República Federativa do Brasil
Ministério da Economia
Instituto Nacional da Propriedade Industrial

(21) BR 112019008025-2 A2

(22) Data do Depósito: 16/11/2018

(43) Data da Publicação Nacional: 18/04/2019

---

(54) Título: MÉTODO IMPLEMENTADO POR COMPUTADOR, MEIO DE ARMAZENAMENTO LEGÍVEL POR COMPUTADOR NÃO TRANSITÓRIO E SISTEMA

(51) Int. Cl.: H04L 29/08.

(71) Depositante(es): ALIBABA GROUP HOLDING LIMITED.

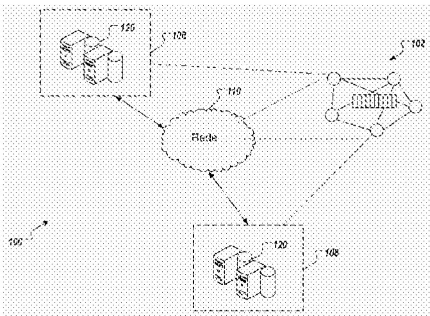
(72) Inventor(es): HONGLIN QIU.

(86) Pedido PCT: PCT CN2018115918 de 16/11/2018

(87) Publicação PCT: WO 2019/072271 de 18/04/2019

(85) Data da Fase Nacional: 18/04/2019

(57) Resumo: As implementações da presente invenção incluem a obtenção, por um nó cliente de um primeiro caso de protocolo de confiança, de um nome de domínio do protocolo de confiança de um segundo caso de protocolo de confiança diferente, em que o nome de domínio do protocolo de confiança é um identificador único do segundo caso de protocolo de confiança em uma rede de protocolo de confiança unificada incluindo múltiplos casos de protocolo de confiança que são ligados de forma comunicativa por dois ou mais retransmissores, o nome de domínio do protocolo de confiança inclui um rótulo legível por humanos e o nome de domínio do protocolo de confiança corresponde exclusivamente a um identificador de cadeia do segundo caso de protocolo de confiança; identificar o identificador da cadeia do segundo caso de protocolo de confiança com base no nome de domínio do protocolo de confiança do segundo caso de protocolo de confiança, em que o identificador de cadeia do segundo caso de protocolo de confiança indica uma configuração de rede de protocolo de confiança do segundo caso de protocolo de confiança; e acessar, por meio do nó cliente, o segundo caso de protocolo de confiança com base na configuração de rede (...).



“MÉTODO IMPLEMENTADO POR COMPUTADOR, MEIO LEGÍVEL POR COMPUTADOR E SISTEMA PARA IMPLEMENTAR UM MÉTODO”

CAMPO DA INVENÇÃO

[001] A presente invenção se refere a métodos implementados por computador para um esquema de nome de domínio para sistemas de protocolo de confiança.

ANTECEDENTES DA INVENÇÃO

[002] Os sistemas de contabilidade distribuída (DLSs), que também podem ser denominados redes de consenso e/ ou redes de protocolo de confiança (*blockchain*), permitem que as entidades participantes armazenem dados de forma segura e imutável. Os DLSs são comumente referidos como redes de protocolo de confiança sem fazer referência a qualquer caso de usuário particular (por exemplo, criptomoedas). Exemplos de tipos de redes de protocolo de confiança podem incluir redes de protocolo de confiança públicas, redes de protocolo de confiança privadas e redes de protocolo de confiança de consórcio. Uma rede de protocolo de confiança pública é aberta para todas as entidades usarem o DLS e participam no processo de consenso. Uma rede de protocolo de confiança privada é fornecida para uma entidade específica, que controla centralmente as permissões de leitura e gravação. Uma rede de protocolo de confiança de consórcio é fornecida para um grupo seleto de entidades, que controlam o processo de consenso e incluem uma camada de controle de acesso.

[003] Os protocolos de confiança são usados em redes de criptomoedas, que permitem aos participantes realizar transações para comprar/ vender mercadorias e/ ou serviços usando uma criptomoeda. Uma criptomoeda comum inclui o Bitcoin. Em redes de criptomoedas, os modelos de manutenção de registros são usados para registrar transações entre usuários. Exemplos de modelos de manutenção de registos inclui um modelo de saída

de transação não utilizada (*unspent transaction output* - UTXO), e o modelo de conta (também referida como modelo baseado em conta ou modelo de conta/ equilíbrio).

DESCRIÇÃO DA INVENÇÃO

[004] As realizações da presente invenção incluem métodos implementados por computador para um esquema de nome de domínio para sistemas de protocolo de confiança. Mais particularmente, as realizações da presente divulgação se referem a um esquema de nome de domínio unificado para interações de cadeia cruzada em sistemas de protocolo de confiança.

[005] Em algumas realizações, as ações incluem obter, por meio de um nó cliente de um primeiro caso de protocolo de confiança, um nome de domínio do protocolo de confiança de um segundo caso de protocolo de confiança diferente, em que o nome de domínio do protocolo de confiança é um identificador exclusivo do segundo caso de protocolo de confiança em uma rede de protocolo de confiança unificada que compreende múltiplos casos de protocolo de confiança que são comunicativamente ligados por dois ou mais retransmissores, o nome de domínio do protocolo de confiança compreende um rótulo legível por humano e o nome de domínio do protocolo de confiança corresponde exclusivamente a um identificador de cadeia do segundo caso de protocolo de confiança; identificar o identificador da cadeia do segundo caso de protocolo de confiança com base no nome de domínio do protocolo de confiança do segundo caso de protocolo de confiança, em que o identificador de cadeia do segundo caso de protocolo de confiança indica uma configuração de rede de protocolo de confiança do segundo caso de protocolo de confiança; e acessar, por meio do nó cliente, o segundo caso de protocolo de confiança com base na configuração de rede de protocolo de confiança indicada pelo identificador de cadeia do segundo caso de protocolo de confiança.

[006] Outras realizações incluem sistemas, aparelhos e

programas de computador correspondentes, configurados para executar as ações dos métodos codificados em dispositivos de armazenamento de computador.

[007] Essas e outras realizações podem incluir, opcionalmente, um ou mais das seguintes características:

[008] Uma primeira característica, combinável com qualquer uma das seguintes características, incluindo ainda a realização de transações de cadeia cruzadas entre o primeiro caso de protocolo de confiança e o segundo caso de protocolo de confiança com base no nome de domínio do protocolo de confiança do segundo caso de protocolo de confiança.

[009] Uma segunda característica, combinável com qualquer uma das seguintes características, em que o rótulo legível por humanos inclui um rótulo baseado em texto.

[0010] Uma terceira característica, combinável com qualquer uma das seguintes características, em que o identificador de cadeia do segundo caso de protocolo de confiança inclui um valor hash de um bloco de gênese do segundo caso de protocolo de confiança e um identificador de rede do segundo caso de protocolo de confiança.

[0011] Uma quarta característica, combinável com qualquer uma das seguintes características, em que cada uma da pluralidade de casos de protocolo de confiança na rede de protocolo de confiança unificada tem apenas um nome de domínio do protocolo de confiança que identifica exclusivamente cada uma da pluralidade de casos de protocolo de confiança.

[0012] Uma quinta característica, combinável com qualquer uma das seguintes características, em que a identificação do identificador da cadeia do segundo caso de protocolo de confiança com base no nome de domínio do protocolo de confiança inclui a identificação do identificador de cadeia do segundo caso de protocolo de confiança, de acordo com as informações de consulta armazenadas localmente no nó cliente com base no nome de domínio do protocolo de confiança.

[0013] Uma sexta característica, combinável com qualquer uma das seguintes características, em que a identificação do identificador da cadeia do segundo caso de protocolo de confiança com base no nome de domínio do protocolo de confiança inclui: enviar, para um servidor de nome de domínio do protocolo de confiança unificado, uma solicitação que inclui o nome de domínio do protocolo de confiança para identificar o identificador de cadeia do segundo caso de protocolo de confiança; e receber, do servidor de nome de domínio do protocolo de confiança unificado, uma resposta que inclui o identificador de cadeia do segundo caso de protocolo de confiança.

[0014] Uma sétima característica, combinável com qualquer uma das seguintes características, em que o primeiro caso de protocolo de confiança e o segundo caso de protocolo de confiança são implementados com base em diferentes plataformas de protocolo de confiança.

[0015] A presente invenção também fornece um ou mais meios de armazenamento legível por computador acoplado a um ou mais processadores e tendo instruções armazenadas no mesmo que, quando executados por um ou mais processadores, fazer com que os um ou mais processadores execute as operações de acordo com realizações dos métodos aqui fornecidos.

[0016] A presente invenção fornece ainda um sistema para implementar os métodos aqui fornecidos. O sistema inclui um ou mais processadores, e um meio de armazenamento legível por computador acoplado a um ou mais processadores com instruções armazenadas no mesmo que, quando executados por um ou mais processadores, fazem com que um ou mais processadores executem operações de acordo com realizações dos métodos aqui fornecidos.

[0017] Entende-se que os métodos de acordo com a presente invenção podem incluir qualquer combinação das realizações e características aqui descritas. Isto é, os métodos de acordo com a presente invenção não estão limitados às combinações de realizações e características especificamente descritas aqui, mas também incluem qualquer combinação das realizações e características fornecidas.

