(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7332087号
(P7332087)

(45)発行日　令和5年8月23日(2023.8.23)

(24)登録日　令和5年8月15日(2023.8.15)

(51)国際特許分類		FI		
H04L 9/10 (2006.01)		H04L	9/10	A
G06F 21/64 (2013.01)		G06F	21/64	
H04L 9/32 (2006.01)		H04L	9/32	200Z

請求項の数　13　（全16頁）

(21)出願番号　特願2021-501022(P2021-501022)
(86)(22)出願日　令和1年7月12日(2019.7.12)
(65)公表番号　特表2021-530177(P2021-530177A)
(43)公表日　令和3年11月4日(2021.11.4)
(86)国際出願番号　PCT/EP2019/068923
(87)国際公開番号　WO2020/020674
(87)国際公開日　令和2年1月30日(2020.1.30)
審査請求日　令和4年7月8日(2022.7.8)
(31)優先権主張番号　18461588.8
(32)優先日　平成30年7月21日(2018.7.21)
(33)優先権主張国・地域又は機関
欧州特許庁(EP)

(73)特許権者　522279483
ビットフォールド アーゲー
スイス国 カントン ズグ バール ６３４０ ミューレガッセ １８
(74)代理人　110000877
弁理士法人ＲＹＵＫＡ国際特許事務所
(72)発明者　ガンカルツ、カミル ラファル
ポーランド共和国、ウッチ ９０－３１８ ヘンリーカ シェンキエビツァ ８２／８４ フンダチア “ブロックチェーン ディベロップメント ファンデーション”内
審査官　行田 悦資

最終頁に続く

(54)【発明の名称】　エアギャッピングされた秘密鍵を用いてトランザクションに署名するためのシステムおよび方法

(57)【特許請求の範囲】

【請求項１】

トランザクションに署名するためのシステムであって、

パブリックネットワークへの通信インタフェースと、

ブロックチェーンネットワーク、または前記パブリックネットワークにおいてアクセス可能なトランザクションサーバを用いてトランザクションを処理するように構成されたコントローラ（１０５）と、

前記コントローラ（１０５）と通信するためのデータインタフェース（１０６）と

を有する第１のモジュールと、

ランダムシーケンスを生成するための乱数生成器と、

シードワードおよび秘密鍵を前記乱数生成器により生成される前記ランダムシーケンスに基づいて生成し、前記シードワードおよび前記秘密鍵を格納し、かつ、署名されたトランザクションを生成することにより前記トランザクションに署名するように構成されたセキュアコントローラと、

前記セキュアコントローラと通信するためのデータインタフェース（２０６、２０７）と

を有する第２のモジュールと、

ブリッジモジュールであって、

コントローラ（３０５）と、

前記コントローラ（３０５）と通信するためのデータインタフェース（３０９）と、

前記第１のモジュールの前記データインタフェース（１０６）が前記第２のモジュール

の前記データインタフェース（２０６、２０７）に決して接続されないように、前記ブリッジモジュールの前記データインタフェース（３０９）を前記第１のモジュールの前記データインタフェース（１０６）または前記第２のモジュールの前記データインタフェース（２０６、２０７）のいずれかに選択的に接続するように構成されたスイッチと
を有する、ブリッジモジュールと
を備え、
前記コントローラ（３０５）は、前記第１のモジュールからトランザクション要求を受信し、前記トランザクション要求を前記第２のモジュールに渡しし、前記第２のモジュールから前記署名されたトランザクションを受信し、かつ、前記署名されたトランザクションを前記第１のモジュールに渡すように構成される、
システム。
【請求項２】
前記スイッチは、単極双投（ＳＰＤＴ）スイッチである、請求項１に記載のシステム。
【請求項３】
前記第２のモジュールの前記セキュアコントローラはさらに、バイオメトリックデータを格納するように構成される、請求項１または２に記載のシステム。
【請求項４】
前記第２のモジュールは、トランザクション認証のために人のバイオメトリックトレイルを電気信号へ変換するように構成されたバイオメトリックセンサを有する、請求項１から３のいずれか一項に記載のシステム。
【請求項５】
前記スイッチはさらに、前記ブリッジモジュールの前記データインタフェース（３０９）が前記第２のモジュールの前記データインタフェース（２０６、２０７）と接続されている場合にのみ前記第２のモジュールに電力を提供するように構成される、請求項１から４のいずれか一項に記載のシステム。
【請求項６】
前記第２のモジュールにおいてワイプ機能を呼び出して、格納された前記シードワードおよび前記秘密鍵を削除し、かつ、前記第１のモジュールからの全てのトランザクションデータおよび財務データをワイプするように構成されたワイプモジュールをさらに備える、請求項１から５のいずれか一項に記載のシステム。
【請求項７】
前記第２のモジュールは、共通ハウジング内で前記ブリッジモジュールと統合される、請求項１から６のいずれか一項に記載のシステム。
【請求項８】
前記第１のモジュールは、共通ハウジング内で前記第２のモジュールおよび前記ブリッジモジュールと統合される、請求項１から７のいずれか一項に記載のシステム。
【請求項９】
前記第２のモジュールの前記データインタフェース（２０６、２０７）は、入力データバッファと出力データバッファとを含む、請求項１から８のいずれか一項に記載のシステム。
【請求項１０】
前記第２のモジュールの前記乱数生成器は、ハードウェアエントロピー生成器である、請求項１から９のいずれか一項に記載のシステム。
【請求項１１】
前記第２のモジュールの前記乱数生成器は、ソフトウェアエントロピー生成器である、請求項１から９のいずれか一項に記載のシステム。
【請求項１２】
請求項１から１１のいずれか一項に記載のシステムを用いてトランザクションに署名するための方法であって、
前記第１のモジュールを前記パブリックネットワークに接続する段階と、

