(19)日本国特許庁(JP)　(12)特　許　公　報(B1)　(11)特許番号
特許第6583841号
(P6583841)
(45)発行日　令和1年10月2日(2019.10.2)　(24)登録日　令和1年9月13日(2019.9.13)

(51)Int.Cl.　F I
G06Q 20/10 (2012.01)　G06Q 20/10

請求項の数 7　(全 22 頁)

(21)出願番号　特願2018-120654(P2018-120654)
(22)出願日　平成30年6月26日(2018.6.26)
審査請求日　平成30年10月30日(2018.10.30)

早期審査対象出願

(73)特許権者　504209655
国立大学法人佐賀大学
佐賀県佐賀市本庄町１番地
(74)代理人　100099634
弁理士　平井　安雄
(72)発明者　中山　功一
佐賀県佐賀市本庄町１番地　国立大学法人佐賀大学内
(72)発明者　森山　裕鷹
佐賀県佐賀市本庄町１番地　国立大学法人佐賀大学内

審査官　池田　聡史

最終頁に続く

(54)【発明の名称】情報通信装置、情報通信方法及び情報通信プログラム

(57)【特許請求の範囲】
【請求項１】
電子データを他のコンピュータに送信するデータ送信手段と、
前記データ送信手段が前記電子データを送信するのに伴って、ブロックチェーンにアクセスするための前記電子データに関するデジタル通貨の送金トランザクションを生成し、当該送金トランザクションを前記ブロックチェーンにブロードキャストする送金制御手段と、
前記電子データを他のコンピュータから受信するデータ受信手段と、
前記データ受信手段が前記電子データを受信するのに伴って、当該電子データの差出人からの前記デジタル通貨の入金状態を前記ブロックチェーンにアクセスして確認し、確認された入金状態に応じて前記電子データの受信を確定する受信制御手段と、
前記受信制御手段が前記電子データの受信を確定した場合に、入金された前記デジタル通貨の一部又は全部を前記電子データに対する受信者の参照、保存、破棄、及び／又は返信の操作種別に応じて返金する返金トランザクションを生成し、前記ブロックチェーンにブロードキャストする返金制御手段とを備えることを特徴とする情報通信装置。
【請求項２】
請求項１に記載の情報通信装置において、
前記電子データの宛先となる受信者を識別するための電子データ利用者識別情報と、ブロックチェーンへのアクセスに必要となる前記受信者を識別するＢＣ利用者識別情報とを対応付けて記憶する対応情報記憶手段を備え、

前記送金制御手段が、前記受信者の電子データ利用者識別情報に対応付けられた前記ＢＣ利用者識別情報に基づいて、前記送金トランザクションを生成する情報通信装置。
【請求項３】
請求項１又は２に記載の情報通信装置において、
前記電子データの差出人となる送信者を識別するための電子データ利用者識別情報と、ブロックチェーンへのアクセスに必要となる前記送信者を識別するＢＣ利用者識別情報とを対応付けて記憶する対応情報記憶手段を備え、
前記受信制御手段が、前記送信者の電子データ利用者識別情報に対応付けられた前記ＢＣ利用者識別情報に基づいて、前記送信者からの前記デジタル通貨の入金状態を前記ブロックチェーンにアクセスして確認する情報通信装置。
【請求項４】
請求項１ないし３のいずれかに記載の情報通信装置において、
前記返金制御手段が、前記電子データの受信を確定した後の当該電子データに対する前記受信者の操作種別に応じて、入金された前記デジタル通貨の返金額を調整する情報通信装置。
【請求項５】
請求項１に記載の情報通信装置において、
前記デジタル通貨の前記ブロックチェーン上で当該デジタル通貨の授受に関する契約処理を実行する契約履行手段が前記ブロックチェーン上に備えられている情報通信装置。
【請求項６】
コンピュータが、
電子データを他のコンピュータに送信するデータ送信ステップと、
前記データ送信ステップで前記電子データが送信されるのに伴って、ブロックチェーンにアクセスするための前記電子データに関するデジタル通貨の送金トランザクションを生成し、当該送金トランザクションを前記ブロックチェーンにブロードキャストする送金制御ステップと、
前記電子データを他のコンピュータから受信するデータ受信ステップと、
前記データ受信ステップで前記電子データが受信されるのに伴って、当該電子データの差出人からの前記デジタル通貨の入金状態を前記ブロックチェーンにアクセスして確認し、確認された入金状態に応じて前記電子データの受信を確定する受信制御ステップと、
前記受信制御ステップで前記電子データの受信が確定された場合に、入金された前記デジタル通貨の一部又は全部を前記電子データに対する受信者の参照、保存及び／又は返信の操作種別に応じて返金する返金トランザクションを生成し、前記ブロックチェーンにブロードキャストする返金制御ステップとを実行することを特徴とする情報通信方法。
【請求項７】
電子データを他のコンピュータに送信するデータ送信手段、
前記データ送信手段が前記電子データを送信するのに伴って、ブロックチェーンにアクセスするための前記電子データに関するデジタル通貨の送金トランザクションを生成し、当該送金トランザクションを前記ブロックチェーンにブロードキャストする送金制御手段、
前記電子データを他のコンピュータから受信するデータ受信手段、
前記データ受信手段が前記電子データを受信するのに伴って、当該電子データの差出人からの前記デジタル通貨の入金状態を前記ブロックチェーンにアクセスして確認し、確認された入金状態に応じて前記電子データの受信を確定する受信制御手段、
前記受信制御手段が前記電子データの受信を確定した場合に、入金された前記デジタル通貨の一部又は全部を前記電子データに対する受信者の参照、保存及び／又は返信の操作種別に応じて返金する返金トランザクションを生成し、前記ブロックチェーンにブロードキャストする返金制御手段としてコンピュータを機能させることを特徴とする情報通信プログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電子データの送受信に伴ってデジタル通貨の授受を行う情報通信装置に関する。
【背景技術】
【０００２】
インフラの整備に伴いネットワークを流れる電子データの通信量は年々増加し、作業の効率化が飛躍的に進歩している。一方で、不特定多数の電子メールアドレスに大量に送信される電子メール（以下、スパムメールという）のような、大量の無価値な電子データがトラフィックを圧迫し、企業の生産性にも影響を及ぼす程になっている。このようなトラフィックの圧迫を解消するために、例えば大量の電子データを送受信している利用者に対して、個別にネットワーク利用の制限を掛けるといった対策がなされている。しかしながら、このような対策は、プロバイダが各契約者に対して個別に対応する必要があり、作業の手間やコストの増大を招いているという問題がある。
【０００３】
一方で、近年ブロックチェーンを利用した分散型ネットワークが実現され、ネットワーク上での決済、証明、契約等の取引を安全に行うことが可能となっている。ブロックチェーンを利用すると、第３者機関を介することなくネットワーク上で安全且つ簡単に適正な取引を行うことができ、今後益々ネットワークを利用した取引が増えると考えられる。
【０００４】
ここで、ブロックチェーンを用いた技術として、例えば特許文献１、２に示す技術が開示されている。特許文献１に示す技術は、対象データＡを生成する際、根拠情報取得部はブロックチェーンから最新ブロックのハッシュ値（根拠情報Ｂ）を取得し、データ生成部は対象データＡを生成し、データ合成部が対象データＡと根拠情報Ｂを合成し、得られた合成データ又はそのハッシュ値に対して、署名処理部が秘密鍵で暗号化を行って署名値Ｃを求め、登録処理部は、署名値Ｃを存在証明サービスに登録し、存在証明サービスはその署名値Ｃを取引情報として含んだブロックをブロックチェーンに追加し、多数のマイナーによるプルーフ・オブ・ワーク等の処理で管理されているブロックチェーンは、特定の管理者に依らずに、ブロック群の正しさが保証されているものである。
【０００５】
また、特許文献２に示す技術は、存在証明の登録対象となる電子データを受け付け、つぎに、この電子データの内容に基づき一義的に決定されるバイト配列をスクリプト中に埋め込んだトランザクションを生成し、つぎに、生成したトランザクションを公開鍵暗号方式にてデジタル署名した上で、仮想通貨のブロックチェーンに取り込むために、仮想通貨ネットワークにブロードキャストし、そして、トランザクションに固有のトランザクション識別子と、バイト配列とを関連付けて管理データベースに登録するものである。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開２０１７－１５７９２６号公報
【特許文献２】特開２０１７－１２３６９２号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
しかしながら、特許文献１、２のいずれも、ネットワークを通じての取引を活性化させることが期待できるが、トラフィックの圧迫解消につながる技術ではない。
【０００８】
本発明は、電子データを送受信する際にデジタル通貨も併せて送金することで、トラフィックを圧迫している大量の無価値な電子データ等を抑制する情報通信装置を提供する。

