

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2020-3907

(P2020-3907A)

(43) 公開日 令和2年1月9日(2020.1.9)

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

F I
G06Q 20/10

テーマコード(参考)
5L055

審査請求 有 請求項の数 7 O L (全 23 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)
 (11) 特許番号 特許第6583841号 (P6583841)
 (45) 特許公報発行日 令和1年10月2日 (2019. 10. 2)

(71) 出願人 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 裕麿
 佐賀県佐賀市本庄町1番地 国立大学法人
 佐賀大学内
 Fターム(参考) 5L055 AA23 AA71

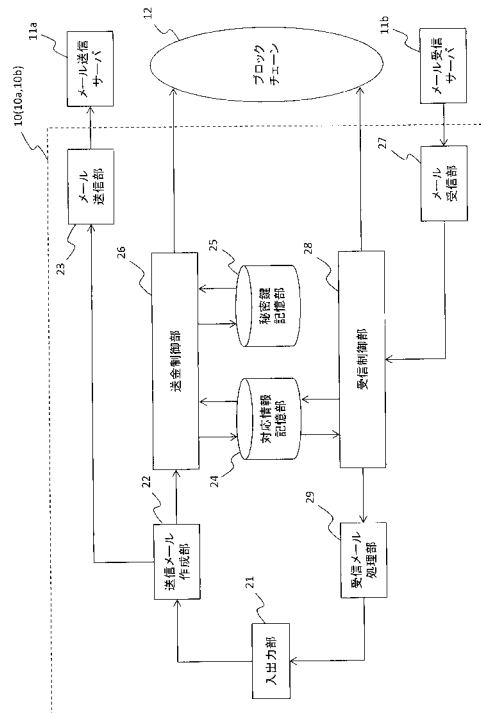
(54) 【発明の名称】 情報通信装置、情報通信方法及び情報通信プログラム

(57) 【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



【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、
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 B C 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 B C 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 B C 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情報通信装置。

【請求項 4】

請求項 3 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 B C 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 B C 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 5】

請求項 3 又は 4 に記載の情報通信装置において、

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情報通信装置。

【請求項 6】

請求項 5 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 7】

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 B C 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 B C 利用者識別情報から前記電子データの受信者の前記 B C 利用者識別情報に対して前記デジタル通貨の送金

10

20

30

40

50

を実行するように制御する情報通信装置。

【請求項 8】

請求項 7 に記載の情報通信装置において、

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情報通信装置。

【請求項 9】

請求項 8 に記載の情報通信装置において、

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情報通信装置。

10

【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。

20

【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。

30

【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、第三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。

40

【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

50

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】

10

【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。

20

【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。

30

【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。

40

【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

50

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。

10

【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。

20

【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。

30

【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。

40

【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

50

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。

10

【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。

20

【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。

30

【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。

40

【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。

50

【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。

10

【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】

20

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。

30

【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。

40

【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】

50

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。

10

【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】

20

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。

30

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。

40

【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

50

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

10

20

30

40

50

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。

10

【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。

20

【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。

30

【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。

40

【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

50

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。

10

【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。

20

【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。

30

【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。

40

【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。

50

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。

10

【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ォ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。

20

【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、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。

30

【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。

40

【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。

50

【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持つ。

（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ォ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。ウォ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、自身のウォレットアカウントとMSC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ォ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ォ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 2 6 から指定された送金額でもよいし、予め契約履行部 9 1 で設定された決まった送金額でもよい。

【 0 0 6 8 】

ブロックチェーン 1 2 が、返金制御部 7 1 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 7 1 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 7 1 から指定された返金額でもよいし、予め契約履行部 9 1 で設定された決まった返金額でもよい。

10

【 0 0 6 9 】

送金制御部 2 6 や返金制御部 7 1 は、情報通信端末 1 0 に対応情報記憶部 2 4 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 1 2 にブロードキャストされた後は、契約履行部 9 1 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。

【 0 0 7 0 】

なお、受信制御部 2 8 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 1 2 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 2 4 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 9 1 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 2 8 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 2 8 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 1 2 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。

20

【 0 0 7 1 】

また、契約履行部 9 1 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 2 9 や入出力部 2 1 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。

