(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7543288号
(P7543288)

(45)発行日　令和6年9月2日(2024.9.2)

(24)登録日　令和6年8月23日(2024.8.23)

(51)国際特許分類			FI		
H04L	*9/32*	*(2006.01)*	H04L	9/32	200Z
G06F	*21/64*	*(2013.01)*	G06F	21/64	
G06Q	*20/38*	*(2012.01)*	G06Q	20/38	320

請求項の数　12　（全31頁）

(21)出願番号　特願2021-547834(P2021-547834)
(86)(22)出願日　令和2年1月30日(2020.1.30)
(65)公表番号　特表2022-520273(P2022-520273A)
(43)公表日　令和4年3月29日(2022.3.29)
(86)国際出願番号　PCT/IB2020/050735
(87)国際公開番号　WO2020/165677
(87)国際公開日　令和2年8月20日(2020.8.20)
審査請求日　令和5年1月4日(2023.1.4)
(31)優先権主張番号　1902086.6
(32)優先日　平成31年2月15日(2019.2.15)
(33)優先権主張国・地域又は機関
英国(GB)
(31)優先権主張番号　1902088.2
(32)優先日　平成31年2月15日(2019.2.15)
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　100108453
弁理士　村山 靖彦
(74)代理人　100110364
弁理士　実広 信哉
(74)代理人　100133400
弁理士　阿部 達彦
(72)発明者　クレイグ・スティーヴン・ライト
イギリス・カーディフ・ＣＦ１０・２ＨＨ・チャーチル・ウェイ・チャーチル・ハウス・セブンス・フロア・アーカート－ダイクス・アンド・ロード・エルエル
最終頁に続く

(54)【発明の名称】　ブロックチェーンネットワークを介した移転を実施するためのコンピュータで実施されるシステムおよび方法

(57)【特許請求の範囲】

【請求項１】

移転者の第1の検証リソースと被移転者の第2の検証リソースとの間でのブロックチェーン上での資産の移転を促進するように動作可能な、ブロックチェーンで実施される簡易的支払検証システムであって、

前記第1の検証リソースは、

少なくとも1つのブロックチェーントランザクションに関する完成したトランザクションデータと、

前記少なくとも1つのブロックチェーントランザクションの完成したマークルパスとを備え、

前記第2の検証リソースは、

i)前記第1の検証リソースから、前記少なくとも1つのブロックチェーントランザクションに関する前記完成したトランザクションデータと、前記少なくとも1つのブロックチェーントランザクションのための前記マークルパスとを受信および/または要求し、

ii)前記少なくとも1つのトランザクションのためのマークル証明を検証するために、前記マークルパスと、前記少なくとも1つのブロックチェーントランザクションに関する前記完成したトランザクションデータとを使用し、

iii)前記マークル証明の検証が成功すると、さらなるトランザクション(Tx3)を前記ブロックチェーンに送信する

ように動作可能である、システム。

【請求項２】
前記さらなるトランザクション(Tx3)は、前記少なくとも1つのブロックチェーントランザクションの出力を費やす入力を備える、請求項1に記載のシステム。
【請求項３】
前記第1および/または第2の検証リソースが、スマートカード、デジタルウォレット、もしくは軽量および/もしくはSPVウォレットであり、またはそれらを備える、請求項1または2に記載のシステム。
【請求項４】
前記第2の検証リソースが、前記第1の検証リソースから、オフチェーン通信を使用して、前記完成したトランザクションデータおよび前記マークルパスを受信および/または要求するように動作可能である、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】
複数の第2の検証リソースと、前記複数の第2の検証リソースと通信するように動作可能な協調コンポーネントとをさらに備える、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1の検証リソースが前記資産の前記移転者であり、前記第2の検証リソースが前記資産の前記被移転者である、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】
前記少なくとも1つのブロックチェーントランザクションの出力を費やすための署名、
移転値、および/または
公開鍵アドレス
のうちの少なくとも1つを、前記第2の検証リソースが前記第1の検証リソースから受信および/もしくは要求するように動作可能でもあり、または前記第1の検証リソースがまた前記第2の検証リソースに送信するように動作可能である、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】
移転者の第1の検証リソースと被移転者の第2の検証リソースとの間でのブロックチェーン上での資産の移転を促進するための簡易的支払検証のブロックチェーンで実施される方法であって、
i)前記第2の検証リソースにおいて、
少なくとも1つのブロックチェーントランザクションに関する完成したトランザクションデータと、
前記少なくとも1つのブロックチェーントランザクションの完成したマークルパスと
を受信するステップであって、前記トランザクションデータおよびマークルパスが、前記トランザクションデータおよびマークルパスを記憶する前記第1の検証リソースから受信される、ステップと、
ii)前記第2の検証リソースによって、前記少なくとも1つのトランザクションのためのマークル証明を検証するために、前記マークルパスと、前記少なくとも1つのブロックチェーントランザクションに関する前記完成したトランザクションデータとを使用するステップと、
iii)前記第2の検証リソースによって、前記少なくとも1つのトランザクションのための前記マークル証明の検証が成功すると、さらなるトランザクション(Tx3)を前記ブロックチェーンに送信するステップと
を備える、方法。
【請求項９】
i)前記少なくとも1つのトランザクションのための前記マークル証明の検証、ならびに/または
ii)前記第1の検証リソースからの前記完成したトランザクションデータおよびマークルパスの受信もしくは要求

というステップがオフチェーンで実行される、請求項8に記載の方法。
【請求項１０】
前記第1の検証リソースが前記資産の前記移転者であり、前記第2の検証リソースが前記資産の前記被移転者である、請求項8または9に記載の方法。
【請求項１１】
前記第1および/もしくは第2の検証リソースが、スマートカード、デジタルウォレット、もしくは軽量および/もしくはSPVウォレットであり、もしくはそれらを備える、請求項8から10のいずれか一項に記載の方法。
【請求項１２】
コンピュータシステムのプロセッサによって実行される結果として、請求項8から11のいずれか一項に記載の方法または請求項1から7のいずれか一項に記載のシステムの実施形態を前記コンピュータシステムに少なくとも実行させる、実行可能命令が記憶された非一時的コンピュータ可読記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は全般に、ネットワークを介したリソースの通信および移転に関し、より具体的には、ブロックチェーンネットワークを介して行われる移転、およびデジタルウォレットにも関する。本発明は特に、限定はされないが、ブロックチェーン上で実施される、またはそれを介して通信される、暗号通貨、トークン、および他のリソースの移転を処理するためのウォレットに適している。本発明は、限定はされないが、デジタルウォレットおよびブロックチェーンベースの通信の、セキュリティ、多用途性、レジリエンス、および効率性を高めることを含む、数々の技術的な利点をもたらす装置と技法を提供する。
【背景技術】
【０００２】
この文書では、すべての形式の電子的なコンピュータベースの分散型台帳を含むものとして、「ブロックチェーン」という用語を使用する。これらは、コンセンサスベースのブロックチェーンおよびトランザクションチェーン技術、認可型台帳および非認可型台帳、共有台帳、ならびにこれらの変形を含む。最もよく知られているブロックチェーン技術の応用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施態様が提案され開発されている。便宜的に、および説明のために、本明細書ではビットコインに言及することがあるが、本発明はビットコインブロックチェーンととも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施態様およびプロトコルが本発明の範囲内にあることに留意されたい。「ビットコイン」という用語は、ビットコインプロトコルから派生した、またはその任意の変形を実施する、プロトコルまたは実施態様のすべての変形を含むものとして本明細書において使用される。「ユーザ」という用語は、本明細書では人またはプロセッサベースのリソースを指すことがある。
【０００３】
ブロックチェーンは、ブロックからなるコンピュータベースの非集中型の分散型システムとして実施されるピアツーピア電子台帳であり、ブロックはトランザクションからなる。各トランザクションは、ブロックチェーンシステムの参加者間でのデジタル資産の管理権の移行を符号化するとともに、少なくとも1つの入力および少なくとも1つの出力を含む、データ構造である。各ブロックは以前のブロックのハッシュを含むので、ブロックは一緒につながれるようになり、ブロックチェーンの発足以来ブロックチェーンに書き込まれているすべてのトランザクションの恒久的で変更不可能な記録を作成する。各ブロックのヘッダは、そのブロックのマークルルートを提供するフィールドを含む。マークルルートは、単一のハッシュが到達するまでブロックからのトランザクションIDのペアを繰り返し一緒にハッシュすることによって生成される。このマークルルートは、トランザクションがブロックの一部であることを検証するための効率的な機構をもたらし、それは、ユーザがブロックチェーン全体をダウンロードすることなく特定のトランザクションを検証する

ことを可能にするからである。

【０００４】

トランザクションには、入力および出力に、スクリプトとして知られている小さいプログラムが埋め込まれており、これが、トランザクションの出力にどのようにアクセスできるか、および誰がアクセスできるかを指定する。ビットコインプラットフォームでは、これらのスクリプトは、スタックベースのスクリプト言語を使用して書かれる。

【０００５】

トランザクションがブロックチェーンに書き込まれるには、トランザクションは「妥当性確認」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確実にするように作業を実行し、無効なトランザクションはネットワークから拒絶される。ノードにインストールされるソフトウェアクライアントは、ロッキングスクリプトおよびアンロッキングスクリプトを実行することによって、未使用トランザクション(UTXO)に対してこの妥当性確認作業を実行する。ロッキングスクリプトおよびアンロッキングスクリプトの実行がTRUEであると評価される場合、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には、トランザクションは、i)トランザクションを受信する第1のノードによって妥当性確認されなければならず、トランザクションが妥当性確認される場合、ノードはそれをネットワークの中の他のノードに中継し、ii)マイナーによって構築された新しいブロックに追加されなければならず、iii)マイニング、すなわち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。(注意: 上で説明されたような妥当性確認は、特定のトランザクションがブロックチェーン上のブロックに含まれているかどうかを確証または確認することを意味するものとして本明細書において使用される「検証」と混同されるべきではない)。

【０００６】

ブロックチェーンにUTXOとして記憶されると、ユーザは、関連する暗号通貨の管理権を、別のトランザクションの中の入力と関連付けられる別のアドレスに移転することができる。これはしばしば、ユーザの暗号通貨と関連付けられる公開鍵および秘密鍵のペアを記憶するデジタルウォレットを使用して行われる。SPVウォレット(簡易的支払検証)を含む、様々な形式の知られている暗号通貨ウォレットがある。

【０００７】

AliceとBobとの間でのSPVベースの暗号通貨の交換では、双方が同じタイプのSPVウォレットを使用する。SPVウォレットは、ユーザの秘密鍵および公開鍵、未使用トランザクション、ならびにブロックヘッダを記憶する。それは、ブロックチェーンネットワークに接続する能力も有する。「ブロックヘッダ」という用語は、当技術分野において知られており、ブロックチェーントランザクションのブロックの一番上で提供されるデータを指すために使用される。ブロックヘッダはブロックを一意に識別するので、ブロックはブロックチェーン上で位置特定され得る。ブロックヘッダは、ブロックの内容全体の固有の概要またはフィンガープリントを提供するデータのフィールドを備える。ブロックヘッダは、そのブロックの中のトランザクションのすべてのハッシュである、マークルルートを含む。ユーザは次いで、ブロックチェーン全体をダウンロードする必要なく、特定のトランザクションがブロックチェーン上の特定のブロックに含まれていたかどうかを確認(すなわち、検証)するために、そのルートを伴うマークル木を探索することが可能である。

