(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6628188号
(P6628188)

(45)発行日　令和2年1月8日(2020.1.8)　(24)登録日　令和1年12月13日(2019.12.13)

(51)Int.Cl.		F I		
G06Q 20/06	(2012.01)	G06Q	20/06	
G06Q 20/12	(2012.01)	G06Q	20/12	300
G06F 21/64	(2013.01)	G06F	21/64	

請求項の数 7　(全 13 頁)

(21)出願番号　特願2016-94676(P2016-94676)
(22)出願日　平成28年5月10日(2016.5.10)
(65)公開番号　特開2017-204070(P2017-204070A)
(43)公開日　平成29年11月16日(2017.11.16)
審査請求日　平成29年12月26日(2017.12.26)

前置審査

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町一丁目５番１号
(73)特許権者　504193837
国立大学法人室蘭工業大学
北海道室蘭市水元町２７番１号
(74)代理人　100127535
弁理士　豊田　義元
(74)代理人　100189898
弁理士　永田　健悟
(72)発明者　渡邉　大喜
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】決済システム、決済方法、トランザクション生成装置及びトランザクション生成プログラム

(57)【特許請求の範囲】
【請求項１】
第１ブロックチェーンと第２ブロックチェーンとを連携させた決済システムであって、
前記第１ブロックチェーン用の支払いトランザクションを内包する第１トランザクションを前記第２ブロックチェーンのネットワークに送信する第１トランザクション生成装置と、
前記第２ブロックチェーンに登録された前記第１トランザクションの情報に応じた第２トランザクションを前記第２ブロックチェーンのネットワークに送信し、前記第１トランザクションが内包する前記支払いトランザクションを前記第１ブロックチェーンのネットワークに送信する第２トランザクション生成装置と、を有し、
前記支払いトランザクションは、当該支払いトランザクションが前記第１ブロックチェーンに登録されることで支払いが確定する支払い情報であって、第１利用者の署名と第２利用者の署名が必要な第２利用者への支払い情報を含み、
前記第１トランザクション生成装置は、前記第１利用者の署名が有って前記第２利用者の署名が無い前記支払いトランザクションを前記第１トランザクションに内包して送信し、
前記第２トランザクション生成装置は、前記支払いトランザクションに前記第２利用者の署名を付与して前記第１ブロックチェーンのネットワークに送信することを特徴とする決済システム。

【請求項２】
前記第１トランザクション生成装置は、前記第２トランザクション生成装置が前記支払いトランザクションを前記第１ブロックチェーンのネットワークに送信する前は、前記支払いトランザクションの内容を変更した支払いトランザクションを内包する第３トランザクションを前記第２ブロックチェーンのネットワークに送信し、
前記第２トランザクション生成装置は、前記第３トランザクションの情報が前記第２ブロックチェーンに登録されている場合は、前記第１トランザクションが内包する前記支払いトランザクションを前記第１ブロックチェーンのネットワークに送信せず、前記第３トランザクションが内包する前記支払いトランザクションを前記第１ブロックチェーンのネットワークに送信することを特徴とする請求項１に記載の決済システム。

【請求項３】
前記支払いトランザクションは、前記第２ブロックチェーンに登録された情報に基づいて正当性が検証されることを特徴とする請求項１又は２のいずれかに記載の決済システム。

【請求項４】
第１ブロックチェーンと第２ブロックチェーンとを連携させた決済方法であって、
第１トランザクション生成装置による、
前記第１ブロックチェーン用の支払いトランザクションを内包する第１トランザクションを前記第２ブロックチェーンのネットワークに送信するステップと、
第２トランザクション生成装置による、
前記第１トランザクションの情報に応じた第２トランザクションを前記第２ブロックチェーンのネットワークに送信するステップと、
前記第１トランザクションが内包する前記支払いトランザクションを前記第１ブロックチェーンのネットワークに送信するステップと、を有し、
前記第１ブロックチェーン用の支払いトランザクションは、当該支払いトランザクションが前記第１ブロックチェーンに登録されることで支払いが確定する支払い情報であって、第１利用者の署名と第２利用者の署名が必要な第２利用者への支払い情報を含み、
前記第１トランザクション生成装置は、前記第１利用者の署名が有って前記第２利用者の署名が無い前記支払いトランザクションを前記第１トランザクションに内包して送信し、
前記第２トランザクション生成装置は、前記支払いトランザクションに前記第２利用者の署名を付与して前記第１ブロックチェーンのネットワークに送信することを特徴とする決済方法。

【請求項５】
第１ブロックチェーンと第２ブロックチェーンとを連携させた決済システムに用いるトランザクション生成装置であって、
前記第１ブロックチェーン用の支払いトランザクションを内包する第１トランザクションを前記第２ブロックチェーンのネットワークに送信するトランザクション送信手段を有し、
前記第１ブロックチェーン用の支払いトランザクションは、当該支払いトランザクションが前記第１ブロックチェーンに登録されることで支払いが確定する支払い情報であって、第１利用者の署名と第２利用者の署名が必要な第２利用者への支払い情報を含み、前記第１トランザクションは前記第２ブロックチェーンへの第２トランザクションの登録を要求する情報を含み、
前記トランザクション送信手段は、前記第１利用者の署名が有って前記第２利用者の署名が無い前記第１ブロックチェーン用の支払いトランザクションを前記第１トランザクションに内包して送信し、