【課題を解決するための手段】
【０００９】
本発明に係る情報通信装置は、電子データを他のコンピュータに送信するデータ送信手段と、デジタル通貨のブロックチェーンにアクセスするための送金トランザクションを生成し、当該送金トランザクションを前記ブロックチェーンにブロードキャストする送金制御手段とを備え、前記データ送信手段が前記電子データを送信するのに伴って、前記送金制御手段が前記電子データに関する前記デジタル通貨の送金トランザクションを生成し、前記ブロックチェーンにブロードキャストするものである。
【００１０】
このように、本発明に係る情報通信装置においては、データ送信手段が、電子データを他のコンピュータに送信し、当該電子データを送信するのに伴って、送金制御手段が、電子データに関するデジタル通貨の送金トランザクションを生成し、ブロックチェーンにブロードキャストするため、電子データの送信と共にデジタル通貨の送金が行われ、電子データの価値（送信者が期待する受信者にとっての電子データの価値）をデジタル通貨で保障することができると共に、大量の無価値な電子データを通信する場合には大量のデジタル通貨が必要となるため、必要以上に電子データを通信することを抑制してトラフィックの圧迫を低減することが可能になるという効果を奏する。
【００１１】
本発明に係る情報通信装置は、前記電子データの宛先となる受信者を識別するための電子データ利用者識別情報と、ブロックチェーンへのアクセスに必要となる前記受信者を識別するＢＣ（ブロックチェーン）識別情報とを対応付けて記憶する対応情報記憶手段を備え、前記送金制御手段が、前記受信者の電子データ利用者識別情報に対応付けられた前記ＢＣ利用者識別情報に基づいて、前記送金トランザクションを生成するものである。
【００１２】
このように、本発明に係る情報通信装置においては、電子データの宛先となる受信者を識別するための電子データ利用者識別情報と、ブロックチェーンへのアクセスに必要となる受信者を識別するＢＣ利用者識別情報とを対応付けて記憶し、送金制御手段が、受信者の電子データ利用者識別情報に対応付けられたＢＣ利用者識別情報に基づいて、送金トランザクションを生成するため、電子データの送信に伴って、その宛先となる受信者へのデジタル通貨の送金を同時に行うことが可能になるという効果を奏する。
【００１３】
本発明に係る情報通信装置は、前記電子データを他のコンピュータから受信するデータ受信手段と、前記データ受信手段が前記電子データを受信するのに伴って、当該電子データの差出人に対応する前記ＢＣ利用者識別情報からの前記デジタル通貨の入金状態を前記ブロックチェーンにアクセスして確認し、確認された入金状態に応じて前記電子データの受信を確定する受信制御手段とを備えるものである。
【００１４】
このように、本発明に係る情報通信装置においては、データ受信手段が、電子データを他のコンピュータから受信し、当該電子データを受信するのに伴って、受信制御手段が、電子データの差出人に対応する前記ＢＣ利用者識別情報からのデジタル通貨の入金状態をブロックチェーンにアクセスして確認し、確認された入金状態に応じて電子データの受信を確定するため、電子データの受信者は、デジタル通貨が入金されて又は所定額以上の入金により価値が保障された電子データに対してのみ受信を確定することができ、価値のない無駄な電子データを表示したり破棄するといった手間を省いて作業の効率化を図ることができるという効果を奏する。
【００１５】
また、電子データの送信者は、受信者側においてデジタル通貨が入金されているか、又は所定額以上の入金がある電子データについてのみ受信が確定される場合に、受信者側で受信を確定させるためにはデジタル通貨の入金が必要となり、それに伴って大量の電子データを送信する場合には大量のコストが掛かってしまうため、無価値な電子データを大量

に送信することを抑制することができるという効果を奏する。

【００１６】

本発明に係る情報通信装置は、前記電子データの差出人となる送信者を識別するための電子データ利用者識別情報と、ブロックチェーンへのアクセスに必要となる前記送信者を識別するＢＣ利用者識別情報とを対応付けて記憶する対応情報記憶手段を備え、前記受信制御手段が、前記送信者の電子データ利用者識別情報に対応付けられた前記ＢＣ利用者識別情報に基づいて、前記送信者からの前記デジタル通貨の入金状態を前記ブロックチェーンにアクセスして確認するものである。

【００１７】

このように、本発明に係る情報通信装置においては、電子データの差出人となる送信者を識別するための電子データ利用者識別情報と、ブロックチェーンへのアクセスに必要となる送信者を識別するＢＣ利用者識別情報とを対応付けて記憶し、受信制御手段が、送信者の電子データ利用者識別情報に対応付けられたＢＣ利用者識別情報に基づいて、送信者からのデジタル通貨の入金状態をブロックチェーンにアクセスして確認するため、電子データの受信に伴って、その差出人となる送信者からのデジタル通貨の入金状態の確認を同時に行うことが可能になるという効果を奏する。

【００１８】

本発明に係る情報通信装置は、前記受信制御手段が前記電子データの受信を確定した場合に、入金された前記デジタル通貨の一部又は全部を返金する返金トランザクションを生成し、前記ブロックチェーンにブロードキャストする返金制御手段を備えるものである。

【００１９】

このように、本発明に係る情報通信装置においては、電子データの受信を確定した場合に、返金制御手段が、入金されたデジタル通貨の一部又は全部を返金する返金トランザクションを生成し、ブロックチェーンにブロードキャストするため、電子データが価値のある適正なデータである場合は、送信者側で当該電子データの送信時に送金したデジタル通貨がそのまま返金され、適正にデータ送信を行った送信者は、何ら損失を生じることなく電子データを送信することができるという効果を奏する。

【００２０】

本発明に係る情報通信装置は、前記返金制御手段が、前記電子データの受信を確定した後の当該電子データに対する前記受信者の操作種別に応じて、入金された前記デジタル通貨の返金額を調整するものである。

【００２１】

このように、本発明に係る情報通信装置においては、返金制御手段が、電子データの受信を確定した後の当該電子データに対する受信者の操作種別に応じて、入金されたデジタル通貨の返金額を調整するため、例えば、電子データが保存された場合は、当該電子データが受信者にとって価値が高いものであるとしてデジタル通貨の返金額を大きくし、電子データが破棄された場合は、当該電子データが受信者にとって価値が低いものであるとしてデジタル通貨の返金額を低くするといった調整が可能となり、価値が低い電子データの通信を抑制することができるという効果を奏する。

【００２２】

本発明に係る情報通信装置は、前記デジタル通貨の前記ブロックチェーン上で当該デジタル通貨の授受に関する契約処理を実行する契約履行手段が前記ブロックチェーン上に備えられており、前記送金制御手段は、前記データ送信手段が前記電子データを送信するのに伴って、前記契約履行手段が、前記電子データの送受信者を識別する電子データ利用者識別情報と、ブロックチェーンへのアクセスに必要となる前記送受信者を識別するＢＣ利用者識別情報とを対応付けた対応情報に基づいて、前記電子データの送信者の前記ＢＣ利用者識別情報から前記電子データの受信者の前記ＢＣ利用者識別情報に対して前記デジタル通貨の送金を実行するように制御するものである。

【００２３】

このように、本発明に係る情報通信装置においては、デジタル通貨のブロックチェーン

上で当該通貨の授受に関する契約処理を実行する契約履行手段をブロックチェーン上に備えており、データ送信手段が電子データを送信するのに伴って、契約履行手段が、電子データの送信者のＢＣ利用者識別情報から電子データの受信者のＢＣ利用者識別情報に対してデジタル通貨の送金を実行するように送金制御手段が制御するため、契約履行手段により電子データの送信に伴うデジタル通貨の送金を信頼性が高いブロックチェーン上で安全に行うことができるという効果を奏する。

【００２４】

本発明に係る情報通信装置は、前記電子データを他のコンピュータから受信するデータ受信手段と、前記データ受信手段が前記電子データを受信するのに伴って、前記契約履行手段が、前記電子データの送信者の前記ＢＣ利用者識別情報から前記電子データの受信者の前記ＢＣ利用者識別情報に対して前記デジタル通貨の入金状態を確認するように制御し、入金状態に応じて前記電子データの受信を確定する受信制御手段とを備えるものである。

【００２５】

このように、本発明に係る情報通信装置においては、データ受信手段が電子データを他のコンピュータから受信し、当該電子データを受信するのに伴って、契約履行手段が、電子データの送信者のＢＣ利用者識別情報から電子データの受信者のＢＣ利用者識別情報に対してデジタル通貨の入金状態を確認するように受信制御手段が制御し、入金状態に応じて電子データの受信を確定するため、契約履行手段により電子データの受信に伴うデジタル通貨の入金確認を信頼性が高いブロックチェーン上で安全に行うことができるという効果を奏する。

【００２６】

本発明に係る情報通信装置は、前記受信制御手段が前記電子データの受信を確定した場合に、前記契約履行手段が、前記電子データの受信者の前記ＢＣ利用者識別情報から前記電子データの送信者の前記ＢＣ利用者識別情報に対して、前記電子データの受信時に入金されていた前記デジタル通貨の一部又は全部の返金を実行するように制御する返金制御手段を備えるものである。

【００２７】

このように、本発明に係る情報通信装置においては、受信制御手段が電子データの受信を確定した場合に、契約履行手段が、電子データの受信者のＢＣ利用者識別情報から電子データの送信者のＢＣ利用者識別情報に対して、電子データの受信時に入金されていたデジタル通貨の一部又は全部の返金を実行するように制御する返金制御手段を備えるため、契約履行手段により電子データが適正に受信された場合のデジタル通貨の返金処理を信頼性が高いブロックチェーン上で安全に行うことができるという効果を奏する。

