ＩＤを証明する署名を取得することで確認できる。またスマートメータレコードの電子署名が正しいことは、例えばスマートメータレコードの所定のハッシュ関数によるハッシュ値と、電子署名を物理発電設備の公開鍵で復号した値との比較によって確認できる。比較の結果一致していれば、電子署名は正しいと判断できる。
【０１５０】
以上の命題を証明するゼロ知識証明が、マッチング正当性証明である。このようなゼロ知識証明としては、例えば非対話型のゼロ知識証明が用いられる。非対話型のゼロ知識証明としてはｚｋ－ＳＮＡＲＫ（Zero-Knowledge Succinct Non-Interactive ARgument of Knowledge）がある。
【０１５１】
ｚｋ－ＳＮＡＲＫを用いた場合には、信頼できる第三者機関により、事前設定としてＣＲＳ（Common Reference String）が生成される。トランザクション生成部１３０は、ＣＲＳと命題とその命題が真である証拠とに基づいて所定の計算を行い、ゼロ知識証明Πを生成する。ブロックチェーンシステム３０のスマートコントラクト４１０は、ＣＲＳ、命題、およびゼロ知識証明Πを用いて検証の計算を行い、結果が１となれば命題が真であることが証明されたと判断する。
【０１５２】
非対話型のゼロ知識証明には、ｚｋ－ＳＮＡＲＫ以外に例えばｚｋ－ＳＴＡＲＫ（Zero-Knowledge Succinct Transparent ARgument of Knowledge）がある。ｚｋ－ＳＴＡＲＫを用いれば信頼できる第三者機関が不要となる。
【０１５３】
マッチング正当性証明は、スマートコントラクト４１０により検証される。スマートコントラクト４１０は、例えば電力マッチングレコードに基づいて以下の検証を行う。
・電力消費設備に電力供給した仮想発電設備による電子署名の正当性
・マッチング対象ＵＴＸＯの正当性（実在するＵＴＸＯを指していること）
・総電力供給期間の正当性（異常値ではないこと、他の電力マッチングレコードとの期間

の重複が存在しないこと（電力マッチングのダブルカウントが発生していないこと））
・マッチング正当性証明の正当性（ゼロ知識証明の命題が真となること）
スマートコントラクト４１０は、以上の内容がすべて正しいと検証できた場合、電力マッチングレコードを含む電力供給権トランザクションレコードをブロックチェーン６０に登録する。
【０１５４】
＜非化石証書の発行と検証＞
ここで電力消費事業者が非化石エネルギーで発電された電力の電力供給権を購入し、自身の電力消費設備で消費した電力に割り当てた場合、その電力消費事業者は、電力供給権の譲渡元の小売電気事業者から非化石証書の発行を受けることができる。
【０１５５】
例えば非化石価値を証明したい電力消費者は、電力を供給した小売電気事業者に非化石証書の発行を依頼する。小売電気事業者のノードは、自身に電力供給権が譲渡された際の電力供給権トランザクションレコードの内容およびその電力供給権をターミネートした時の電力供給権トランザクションレコードの内容を含む非化石証書を生成する。そして小売電気事業者のノードは、生成した非化石証書を、電力消費者のノードに送信する（非化石証書の発行）。
【０１５６】
非化石証書を受領した電力消費者のノードは、発行された非化石証書を、非化石価値検証者４４のノード５００に非化石証書を送信する。非化石価値検証者４４のノード５００は、非化石証書に含まれた各電力供給権トランザクションレコードに対応する電力供給権トランザクションレコード（コミットメント及びゼロ知識証明）をブロックチェーンから取得する。そしてノード５００は、ゼロ知識証明を検証することにより、電力マッチングの内容が正しいことを確認する（非化石証書の検証）。
【０１５７】
＜電力供給権取引および非化石証書の発行・検証の手順＞
次に電力供給権の取引手順について説明する。
図１２は、取引対象の電力の総電力供給期間開始前の処理手順の一例を示すシーケンス図である。図１２の例では、まず発電事業者４１ａと小売電気事業者４３ｂとの間で、発電事業者４１ａが運用する物理発電設備５１ａで発電する電力についての電力供給権の譲渡契約が結ばれている（ステップＳ１１）。電力供給権の譲渡契約は本システム外（例えばオフライン）で行われる。電力供給権の譲渡契約では、物理発電設備５１ａで発電できる電力と総電力供給期間（例えば翌月の一ヶ月間）とが定められる。
【０１５８】
その後、発電事業者４１ａは、自身のノード２００を用いて、物理発電設備５１ａで発電できる電力の電力供給権の譲渡を示す電力供給権トランザクションレコードを生成する。そしてノード２００は、生成した電力供給権トランザクションレコードをブロックチェーンシステム３０に送信する（ステップＳ１２）。この電力供給権トランザクションレコードは、ブロックチェーンシステム３０内のノード４００で受信されたものとする。
【０１５９】
電力供給権トランザクションレコードを受信したノード４００のスマートコントラクト４１０は、受信した電力供給権トランザクションレコードに示される電力供給権の譲渡の内容が正しいかどうかを検証する。そしてスマートコントラクト４１０は、正しいと判断した場合にのみ受信した電力供給権トランザクションレコードをブロックチェーン６０に記録する（ステップＳ１３）。
【０１６０】
例えば小売電気事業者４３ｂは、取得した電力供給権を他の小売電気事業者４３ｂに譲渡する契約を結ぶ（ステップＳ１４）。電力供給権を再譲渡する譲渡契約は本システム外（例えばオフライン）で行われる。契約後、譲渡元の小売電気事業者４３ｂは、自身が有するノード１００ａを用いて電力供給権トランザクションレコードを生成する。そしてノ