トランザクションの詳細をセットアップする段階と、
前記トランザクションが認証されるという承諾を受信する段階と、
前記トランザクション要求を前記ブリッジモジュールへ送信する段階と、
前記第１のモジュールを前記ブリッジモジュールから切断する段階と、
前記ブリッジモジュールを前記第２のモジュールに接続する段階と、
前記トランザクション要求を前記ブリッジモジュールから前記第２のモジュールへ送信する段階と、
前記第２のモジュールを介して前記トランザクションを認証する段階と、
前記第２のモジュールに格納された前記秘密鍵を用いて前記トランザクションに署名して、署名された前記トランザクションを生成する段階と、
署名された前記トランザクションを前記第２のモジュールから前記ブリッジモジュールへ送信する段階と、
前記第２のモジュールを前記ブリッジモジュールから切断する段階と、
前記第１のモジュールを前記ブリッジモジュールに接続する段階と、
署名された前記トランザクションを前記ブリッジモジュールから前記第１のモジュールへ送信する段階と、
署名された前記トランザクションを前記第１のモジュールから前記ブロックチェーンネットワークまたは前記トランザクションサーバへ送信する段階と
を備える、方法。
【請求項１３】
前記第２のモジュールにおける予め定義された回数の連続した試みの間にユーザがトランザクションを認証しない場合、前記第２のモジュールにおいてワイプ機能を呼び出して、格納された前記シードワードおよび前記秘密鍵を削除し、かつ、前記第１のモジュールからの全てのトランザクションデータおよび財務データをワイプする段階をさらに備える、請求項１２に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、トランザクションに署名するためのシステムおよび方法に関する。本開示は特に、暗号通貨またはブロックチェーン（または同様のシステム）が格納されたコンテンツなどのデジタルアセットを管理する場合における電子デバイス内でのエアギャッピングのための、ユーザの視点からの簡便な方法に関する。
【背景技術】
【０００２】
「エアギャッピング」は、コンピューティングマシンのあらゆるネットワーク接続の切断、または少なくともインターネットなどのパブリックネットワークの切断に関連する公知の手順である。言い換えると、エアギャップ、エアウォールまたはエアギャッピングは、パブリックインターネットまたは安全でないローカルエリアネットワークなど、安全でないネットワークからセキュアコンピュータネットワークが物理的に分離されることを保証するために１または複数のコンピュータ上で使用されるネットワークセキュリティ措置である。
【０００３】
結果として、エアギャッピングされたコンピューティングマシンは、リモートエンティティにアクセス不可能であり、かつ、ユーザ（オペレータ）によってのみ手動で動作させられ得る、（情報、信号等に関して）閉じたシステムである。
【０００４】
エアギャッピングの欠点は、エアギャッピングされたコンピューティングマシンとリモートエンティティとの間の情報の転送が、労力集中型であり、エアギャッピングされたマシンに入れられる期待されるソフトウェアアプリケーションまたはデータについての人間によるセキュリティ解析、場合によっては、セキュリティ解析後のデータの人間による手

動での再入力さえ伴うことが多いということである。
【０００５】
さらに、エアギャッピングされたマシンは、典型的には、２つのシステムを動作させて維持する必要がある完全に分離されたハードウェアシステムであり、これは、特に、いわゆる電子ウォレットの場合に不便であり、当該電子デバイス、または当該ウォレットとして機能するコンピュータプログラムに加え、ユーザは、別個のエアギャッピングされたトランザクション署名デバイス（例えば、ネットワーク接続がないコード生成トークン、またはブロックチェーンに格納されたコンテンツへのアクセスもしくは暗号通貨などのデジタルアセットの消費を可能にする秘密鍵を格納したセキュアな冷蔵ハードウェアウォレット）を携帯しなければならない。
【０００６】
「仮想エアギャップ－ＶＡＧシステム」と題された米国特許第ＵＳ８９８４２７５Ｂ２号は、仮想エアギャップと、内部セキュリティコンポーネントと、外部セキュリティコンポーネントと、内部および外部セキュリティコンポーネントと共有メモリとの間に配置されたシステムコンポーネントのメッセージ転送メカニズムとを備えるシステムを開示している。内部システムは、それを内部ネットワークに接続する当該システムに含まれる内部セキュリティコンポーネントおよび他のコンポーネントとから成る。外部システムは、それを外部ネットワークに接続する当該システムに含まれる外部セキュリティコンポーネントおよび他のコンポーネントから成る。
【０００７】
上記を考慮すると、特に電子ウォレット用途必で使用可能なシステムを設計する必要があり、これは、２つの別個のデバイスを必要としないであろうし、使用がより簡便であろう。仮想エアギャップを介してトランザクションに署名するための改善されたシステムおよび方法を提供することも必要である。
【発明の概要】
【０００８】
本発明は、トランザクションに署名するためのシステムに関する。システムは、パブリックネットワークへの通信インタフェースと、ブロックチェーンネットワーク、またはパブリックネットワークにおいてアクセス可能なトランザクションサーバを用いてトランザクションを処理するように構成されたコントローラと、コントローラとの通信のためのデータインタフェースとを有する第１のモジュールを備える。システムは、ランダムシーケンスを生成するための乱数生成器と、シードワードおよび秘密鍵を乱数生成器により生成されるランダムシーケンスに基づいて生成し、シードワードおよび秘密鍵を格納し、かつ、署名されたトランザクションを生成することによりトランザクション要求に署名するように構成されたセキュアコントローラと、セキュアコントローラと通信するためのデータインタフェースとを有する第２のモジュールをさらに備える。システムは、コントローラと、コントローラとの通信のためのデータインタフェースと、第１のモジュールのデータインタフェースが第２のモジュールのデータインタフェースに決して接続されないように、第１のモジュールのデータインタフェースまたは第２のモジュールのデータインタフェースのいずれかにブリッジモジュールのデータインタフェースを選択的に接続するように構成されたスイッチとを有するブリッジモジュールをさらに備える。コントローラは、第１のモジュールからトランザクション要求を受信し、トランザクション要求を第２のモジュールに渡し、署名されたトランザクションを第２のモジュールから受信し、かつ、署名されたトランザクションを第１のモジュールに渡すように構成される。スイッチは、単極双投（ＳＰＤＴ）スイッチであってよい。第２のモジュールのセキュアコントローラはさらに、バイオメトリックデータを格納するように構成され得る。
【０００９】
第２のモジュールは、トランザクション認証のために人のバイオメトリックトレイルを電気信号へ変換するように構成されたバイオメトリックセンサを備え得る。
【００１０】

スイッチはさらに、ブリッジモジュールのデータインタフェースが第２のモジュールのデータインタフェースと接続されている場合にのみ第２のモジュールに電力を提供するように構成され得る。

【００１１】

システムは、第２のモジュールにおいてワイプ機能を呼び出して、格納されたシードワードおよび秘密鍵を削除し、かつ、第１のモジュールからの全てのトランザクションデータおよび財務データをワイプするように構成されたワイプモジュールをさらに備え得る。第２のモジュールは、共通ハウジング内でブリッジモジュールと統合され得る。

【００１２】

第１のモジュールは、共通ハウジング内で第２のモジュールおよびブリッジモジュールと統合され得る。

【００１３】

第２のモジュールのデータインタフェースは、入力データバッファと出力データバッファとを備え得る。第２のモジュールの乱数生成器は、ハードウェアエントロピー生成器であってよい。第２のモジュールの乱数生成器は、ソフトウェアエントロピー生成器であってよい。