【図面の簡単な説明】

【００２８】

【図１】第１の実施形態に係る情報通信装置を用いたシステム構成を示す図である。

【図２】第１の実施形態に係る情報通信装置の構成を示す機能ブロック図である。

【図３】対応情報記憶部に記憶される情報の一例を示す図である。

【図４】受信制御部の処理を示す図である。

【図５】第１の実施形態に係る情報通信装置における電子メールの送信時の処理を示すフローチャートである。

【図６】第１の実施形態に係る情報通信装置における電子メールの受信時の処理を示すフローチャートである。

【図７】第２の実施形態に係る情報通信装置の構成を示す機能ブロック図である。

【図８】第２の実施形態に係る情報通信装置の返金時の処理を示すフローチャートである。

【図９】第３の実施形態に係る情報通信システムのシステム構成を示す機能ブロック図である。

【図１０】実施例におけるシミュレーション実験のメインルーチンを示す図である。

【図１１】実施例におけるシミュレーション結果を示す第１の図である。
【図１２】実施例におけるシミュレーション結果を示す第２の図である。
【発明を実施するための形態】
【００２９】
以下、本発明の実施の形態を説明する。また、本実施形態の全体を通して同じ要素には同じ符号を付けている。
【００３０】
（本発明の第１の実施形態）
本実施形態に係る情報通信装置について、図１ないし図６を用いて説明する。本実施形態に係る情報通信装置は、電子データを送信する際にデジタル通貨を併せて送金することで、送る電子データの価値（送信者が期待する受信者にとっての電子データの価値）や信頼性を保障するものである。また、電子データを受信する際には、この電子データに関してデジタル通貨が適正に入金されているかを確認した上で、正式に受信を確定するものである。
【００３１】
なお、本実施形態においては、電子データの一例として電子メールの送受信について説明するが、本実施形態に係る情報通信装置は電子メールの送受信に限らず、テキスト、静止画、動画、音声等の電子データをネットワークを介して送受信する場合であれば適用することが可能である。
【００３２】
上述したように、ＳＰＡＭメールは、電子メールを利用するユーザにとって非常に迷惑な存在である。電子メールを大量に送信するユーザ（以下、ＳＰＡＭｅｒという）は、広告やコンピュータウイルスの配布、詐欺などの様々な目的で不特定多数のユーザに大量のＳＰＡＭメールを送信する（以下、ＳＰＡＭ攻撃という）。この結果、ネットワークの負荷を増大させ、正当な電子メールの処理に悪影響を与える場合もある。
【００３３】
ＳＰＡＭ攻撃への技術的な対策を大別すると、電子メールの送信サーバに対するＳＰＡＭ判定／対策と、受信された電子メールに対するＳＰＡＭ判定／対策に分けられる。前者は、送信サーバのＩＰアドレスごとにＳＰＡＭメールを送信しているかを判定し、ＳＰＡＭを送信していると判定された送信サーバ（以下、ＳＰＡＭサーバという）に対して、何らかの形で送信を制限する方法である。ＤＮＳブラックリスト（ＤＮＳＢＬ）のように、不適切な送信と判定された電子メールの送信元のＩＰアドレスのリストを公開し、このリストに記載されたＩＰアドレスからの受信を拒否する形で運用される場合が多い。
【００３４】
この方法には，以下のような問題がある。
（１）メールアカウント単位では判定できない。
あるメールアカウントがＳＰＡＭ攻撃し、そのメールアカウントが用いる送信サーバがＳＰＡＭサーバと判定された場合、同じ送信サーバを用いる全てのメールアカウントが同時にメールの送受信を制限される。
（２）最初のＳＰＡＭ攻撃は防げない
ＳＰＡＭ攻撃のほとんどは、セキュリティに問題のある送信サーバを乗っ取るなどの方法により、本来の送信サーバとは異なる送信サーバを不正に経由して送信される場合が多い。このため、ＳＰＡＭサーバと判定される前に次々と異なる送信サーバが利用され、いわゆるイタチごっことなる。また、ＳＰＡＭサーバ判定のコストが必要となる。セキュリティに問題のある送信サーバや、それらが悪意のあるプログラムによって乗っ取られたコンピュータ（ゾンビコンピュータ）が数多くある現在、この方法でＳＰＡＭ攻撃は防がれていない。
【００３５】
後者は、受信された電子メールごとにＳＰＡＭメールであるかを判定し、ＳＰＡＭメールであると判定された電子メールを表示しない、あるいは削除するという方法である。受

信サーバで処理する場合と、受信するユーザが利用するメールクライアントソフトウェア（以下、メーラという）で処理する場合、あるいは受信したユーザ自身が処理する場合がある。

【００３６】

この方法には，以下のような問題がある。

（１）誤判定のリスクがある。

多くのプロバイダやメーラは、ＳＰＡＭメールを判定する機能（以下、フィルタリング機能という）を備えている。電子メールの内容により判定するため、ＳＰＡＭではない電子メールをＳＰＡＭと判定してしまう場合や、逆にＳＰＡＭメールをＳＰＡＭではないと判定してしまう場合がある。特に近年、ＳＰＡＭメールが内容を画像として送信される場合が多く、フィルタリングが機能しない場合も多い。この誤判定は、プロバイダ／サーバ／メーラの各段階で発生する可能性があるため、ＳＰＡＭ攻撃を完全に防ぐことは困難である。

（２）受信するサーバ／メーラ／ユーザに負荷がかかる。

ＳＰＡＭ攻撃を防ぐためには、原則として受信された全ての電子メールに対してＳＰＡＭ判定処理が必要になる。さらに、あるＳＰＡＭ判定処理を利用するユーザが増えると、ＳＰＡＭｅｒは、その処理によりＳＰＡＭと判定されないように新たなＳＰＡＭメールを作成する。このため、常にフィルタリング機能を更新する必要があり、更新されるまでの間ＳＰＡＭ攻撃を受けてしまう。このように、ＳＰＡＭｅｒがＳＰＡＭメールを送信するコストに対し、ＳＰＡＭ攻撃を防ぐコストの方が高く、負荷がかかる。

（３）受信メールの内容を知る必要がある。

ＳＰＡＭ判定処理をするためには、受信した電子メールの内容を知る必要がある。ユーザ端末ではなく、ネットワーク上で電子メールの内容を知ることは、個人情報を送受信者以外が知ることにつながり、プライバシーの点で問題がある。

【００３７】

これまでＳＰＡＭ攻撃を防ぐために、メールアカウントなど送信ユーザ個人に対してＳＰＡＭｅｒを判定する対策が利用されてこなかった。その理由は、メールアカウントは容易に偽造可能であり、メールアカウントとＳＰＡＭｅｒとを対応させることが困難であったためである。これらの問題を解決するために、本実施形態においては、電子メールの送信コストをデジタル通貨により相互に支払うことで、ＳＰＡＭ攻撃を防ぐものである。電子メールでは、適正な宛先となるメールアドレスに送信する場合、送信件数と受信件数はおおよそ一致する。すなわち、Ｎ通の電子メールを送信すれば、Ｎ通の電子メールが受信される。電子メールを利用している一般的なユーザが送信した電子メールの多くは、正しく受信される。一方、ＳＰＡＭｅｒにより無作為なメールアドレスに大量に送信される電子メールの多くは、正しくは受信されない。本発明ではこの違いに着目する。電子メールの送信コストをデジタル通貨で支払い、正しく受信された場合には支払われたデジタル通貨が返却される仕組みにより、適正な電子メールを送信するユーザに負担をかけることなく、適正でない電子メールを送信するユーザ（ＳＰＡＭｅｒ）にデジタル通貨を用いてコストを負担させる。この結果、ＳＰＡＭｅｒがＳＰＡＭメールを送信できないようにして、ＳＰＡＭメールの通信を抑制する。

【００３８】

デジタル通貨は比較的新しい概念であるため、文献によって用語の使い方に違いがある。そのため、本発明におけるデジタル通貨やその周辺の用語について、以下のように定義する。

（１）ブロックチェーン

分散型のデータベースの一種である。ブロックと呼ばれる単位でデータを順番に蓄積していく。各ブロックは、直前のブロックまでのハッシュ値を記録する。これにより、データを途中で改竄するためには、改竄するブロックに続くデータの全てに対してハッシュ値を計算する必要がある。このため、ブロックチェーンのデータの改竄は困難となる。

（２）デジタル通貨

ブロックチェーン技術により実現される仮想の通貨である。有名なビットコインやイーサリアムなど、現実に金銭的な価値を持つデジタル通貨もあるが、金銭的価値を持たないデジタル通貨も多数存在する。ブロックチェーン技術により、デジタル通貨は偽造や複製が極めて困難である。

（３）ウォレット

デジタル通貨を保管または管理するための仕組みである。オンライン上に保存するＷｅｂウォレットから、ネットワークから切り離された端末に保存するコールドウォレットまで、様々な形態が存在する。デジタル通貨のユーザは、デジタル通貨をウォレット上で所有しており、デジタル通貨の送金や受取はウォレット間で行われる。

（４）ウォレットアカウント

ウォレットを識別するＩＤである。各ユーザは、ユニークなウォレットアカウントによりデジタル通貨を管理する。上述したビットコインやイーサリアムでは、公開鍵をウォレットアカウントとして利用している。

（５）トランザクション

ブロックチェーン上に記載されるデジタル通貨の取引データである。一般的には、あるウォレットアカウントから別のウォレットアカウントへの送金が記録されたデータである。デジタル通貨を送金するウォレットアカウントが、自身のウォレットアカウントと送信先のウォレットアカウントを記載したトランザクションに、自身の秘密鍵を用いて署名して送信することで、トランザクションが発行される。

（６）マイニング

発行された複数のトランザクションをブロックチェーンに記載可能な一つのブロックとしてまとめ、ブロックチェーンの先頭に記載する作業である。この作業を行うウォレットアカウントをマイナーと呼ぶ。マイナーによりブロックチェーンに記載されることにより、取引履歴は改竄不可能な形で確定される。トランザクションの発行から確定まで数分の時間を要する。

（７）Mail Send Coin（以下、ＭＳＣという）

仮想通貨の一種として本発明に実装されるデジタル通貨で、金銭的な価値を持つことを目的としないデジタル通貨の一種であり、電子メールの送信時に併せて送金することができる。

【００３９】

次に、本実施形態に係る情報通信装置の構成について説明する。図１は、本実施形態に係る情報通信装置を用いたシステム構成を示す図である。図１において、情報通信システム１は、ユーザが使用し、インターネット１３を介して電子メールの送受信を行う情報通信端末１０（１０ａ，１０ｂ）と、それぞれのユーザが利用する電子メールの送受信を管理するメールサーバ１１（１１ａ，１１ｂ）と、情報通信端末１０ａ，１０ｂのそれぞれの利用者間でやり取りされるデジタル通貨のブロックチェーン（実態は分散型のデータベース）１２とを備える。