ード１００ａは、生成した電力供給権トランザクションレコードをブロックチェーンシステム３０に送信する（ステップＳ１５）。この電力供給権トランザクションレコードは、ブロックチェーンシステム３０内のノード４００で受信されたものとする。

【０１６１】

電力供給権トランザクションレコードを受信したノード４００のスマートコントラクト４１０は、受信した電力供給権トランザクションレコードに示される電力供給権の譲渡の内容が正しいかどうかを検証する。そしてスマートコントラクト４１０は、正しいと判断した場合にのみ受信した電力供給権トランザクションレコードをブロックチェーン６０に記録する（ステップＳ１６）。小売電気事業者４３ａは、自身に譲渡された電力供給権を他の小売電気事業者に再譲渡することができる。このような電力供給権の再譲渡は何度も繰り返すことができる。

【０１６２】

電力消費設備５２ａを運用する電力消費者４２ａは、小売電気事業者４３ａから、ある一定の期間（総電力供給期間）、電力の供給を受ける契約を結ぶ（ステップＳ１７）。この契約は、例えば本システム外（例えばオフライン）で行われる。この契約に従った電力マッチング（供給された電力についての電力供給権トランザクションレコードのターミネート）は総電力供給時間後に行われる。

【０１６３】

図１３は、取引対象の電力の総電力供給期間開始後の処理手順の一例を示すシーケンス図である。電力消費設備５２ａへの電力供給契約に係る電力供給権に対応する物理発電設備５１ａを運用する発電事業者４１ａのノード２００は、物理発電設備５１ａのスマートメータレコードを小売電気事業者４３ａのノード１００に送信する（ステップＳ２１）。また電力消費設備５２ａを運用する電力消費者４２ａのノード３００は、電力消費電設備５２ａのスマートメータレコードを小売電気事業者４３ａのノード１００に送信する（ステップＳ２２）。

【０１６４】

小売電気事業者４３ａのノード１００は、物理発電設備５１ａのスマートメータレコードと電力消費設備５２ａのスマートメータレコードとを３０分単位で一ヶ月分マッチングする（ステップＳ２３）。ノード１００は、電力マッチングにより正当性が検証できた場合、マッチング正当性証明（ゼロ知識証明）を生成する（ステップＳ２４）。ノード１００は、生成したマッチング正当性証明を含む電力マッチングレコードを生成する（ステップＳ２５）。そしてノード１００は、生成した電力マッチングレコード（電力消費設備５２ａでの消費分）を含む電力供給権トランザクションレコードをブロックチェーンシステム３０に送信する（ステップＳ２６）。この電力供給権トランザクションレコードを、ブロックチェーンシステム３０内のノード４００が受信したものとする。

【０１６５】

ノード４００のスマートコントラクト４１０は、マッチング正当性証明の検証を行う（ステップＳ２７）。スマートコントラクト４１０は、マッチングの内容が正しい場合にのみ電力供給権トランザクションレコードをブロックチェーン６０に記録する（ステップＳ２８）。これにより、電力マッチングが行われた電力供給権（電力供給権トランザクションのインプットに設定された電力供給権）はターミネートする。

【０１６６】

なお小売電気事業者４３ａのノード１００は、ステップＳ２６で送信する電力供給権トランザクションレコードに、電力マッチングにおいて余った分の電力に対応する電力供給権を自分自身に譲渡するアウトプットを含めることができる。この電力供給権トランザクションレコードがブロックチェーン６０に記録されることにより、電力マッチングにおいて余った分の電力供給権がお釣りとして自身に戻される。