前記第１ブロックチェーン用のトランザクションに前記第２利用者の署名が付与されて前記第１ブロックチェーンに登録された後、前記第１トランザクションの情報に対応する第２トランザクションが前記第２ブロックチェーンに登録されることを特徴とするトランザクション生成装置。

【請求項６】
第１ブロックチェーンと第２ブロックチェーンとを連携させた決済システムに用いるトランザクション生成装置であって、
前記第２ブロックチェーンに登録された第１トランザクションが内包する前記第１ブロックチェーン用の支払いトランザクションを前記第１ブロックチェーンのネットワークに送信する第１トランザクション送信手段と、
前記第１トランザクションの情報に応じた第２トランザクションを前記第２ブロックチェーンのネットワークに送信する第２トランザクション送信手段と、を有し、
前記第１ブロックチェーン用の支払いトランザクションは、当該支払いトランザクションが前記第１ブロックチェーンに登録されることで支払いが確定する支払い情報であって、第１利用者の署名と第２利用者の署名が必要な第２利用者への支払い情報を含み、前記第１利用者の署名が付与されており、
前記第１トランザクション送信手段は、前記第１ブロックチェーン用のトランザクションに前記第２利用者の署名を付与して前記第１ブロックチェーンのネットワークに送信することを特徴とするトランザクション生成装置。

【請求項７】
請求項５又は６に記載のトランザクション生成装置としてコンピュータを動作させることを特徴とするトランザクション生成プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、中央集権的な管理機構を必要とせずに信頼性を担保可能なブロックチェーンの技術に関し、特にブロックチェーンを連携させる技術に関する。
【背景技術】
【０００２】
ビットコイン（登録商標）などの仮想通貨において、中央集権的な管理機構を必要とせずに、信頼性を担保可能な仕組みとしてブロックチェーン技術が用いられている。ブロックチェーンは、参加者間の仮想通貨の取引情報（トランザクション）がブロックと呼ばれる単位でまとめられて連結されたものである。ブロックチェーンは、Ｐ２Ｐ（Ｐｅｅｒ Ｔｏ Ｐｅｅｒ）ネットワークにおいて参加者が共有する一つの巨大な元帳として機能する。
【０００３】
ブロックチェーン技術の信頼性の高さから、仮想通貨に留まらず、様々な応用が期待されている。一例として、ブロックチェーンにコンテンツの視聴許諾に関する権利情報を記録し、コンテンツの権利管理を実現することも考えられる。
【先行技術文献】
【非特許文献】
【０００４】
【非特許文献１】斉藤賢爾、“ビットコイン－人間不在のデジタル巨石貨幣”、ＷＩＤＥテクニカルレポート
【発明の概要】
【発明が解決しようとする課題】
【０００５】
ブロックチェーン技術を利用する２つの異なるシステムを連携させることで用途を広げ

ることが可能となる。例えば、仮想通貨のシステムにおけるブロックチェーンとコンテンツの視聴許諾に関する権利管理のシステムにおけるブロックチェーンを連携させることによって、仮想通貨の支払いに応じたコンテンツの視聴許諾に関する権利情報の授受の実現が可能となる。

【０００６】

仮想通貨のブロックチェーンとコンテンツ権利管理のブロックチェーンの連携を考えた場合、一般的な方法として、コンテンツを利用する利用者及びコンテンツの視聴許諾を発行する権利者の双方が、両方のブロックチェーンの状況を監視することが考えらえる。より具体的には、利用者は、コンテンツの視聴許諾の対価の支払いに関するトランザクションを仮想通貨のブロックチェーンネットワークに発行する。権利者は、対価の支払いに関するトランザクションが仮想通貨のブロックチェーンに登録されたことを検知し、支払い金額が適当であるかを確認した上で、コンテンツ権利管理のブロックチェーンネットワークにコンテンツの視聴許諾に関するトランザクションを発行する。利用者は、コンテンツ権利管理のブロックチェーンに登録された視聴許諾を確認することでコンテンツの視聴が可能となる。

【０００７】

しかしながら、上記の方法には下記の問題点がある。

【０００８】

第１に、利用者及び権利者にとって、２つのブロックチェーンの状況を同時に監視し、２つのブロックチェーン間で対価の支払いと視聴許諾を関連付けて管理することは手間が大きいという問題がある。

【０００９】

第２に、連携するブロックチェーンの特性が異なる場合、例えば、ブロックの生成タイミング、具体的にはトランザクションの検証が行われ、正規のトランザクションであると承認される間隔が異なる場合には、間隔の長いブロックチェーンの影響を受けるという問題がある。より具体的な例で示すと、仮想通貨のブロックチェーンのブロック生成間隔を１０分とし、コンテンツの視聴許諾に関する権利管理のブロックチェーンのブロック生成間隔を５秒としたとき、仮想通貨のブロックチェーンでの支払いの確認に時間がかかるため、コンテンツの権利管理のブロックチェーンが高速な承認を可能とする特性を有していても、その特性が生かされることはない。

【００１０】

第３に、仮想通貨のブロックチェーンにおいてトランザクション毎に手数料が設定されている場合、多数の極めて少額なコンテンツに関する視聴許諾を利用者が得る際に、対価の総額に対して手数料の総額が占める割合が大きくなるという問題がある。