【００４０】

例えば、情報通信端末１０ａから情報通信端末１０ｂに電子メールを送信する場合、情報通信端末１０ａで作成された電子メールが送信者用のメールサーバ１１ａ及び受信者用のメールサーバを介して情報通信端末１０ｂに送信される。この一連の電子メールの送受信は一般的な方法により行われるものであり、例えばＳＭＴＰサーバやＰＯＰ３サーバを介して行われる。情報通信端末１０ａでは、電子メールの送信と同時にデジタル通貨であるＭＳＣの送金トランザクションが生成され、ブロックチェーン１２にブロードキャストされる。このとき生成される送金トランザクションは、情報通信端末１０ａの利用者Ａのウォレットから情報通信端末１０ｂの利用者Ｂのウォレットに対して、所定量のＭＳＣの送金を実行するものである。

【００４１】

情報通信端末１０ｂは、電子メールを受信（この段階では仮受信）すると共に、送信された電子メールに関してＭＳＣが自分のウォレットに入金されているか又は入金額が所定

額以上あるかといった入金状態を確認するために、ブロックチェーン１２にアクセスする。入金が確認された場合や所定額以上の入金が確認された場合のように入金状態が適正であるときのみ電子メールを正式に受信し、受信トレイに表示する。なお、入金が確認されない場合や入金が所定額を下回る場合のような入金状態が不適正であるときは、そのまま無条件に破棄したりゴミ箱に移動させてもよいし、一旦は受信トレイに表示した上で、ＭＳＣの入金がない電子メールである旨が利用者Ｂにわかる形で表示（例えば、アラート表示、強調表示、色違い表示等）するようにしてもよい。

【００４２】

図２は、本実施形態に係る情報通信装置の構成を示す機能ブロック図である。本実施形態に係る情報通信装置は、図１における情報通信端末１０に相当するものである。図２において、情報通信端末１０は、ユーザの操作に応じて情報の入出力を行う入出力部２１と、入力された操作に応じて送信用の電子メールを作成する送信メール作成部２２と、作成された送信用の電子メールをメールサーバ１１に送信するメール送信部２３と、送受信者のそれぞれのメールアドレスとウォレットアカウントとを対応付けて記憶する対応情報記憶部２４と、ブロックチェーンへのアクセスの際に署名として必要となる秘密鍵を記憶する秘密鍵記憶部２５と、送信メールの差出人のメールアドレス及び宛先のメールアドレスから、対応情報記憶部２４に記憶されている差出人及び宛先のウォレットアカウントを読み出して差出人のウォレットから宛先のウォレットにＭＳＣを送金するための送金トランザクションを生成すると共に、秘密鍵記憶部２５に記憶されている秘密鍵情報を用いて、生成したトランザクションに署名をしてブロックチェーンにブロードキャストする送金制御部２６とを備える。ここまでの構成が電子メールの送信時に必要となる構成である。

【００４３】

続いて電子メールの受信時に必要となる構成について説明する。図２において、自分宛てに送られた電子メールをメールサーバ１１から受信するメール受信部２７と、メール受信部２７が受信した電子メールから差出人のメールアドレスに対応するウォレットアカウントを対応情報記憶部２４から読み出し、ブロックチェーン１２に問い合わせをして、差出人からのＭＳＣの送金の有無及び／又は送金額を確認する受信制御部２８と、差出人からＭＳＣの送金がある場合や送金額が所定額以上ある場合には、受信した電子メールを正式な電子メールとして表示し、そうでない場合には、受信した電子メールを正式な電子メールではないものとして破棄等の処理を行う受信メール処理部２９とを備える。

【００４４】

ここで、送金制御部２６の処理について、より詳細に説明する。図３は、対応情報記憶部２４に記憶される情報の一例を示す図である。対応情報記憶部２４には、ユーザである電子メールの送受信者のそれぞれを識別するための識別情報であるメールアドレスと、ブロックチェーン１２へのアクセスに必要となる識別情報であるウォレットアカウントとが１対１で対応付けられて記憶されている。送金制御部２６は、送信メール作成部２２で作成された送信メールの差出人である自分のメールアドレスから、その対応するウォレットアカウントを抽出する。また、送信メールの宛先のメールアドレスから、その対応するウォレットアカウントを抽出する。これらのウォレットアカウントにより、送金元のウォレットと送金先のウォレットとを特定した送金トランザクションを作成することができる。

【００４５】

なお、上記に説明したように、対応情報記憶部２４に自分のメールアドレスに対応するウォレットアカウントを登録しておき、宛先のメールアドレスと差出人のメールアドレスとに基づいて、それぞれに対応するウォレットアカウントを抽出するようにしてもよいし、対応情報記憶部２４には自分のメールアドレスに対応するウォレットアカウントを登録せずに、自分のウォレットアカウントを別途記憶しておき、対応情報記憶部２４からは宛先のメールアドレスに対応するウォレットアカウントのみを抽出するようにしてもよい。

【００４６】

トランザクションが作成されると、秘密鍵記憶部２５に記憶されている秘密鍵情報で署名することで、作成した送金トランザクションをブロックチェーン１２にブロードキャス

トし、ブロックチェーン１２に送金情報（送金履歴）を書き込むことができる。前述したように、ブロックチェーン１２の改竄は極めて困難であることから、ここで書き込まれた送金情報は、非常に信頼性が高いものとなり、送信した電子メールの価値として機能することができる。

【００４７】

なお、これらの記憶部以外にも、例えば電子メールを送信する際に送金する量を予め設定して記憶しておき、電子メールの送信時に送金トランザクションを作成する際に利用してもよい。また、併せてＭＳＣの残額を記憶しておき、電子メールの送信の際に送金したＭＳＣを差し引いてＭＳＣの残額管理を行うようにしてもよい。

【００４８】

次に、受信制御部２８の処理について、図４を用いてより詳細に説明する。受信制御部２８は、メール受信部２７が受信した電子メールの差出人のメールアドレスから、その対応するウォレットアカウントを抽出する。同時に、宛先となっている自分のメールアドレスからウォレットアカウントを抽出する。これらの抽出したウォレットアカウントから、ブロックチェーン１２に対して問い合わせを行い、差出人のウォレットアカウントから宛先となっている自分のウォレットアカウントに対してのＭＳＣの入金状態を確認する。受信した電子メールの情報と併せて、確認した入金状態に関する情報を受信メール処理部２９に渡す。なお、この場合も、対応情報記憶部２４には自分のメールアドレスに対応するウォレットアカウントを登録せずに、自分のウォレットアカウントを別途記憶しておき、対応情報記憶部２４からは差出人のメールアドレスに対応するウォレットアカウントのみを抽出するようにしてもよい。

【００４９】

電子メールと入金情報を受け取った受信メール処理部２９は、入金状態（入金の有無や所定額以上の入金の有無）に応じて受信した電子メールに対して予め規定されている処理（例えば、普通に受信トレイに表示、入金の有無と共に受信トレイに表示、ごみ箱に破棄、完全破棄、迷惑メールとして処理等）を行う。なお、入金されたＭＳＣの量に応じて受信メール処理部２９の処理を規定してもよい。例えば、入金の量に応じてフォルダの振り分けを行ったり、所定の量以上の入金があった場合には強調表示し、所定の量未満の入金の場合には普通の表示をするようにしてもよい。こうすることで、緊急の用件がある場合などは、多めにＭＳＣを送金することで優先して電子メールの確認を促すことが可能となる。

【００５０】

次に、本実施形態に係る情報通信装置の処理方法について説明する。図５は、本実施形態に係る情報通信装置における電子メールの送信時の処理を示すフローチャートである。図５において、まず、利用者Ａが情報通信端末１０ａの入出力部２１を操作して送信メールを作成する（Ｓ１）。メール送信部２３は、作成された送信メールをメールサーバ１１ａに送信する（Ｓ２）。Ｓ２でメール送信部２３に送信メールが渡されると同時に、送金制御部２６が送信メールの宛先のメールアドレスを受け取る（Ｓ３）。送金制御部２６は、対応情報記憶部２４にアクセスし、宛先のメールアドレス及び差出人である自分のメールアドレスから、それぞれのメールアドレスに対応するウォレットアカウントを抽出する（Ｓ４）。差出人である自分のウォレットアカウントから宛先のウォレットアカウントに対してＭＳＣを送金するための送金トランザクションを生成する（Ｓ５）。秘密鍵記憶部２５から秘密鍵情報を読み出して、生成した送金トランザクションに署名する（Ｓ６）。そして、生成された送金トランザクションがブロックチェーン１２にブロードキャストされて（Ｓ７）、電子メールの送信処理を完了する。

【００５１】

図６は、本実施形態に係る情報通信装置における電子メールの受信時の処理を示すフローチャートである。図６において、まず、メール受信部２７が、メールサーバ１１ｂから電子メールを受信する（Ｓ１）。受信制御部２８が、受信した電子メールの差出人のメールアドレスを受け取る（Ｓ２）。受信制御部２８は、対応情報記憶部２４にアクセスし、

差出人のメールアドレス及び宛先である自分のメールアドレスから、それぞれのメールアドレスに対応するウォレットアカウントを抽出する（Ｓ３）。ブロックチェーン１２に対して、差出人のウォレットアカウントから宛先である自分のウィレットアカウントへのＭＳＣの入金状態を確認する（Ｓ４）。受信メール処理部２９は、受信制御部２８が確認したＭＳＣの入金状態に応じて、受信した電子メールの表示や破棄等の処理を行う（Ｓ５）。表示対象となる電子メールについて、入出力部２１でその内容が表示されて（Ｓ６）、電子メールの受信処理を完了する。

【００５２】

なお、送信時の場合と同様に、対応情報記憶部２４に自分のメールアドレスに対応するウォレットアカウントを登録しておき、宛先のメールアドレスと差出人のメールアドレスとに基づいて、それぞれに対応するウォレットアカウントを抽出するようにしてもよいし、対応情報記憶部２４には自分のメールアドレスに対応するウォレットアカウントを登録せずに、自分のウォレットアカウントを別途記憶しておき、対応情報記憶部２４からは差出人のメールアドレスに対応するウォレットアカウントのみを抽出するようにしてもよい。