【０１６７】

小売電気事業者４３ａのノード１００は、電力マッチングで使用したデータ（３０分単位のスマートメータレコード、コミットメント乱数など）を、ローカルのデータベースに

保存する（ステップＳ２９）。ノード１００は、保存したデータを非化石証書の発行などに利用することができる。

【０１６８】

図１４は、非化石証書の発行と検証の処理手順の一例を示すシーケンス図である。例えば電力消費者４２ａが電力消費設備５２ａ用の電力供給元として取得した電力供給権の電力が、非化石エネルギーで発電を行う物理発電設備で発電された電力であるものとする。この場合、電力消費者４２ａは、ノード３００を用いて、小売電気事業者４３ａのノード１００に、該当する電力供給権に関する非化石証書の発行依頼を送信する（ステップＳ４１）。ノード１００は、その電力供給権の電力マッチング時に保存しておいたデータに基づいて、該当する電力マッチングに対応する電力供給権トランザクションレコードの内容を含む非化石証書を発行する（ステップＳ４２）。ノード１００は、発行した非化石証書をノード３００に送信する。

【０１６９】

ノード３００は、非化石価値を証明したい相手（例えば非化石価値検証者４４）が有するノード５００に、非化石証書を送信する（ステップＳ４３）。ノード５００は、ブロックチェーンシステム３０に該当する取引記録を要求する（ステップＳ４４）。ブロックチェーンシステム３０は、指定された取引の総電力量コミットメントとマッチング正当性証明とをノード５００に送信する（ステップＳ４５）。ノード５００は、総電力量コミットメントとマッチング正当性証明とに基づいて所定の計算を行うことにより、電力マッチングが正当であることを検証する（ステップＳ４６）。例えば非化石価値検証者４４のノード５００には、非化石エネルギーで発電を行う物理発電設備の物理発電設備ＩＤが予め登録されている。非化石価値検証者４４は、非化石証書に示される物理発電設備の物理発電設備ＩＤの正当性を検証し、正当な物理発電設備ＩＤが非化石エネルギーで発電を行う物理発電設備の物理発電設備ＩＤとして予め登録されていることを確認する。

【０１７０】

これにより、電力消費者４２ａが運用する電力消費設備５２ａが非化石エネルギーによって発電された電力を消費したことが確認される。

〔その他の実施の形態〕

第２の実施の形態では非化石エネルギーで生成された資源が電力の場合の例を示したが、水素、バイオ燃料などの他の資源についての取引にも利用することができる。

【０１７１】

上記については単に本発明の原理を示すものである。さらに、多数の変形、変更が当業者にとって可能であり、本発明は上記に示し、説明した正確な構成および応用例に限定されるものではなく、対応するすべての変形例および均等物は、添付の請求項およびその均等物による本発明の範囲とみなされる。