【０００８】

SPVウォレットの利点は、他の形式のウォレットによりブロックチェーンの完全な確認を実行するのではなく、トランザクションが検証されたことを確認するだけでよい(よって「簡易的支払検証」という名前である)ので、電話およびラップトップなどの処理能力とストレージが限られているデバイスが、ビットコインエコシステム内で動作することを可能にするということである。SPVウォレットは、トランザクションのいずれを含む必要もなく、ブロックヘッダのみをダウンロードするので、これは、必要とされるストレージ空間を159GB(2018年11月現在)から43MBに減らし、ストレージ要件は、ビットコインがさ

らに拡大しても一年で4.2MBという一定の量しか増えない。
【０００９】
Aliceが何らかの暗号通貨またはトークン化された資産/リソースをBobに送ることを望むと仮定する。従来のSPVウォレットを使用するときの、AliceとBobとの間の通信フローは次の通りである。
1. Aliceがブロックチェーントランザクション(TX)を作成し、出力においてBobのアドレスを指定し、(Aliceへの以前の未使用トランザクションから)入力のための署名を提供する。
2. Aliceがトランザクションをブロックチェーンネットワークにブロードキャストする。
3. トランザクションが受け入れられたことを検証するために、Bobがネットワークに問い合わせる。
【先行技術文献】
【特許文献】
【００１０】
【文献】国際公開第2017145016号
【非特許文献】
【００１１】
【文献】“ Bitcoin: A Peer-to-Peer Electronic Cash System"、Satoshi Nakamoto、2008年、www.bicoin.org/bitcoin.pdf
【発明の概要】
【発明が解決しようとする課題】
【００１２】
基本的に、ブロックチェーンネットワークは、AliceのウォレットとBobのウォレットとの間の仲介役として働く。しかしながら、これはリソース集約的なプロセスであるだけでなく、ネットワーク接続も必要とする。Aliceのウォレットが実行されているデバイスが何らかの理由でオフラインである場合、移転を完了することはできない。したがって、限定はされないが、あるエンティティ(たとえば、コンピューティングリソース/ノード/デジタルウォレット)から別のエンティティへの電子的な移転を行うためのより信頼でき効率的な機構を実施するための、方法、システム、およびデバイスをどのように提供するかを含む、技術的な課題がある。
【００１３】
したがって、少なくともこれらの技術的な問題を解決する解決策を提供することが望ましい。そのような改善された解決策がここで考案される。したがって、本開示の実施形態によれば、添付の特許請求の範囲において定義されるようなシステムおよび方法が提供される。
【課題を解決するための手段】
【００１４】
本開示によれば、コンピュータおよび/またはブロックチェーンで実施される方法と対応するシステムが提供されてもよい。システムは、1つまたは複数のコンピュータで実施されるリソースを備えてもよい。これらは、ハードウェアおよび/またはソフトウェアで実施されるリソースであってもよい。
【００１５】
本開示の実施形態は、ブロックチェーンネットワーク上での、またはそれを介した、(移転者と被移転者との間での)資産の移転を促進または可能にするように動作可能であってもよい、コンピュータで実施されるリソースを提供してもよい。移転者(資産を送る者)はAliceと呼ばれることがあり、被移転者(資産を受け取る者)はBobと呼ばれることがある。資産は、任意のタイプの資産、たとえば、暗号通貨もしくはトークンの一部分、または、ブロックチェーントランザクションを介して何らかの方法でデジタル的に移転され得る他の何かであってもよく、またはそれを備えてもよい。

【００１６】
追加または代替として、システムは、ブロックチェーントランザクションの検証を促進または可能にするように動作可能であってもよい。これはSPV検証であってもよい。システムはSPVシステムとして説明されることがある。「するように動作可能である」という用語は、「なされる」および「構成される」という用語を含むものとして本明細書において使用される。
【００１７】
本開示の実施形態は、移転者と被移転者との間でのブロックチェーン上での資産の移転を促進するように動作可能なシステムを提供してもよく、このシステムは、
少なくとも1つのブロックチェーントランザクションに関する完成したトランザクションデータと、
少なくとも1つのブロックチェーントランザクションの完成したマークルパスと
を備える、第1の検証リソースと、
第1の検証リソースから、少なくとも1つのブロックチェーントランザクションに関する完成したトランザクションデータと、少なくとも1つのブロックチェーントランザクションのためのマークルパスとを受信および/または要求する
ように動作可能な第2の検証リソースとを備える。
【００１８】
トランザクションデータは、ブロックチェーンプロトコルに従って有効なブロックチェーントランザクションを形成するのに十分なものであるという意味で、完成していてもよい。それは、「完全な」トランザクションデータと呼ばれることがある。第1および/または第2の検証リソースは、追加または代替として、「移転リソース」または単に「コンピュータベースのリソース」と呼ばれてもよい。
【００１９】
第1の検証リソースは実質的に、Aliceに関連して、および/または「オフラインSPVウォレット」という表題のセクションおよび関連する図面において、本明細書において開示されるようなものであってもよい。便宜的に、以後第1の検証リソースはAliceと呼ばれることがあり、第2の検証リソースはBobと呼ばれることがある。第2の検証リソースは実質的に、Bobに関連して、または本明細書において提供される「PoS SPVウォレット」という表題のセクションにおいて、本明細書において説明されるようなものであってもよい。
【００２０】
第2の検証リソースはさらに、少なくとも1つのトランザクションのためのマークル証明を検証するためにマークルパスを使用するように動作可能であってもよい。
【００２１】
有利なことに、マークルパスは、ブロックチェーンネットワーク上のピアから取得されなければならないのではなく、AliceからBobに提供され得る。これは、Bobが、少なくとも1つのトランザクションのローカルSPV確認を実行することを、ブロックチェーンもしくはネットワークにアクセスする必要なく、またはそれと通信する必要なく可能にする。
【００２２】
その上、オフチェーン通信を使用して、BobとAliceとの間で、データ、要求、および応答が(直接)送信されてもよい。「オフチェーン通信」という用語は、通信がブロックチェーンまたはブロックチェーンネットワークを介さないこと、それらに問い合わせないこと、またはそれらと対話しないことを意味することが意図される。Aliceおよび/またはBobは、ネットワーク上のノードまたはピアではなくてもよい。
【００２３】
第2の検証リソースはさらに、マークル証明の検証が成功すると、トランザクションをブロックチェーンに送信するように動作可能であってもよい。これは、本明細書において、および図8と図10を参照して説明され開示されるような、Tx3であってもよい。それは、少なくとも1つのブロックチェーントランザクションの出力(UTXO)を費やす入力を備えるブロックチェーントランザクションであってもよい。

【００２４】
第1および/または第2の検証リソースは、スマートカード、デジタルウォレット、軽量および/もしくはSPVウォレットであってもよく、またはそれらを備えてもよい。
【００２５】
第2の検証リソースは、第1の検証リソースから、オフチェーン通信を使用して、完全なトランザクションデータおよびマークルパスを受信および/または要求するように動作可能であってもよい。「オフチェーン」は、通信がブロックチェーンネットワークおよび/またはブロックチェーンと関わらないこと、それらを介さないこと、またはそれらに問い合わせないことを意味してもよい。
【００２６】
システムはさらに、少なくとも1つのトランザクションのためのマークル証明を検証するためにマークルパスを使用し、検証に成功すると、トランザクションをブロックチェーンに送信するように動作可能であってもよい。検証は、第2の検証リソースにおいて、またはそれによって、(ローカルに)実行されてもよい。それは「オフチェーン」で実行されてもよく、これは、ブロックチェーンネットワークもしくはブロックチェーンに問い合わせることによって、またはそれを使用することによって実行されないことを意味する。
【００２７】
システムはさらに、複数の第2の検証リソースと、複数の検証リソースと通信するように動作可能な協調コンポーネントとを備えてもよい。これは実質的に、「分割業者ウォレット」と本明細書において開示されるようなものであってもよい。
【００２８】
第1の検証リソースは資産の移転者であってもよく、第2の検証リソースは資産の被移転者であってもよい。
【００２９】
少なくとも1つのブロックチェーントランザクションの出力を費やすための署名、
移転値、および/または
公開鍵アドレス
のうちの少なくとも1つを、第2の検証リソースが第1の検証リソースから受信および/もしくは要求するように動作可能であってもよく、または、第1の検証リソースも第2の検証リソースに送信するように動作可能であってもよい。
【００３０】
移転値は、暗号通貨または他のリソースの量であってもよい。それは、移転されるべき資産または資産の値であってもよい。それは支払の量であってもよい。
【００３１】
本開示の実施形態は、ブロックチェーンで実施される方法も提供する。これは、簡易的支払検証方法であってもよい。それは、移転者と被移転者との間でのブロックチェーン上での資産の移転を促進するようになされてもよく、
第2の検証リソースにおいて、
少なくとも1つのブロックチェーントランザクションに関する完成したトランザクションデータと、
少なくとも1つのブロックチェーントランザクションの完成したマークルパスと
を受信するステップを備え、
トランザクションデータおよびマークルパスは、トランザクションデータおよびマークルパスを記憶する第1の検証リソースから受信される。
【００３２】
方法はさらに、少なくとも1つのトランザクションのためのマークル証明を検証するためにマークルパスを使用するステップを備えてもよい。
【００３３】
方法はさらに、マークル証明の検証が成功すると、トランザクションをブロックチェーンに送信するステップを備えてもよい。

【００３４】
以下のステップがオフチェーンで実行されてもよい。
i)マークル証明の検証、ならびに/または
ii)第1の検証リソースからの完成したトランザクションデータおよびマークルパスの受信もしくは要求。
【００３５】
第1の検証リソースは資産の移転者であってもよく、第2の検証リソースは資産の被移転者であってもよい。第2の検証リソースは、マークル証明の検証が成功すると、トランザクションをブロックチェーンに送信するように動作可能であってもよい。第1および/または第2の検証リソースは、スマートカード、デジタルウォレット、または軽量および/もしくはSPVウォレットであってもよく、またはそれらを備えてもよい。
【００３６】
本開示はまた、コンピュータシステムのプロセッサによって実行される結果として、本明細書において特許請求もしくは開示されるような方法またはシステムの実施形態をコンピュータシステムに少なくとも実行させる、実行可能命令が記憶された非一時的コンピュータ可読記憶媒体も提供する。
【００３７】
システムまたはリソースに関連して本明細書において説明されるあらゆる特徴が、本開示の方法に等しく適用可能であり、その逆も当てはまる。
【００３８】
本開示のこれらおよび他の態様は、本明細書において説明される実施形態から明らかであり、またはそれを参照して解明される。ここで、本開示の実施形態は、単なる例として、添付の図面を参照して説明される。
【図面の簡単な説明】
【００３９】
【図１】本開示のある実施形態による、「オフラインSPVウォレット」を示す図である。
【図２】本開示のある実施形態による、「オンラインおよびオフラインSPVウォレット」を示す図である。
【図３】本開示のある実施形態による、「PoS SPVウォレット」を示す図である。
【図４】本開示のある実施形態による、部分的なおよび完成したテンプレートトランザクションならびに関連するマークル証明を示す図である。
【図５】本開示のある実施形態による、分割SPVウォレットを使用してトランザクションを行うときのAliceとBobとの間のデータおよび対話の流れを示す図である。
【図６】使用される本開示の実施形態の概略図である。
【図７】様々な実施形態が実施され得るコンピューティング環境を示す概略図である。
【図８】3つのトランザクションと、それらをブロック(ヘッダ)に関連付けるために使用され得るマークルパスとを示す、概略図である。
【図９】従来のSPV支払方法を示す図である。
【図１０】本開示のある実施形態による方法を示す図である。
【図１１】従来技術において知られているようなバイナリマークル木の例を示す図である。
【図１２】従来技術による、マークルパスを使用した、ルートRにより表される木におけるデータブロックD_1のマークル存在証明を示す図である。
【発明を実施するための形態】
【００４０】
従来技術: マークル木
本開示の実施形態は、マークル木の概念を利用して利益を得るので、背景としてのみ説明を行う。
【００４１】
マークル木は、データの収集のセキュアな検証を可能にする、階層的なデータ構造である。マークル木では、木の中の各ノードはインデックスペア(i, j)を与えられており、N(i,

j)として表されている。インデックスi, jは単に、木の中の特定の位置に関係する数値ラベルである。マークル木の重要な特徴は、そのノードの各々の構築が以下の(簡略的な)式により支配されるということである。

