(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2020-516089
(P2020-516089A)
(43)公表日　令和2年5月28日(2020.5.28)

(51)Int.Cl.		F I		テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675Z
G06F 21/55	(2013.01)	G06F	21/55	

審査請求 有　予備審査請求 未請求　（全 22 頁）

(21)出願番号　特願2019-524992 (P2019-524992)
(86)(22)出願日　平成30年5月10日 (2018.5.10)
(85)翻訳文提出日　令和1年7月2日 (2019.7.2)
(86)国際出願番号　PCT/CN2018/086280
(87)国際公開番号　WO2018/205971
(87)国際公開日　平成30年11月15日 (2018.11.15)
(31)優先権主張番号　201710335973.4
(32)優先日　平成29年5月12日 (2017.5.12)
(33)優先権主張国・地域又は機関
中国 (CN)

(71)出願人　510330264
アリババ・グループ・ホールディング・リミテッド
ＡＬＩＢＡＢＡ　ＧＲＯＵＰ　ＨＯＬＤＩＮＧ　ＬＩＭＩＴＥＤ
英国領，ケイマン諸島，グランド・ケイマン，ジョージ・タウン，ワン・キャピタル・プレイス，フォース・フロア，ピー．オー．ボックス　８４７
(74)代理人　100188558
弁理士　飯田　雅人
(74)代理人　100205785
弁理士　▲高▼橋　史生

最終頁に続く

(54)【発明の名称】ブロックチェーンベースのデータ処理方法およびデバイス

(57)【要約】
本願は、処理されるべきサービスデータの一意性を表し得る属性値を、既に処理されたサービスデータの、ブロックチェーンノード内に記憶された属性値と比較して、処理されるべきサービスデータが既に処理されたかどうかを判定すること、および処理されるべきサービスデータが未だ処理されていないと判定されるとき、処理されるべきサービスデータの処理を開始することを含む、ブロックチェーンベースのデータ処理方法およびデバイスを開示する。したがって、リプレイアタックが効果的に防止され得る。さらに、異なるサービスデータの属性値が異なるので、処理中のあるサービスデータのロッキングのために他のサービスデータを処理することができないという問題が回避され得る。したがって、ブロックチェーンネットワーク内のサービスデータ処理効率が実質的に保証され、ブロックチェーンネットワーク内の全サービスデータスループットが向上する。

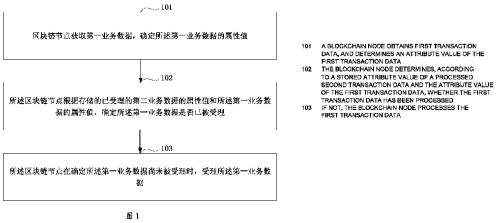


図１

【特許請求の範囲】
【請求項１】
ブロックチェーンベースのデータ処理方法であって、
ブロックチェーンノードによって第1のサービスデータを取得するステップと、
前記第1のサービスデータの属性値を決定するステップであって、前記属性値が前記第1のサービスデータの一意性を表すために使用される、前記第1のサービスデータの属性値を決定するステップと、
既に処理された第2のサービスデータの記憶された属性値と、前記第1のサービスデータの前記属性値とに基づいて、前記第1のサービスデータが既に処理されたかどうかを前記ブロックチェーンノードによって判定するステップと、
前記第1のサービスデータが未だ処理されていないと判定するとき、前記第1のサービスデータをブロックチェーンノードによって処理するステップと
を含むデータ処理方法。
【請求項２】
前記第1のサービスデータが既に処理されたと判定するとき、前記第1のサービスデータの処理を前記ブロックチェーンノードによって放棄するステップ
をさらに含む請求項1に記載のデータ処理方法。
【請求項３】
既に処理された第2のサービスデータの記憶された属性値と、前記第1のサービスデータの前記属性値とに基づいて、前記第1のサービスデータが既に処理されたかどうかを前記ブロックチェーンノードによって前記判定する前記ステップが、
前記第1のサービスデータの前記属性値と同一の属性値があるかどうかについて、既に処理された前記第2のサービスデータの前記記憶された属性値内を前記ブロックチェーンノードによって照会するステップと、
照会結果に基づいて、前記第1のサービスデータが既に処理されたかどうかを前記ブロックチェーンノードによって判定するステップと
を含む請求項1に記載のデータ処理方法。
【請求項４】
前記第1のサービスデータが未だ処理されていないと前記ブロックチェーンノードによって前記判定するステップが、
既に処理された前記第2のサービスデータの前記記憶された属性値から、前記第1のサービスデータの前記属性値と同一である属性値が見つからないと判定するとき、前記第1のサービスデータが未だ処理されていないと前記ブロックチェーンノードによって判定するステップ
を含む請求項3に記載のデータ処理方法。
【請求項５】
前記ブロックチェーンノードによって前記第1のサービスデータの前記属性値を記憶するステップ
をさらに含む請求項1に記載のデータ処理方法。
【請求項６】
処理済みデータベース内に前記第1のサービスデータの前記属性値を前記ブロックチェーンノードによって記憶するステップであって、前記処理済みデータベースが、既に処理されたサービスデータの属性値を記憶する、ステップと、
前記第1のサービスデータの前記属性値の照会索引を前記ブロックチェーンノードによって決定するステップと、
前記照会索引と前記第1のサービスデータの前記属性値との間のマッピング関係を確立するステップと、
をさらに含む請求項1に記載のデータ処理方法。
【請求項７】
前記サービスデータが生成されるとき、前記属性値が取得される請求項1から6のいずれ