【００１１】

本発明は、上記に鑑みてなされたものであり、効率的にブロックチェーンを連携させることを目的とする。

【課題を解決するための手段】

【００１２】

第１の本発明に係る決済システムは、第１ブロックチェーンと第２ブロックチェーンとを連携させた決済システムであって、前記第１ブロックチェーン用の支払いトランザクションを内包する第１トランザクションを前記第２ブロックチェーンのネットワークに送信する第１トランザクション生成装置と、前記第２ブロックチェーンに登録された前記第１トランザクションの情報に応じた第２トランザクションを前記第２ブロックチェーンのネットワークに送信し、前記第１トランザクションが内包する前記支払いトランザクションを前記第１ブロックチェーンのネットワークに送信する第２トランザクション生成装置と、を有し、前記支払いトランザクションは、当該支払いトランザクションが前記第１ブロックチェーンに登録されることで支払いが確定する支払い情報を含むことを特徴とする。

【００１３】

第２の本発明に係る決済方法は、第１ブロックチェーンと第２ブロックチェーンとを連

携させた決済方法であって、第１トランザクション生成装置による、前記第１ブロックチェーン用の支払いトランザクションを内包する第１トランザクションを前記第２ブロックチェーンのネットワークに送信するステップと、第２トランザクション生成装置による、前記第１トランザクションの情報に応じた第２トランザクションを前記第２ブロックチェーンのネットワークに送信するステップと、前記第１トランザクションが内包する前記支払いトランザクションを前記第１ブロックチェーンのネットワークに送信するステップと、を有し、前記支払いトランザクションは、当該支払いトランザクションが前記第１ブロックチェーンに登録されることで支払いが確定する支払い情報を含むことを特徴とする。

【００１４】

第３の本発明に係るトランザクション生成装置は、第１ブロックチェーンと第２ブロックチェーンとを連携させた決済システムに用いるトランザクション生成装置であって、前記第１ブロックチェーン用の支払いトランザクションを内包する第１トランザクションを前記第２ブロックチェーンのネットワークに送信するトランザクション送信手段を有し、前記支払いトランザクションは、当該支払いトランザクションが前記第１ブロックチェーンに登録されることで支払いが確定する支払い情報を含み、前記第１トランザクションは前記第２ブロックチェーンへの第２トランザクションの登録を要求する情報を含むことを特徴とする。

【００１５】

第４の本発明に係るトランザクション生成装置は、第１ブロックチェーンと第２ブロックチェーンとを連携させた決済システムに用いるトランザクション生成装置であって、前記第２ブロックチェーンに登録された第１トランザクションが内包する前記第１ブロックチェーン用の支払いトランザクションを前記第１ブロックチェーンのネットワークに送信する第１トランザクション送信手段と、前記第１トランザクションの情報に応じた第２トランザクションを前記第２ブロックチェーンのネットワークに送信する第２トランザクション送信手段と、を有し、前記支払いトランザクションは、当該支払いトランザクションが前記第１ブロックチェーンに登録されることで支払いが確定する支払い情報を含むことを特徴とする。

【００１６】

第５の本発明に係るトランザクション生成プログラムは、上記トランザクション生成装置の各手段としてコンピュータを動作させることを特徴とする。

【発明の効果】

【００１７】

本発明によれば、効率的にブロックチェーンを連携させることができる。

【図面の簡単な説明】

【００１８】

【図１】本実施の形態における決済システムを含む全体構成図である。

【図２】本実施の形態における決済システムの動作を説明するための図である。

【図３】本実施の形態における決済システムにおいて利用者から権利者への支払いをまとめる動作を説明するための図である。

【発明を実施するための形態】

【００１９】

以下、本発明の実施の形態について図面を用いて説明する。

【００２０】

図１は、本実施の形態における決済システムを含む全体構成図である。本決済システムは、仮想通貨ブロックチェーンＢＣ１での仮想通貨による支払いとコンテンツ権利管理ブロックチェーンＢＣ２でのコンテンツの権利の管理を連携したシステムである。

【００２１】

仮想通貨ブロックチェーンＢＣ１は、仮想通貨ブロックチェーンＢＣ１のＰ２Ｐネットワークに参加するノードによって共有されるブロックチェーンデータである。仮想通貨ブロックチェーンＢＣ１には、仮想通貨の取引履歴が登録される。どこからどこにいくらの

仮想通貨を移動するかといった取引情報を記載したトランザクションが仮想通貨ブロックチェーンＢＣ１のＰ２Ｐネットワークにブロードキャストされると、そのトランザクションを含むブロックが生成されて、生成されたブロックが仮想通貨ブロックチェーンＢＣ１の末尾に追加される。

【００２２】

コンテンツ権利管理ブロックチェーンＢＣ２は、コンテンツ権利管理ブロックチェーンＢＣ２のＰ２Ｐネットワークに参加するノードによって共有されるブロックチェーンデータである。コンテンツ権利管理ブロックチェーンＢＣ２には、コンテンツの権利に関する情報が登録される。コンテンツの権利に関する情報を記載したトランザクションが仮想通貨ブロックチェーンＢＣ１のＰ２Ｐネットワークにブロードキャストされると、そのトランザクションを含むブロックが生成されて、生成されたブロックがコンテンツ権利管理ブロックチェーンＢＣ２の末尾に追加される。コンテンツ権利管理ブロックチェーンＢＣ２に内包されるデータは、トランザクションそのものではなくトランザクションに記載された内容を含むものでもよい。

【００２３】

コンテンツ権利管理ブロックチェーンＢＣ２のＰ２Ｐネットワークには利用者装置１と権利者装置２が接続される。権利者装置２は仮想通貨ブロックチェーンＢＣ１にも接続される。