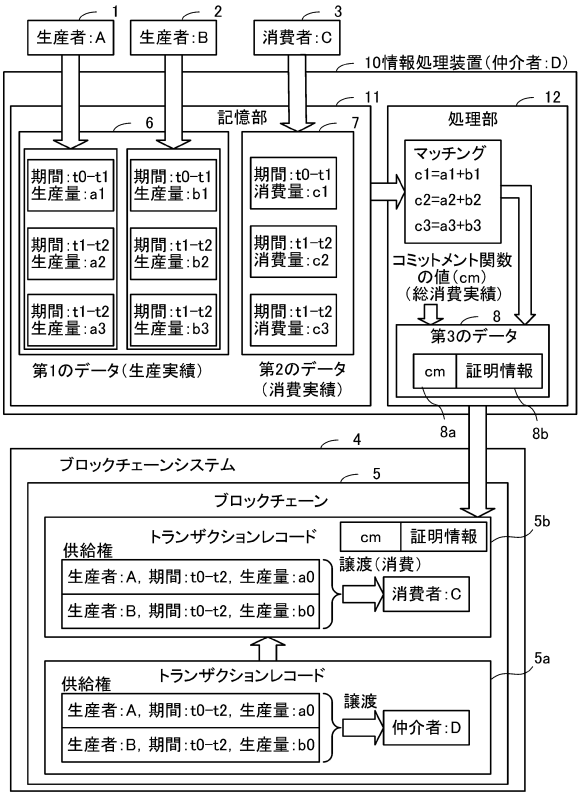
【符号の説明】

【０１７２】

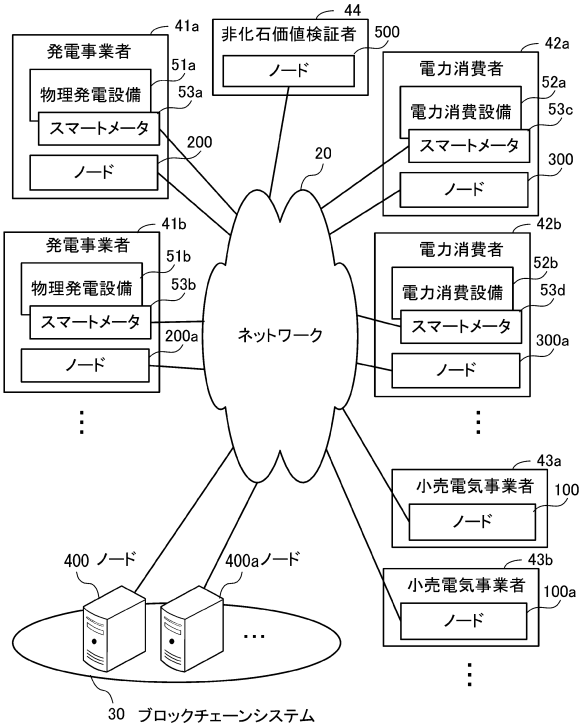
１，２　生産者
３　消費者
４　ブロックチェーンシステム
５　ブロックチェーン
５ａ，５ｂ　トランザクションレコード
６　第１のデータ
７　第２のデータ
８　第３のデータ
８ａ　コミットメント関数の値
８ｂ　証明情報
１０　情報処理装置
１１　記憶部
１２　処理部

【図面】

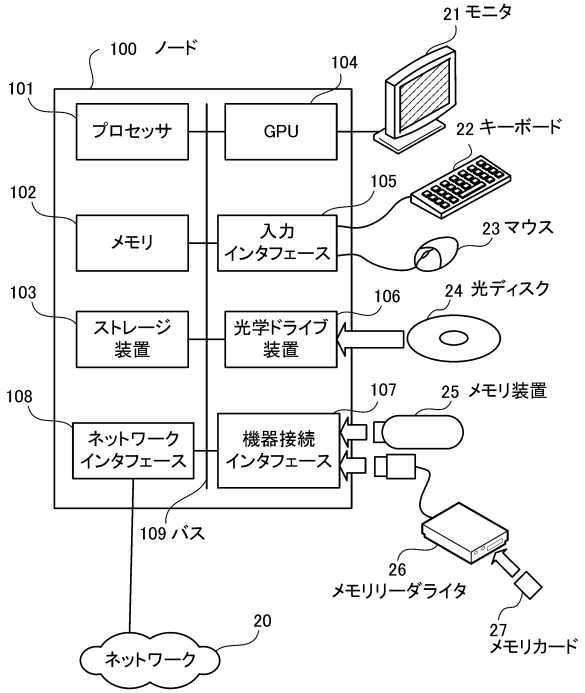
【図１】


1
生産者:A
2
生産者:B
3
消費者:C
10情報処理装置(仲介者:D)
11
記憶部
12
処理部
6
7
期間:t0−t1
生産量:a1
期間:t1−t2
生産量:a2
期間:t1−t2
生産量:a3
期間:t0−t1
生産量:b1
期間:t1−t2
生産量:b2
期間:t1−t2
生産量:b3
期間:t0−t1
消費量:c1
期間:t1−t2
消費量:c2
期間:t1−t2
消費量:c3
マッチング
c1=a1+b1
c2=a2+b2
c3=a3+b3
コミットメント関数
の値(cm)
(総消費実績)
8
第3のデータ
cm
証明情報
第1のデータ(生産実績)
第2のデータ
(消費実績)
8a
8b
4
ブロックチェーンシステム
5
ブロックチェーン
トランザクションレコード
cm
証明情報
5b
供給権
生産者:A, 期間:t0−t2, 生産量:a0
生産者:B, 期間:t0−t2, 生産量:b0
譲渡(消費)
消費者:C
5a
トランザクションレコード
供給権
生産者:A, 期間:t0−t2, 生産量:a0
生産者:B, 期間:t0−t2, 生産量:b0
譲渡
仲介者:D