か一項に記載のデータ処理方法。
【請求項８】
前記属性値が、前記サービスデータのハッシュ値および前記サービスデータのシリアル番号のうちの1つまたは複数を含む請求項1から6のいずれか一項に記載のデータ処理方法。
【請求項９】
第1のサービスデータを取得し、前記第1のサービスデータの属性値を決定するように構成された取得ユニットであって、前記属性値が前記第1のサービスデータの一意性を表すために使用される、取得ユニットと、
既に処理された第2のサービスデータの記憶された属性値と、前記第1のサービスデータの前記属性値とに基づいて、前記第1のサービスデータが既に処理されたかどうかを判定するように構成された判定ユニットと、
前記第1のサービスデータが未だ処理されていないと判定するとき、前記第1のサービスデータを処理するように構成された処理ユニットと、
を備えるブロックチェーンベースのデータ処理デバイス。
【請求項１０】
放棄ユニットをさらに備え、
前記放棄ユニットが、前記第1のサービスデータが既に処理されたと判定するとき、前記第1のサービスデータの処理を放棄するように構成される請求項9に記載のデータ処理デバイス。
【請求項１１】
既に処理された第2のサービスデータの記憶された属性値と、前記第1のサービスデータの前記属性値とに基づいて、前記第1のサービスデータが既に処理されたかどうかを判定ユニットが判定することが、
前記第1のサービスデータの前記属性値と同一の属性値があるかどうかについて、既に処理された前記第2のサービスデータの前記記憶された属性値内を照会すること、および
照会結果に基づいて、前記第1のサービスデータが既に処理されたかどうかを判定すること
を含む請求項9に記載のデータ処理デバイス。
【請求項１２】
前記第1のサービスデータが未だ処理されていないことを処理ユニットが判定することが、
既に処理された前記第2のサービスデータの前記記憶された属性値から、前記第1のサービスデータの前記属性値と同一である属性値が見つからないと判定するとき、前記第1のサービスデータが未だ処理されていないと判定すること
を含む請求項11に記載のデータ処理デバイス。
【請求項１３】
記憶ユニットをさらに備え、
前記記憶ユニットが、前記第1のサービスデータの前記属性値を記憶するように構成される請求項9に記載のデータ処理デバイス。
【請求項１４】
確立ユニットをさらに備え、
前記確立ユニットが、処理済みデータベース内に前記第1のサービスデータの前記属性値を記憶することであって、前記処理済みデータベースが、既に処理されたサービスデータの属性値を記憶するデータベースである、処理済みデータベース内に前記第1のサービスデータの前記属性値を記憶すること、と、
前記第1のサービスデータの前記属性値の照会索引を決定すること、と、
前記照会索引と前記第1のサービスデータの前記属性値との間のマッピング関係を確立すること、と
を行うように構成される請求項9に記載のデータ処理デバイス。

【請求項１５】
前記サービスデータが生成されるとき、前記属性値が取得される請求項9から14のいずれか一項に記載のデータ処理デバイス。
【請求項１６】
前記属性値が、前記サービスデータのハッシュ値および前記サービスデータのシリアル番号のうちの1つまたは複数を含む請求項9から14のいずれか一項に記載のデータ処理デバイス。
【請求項１７】
少なくとも1つのプロセッサおよびメモリを備えるデータ処理デバイスであって、前記メモリは、前記少なくとも1つのプロセッサが、
第1のサービスデータを取得するステップと
前記第1のサービスデータの属性値を決定するステップであって、前記属性値が前記第1のサービスデータの一意性を表すために使用される、前記第1のサービスデータの属性値を決定するステップと、
既に処理された第2のサービスデータの記憶された属性値と、前記第1のサービスデータの前記属性値とに基づいて、前記第1のサービスデータが既に処理されたかどうかを判定するステップと、
前記第1のサービスデータが未だ処理されていないと判定するとき、前記第1のサービスデータを処理するステップと
を実施するようにプログラムを記憶するように構成される、データ処理デバイス。
【請求項１８】
データ処理デバイスと共に使用されるプログラムを含むコンピュータ記憶媒体であって、前記プログラムが、
第1のサービスデータを取得するステップと、
前記第1のサービスデータの属性値を決定するステップであって、前記属性値が前記第1のサービスデータの一意性を表すために使用される、前記第1のサービスデータの属性値を決定するステップと、
既に処理された第2のサービスデータの記憶された属性値と、前記第1のサービスデータの前記属性値とに基づいて、前記第1のサービスデータが既に処理されたかどうかを判定するステップと、
前記第1のサービスデータが未だ処理されていないと判定するとき、前記第1のサービスデータを処理するステップと
を実施するためにプロセッサによって使用可能である、コンピュータ記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本願は、インターネット情報処理技術およびコンピュータ技術の分野に関し、詳細には、ブロックチェーンベースのデータ処理方法およびデバイスに関する。
【背景技術】
【０００２】
ブロックチェーン技術は、分散型台帳技術とも呼ばれ、分散インターネットデータベース技術である。ブロックチェーン技術に基づいて構築されたネットワークは、ブロックチェーンネットワークと呼ばれることがあり、ブロックチェーンネットワークは、ネットワークノード(ブロックチェーンノードとも呼ばれることがあり、以下では略してノードと呼ばれる)を含む。各ノードは少なくとも1つのブロックチェーンに対応し、各ブロックチェーンは少なくとも1つのブロックを含む。ブロックチェーンネットワーク(またはブロックチェーン技術)は分散化され、透明性があり、信頼でき、改ざんすることができない。これらの特徴に基づいて、ブロックチェーン技術はますます広く応用されている。
【０００３】
ブロックチェーン技術の発展と共に、実際にはリプレイアタック技術が行われ得る。リ

プレイアタック技術とは、悪意のあるユーザが、ブロックチェーンネットワークによって既に処理されたブロックチェーンネットワークまたはサービスデータによって処理中のサービスデータを不正に取得し、ブロックチェーンネットワークにサービスデータを再送し、その結果、ブロックチェーンネットワークがサービスデータを再処理することを意味する。たとえば、リプレイアタック技術を使用することによって取得されたサービスデータが「口座Aから口座Bに100元を送金している」と仮定する。口座Aが300元を有する場合、口座Aに対応するユーザにより送られるサービスデータが受信されると、トランザクションデータが処理され、次いで口座Aに200元が残る。悪意のあるユーザがリプレイアタック技術を使用することによってサービスデータを取得することにより、ブロックチェーンネットワークは、悪意のあるユーザによって送られたサービスデータを受信した後に、サービスデータの処理も行い、次いでA口座に100元が残る。このように、リプレイアタック技術がブロックチェーンネットワークのデータセキュリティを脅かすことがわかる。

【０００４】

リプレイアタックを防止するために、Ethereumが各口座について乱数を構成する。サービスデータが口座内で生成されるとき、乱数が自動的に1だけ増加され、値が得られ、値とサービスデータが共にブロックチェーンノードに送られる。したがって、サービスデータを受信するとき、ブロックチェーンノードは、値を使用することによってサービスデータに関する検証を実施し得る。ブロックチェーンノードは、サービスデータが重複したトランザクションではないとの判定するとき、サービスデータを処理し、そうでない場合、サービスデータの処理を放棄する。

【０００５】

しかしながら、サービスデータが生成されるのに伴って乱数が継続的に増加できることを保証するために、同一口座内で生成された2つのサービスデータの一方がブロックチェーンノードに送られるときは、乱数をロックする必要があり、サービスデータが処理されると、乱数がロック解除され得る。言い換えれば、そのような方法がリプレイアタックを防止するために使用されるとき、サービスデータがシリアルモードにおいて処理され、したがってブロックチェーンネットワーク内のサービスデータ処理効率は比較的低い。

【発明の概要】

【発明が解決しようとする課題】

【０００６】

これに鑑みて、本願の実施例は、ブロックチェーンネットワーク内のリプレイアタックをどのように防止するかという問題を緩和して、ブロックチェーントランザクションデータ処理の全スループットを改善するような、ブロックチェーンベースのデータ処理方法およびデバイスを提供する。