【００４２】

【数１】

$$N(i,j) = \begin{cases} H(D_i) & i = j \\ H\big(N(i,k) \parallel N(k+1,j)\big) & i \neq j \end{cases},$$

【００４３】

ここで、k=(i+j-1)/2であり、Hは暗号学的ハッシュ関数である。

【００４４】

これらの式に従って構築されるラベリングされたバイナリマークル木が図11に示されており、この図から、i=jの場合はリーフノードに対応し、これは単に、データD_iの対応する第iのパケットのハッシュであることがわかる。i≠jの場合は内部ノードまたは親ノードに対応し、これは、1つの親(マークルルート)が発見されるまで子ノードを再帰的にハッシュして連結することによって生成される。

【００４５】

たとえば、ノードN(1, 4)は、4つのデータパケットD_1...、D_4から、

N(1,4) = H(N(1,2) ‖ N(3,4))
= [H(N(1,1) ‖ N(2,2)) ‖ H(N(3,3) ‖ N(4,4))]
= [H(H(D_1) ‖ H(2) ‖ H(H(3) ‖ H(4))]

として構築される。

【００４６】

木深度Mは、木の中のノードの最低のレベルとして定義され、ノードの深度mは、そのノードが存在するレベルである。たとえば、図11では、m_{root}=0かつm_{leaf}=Mであり、M=3である。

【００４７】

マークル証明

マークル木の主要な機能は、何らかのデータパケットD_1がN個のデータパケットのリストまたは集合$D \in \{D_1, \ldots, D_N\}$の要素であることを検証することである。検証のための機構は、マークル証明として知られており、所与のデータパケットD_1およびマークルルートRのためのマークルパスとして知られているハッシュの集合を取得することからなる。データパケットのためのマークルパスは単に、「認証パス」としばしば呼ばれることがある、繰り返されるハッシュおよび連結によってルートRを再構築することが必要とされる、ハッシュの最小限のリストである。存在証明は、すべてのパケットD_1、... 、D_Nが証明者に知られている場合、自明に実行され得る。しかしながら、これは、マークルパスよりはるかに大きなストレージオーバーヘッドを必要とし、データ集合全体が証明者に対して利用可能であることも必要とする。マークルパスを使用することとリスト全体を使用することとの比較が以下の表に示されており、ここで、バイナリマークル木を使用し、データブロックNの数が2の整数乗に厳密に等しいと仮定した。そうではないとすると、マークル証明のために必要とされるハッシュの数は、各事例において±1だけ異なるであろう。

【００４８】

【表１】

					マークル木
データパケットの数	8	32	64	256	$N = 2^M$
存在証明のために必要とされるハッシュの数	3	5	7	9	$M = \log_2 N$

表：マークル木の中のリーフノードの数とマークル証明のために必要とされるハッシュの数との関係.

【００４９】

データパケットの数がリーフノードの数に等しい、この簡略化されたシナリオでは、マークル証明を計算するために必要とされるハッシュ値の数は、対数的にスケーリングすることがわかる。N個のデータハッシュを記憶して自明な証明を計算するより、$\log_k N$個のハッシュに関わるマークル証明を計算する方が、明らかに、はるかに効率的で実用的である。

【００５０】

方法

マークルルートRが与えられたとき、データブロックD_1がRによって表される集合$D \in \{D_1, \ldots, D_N\}$に属することを証明するのを望む場合、マークル証明を次のように実行することができる。

i. 信用されるソースからマークルルートRを取得する。

ii. ソースからマークルパスΓを取得する。この場合、Γはハッシュの集合である。

Γ = {N (2, 2), N(3, 4), N(5, 8)}

iii. D_1およびΓを使用してマークル証明を次のように計算する。

a. データブロックをハッシュして以下を取得する。

N(1, 1) = H(D_1)

b. N(2, 2)と連結し、ハッシュして以下を取得する。

N(1, 2) = H(N(1, 1) ¦ ¦ N(2, 2))

c. N(3, 4)と連結し、ハッシュして以下を取得する。

N(1, 4) = H(N(1, 2) ¦ ¦ N(3, 4))

d. N(5, 8)と連結し、ハッシュしてルートを取得する。

N(1, 8) = H(N(1, 4) ¦ ¦ N(5, 8))

R' = N(1, 8)

e. (i)において取得されたルートRと計算されたルートR'を比較する。

I. R'=Rである場合、木におけるD_1の存在、したがってデータ集合Dが確証される。

II. R'≠Rである場合、証明は失敗し、D_1がDの要素であると確証されない。

【００５１】

これは、マークル木およびそのルートによって表されるデータ集合の一部として、何らかのデータの存在証明を提供するための、効率的な機構である。たとえば、データD_1がブロックチェーントランザクションに対応し、ルートRがブロックヘッダの一部として公に利用可能である場合、トランザクションがそのブロックに含まれていたことをすぐに証明

することができる。

【００５２】

我々の例示的なマークル木の一部としてのD_1の存在を認証するプロセスが図12に示されており、これは、マークルパスを使用してルートRによって表される木におけるデータブロックD_1のマークル存在証明を示す。これは、所与のブロックD_1およびルートRのためのマークル証明を実行することが、必要最小限の数のハッシュ値のみを使用することによってマークル木を「上方」に実質的に走査することであることを実証する。

【００５３】

本開示のいくつかの実施形態は、これらの技法を使用してより効率的でセキュアな検証法を提供し、ここでそれに関する議論に注目する。

【００５４】

簡易的支払検証(SPV)

本開示は改善されたSPV解決策を提供するので、参照を簡単にするために、知られているSPV検証技法の概要をここで与える。

【００５５】

以下では、何らかの商品の販売時点において取引することを望むAlice(顧客)およびBob(業者)を考える。Nakamotoホワイトペーパー(“Bitcoin: A Peer-to-Peer Electronic Cash System"、Satoshi Nakamoto、2008年、www.bicoin.org/bitcoin.pdf)において概説されたような従来の方法を使用して、簡易的支払検証(SPV)を使用してこの対話がどのように発生するかを調べる。「本発明の概要」と題されるセクションにおいて、本発明の説明のための実施形態に関して、同じ対話が後で説明される。両方の場合において、3つのブロックチェーントランザクション(Tx)の役割を考える。2つのトランザクションが、Aliceによって所有される消費可能な出力(UTXO)を有する。

・Tx1 - 消費可能な出力(vout-1)を伴うトランザクション

・Tx2 - 消費可能な出力(vout-0)を伴うトランザクション

【００５６】

これらのトランザクションTx1、Tx2は、それらが、何らかの後続のトランザクション、たとえばTx3の入力によって費やされている出力を備えるトランザクションであることを述べる簡潔な方法として、入力トランザクションとして本明細書において言及される。

【００５７】

第3のブロックチェーントランザクションは支払トランザクションである。

・Tx3 - Bobに支払う2つの入力および1つの出力として、vout-0およびvout-1を使用するトランザクション。本発明のより簡単な実証に対して、2つの入力および1つの出力しかない。

【００５８】

これらの3つのトランザクション、およびブロック(ヘッダ)にそれらを関連付けるために使用され得るマークルパスが、図8に概略的に示されている。

【００５９】

SPVの基本的な概念は、Nakamotoホワイトペーパーの頃から存在しており、最初のビットコインクライアント(v 0.1, 2009)において実施された。基本的に、SPVは、ビットコインブロックチェーンの2つの性質を利用する。

1. 所与のトランザクションがマークル木に含まれマークルルートにより表されることを検証するために容易に使用され得るマークル証明、および

2. トランザクションのマークル木のマークルルートを含めることによってトランザクションのブロックを表すブロックヘッダ。

【００６０】

これらの2つの性質を組み合わせることによって、ネットワークによりトランザクションが処理されていることを検証するために、軽量なビットコインクライアントは、ブロックを完全に維持するのではなく、ブロックチェーン全体に対するブロックヘッダのコピーのみを維持するだけでよい。所与のトランザクションが処理されてブロックに含まれてい

ることを検証するために、SPVクライアントは、
・最新のブロックヘッダの完全なリスト、
・対象のトランザクションのためのマークルパス
のみを必要とする。
【００６１】
性質1から、SPVユーザは、上のセクションにおいて説明されたように単にマークルパス認証証明を実行することによって、所与のトランザクションがマークルルートによって表されるマークル木の一部であることを検証できることがわかる。そして、性質2から、SPVクライアントがこのマークルルートを含む有効なブロックヘッダを有する場合、トランザクションはブロックチェーンの中のブロックの一部でもあることがわかる。ビットコインにおいてこのタイプの支払検証を実行することは、「SPV確認」を実行することとして本明細書において呼ばれる。
【００６２】
Nakamotoにより規定されるようなこのSPV機構は、販売時点を含む、SPVクライアントの実施の既存の方法を特徴付ける。重要なことに、SPVの実施における最新技術は、支払がブロックに含まれていることを(ブロックチェーン上の適切な深度、たとえば6まで)確証することによって支払が受け取られたことをユーザが検証するようなパラダイムに基づく。実質的に、これは、トランザクションがマイニングされたことを検証するための、トランザクションのブロードキャスト後確認である。
【００６３】
対照的に、本発明は、トランザクションのブロードキャストの前に必要なSPV確認がトランザクションの入力に対して実行されることを必要とする。力点のこの変化は、無効なトランザクションを扱う際のネットワークに対する負荷とトラフィックを大きく減らす。
【００６４】
既存のSPVシステムにおける第2の重要なパラダイムは、SPVクライアントが、SPV確認のために必要とされるマークルパスを取得するために、ネットワーク上のすべてのノードに問い合わせなければならないということである。これは、「SPVクライアントは、マークルルートおよび関連するトランザクション情報を知っており、フルノードからそれぞれのマークル枝を要求する」ことを述べている、ビットコイン開発者ガイド(https://bitcoin.org/en/developer-guide)において見出され得る。
【００６５】
本発明の実施形態は、軽量なビットコインクライアントのユーザが、所有する未使用トランザクション出力に関するマークルパスの自分のコピーを保持すること、維持すること、またはそれへのアクセス権を少なくとも有することを規定することによって、ネットワークへのこの負担をなくすような、SPV確認に関わる機構と方法を提供する。
【００６６】
図9を参照すると、(トランザクションの時点で)SPVを実施するための従来の方法は次の通りである。
【００６７】
[1]メッセージ: BobからAliceへ
・Bob(業者)が自分の公開鍵アドレスをAlice(顧客)に送信する。Bobのメッセージは、Bobの選ばれた償還スクリプトのハッシュとして提供される任意の他の消費条件に加えて、支払われるべき額も含んでもよい。
・Aliceも、支払トランザクションTx3のトランザクションID TxID3をBobに通信する(図示せず)。
【００６８】
[2]P2PネットワークがAliceとBobとの間の交換を仲介する。
[2.i]メッセージ:AliceからP2Pネットワークへ
・AliceがTx3をネットワークにブロードキャストする。
[2.ii]メッセージ:BobからP2Pネットワークへ

・Bobが、Tx3がブロックチェーンへとマイニングするために受け入れられるかどうかを確認するためにネットワークに問い合わせる。

・Bobが、支払がネットワークによって有効であると見なされることに満足するまで、連続的なクエリ[2.ii]を送信する。Bobは[2.i]が行われる前に問い合わせを開始してもよいことに留意されたい。