【００１４】

本発明は、本明細書において説明するトランザクションに署名するためのシステムを用いてトランザクションに署名するための方法にも関する。方法は、第１のモジュールをパブリックネットワークに接続する段階と、トランザクションの詳細をセットアップする段階と、上記トランザクションが認証されるという承諾を受信する段階と、トランザクション要求をブリッジモジュールへ送信する段階と、第１のモジュールをブリッジモジュールから切断する段階と、ブリッジモジュールを第２のモジュールに接続する段階と、トランザクション要求をブリッジモジュールから第２のモジュールへ送信する段階と、第２のモジュールを介してトランザクションを認証する段階と、第２のモジュールに格納された秘密鍵を用いてトランザクションに署名して、署名されたトランザクションを生成する段階と、署名されたトランザクションを第２のモジュールからブリッジモジュールへ送信する段階と、第２のモジュールをブリッジモジュールから切断する段階と、第１のモジュールをブリッジモジュールに接続する段階と、署名されたトランザクションをブリッジモジュールから第１のモジュールへ送信する段階と、署名されたトランザクションを第１のモジュールからブロックチェーンネットワークまたはトランザクションサーバへ送信する段階とを備える。

【００１５】

方法は、第２のモジュールにおける予め定義された回数の連続した試みの間にユーザがトランザクションを認証しない場合、第２のモジュールにおいてワイプ機能を呼び出して、格納されたシードワードおよび秘密鍵を削除し、かつ、第１のモジュールからの全てのトランザクションデータおよび財務データをワイプする段階をさらに備え得る。

【図面の簡単な説明】

【００１６】

本明細書において提示されるこれらの目的および他の目的は、エアギャッピングされた秘密鍵を用いて仮想エアギャップを介してトランザクションに署名するためのシステムおよび方法を提供することにより達成される。本開示のさらなる詳細および特徴、その性質および様々な利点は、図面に示される好ましい実施形態の以下の詳細な説明からより明らかになるであろう。

【図１】本明細書において提示されるシステムのインターネット接続された第１のモジュールの図を示す。

【図２】本明細書において提示されるシステムの第２のモジュールの図を示す。

【図３】第１のモジュールと第２のモジュールとの間で動作するブリッジモジュールを示す。

【図４】第１のモジュールと、第２のモジュールと、ブリッジとを備えるシステムの概要

を示す。
【図５】図４のシステムを構成するプロセスを示す。
【図６】トランザクション認証の方法を示す。　［表記および用語］以下の詳細な説明のいくつかの部分は、コンピュータメモリ上で実行され得るデータ処理手順、段階またはデータビットに対するオペレーションの他の記号表現に関して提示されている。したがって、コンピュータは、そのような論理段階を実行するので、物理量についての物理操作を必要とする。これらの量は通常、コンピュータシステムにおいて格納され、転送され、組み合わされ、比較され、そうでなければ操作されることが可能な電気信号または磁気信号の形態を取る。一般的に用いられていることを理由として、これらの信号は、ビット、パケット、メッセージ、値、要素、記号、文字、用語、番号等と称される。加えて、これらの用語および同様の用語の全ては、適切な物理量に関連しており、これらの量に適用される簡便な符号に過ぎない。例えば、「処理」または「生成」または「転送」または「実行」または「決定」または「検出」または「取得」または「選択」または「計算」または「生成」等の用語は、物理（電子）量として表されるデータを、コンピュータのレジスタおよびメモリ内で、そのようなメモリもしくはレジスタまたは他のそのような情報ストレージ内の物理量として同様に表される他のデータへと操作および変換するコンピュータシステムの動作および処理を指す。本明細書において言及されるものなど、コンピュータ可読（記憶）媒体は、典型的には、非一時的なものであってよく、および／または非一時的デバイスを備えてよい。この文脈において、非一時的記憶媒体は、有形であり得るデバイスを含んでよい。これは、当該デバイスが具体的な物理形態を有するが、当該デバイスがその物理状態を変え得ることを意味する。したがって、例えば、非一時的は、状態の変化にもかかわらず有形のままであるデバイスを指す。本明細書において利用される場合、「例」という用語は、非限定的な例、事例または例示として機能することを意味する。本明細書において利用される場合、「例えば（ｆｏｒ　ｅｘａｍｐｌｅ）」という用語および「例えば（ｅ．ｇ．）」という用語は、１または複数の非限定的な例、事例または例示のリストを導入する。
【発明を実施するための形態】
【００１７】
　図４に示される全体構造を有する、本明細書において提示されるシステムは、暗号通貨（暗号通貨用の電子ウォレット）を用いて効果的、簡便かつ迅速なリアルタイムの支払いを提供するように特に構成され得るか、または、エアギャッピングされたマシンにとって典型的なセキュリティ措置を同時に提供しつつ、例えばトランザクションへの署名のための外部デバイスを必要としないよう、ブロックチェーン（もしくは同様のシステム）ベースの分散リーダーに格納されたコンテンツに署名するために、当該コンテンツをアップロードするために、もしくは当該コンテンツにアクセスするために構成され得る。
【００１８】
　システムは、暗号通貨との使用に特に有用であるが、特に、ブロックチェーンベースのレジャーまたは同様のシステムにトークン化されている場合、通常の通貨（例えば、ユーロ、米国ドルの電子ウォレット）にも用いられ得る。
【００１９】
　システムは、専用コンポーネントまたはカスタムメイドのＦＰＧＡ（フィールドプログラマブルゲートアレイ）回路もしくはＡＳＩＣ（特定用途向け集積回路）回路を用いて実現され得る。
【００２０】
　図１は、インターネット（または概して、任意のパブリックネットワーク）に接続されたシステムの第１のモジュール１００の図を示す。第１のモジュール１００は、暗号通貨または他のブロックチェーン（または同様のシステム）ベースのサービスを用いた支払いまたはトランザクションの処理に関連する任意の外部サービスとの通信を担う。言い換えると、当該モジュールは通信モジュールである。
【００２１】

第１のモジュール１００は、フラッシュメモリ１０４に通信可能に結合されたデータバス１０１を備える。加えて、システムの他のコンポーネントは、それらがコントローラ１０５により効果的に管理され得るように、データバス１０１に通信可能に結合される。

【００２２】

フラッシュメモリ１０４は、以下で説明する方法の段階を実行すべくコントローラ１０５により実行される１または複数のコンピュータプログラムを格納し得る。さらに、フラッシュメモリ１０４は、第１のモジュール１００の構成パラメータを格納し得る。