【課題を解決するための手段】

【０００７】

以下の技術的解決策が本願の実施例において使用される。

【０００８】

本願の一実施例は、ブロックチェーンノードによって第1のサービスデータを取得すること、および第1のサービスデータの属性値を決定することであって、属性値が第1のサービスデータの一意性を表すために使用される、決定すること、既に処理された第2のサービスデータの記憶された属性値と、第1のサービスデータの属性値とに基づいて、第1のサービスデータが既に処理されたかどうかをブロックチェーンノードによって判定すること、および第1のサービスデータが未だ処理されていないと判定するとき、第1のサービスデータをブロックチェーンノードによって処理することを含む、ブロックチェーンベースのデータ処理方法を提供する。

【０００９】

本願の一実施例はさらに、第1のサービスデータを取得し、第1のサービスデータの属性値を決定するように構成された取得ユニットであって、属性値が第1のサービスデータの一意性を表すために使用される、取得ユニットと、既に処理された第2のサービスデータ

の記憶された属性値と、第1のサービスデータの属性値とに基づいて、第1のサービスデータが既に処理されたかどうかを判定するように構成された判定ユニットと、第1のサービスデータが未だ処理されていないと判定するとき、第1のサービスデータを処理するように構成された処理ユニットと、を含むブロックチェーンベースのデータ処理デバイスを提供する。

【００１０】

本願の実施例において使用される前述の少なくとも1つの技術的解決策は、以下の有益な効果を達成し得る。

【００１１】

本願の実施例では、処理されるべきサービスデータの一意性を表し得る属性値が、既に処理されたサービスデータの、ブロックチェーンノード内に記憶された属性値と比較され、処理されるべきサービスデータが既に処理されたかどうかが判定され、処理されるべきサービスデータが未だ処理されていないと判定されるときにのみ、処理されるべきサービスデータの処理が開始される。したがって、リプレイアタックが実質的に防止され得る。さらに、異なるサービスデータの属性値が異なるので、処理中のあるサービスデータのロッキングのために他のサービスデータを処理することができないという問題が回避され得る。したがって、ブロックチェーンネットワーク内のサービスデータ処理効率が実質的に保証され、ブロックチェーンネットワーク内の全サービスデータスループットが向上する。

【００１２】

ここで説明される添付の図面は、本願のより一層の理解を与えるためのものであり、本願の一部を構成する。本願の例示的実施例および本願の実施例の説明は、本願を説明するためのものであり、本願に関する制限をなすものではない。

【図面の簡単な説明】

【００１３】

【図１】本願の一実施例によるブロックチェーンベースのデータ処理方法を示す概略フローチャートである。

【図２】本願の一実施例によるブロックチェーンベースのデータ処理方法を示す概略フローチャートである。

【図３】本願の一実施例によるブロックチェーンベースのデータ処理デバイスを示す概略構造図である。

【発明を実施するための形態】

【００１４】

本願の目的、技術的解決策、および利点をより明確にするために、以下では、本願の特定の実施例および対応する添付の図面を参照しながら、本願の技術的解決策を明確かつ包括的に説明する。明らかに、記載の実施例は、本願の実施例のすべてではなく一部である。創造的な努力なしに、本願の実施例に基づいて、当業者によって得られるすべての他の実施例は、本願の保護範囲内に包含されるものとする。

【００１５】

以下では、添付の図面を参照しながら、本願の実施例で与えられる技術的解決策を詳細に説明する。

【００１６】

図1は、本願の一実施例によるブロックチェーンベースのデータ処理方法を示す概略フローチャートである。方法は以下のように説明され得る。

【００１７】

ステップ101:ブロックチェーンノードが第1のサービスデータを取得し、第1のサービスデータの属性値を決定する。

【００１８】

ここで、属性値が第1のサービスデータの一意性を表すために使用される。

【００１９】

本願のこの実施例では、別のデバイスによって送られたサービス処理要求を受信するとき、ブロックチェーンノードは、サービス処理要求からサービスデータを取得し得る。この場合のサービスデータは、第1のサービスデータと見なされ得る。

【００２０】

さらに、コンセンサス動作をトリガする前に、ブロックチェーンノードは、複数の記憶されたサービスデータから所定の量のサービスデータを取得し得る。この場合のサービスデータは、複数の第1のサービスデータと見なされ得る。ここで、第1のサービスデータを取得するという特定の実施例には限定されない。

【００２１】

ブロックチェーンノードはサービスデータの処理ノードであり得、またはサービスデータの非処理ノードであり得ることに留意されたい。処理ノードは、別のデバイスからサービスデータを直接的に受信するノードと理解され得、非処理ノードは、ブロードキャストを通じて別のブロックチェーンノードからサービスデータを受信するノードと理解され得る。言い換えれば、1つのサービスデータについて、ブロックチェーンネットワークは、恐らくは1つの処理ノードおよび複数の非処理ノードを含む。

【００２２】

第1のサービスデータを取得するとき、ブロックチェーンノードは第1のサービスデータの属性値を決定し得る。この場合の属性値は、サービスデータが生成されるときに取得される。サービスデータがトランザクションデータである場合、トランザクションデータが生成されるとき、トランザクションデータのシリアル番号も生成され、シリアル番号は、トランザクションデータの属性値、すなわち本願のこの実施例において説明される属性値として使用され得る。さらに、サービスデータが生成されるとき、生成されるトランザクションデータが、所定のアルゴリズムを使用することによってさらに計算され得、得られた計算結果が、サービスデータの属性値と見なされ得る。たとえば、生成されるサービスデータが、ハッシュアルゴリズムを使用することによって計算され、得られたハッシュ値がサービスデータの属性値である。

【００２３】

本願のこの実施例において説明される属性値は、サービスデータのハッシュ値およびサービスデータのシリアル番号のうちの1つまたは複数を含む。

【００２４】

本願のこの実施例では、属性値がサービスデータを一意的に識別し得るので、属性値は、サービスデータが一意であるかどうかを識別するための条件として使用され得ることに留意されたい。

【００２５】

サービスデータの属性値のセキュリティを保証するために、属性値が暗号化され得る。ここでは具体的には限定されない。

【００２６】

ステップ102:ブロックチェーンノードは、既に処理された第2のサービスデータの記憶された属性値と、第1のサービスデータの属性値とに基づいて、第1のサービスデータが既に処理されたかどうかを判定する。

【００２７】

本願のこの実施例では、サービスデータを処理するとき、ブロックチェーンノードは、既に処理されたサービスデータの属性値を記憶する。すなわち、本願のこの実施例で与えられる技術的解決策では、ブロックチェーンノードは、データベースを維持する必要があり、データベースは、ブロックチェーンノードによって既に処理されたサービスデータの属性値を記憶する。したがって、リプレイアタックが行われるとき、処理されるべきサービスデータが重複して処理されるかどうかが、既に処理されたサービスデータの、データベース内に記憶された属性値を使用することによって判定され得る。さらに、処理中のあるサービスデータのロッキングのために他のサービスデータを処理することができないという既存の技術における問題が回避され得る。空間的にわずかに冗長であるが、システム