・Bobが満足する場合、Bobは、次のブロックがマイニングされるのをどちらの当事者も待つことなく、トランザクションを完了したものとして扱ってもよい。

【００６９】

[3]SPV確認(メッセージ): BobからP2Pネットワークへ

・Bobが、次のブロックがマイニングされるのを待機し、ネットワーク上で新しいブロックヘッダがブロードキャストされるにつれて、それらをダウンロードする。

・Bobが「SPV確認」要求をネットワークに送信する。これは、最近マイニングされたブロックの中のマークルルートにTx3を結び付ける、Tx3に対応するマークルパスに対する要求である。

・ネットワークがマークルパスをBobに提供できる場合、Bobは、自分のSPVウォレットを使用してマークル証明を自分で計算し、支払Tx3が処理されたことを確認することができる。

【００７０】

この通信フローが図9に示されている。[2.i]、[2.ii]、および[3]は、P2Pネットワークによって仲介されるので、ネットワーク上のトラフィックに寄与することに留意されたい。既存のSPVパラダイムでは、必要なSPV確認[3]が、

・支払(Tx3)が出された後で、

・支払(Tx3)自体に際して、

・マークルパスを提供する他のネットワークピアの助けにより、

実行されることにも留意されたい。

【００７１】

ここで、この既知の手法を本発明の手法と対比させる。

【００７２】

本開示の実施形態の概要

【００７３】

本開示は、低帯域幅SPVシステムを使用して、ブロックチェーンネットワーク(以後便宜的に「ビットコイン」ネットワークと呼ぶ)上での検証のために改善されたセキュリティ解決策を提供する。本発明の実施形態によれば、リソースの送信者(たとえば、顧客)は、トランザクションが受信者(たとえば、業者)により作成および/または受容されるのに、オンラインである必要はない。受信者のみがオンラインである必要がある。便宜的に、および参照を簡単にするために、「顧客」または「Alice」という用語が「送信者」の代わりに使用され、「業者」または「Bob」という用語が「受信者」の代わりに使用される。

【００７４】

本開示の実施形態は、業者のウォレットがネットワークに接続されることしか必要としないので、従来のSPVトランザクションと比較して新しい、関係者間の通信フローを利用する。これは、顧客が提供する必要のある情報、たとえば変更アドレス、署名などを伴うテンプレート(「未完成のトランザクション」と呼ばれることがある)を業者のウォレットが作成することによって達成される。業者が顧客からこの要求される情報を受信すると、業者はトランザクションをネットワークにブロードキャストする。

【００７５】

したがって、本開示は、ビットコインネットワーク上での単純な支払検証の間の、取引を行う関係者とネットワークとの間の通信と交換のプロセスを、

業者→顧客→ネットワーク→業者

から

業者→顧客→業者→ネットワーク

へと根本的に変更する。

【００７６】

AliceおよびBobは、たとえば国際公開第2017145016号において説明されるものなどの、秘密共有プロトコルを使用してメッセージを内密に交換してもよい。

【００７７】

このプロセスの変更は、顧客のウォレット、また業者のウォレットの両方に対して、新規の設計が必要になるという技術的な問題を生む。したがって、本発明の実施形態は少なくとも以下のことを提供する。

1. Aliceのための新規の顧客ウォレット(「オフラインウォレット」と呼ぶ):

これは、Aliceの公開鍵、秘密鍵、消費可能な出力を含むトランザクション、すべてのブロックヘッダ、および重要なことに、記憶されているトランザクションのマークルパスを記憶する

(ネットワークに接続されるというAliceに対する要件をなくす)

2. Bobのための新規の業者ウォレット(「販売時点(PoS)ウォレット」と呼ぶ):

これは、Bobの公開鍵およびすべてのブロックヘッダを記憶する。

【００７８】

これらの構成要素のより詳細な説明がここで与えられる。

【００７９】

図10を参照すると、本発明のある実施形態による、(トランザクションの時点で)SPVを実施するための例示的な方法が、次のように与えられる。

【００８０】

[1]メッセージ: BobからAliceへ

・Bobが、支払トランザクションテンプレート(テンプレートTx3)をAliceに送信し、Aliceから以下の情報を要求する:

Aliceが支払(Tx3)への入力として費やすことを望む少なくとも1つの出力を備えるすべての入力トランザクション(Tx1およびTx2)に対する完全なトランザクションデータ、

入力トランザクションをそれぞれのブロックヘッダと関連付けられるそれぞれのマークルルートと結び付ける、すべての入力トランザクション(Tx1およびTx2)のためのマークルパス、

完成した(すなわち、埋められたテンプレート)支払トランザクション(Tx3)。

・Bobは自分のアドレスを送信するのではなくAliceから情報を要求していることに留意されたい。

【００８１】

[2]メッセージ: AliceからBobへ

・Aliceが要求された情報をBobに送信する:

Aliceが支払(Tx3)への入力として費やすことを望む少なくとも1つの出力を備えるすべての入力トランザクション(Tx1およびTx2)に対する完全なトランザクションデータ、

入力トランザクションをそれぞれのブロックヘッダと結び付ける、すべての入力トランザクション(Tx1およびTx2)のためのマークルパス、

完全な(すなわち、埋められたテンプレート)支払トランザクション(Tx3)。テンプレートを埋めることに加えて、Aliceは自分の署名も提供する。

【００８２】

[3]SPV確認(ローカル): Bob

・Bobが、

トランザクションTx1およびTx2、

対応するマークルパスPath 1およびPath 2、
Bobのブロックヘッダのローカルリスト
を使用して、入力トランザクションTx1およびTx2に対してSPV確認を実行する。
・これらの確認は、Bobによってローカルに実行され、P2Pネットワークを介さない。
・好ましい実施形態では、この段階において、Bobは、
支払Tx3がBobの予想通りであること、
Aliceの署名がこのトランザクションに対して有効であること
を確実にするために、Aliceから受信した支払Tx3に対して適切な確認も実行する。

【００８３】

[4]メッセージ: BobからP2Pネットワークへ
・Bobが支払トランザクション(Tx3)をP2Pネットワークへブロードキャストする。既存のパラダイムでは、Aliceがトランザクションをネットワークに出す。
・これは、Tx3へのすべての入力に対するSPV確認[3]が肯定的である場合にのみ行われる。

【００８４】

[5]SPV確認(メッセージ): BobからP2Pネットワークへ
・このステップは、SPV方法の既存のパラダイム(より前を参照)におけるステップ[3]と同一である。

【００８５】

この通信フローが図10に示されている。[4]および[5]のみがP2Pネットワークによって仲介されることに留意されたい。ステップ[5]は、既存のSPV技法の反復にすぎず、提案される方法の必要な特徴ではない。これは、完全にするために、かつ既存のパラダイムと本発明の区別のためにここに含まれている。

【００８６】

本開示の実施形態によれば、必要なSPV確認[3]が、
・支払トランザクション(Tx3)が出される前に、
・支払トランザクション(Tx3)への入力トランザクション(Tx1およびTx2)に際して、
・(Aliceにより提供される)マークルパスを提供するためのネットワークピアの助けなしで、
実行されることに留意されたい。

【００８７】

本発明の実施形態の特徴は、限定はされないが、次のことを含む。
・Aliceがオンラインである必要はなく、または、自分ではどのような情報もネットワークに出す必要もない。これはAliceにとってより信頼性がある。これは、ネットワークに接続する能力のないスマートカードなどのデバイスを、Aliceが使用することも可能にする。
・マークルパスを含むことで、BobがAliceからのあらゆる無効な入力をすぐに拒絶することが可能になる。これは、無効なマークルパスを伴う「スパム」トランザクションの提出を拒絶することによって、過剰なネットワークトラフィックを軽減する。
・Bobがネットワークへの特に高速な接続を有することがあるので、Bobがトランザクションを妥当性確認するのがより速くなることがある。
・Bobが、Aliceが署名するためのトランザクションを作成するので、トランザクションの内容に対するより大きな管理権を有し、たとえば、Bobは、トランザクションがネットワークにより受け入れられることを確実にするトランザクションフィーにおいてより多く支払うことを選ぶことがある。
・Bobのウォレットは、どのような秘密鍵も含む必要がない。これは、認証されていない第三者が秘密鍵にアクセスできないので、または秘密鍵を危険にさらすことができないので、セキュリティを高める。

・トランザクションをネットワークに提出する責任はBobにある。
・AliceのSPVウォレットは、秘密鍵とトランザクションに署名するための能力とを有しなければならない。したがって、それは、楕円曲線点乗算を実行するのに十分な能力を有するはずである。

【００８８】

ここで、本開示による構成の様々な構成要素を詳しく考える。

【００８９】

オフラインSPVウォレット

オフラインSPVのある実施形態が図1に概略的に示されており、以下の特徴を備える。

1. TX - Aliceの利用可能な未使用トランザクション出力を含む、プリロードされた完全なトランザクションデータ。この完全なトランザクションデータは、マークルパスと組み合わせて、Aliceが費やしているトランザクションが有効であることのマークル証明を構成する。完全なトランザクションをハッシュすることはトランザクションID(TXID)を与え、これは、Aliceが完了することを望む新しいトランザクションのための入力データの一部として必要とされる。Bobは、TXIDが実際にトランザクションのハッシュであることを検証することが可能でなければならないので、TXIDだけを提供することは不十分であることに留意されたい。これは、Aliceが完全なトランザクションデータをBobに提供する場合にのみ可能であるので、Aliceはそれを保管しなければならず、または必要とされるときにそれへのアクセス権を少なくとも有しなければならない。

2. 秘密/公開鍵 - ウォレットは、トランザクション出力を署名するために秘密鍵の集合へのアクセス権を有しなければならず、トランザクションを行うときに変更アドレスを指定するために公開鍵へのアクセス権を有しなければならない。

3. マークル経路 - トランザクション出力(UTXO)を含むトランザクションの各々の(完成した)マークルパス。これは、TXが有効であることを検証するために、業者の販売時点ウォレットによって使用される。このウォレットによって提供されるマークル証明は、二重消費を防がないが、スパム攻撃に対するフェイルファスト機構として動作するので、ウォレットの堅牢性とセキュリティを高めることに留意されたい。

4. 最小限の処理 - オフラインSPVウォレットは、未使用トランザクションを費やすためにそれに署名することが必要とされる。これは、オフラインウォレット(およびそれがインストールされるデバイス)が、ECDSAなどの暗号アルゴリズムを実施することが可能であることを必要とし、楕円曲線点乗算を実行してハッシュ関数を計算することが可能であるように十分な処理能力が必要とされることを意味する。

5. ブロックヘッダ(任意選択) - オフラインSPVウォレットは、販売時点SPVウォレットへの支払が処理されたことを検証するためにブロックヘッダを含めることを望むことがある。これは、販売時点ウォレットとの対話の後でTXIDおよびマークルパスを記憶することも必要とする。

【００９０】

1つまたは複数の実施形態では、上記は、オンラインとオフラインの両方の状態または機構を伴うウォレットとして実施されてもよい。これは、ウォレットがUTXOおよびマークルパスの集合を更新する必要があるとき、有利であり得る。

【００９１】

そのような実施形態では、Aliceのウォレットは、従来のSPVウォレットと同じ方法で、一時的にネットワークに接続することによってデータをダウンロードすることができる。これは、図2に示されており、オンおよびオフラインSPVウォレットと便宜的に呼ばれることがある。

【００９２】

接続されると、Aliceのウォレットは、完全なトランザクション、マークルパス、およびブロックヘッダをダウンロードすることができる。1つの入力および2つの出力を伴う、当技術分野において知られているような標準的なP2PKHトランザクションは226バイトであり、ブロックヘッダは80バイトであり、100000個のトランザクションを含むブロックの

