(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7587635号
(P7587635)

(45)発行日　令和6年11月20日(2024.11.20)

(24)登録日　令和6年11月12日(2024.11.12)

(51)国際特許分類			FI		
G06Q	*20/12*	*(2012.01)*	G06Q	20/12	300
G06Q	*20/38*	*(2012.01)*	G06Q	20/38	310
G06Q	*50/10*	*(2012.01)*	G06Q	50/10	
H04L	*9/32*	*(2006.01)*	H04L	9/32	200B

請求項の数　7　外国語出願　（全27頁）

(21)出願番号　特願2023-79777(P2023-79777)
(22)出願日　令和5年5月15日(2023.5.15)
(62)分割の表示　特願2021-145100(P2021-145100)の分割
原出願日　平成29年2月21日(2017.2.21)
(65)公開番号　特開2023-103362(P2023-103362A)
(43)公開日　令和5年7月26日(2023.7.26)
審査請求日　令和5年5月15日(2023.5.15)
(31)優先権主張番号　1603117.1
(32)優先日　平成28年2月23日(2016.2.23)
(33)優先権主張国・地域又は機関
英国(GB)
(31)優先権主張番号　1607484.1
(32)優先日　平成28年4月29日(2016.4.29)
最終頁に続く

(73)特許権者　318001991
エヌチェーン ライセンシング アーゲー
スイス・６３００・ツーク・グラーフェナウヴェーク・６
(74)代理人　100107766
弁理士　伊東 忠重
(74)代理人　100070150
弁理士　伊東 忠彦
(74)代理人　100135079
弁理士　宮崎 修
(72)発明者　ライト，クレイグ スティーヴン
イギリス国 シーエフ１０ ２エイチエイチ カーディフ チャーチル ウェイ チャーチル ハウス ７ス フロア アーカート－ダイクス アンド ロード エルエルピー
最終頁に続く

(54)【発明の名称】　デジタルコンテンツの制御及び配信のためのブロックチェーンにより実施される方法

(57)【特許請求の範囲】

【請求項１】

第１ノードにおいてデジタルコンテンツのエピソードを受信する、コンピュータにより実施される方法であって、

第２ノードから、エピソードシークレットを含む暗号化メッセージを受信するステップであって、前記エピソードシークレットは前記デジタルコンテンツに含まれる複数のエピソードのうちの１つのエピソードを識別するために使用され、前記暗号化メッセージは共有対称鍵により暗号化されている、ステップと、

前記第２ノードに、デジタルコンテンツのエピソードを提供するよう要求を送信するステップと、

前記エピソードシークレットからエピソードシークレットハッシュを決定するステップと、

前記エピソードシークレットハッシュ及び前記第２ノードに関連付けられた第２ユーザの第２公開鍵に基づき、支払Ｒｅｄｅｅｍスクリプトを含む暗号通貨支払額を転送するための支払トランザクションを決定するステップと、

前記第１ノードに関連付けられた第１ユーザの第１秘密鍵により、前記支払トランザクションに署名し、前記支払いトランザクションを前記第２ノードに送信するステップと、

前記第２ノードが前記支払トランザクションを検証することに応答して、デジタルコンテンツの前記エピソードにアクセスするステップと、

次のエピソードシークレットを受信し格納するステップと、

を含む方法。
【請求項２】
前記エピソードシークレットは、前記第２ノードにより決定される、請求項１に記載の方法。
【請求項３】
前記第１ノードは、前記共有対称鍵により前記暗号化メッセージを復号する、請求項１に記載の方法。
【請求項４】
第２ノードから第１ノードにデジタルコンテンツのエピソードを送信する、コンピュータにより実施される方法であって、
前記第１ノードに、前記第２ノードから要求可能なデジタルコンテンツのシリーズから、デジタルコンテンツの前記エピソードに関連付けられたエピソードシークレットを含む暗号化メッセージを送信するステップであって、前記エピソードシークレットは前記デジタルコンテンツに含まれる複数のエピソードのうちの１つのエピソードを識別するために使用され、前記暗号化メッセージは共有対称鍵により暗号化されている、ステップと、
前記第１ノードから、デジタルコンテンツの前記エピソードを提供するための要求と支払トランザクションを受信するステップと、
エピソードシークレットハッシュと前記第２ノードに関連付けられた第２ユーザの第２公開鍵に基づき、暗号通貨支払額を転送するための前記支払トランザクションが支払Ｒｅｄｅｅｍスクリプトを含むことを検証するステップと、
次のエピソードシークレットを決定するステップと、
前記第１ノードに前記次のエピソードシークレットを送信するステップと、
デジタルコンテンツの前記エピソードへのアクセスを提供するステップと、
を含む方法。
【請求項５】
前記次のエピソードシークレットを決定するステップは、データストアからの検索、又は新しいエピソードシークレットの生成を含む、請求項４に記載の方法。
【請求項６】
前記次のエピソードシークレットは、デジタルコンテンツの前記エピソードへのアクセスが提供されるのと同時に、前記第１ノードに提供される、請求項４又は５に記載の方法。
【請求項７】
前記第１ノードに、デジタルコンテンツの前記エピソードがアクセス可能であると示す通知を送信するステップ、を更に含む請求項４～６のいずれかに記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、デジタルコンテンツ・シリーズからデジタルコンテンツの支払及び配信のシステム及び方法に関する。本開示は、オンラインデジタルメディアのデジタル権利管理に適用できるが、これに関して限定されない。
【背景技術】
【０００２】
ブロックチェーンは、ブロックにより構成される、コンピュータに基づく非集中型の分散型システムとして実装されるピアツーピア電子台帳である。また、ブロックはトランザクションにより構成される。各トランザクションは、ブロックチェーンシステム内で参加者間のデジタル資産の制御の転送を符号化するデータ構造であり、少なくとも１つのインプット及び少なくとも１つのアウトプットを含む。各ブロックは前のブロックのハッシュを含み、ブロックは共にチェーンになって、その発端からブロックチェーンに書き込まれている全てのトランザクションの永久的な変更不可能なレコードを生成する。トランザクションは、そのインプット及びアウトプットに埋め込まれたスクリプトとして知られる小さなプログラムを含む。スクリプトは、トランザクションのアウトプットがどのように及

び誰によりアクセス可能かを指定する。ビットコインプラットフォーム上で、これらのスクリプトは、スタックに基づくスクリプト言語を用いて記述される。

【０００３】

トランザクションがブロックチェーンに書き込まれるために、「検証され」なければならない。ネットワークノード（マイナー）は、各トランザクションが有効であることを保証するために作業を実行し、無効なトランザクションはネットワークから拒否される。ノードにインストールされたソフトウェアクライアントは、自身のロック及びアンロックスクリプトを実行することにより、この検証作業を未使用トランザクション（ＵＴＸＯ）に対して実行する。ロック及びアンロックスクリプトの実行が真と評価した場合、トランザクションは有効であり、トランザクションはブロックチェーンに書き込まれる。したがって、トランザクションがブロックチェーンに書き込まれるためには、トランザクションは、ｉ）トランザクションを受信した第１ノードにより検証され、トランザクションが検証された場合に、ノードは該トランザクションをネットワーク内の他のノードに中継し、ｉｉ）マイナーにより構築された新しいブロックに追加し、ｉｉｉ）マインされ、つまり過去のトランザクションの公開台帳に追加されなければならない。

【０００４】

ブロックチェーン技術は、暗号通貨実装の使用で最も広く知られているが、デジタル起業家が、新しいシステムを実装するために、ビットコインの基づく暗号通貨セキュリティシステム、及びブロックチェーンに格納可能なデータの両方の使用を探索し始めている。ブロックチェーンが、暗号通貨の領域に限定されない自動タスク及び処理のために使用できれば、非常に有利である。このようなソリューションは、それらの用途において一層多様でありながら、ブロックチェーンの利点（例えば、永久的、イベントの耐タンパレコード、分散処理、等）を利用できる。

【０００５】

現在の研究の一分野は、「スマートコントラクト（smart contracts）」の実装のためのブロックチェーンの使用である。これらは、機械可読取引又は合意の条件の実行を自動化するために設計されたコンピュータプログラムである。自然言語で記述され得る従来の取引と異なり、スマートコントラクトは、結果を生成するためにインプットを処理できるルールを含み、該結果に依存して動作を実行させることのできる、機械実行可能プログラムである。

【０００６】

ブロックチェーンに関連する関心の他の分野は、ブロックチェーンを介する現実世界のエンティティを表し転送するための「トークン」（又は「カラードコイン」）の使用である。潜在的に機密な又は秘密のアイテムは、識別可能な意味又は値を有しないトークンにより表現できる。したがって、トークンは、現実世界のアイテムをブロックチェーンから参照できるようにする識別子として機能する。

【０００７】

デジタル権利管理は、著作権に制約されるデジタルメディアを制御することに関し、デジタルメディアの使用、変更及び配信を制限する制御技術を含む。デジタルメディアは、雑誌、新聞、ポッドキャスト、ソープオペラ、テレビシリーズ、等のような時系列コンテンツのように連続したコンテンツを含み得る。

【０００８】

デジタル権利管理の実装は、それぞれのユーザに関連するノード間で信頼を生成するために鍵交換を伴う、大規模中央システム又は複数のシステムを通じた著作権作品の管理を含むことがある。このようなシステムは管理が困難である場合があり、現行のアクセス権維持は達成することが困難な場合がある。幾つかの代替として、（認証局のような）信頼できる第三者が階層構造を生成するために使用されることがある。しかしながら、これらのシステムのうちの幾つかは、攻撃され易くなり得る大規模なシングルポイント障害を生じることがある。

【０００９】

本願明細書で、用語「ブロックチェーン」は、あらゆる形式の電子的な、コンピュータに基づく、分散台帳を含むよう使用される。これらは、限定ではないが、総意に基づくブロックチェーン及びトランザクションチェーン技術、許可及び未許可台帳、共有台帳、及びそれらの変形を含む。最も広く知られているブロックチェーン技術の用途はビットコイン台帳であるが、他のブロックチェーンの実装が提案され開発されている。ビットコインは便宜上及び説明を目的として本願明細書において言及されるが、本発明はビットコインのブロックチェーンと共に使用することに限定されず、代替のブロックチェーンの実装及びプロトコルが本発明の範囲に含まれることに留意すべきである。

【００１０】

本願明細書を通じて、用語「含む、有する（comprise）」又は「comprises」若しくは「comprising」のような変形は、記述される要素、整数若しくはステップ、又は要素、整数若しくはステップのグループ、の包含を意味すると理解されるが、任意の他の要素、整数若しくはステップ、又は要素、整数若しくはステップのグループを除外しない。

【００１１】

本願明細書に含まれる文書、動作、材料、装置、製品、等の議論は、これらの項目のうちのいずれか又は全部が従来基盤の部分を形成すること、又は本願の各請求項の優先日前に存在していたような本開示の関連分野における共通の一般知識であったとの承認として解釈されるべきではない。

【発明の概要】

【００１２】

本発明は、添付の請求項に定められるように、方法及びシステムを提供する。

【００１３】

本発明は、データの送信及び／又は配信を制御するよう構成された制御方法及び対応するシステムを提供し得る。送信は、コンピュータにより実装された又は通信ネットワークを介して若しくはそれに渡り行われ得る。データはデジタルコンテンツであって良い。本発明は、データの配信／送信を安全にするために暗号法及び／又は暗号化技術を組み込む方法／システムを提供し得る。したがって、本発明は、データ通信のための拡張されたセキュリティソリューションを提供し得る。