性能および処理時間が改善され得る。したがって、ブロックチェーンネットワーク内のサービスデータ処理効率が実質的に保証され、ブロックチェーンネットワーク内の全サービスデータスループットが向上する。

【００２８】

具体的には、ブロックチェーンノードは、第1のサービスデータの属性値と同一の属性値があるかどうかについて、既に処理された第2のサービスデータの記憶された属性値内を照会する。

【００２９】

ブロックチェーンノードは、照会結果に基づいて、第1のサービスデータが既に処理されたかどうかを判定する。

【００３０】

たとえば、ブロックチェーンノードは、既に処理された第2のサービスデータの記憶された属性値を、第1のサービスデータの属性値と比較して、既に処理された第2のサービスデータの属性値内に第1のサービスデータの属性値と同一の属性値があるかどうかを判定する。

【００３１】

既に処理された第2のサービスデータの属性値内に第1のサービスデータの属性値と同一の属性値がある場合、第1のサービスデータが既に処理されたことを示し、第1のサービスデータが無効サービスデータであり、恐らくはリプレイアタックであるとさらに判定され得る。既に処理された第2のサービスデータの属性値内に第1のサービスデータの属性値と同一の属性値がない場合、第1のサービスデータが未だ処理されていないことを示す。

【００３２】

リプレイアタック技術では、サービスデータ(以後、有効サービスデータと呼ばれる)が傍受され、または盗まれたとき、サービスデータが複製され、傍受されたサービスデータと同一の他のサービスデータ(以後、無効サービスデータと呼ばれる)が生成されることに留意されたい。それは、有効サービスデータの属性値が無効サービスデータの属性値と同一であることを示す。

【００３３】

さらに、本願のこの実施例において説明される「第1のサービスデータ」および「第2のサービスデータ」での「第1」および「第2」は、特別な意味を示すわけではなく、相異なるサービスデータの間を区別するために使用されるに過ぎない。

【００３４】

ステップ103:ブロックチェーンノードが、第1のサービスデータが未だ処理されていないと判定するとき、第1のサービスデータを処理する。

【００３５】

本願のこの実施例では、第1のサービスデータが未だ処理されていないと判定すると、ブロックチェーンノードは、第1のサービスデータを処理し得、言い換えれば、サービスデータに関するコンセンサス処理、記憶処理などを実施し得る。

【００３６】

ブロックチェーンノードが第1のサービスデータの処理ノードである場合、第1のサービスデータが未だ処理されていないと判定するとき、ブロックチェーンノードは、第1のサービスデータを処理した後、既存の技術における方法を使用することによって、ブロックチェーンネットワーク内の別のブロックチェーンノードに第1のサービスデータをさらにブロードキャストし得る。

【００３７】

具体的には、第1のサービスデータが未だ処理されていないとブロックチェーンノードによって判定することは、既に処理された第2のサービスデータの記憶された属性値から、第1のサービスデータの属性値と同一である属性値が見つからないと判定するとき、第1のサービスデータが未だ処理されていないとブロックチェーンノードによって判定することを含む。

【００３８】
好ましくは、本願のこの実施例では、方法は、ブロックチェーンノードによって第1のサービスデータの属性値を記憶することをさらに含む。
【００３９】
前述のように、ブロックチェーンノードは、データベース(以後、処理済みデータベースと呼ばれる)を維持し得、処理済みデータベースは、既に処理されたサービスデータの属性値を記憶する。ブロックチェーンノードは、処理済みデータベース内に第1のサービスデータの属性値を記憶し得る。
【００４０】
本願のこの実施例において説明される処理済みデータベースはリレーショナルデータベースであり得、またはKey-Valueデータベースであり得ることに留意されたい。ここでは具体的には限定されない。
【００４１】
好ましくは、処理済みデータベース内に第1のサービスデータの属性値を記憶するとき、ブロックチェーンノードは、第1のサービスデータの属性値についての照会索引をさらに決定し得、照会索引と第1のサービスデータの属性値との間のマッピング関係をさらに確立し得る。これは、ステップ102の実行効率を改善する助けとなり、システム全体のサービスデータ処理性能をさらに改善する。
【００４２】
好ましくは、本願のこの実施例では、方法は、第1のサービスデータが既に処理されたと判定するとき、第1のサービスデータの処理をブロックチェーンノードによって放棄することをさらに含む。
【００４３】
ブロックチェーンノード(この場合、処理ノードを指す)がサービス処理要求を受信するとき、本願のこの実施例の技術的解決策がトリガされて実行されることができ、またはコンセンサスがトリガされる前に実行され得ることに留意されたい。リアルタイムタイミングは、ここでは具体的には限定されず、実際の必要に基づいて決定され得る。
【００４４】
コンセンサスがトリガされる前に前述の解決策が実行される場合、処理ノードか、それとも非処理ノードかの如何に関わらず、コンセンサスが開始される前に、受信されたサービスデータが既に処理されたかどうかを識別する必要があることを意味し、前述の処理済みデータベースが、ブロックチェーンネットワーク内の任意のブロックチェーンノードによってアクセスされ得、言い換えれば、ブロックチェーンネットワーク内で共有されるデータベースである。さらに、ブロックチェーンノードが処理ノードである場合、第1のサービスデータが既に処理されたと判定するとき、ブロックチェーンノードは、第1のサービスデータが既に処理されたという情報を別のブロックチェーンノードにブロードキャストし、その結果、その別のブロックチェーンノードも第1のサービスデータの処理を放棄し得る。この場合の処理は、コンセンサス処理、記憶処理などであり得る。
【００４５】
本願のこの実施例での技術的解決策によれば、処理されるべきサービスデータの一意性を表し得る属性値が、既に処理されたサービスデータの、ブロックチェーンノード内に記憶された属性値と比較され、処理されるべきサービスデータが既に処理されたかどうかが判定され、処理されるべきサービスデータが未だ処理されていないと判定されるとき、処理されるべきサービスデータの処理が開始される。したがって、リプレイアタックが効果的に防止され得る。さらに、異なるサービスデータの属性値が異なるので、処理中のあるサービスデータのロッキングのために他のサービスデータを処理することができないという問題が回避され得る。したがって、ブロックチェーンネットワーク内のサービスデータ処理効率が実質的に保証され、ブロックチェーンネットワーク内の全サービスデータスループットが向上する。
【００４６】

同じ発明の概念に基づいて、図2は、本願の一実施例によるブロックチェーンベースのデータ処理方法を示す概略フローチャートである。方法は以下のように説明され得る。本願のこの実施例では、ブロックチェーンノードがサービス処理要求を受信するときにこの解決策の実行がトリガされる一例が、説明のために使用される。