【００２３】

通信インタフェースモジュール１０２（例えば、Ｗｉ－Ｆｉ（登録商標）、ＧＳＭ（登録商標）、３Ｇ、ＬＴＥ、ＮＦＣ等）は、外部パブリックネットワークとの通信を管理するように構成される。通信モジュール１０２は、ユーザが自分の操作を自ら制御し得るように、専用オン／オフスイッチを有し得る。

【００２４】

コントローラ１０５は、メモリを急速に操作および変更してディスプレイデバイスへの出力向けのフレームバッファ内での画像の生成を加速させるように設計された専門電子回路であるグラフィックス処理ユニット（ＧＰＵ）１０５Ａと、ランダムアクセスメモリ（ＲＡＭ）１０５Ｂと、コンピュータプログラムの命令により指定される基本的な演算オペレーション、論理オペレーション、制御オペレーションおよび入力／出力（Ｉ／Ｏ）オペレーションを実行することにより当該命令を実行するコンピュータ内の電子回路である中央処理装置（ＣＰＵ）１０５Ｃと、第１のモジュール１００の他のコンポーネントとの間でのデータの受信および／または伝送を担うデータインタフェース１０５Ｄとを備えるシステムオンチップであってよい。

【００２５】

典型的には、第１のモジュール１００は、ひとたび準備が整うとセキュアに確認されるトランザクションをユーザがセットアップすることを可能にすべく、通信インタフェース１０２を介して、リモートサーバ、例えば、電子サービスプロバイダのサーバ、エレクトロニックバンキングシステムもしくはブロックチェーン（または同様のシステム）ベースの分散リーダーおよびネットワークとの通信を確立するように構成される。

【００２６】

任意選択的に、第１のモジュールは、トランザクションの特定の変数をユーザが手動で挿入またはそうでなければ定義することから解放されるように、トランザクションデータを指定するコンテナとして用いられ得るＱＲコード（登録商標）の画像などの画像を取得および処理するように構成されたカメラ１０３を備え得る。カメラ１０３は、ユーザが自分の操作を自ら制御し得るように、専用オン／オフスイッチを有し得る。

【００２７】

データバス１０１へのアクセスを可能にするデータインタフェース１０６上でＩ２Ｃ（集積回路間）もしくはＳＰＩ（シリアルペリフェラルインタフェース）または別のプロプライエタリインタフェースを介して、モジュール１００とモジュール３００との間で、データが暗号化形式で伝送され得る。

【００２８】

第１のモジュール１００は、専用デバイスを生成することにより実装され得る。あるいは、第１のモジュール１００のコンポーネントは、典型的なスマートフォンまたは同様のデバイスを適合させることでそのモジュールを上述のように動作するよう構成することにより実装され得る。

【００２９】

図２は、本明細書において提示されるシステムの第２のモジュール２００の図を示す。第２のモジュール２００は、トランザクションの認証を担い、パブリックネットワークに決して接続されない（インターネットなど、または、さらにいかなるネットワークにも接続されない）。

【００３０】

システムは、第２のモジュール２００のオペレーティングシステム（ＲＯＭに格納されていることに起因して、修正される傾向がない）と、任意選択的に、例えば、ブリッジモジュール３００のソフトウェアの修正に基づくハッキングの試みを防止するためなど、ブリッジモジュール３００内のソフトウェアの真正性を検証するための認証鍵とを格納するＲＯＭメモリ２０２に通信可能に結合されたデータバス２０１を備える。加えて、システムの他のコンポーネントは、それらがセキュアコントローラ２０５により管理され得るように、データバス２０１に通信可能に結合される。

【００３１】

第２のモジュール２００は、人のバイオメトリックトレイルを電気信号へ変換するように構成されたバイオメトリックセンサ２０３も（オプションとして）備え得る。バイオメトリックトレイルは主に、バイオメトリックフィンガープリントデータ、虹彩データ、顔画像、音声サンプル等を含む。このデータは、追加のトランザクション認証メカニズムとして機能し得る。

【００３２】

乱数生成器２０４は、統計的にランダムである、すなわち、いかなる特性および区別可能な特徴も生成スキームも有しないランダム数シーケンスを生成するように構成された真の乱数生成器である。これらのランダムシーケンスは、データを暗号化して、秘密鍵の生成に用いられるシードワード（辞書ワード）を生成するために用いられる。好ましくは、乱数生成器２０４は、ハードウェアエントロピー生成器である。ランダム数は、スタンドアロンチップではないコンピュータプログラム（すなわち、ソフトウェアエントロピー生成器）によっても生成され得る。

【００３３】

セキュアコントローラ２０５は、第２のモジュール２００のコンポーネントを管理するように、特に、セキュアトランザクションを認証するように構成される。セキュアコントローラ２０５は、プロセッサ２０５Ａと、フラッシュメモリ２０５Ｂと、動作ＲＡＭメモリ２０５Ｃとを備える。これは、秘密鍵およびバイオメトリックデータ、すなわち、セキュアトランザクションを認証するために必要な全ての要素を格納する。秘密鍵は、暗号化され得る。秘密鍵の解読には、フラッシュメモリ２０５Ｂ内に格納された参照バイオメトリックデータと、バイオメトリックセンサ２０３などのバイオメトリックセンサから読み取られたバイオメトリックデータとを用いたバイオメトリック認証が必要となる。データインタフェース２０５Ｄは、第２のモジュール２００の他のコンポーネントとの間でのデータの受信および／または伝送を担う。

【００３４】

データは、好ましくはＳＰＤＴスイッチ３１０を介してブリッジモジュール３００のインタフェース３０９と通信するように構成されたデータバッファ２０６、２０７の形態のデータインタフェースを介して、モジュール２００とモジュール３００との間で伝送され得る。入力バッファ２０６は、そこからデータを読み取るための第２のモジュールと、その内部にデータを格納するためのブリッジモジュールとによりアクセス可能である。出力バッファ２０７は、その内部にデータを格納するための第２のモジュールによりアクセス可能であり、かつ、そこからデータを読み取るためのブリッジモジュールによりアクセス可能である。データバッファ２０６、２０７の各々は、ＳＰＤＴスイッチ３１０を介してデータバス２０１およびセキュアコントローラ２０５ならびにブリッジモジュール３００のデータインタフェース３０９との通信を処理するための独自の内部処理ユニットと、フラッシュメモリと、データインタフェースとを備え得る。