[0018] Os detalhes de uma ou mais realizações da presente invenção são apresentados nos desenhos anexos e na descrição abaixo. Outras características e vantagens da presente invenção serão evidentes a partir da descrição e desenhos, e das reivindicações.

BREVE DESCRIÇÃO DOS DESENHOS

[0019] A Figura 1 ilustra um exemplo de ambiente que pode ser usado para executar realizações da presente invenção.

[0020] A Figura 2 ilustra um exemplo de arquitetura conceitual de acordo com realizações da presente invenção.

[0021] A Figura 3 ilustra um exemplo de nome de domínio do protocolo de confiança unificado (UBCDN) de um caso de protocolo de confiança, de acordo com realizações da presente invenção.

[0022] A Figura 4 ilustra um exemplo de esquema de gestão de UBCDN em uma rede de protocolo de confiança unificada, de acordo com realizações da presente invenção.

[0023] A Figura 5 ilustra um exemplo de processo para usar um nome de domínio do protocolo de confiança de um caso de protocolo de confiança para interações de cadeia cruzada em uma rede de protocolo de confiança unificada, de acordo com realizações da presente invenção.

[0024] A Figura 6 ilustra um exemplo de processo para autenticar um UBCDN de um caso de protocolo de confiança, de acordo com realizações da presente invenção.

[0025] A Figura 7 descreve um exemplo de processo de um proprietário de um UBCDN de um caso de protocolo de confiança (um proprietário de UBCDN), de acordo com realizações da presente invenção.

[0026] A Figura 8 ilustra um exemplo de processo de um retransmissor para interações de cadeia cruzada em uma rede de protocolo de confiança unificada, de acordo com realizações da presente invenção.

[0027] Os símbolos de referência semelhantes nos vários desenhos indicam elementos semelhantes.

DESCRIÇÃO DE REALIZAÇÕES DA INVENÇÃO

[0028] As realizações da presente invenção incluem métodos implementados por computador para um esquema de nome de domínio para sistemas de protocolo de confiança. Mais particularmente, as realizações da presente divulgação se referem a um esquema de nome de domínio unificado para interações de cadeia cruzada em sistemas de protocolo de confiança.

[0029] Em algumas realizações, as ações incluem ações que incluem a obtenção, por um nó cliente de um primeiro caso de protocolo de confiança, de um nome de domínio do protocolo de confiança de um segundo caso de protocolo de confiança diferente, em que o nome de domínio do protocolo de confiança é um identificador exclusivo do segundo caso de protocolo de confiança em uma rede de protocolo de confiança unificada incluindo múltiplos casos de protocolo de confiança que são comunicativamente ligados por dois ou mais retransmissores, o nome de domínio do protocolo de confiança inclui um rótulo legível por humanos e o nome de domínio do protocolo de confiança corresponde exclusivamente a um identificador de cadeia do segundo caso de protocolo de confiança; identificar o identificador da cadeia do segundo caso de protocolo de confiança com base no nome de domínio do protocolo de confiança do segundo caso de protocolo de confiança, em que o identificador de cadeia do segundo caso de protocolo de confiança indica uma configuração de rede de protocolo de confiança do segundo caso de protocolo de confiança; e acessar, por meio do nó cliente, o segundo caso de protocolo de confiança com base na configuração de rede de protocolo de confiança indicada pelo identificador de cadeia do segundo caso de protocolo de confiança.

[0030] Para fornecer um contexto adicional para realizações da presente invenção, e como introduzidas acima, sistemas de contabilidade distribuída (DLSs), que também podem ser referidos como redes de consenso (por exemplo, constituídas por nós peer-to-peer), e redes de protocolo de confiança, permite que as entidades participantes conduzam transações de forma segura e imutável e armazenem dados. Embora o termo protocolo de confiança seja geralmente associado à rede de criptomoeda do Bitcoin, o protocolo de confiança é aqui utilizado para referir-se geralmente a um DLS sem referência a qualquer caso de uso particular. Como introduzido acima, uma rede de protocolo de confiança pode ser fornecida como uma rede de protocolo de confiança pública, uma rede de protocolo de confiança privada ou uma rede de protocolo de confiança de consórcio.

[0031] Em uma rede de protocolo de confiança pública, o processo de consenso é controlado por nós da rede de consenso. Por exemplo, centenas, milhares, até mesmo milhões de entidades podem cooperar uma rede de protocolo de confiança pública, cada uma das quais opera pelo menos um nó na rede de protocolo de confiança pública. Assim, a rede de protocolo de confiança pública pode ser considerada uma rede pública em relação às entidades participantes. Em alguns exemplos, a maioria das entidades (nós) deve assinar cada bloco, para que o bloco de ser válido, e adicionado ao protocolo de confiança (contabilidade distribuída) da rede de protocolo de confiança. Um exemplo de rede de protocolo de confiança pública inclui a rede de Bitcoin, que é uma rede de pagamento peer-to-peer. A rede de Bitcoin utiliza uma contabilidade distribuída, conhecida como protocolo de confiança. Como observado acima, o termo protocolo de confiança, no entanto, é usado para se referir geralmente a contabilidades distribuídas sem referência particular à rede de Bitcoin.

[0032] Em geral, uma rede de protocolo de confiança pública suporta transações públicas. Uma transação pública é compartilhada com todos os nós dentro da rede de protocolo de confiança pública e é armazenada em um protocolo de confiança global. Um protocolo de confiança global é um protocolo de confiança que é replicado em todos os nós. Ou seja, todos os nós estão em perfeito estado de consenso em relação ao protocolo de confiança global. Para chegar no consenso (por exemplo, concordar com a adição de um bloco a um protocolo de confiança), um protocolo de consenso é implementado dentro da rede de protocolo de confiança pública. Um exemplo de protocolo de consenso inclui, sem limitação, prova de trabalho (POW) implementada na rede de Bitcoin.

[0033] Em geral, uma rede de protocolo de confiança privada é fornecida para uma entidade particular, que controla centralmente as permissões de leitura e gravação. A entidade controla quais nós são capazes de participar da rede de protocolo de confiança. Consequentemente, as redes de protocolo de confiança privadas são geralmente referidas como redes com permissão que colocam restrições sobre quem tem permissão para participar da rede, e sobre o seu nível de participação (por exemplo, apenas em certas transações). Vários tipos de mecanismos de controle de acesso podem ser usados (por exemplo, os participantes existentes votam na adição de novas entidades, uma autoridade reguladora pode controlar a admissão).

[0034] Em geral, uma rede de protocolo de confiança de consórcio é privada entre as entidades participantes. Em uma rede de protocolo de confiança de consórcio, o processo de consenso é controlado por um conjunto autorizado de nós, um ou mais nós sendo operados por uma entidade respectiva (por exemplo, uma instituição financeira, companhia de seguros). Por exemplo, um consórcio de dez (10) entidades (por exemplo, uma instituição financeira, companhia de seguros) pode operar uma rede de protocolo de confiança de consórcio, cada uma operando pelo menos um nó na rede de protocolo de confiança de consórcio. Nesse sentido, a rede de protocolo de confiança de consórcio pode ser considerada uma rede privada em relação às entidades participantes. Em alguns exemplos, cada entidade (nó) deve assinar todos os blocos para que o bloco seja válido e adicionada ao protocolo de confiança. Em alguns exemplos, pelo menos um subconjunto de entidades (nós) (por exemplo, pelo menos 7 entidades) deve assinar todos os blocos para que o bloco seja válido e adicionado ao protocolo de confiança.

[0035] As realizações da presente invenção são aqui descritas em mais detalhe com referência a uma rede de protocolo de confiança de consórcio. Está contemplado, no entanto, que as realizações da presente invenção podem ser realizadas em qualquer tipo apropriado de rede de protocolo de confiança.

[0036] As realizações da presente invenção são aqui descritas em maior detalhe tendo em vista o contexto acima. Mais particularmente, e como apresentado acima, as realizações da presente invenção destinam-se a um esquema de nome de domínio para interações de cadeia cruzada em sistemas de protocolo de confiança.

[0037] Várias plataformas de protocolo de confiança, ambientes ou produtos foram desenvolvidos com base em diferentes tecnologias protocolo de confiança. Exemplos de produtos de protocolo de confiança incluem Ethereum e Bitcoin. A rede de protocolo de confiança atual inclui múltiplos casos de protocolo de confiança implantados com base nos diferentes produtos de protocolo de confiança. Por exemplo, a rede de protocolo de confiança atual inclui múltiplos casos de protocolo de confiança como protocolos de confiança públicos, protocolos de confiança privados, ou protocolos de confiança de consórcio que são desenvolvidos com base em tecnologias Ethereum ou Bitcoin.

[0038] O modo de acesso atual de cada caso de protocolo de confiança requer acesso de um nó cliente (também chamado de terminal do cliente) do protocolo de confiança ou de seus componentes técnicos, como os SDKs. Para se conectar com precisão a um caso de protocolo de confiança específico, o cliente necessita carregar as suas configurações de rede de protocolo de confiança. Essas configurações de rede de protocolo de confiança são tipicamente hash, certificados de membros, etc. Essas configurações são ilegíveis para humanos e é difícil identificar quais cadeias as configurações identificam.