【００４７】

ステップ201:ブロックチェーンノードがサービス処理要求を受信し、サービス処理要求からサービスデータを取得する。

【００４８】

ステップ202:ブロックチェーンノードはサービスデータの属性値を決定する。

【００４９】

この場合の属性値は、サービスデータのシリアル番号、サービスデータのハッシュ値などであり得る。これは具体的には限定されない。

【００５０】

ステップ203:ブロックチェーンノードは、サービスデータの属性値を使用することによって、サービスデータが既に処理されたサービスデータであるかどうかを判定し、サービスデータが既に処理されたサービスデータであると判定される場合、ステップ204を実施し、そうでない場合、ステップ206を実施する。

【００５１】

本願のこの実施例では、サービスデータが既に処理されたサービスデータであるかどうかをブロックチェーンノードが判定することは、限定はしないが、既に処理された第2のサービスデータの記憶された属性値と、第1のサービスデータの属性値とに基づいて、第1のサービスデータが既に処理されたかどうかをブロックチェーンノードによって判定することを含む。

【００５２】

具体的な実施例は、前述のステップ102を参照することができることから、簡略化のために、ここでは詳細は省略される。

【００５３】

ステップ204:ブロックチェーンノードはサービスデータを処理する。

【００５４】

ステップ205:ブロックチェーンノードは、ブロックチェーンネットワーク内の別のブロックチェーンノードにサービスデータをブロードキャストする。

【００５５】

ステップ206:ブロックチェーンノードはサービスデータを放棄する。

【００５６】

同じ発明の概念に基づいて、図3は、本願の一実施例によるブロックチェーンベースのデータ処理デバイスを示す概略構造図である。データ処理デバイスは、取得ユニット301、判定ユニット302、および処理ユニット303を含む。

【００５７】

取得ユニット301は、第1のサービスデータを取得し、第1のサービスデータの属性値を決定するように構成され、属性値が第1のサービスデータの一意性を表すために使用される。

【００５８】

判定ユニット302は、既に処理された第2のサービスデータの記憶された属性値と、第1のサービスデータの属性値とに基づいて、第1のサービスデータが既に処理されたかどうかを判定するように構成される。

【００５９】

処理ユニット303は、第1のサービスデータが未だ処理されていないと判定するとき、第1のサービスデータを処理するように構成される。

【００６０】

本願の別の実施例では、データ処理デバイスは放棄ユニット304をさらに含む。

【００６１】
放棄ユニット304は、第1のサービスデータが既に処理されたと判定するとき、第1のサービスデータの処理を放棄するように構成される。
【００６２】
本願の別の実施例では、既に処理された第2のサービスデータの記憶された属性値と、第1のサービスデータの属性値とに基づいて、第1のサービスデータが既に処理されたかどうかを判定ユニット302が判定することは、第1のサービスデータの属性値と同一の属性値があるかどうかについて、既に処理された第2のサービスデータの記憶された属性値内を照会すること、および照会結果に基づいて、第1のサービスデータが既に処理されたかどうかを判定することを含む。
【００６３】
本願の別の実施例では、第1のサービスデータが未だ処理されていないと処理ユニット303が判定することは、既に処理された第2のサービスデータの記憶された属性値から、第1のサービスデータの属性値と同一である属性値が見つからないと判定するとき、第1のサービスデータが未だ処理されていないと判定することを含む。
【００６４】
本願の別の実施例では、データ処理デバイスは記憶ユニット305をさらに含む。
【００６５】
記憶ユニット305は、第1のサービスデータの属性値を記憶するように構成される。
【００６６】
本願の別の実施例では、データ処理デバイスは確立ユニット306をさらに含む。
【００６７】
確立ユニット306は、処理済みデータベース内に第1のサービスデータの属性値を記憶することであって、処理済みデータベースが、既に処理されたサービスデータの属性値を記憶するデータベースである、処理済みデータベース内に第1のサービスデータの属性値を記憶すること、と、第1のサービスデータの属性値の照会索引を決定すること、と、照会索引と第1のサービスデータの属性値との間のマッピング関係を確立すること、とを行うように構成される。
【００６８】
本願の別の実施例では、サービスデータが生成されるとき、属性値が取得される。
【００６９】
本願の別の実施例では、属性値は、サービスデータのハッシュ値およびサービスデータのシリアル番号のうちの1つまたは複数を含む。
【００７０】
本願のこの実施例において提供されるデータ処理デバイスが、ハードウェアによって実施例され得、またはソフトウェアによって実施例され得ることに留意されたい。ここでは具体的には限定されない。本願のこの実施例において説明されるデータ処理デバイスによれば、処理されるべきサービスデータの一意性を表し得る属性値が、既に処理されたサービスデータの、ブロックチェーンノード内に記憶された属性値と比較され、処理されるべきサービスデータが既に処理されたかどうかが判定され、処理されるべきサービスデータが未だ処理されていないと判定されるときにのみ、処理されるべきサービスデータの処理が開始される。したがって、リプレイアタックが効果的に防止され得る。さらに、異なるサービスデータの属性値が異なるので、処理中のあるサービスデータのロッキングのために他のサービスデータを処理することができないという問題が回避され得る。したがって、ブロックチェーンネットワーク内のサービスデータ処理効率が実質的に保証され、ブロックチェーンネットワーク内の全サービスデータスループットが向上する。
【００７１】
同じ発明の概念に基づいて、本願の一実施例は、少なくとも1つのプロセッサおよびメモリを含むデータ処理デバイスをさらに提供する。
【００７２】

メモリは、第1のサービスデータを取得するステップと、第1のサービスデータの属性値を決定するステップであって、属性値が第1のサービスデータの一意性を表すために使用される、第1のサービスデータの属性値を決定するステップと、既に処理された第2のサービスデータの記憶された属性値と、第1のサービスデータの属性値とに基づいて、第1のサービスデータが既に処理されたかどうかを判定するステップと、第1のサービスデータが未だ処理されていないと判定するとき、第1のサービスデータを処理するステップと、を少なくとも1つのプロセッサが実施するようにプログラムを記憶するように構成される。

【００７３】

同じ発明の概念に基づいて、本願の実施例は、データ処理デバイスと共に使用されるプログラムを含むコンピュータ記憶媒体をさらに提供し、プログラムは、第1のサービスデータを取得するステップと、第1のサービスデータの属性値を決定するステップであって、属性値が第1のサービスデータの一意性を表すために使用される、第1のサービスデータの属性値を決定するステップと、既に処理された第2のサービスデータの記憶された属性値と、第1のサービスデータの属性値とに基づいて、第1のサービスデータが既に処理されたかどうかを判定するステップと、第1のサービスデータが未だ処理されていないと判定するとき、第1のサービスデータを処理するステップとを実施するようにプロセッサによって使用され得る。