【００３５】

第２のモジュール２００は、専用コンポーネントまたはカスタムメイドのＦＰＧＡ回路もしくはＡＳＩＣ回路を用いて実現され得る。第２のモジュール２００は、ブリッジモジュール３００と共に、好ましくは、ＵＳＢインタフェースなどの外部インタフェースを介して第１のモジュールに（ブリッジモジュールのみを介して）接続可能である専用デバイスを形成するように共通ハウジング内で統合される（そのような場合、第１のモジュール

の機能は、スマートフォンまたはラップトップコンピュータなどの汎用デバイスにインストールされるアプリケーションにより提供され得る）。あるいは、モジュール１００、２００、３００の全てが、完全に機能するデバイスを形成するように共通ハウジング内で統合され得る。

【００３６】

図３は、第１のモジュール１００と第２のモジュール２００との間で動作するブリッジモジュール３００を示す。ブリッジモジュール３００の目的は、トランザクション要求を規定して第１のモジュール１００から第２のモジュール２００に渡すこと、および、署名されたトランザクションまたはトランザクションの拒否を受信することである。

【００３７】

第２のモジュール２００と統合されたブリッジモジュール３００は、専用コンポーネントまたはカスタムメイドのＦＰＧＡ回路もしくはＡＳＩＣ回路を用いて実現され得る。モジュール２００、３００は、第１のモジュール１００に接続可能である追加のモジュールを構成し得るか、または第１のモジュール１００と統合され得る。

【００３８】

ブリッジモジュール３００は、メモリ３０３に通信可能に結合されたデータバス３０１を備える。加えて、システムの他のコンポーネントは、それらがコントローラ３０５により管理され得るように、データバス３０１に通信可能に結合される。

【００３９】

第１のモジュール１００とブリッジ３００との間または第２のモジュール２００とブリッジ３００との間のいずれかで所定の時間に、データが伝送され得る。最大限のセキュリティのために、システムは、データの伝送、また、任意選択的に電力の供給を制御するＳＰＤＴスイッチ３１０の使用によって３つのモジュール１００、２００、３００の全てがいつでも同時にアクティブになることが可能にならないように構成される。

【００４０】

コントローラ３０５は、コントローラ１０５と同じまたは同様のサブコンポーネントを備えるシステムオンチップであってよい。

【００４１】

オン／オフスイッチ３０４は、ユーザにより操作された場合にデバイスのオンまたはオフを切り替えるように構成される。他の典型的なコンポーネントは、好ましくはタッチセンサ式ディスプレイであるディスプレイ３０６と、ユーザとの通信のためのコンポーネントを形成するスピーカ３０２とを含む。

【００４２】

ブリッジモジュール３００は、モバイルデバイスとして動作するよう意図されているので、好ましくは、バッテリ３０７から電力を供給される。典型的なバッテリ充電手段（無線充電（例えば、）Ｑｉ規格によるもの）および典型的なプラグチャージャ接続など）も、ブリッジモジュール３００の電源３０７内に存在し得る。ＢＭＳ（バッテリ管理システム）モジュール３０８は、例えば、バッテリの長い耐用期間を維持するために、バッテリの充電、放電およびオペレーション全体を管理するように構成される。

【００４３】

ブリッジモジュール３００は、第１のモジュール１００のインタフェース１０６または第２のモジュール２００のデータバッファ２０６、２０７の両方とＳＰＤＴスイッチ３１０を介して通信するように構成されたデータインタフェース３０９を備える。

【００４４】

ＳＰＤＴ（単極双投スイッチ）モジュール３１０は、電力およびデータ伝送機能をこれらのモジュールのうちの１つだけに、つまり、第１のモジュール１００または第２のモジュール２００のいずれかに一度に提供するように構成される。モジュール３１０は、一方が電力用で他方がデータ伝送用である、単一のアクチュエータにより常に共に切り替えられる２つのＳＰＤＴスイッチを含み得る。ハードウェアスイッチにより、第１のモジュールを電力から完全に切断されるようにするか、または、少なくともその通信インタフェー

ス１０２を電力から完全に切断されるようにすることにより、侵入者または悪意のあるソフトウェアからの追加のレベルのセキュリティが提供される。なぜなら、それは、第２のモジュールへのアクセスがなく、第２のモジュールにより署名されるようにトランザクション要求を改ざんする可能性がないからである。

【００４５】

他のタイプの切り替えモジュールは、第１のモジュール１００のデータインタフェース１０６が第２のモジュール２００のデータインタフェース２０６、２０７に決して接続されないようにする機能をそれらが提供する限り、ＳＰＤＴスイッチの場所において用いられ得る。

【００４６】

図４は、第１のモジュール１００と、第２のモジュール２００と、ブリッジモジュール３００とを備えるシステムの概要を示す。ブリッジモジュール３００は、ＳＰＤＴスイッチ３１０を介して、任意の所定の時間に、第１のモジュール１００または第２のモジュール２００のいずれかに選択的に接続される。ＳＰＤＴスイッチ３１０は、（少なくとも第２のモジュールへの）データの伝送および電力の供給を制御する。

【００４７】

ワイプモジュール４０１もシステム内に任意選択的に存在してよく、セキュリティ上の理由で「デバイスをワイプする」機能を即座に呼び出すように構成されてよい。ひとたびワイプモジュール４０１がアクティブ化されると、第２のモジュールがアクティブ化され、データをパーソナライズすることなくその工場設定を復元すべく、そこからの秘密鍵、シードワードおよびバイオメトリックデータを削除するためにコマンドが第２のモジュールへ送信される。次に、第１のモジュールがアクティブ化され、トランザクション履歴、連絡先アドレスおよび任意の他のアドレスまたは財務データが削除される。ワイプモジュール４０１は、専用の「パニックボタン」の形態を有し得る。あるいは、ワイプモジュール４０１は、ユーザが特定の一連の他のボタンを押すことによりアクティブ化され得る。

【００４８】

したがって、システム４００は、第１のモジュール１００、第２のモジュール２００およびブリッジモジュール３００という少なくとも３つのモジュールへ分割されることにより、トランザクションのセキュリティ問題を解決でき、これにより、モジュール１００とモジュール２００との間で情報を渡すことが可能になる共に、それらが互いに無関係に動作することが可能になる。第２のモジュール２００は、パブリックネットワーク（インターネットなど）に決して接続されずに、秘密鍵を用いて（特に、パスワードもしくはＰＩＮコードまたはバイオメトリックデータ等を提供することにより）トランザクションを認証して署名するように構成される。

【００４９】

特に、第２のモジュール２００は、パブリックネットワークに決して接続されない。なぜなら、任意の所与の事例におけるブリッジモジュール３００は、第１のモジュール１００または第２のモジュール２００のいずれかに接続され得るからである。したがって、リモートエンティティ（スパイソフトウェアを動作させるハッカーまたはマシン）が、本明細書において提示されるデバイスから認証データをキャプチャすることは不可能である。また、第１のモジュール１００は、第２のモジュール２００のデータおよびコンテンツに対するいかなる形態のアクセスも有しない。