[0039] A presente invenção fornece um esquema de nome de domínio para a rede de protocolo de confiança. Especificamente, um nome de domínio do protocolo de confiança unificado (UBCDN) é fornecido para servir como um identificador exclusivo de cada caso de protocolo de confiança (também referido como um caso de rede de protocolo de confiança ou cadeia) na rede de protocolo de confiança. Um caso de protocolo de confiança pode ser, por exemplo, uma implementação ou prática de um protocolo de confiança baseado em uma plataforma protocolo de confiança ou tecnologia (por exemplo, Ethereum). Cada UBCDN unicamente vincula um nome de domínio de um caso de protocolo de confiança (também conhecido como um nome de domínio do protocolo de confiança) com uma configuração de rede correspondente do caso de protocolo de confiança (também referido como uma configuração de rede de protocolo de confiança). Em algumas realizações, a configuração de rede de protocolo de confiança pode ser representada ou indicada por um identificador de cadeia. Um nó cliente de um caso de protocolo de confiança pode obter uma configuração de rede de protocolo de confiança correspondente, analisando o UBCDN para identificar o identificador da cadeia. Com base da configuração da rede de protocolo de confiança, o nó cliente pode conectar-se a, ou de outra forma acessar, o caso específico do protocolo de confiança.

[0040] O esquema de nome de domínio descrito pode fornecer um protocolo unificado para interações entre sistemas de protocolo de confiança em uma rede de protocolo de confiança unificada (ou global) que inclui múltiplas ou todos os casos de protocolo de confiança implantados, com base em diferentes produtos ou tecnologias de protocolo de confiança. Todos os casos de protocolo de confiança na rede de protocolo de confiança unificada seguem o mesmo esquema de nome de domínio e são atribuídos UBCDNs exclusivos. Em algumas realizações, cada caso de protocolo de confiança na rede de protocolo de confiança unificada é atribuído um único UBCDN que pode ser reconhecido por todos os casos de protocolo de confiança na rede de protocolo de confiança unificada, independentemente de diferentes plataformas, tecnologias, ou retransmissores que são usadas na rede de protocolo de confiança unificada. Em algumas realizações, o UBCDN define um domínio de autonomia administrativa, autoridade ou controle de um caso de protocolo de confiança dentro da rede de protocolo de confiança unificada. Em algumas realizações, a rede de protocolo de confiança unificada pode ser considerada como uma contrapartida da Internet na rede IP, enquanto o UBCDN pode ser considerado como um mapeamento de um nome de domínio de um recurso de IP na rede de IP com um endereço de IP do Recurso de IP.

[0041] Cada caso de protocolo de confiança na rede de protocolo de confiança unificada pode ser identificado exclusivamente por um UBCDN correspondente, de modo a facilitar as comunicações de cadeia múltipla ou cruzada. Por exemplo, ao contrário de realizações de cadeia cruzada existentes como COSMOS, que usa uma cadeia de retransmissor para interações de cadeia cruzada, na qual cada protocolo de confiança é atribuído a um identificador (ID) dentro da rede de cadeia de retransmissor, mas o ID tem apenas um escopo local e não pode ser reutilizado em outras redes de cadeias de retransmissor, no esquema de nome de domínio descrito, o UBCDN pode ser usado e é reconhecido globalmente por todos os casos protocolo de confiança na rede de protocolo de confiança unificada, apesar de quantas cadeias de retransmissor estão incluídas na rede de protocolo de confiança unificada.

[0042] Além disso, o esquema de nomes de domínio descrito simplifica o protocolo de identificação ou endereçamento para interações de cadeia cruzada em sistemas de protocolo de confiança. Por exemplo, no esquema de nome de domínio descrito, um único UBCDN é suficiente para identificar de forma exclusiva um caso de protocolo de confiança e é reconhecível globalmente por todos os casos de protocolo de confiança na rede de protocolo de confiança unificada para interações entre diferentes redes de protocolo de confiança, enquanto que no COSMOS um caso de protocolo de confiança é designado a múltiplos IDs diferentes quando o caso de protocolo de confiança se associa a múltiplas cadeias de retransmissores para o caso de protocolo de confiança interagir com outros protocolos de confiança.

[0043] Além disso, o UBCDN pode incluir um identificador ou rótulo legível por humanos, ajudando os usuários a memorizar e chegar a um caso de protocolo de confiança facilmente, e assim promove a adoção ou o uso do caso de protocolo de confiança. Por exemplo, operadores ou proprietários de protocolos de confiança públicos, protocolos de confiança privados ou protocolos de confiança de consórcio podem escolher nomes de domínio do protocolo de confiança que correspondem aos seus nomes, ajudando os usuários a lembrar os identificadores dos casos de protocolo de confiança, e ainda facilita a tradução, resolução, ou outra identificação do identificadores de cadeia correspondentes aos nomes de domínio do protocolo de confiança, acelerando as interações de cadeia cruzada na rede de protocolo de confiança unificada.

[0044] Além de fornecer nomes facilmente reconhecíveis e memorizável para identificar casos de protocolo de confiança, o UBCDN permite que um caso de protocolo de confiança mantenha seu nome de domínio do protocolo de confiança mesmo que a configuração de rede subjacente do caso de protocolo de confiança seja alterado (por exemplo, por atualização do sistema ou movimentação ou migração para um local físico diferente na topologia de endereços da rede). No caso de tal mudança ou atualização, o identificador de cadeia do caso de protocolo de confiança pode ser alterado enquanto o nome de domínio do protocolo de confiança pode permanecer o mesmo. O proprietário de UBCDN pode alterar o mapeamento do nome de domínio do protocolo de confiança ao identificador de cadeia atualizado e permitir que outros (por exemplo, outros casos de protocolo de confiança ou nós clientes) utilizem o mesmo nome de domínio do protocolo de confiança para se referir e acessar o caso de protocolo de confiança.

[0045] A Figura 1 representa um exemplo de ambiente (100) que pode ser utilizado para executar realizações da presente invenção. Em alguns exemplos, o ambiente de exemplo (100) permite que entidades participem em uma rede de protocolo de confiança de consórcio (102). O ambiente de exemplo (100) inclui sistemas ou dispositivos de computação (106, 108) e uma rede (110). Em alguns exemplos, a rede (110) inclui uma rede de área local (LAN), rede de longa distância (WAN), a Internet ou uma combinação dos mesmos, e conecta web sites, dispositivos de usuário (por exemplo, dispositivos de computação) e sistema de back-end. Em alguns exemplos, a rede (110) pode ser acessada através de um link de comunicação com fio e/ ou sem fio.

[0046] No exemplo descrito, os sistemas de computação (106, 108) podem incluir qualquer sistema de computação apropriado que permita a participação como um nó na rede de protocolo de confiança de consórcio (102). Exemplos de dispositivos de computação incluem, sem limitação, um servidor, um computador de mesa, um computador laptop, um dispositivo de computação de tablet e um smartphone. Em alguns exemplos, os sistemas de computação (106, 108) hospedam um ou mais serviços implementados por computador para interagir com a rede de protocolo de confiança de consórcio (102). Por exemplo, o sistema de computação (106) pode hospedar serviços implementados por computador de uma primeira entidade (por exemplo, usuário A), como um sistema de gerenciamento de transações que a primeira entidade usa para gerenciar suas transações com uma ou mais entidades (por exemplo, outros usuários). O sistema de computação (108) pode hospedar serviços implementados por computador de uma segunda entidade (por exemplo, usuário B), como um sistema de gerenciamento de transação que a segunda entidade usa para gerenciar suas transações com uma ou mais outras entidades (por exemplo, outros usuários). No exemplo da Figura 1, a rede de protocolo de confiança de consórcio (102) é representada como uma rede peer-to-peer de nós, e os sistemas de computação (106, 108) fornecem nós da primeira entidade e segunda entidade, respectivamente, que participam na rede de protocolo de confiança de consórcio (102).

[0047] A Figura 2 ilustra um exemplo de arquitetura conceptual (200) de acordo com realizações da presente invenção. A arquitetura conceitual exemplificativa (200) inclui uma camada de entidade (202), uma camada de serviços hospedados (204) e uma camada de rede de protocolo de confiança (206). No exemplo representado, a camada de entidade (202) inclui três entidades, Entity_1 (E1), Entity_2 (E2) e Entity_3 (E3), cada entidade possuindo um respectivo sistema de gestão de transações (208).

[0048] No exemplo descrito, a camada de serviços hospedados (204) inclui interfaces (210) para cada sistema de gestão de transações (208). Em alguns exemplos, um sistema de gestão de transações (208) respetivo comunica com uma respetiva interface (210) através de uma rede (por exemplo, a rede (110) da Figura 1) usando um protocolo (por exemplo, protocolo de transferência de hipertexto seguro (HTTPS)). Em alguns exemplos, cada interface (210) fornece uma conexão de comunicação entre um sistema de gestão da respectiva transação (208), e a camada de rede de protocolo de confiança (206). Mais particularmente, a interface (210) se comunica com uma rede de protocolo de confiança (212) da camada de rede de protocolo de confiança (206). Em alguns exemplos, a comunicação entre uma interface (210) e a camada de rede de protocolo de confiança (206) é conduzida utilizando chamadas de procedimento remoto (RPCs). Em alguns exemplos, as interfaces (210) "hospedam" os nós de rede de protocolo de confiança para os respectivos sistemas de gestão de transação (208). Por exemplo, as interfaces (210) fornecem a interface de programação de aplicativos (API) para acessar a rede de protocolo de confiança (212).