【００７４】

具体的な実施例は、前述の実施例を参照することができることから、簡略化のために、ここでは詳細は省略される。

【００７５】

1990年代では、技術の改良が、ハードウェア改良(たとえば、ダイオード、トランジスタ、スイッチなどの回路構造に関する改良)と、ソフトウェア改良(方法手順に関する改良)との間で明確に区別され得る。しかしながら、技術の発展と共に、多くの方法手順の改良は、ハードウェア回路構造の直接的改良と見なされ得る。設計者は、ハードウェア回路に対する改良型の方法手順をほぼすべてプログラムし、対応するハードウェア回路構造を取得する。したがって、方法手順の改良がハードウェアエンティティモジュールを使用することによって実装することはできないと言うことはできない。たとえば、プログラマブル論理デバイス(PLD)(たとえば、フィールドプログラマブルゲートアレイ(FPGA))はそのような集積回路である。プログラマブル論理デバイスの論理機能は、ユーザによって実行されるコンポーネントプログラミングによって決定される。設計者は、専用集積回路チップを設計および製造するようにチップ製造業者に要求することなく、自発的なプログラミングを実施して、デジタルシステムを単一のPLDに「統合」する。さらに、集積回路チップを手作業で製造する代わりに、プログラミングは主に、プログラム開発中に使用されるソフトウェアコンパイラに類似した「論理コンパイラ」ソフトウェアによって実装される。コンパイル前の元のコードは、ハードウェア記述言語(HDL)と呼ばれる特定のプログラミング言語でも書かれ、ABEL(Advanced Boolean Expression Language)、AHDL(Altera Hardware Description Language)、Confluence、CUPL(Cornell University Programming Language)、HDCal、JHDL(Java Hardware Description Language)、Lava、Lola、MyHDL、PALASM、およびRHDL(Ruby Hardware Description Language)などの複数のタイプのHDLがある。現在は、VHDL(Very-High-Speed Integrated Circuit Hardware Description Language)およびVerilogが最も一般的に使用されている。方法の手順
が必要とするのは、論理的方法の手順を実装するハードウェア回路が容易に取得され得るように、論理的にプログラミングを行い、上述のハードウェア記述言語を使用することによって集積回路にプログラムすることだけであることも、当業者にとっては明らかであるはずである。

【００７６】

コントローラは、任意の適切な方法を使用することによって実装され得る。たとえば、コントローラは、マイクロプロセッサもしくはプロセッサ、またはコンピュータ可読媒体、論理ゲート、スイッチ、特定用途向け集積回路(ASIC)、プログラマブル論理コントロー

ラ、またはマイクロプロセッサまたはプロセッサによって実行され得るコンピュータ可読プログラムコード(ソフトウェアやファームウェアなど)を記憶する組込みマイクロプロセッサであり得る。コントローラの例には、限定はしないが、以下のマイクロプロセッサが含まれる。ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20、およびSilicone Labs C8051F320。メモリコントローラはまた、メモリの制御論理の一部として実装され得る。純粋なコンピュータ可読プログラムコードを使用することによってコントローラが実装され得ることも当業者には知られており、方法のステップが、論理ゲート、スイッチ、特定用途向け集積回路、プログラマブル論理コントローラ、組込みマイクロコントローラなどの形態で同一の機能をコントローラがさらに実装することを可能にするように論理的にプログラムされ得る。したがって、コントローラはハードウェア構成要素と見なされ得、コントローラ内に含まれ、様々な機能を実装するように構成される装置も、ハードウェア構成要素内の構造と見なされ得る。代替として、様々な機能を実装するように構成された装置は、方法を実装するためのソフトウェアモジュールと、ハードウェア構成要素内の構造の両方と見なされ得る。

【００７７】

記載の実施例において説明されるシステム、装置、モジュール、またはユニットは、コンピュータチップまたはエンティティによって実現され得、または一定の機能を有する製品によって実現され得る。典型的な実現されたデバイスはコンピュータである。コンピュータは、たとえばパーソナルコンピュータ、ラップトップコンピュータ、セルラーフォン、カメラフォン、スマートフォン、携帯情報端末、メディアプレーヤ、ナビゲーションデバイス、eメールデバイス、ゲームコンソール、タブレットコンピュータ、またはウェアラブルデバイス、あるいはこれらのデバイスのいずれかの組合せであり得る。

【００７８】

説明しやすいように、機能を様々なユニットに分割することによって、記載の装置が説明される。もちろん、本願が実現されるとき、ユニットの機能が、1つまたは複数のソフトウェアおよび/またはハードウェア内で実現され得る。

【００７９】

本開示の実施例が方法、システム、またはコンピュータプログラム製品として提供され得ることを当業者は理解されたい。したがって、本開示は、ハードウェアのみの実施例、ソフトウェアのみの実施例、またはソフトウェアとハードウェアの組合せを有する実施例の形態を使用し得る。さらに、本開示は、コンピュータ使用可能プログラムコードを含む1つまたは複数のコンピュータ使用可能記憶媒体(限定はしないが、ディスクメモリ、CD-ROM、光メモリを含む)上に実装されるコンピュータプログラム製品の形態を使用し得る。

【００８０】

本開示が、本開示の実施例による方法、デバイス(システム)、およびコンピュータプログラム製品のフローチャートおよび/またはブロック図を参照しながら説明される。コンピュータプログラム命令が、フローチャートおよび/またはブロック図内の各プロセスおよび/または各ブロックと、フローチャートおよび/またはブロック図内のプロセスおよび/またはブロックの組合せとを実現するように使用され得ることを理解されたい。これらのコンピュータプログラム命令は、汎用コンピュータ、専用コンピュータ、組込みプロセッサ、または任意の他のプログラマブルデータ処理デバイスのプロセッサがマシンを生成するために提供され得、その結果、任意の他のプログラマブルデータ処理デバイスのコンピュータまたはプロセッサによって実行される命令が、フローチャート内の1つまたは複数のプロセス内、またはブロック図内の1つまたは複数のブロック内の特定の機能を実現するための装置を生成する。

【００８１】

これらのコンピュータプログラム命令は、コンピュータまたは任意の他のプログラマブルデータ処理デバイスに特定の方法において動作するように命令し得るコンピュータ可読メモリ内に記憶され得、その結果、コンピュータ可読メモリ内に記憶された命令が、命令装置を含むアーチファクトを生成する。命令装置は、フローチャート内の1つまたは複数

のプロセス内、および/またはブロック図内の1つまたは複数のブロック内の特定の機能を実現する。

【００８２】

これらのコンピュータプログラム命令は、コンピュータまたは別のプログラマブルデータ処理デバイスにロードされ得、その結果、一連の動作およびステップがコンピュータまたは別のプログラマブルデバイス上で実施され、コンピュータ実装処理が生成される。したがって、コンピュータまたは別のプログラマブルデバイス上で実行される命令は、フローチャート内の1つまたは複数のプロセス内、またはブロック図内の1つまたは複数のブロック内の特定の機能を実現するためのステップを提供する。

【００８３】

典型的構成では、コンピューティングデバイスは、1つまたは複数のプロセッサ(CPU)、1つまたは複数の入力/出力インターフェース、1つまたは複数のネットワークインターフェース、および1つまたは複数のメモリを含む。