中のトランザクションのためのマークルパスは約560バイトである。3つすべてを組み合わせることは、AliceのSPVウォレットの更新には新しい入力当たり1MB未満のデータしかダウンロードする必要がないことを意味する。これは、低帯域幅の接続でも達成することができ、これは高度に有利である。

【００９３】

この実施態様を使用するウォレットは、必要なときにネットワークに接続する能力を維持しながら、ブロックチェーンを使用したオフライン支払および検証を促進することが可能であるという利点をもたらすので、有利である。ブロックヘッダのリストを更新し、新しいTXおよび関連するマークルパスを取得し、さらに必要とされるときにトランザクションを送信するための、追加のオンライン状態が使用され得る。

【００９４】

ソフトウェアアプリケーションおよびコンタクトレス支払カードを含む、オンラインおよびオフラインSPVのための、複数の使用事例がある。

【００９５】

PoS SPVウォレット

PoS SPVウォレットは、上で説明されたようなオフラインSPVウォレットを使用している、Aliceからの移転を受け入れるためにBobに対して必要とされる最小限の機能を達成するように設計される。これらの要件は、Bobが、

・販売時点トランザクションテンプレートを生成することが可能でなければならない

・ブロックヘッダと関連付けられるマークル証明を計算することが可能でなければならない

・UTXO集合のクエリを含めて、ネットワークに接続してブロードキャストすることが可能でなければならない

・支払を受け取るための公開鍵アドレスを管理することが可能でなければならない

・AliceのUTXOを含む完全なTXデータのリストを更新することが可能でなければならない

というものである。

【００９６】

すべての上の要件は、図3に示される概略的な設計に従ったPoS SPVウォレットによって満たされ、以下の特徴を備える。

1．ブロックヘッダ - PoS SPVウォレットが、ブロックチェーンの中のブロックに対応するブロックヘッダデータのリストの最新のコピーを維持する。トランザクションおよびそのマークルパスを提示されると、PoS SPVウォレットは、マークルルートへの繰り返されるハッシュによって単純なマークル証明を実行することができる。

このルートを関連するブロックヘッダの中のルートと比較することによって、Bobは、誤りのあるまたは不正な支払を検出するための効率的なフェイルファスト機構を有する。

2．ネットワーク接続性 - PoS SPVウォレットは、ネットワークに接続する能力を有する。これは、限定はされないが、新しい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にブロードキャストし、現在のUTXO集合における特定のUTXOの存在について問い合わせる能力を含む。

3．公開鍵の記憶 - PoS SPVウォレットは、Bobがそこからの資産または支払の受け取りを望む公開鍵アドレスを記憶することのみが必要である。これは、たとえば、決定論的な秘密(国際公開第2017/0145016号において開示されるものなど)を使用すること、または階層的な決定論的ウォレット構造を使用することなどによって、いくつかの方法で行われ得る。

販売時点において、関連する秘密鍵ではなく公開鍵アドレスのみを記憶することによって、Bobの秘密鍵が危険にさらされず、したがって基金が保護されるので、「カー

ド存在」トランザクションのためのセキュリティは大きく改善される。

4. 最小限の処理 - PoS SPVウォレットは、Aliceによって埋められるテンプレートに基づいて、マークル証明の最小限の処理だけを実行することが必要とされる。

これは、マークルパスを独立に取得するためにフルブロックを繰り返し処理することの負担を大きく減らし、これは、販売時点/トランザクションプロセスを促進し、ネットワークにわたるリソースの移転を促進し、BobとAliceの両方の効率を改善する。

【００９７】

少なくとも1つの実施形態では、販売時点SPVウォレットは、Bobが常にブロックチェーンの履歴における任意のトランザクションのためのマークルパスについてSPV確認を実行できることを保証するために、ブロックヘッダのリスト全体のコピーを維持することに留意されたい。しかしながら、Bobが、ブロックヘッダの完全なリストを維持しないこと、たとえば消費可能な出力を伴うトランザクションを含まないブロックに対応するものを維持することを選ぶことがあってもよい。この場合、Bobは、まだ持っていないブロックヘッダを取得するために、第三者に時々問い合わせなければならないことがあることを理解されたい。次のセクションでは、Bobが1つまたは複数の実施形態に従ってAliceに送信する業者販売時点テンプレートを詳述し、Bobがすべてのブロックヘッダの完成したリストを有しない場合、Bobはこのテンプレートへの自分の未使用トランザクション出力と関連付けられるブロックヘッダに対する要求を組み込み得ることを理解されたい。

【００９８】

PoS SPVウォレットテンプレート

図4を見ると、BobのPoS SPVウォレットが、以下のフォーマットでAliceのオフライン(またはオフ/オンライン)ウォレットの情報を要求する。

1. TX/UTX - Aliceの消費可能なトランザクションからの完全なトランザクションデータ(上で説明されたような)。

2. トランザクションテンプレート - Bobの出力アドレスとAliceから要求されている暗号通貨の量とを(少なくとも)備える、部分的に完成したブロックチェーントランザクション。トランザクションが完了するには、Aliceのオフラインウォレットは、自分の未使用トランザクション出力からのTXID、使用されるべき消費可能TX出力の各々のための有効な署名、および変更アドレスを(少なくとも)提供しなければならない。

3. マークルパス - 完全な完成したトランザクションと組み合わされると、AliceのTXがブロックに含まれ、したがって有効であることを検証するために、マークル証明が構築され得る。

【００９９】

最も簡単な場合では、Aliceは、P-o-Sにおいて商品と引き換えに有効な支払トランザクションTx3をBobに提供する必要があることに留意されたい。本発明の少なくとも1つの実施形態によれば、Bobは、これを促進するために業者テンプレートを提供するが、テンプレートが使用されないことも想起可能である。たとえば、Aliceが価格およびBobのアドレスを事前にすでに知っている場合、Aliceは自分の支払を構築してそれを直接Bobに送信することができる。Aliceはまた、必要とされる署名および出力点参照を、テンプレート自体を明示的に「埋める」ことなく提供し得る。

【０１００】

完全なトランザクション(図4の(1)参照)およびマークル証明(図4の(3)参照)は、Aliceによって送信され、Bobによって処理され得る。これは、AliceがBobのテンプレートを完成させる(図4の(2)参照)ことと並列に、かつ独立に行われ得る。

【０１０１】

遅延されたトランザクション提出

オンライン販売業者などのためのいくつかの場合には、支払トランザクションを一定の間隔でバッチとして提出することが有利であることがある。これは、改善された/最適なネットワーク接続が利用可能になることなどを待機するなどの技術的な理由で、会計上の目的で、または生じるトランザクションフィーの総額を減らすために、有利であることがあ

る。

【０１０２】

業者Bobに対して、これは追加の課題をもたらさないが、顧客Aliceに対して、これは、Bobが最終的に署名されたトランザクションをネットワークに提出するまで、Aliceの変更アドレスと関連付けられる暗号通貨をAliceが使用することが可能ではないことを意味する。

【０１０３】

この問題に対する解決策は、BobがAliceに提供するテンプレート内のトランザクションを処理する際の人工的な遅延をBobが指定することである。Aliceのオフラインウォレットは、このことを、Bobへの支払により生成される変更が、バッチにされたトランザクションをネットワークに提出する前の業者の所定の時間の間は費やすことが不可能であることを意味するものとして、解釈することができる。このシナリオでは、Bobには追加のリスクはなく、それは、業者がトランザクションのバッチを提出する前に二重消費の証拠を見つけた場合には、購入された商品の配達を取り消すことができるからであることに留意されたい。

【０１０４】

PoS SPVウォレットへの拡張 - 分割ウォレット

上で説明されたPoS SPVウォレットへの拡張として、Bobが、異なる機能を伴ういくつかの接続されたウォレットを利用するのが望ましいことがあり、これは単一の分割ウォレットシステムとして扱われ得る。

【０１０５】

したがって、本発明のいくつかの実施形態は、1つまたは多数の販売時点ウォレットを協調させることができるより高度なマスターSPVを導入することによって、販売時点(P-o-S)SPVの基本的な概念を基にする。1つまたは複数のP-o-S SPVとのマスターSPVの組合せは、本明細書では「分割ウォレット」システムであると考えられる。

【０１０６】

本発明の実施形態による分割ウォレットシステムは、マスターSPV構成要素によって協調させられる、支払端末として動作する少なくとも1つのPoS SPVウォレットを備える。マスターSPVの機能は、ウォレットが、

・P-o-S SPVの公開鍵アドレスと関連付けられる秘密鍵を記憶することを可能にする。

・ブロックヘッダと関連付けられるマークル証明を計算することを可能にする。

・UTXO集合のクエリを含めて、ブロックチェーンネットワークに接続してブロードキャストすることを可能にする。

・支払端末として機能する少なくとも1つのPoS SPVウォレットと通信することを可能にする。

【０１０７】

すべての簡単な支払検証システムのように、マスターウォレットは、所与のトランザクションのためのマークル存在証明を確認することなどの、良いSPVのすべての基本的な機能を実行することが可能であるべきである。これは、販売時点からBobがブロードキャストするあらゆるトランザクションがネットワークにより受け入れられてブロックに含まれていることを、Bobが確認できることを意味する。しかしながら、重要なことに、本発明の実施形態によるマスターウォレットは、少なくとも1つのより簡単なPos SPVウォレットと通信し、それにより処理される支払を協調させる。

【０１０８】

マスターSPVが、Bobの支払アドレスのための秘密鍵を記憶することが有利であり得る。これは、Bobが、分割ウォレットシステムを使用するときに、自分の支払処理についてより高いセキュリティを有することを可能にする。しかしながら、Bobの秘密鍵を記憶することはマスターウォレットの任意選択の能力であり、その主要な機能は、複数の販売時

点ウォレットからの支払を統合して協調させることである。

【０１０９】

基本的なマスターSPVのみを使用する、業者分割ウォレットのこの実施態様では、業者-顧客の対話は厳密に修正されない。PoS SPVウォレットは依然として、マークルパスについて同じ確認を実行し、UTXO集合について同じクエリをネットワークに行わなければならない。プロセスの違いには、以下のことがある。

・AliceとBobによって使用されるべきP-o-S SPV端末の選択。

・マスターSPVがバックグラウンドでブロックチェーンと継続的に同期すべきである。

・Bobの支払アドレスと関連付けられる秘密鍵がマスターウォレットから専用の管理を受ける。これは、販売時点ウォレットにおいて公開鍵アドレスを記憶することだけによって以前にもたらされたセキュリティに、構造を追加する。

【０１１０】

分割ウォレットの実施態様の一部として使用されるマスターウォレットは通常、セキュリティ上の問題と実用上の問題の両方で、会社のバックオフィスまたはヘッドオフィスなどの、販売時点SPVに対して別々の位置に存在することに留意されたい。業者-顧客の対話は、図5に示されるように視覚化され得る。

【０１１１】

論じられたように、業者分割ウォレットの一部として簡単なマスターSPVを使用するこの実施態様は、Bobに対する有用性を有するが、それでも、分割ウォレットが適切なレベルの二重消費保護を提供すべきである場合、UTXO集合のクエリに応答するためにネットワークに依存する。

【０１１２】

これは、マスターSPVがmempoolの固有のコピーも保持するより強力なタイプのマスターウォレットにより置き換えられるような、1つまたは複数の実施形態に従って対処されてもよい。そのようなマスターウォレットを装備する分割ウォレットアーキテクチャは、顧客のUTXOが現在のUTXO集合の一部ではないかどうかを確認するために、ネットワークに問い合わせる必要はない。