【００２４】

利用者装置１は、コンテンツを視聴する利用者が使用する装置である。利用者装置１は、コンテンツ視聴の許諾を要求するときに、仮想通貨ブロックチェーンＢＣ１用の支払いトランザクションを内包した許諾要求トランザクションをコンテンツ権利管理ブロックチェーンＢＣ２のＰ２Ｐネットワークに送信する。支払いトランザクションには、コンテンツ視聴の許諾の対価に相当する仮想通貨を権利者に移動する支払い情報が記載される。

【００２５】

権利者装置２は、コンテンツ権利管理ブロックチェーンＢＣ２にコンテンツを登録したコンテンツの権利者が使用する装置である。権利者装置２は、許諾要求トランザクションに応じたコンテンツ視聴の権利を許諾する情報を記載した許諾トランザクションをコンテンツ権利管理ブロックチェーンＢＣ２のＰ２Ｐネットワークに送信するとともに、許諾要求トランザクションが内包する支払いトランザクションを仮想通貨ブロックチェーンＢＣ１のＰ２Ｐネットワークに送信する。許諾トランザクションがコンテンツ権利管理ブロックチェーンＢＣ２に登録されると、コンテンツの視聴が可能になる。支払いトランザクションが仮想通貨ブロックチェーンＢＣ１に登録されると支払いが確定する。以下、利用者装置１と権利者装置２について説明する。

【００２６】

利用者装置１は、トランザクション生成部１１、同期部１２、記憶部１３、及びコンテンツ再生部１４を備える。

【００２７】

トランザクション生成部１１は、支払い情報を記載した仮想通貨ブロックチェーンＢＣ１用の支払いトランザクションを生成し、支払いトランザクションを内包した許諾要求トランザクションをコンテンツ権利管理ブロックチェーンＢＣ２のＰ２Ｐネットワークに送信する。

【００２８】

より具体的には、トランザクション生成部１１は、仮想通貨ブロックチェーンＢＣ１に登録された未使用（他のトランザクションの入力となっていない）のトランザクションの情報と、利用者の電子署名と、利用者の電子署名を検証するための情報を入力とし、コンテンツ視聴の対価に相当する仮想通貨（支払い金額）と支払先（権利者）を特定する情報を出力として、仮想通貨ブロックチェーンＢＣ１用の支払いトランザクションを生成する。

【００２９】

トランザクション生成部１１は、生成した支払いトランザクションをコンテンツ視聴の許諾を要求する許諾要求トランザクションに内包し、許諾要求トランザクションをコンテンツ権利管理ブロックチェーンＢＣ２のＰ２Ｐネットワークに送信する。

【００３０】

同期部１２は、コンテンツ権利管理ブロックチェーンＢＣ２のＰ２Ｐネットワークで共有されるブロックチェーンデータを取得して記憶部１３に記憶する。

【００３１】

コンテンツ再生部１４は、記憶部１３に記憶されたブロックチェーンデータ内のコンテンツ視聴の許諾情報を参照してコンテンツを再生する。コンテンツ視聴の許諾情報は、権利者装置２が生成した許諾トランザクションに含まれる情報であり、コンテンツ権利管理ブロックチェーンＢＣ２に登録された情報である。

【００３２】

権利者装置２は、トランザクション生成部２１、同期部２２、記憶部２３、及びトランザクション送信部２４を備える。

【００３３】

トランザクション生成部２１は、許諾要求トランザクションが内包する支払いトランザクションの正当性を検証し、コンテンツ視聴を許諾する許諾トランザクションをコンテンツ権利管理ブロックチェーンＢＣ２のＰ２Ｐネットワークに送信する。支払いトランザクションの正当性の検証では、支払いトランザクションに記載された支払い先及び支払い金額は適切であるか、支払いトランザクションは仮想通貨ブロックチェーンＢＣ１において有効となるかを検証する。

【００３４】

同期部２２は、コンテンツ権利管理ブロックチェーンＢＣ２のＰ２Ｐネットワークで共有されるブロックチェーンデータを取得して記憶部２３に記憶する。

【００３５】

トランザクション送信部２４は、許諾要求トランザクションが内包する支払いトランザクションを取り出し、支払いトランザクションを仮想通貨ブロックチェーンＢＣ１のＰ２Ｐネットワークに送信する。

【００３６】

利用者装置１及び権利者装置２が備える各部は、演算処理装置、記憶装置等を備えたコンピュータにより構成して、各部の処理がプログラムによって実行されるものとしてもよい。このプログラムは利用者装置１及び権利者装置２が備える記憶装置に記憶されており、磁気ディスク、光ディスク、半導体メモリ等の記録媒体に記録することも、ネットワークを通して提供することも可能である。

【００３７】

次に、本実施の形態における決済システムの動作について説明する。

【００３８】

図２は、本実施の形態における決済システムの動作を説明するための図である。同図では、コンテンツ権利管理ブロックチェーンＢＣ２に登録される情報と仮想通貨ブロックチェーンＢＣ１に登録される情報を示している。

【００３９】

利用者装置１は、支払いトランザクションＴＸ１－１と支払いトランザクションＴＸ１－１を内包する許諾要求トランザクションＴＸ２－１を生成し、許諾要求トランザクションＴＸ２－１をコンテンツ権利管理ブロックチェーンＢＣ２のＰ２Ｐネットワークに送信する（ステップＳ１１）。