【００１４】

本願明細書では、用語「エピソード」は、用語「部分」と同義的に使用されることがある。しかしながら、本発明により送信され、配信され、及び／又は制御されるデジタルコンテンツは、ブロードキャストメディアの一回分、論理的チャプタ若しくはエピソード、又は芸術的コンテンツに限定されない。本願明細書及び請求項中の用語「エピソード」は、デジタルコンテンツの「部分」又は「単位」又は「量」を意味する。同様に、用語「シリーズ」は、本願明細書では、ブロードキャストシリーズの意味で、単にシリーズを意味する。シリーズは、単にデジタルコンテンツの複数の部分、グループ又は関連付けであって良い。「シリーズ」は、必ずしも順次的又は年代順を示すことに限定されない。さらに、本発明は、デジタルコンテンツの特性又は形式に関して限定されない。デジタルコンテンツは、娯楽メディアに限定されないが、任意の種類のデジタルコンテンツに関連して良い。

【００１５】

本発明は、システムであって、第１ユーザが共通アドレスにおける暗号通貨額に関連付けられる、システムを提供し得る。暗号通貨は、「保証金額」として参照されることがある。アドレスは、ネットワーク上のアドレスであって良い。アドレスはブロックチェーンアドレスであって良い。アドレスは、暗号鍵から導出され又はそれに関連付けられて良い。共通アドレスからの使用は、第１ユーザの少なくとも第１秘密鍵（V_1）及び第２ユーザの第２秘密鍵（V_2）の（デジタル）署名を必要とし得る。これは、所与の種類のブロックチェーントランザクションの使用により指定されて良い。トランザクション種類は、ブロックチェーンプロトコルの部分であり又はその中で定められて良い。

【００１６】

システムであって、
第１処理装置を有する、第１ユーザに関連付けられた第１ノードであって、
（Ａ）通信ネットワークを介して、デジタルコンテンツ・シリーズからデジタルコンテンツ・エピソード（ｉ）を提供するよう、前記第２ノードに要求を送信し、
（Ｂ）共通アドレスから前記第２ユーザへ暗号通貨支払額（Ｂ２）を転送するために、ブロックチェーントランザクション（$Ｅ_{ｉ}$）を決定し及び／又は生成し、前記暗号通貨支払額（Ｂ２）は、前記第１ユーザにより要求された前記デジタルコンテンツ・シリーズの中のデジタルコンテンツのエピソード数に基づき、
（Ｃ）前記第１秘密鍵（$Ｖ_{1}$）により前記支払トランザクション（$Ｅ_{ｉ}$）に署名し、次に前記支払トランザクション（$Ｅ_{ｉ}$）を前記第２ノードへ送信する、第１ノードと、
第２処理装置を有する、前記第２ユーザに関連付けられた第２ノードであって、
（Ｉ）前記通信ネットワークを介して、前記第１秘密鍵（$Ｖ_{1}$）により署名された前記デジタルコンテンツ・エピソード（ｉ）及び前記支払トランザクション（$Ｅ_{ｉ}$）を提供するための、前記第１ノードからの前記要求を受信し、
（ＩＩ）前記支払トランザクションを検証するよう構成され、前記支払トランザクションが前記第２ユーザへの前記暗号通貨支払額（Ｂ２）を含むことを検証することを含み、検証した結果に基づき、前記第２処理装置は、更に、
（ＩＩＩ）前記通信ネットワークを介して、前記第１ノードに利用可能にされるべき前記デジタルコンテンツ・エピソード（ｉ）へのアクセスを提供し、
（ＩＶ）前記第２ユーザの前記第２秘密鍵（$Ｖ_{2}$）により、前記支払トランザクションに共同署名し、前記共同署名した支払トランザクションをピアツーピア分散台帳へ送信するよう構成される、第２ノードと、
を含むシステム。

【００１７】

前記システムにおいて、前記第１処理装置は、ステップ（Ａ）から（Ｄ）を繰り返すことにより、前記デジタルコンテンツ・シリーズから次のデジタルコンテンツ・エピソードを要求するよう更に構成されて良い。前記第２処理装置は、前記要求を受信し、ステップ（Ｉ）から（ＩＩＩ）を繰り返すことにより前記次のデジタルコンテンツ・エピソードを配信するよう更に構成されて良く、前記支払トランザクションに共同署名しピアツーピア分散台帳へ送信するステップ（ＩＶ）は、前記次のエピソードを含むデジタルコンテンツ・エピソードの数を有する支払トランザクションに対して実行される。

有利なことに、本発明により提供される利点のうちの１つは、デジタルコンテンツの各部分が、更なる又は後の部分の（又はそれに関連付けられた）暗号鍵と一緒に暗号化されることである。鍵の使用は、デジタルコンテンツの部分が解読されていることの技術的証拠を提供する。したがって、デジタルコンテンツがアクセスされている、例えば閲覧され若しくは何らかの方法で消費され／使用されていることが決定できる。

【００１８】

前記システムにおいて、前記第１ユーザは前記共通アドレスに前記暗号通貨保証金額を預金して良く、前記第１処理装置は、通信ネットワークを介して、前記第１ユーザから前記共通アドレスへの前記暗号通貨保証金額（Ｂ１）の第１トランザクションをピアツーピア分散台帳（以後、単に「ブロックチェーン」として参照される場合がある）に記録するために、第１データアウトプット（$Ｏ_{1}$）を送信するよう構成される。

【００１９】

前記システムにおいて、指定時間の後、前記共通アドレスからの前記暗号通貨保証金額のトランザクションを伴わず、前記暗号通貨保証金額（Ｂ１）が返金されて良い。前記第１処理装置は、前記第１ユーザの第１秘密鍵（$Ｖ_{1}$）により、前記共通アドレスから前記第１ユーザへ前記暗号通貨保証金額（Ｂ１）を転送する第２トランザクションに共同署名するよう更に構成されて良い。前記第２処理装置は、前記第２秘密鍵（$Ｖ_{2}$）で、第２トランザクションに共同署名し、前記第１秘密鍵（$Ｖ_{1}$）及び前記第２秘密鍵（$Ｖ_{2}$）の両方により共同署名された第２トランザクションは、ピアツーピア分散台帳へ送信され、前

記暗号通貨保証金額（Ｂ１）を返金するために指定時間の後に有効にされ、前記指定時間の前に、前記共同署名された第２トランザクションを前記ピアツーピア分散台帳へ送信する、よう更に構成されて良い。

【００２０】

前記システムにおいて、前記第２処理装置は、前記通信ネットワークを介して、前記第１ユーザにより要求されるために利用可能な、前記デジタルコンテンツ・シリーズからの前記デジタルコンテンツ・エピソードに関連付けられたエピソードシークレット（S_i）を送信するよう更に構成されて良い。前記第１処理装置は、前記通信ネットワークを介して、前記エピソードシークレット（S_i）を受信し、前記エピソードシークレット（S_i）からエピソードシークレットハッシュ（H_i）を決定するよう更に構成されて良い。前記暗号通貨支払額（Ｂ２）を前記第２ユーザへ転送する支払トランザクション（E_i）を決定することは、前記第１処理装置が、前記エピソードシークレットハッシュ（H_i）と、前記第２ユーザの前記第２秘密鍵（V_2）との暗号対である第２公開鍵（P_2）と、に基づき支払Ｒｅｄｅｅｍスクリプト（ＳＲ１）を更に決定するよう構成されることを含む。前記第２処理装置が前記支払トランザクション（E_i）を検証するとき、前記第２処理装置は、前記支払Ｒｅｄｅｅｍスクリプト（ＲＳ１）が前記エピソードシークレットハッシュ（H_i）及び前記第２公開鍵（P_2）に基づくことを検証するよう更に構成される。

【００２１】

前記システムにおいて、前記第２処理装置は、前記デジタルコンテンツ・シリーズからの前記次のデジタルコンテンツ・エピソード（S_{i+1}）に関連付けられた次のエピソードシークレット（S_{i+1}）を決定し、前記次のエピソードシークレット（S_i）から次のエピソードシークレットハッシュ（H_{i+1}）を決定するよう更に構成されて良く、前記デジタルコンテンツ・エピソードを送信するステップ（ＩＩＩ）で又はその後に、前記第２処理装置は、前記通信ネットワークを介して、前記第１ノードへ次のエピソードシークレット（S_{i+1}）を送信するよう更に設けられる。前記第１処理装置は、前記通信ネットワークを介して、前記エピソードシークレット（S_{i+1}）を受信し、前記エピソードシークレット（S_{i+1}）から次のエピソードシークレットハッシュ（H_{i+1}）を決定するよう更に構成されて良い。対応する次の支払トランザクション（E_{i+1}）は、前記次のエピソードシークレットハッシュ（H_{i+1}）と前記第２公開鍵（P_2）とに基づき、次の支払Ｒｅｄｅｅｍスクリプト（ＲＳ２）を含む。前記第２処理装置が次の支払トランザクション（E_{i+1}）を検証するとき、前記第２処理装置は、前記次の支払Ｒｅｄｅｅｍスクリプト（ＲＳ２）が前記次のエピソードシークレットハッシュ（H_{i+1}）及び前記第２公開鍵（P_2）に基づくことを検証するよう更に構成される。

【００２２】

前記システムにおいて、前記支払トランザクション（E_i）は、前記共通アドレスから前記第１ユーザへの、前記第１ユーザへの暗号通貨おつり額（Ｂ３）の転送を更に有し、前記暗号通貨おつり額（Ｂ３）は、前記暗号通貨支払額（Ｂ２）だけ少ない前記暗号通貨保証金額（Ｂ１）に基づく。

【００２３】

前記システムにおいて、前記第２処理装置は、前記第１ノードと前記第２ノードとの間の共通シークレットを決定するよう更に構成されて良い。前記通信ネットワークを介する、前記デジタルコンテンツ・エピソードへのアクセスを提供することは、前記第２処理装置が、１又は複数のデジタルコンテンツ・エピソードを、前記共通シークレットに基づく鍵で暗号化して、１又は複数の暗号化デジタルコンテンツ・エピソードを提供し、前記１又は複数の暗号化デジタルコンテンツ・エピソードを送信することを含む。前記第１処理装置は、前記第１ノードと前記第２ノードとの間の共通シークレットを決定し、前記通信ネットワークを介して、前記１又は複数の暗号化デジタルコンテンツ・エピソードを受信し、前記１又は複数の暗号化デジタルコンテンツ・エピソードを、前記共通シークレットに基づく鍵で復号化して、前記１又は複数のデジタルコンテンツ・エピソードを提供するよう更に構成されて良い。