【０１１３】

mempoolの固有のコピーを有するマスターウォレットは、従来の非マイニング「フルノード」クライアントと同様に機能するが、有利なことに、ブロックチェーンの完全なコピーを保持する必要がない。代わりに、このタイプのマスターウォレットは、ブロックヘッダおよびmempoolの固有のローカルコピーのみを保持する。mempoolのコピーは、ネットワークと同期することによってローカルに構築されるか、または、信用される第三者もしくはサービスから得られるかのいずれかであり得る。

【０１１４】

mempoolの固有のコピーを有するマスターSPVウォレットを使用した分割ウォレットの実施態様は、業者の観点から業者-顧客の対話を変える。

図5に関連して上で説明されたものからの、対話の主な変化が、ステップ4および5において明らかにされる。

・ステップ4において、業者は、UTXO集合のさらなるクエリを追加するのではなく、トランザクションをネットワークにブロードキャストするだけである。

・ステップ5において、業者は今や、競合するトランザクションのためのmempoolを確認することによって、顧客のトランザクションの有効性について固有の確認を実行する。業者は次いで、mempoolの同期されたコピーの状態に基づいて、どのような行動をとるかを決定することができる。

【０１１５】

用いられる発明の例示

AliceがBobから何かを買うことを望むような、典型的な業者-顧客の対話を考える。本発明のある実施形態によれば、プロセスは、以下で概説されるように、かつ図6を参照し

て実行される。

1. Bobが、部分的に完成したブロックチェーントランザクションを作成し、Aliceから以下の情報を要求する。これは、Aliceが埋めるためのテンプレートとして一緒にパッケージングされ得る。

a. 購入を完了するためにAliceが費やすTX出力

b. Aliceのための(ビットコイン)変更アドレス

c. Aliceからの署名

d. TXのためのマークルパス(これはトランザクションの一部を形成しない)

2. Aliceが必要とされる情報を提供することによってテンプレートを完成させる。

3. Bobが、Aliceが提供したTXの有効性を確認するために、マークル証明を実行する。証明が有効ではない場合、Bobは、AliceのTXがブロックチェーンにおいて有効であったことがないことを知り、トランザクションを拒絶する。有利なことに、これはフェイルファスト機構である。

4. Bobが、完成したトランザクションをネットワークにブロードキャストし、UTXO集合を問い合わせる。

a. ブロードキャストは、マイナーがトランザクションをブロックへとマイニングする試みを開始することを可能にする。

b. クエリは、Aliceによって提供される表面上は有効なUTXOがまだUTXO集合の中にあるかどうかを尋ねる。

これは、Aliceによる二重消費の防止のための機構である。

5. ネットワークがBobのUTXOクエリに応答する。これは、Bobが以下の行動指針のうちの1つを採用することを可能にする。

a. AliceのUTXOがまだUTXO集合の一部である場合、Bobは、二重消費のリスクを最小限にしながら支払を受け入れることができる。

i. Bobがとるリスクは、何らかの時間間隔τの間、このクエリでネットワークノードにポーリングを続けることによって、最小限にされ得る。

ii. 何らかの信頼区間内で、信用できる大半のノードにBobが問い合わせることを確実にするために、ベイズ分析が利用され得る。

b. AliceのUTXOがUTXO集合の一部ではない場合、BobはAliceの支払を拒絶する。

【０１１６】

上で言及されたように、本発明の実施形態は、様々な形式での使用および実施に役立つ。これらは、たとえば支払カードを含み得る。

【０１１７】

当技術分野において知られているように、従来のSPVウォレットは、ブロックチェーン内の深度を確認することによって、トランザクションが二重消費ではないことを検証し、この深度の確認は、ネットワークに問い合わせることにより行う。トランザクションがマイナーによって妥当性確認され、ブロックに含まれると、トランザクションは1回の確証を有する。ブロックチェーンに追加されるあらゆる追加のブロックが、確証を1だけ増やし、各々の新しい確認のたびに、二重消費のリスクは低下する。従来のSPVウォレットは、6回の確証を有するまで、「未確証」としてトランザクションを表示する。

【０１１８】

しかしながら、デフォルトの6回確証の規則はビットコインにとって重要ではない。すべての業者が、支払について満足するまでに6つのブロック(または1つのブロックすら)が生成されるのを待つことを望むとは限らない。"0-conf"は、ブロックにまだ含まれていないトランザクションを表記するために、本技術分野において使用される用語である。Aliceが自分のトランザクションを完成させると、Aliceは、それをネットワークにブロードキャストし、Bobは(少なくとも)mempoolの中でそれを見つけることが可能であるはずである。

【０１１９】
本発明は、トランザクションをブロードキャストすることの負担を、送信者のAliceではなく受信者のBobに移し、それにより、必要とされるCPUを最小限にし、Aliceの体験を改善する。Bobは、ネットワークへのAliceの接続に依存する必要がないので、トランザクションプロセスに対するより高度な管理権を有するが、Aliceのセキュリティを危険にさらすほどの管理権を持たない。基本的に、Alice(だけ)が、デジタル署名を提供することによって、トランザクションを受け入れ、または拒絶する権限を有する。
【０１２０】
マークルパスは二重消費を防がず、それは、ネットワークによって中継されているトランザクションがmempoolの中にあることをBobが理解できるときにのみ0-confに達するからである。代わりに、それは、Bobが存在しないUTXOを消費するための試みを直ちに拒絶することを可能にする、フェイルファスト機構として機能する。これは、特に、ブロードキャストしてフルノードに問い合わせるのにかかる時間は接続が悪い場合には数秒以上であることがあり、スパム攻撃の仲介者としてBobが使用されるのを防ぐので、有用である。
【０１２１】
オフライン支払が有効であると、プリペイドスマートカードなどのハードウェアが、ビットコインエコシステムに統合され得る。支払カードは、秘密鍵ならびにUTXO、完成したトランザクション、およびマークルパスを記憶するための、データ容量を必要とする。それは、ECDSA署名アルゴリズムを実施するために、何らかの処理能力も必要とする。Table 1(表2)は、登録のときに利用可能ないくつかの電子カードタイプのリストを示す。
【０１２２】
【表２】

	最大データ容量	処理能力	カードのコスト(米ドル)	リーダ/接続のコスト
磁気ストライプカード	140 バイト	なし	$0.20-$0.75	$750
集積回路メモリカード	1 kB	なし	$1-$2.50	$500
集積回路プロセッサカード	8 kB	8 ビット CPU (23 ビットまでの将来的な拡張)	$7-$15	$500

Table 1:典型的な支払カードの仕様

【０１２３】
二重消費保護
顧客Aliceが、店で物理的な商品と暗号通貨を交換することを望んでいると仮定する。従来、Aliceは、販売時点(POS)でトランザクションをブロックチェーンネットワークに送信し、業者Bobは、このトランザクションが
(a) ネットワークにより受け入れられるものとしてBobに返ってくること、または、

(b) ブロックにおいて(またはn-confの場合はn個のブロックまで)確証されることのいずれかを確認したときにのみ、Aliceが商品を持ち去るのを許容する。

【０１２４】

シナリオ(a)では、Bobは、BobへのAliceの支払トランザクションが有効であることを知っており、マイナーはこの支払をブロックへとマイニングすることを試みるであろう。これは、Aliceが遠隔から競合するトランザクションを出すことにより開始される単純な二重消費からBobを保護しないが、このシナリオは、従来のブロックヘッダベースのSPVと調和する。

【０１２５】

シナリオ(b)では、Bobは、支払トランザクションが有効であり、かつ二重消費されていないことを知っている。しかしながら、これは、Bobがフルノードを運営して次のブロックをその場でダウンロードすることを必要とする。また、ビットコインネットワークでは、これは、Aliceが商品とともに施設を去ってもよくなるまで、平均で10分かかる。

【０１２６】

この問題の陳述において、軽減しようとしている攻撃はAliceによる単純な二重消費であるので、Bobにとっては0-confセキュリティで十分であると仮定していることに留意されたい。1つまたは複数のブロックが、第3の敵対者であるCarolの異なる攻撃ベクトルを軽減すべきであると要求することは、ネットワーク全体を圧倒させる。

【０１２７】

以下の表は、シナリオ(a)と(b)のいずれもが独立に、そのような顧客-業者の対話にとってどのように許容可能ではないかを示す。この表は、シナリオa)およびb)のトランザクションの特徴を示す。

【０１２８】

【表３】

要因	シナリオ(a)	シナリオ(b)
Bob に対する二重消費保護	許容不可	許容可
10 秒未満の平均トランザクション時間	許容可	許容不可
10 分未満の平均トランザクション時間	許容可	許容不可
SPV 互換* (Bob)	許容可	許容不可
SPV 互換* (Alice)	許容可	許容可

【０１２９】

*は、この関係者に対してフルノードの要件がないことを意味する。これらの基準のすべてを満たす解決策のみが、大半のトランザクションに対してBob(業者)とAlice(顧客)の両方にとって許容可能である。

【０１３０】

本明細書において開示される業者PoSウォレットの実施形態は、以下の利点を提供する。

・業者に対する二重消費保護
・瞬時の(〈〈10秒)平均トランザクション時間
・顧客と業者の両方が販売時点でSPVウォレットを使用できる

【０１３１】

【表４】

要因	シナリオ(a)	シナリオ(b)	業者 SPV
Bob に対する二重消費保護	No	Yes	Yes
10 秒未満の平均トランザクション時間	Yes	No	Yes
10 分未満の平均トランザクション時間	Yes	No	Yes
SPV 互換* (Bob)	Yes	No	Yes
SPV 互換* (Alice)	Yes	Yes	Yes

【０１３２】
本発明の実施形態は、既存のSPV/暗号通貨トランザクションのレートをはるかに上回る性能と結果を提供し、少なくとも、瞬時性に関して既存のチップアンドピン/コンタクトレス端末支払操作に匹敵することが可能であると予想される。
【０１３３】
その上、本発明は、約1時間(すなわち、6-conf)以内で高い確実度で支払が清算され承認されることも可能にする。これは、最大60日、すなわちVISAおよびMastercardの清算時間という、現在の支払清算時間よりはるかに優れている。
【０１３４】
可変のリスク
業者として、Bobは、販売時点において支払を受け入れるためのレイテンシを調整することができる。最短のポーリング間隔τを選ぶことによって、Bobは、許容可能な二重消費のリスクについての問題となる上限を設定する。このことは、業者の支払処理において、より高い効率性とフレキシビリティを可能にできる。
【０１３５】
加えて、Bobは、テンプレートを生成するとき、トランザクションのためのマイニングフィーを設定することができる。このフィーを誰が払うかは必ずしも問題ではないが、業者により許容可能であると見なされるレベルに二重消費のリスクを設定するためのパラメータとして、その値が使用され得る。
【０１３６】
全体として、販売時点の時間遅延およびトランザクションのためのマイニングフィーは、業者によって設定され得る、かつ、顧客のデジタル署名により同意され得る、2つのパラメータであり、これらは、ケースバイケースで効率性とリスクを実質的に調整できる。これは、たとえば、交換されることになる商品の価値に依存してもよい。
【０１３７】
ここで図7を見ると、本開示の少なくとも1つの実施形態を実践するために使用されてもよいコンピューティングデバイス2600の説明のための簡略化されたブロック図が提供されている。様々な実施形態において、コンピューティングデバイス2600は、上で示され説明されたシステムのいずれかを実施するために使用されてもよい。たとえば、コンピューティングデバイス2600は、データサーバ、ウェブサーバ、ポータブルコンピューティングデバイス、パーソナルコンピュータ、または任意の電子コンピューティングデバイスとして使用するために構成されてもよい。図7に示されるように、コンピューティングデバイス2600は、メインメモリ2608および永続ストレージ2610を含むストレージサブシステム2606と通信するように構成され得る、1つまたは複数のレベルのキャッシュメモリおよびメモリコントローラ(まとめて2602と表記される)を伴う1つまたは複数のプロセッサを含んでもよい。示されるように、メインメモリ2608は、ダイナミックランダムアク