[0049] Como aqui descrito, a rede de protocolo de confiança (212) é fornecida como uma rede peer-to-peer incluindo um número de nós (214) que gravam informações de forma imutável em um protocolo de confiança (216). Embora um único protocolo de confiança (216) seja esquematicamente representado, várias cópias do protocolo de confiança (216) são fornecidas, e são mantidas através da rede de protocolo de confiança (212). Por exemplo, cada nó (214) armazena uma cópia do protocolo de confiança. Em algumas realizações, o protocolo de confiança (216) armazena informações associadas a transações que são realizadas entre duas ou mais entidades que participam da rede de protocolo de confiança de consórcio.

[0050] A Figura 3 ilustra um exemplo de nome de domínio do protocolo de confiança unificado (UBCDN) (300) de um caso de protocolo de confiança, de acordo com realizações da presente invenção. O UBCDN (300) pode incluir um nome de domínio do protocolo de confiança (310) e um identificador de cadeia correspondente (320) do caso de protocolo de confiança. O nome de domínio do protocolo de confiança (310) pode ser legível por humanos. O identificador de cadeia (320) pode indicar uma configuração de rede de protocolo de confiança do caso de protocolo de confiança e permite o acesso ao caso de protocolo de confiança com base nas configurações de rede de protocolo de confiança. Em algumas realizações, o UBCDN (300) pode incluir campos adicionais ou ser representado como uma string ou outra estrutura de dados.

[0051] O nome de domínio do protocolo de confiança (310) pode ser de fácil utilização. Por exemplo, o nome de domínio do protocolo de confiança (310) pode ser um rótulo baseada em texto que é mais fácil de memorizar do que o correspondente identificador de cadeia numérica (320) (por exemplo, um endereço hexadecimal de 40 caracteres usado nos protocolos Ethereum. Em algumas realizações, o nome de domínio do protocolo de confiança (310) pode ser representado como uma string ou outra estrutura de dados.

[0052] Em algumas realizações, o nome de domínio do protocolo de confiança (310) pode ter uma sintaxe definida para facilitar ainda mais a compreensão da origem, propriedade ou organização do caso de protocolo de confiança subjacente. Por exemplo, o nome de domínio do protocolo de confiança (310) pode ser projetado de maneira semelhante ao nome de domínio na rede de IP. O nome de domínio do protocolo de confiança (310) pode incluir uma ou mais partes ou rótulos. O um ou mais rótulos podem ser concatenados e ter uma hierarquia de domínios descendente do rótulo da direita para a esquerda no nome. Cada rótulo à esquerda especifica uma subdivisão ou subdomínio do domínio para a direita. Por exemplo, um nome de domínio do protocolo de confiança (310) da *cadeia1. organização1* indica que o caso de protocolo de confiança *chain1* subjacente é um subdomínio do domínio da *organização1* e pertence à *organização1.* Em algumas realizações, o nome de domínio do protocolo de confiança (310) pode definir uma sintaxe adicional ou diferente.

[0053] O identificador da cadeia (320) pode incluir um identificador endereçável que é usado para endereçar e acessar o caso de protocolo de confiança na rede de protocolo de confiança. O identificador de cadeia (320) pode indicar uma configuração de rede de protocolo de confiança do caso de protocolo de confiança e permitir o acesso ao caso de protocolo de confiança com base nas configurações de rede de protocolo de confiança. Por exemplo, múltiplos casos de protocolo de confiança podem ser implantados com base na tecnologia Ethereum. O caso de protocolo de confiança pode ser, por exemplo, uma cadeia MainNet, uma cadeia de teste, uma cadeia particular, ou uma cadeia de consórcio. Um cliente Ethereum pode estabelecer uma conexão com um caso de protocolo de confiança Ethereum carregando o bloco de gênese (isto é, o primeiro bloco) do caso de protocolo de confiança Ethereum. O bloco de gênese é equivalente a um identificador único do caso de protocolo de confiança Ethereum. Assim, em algumas realizações, um ou mais campos (por exemplo, um valor hash) do bloco de gênese de um caso de protocolo de confiança Ethereum pode ser extraída como o identificador de cadeia (320) do caso de protocolo de confiança Ethereum. Em algumas realizações, o identificador de cadeia de um caso de protocolo de confiança pode incluir um valor hash de um bloco de gênese do caso de protocolo de confiança, bem como um ID de rede que identifica o caso de protocolo de confiança. Em algumas realizações, o ID da rede permite transações no caso do protocolo de confiança para parecer diferente das outras cadeias, por exemplo, assinando transações de forma diferente, dependendo da ID de rede usava. Como tal, a ID de rede indica uma configuração de rede adicional que pode ser usada para vincular ou, de outra forma, acessar o caso do protocolo de confiança. O identificador da cadeia (320) pode incluir componentes ou campos adicionais ou diferentes, por exemplo, dependendo da tecnologia protocolo de confiança subjacente ou plataforma do caso de protocolo de confiança.

[0054] O UBCDN (300) cria um mapeamento um-para-um do nome de domínio do protocolo de confiança (310) e seu identificador de cadeia correspondente (320) do caso de protocolo de confiança. Dado o nome de domínio do protocolo de confiança (310), o seu identificador de cadeia correspondente (320) pode ser traduzido, resolvido, ou de outro modo identificado, e vice-versa. Como tal, um nó pode acessar o caso de protocolo de confiança com base na configuração de rede de protocolo de confiança indicada pelo identificador de cadeia (320). Como uma analogia, o nome de domínio do protocolo de confiança (310) de um caso de protocolo de confiança é semelhante a um nome de domínio de acordo com o Sistema de Nomes de Domínio (DNS) de um recurso de Protocolo de Internet (IP) (por exemplo, *example.com*) e o identificador de cadeia (320) é semelhante ao endereço de IP da característica de IP na rede de IP.

[0055] Em algumas realizações, para um determinado nome de domínio do protocolo de confiança (310), seu identificador de cadeia correspondente (320) pode ser traduzido, resolvido ou de outra forma identificado usando informações de consulta de UBCDN que estão em cache ou não armazenadas localmente, dentro de um computador de consulta, ou remotamente na rede de protocolo de confiança unificada (por exemplo, em um servidor UBCDN central). As informações de consulta de UBCDN podem incluir múltiplos UBCDN (300), cada UBCDN (300) correspondendo a múltiplos casos de protocolo de confiança. As informações de consulta do UBCDN podem ser armazenadas, por exemplo, em uma tabela de consulta ou em outra estrutura de dados. O um ou mais nós (por exemplo, um nó de cliente, um nó de consenso, ou um nó de retransmissor) ou um servidor na rede de protocolo de confiança unificada pode armazenar informações de consulta de UBCDN. Ao pesquisar com base nas informações de consulta do UBCDN, um identificador de cadeia (320) correspondente a um determinado nome de domínio do protocolo de confiança (310) pode ser identificado e vice-versa.

[0056] Quando a informação de UBCDN é armazenada em cache localmente, o processo de consulta de UBCDN pode ser mais rápido do que realizar uma consulta remota de UBCDN, por exemplo, em um servidor de UBCDN remoto. Em algumas realizações, na última consulta remota de UBCDN, um usuário insere um nome de domínio do protocolo de confiança (310), por exemplo, "*cadeia1. organization1*" em um SDK do dispositivo de computação do usuário (ou seja, o nó cliente). O nó cliente envia uma solicitação ou consulta que inclui o nome de domínio do protocolo de confiança (310) "*cadeia1. organização1*" para um servidor de UBCDN remoto, por exemplo, através da Internet fora da cadeia. Ao receber a solicitação, o servidor remoto de UBCDN procura nas informações de consulta de UBCDN uma entrada correspondente ao nome de domínio do protocolo de confiança (310) "*cadeia1. organização1*" e identifica o identificador de cadeia (320) correspondente ao nome de domínio do protocolo de confiança (310). Em seguida, o servidor de UBCDN remoto responde ao nó cliente com o identificador de cadeia (320) correspondente ao nome de domínio do protocolo de confiança (310), por exemplo, enviando uma resposta incluindo o identificador de cadeia (320) correspondente para o nome de domínio do protocolo de confiança (310) para o nó cliente.

[0057] A Figura 4 ilustra um exemplo de esquema de gerenciamento de UBCDN (400) em uma rede de protocolo de confiança unificada, de acordo com realizações da presente invenção. O exemplo do esquema de gerenciamento de UBCDN (400) pode fornecer confiança e segurança aprimoradas para comunicações de cadeia cruzada baseadas no UBCDN. Em algumas realizações, o exemplo de esquema de gestão de UBCDN (400) conta com uma infraestrutura de chave pública (PKI) para estabelecer confiança na rede de protocolo de confiança unificada.

[0058] Por exemplo, uma autoridade de certificação (CA) (410) (por exemplo, o operador da PKI) pode ser usada. A CA (410) emite um certificado de domínio ("Certif. de Domínio") (420a, 420b e 420c) (coletivamente, certificado de domínio (420)) para cada proprietário de um UBCDN (430a, 430b e 430c) (coletivamente, proprietário de UBCDN (430)). O proprietário UBCDN (430) pode ser, por exemplo, um proprietário ou operador do caso de protocolo de confiança. Como ilustrado, o proprietário UBCDN (430a) é um proprietário de um nome de domínio do protocolo de confiança "Exemplo1.cadeia," o proprietário de UBCDN (430b) é um proprietário de um nome de domínio do protocolo de confiança "Exemplo2.cadeia", e o proprietário de UBCDN (430b) é um proprietário de um nome de domínio do protocolo de confiança "ExemploN.cadeia."