【００２４】
前記システムにおいて、前記第２処理装置は、共通シークレット基づく鍵で暗号化された、前記エピソードシークレット（S_i）、及び／又は前記次のエピソードシークレット（S_{i+1}）に基づき、暗号化メッセージを決定するよう更に構成されて良い。前記第１処理装置は、前記共通シークレット基づく鍵で暗号化メッセージを復号化することにより、前記エピソードシークレット（S_i）、及び／又は前記次のエピソードシークレット（S_{i+1}）を決定するよう更に構成されて良い。
【００２５】
デジタルコンテンツを受信する、コンピュータにより実施される方法であって、第１ユーザに関連付けられた第１ノードは第２ノードに関連付けられた第２ユーザへの支払と引き換えにデジタルコンテンツを受信し、前記第１ユーザは共通アドレスにある暗号通貨保証金額（Ｂ１）に関連付けられ、前記共通アドレスからの使用は前記第１ユーザの第１秘密鍵（V_1）及び前記第２ユーザの第２秘密鍵（V_2）の両方の署名を必要とし、前記方法は、
（Ａ）前記通信ネットワークを介して、前記第２ノードへ、デジタルコンテンツ・シリーズからデジタルコンテンツ・エピソード（ｉ）を提供する要求を送信するステップと、
（Ｂ）前記共通アドレスから前記第２ユーザへ暗号通貨支払額（Ｂ２）を転送するために、支払トランザクション（E_i）を決定するステップであって、前記暗号通貨支払額（Ｂ２）は、前記第１ユーザにより要求された前記デジタルコンテンツ・シリーズの中のデジタルコンテンツ・エピソードの数に基づく、ステップと、
（Ｃ）前記第１秘密鍵（V_1）により前記支払トランザクション（E_i）に署名するステップであって、次に前記支払トランザクション（E_i）を前記第２ノードへ送信して、前記第２ノードに前記支払トランザクションを検証させる、ステップと、を含み、
前記第２ノードが、前記支払トランザクションは前記暗号通貨支払額（Ｂ２）を含むことを検証したことに基づき、前記方法は、
（Ｄ）前記通信ネットワークを介して、前記デジタルコンテンツ・エピソード（ｉ）にアクセスするステップ、を更に含む方法。
【００２６】
前記方法は、ステップ（Ａ）から（Ｄ）を繰り返すことにより、前記デジタルコンテンツ・シリーズから次のデジタルコンテンツ・エピソードを要求するステップ、を更に含んで良い。
【００２７】
前記方法は、前記第１ユーザが、通信ネットワークを介して、前記第１ユーザから前記共通アドレスへの前記暗号通貨保証金額（Ｂ１）の第１トランザクションをピアツーピア分散台帳に記録するために、第１データアウトプット（Ｏ１）を送信するステップにより、前記共通アドレスに前記暗号通貨保証金額（Ｂ１）を手付け金として支払うことを更に含んで良い。
【００２８】
前記方法の別の例では、指定時間の後に、前記共通アドレスからの前記暗号通貨保証金額（Ｂ１）のトランザクションを伴わず、前記暗号通貨保証金額（Ｂ１）が返金され、前記方法は、前記第１ユーザの前記第１秘密鍵（V_1）により、前記共通アドレスから前記第１ユーザへ前記暗号通貨保証金額（Ｂ１）を転送する第２トランザクションに共同署名するステップであって、前記第２ユーザにより前記第２秘密鍵（V_2）で共同署名された共同署名第２トランザクションは、前記ピアツーピア分散台帳へ送信され、前記指定時間の後に、前記暗号通貨保証金額（Ｂ１）を返金するために有効にされる、ステップ、を更に含む。
【００２９】
前記方法は、前記通信ネットワークを介して、前記デジタルコンテンツ・シリーズから、前記第１ユーザにより要求されるために利用可能な、前記デジタルコンテンツ・エピソードに関連付けられたエピソードシークレット（S_i）を受信するステップと、前記エピ

ソードシークレット（S_i）からエピソードシークレットハッシュ（H_i）を決定するステップを更に含んで良い。前記支払トランザクション（E_i）の中の前記第２ユーザへの前記暗号通貨支払額（Ｂ２）は、前記エピソードシークレットハッシュ（H_i）と、前記第２ユーザの前記第２秘密鍵（V_2）との暗号対である第２公開鍵（P_2）と、に基づく支払Ｒｅｄｅｅｍスクリプト（ＳＲ１）を含む。

【００３０】

前記方法において、ステップ（Ｄ）において又はその後に、前記方法は、前記通信ネットワークを介して、前記デジタルコンテンツ・シリーズからの前記次のデジタルコンテンツ・エピソード（S_{i+1}）に関連付けられた次のエピソードシークレット（S_{i+1}）を受信するステップ、を更に含んで良い。前記デジタルコンテンツ・シリーズからの前記次のエピソードを要求するステップは、前記次のデジタルコンテンツ・エピソード（S_{i+1}）から次のエピソードシークレットハッシュ（H_{i+1}）を決定するステップを含み、対応する次の支払トランザクション（E_{i+1}）は、前記次のエピソードシークレットハッシュ（H_{i+1}）及び前記第２公開鍵（P_2）に基づく次の支払Ｒｅｄｅｅｍスクリプト（ＲＳ２）を含む。

【００３１】

前記方法において、前記支払トランザクション（E_i）は、前記共通アドレスから前記第１ユーザへの、暗号通貨おつり額（Ｂ３）の転送を更に含んで良く、前記暗号通貨おつり額（Ｂ３）は、前記暗号通貨支払額（Ｂ２）だけ少ない前記暗号通貨保証金額（Ｂ１）に基づく。

【００３２】

前記方法は、前記第１ノードと前記第２ノードとの間の共通シークレットを決定するステップ、を更に含んで良く、前記通信ネットワークを介して、前記デジタルコンテンツ・エピソードにアクセスするステップは、前記通信ネットワークを介して、暗号化デジタルコンテンツ・エピソードを受信するステップと、前記共通シークレットに基づく鍵により前記暗号化デジタルコンテンツ・エピソードを復号化して、前記デジタルコンテンツ・エピソードを提供するステップと、を含む。

【００３３】

前記エピソードシークレット（S_i）、及び／又は前記次のエピソードシークレット（S_{i+1}）を受信すると、前記方法は、前記共通シークレットに基づく鍵で暗号化メッセージを復号化することにより、前記エピソードシークレット（S_i）、及び／又は前記次のエピソードシークレット（S_{i+1}）を決定するステップを更に含んで良い。

【００３４】

デジタルコンテンツの配信を制御する、コンピュータにより実施される方法であって、第１ユーザに関連付けられた第１ノードは第２ノードに関連付けられた第２ユーザへの支払と引き換えにデジタルコンテンツを受信し、前記第１ユーザは共通アドレスにある暗号通貨保証金額（Ｂ１）に関連付けられ、前記共通アドレスからの使用は前記第１ユーザの第１秘密鍵（V_1）及び前記第２ユーザの第２秘密鍵（V_2）の両方の署名を必要とし、前記方法は、

（Ｉ）前記通信ネットワークを介して、前記第１ノードから、デジタルコンテンツ・シリーズからデジタルコンテンツ・エピソード（ｉ）を提供する要求を受信するステップと、

（ＩＩ）前記共通アドレスから前記第２ユーザへ暗号通貨支払額（Ｂ２）を転送する、前記第１秘密鍵（V_1）で署名された支払トランザクション（E_i）を受信するステップであって、前記暗号通貨支払額（Ｂ２）は、前記第１ユーザにより要求された前記デジタルコンテンツ・シリーズの中のデジタルコンテンツ・エピソードの数に基づく、ステップと、

（ＩＩＩ）前記支払トランザクションを検証するステップであって、前記支払トランザクションが前記第２ユーザへの前記暗号通貨支払額（Ｂ２）を含むことを検証することを含む、ステップと、を含み、検証の結果に基づき、前記方法は、

（ＩＶ）前記通信ネットワークを介して、前記デジタルコンテンツ・エピソードへのア

クセスを前記第１ノードに提供するステップと、
（Ｖ）前記第２ユーザの前記第２秘密鍵（$Ｖ_2$）で、前記支払トランザクションに共同署名し、前記共同署名された支払トランザクションを前記ピアツーピア分散台帳へ送信するステップと、を更に含む方法。
【００３５】
前記方法は、ステップ（Ｉ）から（ＩＶ）を繰り返すことにより、前記デジタルコンテンツ・エピソードから次のデジタルコンテンツ・エピソードを配信するステップであって、ステップ（Ｖ）は、前記次のエピソードを含むデジタルコンテンツ・エピソードの数を有する支払トランザクションに対して実行される、ステップ、を更に含んで良い。
【００３６】
前記方法の一例において、指定時間の後、前記共通アドレスからの前記暗号通貨保証金額のトランザクションを伴わず、前記暗号通貨保証金額（Ｂ１）が前記第１ユーザに返金されて良い。したがって、前記方法は、前記第２ユーザの前記第２秘密鍵（$Ｖ_1$）により、前記共通アドレスから前記第１ユーザへ前記暗号通貨保証金額（Ｂ１）を転送する第２トランザクションに共同署名するステップを更に含んで良く、前記第１ユーザにより前記第１秘密鍵（$Ｖ_1$）で共同署名された、前記共同署名された第２トランザクションは、前記ピアツーピア分散台帳へ送信され、前記指定時間の後に、前記暗号通貨保証金額（Ｂ１）を返金するために有効にされる。さらに、前記共同署名支払トランザクションを前記ピアツーピア分散台帳へ送信するステップは、前記指定時間の前に実行される。
【００３７】
前記方法は、前記通信ネットワークを介して、前記デジタルコンテンツ・シリーズから、前記第１ユーザにより要求されるために利用可能な、前記デジタルコンテンツ・エピソードに関連付けられたエピソードシークレット（$Ｓ_i$）を送信するステップと、前記エピソードシークレット（$Ｓ_i$）からエピソードシークレットハッシュ（$Ｈ_i$）を決定するステップを更に含んで良い。前記支払トランザクション（$Ｅ_i$）を検証するステップは、前記第２ユーザへの前記暗号通貨支払額（Ｂ２）を転送する対応する支払Ｒｅｄｅｅｍスクリプト（ＲＳ１）が、前記エピソードシークレットハッシュ（$Ｈ_i$）と、前記第２ユーザの前記第２秘密鍵（$Ｖ_2$）との暗号対である第２公開鍵（$Ｐ_2$）と、に基づくことを検証するステップを含む。
【００３８】
前記方法は、デジタルコンテンツ・シリーズからの次のデジタルコンテンツ・エピソード（$Ｓ_{i+1}$）に関連付けられた次のエピソードシークレット（$Ｓ_{i+1}$）を決定するステップと、前記次のエピソードシークレット（$Ｓ_i$）から次のエピソードシークレットハッシュ（$Ｈ_{i+1}$）を決定するステップと、を更に含んで良い。ステップ（ＩＶ）において又はその後に、前記方法は、前記通信ネットワークを介して、次のエピソードシークレット（$Ｓ_{i+1}$）を前記第１ノードへ送信するステップを更に含んで良い。前記次のエピソードについて次の支払トランザクションを検証するとき、前記方法は、前記第２ユーザへの前記次の暗号通貨支払額を転送する次の支払Ｒｅｄｅｅｍスクリプト（ＲＳ２）が、前記次のエピソードシークレットハッシュ（$Ｈ_{i+1}$）及び前記第２公開鍵（$Ｐ_2$）に基づくことを検証するステップを更に含む。
【００３９】
前記方法において、前記支払トランザクション（$Ｅ_i$）は、前記共通アドレスから前記第１ユーザへの、前記第１ユーザへの暗号通貨おつり額（Ｂ３）の転送を更に有して良く、前記暗号通貨おつり額（Ｂ３）は、前記暗号通貨支払額（Ｂ２）だけ少ない前記暗号通貨保証金額（Ｂ１）に基づく。
【００４０】
前記方法は、前記第１ノード及び前記第２ノードの間の共通シークレットを決定するステップを更に含んで良い。前記通信ネットワークを介して、前記デジタルコンテンツ・エピソードへのアクセスを提供するステップは、前記共通シークレットに基づく鍵で、前記デジタルコンテンツ・エピソードを暗号化するステップと、前記通信ネットワークを介し