セスメモリ(DRAM)2618と読取り専用メモリ(ROM)2620とを含み得る。ストレージサブシステム2606およびキャッシュメモリ2602は、本開示において説明されたようなトランザクションおよびブロックと関連付けられる詳細などの、情報の記憶のために使用されてもよい。プロセッサ2602は、本開示において説明されたような任意の実施形態のステップまたは機能を提供するために利用されてもよい。

【０１３８】

プロセッサ2602はまた、1つまたは複数のユーザインターフェース入力デバイス2612、1つまたは複数のユーザインターフェース出力デバイス2614、およびネットワークインターフェースサブシステム2616と通信することができる。

【０１３９】

バスサブシステム2604は、コンピューティングデバイス2600の様々なコンポーネントおよびサブシステムが意図されるように互いに通信することを可能にするための機構を提供してもよい。バスサブシステム2604は単一のバスとして概略的に示されているが、バスサブシステムの代替の実施形態は複数のバスを利用してもよい。

【０１４０】

ネットワークインターフェースサブシステム2616は、他のコンピューティングデバイスおよびネットワークへのインターフェースを提供してもよい。ネットワークインターフェースサブシステム2616は、他のシステムからデータを受信し、コンピューティングデバイス2600から他のシステムにデータを送信するためのインターフェースとして働いてもよい。たとえば、ネットワークインターフェースサブシステム2616は、データ技術者がデバイスをネットワークに接続することを可能にすることがあるので、データ技術者がデータセンターなどの離れた位置にいる間にデータをデバイスに送信してデバイスからデータを受信することが可能であることがある。

【０１４１】

ユーザインターフェース入力デバイス2612は、キーボード、統合されたマウス、トラックボール、タッチパッド、またはグラフィクスタブレットなどのポインティングデバイス、スキャナ、バーコードスキャナ、ディスプレイに組み込まれたタッチスクリーン、音声認識システム、マイクロフォンなどのオーディオ入力デバイス、および他のタイプの入力デバイスなどの、1つまたは複数のユーザ入力デバイスを含んでもよい。一般に、「入力デバイス」という用語の使用は、コンピューティングデバイス2600に情報を入力するためのすべての可能なタイプのデバイスおよび機構を含むことが意図されている。

【０１４２】

1つまたは複数のユーザインターフェース出力デバイス2614は、ディスプレイサブシステム、プリンタ、またはオーディオ出力デバイスなどの非視覚的ディスプレイなどを含んでもよい。ディスプレイサブシステムは、陰極線管(CRT)、液晶ディスプレイ(LCD)などのフラットパネルデバイス、発光ダイオード(LED)ディスプレイ、またはプロジェクションデバイスもしくは他のディスプレイデバイスであってもよい。一般に、「出力デバイス」という用語の使用は、コンピューティングデバイス2600から情報を出力するためのすべての可能なタイプのデバイスおよび機構を含むことが意図されている。1つまたは複数のユーザインターフェース出力デバイス2614は、たとえば、説明されるプロセスおよびその変形を実行するアプリケーションとのユーザの対話を、そのような対話が適切である可能性があるときに促進するための、ユーザインターフェースを提示するために使用されてもよい。

【０１４３】

ストレージサブシステム2606は、本開示の少なくとも1つの実施形態の機能を提供してもよい基本的なプログラミングおよびデータ構造物を記憶するための、コンピュータ可読記憶媒体を提供してもよい。アプリケーション(プログラム、コードモジュール、命令)は、1つまたは複数のプロセッサによって実行されると、本開示の1つまたは複数の実施形態の機能を提供してもよく、ストレージサブシステム2606に記憶されてもよい。これらのアプリケーションモジュールまたは命令は、1つまたは複数のプロセッサ2602によって実

行されてもよい。ストレージサブシステム2606は追加で、本開示に従って使用されるデータを記憶するためのリポジトリを提供してもよい。たとえば、メインメモリ2608およびキャッシュメモリ2602は、プログラムおよびデータのための揮発性ストレージを提供することができる。永続ストレージ2610は、プログラムおよびデータのための永続(不揮発性)ストレージを提供することができ、フラッシュメモリ、1つまたは複数のソリッドステートドライブ、1つまたは複数の磁気ハードディスクドライブ、関連するリムーバブルメディアを伴う1つまたは複数のフロッピーディスクドライブ、関連するリムーバブルメディアを伴う1つまたは複数の光学ドライブ(たとえば、CD-ROMまたはDVDまたはBlue-Rayドライブ)、および他の同様のストレージメディアを含んでもよい。そのようなプログラムおよびデータは、本開示において説明されるような1つまたは複数の実施形態のステップを行うためのプログラム、ならびに、本開示において説明されるようなトランザクションおよびブロックと関連付けられるデータを含み得る。

【０１４４】

コンピューティングデバイス2600は、ポータブルコンピュータデバイス、タブレットコンピュータ、ワークステーション、または以下で説明される任意の他のデバイスを含む、様々なタイプであってもよい。加えて、コンピューティングデバイス2600は、1つまたは複数のポート(たとえば、USB、ヘッドフォンジャック、Lightningコネクタなど)を通じてコンピューティングデバイス2600に接続されてもよい別のデバイスを含んでもよい。コンピューティングデバイス2600に接続されてもよいデバイスは、光ファイバコネクタを受け入れるように構成される複数のポートを含んでもよい。したがって、このデバイスは、処理のためにデバイスをコンピューティングデバイス2600に接続するポートを通じて送信されてもよい電気信号へと、光信号を変換するように構成されてもよい。コンピュータとネットワークの変化し続ける性質により、図7に図示されるコンピューティングデバイス2600の説明は、デバイスの好ましい実施形態を例示するための具体的な例として意図されているにすぎない。図7に図示されるシステムより多数または少数の構成要素を有する多くの他の構成が可能である。

【０１４５】

「ブロックチェーントランザクション」という用語は、ブロックチェーンネットワークを介したデジタルリソースまたは資産の管理権の移転を達成するために暗号鍵の使用を実施するデータ構造を指すために使用されてもよい。上述のように、トランザクションがブロックチェーンに書き込まれるには、トランザクションは、i)トランザクションを受信する第1のノードによって妥当性確認されなければならず、トランザクションが妥当性確認される場合、ノードはそれをネットワークの中の他のノードに中継し、ii)マイナーによって構築された新しいブロックに追加されなければならず、iii)マイニング、すなわち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。マイナーによって実行される作業の性質は、ブロックチェーンを維持するために使用される合意機構のタイプに依存することが理解されるだろう。Proof of work(PoW)が元のビットコインプロトコルと関連付けられるが、proof of stake (PoS)、delegated proof of stake (DPoS)、proof of capacity (PoC)、proof of elapsed time (PoET)、proof of authority (PoA)などの他のコンセンサス機構が使用されてもよいことが理解されるだろう。異なるコンセンサス機構は、マイニングがノード間でどのように分布するかという点で異なり、ブロックのマイニングに成功する確率は、たとえば、マイナーのハッシュパワー(PoW)、マイナーにより保持される暗号通貨の量(PoS)、代表マイナーに供与される暗号通貨の量(DPoS)、暗号パズルに対する所定の解法を記憶するマイナーの能力(PoC)、マイナーにランダムに割り当てられる待機時間(PoET)などに依存する。

【０１４６】

通常、マイナーは、ブロックをマイニングするための動機付けまたは報酬を与えられる。たとえば、ビットコインブロックチェーンは、新しく発行される暗号通貨(ビットコイン)およびブロックにおけるトランザクションと関連付けられる手数料(トランザクションフィー)をマイナーに報酬として与える。ビットコインブロックチェーンでは、発行される暗

号通貨の量は時間とともに減少し、最終的には動機付けはトランザクションフィーだけになる。したがって、トランザクションフィーの取り扱いは、ビットコインブロックチェーンなどの公開ブロックチェーンにデータをコミットするための基礎となる機構の一部であることが理解されるだろう。

【０１４７】

前に言及されたように、所与のブロックの中の各トランザクションは、ブロックチェーンシステムの参加者間でのデジタル資産の管理権の移行を符号化する。デジタル資産は、必ずしも暗号通貨に相当しなくてもよい。たとえば、デジタル資産は、文書、画像、物理的な物体などのデジタル表現などに関係してもよい。マイナーへの暗号通貨および/またはトランザクションフィーの支払は単に、必要な作業を実行することによってブロックチェーンの中のブロックの有効性を維持するための動機付けとして働いてもよい。ブロックチェーンと関連付けられる暗号通貨がマイナーのためのセキュリティとして働き、ブロックチェーン自体は暗号通貨以外のデジタル資産に主に関連するトランザクションのための台帳であるということがあってもよい。いくつかの場合、参加者間での暗号通貨の移転は、トランザクションの台帳を維持するためにブロックチェーンを使用するエンティティとは異なるエンティティによって扱われるということがあってもよい。

【０１４８】

上で言及された実施形態は本発明を限定するのではなく例示すること、および、添付の特許請求の範囲により定義されるような本発明の範囲から逸脱することなく、当業者が多くの代替的な実施形態を設計することが可能であることに、留意されたい。請求項において、括弧の中に置かれたあらゆる参照符号は、請求項を限定するものとして解釈されるべきではない。「備える(comprising)」および「備える(comprises)」などの語は、任意の請求項または明細書に列挙されるもの以外の要素またはステップの存在を全体として排除するものではない。本明細書では、「備える(comprises)」は「含む(includes)またはからなる(consists of)」を意味し、「備える(comprising)」は「含む(including)またはからなる(consisting of)」を意味する。「動作可能である」または「ように動作可能である」は、「なされる/ようになされる」および「構成される/ように構成される」を含む。単数形での要素への言及は、そのような要素の複数形での言及を排除せず、その逆も当てはまる。本発明は、いくつかの別個の要素を備えるハードウェアによって、および適切にプログラムされたコンピュータによって実施されてもよい。いくつかの手段を列挙するデバイスの請求項において、これらの手段のいくつかは、ハードウェアの1つの同じ項目によって具現化されてもよい。ある対策が相互に異なる従属請求項に記載されているという単なる事実は、これらの対策の組合せを使用して利益を得ることができないことを示すものではない。

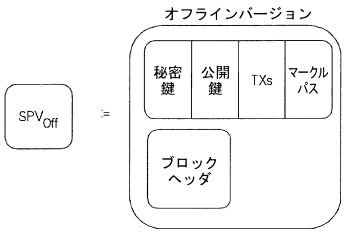
【符号の説明】

【０１４９】

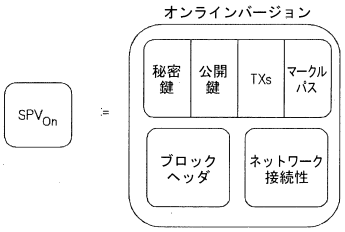
2602 プロセッサ
2604 バスサブシステム
2606 ストレージサブシステム
2608 メインメモリ
2610 永続ストレージ
2612 ユーザインターフェース入力デバイス
2614 ユーザインターフェース出力デバイス
2616 ネットワークインターフェースサブシステム
2618 RAM
2620 ROM
2624 クロック