[0059] Em algumas formas de realização, o proprietário de UBCDN (430) pode obter um certificado de domínio (420) através da aplicação aa CA (410) com um pedido de assinatura de certificado (não mostrado na Figura 4). Em algumas realizações, a solicitação de certificado é um documento eletrônico que contém o nome de domínio do protocolo de confiança, as informações do caso de protocolo de confiança (por exemplo, o identificador de cadeia ou outras configurações de rede), e uma chave pública do proprietário de UBCDN (430). Após a verificação de que o proprietário de UBCDN (430) tem o direito de gerir administrativamente o nome de domínio do protocolo de confiança do caso de protocolo de confiança, a CA (410) pode assinar a solicitação, produzindo assim um certificado de domínio público (420). Em algumas realizações, o certificado de domínio (420) pode ser servido para qualquer nó (por exemplo, um nó cliente, um nó consenso ou um nó retransmissor) que gostaria de acessar o caso de protocolo de confiança subjacente do nome de domínio do protocolo de confiança (por exemplo, “Exemplo1. cadeia”) e prova para o nó que a CA (410) confia e emitiu um certificado para o proprietário de UBCDN (430).

[0060] O certificado de domínio (420) pode incluir um nome de domínio do protocolo de confiança (por exemplo, “Exemplo1.cadeia”) e uma chave pública do proprietário de UBCDN (430). O proprietário de UBCDN (430) é o detentor da chave privada correspondente à chave pública. O CA (410) pode assinar digitalmente o nome de domínio do protocolo de confiança e a chave pública do proprietário de UBCDN (430) usando a própria chave privada da CA. O certificado de domínio (420) pode incluir a assinatura digital assinada pela CA (410) no nome de domínio do protocolo de confiança e a chave pública do proprietário de UBCDN (430).

[0061] Como descrito em relação à Figura 3, um UBCDN pode incluir um nome de domínio do protocolo de confiança (por exemplo, “Exemplo1.cadeia”) e um identificador de cadeia correspondente. O proprietário de UBCDN (430) pode publicar o UBCDN e assinar o UBCDN usando a chave privada do proprietário de UBCDN (430). Em algumas realizações, o proprietário de UBCDN (430) publica uma ou mais mensagens de UBCDN (por exemplo, mensagens UBCDN (440A, 450A, 440)) de modo que o UBCDN pode ser autenticado ou verificado.

[0062] Em algumas realizações, as mensagens UBCDN (440) podem incluir o UBCDN, uma assinatura digital de UBCDN resultante, e uma certificado de domínio. O certificado de domínio pode ser o respectivo certificado de domínio (420) recebido da CA (410). O UBCDN pode incluir o nome de domínio do protocolo de confiança e o identificador de cadeia (por exemplo, o nome de domínio do protocolo de confiança (310) e o identificador de cadeia (320), como descrito em relação à Figura 3). Como ilustrado, o proprietário de UBCDN (430a) emite uma mensagem de UBCDN (440a) que inclui o nome de domínio do protocolo de confiança (442a) “Exemplo1.cadeia” e um identificador de cadeia correspondente (444a) “Identificador de Cadeia V0”, uma assinatura digital (446a) e um certificado de domínio (448a). O certificado de domínio (448a) pode ser o certificado de domínio (420a) emitido pela CA (410) e recebido pelo proprietário de UBCDN (430a) da CA (410). A assinatura digital (446a) pode resultar da assinatura do proprietário de UBCDN (430a) do UBCDN (isto é, o nome de domínio do protocolo de confiança (442a) “Exemplo1.cadeia” e um identificador de cadeia correspondente (444a) “Identificador de Cadeia V0”, neste caso) usando a chave privada do proprietário de UBCDN (430a).

[0063] Similarmente, o proprietário UBCDN (430b) emite uma mensagem de UBCDN (440b) que inclui o nome de domínio do protocolo de confiança (442b) “Exemplo2.cadeia” e um identificador de cadeia correspondente (444b) “Identificador de Cadeia Vx”, uma assinatura digital (446b) e um certificado de domínio (448b). O certificado de domínio (448b) pode ser o certificado de domínio (420b) emitido pela CA (410) e recebido pelo proprietário de UBCDN (430b) a partir da CA (410). A assinatura digital (446a) pode resultar de assinatura do proprietário de UBCDN (430b) do UBCDN (isto é, o nome de domínio do protocolo de confiança (442b) “ Exemplo2.cadeia” e um identificador de cadeia (444a) correspondente “Identificador de Cadeia V0” neste caso), utilizando a chave privada do proprietário de UBCDN (430b).

[0064] Em algumas realizações, um processo de autenticação ou verificação pode ser executado, por exemplo, por qualquer nó na rede de protocolo de confiança unificada ou por terceiros para verificar a validade de um UBCDN baseado na mensagem de UBCDN. Isso pode garantir a segurança que é importante para o comércio eletrônico, especialmente em conexão com transações de pagamento móvel para interações de cadeia cruzada em sistemas de protocolo de confiança.

[0065] Em algumas realizações, o processo de autenticação ou verificação pode incluir, por exemplo, a verificação de que o nome de domínio do protocolo de confiança é o mesmo que o nome de domínio do protocolo de confiança no certificado de domínio; verificar se o proprietário de UBCDN (por exemplo, o proprietário de UBCDN (430a)) é o detentor do nome de domínio do protocolo de confiança (por exemplo, "o nome de domínio do protocolo de confiança (442a)" Exemplo1.cadeia") verificando a assinatura digital no UBCDN (por exemplo, a assinatura digital (446a)) usando a chave pública no certificado de domínio (por exemplo, o certificado de domínio (420a)) emitido pela CA (410), e verificar que o certificado de domínio (por exemplo, o certificado de domínio (448a)) é emitido pela CA (410) confiável.

[0066] Em algumas realizações, depois de verificar a validade do UBCDN, por exemplo, com base no processo de autenticação ou verificação, um nó cliente pode usar o UBCDN para interações de cadeia cruzada na rede de protocolo de confiança unificada. Por exemplo, o nó cliente pode receber e ler uma mensagem de UBCDN, verificar a validade ou legalidade do UBCDN e confirmar que o UBCDN é emitido pelo proprietário de UBCDN; e, em seguida, usar o UBCDN para identificar e acessar o caso de protocolo de confiança de forma exclusiva, por exemplo, identificando o identificador de cadeia correspondente ao nome de domínio do protocolo de confiança no UBCDN.

[0067] A Figura 5 ilustra um exemplo de processo (500) para usar um nome de domínio do protocolo de confiança de um caso de protocolo de confiança para interações de cadeia cruzada em uma rede de protocolo de confiança unificada, de acordo com realizações da presente invenção. Em algumas realizações, o exemplo de processo (500) pode ser executado usando um ou mais programas executáveis por computador executados usando um ou mais dispositivos de computação. Para clareza de apresentação, a descrição que se segue descreve geralmente o processo (500) no contexto das outras figuras nesta descrição. Por exemplo, o exemplo de processo (500) pode ser executado por um nó cliente de um primeiro caso de protocolo de confiança, tal como, o sistema de computação (106) ou (108) da rede de protocolo de confiança protocolo de confiança (102), como descrito em relação à Figura 1, ou o nó (214) da rede de protocolo de confiança (212), como descrito em relação Figura 2. No entanto, será entendido que o processo (500) pode ser realizado, por exemplo, por qualquer sistema, ambiente, software e hardware adequados, ou uma combinação de sistemas, ambientes, software e hardware, conforme apropriado. Em algumas realizações, várias etapas do processo (500) podem ser executadas em paralelo, em combinação, em loops ou em qualquer ordem.

[0068] Em (510), um nó cliente de um primeiro caso de protocolo de confiança obtém um nome de domínio do protocolo de confiança de um segundo caso de protocolo de confiança diferente. Em algumas realizações, o primeiro caso de protocolo de confiança e o segundo caso de protocolo de confiança são implementados com base em diferentes plataformas de protocolo de confiança. Em algumas realizações, o primeiro caso de protocolo de confiança e o segundo caso de protocolo de confiança pertencem a diferentes proprietários ou operadores. O primeiro exemplo de protocolo de confiança e o segundo exemplo de protocolo de confiança estão em uma rede de protocolo de confiança unificado incluindo um número de casos de protocolo de confiança que estão ligados em comunicação por dois ou mais retransmissores.

[0069] O nome de domínio do protocolo de confiança é um identificador exclusivo do segundo caso de protocolo de confiança na rede de protocolo de confiança unificada, mesmo que a rede de protocolo de confiança unificada inclua dois ou mais retransmissores. Em algumas realizações, cada um dos números de casos de protocolo de confiança na rede de protocolo de confiança unificada possui apenas um nome de domínio do protocolo de confiança que identifica exclusivamente cada um dos números de casos de protocolo de confiança na rede de protocolo de confiança unificada.

[0070] O nome de domínio do protocolo de confiança inclui um rótulo legível por humanos. Em algumas realizações, o rótulo legível por humanos inclui um rótulo baseado em texto. O nome de domínio do protocolo de confiança corresponde exclusivamente a um identificador de cadeia do segundo caso de protocolo de confiança. O nome de domínio do protocolo de confiança e o identificador de cadeia podem ser representados por um UBCDN tal como o UBCDN (300), como descrito na Figura 3. Como exemplo, o nome de domínio do protocolo de confiança pode ser o nome de domínio do protocolo de confiança (310), enquanto o identificador de cadeia pode ser o identificador de cadeia (320) correspondente no UBCDN (300).