【００８４】

メモリは、コンピュータ可読媒体内の非永続的メモリ、ランダムアクセスメモリ(RAM)、および/または不揮発性メモリ、たとえば読取り専用メモリ(ROM)またはフラッシュメモリ(フラッシュRAM)を含み得る。メモリはコンピュータ可読媒体の一例である。

【００８５】

コンピュータ可読媒体は、任意の方法または技術を使用することによって情報記憶を実現し得る、永続的、非永続的、移動可能、および移動不能媒体を含む。情報は、コンピュータ可読命令、データ構造、プログラムモジュール、または他のデータであり得る。コンピュータ記憶媒体には、限定はしないが、パラメータランダムアクセスメモリ(PRAM)、静的ランダムアクセスメモリ(SRAM)、ダイナミックランダムアクセスメモリ(DRAM)、別のタイプのランダムアクセスメモリ(RAM)、読取り専用メモリ(ROM)、電気消去可能プログラマブル読取り専用メモリ(EEPROM)、フラッシュメモリもしくは別のメモリ技術、コンパクトディスク読取り専用メモリ(CD-ROM)、デジタルバーサタイルディスク(DVD)もしくは別の光ストレージ、磁気テープ、磁気ディスクストレージ、別の磁気記憶デバイス、またはコンピューティングデバイスによってアクセスされ得る情報を記憶するのに使用され得る任意の他の非伝送媒体が含まれる。本明細書での定義に基づいて、コンピュータ可読媒体は、一時コンピュータ可読媒体(一時媒体)、たとえば変調されたデータ信号および/または搬送波を含む。

【００８６】

「含む」という用語、またはその任意の他の変形は、非排他的包含をカバーするものとし、したがって、要素のリストを含むプロセス、方法、商品、またはデバイスは、それらの要素だけでなく、明白に列挙されない他の要素をも含み、またはそのようなプロセス、方法、商品、もしくはデバイスに固有の要素をさらに含むことに留意されたい。「...を含む」に先行する要素は、より多くの制約なしに、要素を含むプロセス、方法、商品、またはデバイス内の追加の同一の要素の存在を除外するものではない。

【００８７】

本願は、コンピュータ、たとえばプログラムモジュールによって実行されるコンピュータ実行可能命令の一般的状況において説明され得る。一般に、プログラムモジュールは、特定のタスクを実行し、または特定の抽象データタイプを実装するためのルーチン、プログラム、オブジェクト、コンポーネント、データ構造などを含む。本願はまた、分散コンピューティング環境でも実施され得る。分散コンピューティング環境では、通信ネットワークを通じて接続されたリモート処理デバイスによってタスクが実施される。分散コンピューティング環境では、プログラムモジュールは、記憶デバイスを含むローカルコンピュータ記憶媒体とリモートコンピュータ記憶媒体のどちらにも配置され得る。

【００８８】

本明細書での実施例はすべて、漸進的に説明される。実施例の同一または類似の部分については、相互に実施例を参照されたい。各実施例は、他の実施例との違いに焦点を当て

る。具体的には、システムの実施例は、基本的には方法の実施例に類似しており、したがって簡潔に説明される。関連部分については、方法の実施例の部分的説明を参照されたい。

【００８９】

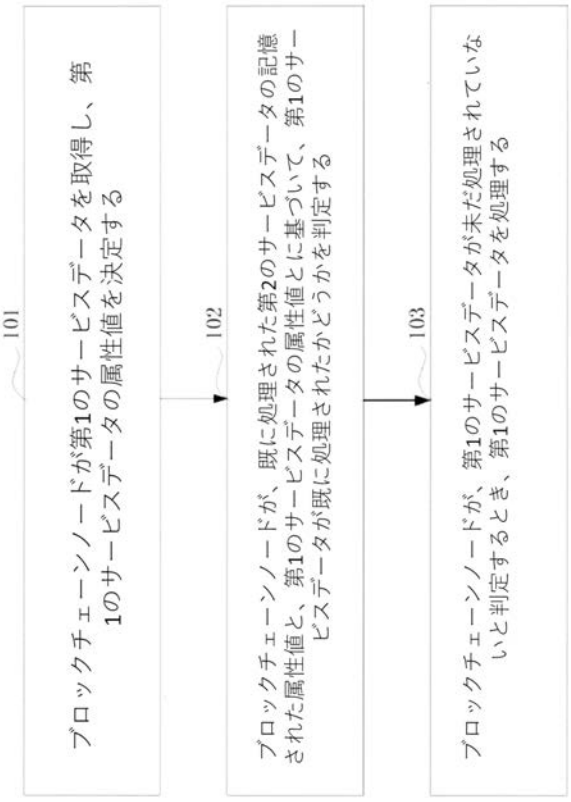
上記の説明は本願の実施例に過ぎず、本願を限定するものではない。当業者は、本願に対する様々な修正および変更を行い得る。本願の精神および原理内で行われる任意の修正、等価な置換、改良などは、本願の特許請求の範囲内に包含されるものとする。