【００５０】

図５は、システム４００の構成プロセスを示す。段階５０１において、システム４００は、パブリックネットワークから切断されたままである。なぜなら、第１のモジュールがオフにされているからである。次に、段階５０２において、ユーザの認証の方法、例えば、ＰＩＮ、パスワード、バイオメトリックスキャン等が選択される。認証および関連応答のパラメータが、第２のモジュール２００のセキュアコントローラ２０５に格納される。続いて、段階５０３において、一連のキーワード（シード）が、特に暗号通貨用の確定的なウォレットの処理に関連して、公知の方法に従って生成される。シードは、秘密鍵がリ

セットされた場合にデバイスへのアクセスを復元するために用いられ得る。例えば、第２のモジュール２００は、一連のキーワードをランダム方式で生成することを可能にする、例えばＢＩＰ－３９規格による辞書をＲＯＭメモリ２０２内に備え得る。一連のキーワードは、２４個または３６個ものキーワードを含み得る。これにより、キーワードの同じランダムシーケンスがある２つのデバイスを有するリスクが軽減される。次に、段階５０４において、秘密鍵または鍵のセットが、シードに基づいて生成される。秘密鍵および一連のキーワードは、第２のモジュール２００のセキュアコントローラ２０５のフラッシュメモリに格納され（５０５）、加えて、デバイスに対するセキュリティのレベルの向上を保証するために、パスワード、ＰＩＮまたはバイオメトリックトレイルを用いて暗号化され得る。図５のプロセスが実行された後に、システム４００は、インターネットなどの外部パブリックネットワークとの通信モジュール１０２の接続と共に、第１のモジュール１００を構成および起動し得る。

【００５１】

図６は、本明細書において提示されるデバイスを用いたトランザクション認証の方法を示す。まず、段階６０１において、第２のモジュール２００がオンに切り替えられ、段階６０２において、ユーザが、デバイスへのさらなるアクセスを可能にすべくパスワード、ＰＩＮまたはバイオメトリックデータを入力することにより、デバイスへのアクセスを認証する。入力されたパスワードが承認された場合、第２のモジュール２００はオフに切り替えられ、第１のモジュール１００はオンに切り替えられる。

【００５２】

次に、段階６０４において、第１のモジュール１００がパブリックネットワーク（例えば、オンラインサービス、銀行、通貨交換サービス、ブロックチェーンネットワーク、インターネットネットワーク）に接続され、段階６０５において、トランザクションの詳細（受信者データ、目的等など）がセットアップされ、段階６０６において、トランザクションの量が与えられる。この目的で、外部パブリックネットワークのリモートサーバ、または第１のモジュール１００においてインストールされたアプリケーションは、典型的には、トランザクションをセットアップするために必要とされる任意の関連情報の入力を可能にする適切なユーザインタフェースを提供する。

【００５３】

次に、段階６０７において、暗号通貨において典型的な、いわゆるマイニング手数料が決定され得る（通常の通貨の場合、この段階において、他のトランザクション手数料が決定され得る）。続いて、段階６０８において、上記トランザクションが適切に定義され、上記トランザクションが認証されるべきであることをユーザが確認し得る（第１のモジュール１００がユーザから確認を受信する）。

【００５４】

ユーザが上記トランザクションを認証することを望んでいる場合、トランザクションの詳細を既に所有している第１のモジュール１００は、段階６０９において、トランザクション要求をブリッジモジュールへ送信し、段階６１０において、上記パブリックネットワークから切断される。次に、第１のモジュール１００は、ＳＰＤＴスイッチ３１０により、ブリッジからも通信可能に切断される。

【００５５】

次に、第２のモジュール２００は、段階６１１において、（上記ＳＰＤＴスイッチ３１０を用いて）オンに切り替えられ、段階６１２において、ブリッジモジュールからトランザクション要求を受信する。段階６１３において、ユーザは、パスワード、ＰＩＮおよび／またはバイオメトリックデータなどの入力データを用いて、第２のモジュール２００を介してトランザクションを認証する。ユーザは、その認証情報を提供する前に、トランザクションの詳細を第２のモジュールモードにおいてダブルチェックする可能性があり、これは、スクリーン上に表示される。したがって、それは、セキュリティの別の層であり、「見た（署名した）ままのものが得られる（トランザクション）」としてまとめられ得る。既に論じたように、認証は、デバイスが外部パブリックネットワークから切断された場

合に行われ、第１のモジュールは、いかなるデータへのアクセスも有しない。
【００５６】
さらに、段階６１４において、トランザクションは、第２のモジュールのセキュアコントローラ２０５に格納された秘密鍵を用いて署名される。次に、段階６１５において、第２のモジュール２００は、署名されたトランザクションをブリッジモジュール３００へ送信する。
【００５７】
次に、段階６１６において、第２のモジュール２００は、オフに切り替えられ、第１のモジュール１００は、オンに切り替えられ、通信インタフェース１０２を介してパブリックネットワークに接続される。段階６１７において、ブリッジモジュール３００は、署名されたトランザクションを第１のモジュール１００へ送信し、段階６１８において、第１のモジュール１００は、署名されたトランザクションをブロックチェーンネットワークまたはリモートサーバへ送信する。
【００５８】
任意選択的に、予め定義された回数の連続した試み（例えば、３回または５回の試み）の間にユーザがトランザクションを認証できない場合、第２のモジュールは、ワイプモジュール４０１の機能に関して論じたワイプオペレーションを実行し得ると共に、前述の一連のキーワードを用いて新しいアクティブ化を待機し得る（図５を参照のこと）。
【００５９】
提示された方法およびシステムにより、使用の容易さを損なうことなく電子ウォレットのセキュリティを改善することが可能になる。したがって、それらは、有用、具体的かつ有形の結果を提供する。
【００６０】
本開示によれば、暗号通貨および他のブロックチェーンベースのまたは格納されたコンテンツなどの電子通貨でのトランザクションにアクセスして当該トランザクションを実行するための秘密鍵のセキュアな格納を担うデバイスが提示される。したがって、当該概念が抽象的ではないことのマシン試験または変換試験が遂行される。
【００６１】
本明細書において開示される方法の少なくとも一部は、コンピュータで実装され得る。したがって、システムは、全体的にハードウェアの実施形態、全体的にソフトウェアの実施形態（ファームウェア、常駐ソフトウェア、マイクロコード等を含む）、または全てが本明細書において概して「回路」、「モジュール」または「システム」と称され得るソフトウェア態様とハードウェア態様とを組み合わせた実施形態の形態を取り得る。
【００６２】
さらに、本システムは、コンピュータプログラム製品の形態を取ってよく、当該コンピュータプログラム製品は、表現としての任意の有形の媒体であって、当該媒体において具現化されるコンピュータ使用可能プログラムコードを有する、媒体で具現化される。
【００６３】
当業者であれば、こ仮想エアギャップを介してトランザクションに署名するための前述の方法が１または複数のコンピュータプログラムにより実行および／または制御され得ることを容易に認識し得る。そのようなコンピュータプログラムは、典型的には、コンピューティングデバイス内のコンピューティングリソースを利用することにより実行される。アプリケーションが非一時的媒体に格納される。非一時的媒体の例は、例えばフラッシュメモリなどの不揮発性メモリであるが、揮発性メモリの例はＲＡＭである。コンピュータ命令は、プロセッサにより実行される。これらのメモリは、コンピュータで実装される方法の全ての段階を本明細書において提示される技術的概念に従って実行するコンピュータ実行可能命令を含むコンピュータプログラムを格納するための例示的な記録媒体である。
【００６４】
特定の好ましい実施形態を参照して、本明細書において提示されるシステムおよび方法を示し、説明し、かつ、定義したが、前述の明細書における実装のそのような参照および