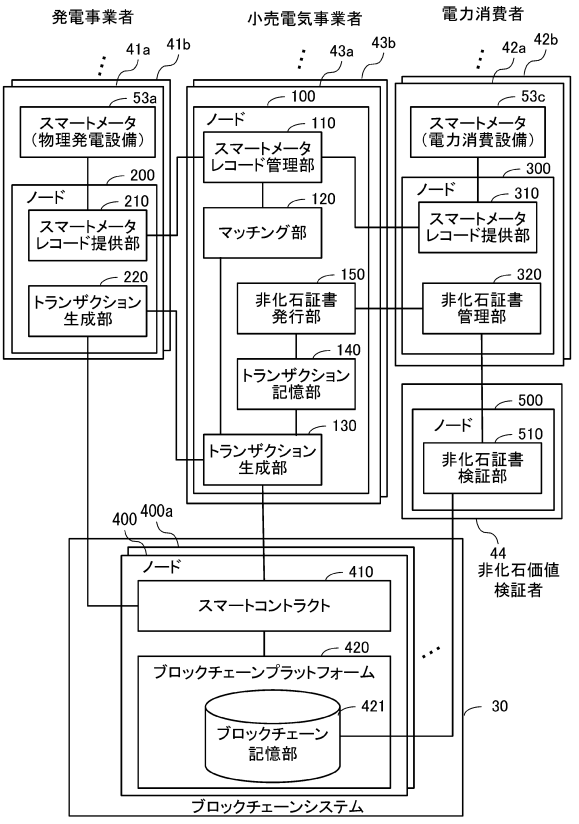
【図２】


41a
発電事業者
51a
物理発電設備
53a
スマートメータ
200
ノード
44
非化石価値検証者
500
ノード
42a
電力消費者
52a
電力消費設備
53c
スマートメータ
300
ノード
20
41b
発電事業者
51b
物理発電設備
53b
スマートメータ
200a
ノード
ネットワーク
42b
電力消費者
52b
電力消費設備
53d
スマートメータ
300a
ノード
43a
小売電気事業者
100
ノード
400 ノード
400aノード
43b
小売電気事業者
100a
ノード
30 ブロックチェーンシステム

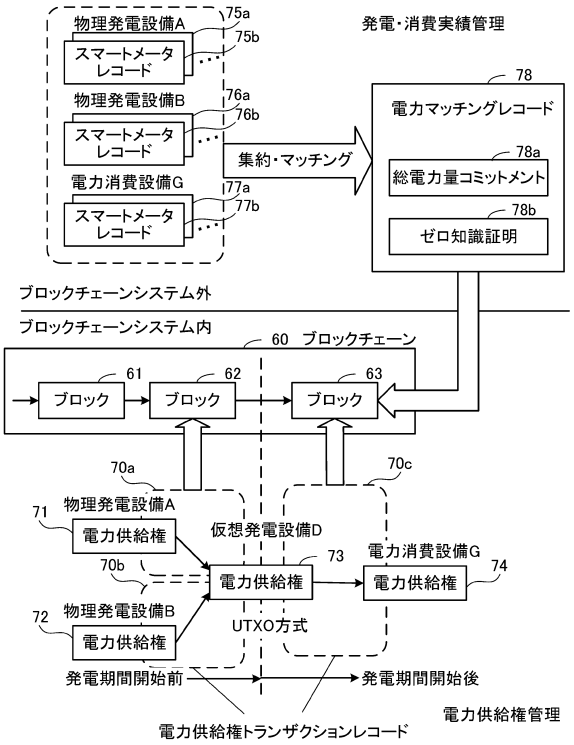
【図３】


21 モニタ
100 ノード
104
101
プロセッサ
GPU
22 キーボード
105
102
メモリ
入力
インタフェース
23 マウス
106
24 光ディスク
103
ストレージ
装置
光学ドライブ
装置
107
25 メモリ装置
108
ネットワーク
インタフェース
機器接続
インタフェース
109 バス
26
メモリリーダライタ
27
メモリカード
20
ネットワーク