て、前記暗号化デジタルコンテンツ・エピソードを送信するステップと、を含んで良い。
【００４１】
前記方法において、前記エピソードシークレット（S_i）、及び／又は前記次のエピソードシークレット（S_{i+1}）を送信するステップは、前記エピソードシークレット（S_i）、及び／又は前記次のエピソードシークレット（S_{i+1}）に基づき、前記共通シークレットに基づく鍵で暗号化された暗号化メッセージを決定するステップを更に含んで良い。
【００４２】
上述の本発明の任意の実施形態は、第１及び第２ノードに共通なシークレットを決定する方法、及び／又は該方法を実行するよう構成されたシステムを含み得る。前記方法は、
少なくとも第１ノードマスタ秘密鍵及び生成器値に基づき、第１ノード第２秘密鍵を決定するステップと、
少なくとも第２ノードマスタ秘密鍵及び前記生成器値に基づき、第２ノード第２秘密鍵を決定するステップと、
を含んで良く（又は前記システムは、上記のステップを実行するよう動作して良く）、
前記第１ノードにおいて前記共通シークレット（ＣＳ）を決定するステップは、前記第１ノード第２秘密鍵及び前記第２ノード第２公開鍵に基づいて良く、前記第２ノードにおいて前記共通シークレット（ＣＳ）を決定するステップは、前記第２ノード第２秘密鍵及び前記第１ノード第２公開鍵に基づいて良く、
前記第１ノード第２公開鍵及び前記第２ノード第２公開鍵は、それぞれ、少なくとも前記第１／第２ノードマスタ鍵及び前記生成器値に基づいて良い。
前記生成器値は、メッセージであり、又はメッセージから導出されて良い。生成器値は、ブロックチェーントランザクション（Ｔｘ）に格納されたメタデータから導出されて良い。
【００４３】
処理装置を有する装置であって、上述の方法のうちのいずれか１つを実行する装置。
【００４４】
コンピュータプログラムであって、処理装置に上述の方法のうちのいずれか１つを実施させる機械可読命令を含むコンピュータプログラム。
【００４５】
本発明の一実施形態又は態様に関して説明された任意の機能は、本発明の１又は複数の他の実施形態／態様に適用されても良い。本発明のシステムに関連して記載された任意の特徴は、本発明の方法に適用されて良く、逆も同様である。
【図面の簡単な説明】
【００４６】
本開示の例は、以下の図面を参照して記載される。
【００４７】
【図１】デジタルコンテンツを配信する例示的なシステムの概略図である。
【００４８】
【図２】第１ユーザ、第２ユーザ、及び共通アドレスの間のトランザクションを示す図である。
【００４９】
【図３】デジタルコンテンツを配信する及び受信するコンピュータにより実施される方法のフローチャートである。
【００５０】
【図４】返金トランザクションを初期化し及び生成するコンピュータにより実施される方法のフローチャートである。
【００５１】
【図５】一例によるデジタルコンテンツを配信する及び受信するコンピュータにより実施される方法の詳細なフローチャートである。
【００５２】

【図６】処理装置の簡略な例を示す。
【発明を実施するための形態】
【００５３】
＜概要＞
あるノードからのデジタルコンテンツの配信及び送信、及びデジタルコンテンツの別のノードからの受信を制御するシステム、装置、及び方法が、以下に記載される。図１は、通信ネットワーク８を介して、第２ユーザ７に関連付けられた第２ノード１７と通信する、第１ユーザ５に関連付けられた第１ノード１５を含むシステム１を示す。本例では、第１ユーザ５は、第１ノード１５においてデジタルコンテンツを受信することを要求でき、第２ユーザは、第２ノード１７を介して、デジタルコンテンツへのアクセスを提供する。第２ノード１７は、第１データストア１８から第１ノード１５へデジタルコンテンツを送信するステップ、及びコンテンツサーバ３に関連付けられた第２データストア１１にあるデジタルコンテンツを通信ネットワーク８を介して第１ノード１５に利用可能にするステップ、を含む多数の方法でデジタルコンテンツへのアクセスを提供し得る。
【００５４】
第１ノード１５及び／又は第２ノード１７は、通信ネットワーク８を介して、ピアツーピア分散台帳（ブロックチェーン）９と通信する。ブロックチェーン９は、トランザクションを受信し及び記録するために、１又は複数の処理装置１９に関連付けられて良い。ピアツーピア分散台帳の一例は、ビットコインプロトコルに基づくトランザクション（Ｔｘｓ）の分散台帳であるブロックチェーンを含む。したがって、台帳に関連付けられた処理装置１９は、「マイナー」により使用され又はそれに関連付けられた処理装置であって良い。
【００５５】
図２を参照すると、第１ユーザ５は、第２ユーザ７から、デジタルコンテンツ・シリーズからの未知数のデジタルコンテンツを購入したいと望み得る。第１ユーザ５にデジタルコンテンツを利用可能にする前に、第２ユーザ７は、第２ユーザ７がデジタルコンテンツに対して支払われることの信用を提供するために、保証金（デポジット）を要求する。
【００５６】
保証金を提供するために、第１ユーザ５は、第１トランザクション２１を実行して、共通アドレス２３へ暗号通貨保証金額（Ｂ１）を転送して良い。共通アドレス２３は、ビットコインプロトコルに従うＰ２ＳＨ（pay－to－script－hash）であって良く、共通アドレス２３からの使用は、第１ユーザ５の第１秘密鍵（$Ｖ_1$）及び第２ユーザ７の第２秘密鍵（$Ｖ_2$）の両方の署名を必要とする。つまり、共通アドレス２３からのトランザクションは、第１ユーザ５及び第２ユーザ７の両者により署名されなければならない。これにより、両者は、保証金が両者からの承認無しに使用されないという信用を有することができる。代替のマルチシグネチャ方法が共通アドレス２３からのトランザクションを認可するために使用されて良いことが理解される。
【００５７】
幾つかの例では、保証金は、時間制限されて良い。それにより、第１ユーザ５が指定時間内にデジタルコンテンツ・エピソードを受信することを要求しない場合（及び／又は他の条件で）、保証金は第１ユーザ５に返金される。この一例は、暗号通貨保証金額（Ｂ１）を第１ユーザ５に返金する第２トランザクション２５として、図２に示される。幾つかの例では、これは、第１ユーザ５及び第２ユーザ７の両者に、共通アドレス２３から第１ユーザ５への第２トランザクションに共同署名させることにより達成できる。ここで、第２トランザクションは指定時間の後にのみ有効にされる。例えば、指定時間は、Ｕｎｉｘ時間で表現される将来のｄ日間であって良い。この第２トランザクションは、次にブロードキャストされる。ここで、第２トランザクションは、指定時間後に有効トランザクションになる。
【００５８】
したがって、共通アドレスからの暗号通貨保証金額を使用する競合トランザクションが

指定時間前にブロードキャストされた場合、該競合トランザクションは有効トランザクションになる。指定時間の後に有効競合トランザクションをブロードキャストすることが、第２ユーザ７の関心事である。この後、暗号通貨保証金額（Ｂ１）が第１ユーザ（５）に返金される。本例では、これらの競合トランザクションは、第２ユーザ７が支払を受けるトランザクションを表すので、支払トランザクション２７、２７’、２７’’と称される。

【００５９】

支払トランザクション２７の生成を含む、デジタルコンテンツをどのように配信するかの簡単な例は、図３を参照して以下に記載される。図３は、第１ノード１５及び第２ノード１７により実行されるそれぞれの方法１００、２００を示す。

【００６０】

第１ユーザ５は、デジタルコンテンツ・シリーズからのデジタルコンテンツ・エピソードを受信したいと望むと、第１ノード１５を用いて、デジタルコンテンツについて要求を生成する。第１ノード１５（コンピュータ、モバイル通信装置、テレビジョン、等であって良い）は、通信ネットワーク８を介して、デジタルコンテンツ・エピソードを提供するための要求を第２ノード１５へ送信する（１１０）第１処理装置２３を含む。

【００６１】

第１ノード１５は、さらに、共通アドレス２３から第２ユーザ７へ暗号通貨支払額（Ｂ２）を転送する支払トランザクション（E_i）２７を決定する１２０。支払額（Ｂ２）は、第１ユーザ５により要求されたデジタルコンテンツ・シリーズの中のデジタルコンテンツ・エピソードの数に基づく。これは、以前に要求された（及び受信された）が第２ユーザ７により支払の受信されていないエピソードを含んで良い。簡略された例では、第２支払額（Ｂ２）は、要求されたエピソード数（ｉ）を各エピソードの価格（ｐ）で乗算したものであって良い。

【００６２】

第１ノード１５は、次に、第１秘密鍵（V_1）で、支払トランザクション（E_i）２７に署名する１３０。支払トランザクション（E_i）２７は、次に、第２ノード１７へ送信される。支払トランザクション（E_i）は第１秘密鍵（V_1）により署名されるだけであり、第２ノード１７が第２秘密鍵（V_2）で署名することを必要とするので、これは未だ有効なトランザクションではない。

【００６３】

第２ユーザ７に関連付けられた第２ノード１７を検討すると、第２ノードは、メインフレームコンピュータ、デスクトップコンピュータ、等を含んで良い第２処理装置２３’を有する。第２ノード１７の第２処理装置は、通信ネットワーク８を介して、第１ノード１５から、デジタルコンテンツ・エピソード及び第１秘密鍵（V_1）で署名された支払トランザクション（E_i）を提供するための要求を受信する２１０。

【００６４】

第２ノード１７がデジタルコンテンツ・エピソードを第１ノード１５及び第１ユーザ５に利用可能にする前に、第２ノード１７は、第２ユーザ１７が支払を受信できることを決定する必要がある。したがって、第２ノード１７は、次に、支払トランザクション（E_i）２７を検証する２２０。これは、支払トランザクション（E_i）２７が第２ユーザ７への暗号通貨支払額（Ｂ２）を含むことを検証することを含む。実際の例では、これは、正確な額の暗号通貨及び正確な宛先を決定することを含んで良い。

【００６５】

支払トランザクション（E_i）（つまり、特に、第２ユーザ７が支払われること）の検証に基づき、第２ノード１７は、次に、通信ネットワーク８を介して、第１ノード１５に利用可能にされるデジタルコンテンツ・エピソードへのアクセスを提供する２３０。また、これは、第１ノードがデジタルコンテンツ・エピソードにアクセスすることを許可する１４０。

【００６６】

支払トランザクション（E_i）２７を実行するために、第２ノード１７は、次に、第２

ユーザ５の第２秘密鍵（V_2）で支払トランザクション（E_i）２７に共同署名し２４０、共同署名した支払トランザクションをブロックチェーン９へ送信する。したがって、暗号通貨支払額（Ｂ２）は、暗号通貨保証金額（Ｂ１）を有した共通アドレス２３から転送される。

【００６７】

幾つかの例では、第１ユーザ５は、更なるエピソードを要求し受信する機会を有して良い。したがって、第２ユーザ１７は、（第１ユーザ５に提供された更なるエピソードから）より多くの支払を受信する機会を有して良く、したがって、第２トランザクション２５の保証金を返金する指定時間の近くの時間まで、共同署名し、共同署名支払トランザクションをブロックチェーン９へ送信するステップ２４０を遅らせて良い。次のエピソードを配信する一例が以下に記載される。

【００６８】

第１ノード１５は、次のエピソードについて、上述のステップ１１０、１２０、及び１３０を繰り返すことにより、デジタルコンテンツ・シリーズからの次のデジタルコンテンツ・エピソードについての要求を生成する。重要なことに、暗号通貨支払額は、次のエピソード（及び支払が行われていない、シリーズの中の前のエピソード）を考慮して調整される。第２ノード１７は、同様に、要求を受信し、上述のステップ２１０～２３０を繰り返すことにより次のデジタルコンテンツ・エピソードを配信する。

【００６９】

したがって、第２ノード１７は、２つの支払トランザクションを有する：第１支払トランザクション（E_i）２７は、デジタルコンテンツ・エピソード次第の暗号通貨支払額を含み、第２支払トランザクション（E_{i+1}）２７’は、次のデジタルコンテンツ・エピソード次第の及びそれを含む暗号通貨支払額を含む。第２ユーザ７は最大支払額を受信することに関心があるので、第２ノード１７は、次のエピソードの支払を含む支払を含む共同署名支払トランザクション２７’、つまり第２支払トランザクション（E_{i+1}）２７’に署名し送信するだけで良い２４０。したがって、第１支払トランザクション（E_i）２７は、第２ノード１７により廃棄されて良い。