[0071] Em (520), o nó cliente do primeiro caso de protocolo de confiança identifica o identificador de cadeia do segundo caso de protocolo de confiança com base no nome de domínio do protocolo de confiança do segundo caso de protocolo de confiança, em que o identificador de cadeia do segundo caso de protocolo de confiança indica uma configuração de rede de protocolo de confiança do segundo caso de protocolo de confiança. Em algumas realizações, o identificador de cadeia do segundo caso de protocolo de confiança inclui um valor hash de um bloco de gênese do segundo caso de protocolo de confiança e um identificador de rede do segundo caso de protocolo de confiança, por exemplo, como descrito em relação à Figura 3.

[0072] Em algumas realizações, a identificação do identificador de cadeia do segundo caso de protocolo de confiança com base no nome de domínio do protocolo de confiança inclui a identificação do identificador de cadeia do segundo caso de protocolo de confiança de acordo com as informações de consulta armazenadas localmente no nó cliente com base no nome de domínio do protocolo de confiança.

[0073] Em algumas realizações, a identificação do identificador de cadeia do segundo caso de protocolo de confiança com base no nome de domínio do protocolo de confiança inclui a identificação do identificador de cadeia do segundo caso de protocolo de confiança de um servidor de nome de domínio do protocolo de confiança unificado remoto com base no nome de domínio do protocolo de confiança. Por exemplo, o nó cliente do primeiro caso de protocolo de confiança envia uma solicitação ou consulta para o servidor de nome de domínio do protocolo de confiança unificado. A solicitação inclui o nome de domínio do protocolo de confiança para identificar o identificador de cadeia do segundo caso de protocolo de confiança. Em seguida, o nó cliente do primeiro caso de protocolo de confiança recebe, do servidor de nome de domínio do protocolo de confiança unificado, uma resposta à solicitação, em que a resposta inclui o identificador de cadeia do segundo caso de protocolo de confiança.

[0074] Em (530), o nó cliente do primeiro caso de protocolo de confiança acessa o segundo caso de protocolo de confiança com base na configuração de rede de protocolo de confiança indicada pelo identificador de cadeia do segundo caso de protocolo de confiança. Por exemplo, o primeiro caso de protocolo de confiança acessa o segundo caso de protocolo de confiança por meio de um nó cliente do segundo caso de protocolo de confiança com base no valor hash do bloco de gênese do segundo caso de protocolo de confiança indicado pelo identificador de cadeia do segundo caso de protocolo de confiança. Em algumas realizações, o primeiro caso de protocolo de confiança acessa o segundo caso de protocolo de confiança através de um nó cliente do segundo protocolo de confiança usando um retransmissor (por exemplo, um nó de retransmissor ou uma cadeia de retransmissor) ou outro aplicativo que esteja comunicativamente vinculado ao primeiro caso de protocolo de confiança e ao segundo caso de protocolo de confiança.

[0075] Em algumas realizações, para acessar e obter dados do segundo caso de protocolo de confiança, o nó cliente do segundo caso de protocolo de confiança pode configurar uma configuração de rede, como um endereço IP e um número de porta de um nó (por exemplo, um nó de consenso) do segundo protocolo de confiança e o valor hash do bloco de gênese do segundo caso de protocolo de confiança. O nó cliente do segundo caso de protocolo de confiança pode se conectar ao nó do segundo caso de protocolo de confiança através do endereço de IP e o número da porta do nó do segundo caso de protocolo de confiança. O nó cliente do segundo caso de protocolo de confiança pode ler, recuperar, fazer download ou, de outro modo, obter os dados do nó do segundo caso de protocolo de confiança e verificar se os dados obtidos são provenientes do segundo caso de protocolo de confiança, por exemplo, com base em um protocolo de Verificação de Pagamento Simples (SPV) do segundo caso de protocolo de confiança para determinar se os dados obtidos apontam para o valor hash do bloco de gênese do segundo caso de protocolo de confiança.

[0076] Em (540), o nó cliente do primeiro caso de protocolo de confiança executa transações de cadeia cruzada entre o primeiro caso de protocolo de confiança e o segundo caso de protocolo de confiança com base no nome de domínio do protocolo de confiança do segundo caso de protocolo de confiança. Em algumas realizações, a execução de transações de cadeia cruzadas entre o primeiro caso de protocolo de confiança e o segundo caso de protocolo de confiança inclui o envio, pelo primeiro caso de protocolo de confiança, de uma solicitação de cadeia cruzada que inclui o nome de domínio do protocolo de confiança do segundo caso de protocolo de confiança e uma solicitação de dados, para um retransmissor que está comunicativamente ligado ao primeiro caso de protocolo de confiança e ao segundo caso de protocolo de confiança. O retransmissor recebe a solicitação de cadeia cruzada e lê o nome de domínio do protocolo de confiança do segundo caso de protocolo de confiança, carrega a configuração de rede de protocolo de confiança correspondente do segundo caso de protocolo de confiança, usa a configuração para conectar-se ao segundo caso de protocolo de confiança. O retransmissor pode recuperar, baixar ou, de outra forma, receber os dados solicitados do segundo caso de protocolo de confiança e enviar os dados solicitados para o primeiro caso de protocolo de confiança.

[0077] A Figura 6 ilustra um exemplo de processo (600) para autenticar um UBCDN de um caso de protocolo de confiança, de acordo com realizações da presente invenção. Em algumas realizações, o exemplo de processo (600) pode ser executado usando um ou mais programas executáveis por computador executados usando um ou mais dispositivos de computação. Para clareza de apresentação, a descrição que se segue descreve geralmente o processo (600) no contexto das outras figuras nesta descrição. Por exemplo, o exemplo de processo (600) que pode ser executado pelo sistema de computação (106) ou (108) da rede de protocolo de confiança de consórcio (102), como descrito em relação à Figura 1, ou o nó (214) da rede de protocolo de confiança (212), como descrito em relação à Figura 2. No entanto, será entendido que o processo (600) pode ser realizado, por exemplo, por qualquer sistema, ambiente, software e hardware adequados, ou uma combinação de sistemas, ambientes, software e hardware, conforme apropriado. Em algumas realizações, várias etapas do processo (600) podem ser executadas em paralelo, em combinação, em loops ou em qualquer ordem.

[0078] No (610), um sistema de computação obtém uma mensagem de nome de domínio do protocolo de confiança unificado (UBCDN) de um caso de protocolo de confiança. Em algumas realizações, o sistema de computação é um terceiro da rede de protocolo de confiança unificada. Em algumas realizações, o sistema de computação é um nó cliente de um segundo caso de protocolo de confiança diferente do caso de protocolo de confiança na rede de protocolo de confiança unificada.

[0079] A mensagem de UBCDN pode ser, por exemplo, a mensagem de UBCDN (440) como descrito em relação à Figura 4. A mensagem de UBCDN inclui um UBCDN do caso de protocolo de confiança, uma assinatura digital de um proprietário de UBCDN no UBCDN; e um certificado de domínio do UBCDN.

[0080] O UBCDN do caso de protocolo de confiança inclui um nome de domínio do protocolo de confiança do caso de protocolo de confiança, em que o nome de domínio do protocolo de confiança é um identificador exclusivo do caso de protocolo de confiança em uma rede de protocolo de confiança unificado incluindo um número de casos de protocolo de confiança que estão ligados de forma comunicativa por dois ou mais retransmissores. O nome de domínio do protocolo de confiança inclui um rótulo legível por humanos e um identificador de cadeia do caso de protocolo de confiança correspondendo exclusivamente ao nome de domínio do protocolo de confiança.

[0081] Em algumas realizações, o certificado de domínio do UBCDN inclui do nome de domínio do protocolo de confiança do caso de protocolo de confiança, a chave pública do proprietário de UBCDN, e uma assinatura digital da CA no nome de domínio do protocolo de confiança do caso de protocolo de confiança e a chave pública do proprietário de UBCDN.

[0082] Em (620), o sistema de computação verifica se o certificado de domínio do UBCDN é emitido por uma autoridade de certificação (CA) confiável usando uma chave pública da autoridade de certificação. Em algumas realizações, a assinatura digital da autoridade de certificação é obtida pela assinatura da autoridade de certificação no nome de domínio do protocolo de confiança do caso de protocolo de confiança e pela chave pública do proprietário de UBCDN usando uma chave privada da autoridade de certificação correspondente à chave pública da autoridade de certificação. Em algumas realizações, verificar se o certificado de domínio do UBCDN é emitido por uma autoridade de certificação confiável usando uma chave pública da autoridade de certificação, inclui verificar se o certificado de domínio do UBCDN é emitido pela CA usando o certificado de domínio, a assinatura digital da CA e a chave pública da CA.