【００４０】

ところで、出金の際にトランザクションに対して複数人の電子署名を必要とするマルチシグネチャ（以下、マルチシグ）という方式がある。本実施例では、出金元として利用者の電子署名と権利者の電子署名が必要なマルチシグのアドレスを用いる。支払いトランザクションＴＸ１－１には、マルチシグのアドレスから権利者のアドレスへの支払い情報が

記載される。利用者はマルチシグのアドレスに所定の金額を予めデポジットしておく。例えば、利用者のアドレスからマルチシグのアドレスへ所定の金額を移動するトランザクションを仮想通貨ブロックチェーンＢＣ１に登録しておく。このトランザクションを入力に設定して支払いトランザクションＴＸ１－１を生成できる。

【００４１】

利用者装置１は利用者の秘密鍵を保持しているので利用者の電子署名を付与することはできるが、権利者の電子署名を付与することはできない。支払いトランザクションＴＸ１－１は利用者の電子署名が付与されているが、権利者の電子署名が付与されていない不完全なトランザクションである。許諾要求トランザクションＴＸ２－１には、視聴を要求する利用者の情報やコンテンツの情報が含まれる。

【００４２】

許諾要求トランザクションＴＸ２－１がコンテンツ権利管理ブロックチェーンＢＣ２のＰ２Ｐネットワークにブロードキャストされると、許諾要求トランザクションＴＸ２－１を含むブロックＢ２がコンテンツ権利管理ブロックチェーンＢＣ２のＰ２Ｐネットワークに参加するノードによって生成されてコンテンツ権利管理ブロックチェーンＢＣ２に追加される。なお、支払いトランザクションＴＸ１－１を内包する許諾要求トランザクションＴＸ２－１がコンテンツ権利管理ブロックチェーンＢＣ２に登録されても支払いが完了したことにはならない。支払いトランザクションＴＸ１－１が仮想通貨ブロックチェーンＢＣ１に登録されたときに支払いが確定する。現段階は仮払いの状態である。

【００４３】

権利者装置２は、コンテンツ権利管理ブロックチェーンＢＣ２を同期して、許諾要求トランザクションＴＸ２－１を含むブロックＢ２を取得して記憶部２３に蓄積し、許諾要求トランザクションＴＸ２－１に内包された支払いトランザクションＴＸ１－１の正当性を検証する（ステップＳ１２）。

【００４４】

本実施例では、権利者装置２が支払いトランザクションＴＸ１－１の正当性を検証しているが、利用者装置１が許諾要求トランザクションＴＸ２－１を送信する際に正当性を検証してもよいし、許諾要求トランザクションＴＸ２－１を含むブロックＢ２を生成する装置がブロックＢ２を生成する際に支払いトランザクションＴＸ１－１の正当性を検証してもよい。

【００４５】

権利者装置２は、コンテンツ視聴を許諾する許諾トランザクションＴＸ２－２をコンテンツ権利管理ブロックチェーンＢＣ２のＰ２Ｐネットワークに送信する（ステップＳ１３）。コンテンツ権利管理ブロックチェーンＢＣ２のＰ２Ｐネットワークにより、許諾トランザクションＴＸ２－２を含むブロックＢ２がコンテンツ権利管理ブロックチェーンＢＣ２に追加される。

【００４６】

利用者装置１は、コンテンツ権利管理ブロックチェーンＢＣ２を同期して、許諾トランザクションＴＸ２－２を含むブロックＢ２を取得して記憶部１３に蓄積する（ステップＳ１４）。許諾トランザクションＴＸ２－２に記載された情報に基づいてコンテンツの視聴が可能になる。

【００４７】

支払いを確定するとき、権利者装置２は、許諾要求トランザクションＴＸ２－１に内包された支払いトランザクションＴＸ１－１を取り出し、支払いトランザクションＴＸ１－１に権利者の電子署名を付与して完全なトランザクションとし、支払いトランザクションＴＸ１－１を仮想通貨ブロックチェーンＢＣ１のＰ２Ｐネットワークに送信する（ステップＳ１５）。支払いトランザクションＴＸ１－１が仮想通貨ブロックチェーンＢＣ１のＰ２Ｐネットワークにブロードキャストされると、支払いトランザクションＴＸ１－１を含むブロックＢ１が仮想通貨ブロックチェーンＢＣ１のＰ２Ｐネットワークに参加するノードによって生成されて仮想通貨ブロックチェーンＢＣ１に追加される。これにより、マル

チシグのアドレスから権利者のアドレスへ支払い金額に相当する仮想通貨が移動し、権利者への支払いが確定する。このとき、支払いトランザクションＴＸ１－１に、コンテンツ権利管理ブロックチェーンＢＣ２での支払いを照会可能な情報を含めてもよい。支払いを参照可能な情報としては、例えば、許諾要求トランザクションＴＸ２－１のトランザクションＩＤや許諾要求トランザクションＴＸ２－１を含むブロックＢ２のブロック番号がある。

【００４８】

仮想通貨ブロックチェーンＢＣ１において権利者への支払いが確定後、仮想通貨ブロックチェーンＢＣ１での支払いを照会可能な情報を含めた支払い確定トランザクションＴＸ２－３をコンテンツ権利管理ブロックチェーンＢＣ２のＰ２Ｐネットワークに送信してもよい（ステップＳ１６）。支払いを照会可能な情報としては、例えば、支払いトランザクションＴＸ１－１のトランザクションＩＤや支払いトランザクションＴＸ１－１を含むブロックＢ１のブロック番号がある。