【００５３】

このように、本実施形態に係る情報通信装置においては、電子データの送信時に併せてデジタル通貨を送金することで、電子データの価値や信頼性を保障することが可能となる。

【００５４】

また、電子メールの送信者は、電子メールを送信する際にデジタル通貨を併せて送金することが前提となるため、大量のＳＰＡＭメールなどを送信するＳＰＡＭｅｒは、いずれデジタル通貨の残額がゼロとなり、電子メールの送信と共にデジタル通貨の送金ができなくなる。つまり、ＳＰＡＭメールなどの価値のない大量の電子データの通信を抑制し、通信トラフィックの圧迫を解消することが可能になる。

【００５５】

なお、送信メールと受信メールとの件数に大きな差がない一般ユーザは、デジタル通貨の残額がゼロになる可能性は低く、仮にデジタル通貨がなくなっても適度な計算量のマイニングによる補充を可能とすることで電子メールの送信が可能となる。

【００５６】

また、送金処理の方法は、上述したようにトランザクションを処理することで行われるようにしてもよいし、トークンを利用することで行われるようにしてもよい。すなわち、デジタル通貨の所有権が、自分から他人又は他人から自分に移転する処理であればどのような処理方法が利用されてもよい。

【００５７】

また、本実施形態に係る情報通信装置の機能は、メールの送受信を行う一般的に利用されているメールソフト（メーラ）に拡張機能（アドオン）として実装されるようにしてもよい。つまり、メーラが以下のような機能を有するように構成されてもよい。

（１）アカウント管理機能：メールアドレスに対応するウォレットアカウントを管理する機能を持ち、自身のメールアカウントに対応するウォレットアカウントのみならず、送信先のメールアカウントに対応するウォレットアカウントのデータももつ。

（２）ＭＳＣ対応機能：受信した電子メールと送金されたＭＳＣとを対応させる機能を有し、そのデータを保存する機能を持つ。

（３）迷惑メール振り分け機能：受信したそれぞれの電子メールに対応するＭＳＣの着金額に応じて、電子メールを迷惑メールフォルダに振り分ける機能を持つ。

（４）送金機能：自身のメールアドレスに対応するウェレットアカウントから送金する機能、およびその送金額を決定する機能を持つ。

（５）アカウント確認機能：最初のメール送信時に、送信先メールアドレスに対応するウォレットアカウントを確認する機能を持つ。ウェレットアカウントが未知のメールアカウントに電子メールを送信すると、送信先のメーラに、自身のウェレットアカウントとＭＳ

Ｃの送金額を送る。メール受信側のメーラは、相手のウォレットアカウントとＭＳＣの送金額に応じて、自身のメールアドレスに対応するウェレットアカウントを送る。送信側のメーラは、送られてきた送信先のメールアドレスとウェレットアカウントに従い、ＭＳＣを送金する。
（６）マイニング機能：メール送信時に送金するＭＳＣが不足する場合、多数のユーザが発行したＭＳＣのトランザクションをマイニングすることでＭＳＣを補充する。ＳＰＡＭｅｒもこの機能によりＭＳＣを補充できるが、かなりの計算コストがかかる。
以上のような機能をメーラの拡張機能として追加してもよい。

【００５８】

（本発明の第２の実施形態）

本実施形態に係る情報通信装置について、図７及び図８を用いて説明する。本実施形態に係る情報通信装置は、前記第１の実施形態に係る情報通信装置の機能を拡張したものであり、電子データの受信時において、適正に受信して参照された電子データについては、受信時に入金されたＭＳＣを返金する機能を備えるものである。

なお、本実施形態において、前記第１の実施形態を重複する説明は省略する。

【００５９】

図７は、本実施形態に係る情報通信装置の構成を示す機能ブロック図である。前記第１の実施形態における図２の構成と異なるのは、新たに返金制御部７１を備えることである。返金制御部７１は、受信メール処理部２９が実行した受信メールに対する処理内容や、利用者Ｂにより入出力部２１で行われた操作内容に応じて、電子メールを受信した際に入金されたＭＳＣの一部又は全部を返金する。

【００６０】

具体的には、例えば、受信した電子メールがＳＰＡＭメールであると判断され、受信メール処理部２９で破棄された場合には、一切返金処理を行わない。一方、受信トレイには表示されたものの、利用者Ｂが入出力部２１の操作を行わず内容を参照しなかったり、参照したものの最終的には破棄するような処理を行った場合には、一部のＭＳＣのみを返金する。利用者Ｂが最終的に受信メールの内容を参照し、保存した場合や、当該受信メールに対して返信メールを作成して送信したような場合には全部のＭＳＣを返金するといった処理を行う。

【００６１】

返金の処理は、前記第１の実施形態における電子メール送信時に行う送金の処理と同様であり、返金制御部７１が、対応情報記憶部２４にアクセスし、受信した電子メールの差出人のメールアドレスからウォレットアカウントを抽出する。なお、自分のウォレットアカウントが対応情報記憶部２４に登録されている場合は、このときに宛先である自分のメールアドレスから対応するウォレットアカウントを併せて抽出する。

【００６２】

宛先である自分のウォレットアカウントから差出人のウォレットアカウントに対して、上記で決定した返金額の送金トランザクション（以下、返金トランザクションという）を生成し、秘密鍵記憶部２５に記憶されている秘密鍵情報で署名する。生成された返金トランザクションをブロックチェーン１２にブロードキャストして返金処理を実行する。なお、返金処理が発生した際には、その旨を差出人に対して通知するようにしてもよい。

【００６３】

上記返金処理の方法について、図８を用いて説明する。図８は、本実施形態に係る情報通信装置の返金時の処理を示すフローチャートである。まず、電子メール受信時の処理における受信メール処理部２９の処理内容又は入出力部２１の処理内容を返金制御部７１が受け取る（Ｓ１）。返金制御部７１は、受け取った処理内容に応じて返金額を決定する（Ｓ２）。返金先となる受信メールの差出人のメールアドレスを受け取る（Ｓ３）。対応情報記憶部２４にアクセスし、差出人のメールアドレス及び宛先である自分のメールアドレスから、それぞれのメールアドレスに対応するウォレットアカウントを抽出する（Ｓ４）。受信メールの宛先である自分のウォレットアカウントから差出人のウォレットアカウン

トに対してＭＳＣを送金するための返金トランザクションを生成する（Ｓ５）。秘密鍵記憶部２５から秘密鍵情報を読み出して、生成した返金トランザクションに署名する（Ｓ６）。そして、生成された返金トランザクションがブロックチェーン１２にブロードキャストされて（Ｓ７）、返金処理を完了する。

【００６４】

このように、本実施形態に係る情報通信装置においては、適正に受信された電子データについては、受信時に入金されたＭＳＣを返金する機能を有するため、送信者は、適正な電子データを送金する限りはデジタル通貨が減ることはなく、ノーリスクで信頼性や価値が付加された電子データを送信することが可能となる。逆に、ＳＰＡＭｅｒなどの悪質な送信者は、送金したデジタル通貨が返金されない可能性が高くなるため、リスクが非常に高くなり、ＳＰＡＭメールなどの価値のない大量の電子データの通信を抑制し、通信トラフィックの圧迫を解消することが可能になる。

【００６５】

（本発明の第３の実施形態）

本実施形態に係る情報通信システムについて、図９を用いて説明する。本実施形態に係る情報通信システムは、前記各実施形態の場合と同様に、電子データの送信と同時にデジタル通貨の送金を行うものであるが、送金に関する処理を全てブロックチェーン上で行うものである。

なお、本実施形態において前記各実施形態と重複する説明は省略する。

【００６６】

上述したように、本実施形態においては、送金や返金の処理をブロックチェーン上で行う、所謂スマートコントラクトを利用するものである。図９は、本実施形態に係る情報通信システムのシステム構成を示す機能ブロック図である。図９においては、第１の実施形態における図２や第２の実施形態における図７の場合と異なり、対応情報記憶部２４をそれぞれの情報通信端末１０ａ，１０ｂに備えていない。その代わりに、ブロックチェーン１２上に、ＭＳＣのブロックチェーン１２上での授受に関する契約処理を実行する契約履行部９１を備えている。

【００６７】

契約履行部９１は、対応情報記憶部２４に記憶されていた情報と同じ情報を有しており、ブロックチェーン１２が、情報通信端末１０ａの送金制御部２６から送信メールの情報を受け取った際には、差出人のウォレットから宛先のウォレットに対して所定量の送金処理を実行する。なお、このとき、送金制御部２６から送られる送信メールの情報としては、例えば、差出人のメールアドレス、宛先のメールアドレス、必要に応じて送金額や電子メールの送信処理である旨の情報等が送られるようにしてもよい。また、送金処理における送金額は、例えば、送金制御部２６から指定された送金額でもよいし、予め契約履行部９１で設定された決まった送金額でもよい。

【００６８】

ブロックチェーン１２が、返金制御部７１から受信メールの情報を受け取った際には、宛先のウォレットから差出人のウォレットに対して所定量の返金処理を実行する。なお、このときも、返金制御部７１から送られる受信メールの情報としては、例えば、宛先のメールアドレス、差出人のメールアドレス、必要に応じて返金額や電子メールの受信処理である旨の情報等が送られるようにしてもよい。また、返金処理における返金額は、例えば、返金制御部７１から指定された返金額でもよいし、予め契約履行部９１で設定された決まった返金額でもよい。

【００６９】

送金制御部２６や返金制御部７１は、情報通信端末１０に対応情報記憶部２４を有していないので、メールアドレスに対応するウォレットアカウントの情報を抽出する必要がなく、送信メールや受信メールのメールアドレスの情報（必要に応じて送金額や返金額の情報）のみを使って送金トランザクションや返金トランザクションを生成する。各トランザクションがブロックチェーン１２にブロードキャストされた後は、契約履行部９１が予め