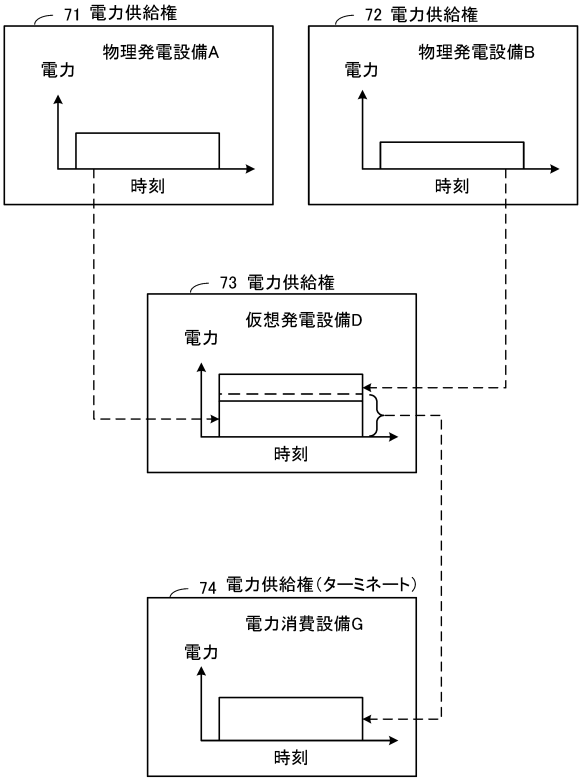
【図４】


発電事業者
小売電気事業者
電力消費者
41a
41b
43a
43b
42a
42b
53a
スマートメータ
(物理発電設備)
200
ノード
210
スマートメータ
レコード提供部
220
トランザクション
生成部
100
ノード
110
スマートメータ
レコード管理部
120
マッチング部
150
非化石証書
発行部
140
トランザクション
記憶部
130
トランザクション
生成部
53c
スマートメータ
(電力消費設備)
300
ノード
310
スマートメータ
レコード提供部
320
非化石証書
管理部
500
ノード
510
非化石証書
検証部
44
非化石価値
検証者
400
400a
ノード
410
スマートコントラクト
420
ブロックチェーンプラットフォーム
421
ブロックチェーン
記憶部
30
ブロックチェーンシステム

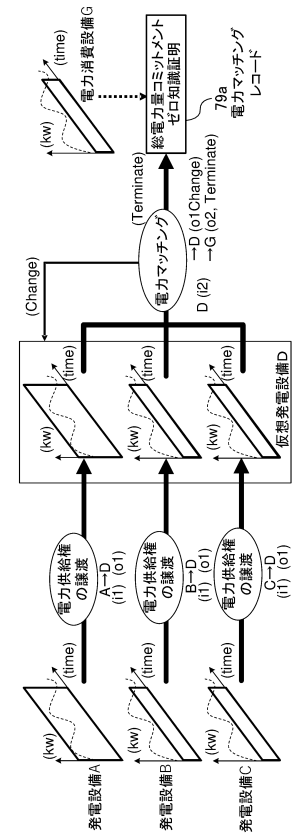
【図５】


物理発電設備A
75a
75b
スマートメータ
レコード
発電・消費実績管理
78
電力マッチングレコード
物理発電設備B
76a
76b
集約・マッチング
78a
総電力量コミットメント
電力消費設備G
77a
77b
78b
ゼロ知識証明
ブロックチェーンシステム外
ブロックチェーンシステム内
60 ブロックチェーン
61
62
63
ブロック
70a
70c
71
物理発電設備A
電力供給権
仮想発電設備D
73
電力消費設備G
70b
74
72
物理発電設備B
UTXO方式
発電期間開始前
発電期間開始後
電力供給権管理
電力供給権トランザクションレコード

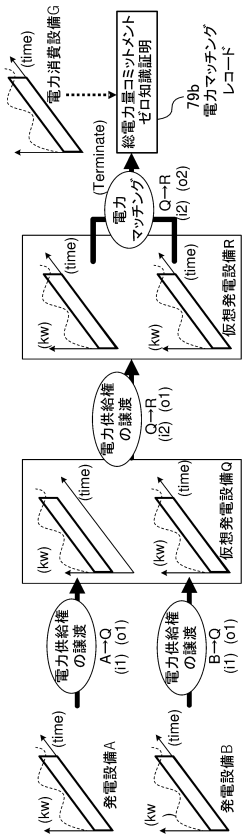
【図６】


71 電力供給権
物理発電設備A
電力
時刻
72 電力供給権
物理発電設備B
電力
時刻
73 電力供給権
仮想発電設備D
電力
時刻
74 電力供給権（ターミネート）
電力消費設備G
電力
時刻

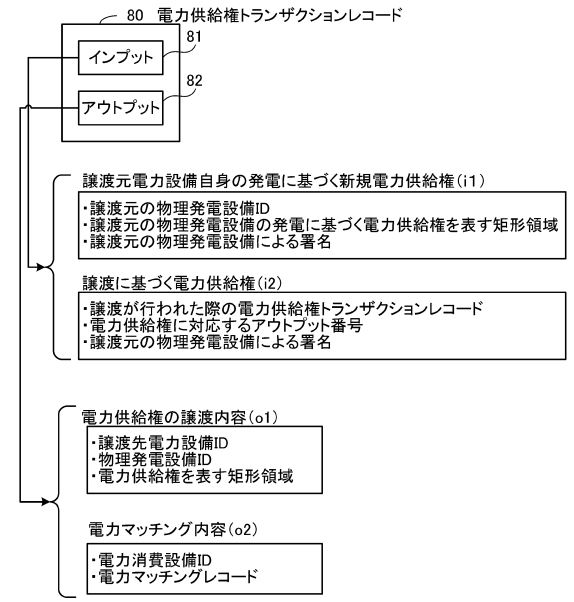
【図７】


電力消費設備G
(time)
(kw)
総電力量コミットメント
ゼロ知識証明
79a
電力マッチング
レコード
(Terminate)
電力マッチング
D (i2)
→D (o1Change)
→G (o2, Terminate)
(Change)
仮想発電設備D
電力供給権
の譲渡
A→D
(i1) (o1)
B→D
(i1) (o1)
C→D
(i1) (o1)
発電設備A
発電設備B
発電設備C