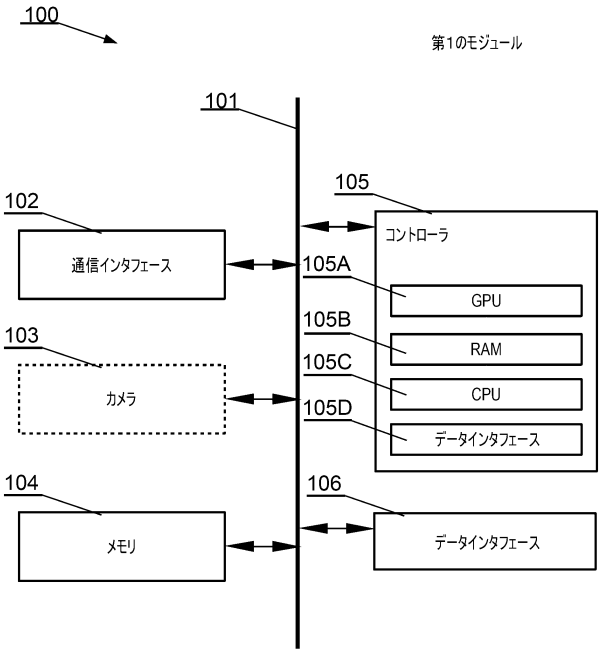
例は、当該方法または当該システムに対するいかなる限定も示唆していない。しかしながら、技術的概念のより広い範囲から逸脱することなく、それらに対して様々な修正および変更が行われ得ることは明らかであろう。提示された好ましい実施形態は、例示的なものに過ぎず、本明細書において提示された技術的概念の範囲を網羅したものではない。

【００６５】

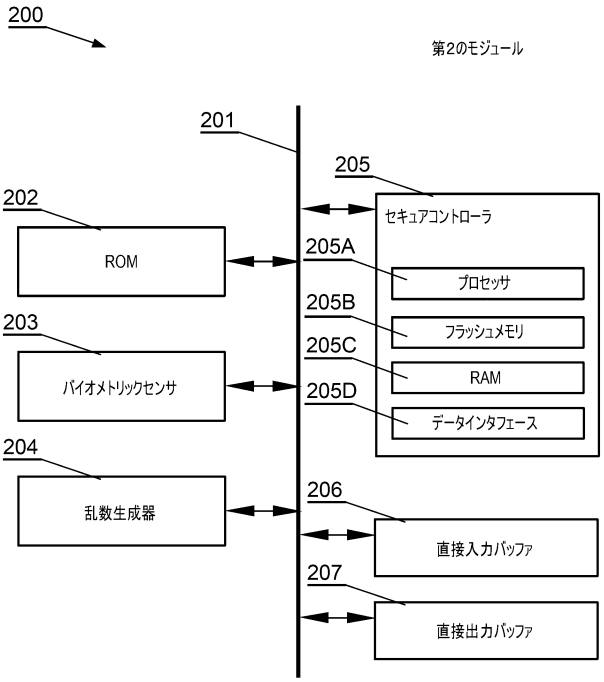
したがって、保護範囲は、本明細書において説明した好ましい実施形態に限定されないが、以下の特許請求の範囲によってのみ限定される。

【図面】

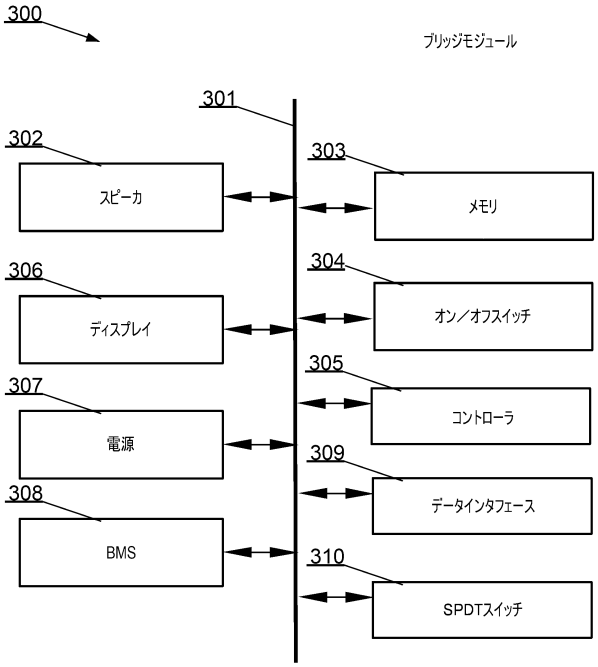
【図１】


100
第1のモジュール
101
102
通信インタフェース
103
カメラ
104
メモリ
105
コントローラ
105A
GPU
105B
RAM
105C
CPU
105D
データインタフェース
106
データインタフェース