30

【 0 0 7 2 】

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。

【 0 0 7 3 】

（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。

40

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。

【 0 0 7 4 】

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 2 4、送金制御部 2 6、受信制御部 2 8 及び / 又は返金制御部 7 1 がメールサーバ 1 1 に備えられている。つまり、情報通信端末 1 0 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 M S C 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 M S C 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 2 9 や入出力部 2 1 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 1 1 が行うものである。なお、ブロックチェーン 1 2 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。

50

【 0 0 7 5 】

また、上記の構成において、メールサーバ 1 1 の秘密鍵を記憶する秘密鍵記憶部 2 5 を当該メールサーバ 1 1 上に備えるようにし、送金の署名を情報通信端末 1 0 で実行せずにメールサーバ 1 1 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。

【 0 0 7 6 】

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。

10

【 0 0 7 7 】

なお、上記各実施形態において、対応情報記憶部 2 4、送金制御部 2 6、秘密鍵記憶部 2 5、受信制御部 2 8 及び返金制御部 7 1 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 1 0 内、ブロックチェーン 1 2 上、メールサーバ 1 1 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 2 4 をブロックチェーン 1 2 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 1 1 内で実行し、返金額を決定する処理を情報通信端末 1 0 内で実行するような構成であってもよい。

【 実施例 】

【 0 0 7 8 】

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。

20

【 0 0 7 9 】

シミュレーション実験のメインルーチンを図 1 0 に示す。

(1) 初期設定：仮想空間内に、本発明の情報通信装置 1 0 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 1 MSC 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。

30

(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 1 MSC 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、1 MSC 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。

40

(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пам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。

50

(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】

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

10

【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】

20

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】

30

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。

40

【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

50

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を手に入れられない限り、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。