[0083] Em (630), em resposta a verificação de que o certificado de domínio do UBCDN é emitido pela CA, o sistema de computação verifica se o UBCDN é emitido pelo proprietário de UBCDN usando uma chave pública do proprietário de UBCDN. Em algumas realizações, a assinatura digital do proprietário de UBCDN é obtida pelo proprietário de UBCDN assinando o UBCDN utilizando uma chave privada correspondente à chave pública do proprietário de UBCDN. Em algumas realizações, verificar se o UBCDN do caso de protocolo de confiança é emitido pelo proprietário de UBCDN usando uma chave pública do proprietário de UBCDN, incluindo verificar que o UBCDN é emitido pelo proprietário de UBCDN utilizando o UBCDN, a assinatura digital do proprietário de UBCDN, e a chave pública do proprietário de UBCDN. Por exemplo, o proprietário de UBCDN pode assinar o UBCDN usando a chave privada do proprietário e gerar uma assinatura digital, por exemplo, de acordo com um algoritmo assinado. O sistema de computação como um destinatário da mensagem de UBCDN pode determinar se o UBCDN é emitido pelo proprietário de UBCDN usando o UBCDN, a assinatura digital e a chave pública do proprietário, por exemplo, de acordo com um algoritmo de verificação de assinatura.

[0084] Em (640), em resposta a verificar que o UBCDN é emitido pelo proprietário de UBCDN, o sistema de computação executa transações de cadeia cruzadas entre o caso de protocolo de confiança e o segundo caso de protocolo de confiança com base no nome de domínio do protocolo de confiança do caso de protocolo de confiança, por exemplo, de acordo com o exemplo de processo (500) como descrito em relação à Figura 5.

[0085] A Figura 7 ilustra um exemplo de processo (700) de um proprietário de um UBCDN de um caso de protocolo de confiança (um proprietário de UBCDN), de acordo com realizações da presente invenção. Em algumas realizações, o exemplo de processo (700) pode ser realizado usando um ou mais programas executáveis por computador executados usando um ou mais dispositivos de computação. Para clareza de apresentação, a descrição que se segue descreve geralmente o processo (700) no contexto das outras figuras nesta descrição. Por exemplo, o exemplo de processo (700) pode ser executado pelo proprietário de UBCDN (430) como descrito em relação à Figura 4. No entanto, será entendido que o processo (700) pode ser realizado, por exemplo, por qualquer sistema, ambiente, software e hardware adequados, ou uma combinação de sistemas, ambientes, software e hardware, conforme apropriado. Em algumas realizações, várias etapas do processo (700) podem ser executadas em paralelo, em combinação, em loops ou em qualquer ordem.

[0086] Em (710), um proprietário de um UBCDN de um caso de protocolo de confiança (um proprietário de UBCDN, como o proprietário de UBCDN (430)) obtém, de uma autoridade de certificação confiável (CA) (por exemplo, a CA (410)), um certificado de domínio (por exemplo, o certificado de domínio (420)) do UBCDN do caso de protocolo de confiança. O UBCDN do caso de protocolo de confiança inclui um nome de domínio do protocolo de confiança do caso de protocolo de confiança e um identificador de cadeia do caso de protocolo de confiança correspondente exclusivamente para o nome de domínio do protocolo de confiança. O UBCDN pode ser, por exemplo, o UBCDN (300), como descrito em relação à Figura 3. O nome de domínio do protocolo de confiança é um identificador exclusivo do caso de protocolo de confiança em uma rede de protocolo de confiança unificada, incluindo um número de casos de protocolo de confiança que estão comunicativamente ligadas por dois ou mais retransmissores. Em algumas realizações, o nome de domínio do protocolo de confiança inclui um rótulo legível por humanos. O identificador da cadeia indica uma configuração de rede de protocolo de confiança do caso de protocolo de confiança.

[0087] O certificado de domínio do UBCDN inclui o nome de domínio do protocolo de confiança do caso de protocolo de confiança, uma chave pública do proprietário de UBCDN, e uma assinatura digital da CA no nome de domínio do protocolo de confiança do caso de protocolo de confiança e a chave pública do proprietário de UBCDN. O certificado de domínio do UBCDN pode ser, por exemplo, o certificado de domínio (420), como descrito em relação à Figura 4

[0088] Em (720), o proprietário de UBCDN assina o UBCDN do caso de protocolo de confiança, por exemplo, usando a chave privada do proprietário de UBCDN, por exemplo, de acordo com um algoritmo de assinatura.

[0089] Em (730), o proprietário de UBCDN publica uma mensagem de UBCDN (por exemplo, a mensagem de UBCDN (440a ou 440b)) do caso de protocolo de confiança. A mensagem de UBCDN inclui o UBCDN do caso de protocolo de confiança, uma assinatura digital do proprietário de UBCDN resultante da assinatura do UBCDN, e o certificado de domínio do

UBCDN.

[0090] Em (740), o proprietário de UBCDN identifica um identificador de cadeia atualizado do caso de protocolo de confiança indicando uma configuração de rede de protocolo de confiança atualizada do caso de protocolo de confiança. Por exemplo, uma alteração ou atualização da configuração de rede de protocolo de confiança do caso de protocolo de confiança pode ocorrer (por exemplo, devido à atualização do sistema ou à movimentação da localização física de um ou mais dispositivos de computação, como o bloco de gênese). O identificador de cadeia pode ser atualizado para refletir a atualização da configuração de rede de protocolo de confiança do caso de protocolo de confiança (por exemplo, atualizando o valor hash do bloco de gênese do caso de protocolo de confiança). Por exemplo, como ilustrado na Figura 4, para o mesmo nome de domínio do protocolo de confiança (442a) “Exemplo1.cadeia,” o identificador de cadeia (444a) “Identificador de Cadeia V0” foi atualizado para um identificador de cadeia (454a) “Identificador de Cadeia V1”, para refletir a alteração da configuração de rede de protocolo de confiança do caso de protocolo de confiança.

[0091] Em (750), o proprietário de UBCDN assina um UBCDN atualizado do caso de protocolo de confiança, por exemplo, usando a chave privada do proprietário de UBCDN. O UBCDN atualizado do caso de protocolo de confiança inclui o nome de domínio do protocolo de confiança do caso de protocolo de confiança e o identificador de cadeia atualizado do caso de protocolo de confiança. Por exemplo, como ilustrado na Figura 4, o UBCDN atualizado do caso de protocolo de confiança inclui o mesmo nome de domínio do protocolo de confiança (442a) “Exemplo1.cadeia” e o identificador de cadeia atualizado (454a) “Cadeia Identificador V1”.

[0092] Em (760), o proprietário de UBCDN publica uma mensagem de UBCDN atualizada do caso de protocolo de confiança. A mensagem de UBCDN atualizada inclui o UBCDN atualizado do caso de protocolo de confiança, uma assinatura digital atualizada do proprietário de UBCDN resultante da assinatura do UBCDN atualizado, e o certificado de domínio do UBCDN. Por exemplo, como representado na Figura 4, o proprietário do UBCDN (430a) emite uma mensagem atualizada de UBCDN (450a) que inclui o nome de domínio do protocolo de confiança (442a) “Exemplo1.cadeia” e o identificador de cadeia atualizado (454a) “Identificador de cadeia V1”, uma assinatura digital (456a) e um certificado de domínio (458a). O certificado de domínio (458a) pode ser o certificado de domínio (420a) emitido pela CA (410) e recebido pelo proprietário de UBCDN (430a) da CA (410). A assinatura digital atualizada (456a) pode resultar da assinatura pelo proprietário de UBCDN (430a) do UBCDN atualizado (isto é, o nome de domínio do protocolo de confiança (442a) “Exemplo1.cadeia” e o identificador de cadeia atualizado (454a) “Identificador de Cadeia V0” neste caso) usando a chave privada do proprietário de UBCDN (430a).

[0093] A Figura 8 ilustra um exemplo de processo (800) de um retransmissor para interações de cadeia cruzada em uma rede de protocolo de confiança unificada, de acordo com realizações da presente invenção. A rede de protocolo de confiança unificada inclui múltiplos casos de protocolo de confiança que estão ligados de forma comunicativa por dois ou mais retransmissores. Em algumas realizações, o exemplo de processo (800) pode ser realizado usando um ou mais programas executáveis por computador executados usando um ou mais dispositivos de computação. Para clareza de apresentação, a descrição que se segue descreve geralmente o processo (800) no contexto das outras figuras nesta descrição. Por exemplo, o exemplo de processo (800), que pode ser executado pelo retransmissor em uma rede de protocolo de confiança unificada. Contudo, será entendido que o processo (800) pode ser executado, por exemplo, por qualquer sistema, ambiente, software e hardware adequados, ou uma combinação de sistemas, ambientes, software e hardware, conforme apropriado. Por exemplo, o retransmissor pode ser um nó (por exemplo, o sistema de computação (106) ou (108) como descrito em relação à Figura 1 ou o nó (214) como descrito em relação à Figura 2), um caso de protocolo de confiança (por exemplo, uma rede de protocolo de confiança (102) ou a rede de protocolo de confiança (212)), ou outro sistema de computador na rede de protocolo de confiança unificada. Em algumas realizações, várias etapas do processo (800) podem ser executadas em paralelo, em combinação, em loops ou em qualquer ordem.

[0094] Em (810), o retransmissor, que está ligado de forma comunicativa a um primeiro caso de protocolo de confiança e a um segundo caso de protocolo de confiança na rede de protocolo de confiança unificada, identifica um nome de domínio do protocolo de confiança de um primeiro caso de protocolo de confiança. O nome de domínio do protocolo de confiança do primeiro caso de protocolo de confiança é um identificador exclusivo do primeiro caso de protocolo de confiança e corresponde exclusivamente a um identificador de cadeia do primeiro caso de protocolo de confiança na rede de protocolo de confiança unificada. Em algumas realizações, o nome de domínio do protocolo de confiança do primeiro caso de protocolo de confiança inclui um primeiro rótulo legível por humanos.