【００４９】

続いて、本実施の形態における決済システムにおいて利用者から権利者への支払いをまとめる動作について説明する。支払いトランザクションを仮想通貨ブロックチェーンＢＣ１に登録するためには、支払いトランザクションを含むブロックを生成した者に対する手数料が必要である。利用者から権利者への支払いをまとめて決済することで、仮想通貨ブロックチェーンＢＣ１での手数料を削減することが可能となる。

【００５０】

図３は、本実施の形態における決済システムにおいて利用者から権利者への支払いをまとめる動作を説明するための図である。図３の例では、図２において権利者装置２が支払いトランザクションＴＸ１－１を仮想通貨ブロックチェーンＢＣ１へ送信する前に（ステップＳ１５の前）、利用者が別のコンテンツ視聴の許諾を要求している。

【００５１】

利用者装置１は、支払いトランザクションＴＸ１－２と支払いトランザクションＴＸ１－２を内包する許諾要求トランザクションＴＸ２－４を生成し、許諾要求トランザクションＴＸ２－４をコンテンツ権利管理ブロックチェーンＢＣ２のＰ２Ｐネットワークに送信する（ステップＳ２１）。ここで、利用者装置１は前回の支払いトランザクションＴＸ１－１の支払いが確定していないことを検知すると、支払いトランザクションＴＸ１－１の内容を変更して支払いトランザクションＴＸ１－２を生成する。具体的には、支払いトランザクションＴＸ１－２には、前回の支払い金額（３００円）に今回の支払い金額（４００円）を加算した支払い金額（７００円）を記載する。利用者装置１は、支払いトランザクションＴＸ１－２に再度利用者の電子署名を付与する。

【００５２】

権利者装置２は、許諾要求トランザクションＴＸ２－４が内包する支払いトランザクションＴＸ１－２の正当性を検証する（ステップＳ２２）。ここでの支払いトランザクションＴＸ１－２の正当性の検証は、例えば、支払いトランザクションＴＸ１－２に記載された支払い金額（７００円）からひとつ前の支払いトランザクションＴＸ１－１に記載された支払い金額（３００円）を引いた金額が、新たなコンテンツ視聴の許諾に必要な金額（４００円）と等しいか否かを判定する。仮払いの金額、視聴を許諾したコンテンツなどの情報は全てコンテンツ権利管理ブロックチェーンＢＣ２に登録されているので、権利者装置２は、コンテンツ権利管理ブロックチェーンＢＣ２に登録された情報に基づいて正当性を検証することができる。

【００５３】

権利者装置２が利用者に新たなコンテンツの視聴を許諾する許諾トランザクションＴＸ２－５を送信し、利用者装置１が許諾トランザクションＴＸ２－５を取得することで（ステップＳ２３，Ｓ２４）、利用者は新たなコンテンツの視聴が可能となる。

【００５４】

権利者装置２は、任意のタイミング（例えば月末）で、支払いを確定する。

【００５５】
支払いを確定するとき、権利者装置２は、コンテンツ権利管理ブロックチェーンＢＣ２に登録されている最新の支払いトランザクションＴＸ１－２を取得し、支払いトランザクションＴＸ１－２に権利者の電子署名を付与して仮想通貨ブロックチェーンＢＣ１のＰ２Ｐネットワークに送信する（ステップＳ２５）。最新の支払いトランザクションＴＸ１－２には累積した支払い金額が記載されているので、最新の支払いトランザクションＴＸ１－２より前の支払いトランザクションＴＸ１－１を送信しない。
【００５６】
仮想通貨ブロックチェーンＢＣ１において権利者への支払いが確定後、仮想通貨ブロックチェーンＢＣ１での支払いを照会可能な情報を含めた支払い確定トランザクションＴＸ２－６をコンテンツ権利管理ブロックチェーンＢＣ２のＰ２Ｐネットワークに送信してもよい（ステップＳ２６）。
【００５７】
利用者装置１は、支払い確定トランザクションＴＸ２－６を確認した後にコンテンツ視聴の許諾を要求するときは、支払い金額の累積額を０にリセットして新たな支払いトランザクションを生成する。
【００５８】
次に、マルチシグネチャ方式を用いる利点について説明する。
【００５９】
上記実施例では、利用者の電子署名と権利者の電子署名が必要なマルチシグから権利者へ仮想通貨を移動する支払いトランザクションを許諾要求トランザクションに内包したが、利用者のみの電子署名で有効となる支払いトランザクションを用いることもできる。ただし、このような支払いトランザクションを用いた場合、以下の問題が考えられる。
【００６０】
第１に、コンテンツ権利管理ブロックチェーンＢＣ２のＰ２Ｐネットワークに参加する権利者装置２以外の装置が支払いトランザクションを取得して仮想通貨ブロックチェーンＢＣ１に登録できてしまうという問題がある。この場合、権利者装置２は支払いを確定するタイミングを制御できなくなり、支払いをまとめることが難しくなる。
【００６１】
マルチシグを用いた場合は、許諾要求トランザクションが内包する支払いトランザクションは権利者の電子署名が無く不完全なトランザクションである。権利者装置２以外の装置がこの支払いトランザクションを取得して仮想通貨ブロックチェーンＢＣ１へ送信しても登録されない。したがって、権利者装置２のみが支払いトランザクションに権利者の電子署名を付与して仮想通貨ブロックチェーンＢＣ１へ登録できる。
【００６２】
第２に、利用者が、支払いトランザクションの入力に設定した未使用のトランザクションを別のトランザクションの入力に使用できてしまうという問題がある。例えば、利用者装置１が支払いトランザクションを生成して許諾要求トランザクションに内包して送信した後、支払いトランザクションの入力に設定した未使用のトランザクションを別のトランザクションの入力として仮想通貨を用いた場合、権利者装置２が許諾要求トランザクションから支払いトランザクションを取得して仮想通貨ブロックチェーンＢＣ１へ送信すると、仮想通貨の二重譲渡となり支払いが確定しないおそれがある。
【００６３】
マルチシグを用いた場合は、マルチシグの仮想通貨を使用する際には利用者の電子署名と権利者の電子署名の両方が必要なので、利用者が勝手にマルチシグの仮想通貨を使用することはできない。したがって、権利者装置２は、任意のタイミングで確実に支払いを確定させることができる。
【００６４】
以上説明したように、本実施の形態によれば、利用者装置１が仮想通貨ブロックチェーンＢＣ１用の支払いトランザクションを内包する許諾要求トランザクションをコンテンツ