【００７０】

本開示は、信頼レベルがより低いデジタルコンテンツを通信し、送信し、及び／又は配信するシステムを提供し得る。例えば、第１ユーザ５及び／又は第２ユーザ７の詐欺行為への露出度が最小化できる。一例では、第２ユーザ７が彼らの義務を果たすことができない場合、第１ユーザへの露出（例えば、潜在的な損失）は、（残りの額は返金されるので）１個のデジタルコンテンツ・エピソードの価格になり得る。

【００７１】

本開示は、シングルポイント障害及び攻撃に対する脆弱性を有し得る認証局のような他の第三者及び階層構造に依存しないシステムも提供できる。暗号技術の使用は、本発明により提供される送信／制御構成のセキュリティを向上する。

【００７２】

詳細な例は、説明を目的として以下に記載される。

【００７３】

＜初期化－暗号プロトコル＞

第１ノード５及び第２ノード７は、通信ネットワーク８を介して互いにセキュアな通信１０１、２０１を確立する。これは、共有対称暗号鍵（Ｓ）による暗号通信を含み得る。幾つかの例では、対称暗号鍵は、共有される共通シークレットに基づく。この共通シークレットを決定する技術は、次の通りであって良い：

少なくとも第１ノードマスタ秘密鍵及び生成器値に基づき、第１ノード第２秘密鍵を決定するステップと、

少なくとも第２ノードマスタ秘密鍵及び生成器値に基づき、第２ノード第２秘密鍵を決定するステップと、を含み、

第１ノードにおいて共通シークレット（ＣＳ）を決定するステップは、第１ノード第２

秘密鍵及び第２ノード第２公開鍵に基づき、第２ノードにおいて共通シークレット（ＣＳ）を決定するステップは、第２ノード第２秘密鍵及び第１ノード第２公開鍵に基づく。第１ノード第２公開鍵及び第２ノード第２公開鍵は、それぞれ、第１／第２ノードマスタキー及び生成器値に基づく。

【００７４】

共有される共通シークレットに基づき鍵を導出する方法は、本願明細書で後に詳述される。

【００７５】

＜共通アドレスへの暗号通貨保証金＞

共通アドレスへの第１トランザクション２１内の保証金を生成するために、第１ノードは共通アドレスを決定する必要がある。Ｐ２ＳＨ（pay to script hash）システムでは、これは、公開鍵（署名に使用される秘密鍵に対応する）に基づいて良い。一例では、これは、第１ノード５に既知であるべき第１ユーザ５の第１秘密鍵（V_1）に対応する第１公開鍵（P_1）を決定するステップを含む。これは、第２ノード１７、第三者、又はデータストアから第２公開鍵（P_2）を受信することにより決定され得る第２ユーザ５の第２公開鍵（P_2）を決定するステップも含む。第２公開鍵（P_2）は、必ずしもセキュアな方法で送信される必要はないが、幾つかの例では、第２公開鍵（P_2）は共有対称暗号鍵（Ｓ）で暗号化されて良い。

【００７６】

暗号鍵保証金額（Ｂ１）は、第１及び第２ユーザ５、７により相互に合意された額であって良い。しかしながら、暗号鍵保証金額（Ｂ１）は、デジタルコンテンツ・シリーズの中のデジタルコンテンツ・エピソードの受信可能な最大数の価格と等価であることが望ましい。これは、第１ユーザ５が全てのエピソードを受信して見ることを決定した場合に、保証金が全部のエピソードに対して支払うのに十分であることを保証する。したがって、シリーズは、エピソード数ｎを有し、エピソード当たりの価格はｐである場合、暗号通貨保証金額（Ｂ１）はｎ×ｐである。

【００７７】

暗号通貨保証金額（Ｂ１）を転送する第１トランザクション（A_1）２１の一例は、以下の表１及び２に示される。

【００７８】

［表１］第１トランザクション（A_1）

【表１】

トランザクション識別子			A_1
バージョン番号			
インプット数			1
インプット（アンロック）	前のトランザクション	ハッシュ	A_0
		アウトプットインデックス	
	署名スクリプト長		
	署名スクリプト		<アリスの署名><アリスの公開鍵>
	シーケンス番号		
アウトプット数			1
アウトプット（ロック）	値		*np*
	公開鍵スクリプト長		
	公開鍵スクリプト		OP_HASH160 <hash160(redeem script)> OP_EQUAL
ロック時間			0

【００７９】

［表２］トランザクション（A_1）のＲｅｄｅｅｍスクリプト

【表２】

Redeemスクリプト	OP_2 〈アリスの公開鍵〉〈ボブの公開鍵〉 OP_2 OP_CHECKMULTISIG

【００８０】
本例では、第１トランザクション（A_1）２１は、第１ユーザ（「アリス」）５の前のブロックチェーントランザクションからのインプット（第１ユーザの署名を必要とする）、共通アドレス（２３）へのアウトプット、を有する。本例では、アウトプットは、第１ユーザの公開鍵（P_1、「アリスの公開鍵」）及び第２ユーザの公開鍵（P_2、「ボブの公開鍵」）を含むＲｅｄｅｅｍスクリプトに基づくハッシュである。つまり、第１ブロックチェーントランザクション（A_1）２１のアウトプットを償還すること（redeeming）は、第１秘密鍵（V_1）による第１ユーザ５の及び第２秘密鍵（V_2）による第２ユーザ７の両者の署名を必要とする。
【００８１】
上述の第１トランザクション（A_1）２１を記録するステップは、図４に示されるような、第１ユーザ５により実行される方法１００に示される。ここで、第１ノードは、第１ノード１５は、ブロックチェーン９上に第１ユーザ５から共通アドレス（２３）への暗号通貨保証金額の第１トランザクションを記録するために、通信ネットワーク８を介して、第１データアウトプット（Ｏ１）を送信する。
【００８２】
＜返金トランザクションの生成＞
暗号通貨保証金額（Ｂ１）が指定時間の終了後に返金されるように、第２ブロックチェーントランザクション２５が次に生成される。
【００８３】
これは、第１ノード１５が第２トランザクション２５を生成するステップであって、将来の指定時間の後にのみ、暗号通貨保証金額（Ｂ１）を第１ユーザ５へ（back to）返す（spending）ステップを含む、ステップを含んで良い。指定時間は、Ｕｎｉｘ時間で表現される将来のｄ日間のロック時間を、第２トランザクションに設定するステップを含んで良い。
【００８４】
暗号通貨保証金額（Ｂ１）を返金する第２トランザクション（A_2）２５の一例は、以下の表３に示される。
【００８５】
［表３］第２トランザクション（A_2）

【表３】

トランザクション識別子			A_2
バージョン番号			
インプット数			1
インプット（アンロック）	前のトランザクション	ハッシュ	A_1
		アウトプットインデックス	0
	署名スクリプト長		
	署名スクリプト		OP_0 <アリスの署名> <ボブの署名> <redeem script>
	シーケンス番号		
アウトプット数			1
アウトプット（ロック）	値		*np*
	公開鍵スクリプト長		
	公開鍵スクリプト		OP_DUP OP_HASH160 <hash160(アリスの公開鍵)> OP_EQUALVERIFY OP_CHECKSIG
ロック時間			Unix時間で表現される将来のd日間（1970年1月1日 00:00:00UTCから経過した秒数）

【００８６】

本例では、第２トランザクション（Ａ$_2$）２５は、第１トランザクション（Ａ$_1$）２１からのインプットを有する。共通アドレス（２３）２３からのインプットをアンロックすることは、第１秘密鍵（Ｖ$_1$）による第１ユーザの署名及び第２秘密鍵（Ｖ$_2$）による第２ユーザの署名の両方を必要とする。本例では、アウトプットは、第１ユーザ５に暗号通貨保証金額（本例ではｎｐ）を返金する。したがって、アウトプットは、第１ユーザの公開鍵（Ｐ$_1$、「アリスの公開鍵」）のハッシュのみに基づく。つまり、第１ブロックチェーントランザクション（Ａ$_1$）２１のアウトプットを償還すること（redeeming）は、第１ユーザ５が彼ら自身の返金暗号通貨を自由に使用できるべきなので、第１秘密鍵（Ｖ$_1$）による第１ユーザ５の署名のみを必要とする。

【００８７】

重要なことに、第２トランザクション（Ａ$_2$）２５は、指定時間の後にのみ有効である。指定時間は、本例では、トランザクションが指定時間の後にのみ有効になるロック時間機能により達成される。例えば、ｄ日間（Ｕｎｉｘ時間で表現される）である。

【００８８】

第２トランザクション（Ａ$_2$）２５を記録するステップは、図４に、第１ノード１５により実行されるステップ１０５、１０７、及び第２ノード１７により実行されるステップ２０３、２０５、２０７として示される。第１ノード１５は、第１ユーザ５の第１秘密鍵（Ｖ$_1$）で、第２トランザクションに共同署名する１０５。この第２トランザクション（Ａ$_2$）２５は、次に、第２秘密鍵（Ｖ$_2$）で署名されるために、通信ネットワーク８を介して第２ノード１７へ送信される１０７。また第２ノード１７は、第２トランザクション（Ａ$_2$）２５を受信する２０３。さらに、第２ノード１７は、第２ユーザ７の第２秘密鍵（Ｖ$_2$）で第２トランザクション（Ａ$_2$）２５に共同署名する２０５。両方の秘密鍵により署名された第２トランザクション（Ａ$_2$）２５は、次に、通信ネットワーク８を介してブロックチェーン９へ送信され２０７、ブロックチェーン９において、（支払トランザクション２７のような）他の有効トランザクションが指定時間の前に送信されない場合に、暗号通貨保証金額（Ｂ１）を返金するために、該指定時間の後に有効にされる。

【００８９】

理解されるべきことに、これらのステップは他の順序で実行されて良い。例えば、第２ノード１７は、第２トランザクションに先ず署名し、次に署名するために第１ノードへ送信して良い。いずれかのノードが（署名する前に）第２トランザクションを生成でき、い

ずれかのノードが共同署名したトランザクションをブロックチェーン９へ送信できることが理解される。他の例では、第１及び第２ノード１５、１７は、トランザクションを他の中間ノードへ送信して良く、該中間ノードがトランザクションを他のノード及び／又はブロックチェーン９へ送信する。

【００９０】

＜デジタルコンテンツを再要求し、支払トランザクションを決定する＞

デジタルコンテンツを再要求し、及び支払トランザクションを生成する方法は、図５を参照して以下に記載される。

【００９１】

第２ノード１７は、各デジタルコンテンツ・エピソード（ｉ）について、対応するエピソードシークレット（Ｓ$_i$）を決定する。エピソードシークレット（Ｓ$_i$）は、シークレットを知っている者、特に第１ユーザ５及び第２ユーザ７について、エピソード（ｉ）を識別するために使用できる。これは、情報がブロックチェーン９へ送信される場合にプライバシを維持するために有用である得る。

【００９２】

第２ノード１７は、第１ノード１７へ、デジタルコンテンツ・シリーズの中の第１デジタルコンテンツ・エピソードのエピソードシークレット（Ｓ$_i$）を送信する２０８。本例では、第１ユーザ５及び第１ノード１５に利用可能な以下のエピソードのエピソードシークレットのみが、送信される。後続のエピソードシークレットは、第１ノード１５が第１エピソードにアクセスするまで、公表されない。これは、エピソードが順次アクセスされることを保証する。