プログラミングされた契約処理に従って、送金処理や返金処理を行う。

【００７０】

なお、受信制御部２８の処理について、入金状態の確認を行うためにブロックチェーン１２に問い合わせる際に差出人のウォレットアカウントが必要となってくるが、対応情報記憶部２４を備えていないため、差出人のウォレットアカウントが不明である。そこで、契約履行部９１は、（返金処理と区別された形で）受信メールの情報を受け取った際に、受信メールの差出人のメールアドレスと宛先のメールアドレスとから、差出人のウォレットから宛先のウォレットに送金の履歴が有るかどうかを検索し、その有無や送金額を受信制御部２８に返すような確認処理の機能を備えてもよい。そうすることで、受信制御部２８は、受信メールの情報を返金処理と区別された形でブロックチェーン１２に送信することで、送金の有無や送金額を確認することが可能となる。

【００７１】

また、契約履行部９１は、上述した送金処理、返金処理、入金の確認を行う確認処理以外にも、例えば、各ウォレットの残額の記憶や管理、受信メール処理部２９や入出力部２１の処理に応じて返金額を決定する処理等を行うようにしてもよい。

【００７２】

このように、本実施形態に係る情報通信システムにおいては、契約履行部により電子データの送信に伴うデジタル通貨の送金や返金を信頼性が高いブロックチェーン上で安全に行うことができる。

【００７３】

（その他の実施形態）

その他の実施形態に係る情報通信装置及び情報通信システムについて説明する。本実施形態に係る情報通信システムは、電子データを送信する際にデジタル通貨を併せて送金する機能は共通するものの、システム構成が異なるものである。

なお、本実施形態において前記各実施形態と重複する説明は省略する。

【００７４】

本実施形態に係る情報通信システムにおいては、対応情報記憶部２４、送金制御部２６、受信制御部２８及び／又は返金制御部７１がメールサーバ１１に備えられている。つまり、情報通信端末１０では電子メールの送受信処理だけを行い、電子メールの送信と共にＭＳＣを送金する処理の制御、電子メールを受信した際に差出人からのＭＳＣの入金状態を確認する処理の制御、受信した電子メールに対する受信メール処理２９や入出力部２１の処理に応じた返金額の演算処理、受信した電子メールの差出人への返金処理の制御をメールサーバ１１が行うものである。なお、ブロックチェーン１２では、各制御処理で生成されたトランザクションを実行するだけである。

【００７５】

また、上記の構成において、メールサーバ１１の秘密鍵を記憶する秘密鍵記憶部２５を当該メールサーバ１１上に備えるようにし、送金の署名を情報通信端末１０で実行せずにメールサーバ１１上で当該メールサーバごとに行うようにしてもよい。そうすることで、メールサーバ単位で信頼性を確保した電子メールの送受信が可能になる。

【００７６】

このように、デジタル通貨に関わる処理をメールサーバで行うことで、メールサーバを本発明の情報通信装置として機能させ、各ユーザはデジタル通貨の授受を意識することなく、電子データの送受信を安全で適正に行うことが可能となる。また、メールサーバ内でデジタル通貨に関わる処理を完結させることで、Ｗｅｂメールなどの送受信の際にも本発明を適用することが可能となる。

【００７７】

なお、上記各実施形態において、対応情報記憶部２４、送金制御部２６、秘密鍵記憶部２５、受信制御部２８及び返金制御部７１の全ての構成を必ずしも共通の箇所（例えば、情報通信端末１０内、ブロックチェーン１２上、メールサーバ１１内等）に備える必要はない。例えば、一例として、対応情報記憶部２４をブロックチェーン１２上に構築し、送

金処理、入金確認処理及び返金処理をメールサーバ１１内で実行し、返金額を決定する処理を情報通信端末１０内で実行するような構成であってもよい。

【実施例】

【００７８】

本発明に係る情報通信装置について、ＳＰＡＭ攻撃を防げるかどうかのシミュレーションを行った。本シミュレーションにおいては、本発明の利用者からＳＰＡＭｅｒがいなくなることを目的としていることから、本発明を利用しないユーザについては、実験モデルには含めないものとする。

【００７９】

シミュレーション実験のメインルーチンを図１０に示す。

（１）初期設定：仮想空間内に、本発明の情報通信装置１０を利用するＮ人のユーザを作成する。すべてのユーザが所持するＭＳＣの初期値をＭとする。Ｎ人のうち、ＳＰＡＭｅｒの人数をＳ人、一般ユーザを（Ｎ－Ｓ）人とする。

（２）メール送信・デジタル通貨の送金：一般ユーザが、自分自身とＳＰＡＭｅｒを除くユーザから、無作為に選ばれた宛先に一通のメールを送信し、同時に１ＭＳＣを送金する。この時、送金に必要なＭＳＣを所持していない場合、本発明の情報通信装置を使ったメールの送信は行わない。

（３）返金：（Ｎ－Ｓ）人の一般ユーザが送信する全てのメールは、ＳＰＡＭではないものとし、送信先メールアカウントに対応するウォレットアカウントに入金後、その同額である１ＭＳＣが返金される。

（４）一般ユーザループ：（２）～（３）を（Ｎ－Ｓ）人の一般ユーザに対して繰り返す。なお、一般ユーザはマイニングをしないものとする。

（５）メール送信・デジタル通貨の送金：ＳＰＡＭｅｒがメールの送信とＭＳＣの送金を行う。自分自身を除くすべてのユーザから無作為に宛先ユーザを選び、一通のスパムメールを送信し、１ＭＳＣを送金する。この時、送金するデジタル通貨が無ければメールの送信は行わない。

（６）返金：ＳＰＡＭｅｒが送信する全てのメールはＳＰＡＭとし、ＳＰＡＭｅｒが送金するＭＳＣは返金されない。

（７）収益：送信されたＳＰＡＭごとに、確率ｐでＳＰＡＭｅｒは収益ｂを得る。ＳＰＡＭｅｒは、収益ｂと同額のＭＳＣをマイニングにより得る。

（８）スパムメール送信ループ：（５）～（７）をＴ回繰り返す。Ｔの値は、０≦Ｔ＜Ｎを満たす自然数から一様乱数で選ばれた値である。すなわち、個々のＳＰＡＭｅｒは、単位時間ごとに、自分以外に重複なく、Ｔ通のＳＰＡＭを送信するものとする。

（９）ＳＰＡＭｅｒループ：（５）～（８）を全ＳＰＡＭｅｒに関して繰り返す。

（１０）単位時間ループ：（２）～（９）を１単位時間として繰り返す。これに基づく時刻をｔであらわす。

【００８０】

本シミュレーション実験では、Ｎ＝１０，０００，Ｍ⊂｛９８０，１，０００，１，０２０｝，Ｓ⊂｛３００，５００，７００｝とする。また、ＳＰＡＭｅｒが得る収益Ｐの確率分布を以下の式（１）で示す。

【００８１】

【数１】

$$P = 1000 \times (C)^{(-x)} \qquad (1)$$

【００８２】

ここで、Ｃを定数（２７）とし、ｘの値は０＜ｘ＜３３０を満たす一様分布の乱数とする。

【００８３】

上記の条件でＳＰＡＭｅｒの人数Ｓ＝５００とし、３種類のＭＦＣの初期値（Ｍ⊂｛９８０，１０００，１０２０｝）ごとに、１００回のシミュレーション実験を行った。送信

されたすべての電子メールに対するＳＰＡＭの比率の平均値の推移を図１１に示す。横軸が単位時間ｔであり、縦軸が送信されたすべての電子メールに対するＳＰＡＭの比率の１００試行の平均値ｒａｔｉｏである。

【００８４】

図１１に示された通り、各ユーザが持つＭＳＣの初期値Ｍに応じて、ＳＰＡＭ比率が減少する速度は異なるものの、いずれの値であってもＳＰＡＭ比率が確実に減少することが示された。

【００８５】

ＭＦＣの初期値Ｍ＝１０００とし、３種類のＳＰＡＭｅｒの人数（Ｓ⊂｛３００，５００，７００｝）ごとに、１００回のシミュレーション実験を行った。送信されたすべての電子メールに対するＳＰＡＭの比率の平均値の推移を図１２に示す。横軸が単位時間ｔであり、縦軸が送信されたすべての電子メールに対するＳＰＡＭの比率の１００試行の平均値ｒａｔｉｏである。

【００８６】

図１２に示された通り、ＳＰＡＭｅｒが得る収益の確率分布に応じて、ＳＰＡＭ比率が減少する速度は異なるものの、いずれの値であってもＳＰＡＭ比率が確実に減少することが示された。

【００８７】

以上のシミュレーション結果から、ユーザが持つＭＳＣの初期値やＳＰＡＭｅｒが得る収益の確率分布の違いにより、ＳＰＡＭ比率が減少する速度は異なるものの、ＳＰＡＭ比率が確実に減少することが示された。この結果は、本発明の情報通信装置を利用するユーザ同士で送信される電子メールについては、ＳＰＡＭが存在せず、ＳＰＡＭ攻撃が防止できることを示している。一方、本発明に係る情報通信装置を利用しないユーザからの受信メールに対しては、ＳＰＡＭを防止できるものではない。このため、ＳＰＡＭｅｒは、本発明に係る情報通信装置を利用せず、一般ユーザのみが本発明を利用することが想定される。すなわち、ＳＰＡＭを送信しない一般ユーザは、本発明を利用することで、本発明を利用して送信された電子メールはＳＰＡＭではないことが高い確率で確認できることが示された。