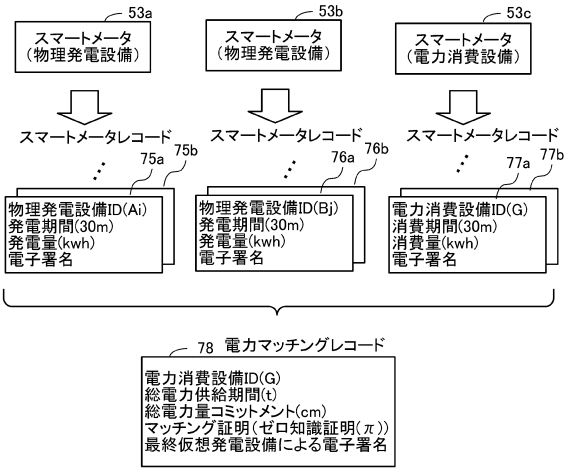
【図８】


電力消費設備G
(time)
(kw)
総電力量コミットメント
ゼロ知識証明
79b
電力マッチング
レコード
(Terminate)
電力
マッチング
Q→R
(i2) (o2)
仮想発電設備R
電力供給権
の譲渡
Q→R
(i2) (o1)
仮想発電設備Q
電力供給権
の譲渡
A→Q
(i1) (o1)
電力供給権
の譲渡
B→Q
(i1) (o1)
発電設備A
発電設備B