【図面】

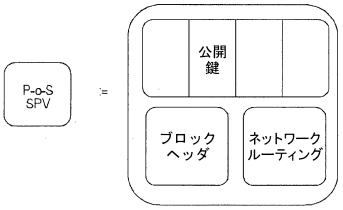
【図１】


オフラインバージョン
SPV$_{Off}$
:=
秘密鍵
公開鍵
TXs
マークルパス
ブロックヘッダ

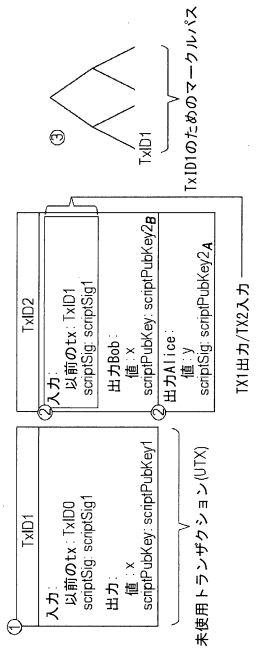
【図２】


オンラインバージョン
SPV$_{On}$
:=
秘密鍵
公開鍵
TXs
マークルパス
ブロックヘッダ
ネットワーク接続性

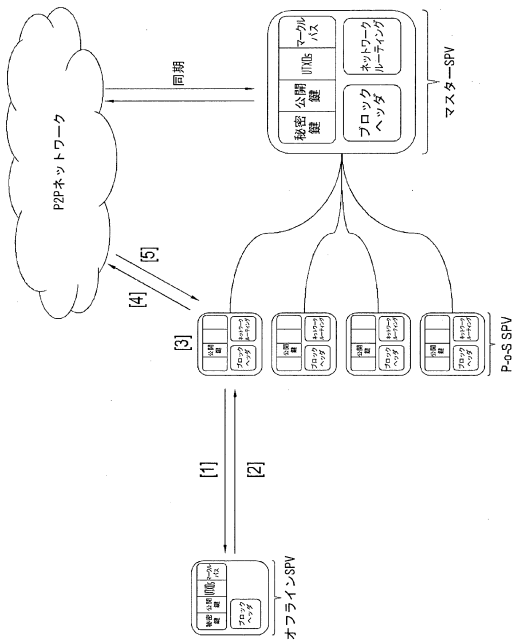
【図３】


P-o-S SPV
:=
公開鍵
ブロックヘッダ
ネットワークルーティング

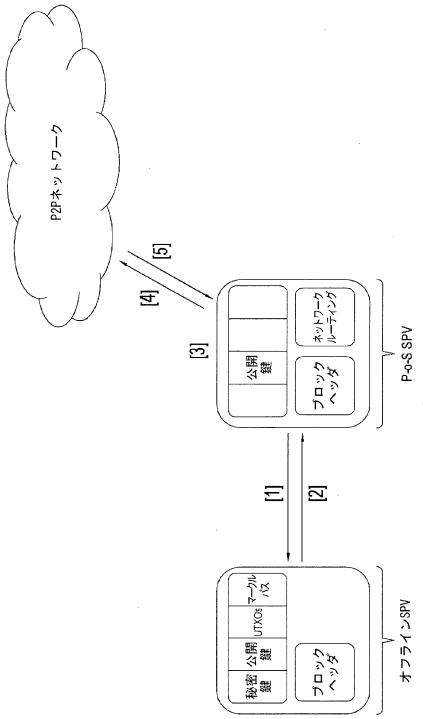
【図４】


TxID1のためのマークルパス
TxID1
③
TxID2
入力:
以前のtx: TxID1
scriptSig: scriptSig1
出力Bob:
値: x
scriptPubKey: scriptPubKey2B
出力Alice:
値: y
scriptSig: scriptPubKey2A
②
TX1出力/TX2入力
TxID1
入力:
以前のtx: TxID0
scriptSig: scriptSig1
出力:
値: x
scriptPubKey: scriptPubKey1
①
未使用トランザクション(UTX)

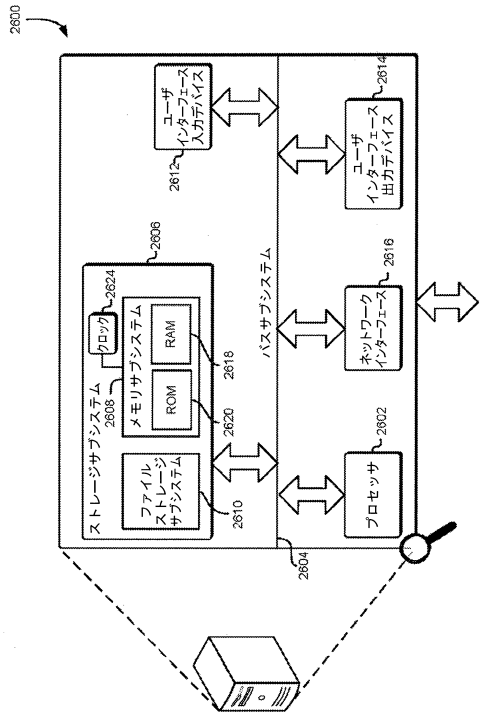
【図５】



【図６】



【図７】



【図８】

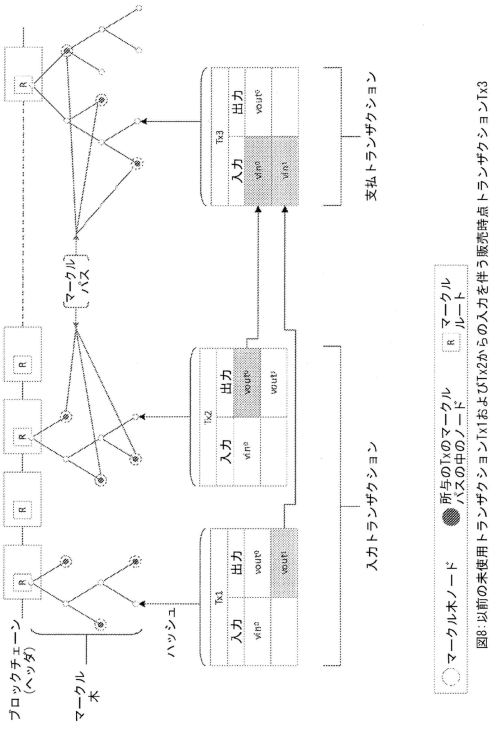
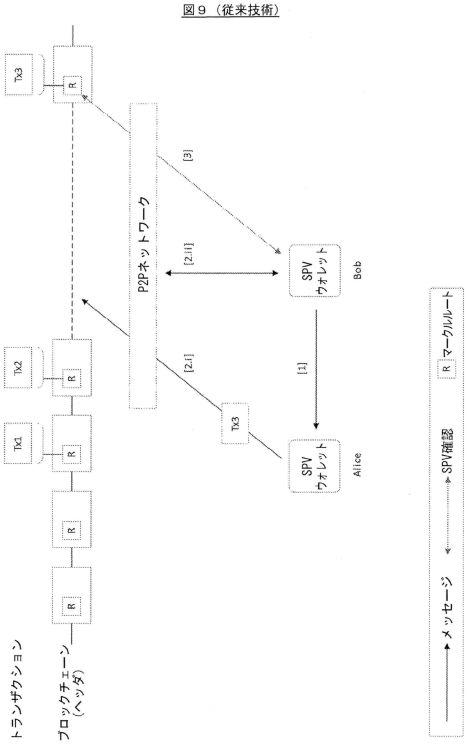
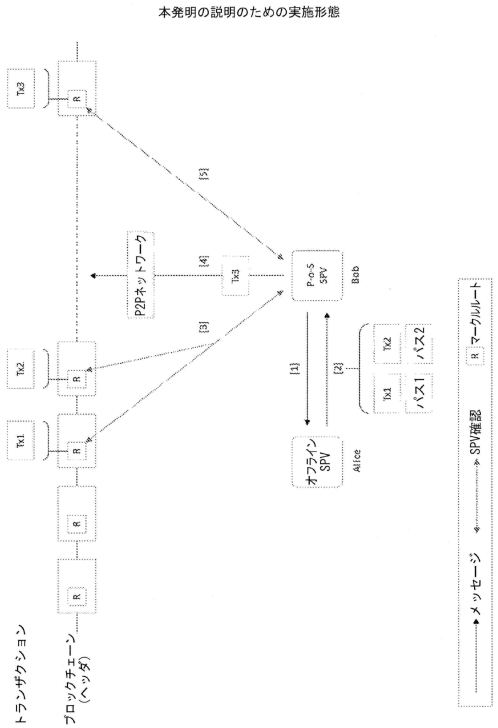


図8：以前の未使用トランザクションTx1およびTx2からの入力を伴う販売時点トランザクションTx3

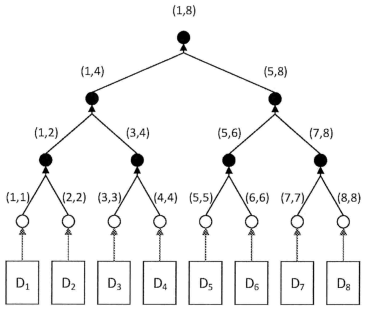
【図９】



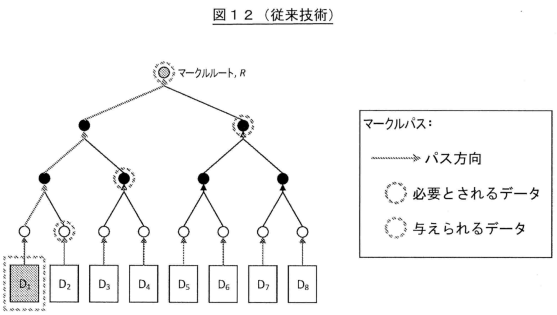
【図１０】



【図１１】



【図１２】



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 1902090.8
(32)優先日 平成31年2月15日(2019.2.15)
(33)優先権主張国・地域又は機関
英国(GB)
(31)優先権主張番号 1902089.0
(32)優先日 平成31年2月15日(2019.2.15)
(33)優先権主張国・地域又は機関
英国(GB)
(31)優先権主張番号 1902092.4
(32)優先日 平成31年2月15日(2019.2.15)
(33)優先権主張国・地域又は機関
英国(GB)
ピー内
(72)発明者 ジャック・オーウェン・デイヴィーズ
イギリス・カーディフ・ＣＦ１０・２ＨＨ・チャーチル・ウェイ・チャーチル・ハウス・セブンス・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
(72)発明者 アレクサンダー・テニソン・マッケイ
イギリス・カーディフ・ＣＦ１０・２ＨＨ・チャーチル・ウェイ・チャーチル・ハウス・セブンス・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 中里 裕正
(56)参考文献 米国特許出願公開第２０１９／００２６１４６（ＵＳ，Ａ１）
国際公開第２０１８／２２４９５４（ＷＯ，Ａ１）
アンドレアス・Ｍ・アントノプロス，ビットコインとブロックチェーン 暗号通貨を支える技術，ＮＴＴ出版，2016年07月21日，pp.147-182
DAI, W. et al.，SBLWT: A Secure Blockchain Lightweight Wallet Based on Trustzone，IEEE Access，[online]，2018年08月15日，Vol.6，pp.40638-40648，〈DOI:10.1109/ACCESS.2018.2856864〉，[2024年2月9日検索]
SHI, F., QIN, Z. and MCCANN, J. A.，OPPay: Design and Implementation of A Payment System for Opportunistic Data Services，2017 IEEE 37th International Conference on Distributed Computing Systems，2017年06月，pp.1618-1628
SAKAKIBARA, Y. et al.，A Hardware-Based Caching System on FPGA NIC for Blockchain，IEICE TRANSACTIONS on Information and Systems，Vol.E101-D No.5，2018年02月02日，pp.1350-1360
(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０６Ｆ ２１／６４
Ｇ０６Ｑ ２０／３８
ＪＳＴＰｌｕｓ／ＪＭＥＤＰｌｕｓ／ＪＳＴ７５８０（ＪＤｒｅａｍＩＩＩ）
ＩＥＥＥ Ｘｐｌｏｒｅ