権利管理ブロックチェーンＢＣ２のＰ２Ｐネットワークに送信し、権利者装置２が許諾要求トランザクションに応じた許諾トランザクションをコンテンツ権利管理ブロックチェーンＢＣ２のＰ２Ｐネットワークに送信するとともに、許諾要求トランザクションに内包された支払いトランザクションを仮想通貨ブロックチェーンＢＣ１に送信することで、利用者及び権利者はコンテンツ権利管理ブロックチェーンＢＣ２を監視するだけで対価の支払いと視聴許諾を管理することが可能となる。また、コンテンツ視聴の許諾の要求から許諾までの時間は、コンテンツ権利管理ブロックチェーンＢＣ２の特性のみで決まるので、コンテンツ権利管理ブロックチェーンＢＣ２の特性を生かすことができる。

【００６５】

本実施の形態によれば、利用者の電子署名と権利者の電子署名が必要なマルチシグを用いることで、権利者は、任意のタイミングで、確実に支払いを確定させることができる。

【００６６】

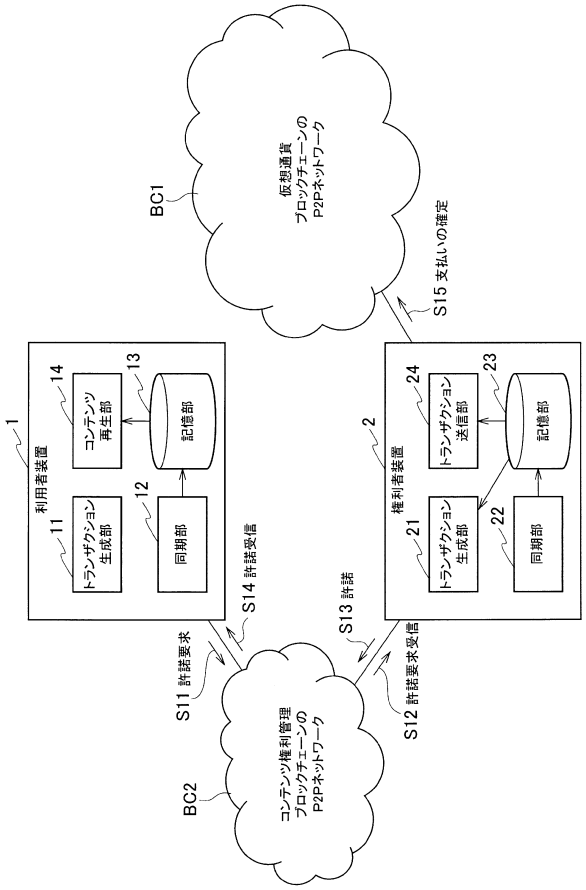
本実施の形態によれば、利用者装置１は、コンテンツ視聴の許諾を要求する際に、前回の支払いトランザクションでの支払いが確定していないときは、前回の支払いトランザクションに記載された支払い金額に今回のコンテンツ視聴の許諾に必要な金額を加算した新たな支払いトランザクションを生成し、権利者装置２は、新たな支払いトランザクションを内包する許諾要求トランザクションがコンテンツ権利管理ブロックチェーンＢＣ２に登録されている場合は、新たな支払いトランザクションより前の支払いトランザクションを仮想通貨ブロックチェーンＢＣ１に送信しないで、新たな支払いトランザクションのみを仮想通貨ブロックチェーンＢＣ１に送信することにより、コンテンツ視聴の許諾に対する支払い金額をまとめることができ、仮想通貨ブロックチェーンＢＣ１での手数料を削減することが可能となる。