【００８８】

このように、本発明に係る情報通信装置は、送信サーバに対する従来の対策に比べて、以下の点で優位である。本発明は、メールアカウント単位でＳＰＡＭ攻撃を防げるため、一般ユーザとＳＰＡＭｅｒが同一の送信サーバを使っている場合でも、ＳＰＡＭｅｒからのＳＰＡＭ攻撃のみを防止できる。また、従来はＳＰＡＭ攻撃が発生後にその送信サーバからの着信を拒否するため、一定の期間ＳＰＡＭを自由に送信できた。このため、次から次へと送信サーバを変更することにより、ＳＰＡＭ攻撃が可能であった。本発明では、何らかの手段でＭＳＣを手に入れない限り、送信サーバを変更してもＳＰＡＭ攻撃ができない。一方、一般ユーザは、送信サーバを変更しても、自らの所持するＭＳＣを用いてメールの送信が可能である。

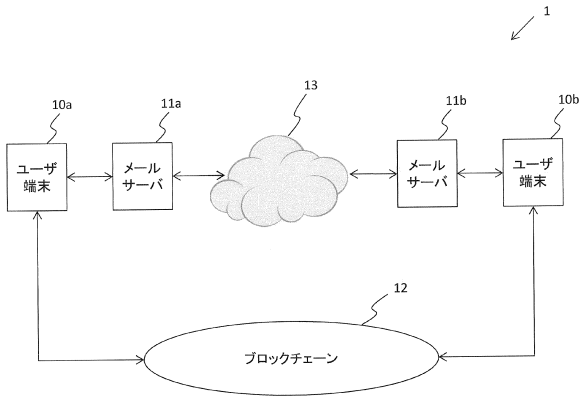
【００８９】

また、本発明は、従来の受信メールに対する対策（フィルタリング）に比べて、以下の点で優位である。本発明は、ＭＳＣの入金状態でＳＰＡＭメールを判定する。これは、電子メールを送信する立場から見ると、ＭＳＣをつけることで送信した電子メールがＳＰＡＭと判定されないことが保証される。また、電子メールを受信する立場から見ると、ＭＳＣの入金がある電子メールであれば、仮に受信した電子メールがＳＰＡＭであっても、ＭＳＣが自分のウォレットアカウントに入金されるため、損をすることはない。本発明のシミュレーション実験で示された通り、本発明を利用して送られた電子メールには、いずれＳＰＡＭが含まれなくなるため、誤判定のリスクが少ない。また、本発明は、ＳＰＡＭメールと判定するために、メールの内容を知る必要はなく、ＭＳＣの入金状態を確認するだけで良い。このため、受信するサーバ／メーラに負荷がかからず、プライバシーの問題も発生しない。

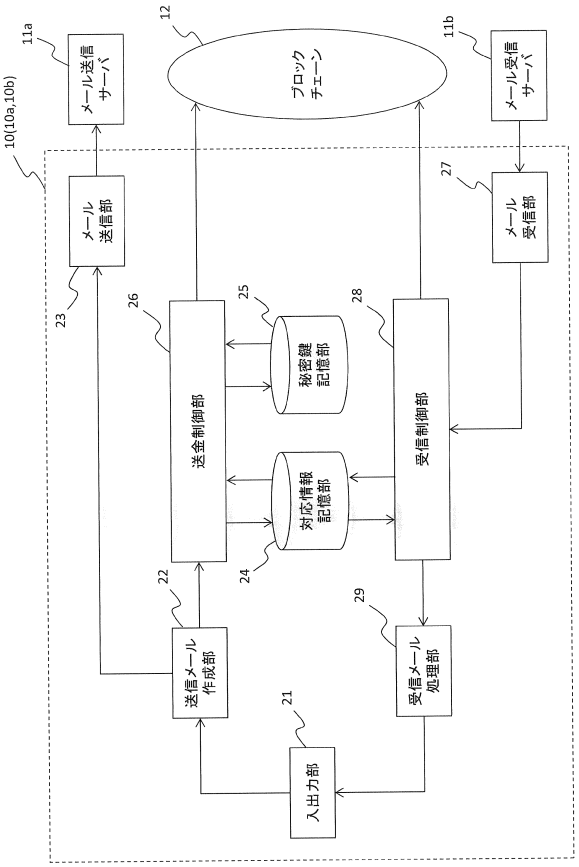
【符号の説明】
【００９０】
１　情報通信システム
１０（１０ａ，１０ｂ）　情報通信端末
１１（１１ａ，１１ｂ）　メールサーバ
１２　ブロックチェーン
２１　入出力部
２２　送信メール作成部
２３　メール送信部
２４　対応情報記憶部
２５　秘密鍵記憶部
２６　送金制御部
２７　メール受信部
２８　受信制御部
２９　受信メール処理部
７１　返金制御部
９１　契約履行部

【要約】　（修正有）
【課題】電子データを送受信する際にデジタル通貨も併せて送金し、トラフィックを圧迫する大量の無価値な電子データ等を抑制する情報通信装置を提供する。
【解決手段】電子データを他のコンピュータに送信するメール送信部２３と、デジタル通貨のブロックチェーン１２にアクセスするための送金トランザクションを生成してブロックチェーン１２にブロードキャストする送金制御部２６を備える。メール送信部２３が電子データを送信するのに伴って、送金制御部２６が電子データに関するデジタル通貨の送金トランザクションを生成し、ブロックチェーン１２にブロードキャストする。電子データを他のコンピュータから受信するメール受信部２７と、データ受信手段が電子データを受信するのに伴って、電子データの差出人からのデジタル通貨の入金状態をブロックチェーン１２にアクセスして確認し、入金状態に応じて電子データの受信を確定する受信制御部２８を備える。
【選択図】図２

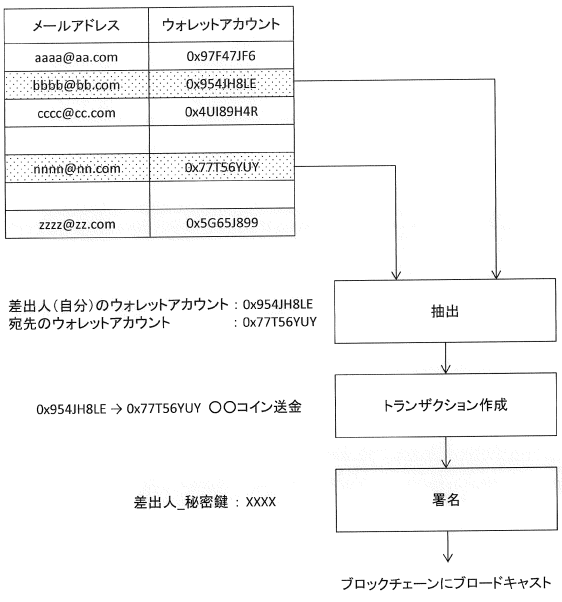
【図１】


1
10a
11a
13
11b
10b
ユーザ端末
メールサーバ
メールサーバ
ユーザ端末
12
ブロックチェーン

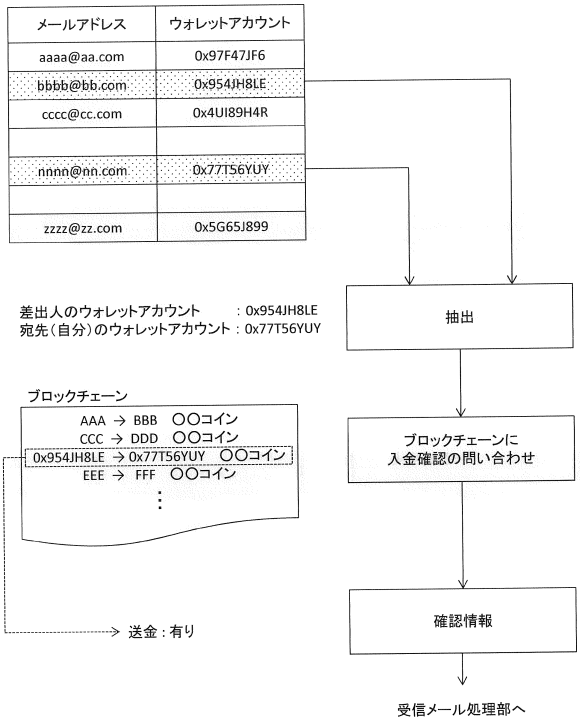
【図２】


12
11a
11b
メール送信サーバ
ブロックチェーン
メール受信サーバ
10(10a,10b)
27
メール送信部
メール受信部
23
26
25
28
秘密鍵記憶部
送金制御部
受信制御部
対応情報記憶部
22
24
29
送信メール作成部
受信メール処理部
21
入出力部

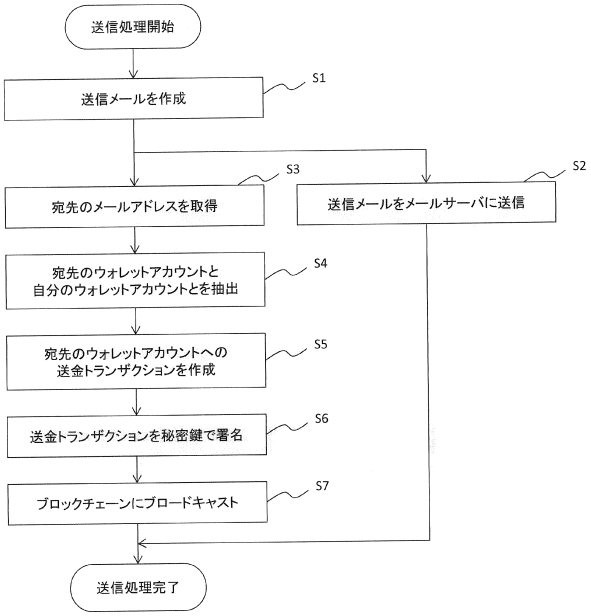
【図３】


メールアドレス
ウォレットアカウント
aaaa@aa.com
0x97F47JF6
bbbb@bb.com
0x954JH8LE
cccc@cc.com
0x4UI89H4R
nnnn@nn.com
0x77T56YUY
zzzz@zz.com
0x5G65J899
差出人（自分）のウォレットアカウント：0x954JH8LE
宛先のウォレットアカウント：0x77T56YUY
抽出
0x954JH8LE → 0x77T56YUY ○○コイン送金
トランザクション作成
差出人_秘密鍵：XXXX
署名
ブロックチェーンにブロードキャスト