【００９３】

エピソードシークレット（Ｓ$_i$）を送信するとき２０８、第２ノード１１７は、エピソードシークレット（Ｓ$_i$）の秘密性を維持するために、共有対称暗号鍵（Ｓ）でエピソードシークレット（Ｓ$_i$）を暗号化することにより、暗号化メッセージを生成し送信して良い。第１ノード１５は、次に、第２ノード１７から、エピソードシークレット（Ｓ$_i$）を含む暗号化メッセージを受信する１０８。第１ノード１５は、次に、共有対称暗号鍵（Ｓ）により暗号化メッセージを復号化して、エピソードシークレット（Ｓ$_i$）を得る。

【００９４】

第１ノード１５は、第１ユーザ５が第１デジタルコンテンツ・エピソードにアクセスするまで、データストアにエピソードシークレット（Ｓ$_i$）を格納して良い。指定時間が終了していないとすると（つまり、ｄ日の前である）、方法１００は、第１ノード１５において、通信ネットワーク８を介して、第１デジタルコンテンツ・エピソードを提供するよう、第２ノード１７へ要求を送信するステップ１１０を含む。この要求は、後述する第１ノードにおいて決定された１２０、第１エピソードについての支払トランザクション２７を伴う。

【００９５】

＜支払トランザクションを決定する＞

支払トランザクション（Ｅ$_i$）２７は、有効な場合、共通アドレス（２３）（特に、それからの暗号通貨保証金額（Ｂ１））から使用され、したがって、第１ユーザ５及び第２ユーザ７の両者の署名を必要とする。したがって、支払トランザクション（Ｅ$_i$）２７を決定した後に、第１ノード１５は、支払トランザクション（Ｅ$_i$）２７に署名して、ブロックチェーン９へ送信する前に共同署名するために第２ノード１７へ送信する必要がある。

【００９６】

第１ノード１５は、先ず、エピソードシークレット（Ｓ$_i$）からエピソードシークレットハッシュ（Ｈｉ）を決定する１２１。これは、ＯＰ＿ＨＡＳＧ１６０のようなハッシュ関数を使用するステップを含んで良い（ここで、インプットは２回、ＳＨＡ－２５６により及び次にＲＩＰＥＭＤ－１６０により、ハッシュされる）。理解されるべきことに、他のハッシュ関数が適切であっても良い。

【００９７】

支払トランザクション（E_i）２７は、本例では、Ｐ２ＳＨの形式である。したがって、支払トランザクション（E_i）２７を決定するステップは、本例ではエピソードシークレットハッシュ（H_i）と第２ユーザ７の第２公開鍵（P_2）とに基づく支払Ｒｅｄｅｅｍスクリプト（ＲＳ１）であるＲｅｄｅｅｍスクリプトを決定するステップを更に含む。Ｒｅｄｅｅｍスクリプトにエピソードシークレットハッシュ（H_i）を含むことは、この特定の支払トランザクションが（エピソードシークレットハッシュ（H_i）及びエピソードシークレット（S_i）に関連付けられた）特定のエピソードのアクセスに関連することの証明として使用できる。第２に、第２ユーザ７の第２公開鍵（P_2）は、対応する第２秘密鍵（V_1）を有する第２ユーザ７だけが該支払を使用できることを保証する。

【００９８】

支払トランザクション（E_i）２７を決定するステップ１２０は、第２ノード７の暗号通貨支払額（Ｂ２）を決定するステップを更に含む。第１エピソードの場合には、この支払額は、第１エピソードの価格である。しかしながら、第１ユーザ５は、後続のエピソードについての更なる要求を生成するので、暗号通貨支払額（Ｂ２）は、要求されたエピソードに基づき変化する。簡単な例では、これは、エピソード数をエピソード当たりの価格により乗算したものであって良い。

【００９９】

第２ユーザ７へのアウトプットに加えて、支払トランザクション（E_i）２７は、第１ユーザ５に戻される別のアウトプットを含んで良い。この第１ユーザ５に戻されるアウトプットは、第１ユーザに戻される暗号通貨保証金額（Ｂ１）のおつりを表して良い。一例では、第１ユーザ５への暗号通貨おつり額（Ｂ３）は、暗号通貨支払額（Ｂ２）だけ少ない暗号通貨保証金額（Ｂ１）に基づいて良い。

【０１００】

方法１００は、次に、第１秘密鍵（V_1）により、支払トランザクション（E_i）２７に署名し、続いて、第２ノード１７に支払トランザクションを検証させるために、支払トランザクション（E_i）２７を第２ノード１７へ送信するステップ１３０を含む。

【０１０１】

支払トランザクション（E_i）の一例は、表４及び５に示される。

【０１０２】

［表４］支払トランザクション（E_i）

【表４】

トランザクション識別子			E_i
バージョン番号			
インプット数			1
インプット（アンロック）	前のトランザクション	ハッシュ	A_1
		アウトプットインデックス	0
	署名スクリプト長		
	署名スクリプト		〈アリスの署名〉〈ボブの署名〉〈redeem script〉
	シーケンス番号		
アウトプット数			2
アウトプット1（ロック）	値		ip
	公開鍵スクリプト長		
	公開鍵スクリプト		OP_HASH160 〈hash160(redeem script)〉 OP_EQUAL
アウトプット2（ロック）	値		$(n-i)p$
	公開鍵スクリプト長		
	公開鍵スクリプト		OP_DUP OP_HASH160 〈hash160(アリスの公開鍵)〉 OP_EQUALVERIFY OP_CHECKSIG
ロック時間			0

【０１０３】

［表５］アウトプット１　支払トランザクション（Ｅ$_i$）のＲｅｄｅｅｍスクリプト

【表５】

Redeemスクリプト	OP_HASH160 〈h_i〉 OP_EQUALVERIFY 〈ボブの公開鍵〉 OP_CHECKSIG

【０１０４】

このトランザクションへのインプットは、支払トランザクションが共通アドレス（２３）から使用されているので、第１ユーザ５の第１秘密鍵（Ｖ$_1$）の署名（「アリスの署名」）及び第２ユーザ７の第２秘密鍵（Ｖ$_2$）の署名（「ボブの署名」）の両方の署名を必要とするアンロックスクリプトを含む。

【０１０５】

「アウトプット１」は、暗号通貨支払額（Ｂ２）の第２ユーザ７へのアウトプットを示す。このアウトプットは、表５に示す支払Ｒｅｄｅｅｍスクリプト（ＲＳ１）により償還され（redeem）得る。表５は、上述のようにエピソードシークレットハッシュ（Ｈ$_i$）及び第２ユーザ公開鍵（Ｐ$_2$）（「ボブの公開鍵」）に基づく。

【０１０６】

「アウトプット２」は、第２ユーザ７に戻る暗号通貨おつり額（Ｂ３）であるアウトプットを示す。第１ユーザがこの暗号通貨おつり額（Ｂ３）を自由に使用できるべきなので、アウトプットスクリプトは、第１ユーザの公開鍵Ｐ$_1$（アリスの公開鍵）に基づくことに留意する。

【０１０７】

＜支払トランザクションを検証する＞

第２ノード１７は、通信ネットワーク８を介して、第１デジタルコンテンツ・エピソードを提供する要求を受信する２１０。相応して、第２ノード１７は、さらに、第１ノード１５から、第１秘密鍵（Ｖ$_1$）で署名された支払トランザクション（Ｅ$_i$）を受信することが期待される。

【０１０８】

デジタルコンテンツ・エピソードを提供する要求に合意する前に、第２ノードは、第１

ユーザ７が彼らが支払を受け取ることの信用を有することができるように、支払トランザクション（E_i）を検証する。

【０１０９】

第２ノード１７は、エピソードシークレット（S_i）からエピソードシークレットハッシュ（H_i）を決定する１２１。これは、第１ノード１５と同じ方法で、ハッシュ関数を使用するステップを含んで良い。第２ノードは、次に、受信した支払トランザクション（E_i）が第２ノード７への暗号通貨支払額（Ｂ２）を含むことを検証する２２０。これは、値が要求されたエピソード数を価格で乗算したものに等しいことを検証することにより、（表４の「アウトプット１」の中のアウトプット値のような）アウトプット値が正しい値であることを検証することを含み得る。

【０１１０】

検証するステップ２２０は、支払Ｒｅｄｅｅｍスクリプト（ＲＳ１）がエピソードシークレットハッシュ（H_i）及び第２公開鍵（P_2）に基づくことを検証するステップを更に含んで良い。これは、受信した支払トランザクション（E_i）の中の（Ｒｅｄｅｅｍスクリプトに基づく）アウトプットスクリプトを、エピソードシークレットハッシュ（H_i）及び第２公開鍵（P_2）の既知の値（又はその派生物）の対応するハッシュと比較することにより達成できる。この比較が、アウトプットスクリプトは正しいエピソードシークレットハッシュ（H_i）及び第２公開鍵（P_2）を有する期待Ｒｅｄｅｅｍスクリプトに一致することを示す場合、第２ノード１７（及び第２ユーザ７）は、受信した支払トランザクション（E_i）のｂｏｎａ　ｆｉｄｅの信用を有することができる。

【０１１１】

第２ノード１７は支払トランザクション（E_i）２７に署名して、直ちにブロックチェーン９へ送信できるが、第２ユーザ７は、第１ユーザ５が更なるデジタルコンテンツ・エピソードについての更なる要求を生成し得るので、指定時間に近くなるまで、そのしようとしない。

【０１１２】

検証が成功した後に、第２ノード１７は、次に、要求されたエピソードへのアクセス、及び第１ノードが更なるコンテンツ（次のエピソードである）を要求できるように次のエピソードシークレットを第１ノード１５に提供する。

【０１１３】

＜次のエピソードシークレットを決定する＞

第２ノード１７は、次に、シリーズの中にもうエピソードが無くなるまで、デジタルコンテンツ・シリーズの中の（エピソード（ｉ）の後の提供されるべきエピソードである）次のエピソードｉ＋１の次のエピソードシークレット（S_{i+1}）を決定する２２１。これは、データストア１８から次のエピソードシークレット（S_{i+1}）を読み出すステップ、又は新しいシークレットを生成するステップを含んで良い。次のエピソードシークレット（S_{i+1}）は、次のエピソードシークレットハッシュ（H_{i+1}）を決定するために使用される。次のエピソードシークレットハッシュ（H_{i+1}）は、第１ユーザ５が将来に次のエピソードについて要求を生成することを決定した場合に、次の支払トランザクションの中で使用される。

【０１１４】

次のエピソードシークレット（S_{i+1}）は、第２ノードが現在要求されたデジタルコンテンツ・エピソードへのアクセスを提供するのと同時に、第１ノード１５に提供されて良い。

【０１１５】

＜デジタルコンテンツへのアクセスを提供する＞

支払トランザクション（E_i）２７が検証されると、第２ノード１７は、第１ノード１５にデジタルコンテンツ・エピソードへのアクセスを提供する２３０。これは、多数の方法で達成できる。一例では、第２ノード１７はデジタルコンテンツ・エピソードを共有対称暗号鍵（Ｓ）で暗号化し、暗号化デジタルコンテンツ・エピソードを通信ネットワーク

８を介して第１ノード１５へ送信して良い。別の例では、第２ノードは、暗号化デジタルコンテンツ・エピソードを、コンテンツサーバ３に関連付けられたデータストア１１において提供して良い。それにより、第１ノード１５は、第１ノード１５にとって適切な時間に、データストア１１から暗号化エピソードを受信できる。更に別の例では、第２ノード１５は、エピソードを復号化するために、エピソード固有暗号鍵を提供して良い。

【０１１６】

一例では、要求されたデジタルコンテンツ・エピソード（ｉ）は、次のエピソードシークレット（S_{i+1}）と連結されて良い。連結は、次に、共有対称暗号鍵により暗号化されて良く、第２ノード１７は、次に、暗号化された連結へのアクセスを提供する。