【符号の説明】

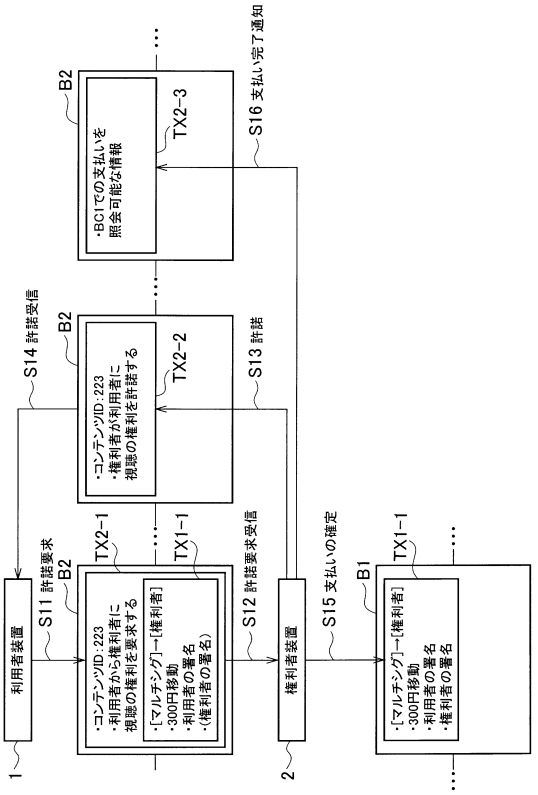
【００６７】

ＢＣ１…仮想通貨ブロックチェーン
ＢＣ２…コンテンツ権利管理ブロックチェーン
１…利用者装置
１１…トランザクション生成部
１２…同期部
１３…記憶部
１４…コンテンツ再生部
２…権利者装置
２１…トランザクション生成部
２２…同期部
２３…記憶部
２４…トランザクション送信部

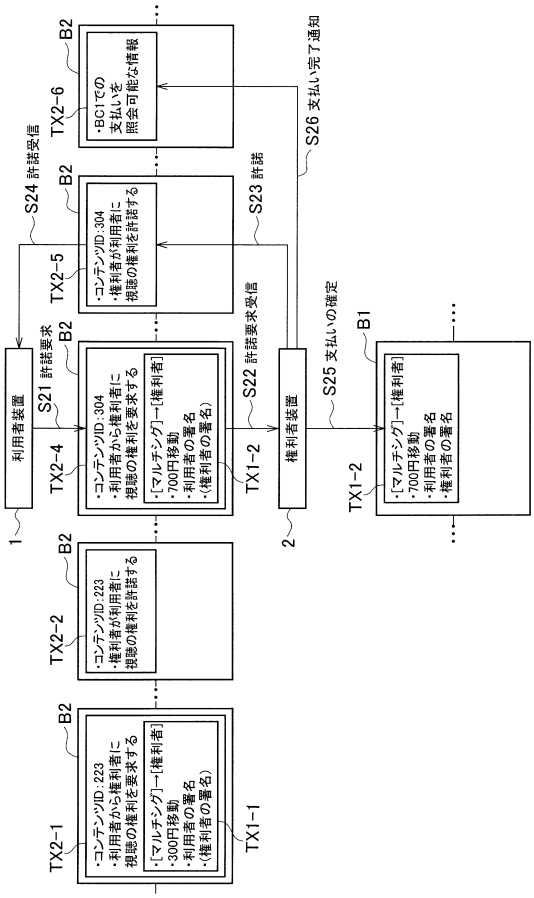
【図１】


BC1
仮想通貨
ブロックチェーンの
P2Pネットワーク
S15 支払いの確定
1
利用者装置
11
トランザクション
生成部
12
同期部
13
記憶部
14
コンテンツ
再生部
S14 許諾受信
S11 許諾要求
BC2
コンテンツ権利管理
ブロックチェーンの
P2Pネットワーク
S12 許諾要求受信
S13 許諾
2
権利者装置
21
トランザクション
生成部
22
同期部
23
記憶部
24
トランザクション
送信部

【図２】


1
利用者装置
S11 許諾要求
B2
TX2-1
・コンテンツID:223
・利用者から権利者に
視聴の権利を要求する
・[マルチシング]→[権利者]
・300円移動
・利用者の署名
・(権利者の署名)
TX1-1
S12 許諾要求受信
2
権利者装置
S15 支払いの確定
B1
TX1-1
・[マルチシング]→[権利者]
・300円移動
・利用者の署名
・権利者の署名
S16 支払い完了通知
S14 許諾受信
TX2-2
・コンテンツID:223
・権利者が利用者に
視聴の権利を許諾する
S13 許諾
TX2-3
・BC1での支払いを
照会可能な情報

【図３】


1
利用者装置
S21 許諾要求
B2
TX2-4
・コンテンツID:304
・利用者から権利者に
視聴の権利を要求する
・[マルチシング]→[権利者]
・700円移動
・利用者の署名
・(権利者の署名)
TX1-2
S22 許諾要求受信
2
権利者装置
S25 支払いの確定
B1
TX1-2
・[マルチシング]→[権利者]
・700円移動
・利用者の署名
・権利者の署名
S26 支払い完了通知
S24 許諾受信
TX2-5
・コンテンツID:304
・権利者が利用者に
視聴の権利を許諾する
S23 許諾
TX2-6
・BC1での
支払いを
照会可能な情報
TX2-2
・コンテンツID:223
・権利者から利用者に
視聴の権利を許諾する
TX1-1
・コンテンツID:223
・利用者から権利者に
視聴の権利を要求する
・[マルチシング]→[権利者]
・300円移動
・利用者の署名
・(権利者の署名)

フロントページの続き

(72)発明者　藤村　滋
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内
(72)発明者　中平　篤
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内
(72)発明者　宮崎　泰彦
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内
(72)発明者　大橋　盛徳
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内
(72)発明者　丸山　剛一
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内
(72)発明者　阿久津　明人
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内
(72)発明者　岸上　順一
北海道室蘭市水元町２７番１号　国立大学法人室蘭工業大学内

審査官　大野　朋也

(56)参考文献　特開２００５－３３９０８４（ＪＰ，Ａ）
特開２００２－２９７５５４（ＪＰ，Ａ）
国際公開第２０１１／１３８８３３（WO，Ａ１）
国際公開第２０１５／１７１５８０（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　１０／００－９９／００
Ｇ０６Ｆ　２１／６４