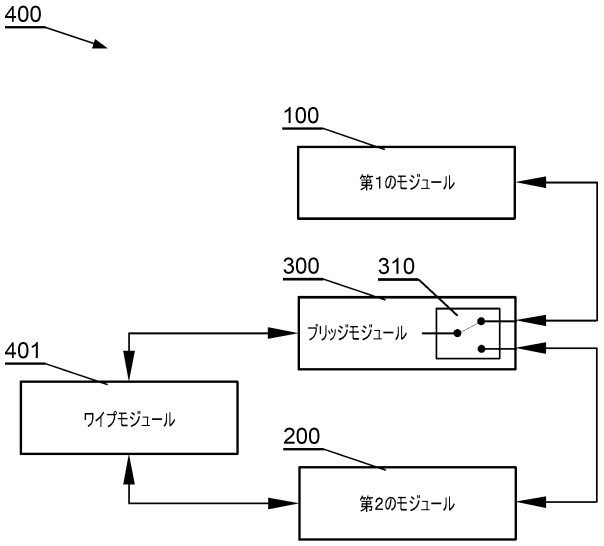
【図２】


200
第2のモジュール
201
202
ROM
203
バイオメトリックセンサ
204
乱数生成器
205
セキュアコントローラ
205A
プロセッサ
205B
フラッシュメモリ
205C
RAM
205D
データインタフェース
206
直接入力バッファ
207
直接出力バッファ

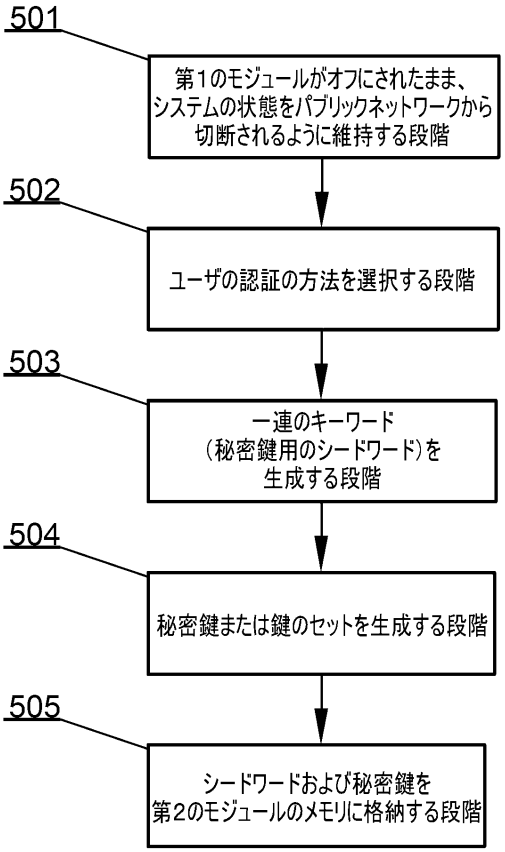
【図３】


300
ブリッジモジュール
301
302
スピーカ
303
メモリ
304
オン／オフスイッチ
305
コントローラ
306
ディスプレイ
307
電源
308
BMS
309
データインタフェース
310
SPDTスイッチ

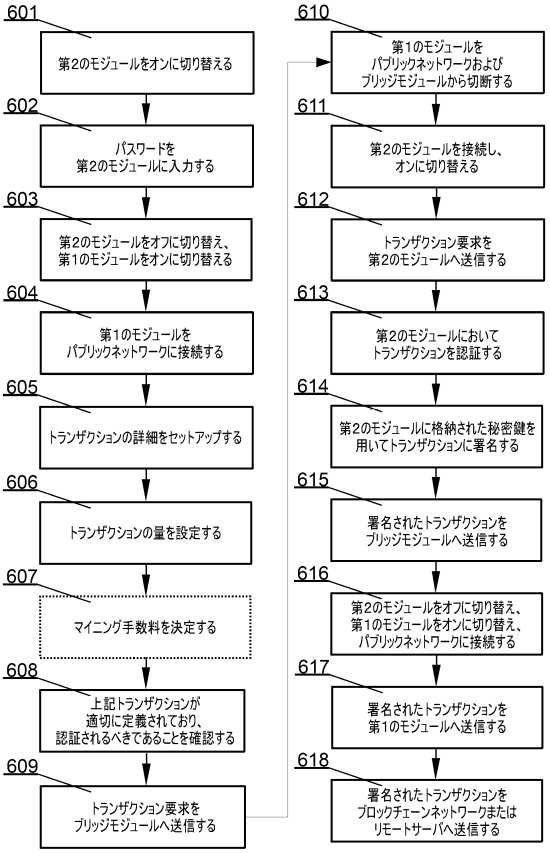
【図４】


400
100
第1のモジュール
300
310
ブリッジモジュール
401
ワイプモジュール
200
第2のモジュール

【図５】


501
第1のモジュールがオフにされたまま、システムの状態をパブリックネットワークから切断されるように維持する段階
502
ユーザの認証の方法を選択する段階
503
一連のキーワード（秘密鍵用のシードワード）を生成する段階
504
秘密鍵または鍵のセットを生成する段階
505
シードワードおよび秘密鍵を第2のモジュールのメモリに格納する段階

【図６】


601
第2のモジュールをオンに切り替える
602
パスワードを第2のモジュールに入力する
603
第2のモジュールをオフに切り替え、第1のモジュールをオンに切り替える
604
第1のモジュールをパブリックネットワークに接続する
605
トランザクションの詳細をセットアップする
606
トランザクションの量を設定する
607
マイニング手数料を決定する
608
上記トランザクションが適切に定義されており、認証されるべきであることを確認する
609
トランザクション要求をブリッジモジュールへ送信する
610
第1のモジュールをパブリックネットワークおよびブリッジモジュールから切断する
611
第2のモジュールを接続し、オンに切り替える
612
トランザクション要求を第2のモジュールへ送信する
613
第2のモジュールにおいてトランザクションを認証する
614
第2のモジュールに格納された秘密鍵を用いてトランザクションに署名する
615
署名されたトランザクションをブリッジモジュールへ送信する
616
第2のモジュールをオフに切り替え、第1のモジュールをオンに切り替え、パブリックネットワークに接続する
617
署名されたトランザクションを第1のモジュールへ送信する
618
署名されたトランザクションをブロックチェーンネットワークまたはリモートサーバへ送信する

フロントページの続き

(56)参考文献 特開２００３－１１０５４４（ＪＰ，Ａ）
国際公開第２０１７／１１２４６９（WO，Ａ１）
米国特許第０６２６８７８９（ＵＳ，Ｂ１）
特開２０１８－０９３４３４（ＪＰ，Ａ）
米国特許出願公開第２０１０／０３１８７８５（ＵＳ，Ａ１）
特開２０１７－２０８０８５（ＪＰ，Ａ）
特開２０１８－１１２８２７（ＪＰ，Ａ）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／１０
Ｇ０６Ｆ　２１／６４
Ｈ０４Ｌ　９／３２