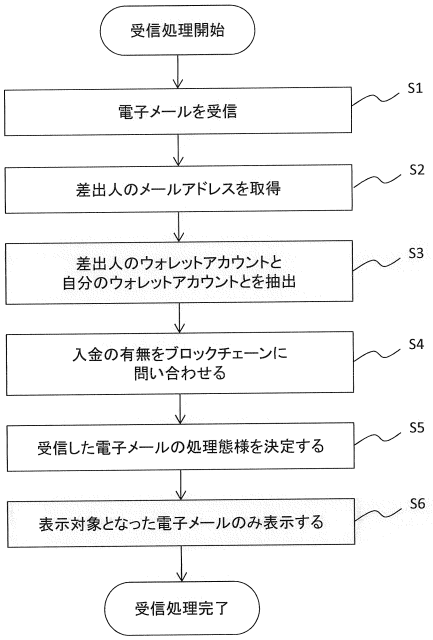
【図４】


メールアドレス
ウォレットアカウント
aaaa@aa.com
0x97F47JF6
bbbb@bb.com
0x954JH8LE
cccc@cc.com
0x4UI89H4R
nnnn@nn.com
0x77T56YUY
zzzz@zz.com
0x5G65J899
差出人のウォレットアカウント：0x954JH8LE
宛先（自分）のウォレットアカウント：0x77T56YUY
抽出
ブロックチェーン
AAA → BBB ○○コイン
CCC → DDD ○○コイン
0x954JH8LE → 0x77T56YUY ○○コイン
EEE → FFF ○○コイン
ブロックチェーンに入金確認の問い合わせ
送金：有り
確認情報
受信メール処理部へ

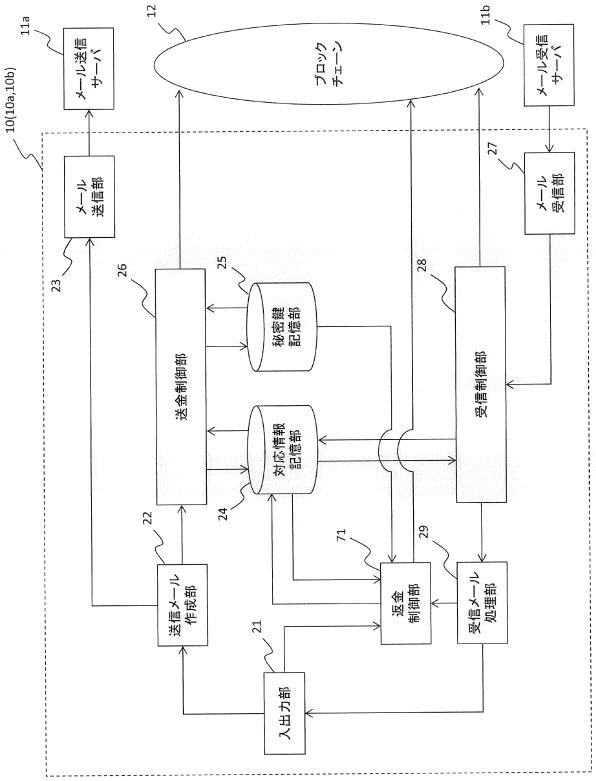
【図５】


送信処理開始
送信メールを作成
S1
宛先のメールアドレスを取得
S3
送信メールをメールサーバに送信
S2
宛先のウォレットアカウントと
自分のウォレットアカウントとを抽出
S4
宛先のウォレットアカウントへの
送金トランザクションを作成
S5
送金トランザクションを秘密鍵で署名
S6
ブロックチェーンにブロードキャスト
S7
送信処理完了

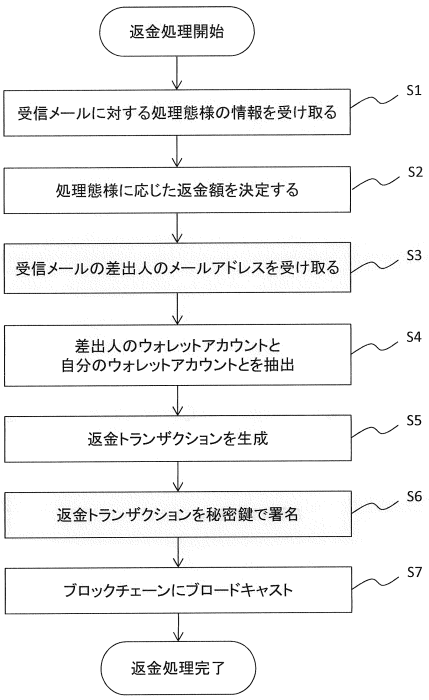
【図６】


受信処理開始
電子メールを受信
S1
差出人のメールアドレスを取得
S2
差出人のウォレットアカウントと
自分のウォレットアカウントとを抽出
S3
入金の有無をブロックチェーンに
問い合わせる
S4
受信した電子メールの処理態様を決定する
S5
表示対象となった電子メールのみ表示する
S6
受信処理完了

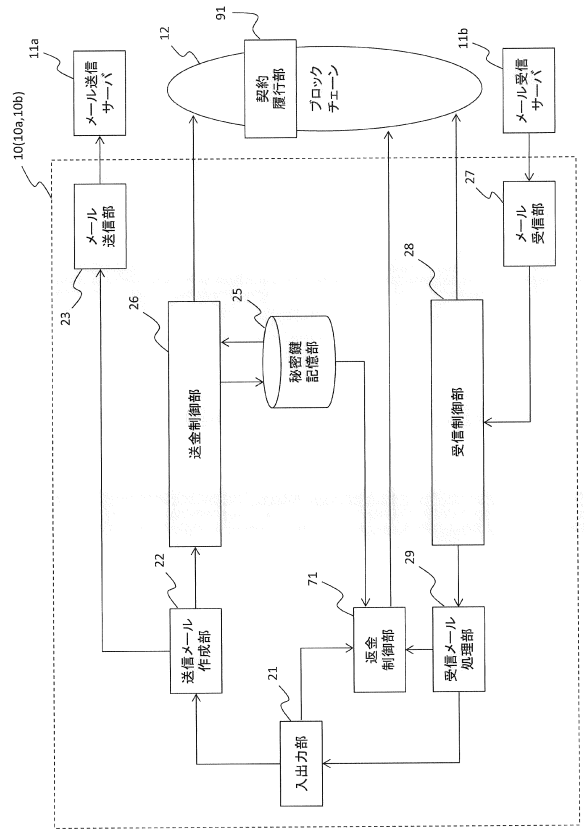
【図７】


11a
メール送信サーバ
12
ブロックチェーン
11b
メール受信サーバ
10(10a,10b)
メール送信部
23
メール受信部
27
26
送金制御部
25
秘密鍵記憶部
28
受信制御部
対応情報記憶部
24
22
送信メール作成部
71
返金制御部
29
受信メール処理部
21
入出力部

【図８】

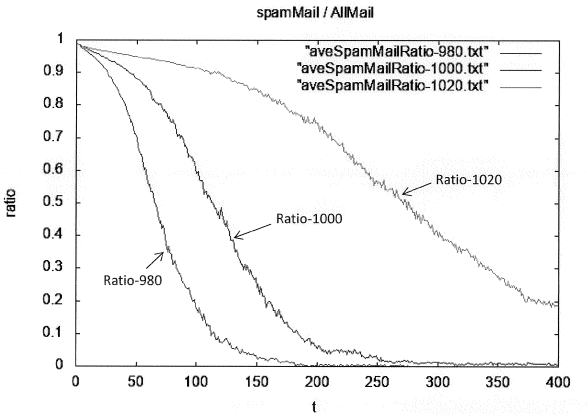

返金処理開始
受信メールに対する処理態様の情報を受け取る
S1
処理態様に応じた返金額を決定する
S2
受信メールの差出人のメールアドレスを受け取る
S3
差出人のウォレットアカウントと
自分のウォレットアカウントとを抽出
S4
返金トランザクションを生成
S5
返金トランザクションを秘密鍵で署名
S6
ブロックチェーンにブロードキャスト
S7
返金処理完了

【図９】

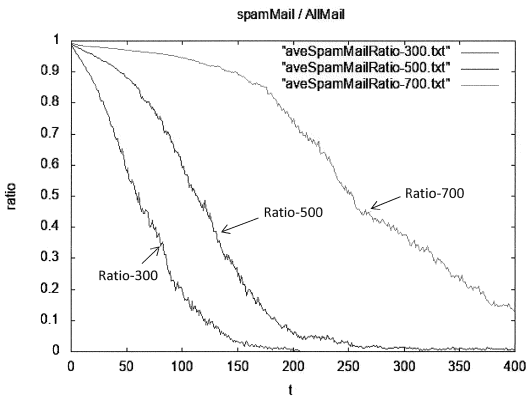


【図１０】

【図１１】



【図１２】



フロントページの続き

(56)参考文献 米国特許出願公開第２００７／０２７１３４２（ＵＳ，Ａ１）
特開２０１７－１２３６９２（ＪＰ，Ａ）
特開２０１６－１６２４３１（ＪＰ，Ａ）
特開２０１７－１２３１１６（ＪＰ，Ａ）
米国特許出願公開第２０１７／０３５９２８８（ＵＳ，Ａ１）
特開２００７－３２４６３４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　１０／００ － ９９／００
Ｇ０６Ｆ　１３／００