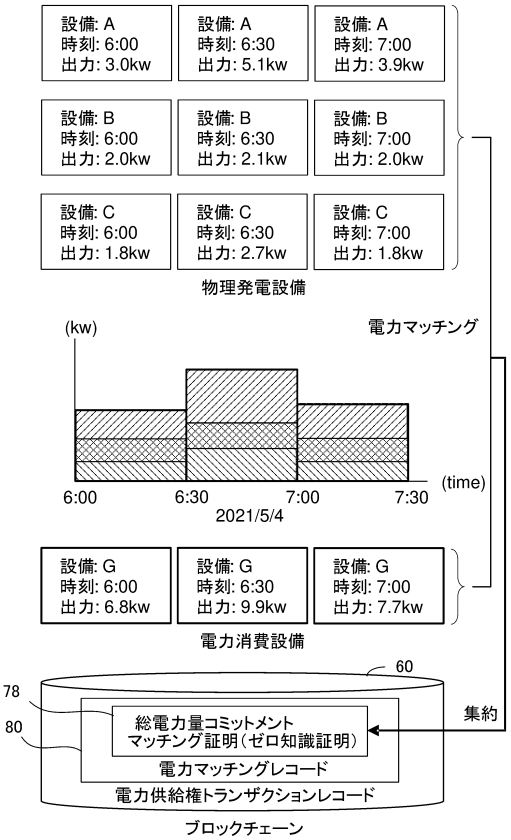
【図９】



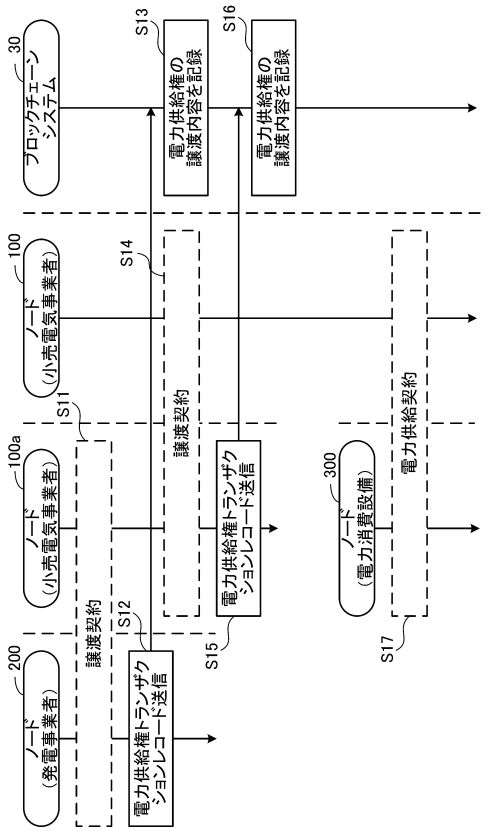
【図１０】



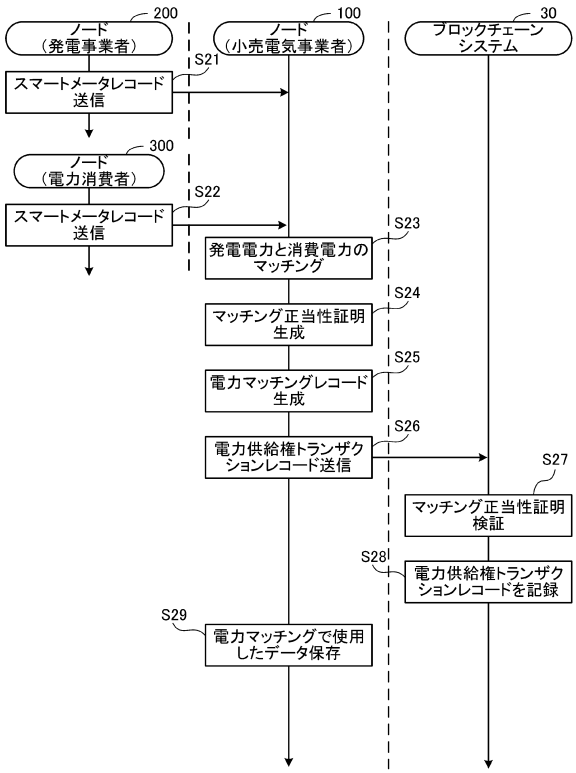
【図１１】



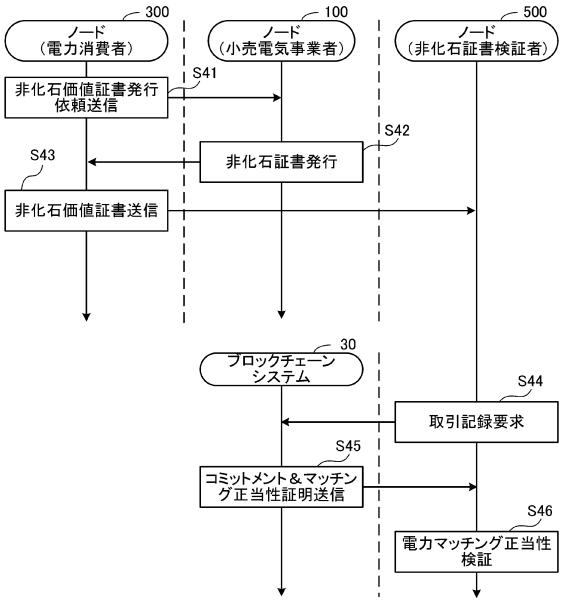
【図１２】



【図１３】


200
ノード
（発電事業者）
100
ノード
（小売電気事業者）
30
ブロックチェーン
システム
S21
スマートメータレコード
送信
300
ノード
（電力消費者）
S22
スマートメータレコード
送信
S23
発電電力と消費電力の
マッチング
S24
マッチング正当性証明
生成
S25
電力マッチングレコード
生成
S26
電力供給権トランザク
ションレコード送信
S27
マッチング正当性証明
検証
S28
電力供給権トランザク
ションレコードを記録
S29
電力マッチングで使用
したデータ保存

【図１４】


300
ノード
（電力消費者）
100
ノード
（小売電気事業者）
500
ノード
（非化石証書検証者）
S41
非化石価値証書発行
依頼送信
S42
非化石証書発行
S43
非化石価値証書送信
30
ブロックチェーン
システム
S44
取引記録要求
S45
コミットメント＆マッチン
グ正当性証明送信
S46
電力マッチング正当性
検証

フロントページの続き

(56)参考文献 特開２０１９－１３３６３０（ＪＰ，Ａ）
特開２０２０－８７２０９（ＪＰ，Ａ）
特開２０２０－１１９１４３（ＪＰ，Ａ）
特開２０１９－１４４８５１（ＪＰ，Ａ）
小櫻文彦，“電力の需要家間取引をブロックチェーン上で実現”，ＯＨＭ，日本，株式会社オーム社，2019年07月05日，第106巻, 第7号, ISSN0386-5576，pp.36～38
中村誠吾ほか３名，“第3章 1 記録されるデータの構造”, “第3章 4.3 UTXO型での二重取引防止”, “第6章 3 個人間電力取引”，ブロックチェーン システム設計，第１版, ISBN978-4-86594-115-9，株式会社リックテレコム，2018年08月02日，pp.36～43, 52, 114～117
佐藤哲平ほか２名，“ブロックチェーンシステムにおける匿名信頼性付与手法の実装・評価”，２０２０年 暗号と情報セキュリティシンポジウム予稿集， 電子情報通信学会情報セキュリティ（ＩＳＥＣ）研究，2020年01月21日，1D1-4，pp.1～6
岡本龍明ほか１４名，“第4章 ゼロ知識証明モデルと計算量理論”，暗号・ゼロ知識証明・数論，初版１刷, ISBN4-320-02740-X，共立出版株式会社，1995年06月01日，pp.73～91

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