【０１１７】

第２ノード１７は、次に、通信ネットワーク８を介して、第１ノード１５へ、要求されたデジタルコンテンツ・エピソード（ｉ）がアクセスされるために利用可能であることを示す通知を送信して良い。

【０１１８】

一方、第１ノード１５は、次に、（例えば、データストア１１からダウンロードする又は第２ノード１７から直接、等により）暗号化された連結にアクセスし、共有対称暗号鍵により復号化する１４０。これは、第１ノード１５において、デジタルコンテンツ・エピソード（ｉ）及び次のエピソードシークレット（S_{i+1}）を提供する。重要なことに、これは、消費のために及び次のエピソード（つまり、次のエピソードシークレット（S_{i+1}））を得る手段のために、第１ユーザにデジタルコンテンツ・エピソードを提供する。第１ノード１５は、後の使用のために、次のエピソードシークレット（S_{i+1}）を格納して良い１４１。

【０１１９】

理解されるべきことに、幾つかの代替では、次のエピソードシークレットは、他の時間に第２ノード１７から第１ノード１５へ送信されて良く２２３、デジタルコンテンツ・エピソードと連結されない。これは、通信ネットワークを介して別個の暗号化メッセージとして、次のエピソードシークレット（S_{i+1}）を送信するステップを含んで良い。

【０１２０】

＜次のエピソードを再要求する＞

第１ユーザ５が次のエピソードｉ＋１を見たいと望む場合、第１ノード１５は、上述の、デジタルコンテンツ・エピソードについての要求を送信するステップ１１０、次の支払トランザクションを決定するステップ１２０、及び次の支払トランザクションに署名するステップ１３０を繰り返して良い。これは、次のエピソードシークレット（S_{i+1}）及び対応する決定された次のエピソードシークレットハッシュ（H_{i+1}）により行うことができる。また、第２ノード１５は、要求及び次の支払トランザクションを受信するステップ２１０、次の支払トランザクションを検証するステップ２２０、及び次のエピソードへのアクセスを提供するステップ２３０を繰り返す。

【０１２１】

これらは、全部のデジタルコンテンツ・エピソードが第１ノード１５によりアクセスされるまで、又は指定時間ｄ日間の終了に近い又は終了するとき、繰り返され得る。これらの状況では、第２ノード１５は、次に、第２ユーザ７への支払を実施する後続のステップを実行する。

【０１２２】

＜支払トランザクションに共同署名する＞

デジタルコンテンツ・シリーズの中の全部のエピソードが第１ノード１５によりアクセスされると、更なる支払トランザクション２７’’が存在しないので、第２ユーザ７は、支払を受信するために、最後の支払トランザクション（E_i）２７’’に共同署名しようとする。代替として、指定時間の終了期間が近付いている場合、第１ユーザ５が更なる要求を生成する可能性が低いので、第２ユーザ７は、最後の支払トランザクション（E_i）２７’’に共同署名しようとする。更に重要なことに、支払トランザクション（E_i）は、共同署名

され、第２トランザクション（返金トランザクション）が有効になる前に該支払トランザクション（Ｅ$_i$）が確実に記録されるために、指定時間の前にブロックチェーン９へ送信されなければならない。

【０１２３】

したがって、方法２００は、第２ノード１７が第２秘密鍵（Ｖ$_2$）で最後の支払トランザクション（Ｅ$_i$）２７’’に共同署名し、共同署名した支払トランザクションをブロックチェーン９へ送信するステップ２４０を含む。

【０１２４】

第２ユーザ７が暗号通貨支払額（Ｂ２）を使用したいと望むとき、第２ノード１７は、第２ユーザ秘密鍵（Ｖ$_2$）及び支払トランザクション（Ｅ$_i$）の中のエピソードシークレットハッシュ（Ｈ$_i$）に対応するエピソードシークレット（Ｓ$_i$）で署名することにより表５に示されるＲｅｄｅｅｍスクリプトに署名することにより、トランザクションをアンロックする。これは、以下の表６のアンロックスクリプトに示される。表５に示すフォーマットのＲｅｄｅｅｍスクリプトは、第２ノード１７により、第２ユーザ公開鍵（Ｐ$_2$）及びエピソードシークレット（Ｓ$_i$）に基づき決定され得ることに留意する。ここで、エピソードシークレット（Ｓ$_i$）はエピソードシークレットハッシュ（Ｈ$_i$）を導出するために使用される。

【０１２５】

［表６］暗号通貨支払額を使用する第２ユーザ。

【表６】

トランザクション識別子			B
バージョン番号			
インプット数			1
インプット（アンロック）	前のトランザクション	ハッシュ	E_i
		アウトプットインデックス	0
	署名スクリプト長		
	署名スクリプト		<ボブの署名> <s_i> <redeem script>
	シーケンス番号		
アウトプット数			
アウトプット（ロック）	値		*ip*
	公開鍵スクリプト長		[ボブがどのように使用するかに依存する]
	公開鍵スクリプト		[ボブがどのように使用するかに依存する]

【０１２６】

＜変形＞

本開示の広範な一般的範囲から逸脱せずに、多数の変形及び／又は変更が上述の実施形態に対して行われることが、当業者により理解される。本発明の実施形態は、したがって、あらゆる面で、単に説明であり限定的でないと考えられる。

【０１２７】

ある例示的変形では、各支払トランザクション（Ｅ$_i$）は、それ自体が、有効になる前のそれぞれの支払指定時間を有して良い。例えば、支払指定時間は、支払トランザクション（Ｅ$_i$）が第２トランザクションの前に有効トランザクションであるように、第２トランザクション（つまり、返金トランザクション）の指定時間（例えば、ｄ日間）の前の時間（例えば、ｄ－１日）であって良い。

【０１２８】

したがって、この変形では、第２ノード１７は、支払トランザクションを検証すると、支払トランザクション（Ｔｘ）に直ちに共同署名し、ブロックチェーン９へ送信して良い。

【０１２９】

後続の支払トランザクションについて、これらの後続の支払トランザクションは、先行する支払トランザクションの指定時間（例えば、ｄ－１日間）より早い、それぞれの指定時間（例えば、ｄ－２日間）を有する。したがって、後続の支払トランザクションは、共同署名されブロックチェーン９へ送信されると、より早い支払トランザクション及び第２（返金）トランザクションより先行し、有効にされる。この変形の利点は、第２ノード１７が第２（返金）トランザクションの指定時間に近い時間において障害を有する場合、支払トランザクションが既に共同署名されブロックチェーン９へ送信されているので、第２ユーザ７が依然として支払を受信することである。

【０１３０】

＜共有共通シークレットに基づく共有対称鍵＞

２つのノードの間の共通シークレットを生成する方法は、以下に説明される。共通シークレットは、暗号鍵の生成において使用され得る。

【０１３１】

＜共通シークレットを決定する＞

方法は、共通シークレットをノードのうちのいずれか１つへ及び／又はそれから送信させる必要がなく、２つのノードの間の共通シークレットの生成を可能にする。各ノードは、それぞれ（楕円曲線暗号対のような）非対称暗号対を有し、各対は、マスタ秘密鍵及びマスタ公開鍵を含む。例えば、第１ノードは、マスタ秘密鍵（V_{1P}）及びマスタ公開鍵（P_{1P}）を有して良く、第２ノードは、マスタ秘密鍵（V_{1E}）及びマスタ公開鍵（P_{1E}）を有して良い。各ノードのそれぞれ第２秘密鍵及び公開鍵は、マスタ秘密鍵、マスタ公開鍵、及び生成器値に基づき決定されて良い。生成器値（又は生成器値を導出するために使用されるメッセージ）は、ノードへ及び／又はそれから、通信される。

【０１３２】

共通シークレットは、第２秘密鍵及び公開鍵に基づき、ノードの各々において決定されて良い。第１ノード及び第２ノードの間の共通シークレットを決定する一例が以下に記載される。第１及び第２ノードの両者は、両ノードに共通な生成器値を決定する。生成器値は、メッセージにより受信されて良く、又はメッセージから導出されて良い。

【０１３３】

第１ノードにおいて、共通シークレット（ＣＳ）は、

（ｉ）第１ノードマスタ秘密鍵（V_{1P}）及び生成器値（ＧＶ）に基づく第１ノード第２秘密鍵（V_{2P}）と、

（ｉｉ）第２ノードマスタ公開鍵（P_{1E}）及び生成器値（ＧＶ）に基づく第２ノード第２公開鍵（P_{2E}）と、に基づく。

【０１３４】

第２ノードにおいて、共通シークレット（ＣＳ）は、

（ｉｉｉ）第１ノードマスタ公開鍵（P_{1P}）及び生成器値（ＧＶ）に基づく第１ノード第２公開鍵（P_{2P}）と、

（ｉｖ）第２ノードマスタ秘密鍵（V_{1E}）及び生成器値（ＧＶ）に基づく第２ノード第２秘密鍵（V_{2E}）と、に基づく。

【０１３５】

したがって、共通シークレットは、次の通りである。

【０１３６】

$$\text{共通シークレット（ＣＳ）} = (V_{2P} \times P_{2E}) = (P_{2P} \times V_{2E})$$

【０１３７】

＜情報を安全に送信する＞

共通シークレットは、セキュアな送信のために情報を暗号化するために使用できる。例えば、対称鍵は共通シークレットに基づいて良い。両方のノードが同じ共通シークレットを有するので、それらは、（例えば非セキュアなネットワークを介して）２つのノードの間で送信される情報を暗号化し及び復号化するために使用可能な同じ対称鍵を決定できる。

【０１３８】

＜処理装置＞

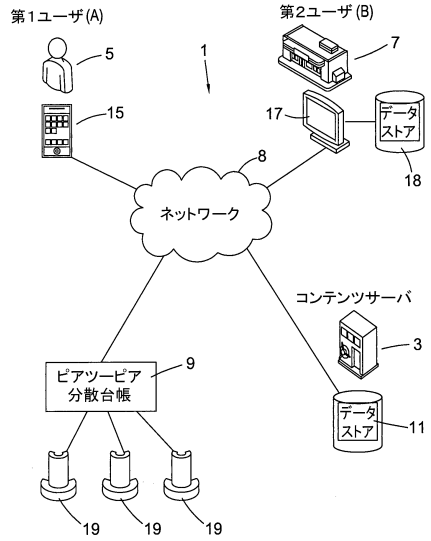
上述のように、第１ユーザ５及び第２ユーザ７は、それぞれ第１ノード１５及び第２ノード１７に関連付けられる。第１ノード１５及び第２ノード１７は、コンピュータ、タブレットコンピュータ、モバイル通信装置、コンピュータサーバ、コンピュータ端末、等のような電子装置であって良い。このような電子装置は、処理装置を含んで良い。したがって、第１ノードは第１処理装置２３を有し、第２ノード１７は第２処理装置２３’’を有する。電子装置は、データストア１１、１８及びユーザインタフェースにも関連付けられて良い。ユーザインタフェースの例は、キーボード、マウス、モニタ、タッチスクリーンディスプレイ、等を含む。ブロックチェーン９は、複数の処理装置１９にも関連付けられて良い。