10

【符号の説明】

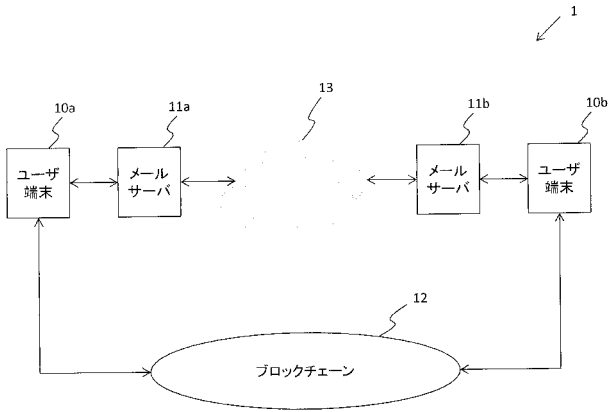
【0090】

- 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

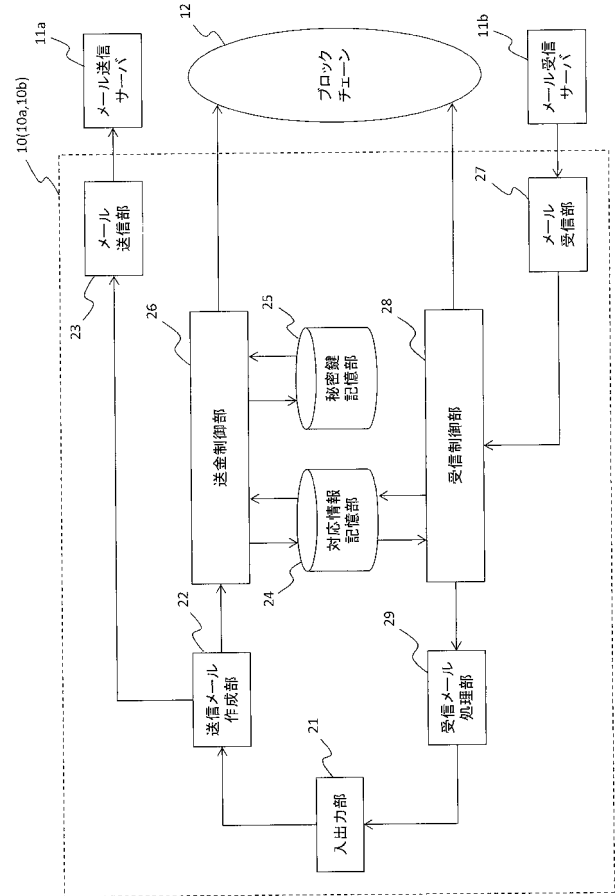
20

30

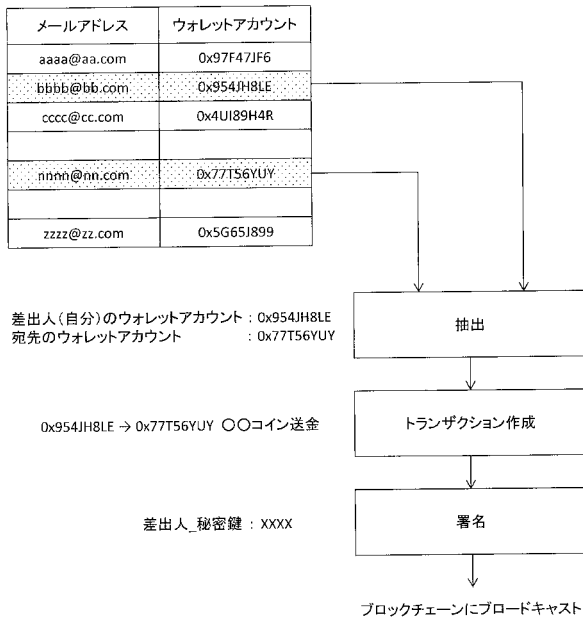
【図1】



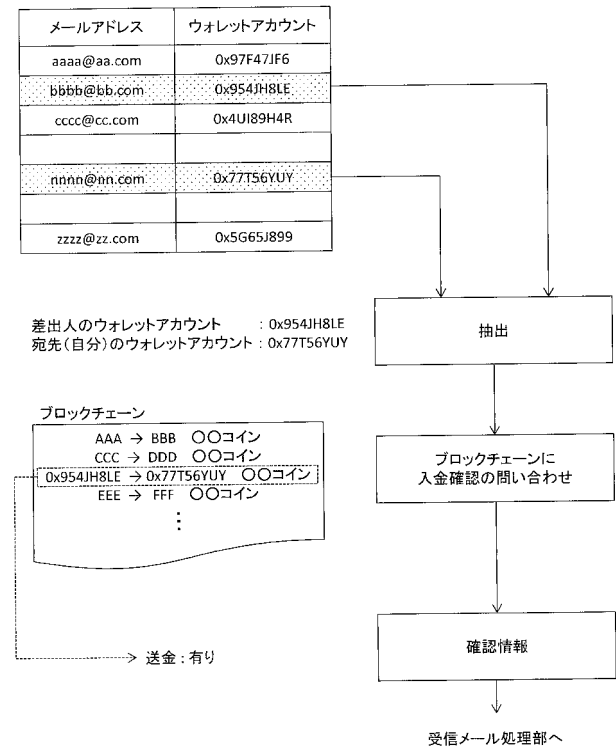
【図2】



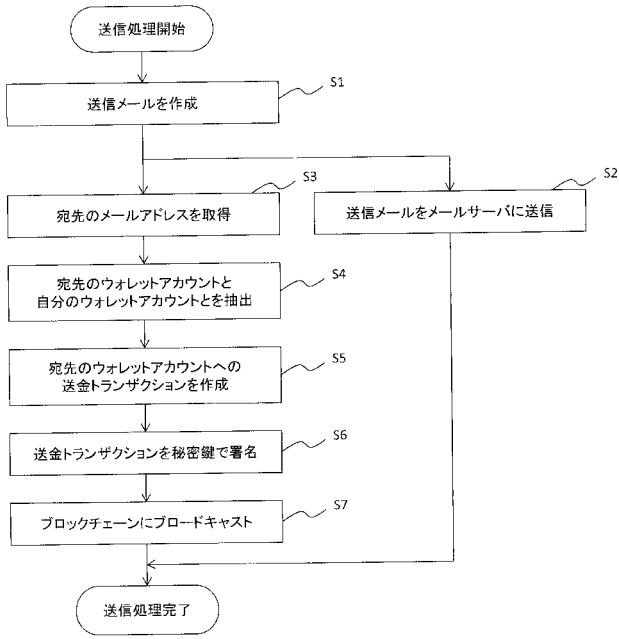
【図3】



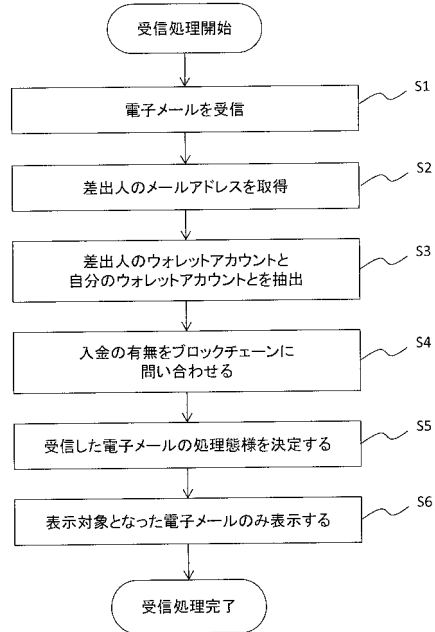