【符号の説明】

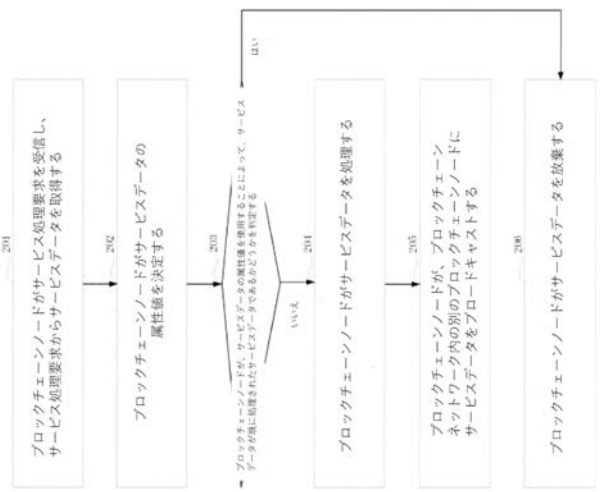
【００９０】

301　取得ユニット
302　判定ユニット
303　処理ユニット
304　放棄ユニット
305　記憶ユニット
306　確立ユニット

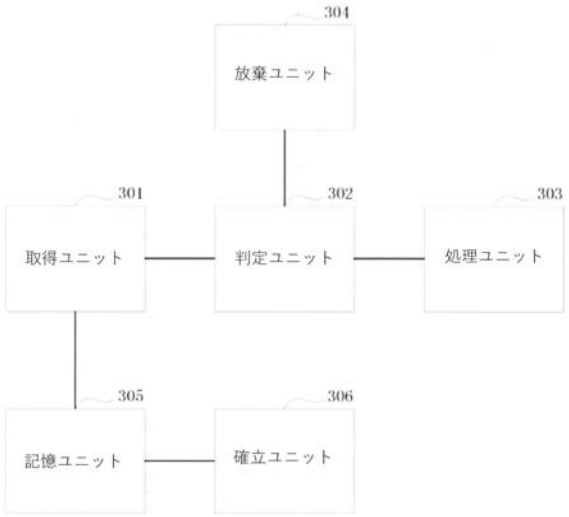
【図１】



【図２】



【図３】



【手続補正書】
【提出日】令和1年7月2日(2019.7.2)
【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】
ブロックチェーンベースのデータ処理のための方法であって、
ブロックチェーンノードによって複数のサービスデータを含む第1のサービスデータを取得するステップと、
前記第1のサービスデータの属性値を決定するステップであって、前記属性値が前記第1のサービスデータの一意性を表すために使用される、前記第1のサービスデータの属性値を決定するステップと、
既に処理された第2のサービスデータの記憶された属性値と、前記第1のサービスデータの前記属性値とに基づいて、前記第1のサービスデータが既に処理されたかどうかを前記ブロックチェーンノードによって判定するステップと、
前記第1のサービスデータが未だ処理されていないと判定するとき、前記第1のサービスデータをブロックチェーンノードによって処理するステップと
を含む方法。
【請求項２】
前記第1のサービスデータが既に処理されたと判定するとき、前記第1のサービスデータの処理を前記ブロックチェーンノードによって放棄するステップ
をさらに含む請求項1に記載の方法。

【請求項３】
前記第1のサービスデータが既に処理されたかどうかを判定するステップが、
前記第1のサービスデータの前記属性値と同一の属性値があるかどうかについて、既に処理された前記第2のサービスデータの前記記憶された属性値内を前記ブロックチェーンノードによって照会するステップと、
照会結果に基づいて、前記第1のサービスデータが既に処理されたかどうかを前記ブロックチェーンノードによって判定するステップと
を含む請求項1に記載の方法。
【請求項４】
前記第1のサービスデータが未だ処理されていないと前記ブロックチェーンノードによって判定するステップが、
既に処理された前記第2のサービスデータの前記記憶された属性値から、前記第1のサービスデータの前記属性値と同一である属性値が見つからないと判定するとき、前記第1のサービスデータが未だ処理されていないと前記ブロックチェーンノードによって判定するステップ
を含む請求項3に記載の方法。
【請求項５】
前記第1のサービスデータが既に処理されたと前記ブロックチェーンノードによって判定するステップが、
前記属性値が、既に処理された前記第2のサービスデータの前記記憶された属性値からの、前記第1のサービスデータの前記属性値と同一であることが判明したと判定するとき、前記第1のサービスデータが既に処理されたと前記ブロックチェーンノードによって判定するステップと、
前記第1のサービスデータが無効サービスデータであると判定するステップと
を含む請求項3に記載の方法。
【請求項６】
前記ブロックチェーンノードによって前記第1のサービスデータの前記属性値を記憶するステップ
をさらに含む請求項1に記載の方法。
【請求項７】
処理済みデータベース内に前記第1のサービスデータの前記属性値を前記ブロックチェーンノードによって記憶するステップであって、前記処理済みデータベースが、既に処理されたサービスデータの属性値を記憶する、ステップと、
前記第1のサービスデータの前記属性値の照会索引を前記ブロックチェーンノードによって決定するステップと、
前記照会索引と前記第1のサービスデータの前記属性値との間のマッピング関係を確立するステップと
をさらに含む請求項1に記載の方法。
【請求項８】
前記第1のサービスデータが生成されるとき、前記属性値が取得される請求項1に記載の方法。
【請求項９】
前記属性値が、前記第1のサービスデータのハッシュ値および前記第1のサービスデータのシリアル番号のうちの1つまたは複数を含む請求項1に記載の方法。
【請求項１０】
前記属性値が暗号化データを含む請求項1に記載の方法。
【請求項１１】
ブロックチェーンベースのデータ処理のためのデバイスであって、請求項1から10のいずれか一項に記載の方法を実施するように構成された複数のモジュールを備えるデバイス。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/086280

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; CNKI; VEN; USTXT; EPTXT; WOTXT: 区块链, 重放攻击, 双花, 双重, 支付, 花费, 消费, 重复, 交易, 标识, 属性, 身份, 唯一, block chain, double spend+, double bill+, transaction, ID, unique

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103036696 A (CHINA MOBILE GROUP GANSU CO., LTD.), 10 April 2013 (10.04.2013), description, paragraphs [0048]-[0111]	1-18
A	CN 105931052 A (SICHUAN UNIVERSITY), 07 September 2016 (07.09.2016), entire document	1-18
A	WO 2017006136 A1 (BARCLAYS BANK PLC), 12 January 2017 (12.01.2017), entire document	1-18

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 July 2018	27 July 2018
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer SUN, Huizhu Telephone No. 86-(512)-88996093

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/086280

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103036696 A	10 April 2013	CN 103036696 B	25 May 2016
CN 105931052 A	07 September 2016	None	
WO 2017006136 A1	12 January 2017	EP 3320502 A1	16 May 2018
		IN 201827004407 A	11 May 2018

Form PCT/ISA/210 (patent family annex) (January 2015)

国际检索报告

国际申请号
PCT/CN2018/086280

A. 主题的分类

H04L 29/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNABS;CNTXT;CNKI;VEN;USTXT;EPTXT;WOTXT：区块链，重放攻击，双花，双重，支付，花费，消费，重复，交易，标识，属性，身份，唯一，block chain，double spend+，double bill+，transaction，ID，unique

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 103036696 A (中国移动通信集团甘肃有限公司) 2013年 4月 10日 (2013-04-10) 说明书第[0048]-[0111]段	1-18
A	CN 105931052 A (四川大学) 2016年 9月 7日 (2016-09-07) 全文	1-18
A	WO 2017006136 A1 (BARCLAYS BANK PLC) 2017年 1月 12日 (2017-01-12) 全文	1-18

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2018年 7月 9日	2018年 7月 27日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 孙慧珠 电话号码 86-(512)-88996093

表 PCT/ISA/210 (第2页) (2015年1月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/086280

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	103036696	A	2013年 4月 10日	CN	103036696	B	2016年 5月 25日
CN	105931052	A	2016年 9月 7日		无		
WO	2017006136	A1	2017年 1月 12日	EP	3320502	A1	2018年 5月 16日
				IN	201827004407	A	2018年 5月 11日

表 PCT/ISA/210（同族专利附件）（2015年1月）

フロントページの続き

(81)指定国・地域 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT

（特許庁注：以下のものは登録商標）
１．ＪＡＶＡ

(72)発明者 ホンリン・チウ
中華人民共和国・３１１１２１・ゼジャン・ハンジョウ・ユ・ハン・ディストリクト・ウェスト・ウェン・イ・ロード・ナンバー・９６９・ビルディング・３・５／エフ・アリババ・グループ・リーガル・デパートメント