【０１３９】

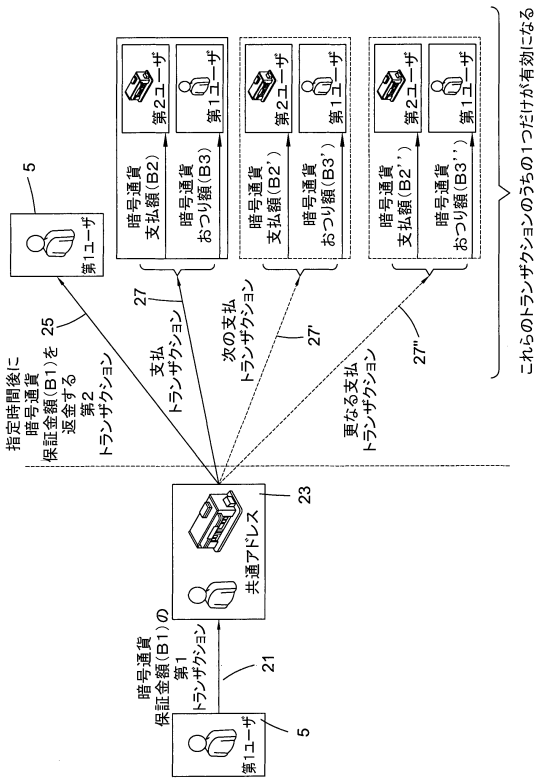
図６は、処理装置１９、２３の一例を示す。処理装置１９、２３は、バス１５３０を介して互いに通信する、プロセッサ１５１０、メモリ１５２０、及びインタフェース装置１５４０を含む。メモリ１５２０は、上述の方法１００、２００を実施するための命令及びデータを格納し、プロセッサ１５１０は、メモリ１５２０からの（コンピュータプログラムのような）該命令を実行して、方法１００、２００を実施する。インタフェース装置１５４０は、通信ネットワーク８、及び幾つかの例ではユーザインタフェース及びデータストア１１、１８のような周辺機器との通信を実現する通信モジュールを含んで良い。留意すべきことに、処理装置１５１０は独立名ネットワーク要素であって良いが、処理装置１５１０は別のネットワーク要素の部分であっても良い。さらに、処理装置１９、２３により実行される幾つかの機能は、複数のネットワーク要素の間で分散されて良い。例えば、第１ユーザ５は、（第１ユーザのモバイル通信装置、タブレット、デスクトップコンピュータ、ホームメディアプレイヤ、テレビジョン、等のような）複数の処理装置２３に関連付けられて良く、方法１００のステップは、実行され、これらの装置のうちの１つより多くに渡り分散されて良い。

【図面】

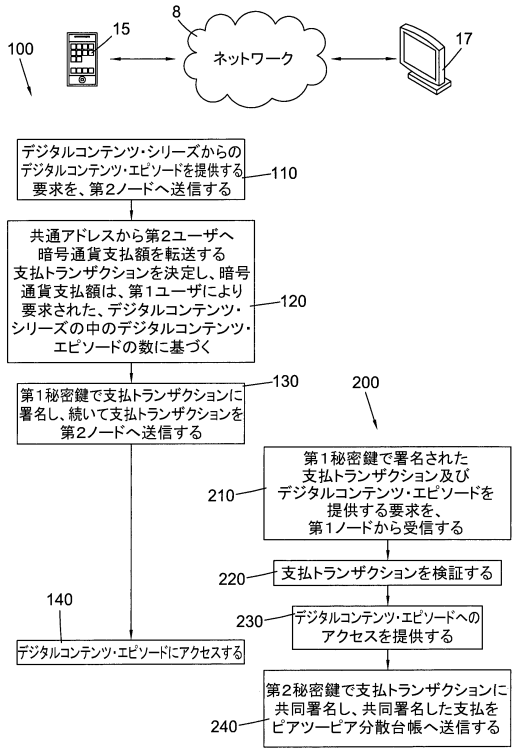
【図１】


第1ユーザ(A)
第2ユーザ(B)
1
5
7
15
17
データストア
18
8
ネットワーク
コンテンツサーバ
3
9
ピアツーピア分散台帳
データストア
11
19
19
19

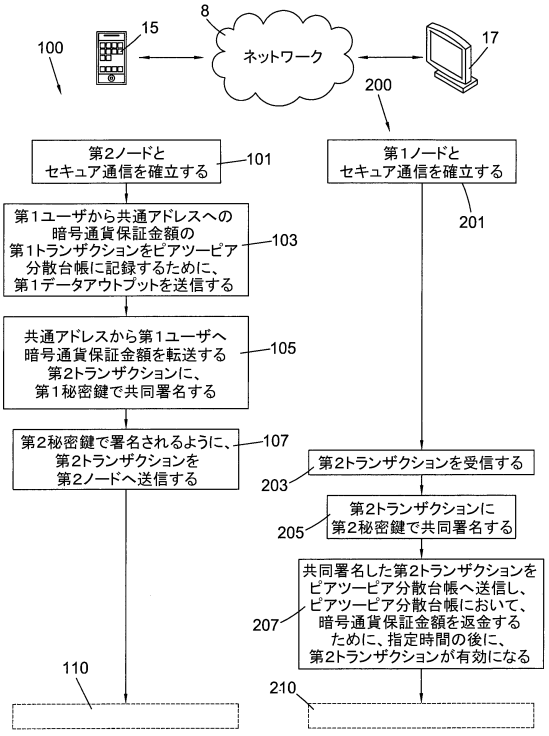
【図２】


第2ユーザ
第1ユーザ
暗号通貨支払額(B2)
暗号通貨おつり額(B3)
暗号通貨支払額(B2')
暗号通貨おつり額(B3')
暗号通貨支払額(B2'')
暗号通貨おつり額(B3'')
これらのトランザクションのうちの1つだけが有効になる
5
第1ユーザ
27
25
27'
27''
指定時間後に暗号通貨保証金額(B1)を返金する第2トランザクション
支払トランザクション
次の支払トランザクション
更なる支払トランザクション
23
共通アドレス
暗号通貨保証金額(B1)の第1トランザクション
21
5
第1ユーザ

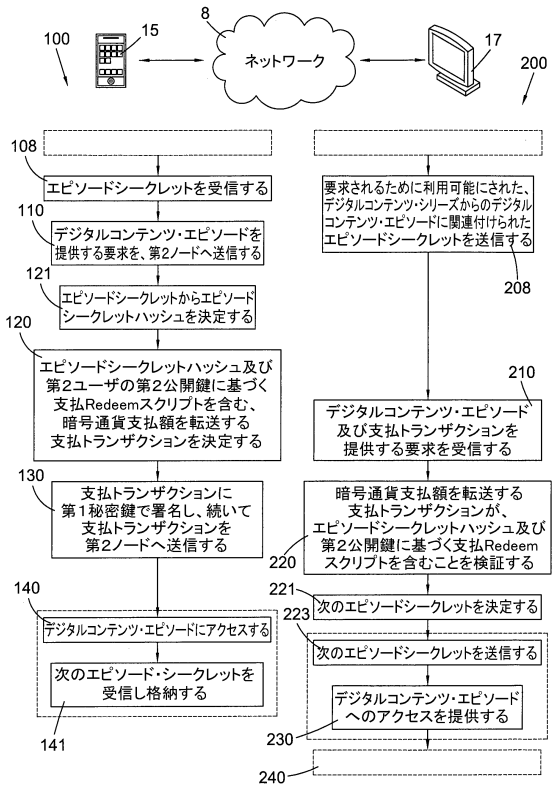
【図３】


100
15
8
ネットワーク
17
デジタルコンテンツ・シリーズからのデジタルコンテンツ・エピソードを提供する要求を、第2ノードへ送信する
110
共通アドレスから第2ユーザへ暗号通貨支払額を転送する支払トランザクションを決定し、暗号通貨支払額は、第1ユーザにより要求された、デジタルコンテンツ・シリーズの中のデジタルコンテンツ・エピソードの数に基づく
120
第1秘密鍵で支払トランザクションに署名し、続いて支払トランザクションを第2ノードへ送信する
130
200
第1秘密鍵で署名された支払トランザクション及びデジタルコンテンツ・エピソードを提供する要求を、第1ノードから受信する
210
支払トランザクションを検証する
220
デジタルコンテンツ・エピソードへのアクセスを提供する
230
140
デジタルコンテンツ・エピソードにアクセスする
第2秘密鍵で支払トランザクションに共同署名し、共同署名した支払をピアツーピア分散台帳へ送信する
240

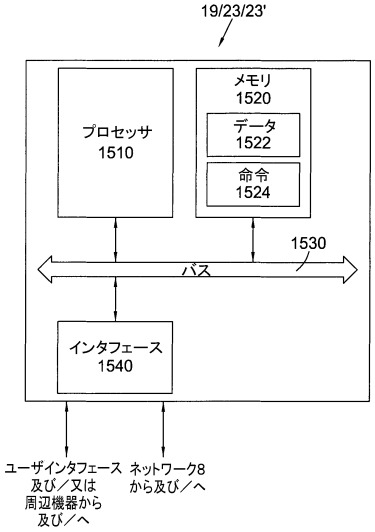
【図４】


100
15
8
ネットワーク
17
200
第2ノードとセキュア通信を確立する
101
第1ノードとセキュア通信を確立する
201
第1ユーザから共通アドレスへの暗号通貨保証金額の第1トランザクションをピアツーピア分散台帳に記録するために、第1データアウトプットを送信する
103
共通アドレスから第1ユーザへ暗号通貨保証金額を転送する第2トランザクションに、第1秘密鍵で共同署名する
105
第2秘密鍵で署名されるように、第2トランザクションを第2ノードへ送信する
107
第2トランザクションを受信する
203
第2トランザクションに第2秘密鍵で共同署名する
205
共同署名した第2トランザクションをピアツーピア分散台帳へ送信し、ピアツーピア分散台帳において、暗号通貨保証金額を返金するために、指定時間の後に、第2トランザクションが有効になる
207
110
210

【図５】


100
15
8
ネットワーク
17
200
108
エピソードシークレットを受信する
110
デジタルコンテンツ・エピソードを提供する要求を、第2ノードへ送信する
121
エピソードシークレットからエピソードシークレットハッシュを決定する
120
エピソードシークレットハッシュ及び第2ユーザの第2公開鍵に基づく支払Redeemスクリプトを含む、暗号通貨支払額を転送する支払トランザクションを決定する
130
支払トランザクションに第1秘密鍵で署名し、続いて支払トランザクションを第2ノードへ送信する
140
デジタルコンテンツ・エピソードにアクセスする
次のエピソード・シークレットを受信し格納する
141
要求されるために利用可能にされた、デジタルコンテンツ・シリーズからのデジタルコンテンツ・エピソードに関連付けられたエピソードシークレットを送信する
208
210
デジタルコンテンツ・エピソード及び支払トランザクションを提供する要求を受信する
220
暗号通貨支払額を転送する支払トランザクションが、エピソードシークレットハッシュ及び第2公開鍵に基づく支払Redeemスクリプトを含むことを検証する
221
次のエピソードシークレットを決定する
223
次のエピソードシークレットを送信する
デジタルコンテンツ・エピソードへのアクセスを提供する
230
240

【図６】


19/23/23'
プロセッサ
1510
メモリ
1520
データ
1522
命令
1524
1530
バス
インタフェース
1540
ユーザインタフェース及び／又は周辺機器から及び／へ
ネットワーク8から及び／へ

フロントページの続き

(33)優先権主張国・地域又は機関
英国(GB)
(31)優先権主張番号 1619301.3
(32)優先日 平成28年11月15日(2016.11.15)
(33)優先権主張国・地域又は機関
英国(GB)
内
(72)発明者 サヴァナ，ステファヌ
イギリス国 シーエフ１０ ２エイチエイチ カーディフ チャーチル ウェイ チャーチル ハウス ７ス フロア アーカート－ダイクス アンド ロード エルエルピー 内
審査官 板垣 有紀
(56)参考文献 特開２００８－０９９１３８（ＪＰ，Ａ）
米国特許出願公開第２０１４／０２３６７７４（ＵＳ，Ａ１）
特開２００７－３１１９３６（ＪＰ，Ａ）
(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｑ １０／００ － ９９／００
Ｈ０４Ｌ ９／３２