【図4】



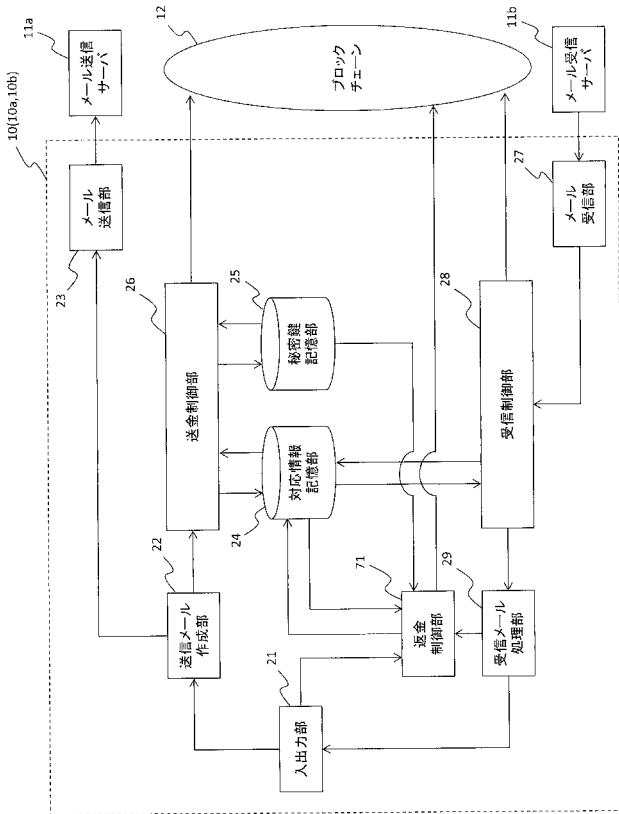
【図 5】



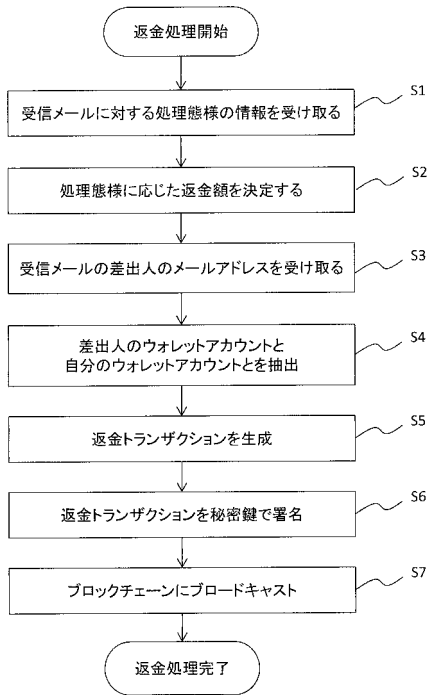
【図 6】



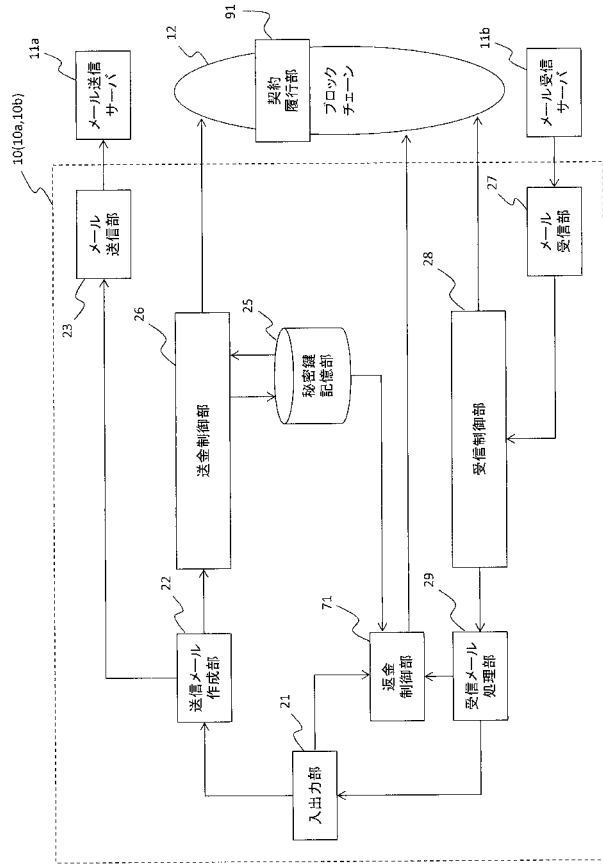
【図 7】



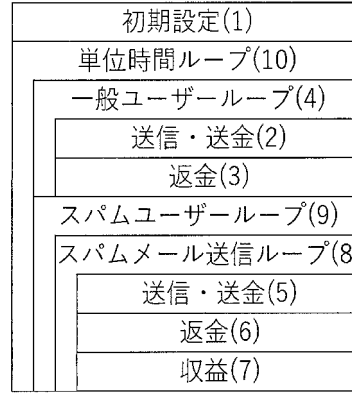
【図 8】



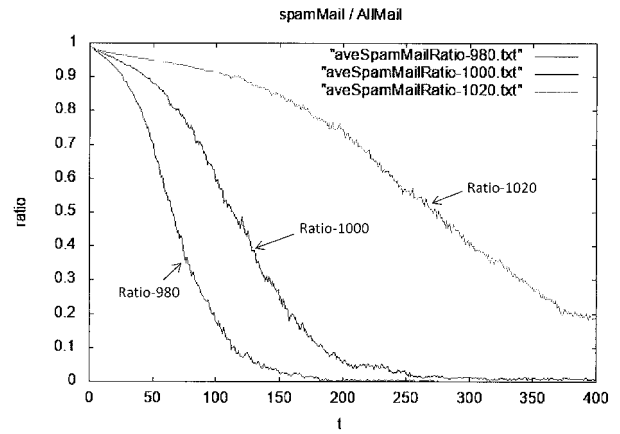
【図 9】



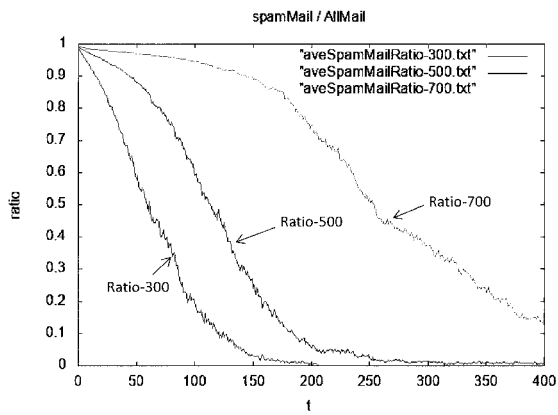
【図 10】



【図 11】



【図 12】



【手続補正書】

【提出日】令和1年6月28日(2019.6.28)

【手続補正1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【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/又は返金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。

【手続補正書】

【提出日】令和1年7月26日(2019.7.26)

【手続補正 1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】請求項 6

【補正方法】変更

【補正の内容】

【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。