[0095] Em (820), o retransmissor identifica um nome de domínio do protocolo de confiança do segundo caso de protocolo de confiança. O nome de domínio do protocolo de confiança do segundo caso de protocolo de confiança é um identificador exclusivo do segundo caso de protocolo de confiança e corresponde exclusivamente a um identificador de cadeia do segundo caso de protocolo de confiança na rede de protocolo de confiança unificada. Em algumas realizações, o nome de domínio do protocolo de confiança do segundo caso de protocolo de confiança inclui um segundo rótulo legível por humanos.

[0096] Em algumas realizações, um retransmissor pode designar um identificador local para cada protocolo de confiança que está ligado de forma comunicativa. O identificador local é designado para o uso do retransmissor e não pode ser usado por outros nós ou retransmissores na rede de protocolo de confiança unificada. Em algumas realizações, identificar um nome de domínio do protocolo de confiança do primeiro caso de protocolo de confiança inclui utilizar o nome de domínio do protocolo de confiança do primeiro caso de protocolo de confiança como o identificador local do primeiro caso de protocolo de confiança ou substituir a identificador local do primeiro caso de protocolo de confiança com o nome de domínio do protocolo de confiança do primeiro caso de protocolo de confiança. Da mesma forma, a identificação de um nome de domínio do protocolo de confiança do segundo caso de protocolo de confiança inclui o uso do nome de domínio do protocolo de confiança do segundo caso de protocolo de confiança como o identificador local do segundo caso de protocolo de confiança ou a substituição do identificador exclusivo do segundo caso de protocolo de confiança pelo nome de domínio do protocolo de confiança do segundo caso de protocolo de confiança.

[0097] Em (830), o retransmissor recebe uma solicitação de acesso para acessar o segundo caso do protocolo de confiança. O pedido de acesso inclui do nome de domínio do protocolo de confiança do segundo caso de protocolo de confiança.

[0098] Em (840), o retransmissor identifica o identificador de cadeia do segundo caso de protocolo de confiança com base no nome de domínio do protocolo de confiança do segundo caso de protocolo de confiança. O identificador de cadeia do segundo caso de protocolo de confiança indica uma configuração de rede de protocolo de confiança do segundo caso de protocolo de confiança.

[0099] Em algumas realizações, a identificação do identificador de cadeia do segundo caso de protocolo de confiança com base no nome de domínio do protocolo de confiança do segundo caso de protocolo de confiança inclui a identificação do identificador da cadeia do segundo caso de protocolo de confiança, de acordo com as informações de consulta armazenadas localmente no retransmissor com base no nome de domínio do protocolo de confiança.

[00100] Em algumas realizações, identificar o identificador de cadeia do segundo caso de protocolo de confiança com base no nome de domínio do protocolo de confiança do segundo caso de protocolo de confiança inclui a identificação do identificador de cadeia do segundo caso de protocolo de confiança com base no nome de domínio do protocolo de confiança do segundo caso de protocolo de confiança de um servidor remoto de nome de domínio do protocolo de confiança unificado.

[00101] Em (850), o retransmissor fornece acesso ao segundo caso de protocolo de confiança para o primeiro caso de protocolo de confiança com base na configuração de rede de protocolo de confiança indicada pelo identificador de cadeia do segundo caso de protocolo de confiança. Em algumas realizações, o retransmissor fornece acesso ao segundo caso de protocolo de confiança para o primeiro caso de protocolo de confiança de acordo com um protocolo de comunicação concebido para interações de cadeia cruzada. Por exemplo, o retransmissor pode carregar a configuração de rede de protocolo de confiança indicada pelo identificador de cadeia do segundo caso de protocolo de confiança correspondente ao nome de domínio do protocolo de confiança do segundo caso de protocolo de confiança. O retransmissor usa a configuração de rede de protocolo de confiança para se conectar ao segundo caso de protocolo de confiança, obtém um resultado

solicitado pelo primeiro caso de protocolo de confiança do segundo caso de protocolo de confiança e retorna o resultado solicitado pelo primeiro caso de protocolo de confiança ao primeiro caso de protocolo de confiança, por exemplo, de acordo os exemplos de técnicas descritas em relação à Figura 5.

[00102] Em algumas realizações, fornecer, pelo retransmissor, acesso ao segundo caso de protocolo de confiança para o primeiro caso de protocolo de confiança com base na configuração de rede de protocolo de confiança indicada pelo identificador da cadeia do segundo caso de protocolo de confiança inclui o fornecimento, pelo retransmissor, do acesso ao segundo caso de protocolo de confiança ao primeiro caso de protocolo de confiança através de um segundo retransmissor.

[00103] Em algumas realizações, a configuração de rede de protocolo de confiança indicada pelo identificador de cadeia do segundo caso de protocolo de confiança é identificada pelo segundo retransmissor com base no mesmo identificador de cadeia do segundo caso de protocolo de confiança. Em algumas realizações, o segundo caso de protocolo de confiança é acessado pelo segundo retransmissor baseado na configuração de rede de protocolo de confiança indicada pelo identificador de cadeia do segundo caso de protocolo de confiança. Em outras palavras, o primeiro caso de protocolo de confiança pode usar o mesmo nome de domínio do segundo caso de protocolo de confiança, independentemente de qual retransmissor é, ou quantos retransmissores são usados para interagir com o segundo caso de protocolo de confiança.

[00104] Em algumas realizações, a configuração de rede de protocolo de confiança indicada pelo identificador de cadeia do segundo caso de protocolo de confiança é identificada pelo segundo retransmissor de acordo com a informação de busca armazenada localmente no segundo retransmissor baseado no mesmo identificador de cadeia do segundo caso de protocolo de

confiança.

[00105] Em algumas realizações, a configuração de rede de protocolo de confiança indicada pelo identificador de cadeia do segundo caso de protocolo de confiança é identificada pelo segundo retransmissor baseado no nome de domínio do protocolo de confiança do segundo caso de protocolo de confiança de um nome de domínio unificado de protocolo de confiança remoto servidor.

[00106] As características descritas podem ser implementadas em circuitos eletrônicos digitais ou em hardware de computador, firmware, software ou em combinações dos mesmos. O aparelho pode ser implementado em um produto de programa de computador tangivelmente incorporado em um veículo de informação (por exemplo, em um dispositivo de armazenamento legível por máquina) para realização por um processador programável; e as etapas do método podem ser realizadas por um processador programável executando um programa de instruções para executar funções das realizações descritas operando nos dados de entrada e gerando a saída. As características descritas podem ser implementadas vantajosamente em um ou mais programas de computador que são executáveis em um sistema programável incluindo pelo menos um processador programável acoplado para receber dados e instruções de, e para transmitir dados e instruções a, um sistema de armazenamento de dados, pelo menos um dispositivo de entrada e pelo menos um dispositivo de saída. Um programa de computador é um conjunto de instruções que podem ser usados, direta ou indiretamente, em um computador para realizar uma determinada atividade ou obter um certo resultado. Um programa de computador pode ser escrito em qualquer forma de linguagem de programação, incluindo idiomas compilados ou interpretados, e pode ser implementado de qualquer forma, incluindo como um programa independente ou como um módulo, componente, sub-rotina ou outra unidade adequada para

uso em um ambiente de computação.

[00107] Processadores adequados para a realização de um programa de instruções incluem, a título de exemplo, microprocessadores de uso geral e especial, e o único processador ou um de múltiplos processadores de qualquer tipo de computador. Geralmente, um processador receberá instruções e dados de uma memória somente leitura ou de uma memória de acesso aleatório ou de ambas. Os elementos de um computador podem incluir um processador para executar instruções e uma ou mais memórias para armazenar instruções e dados. Geralmente, um computador pode também incluir, ou está operacionalmente acoplado para se comunicar com, um ou mais dispositivos de armazenamento em massa para armazenar arquivos de dados; tais dispositivos incluem discos magnéticos, como discos rígidos internos e discos removíveis; discos magneto-ópticos; e discos ópticos. Dispositivos de armazenamento adequados para incorporar de forma tangível instruções e dados de programas de computador incluem todas as formas de memória não volátil, incluindo, por exemplo, dispositivos de memória semicondutores, tais como EPROM, EEPROM e dispositivos de memória flash; discos magnéticos, como discos rígidos internos e discos removíveis; discos magneto-ópticos; e discos de CD-ROM e DVD-ROM. O processador e a memória podem ser suplementados por, ou incorporados nos, circuitos integrados específicos de aplicativo (ASICs).

[00108] Para fornecer a interação com um usuário, as características podem ser implementadas em um computador com um dispositivo de exibição, como um monitor de tubo de raio catódico (CRT) ou de cristal líquido (LCD) para exibir informações ao usuário e um teclado e um dispositivo apontador, como um mouse ou uma trackball, pelos quais o usuário pode fornecer entrada para o computador.

[00109] As características podem ser implementadas em um

sistema de computador que inclua um componente de painel administrativo (*back-end*), como um servidor de dados, ou que inclua um componente de middleware, como um servidor de aplicativos ou um servidor da Internet, ou que inclua um componente de interface de interação com o usuário (*front-end*), como um computador cliente com uma interface gráfica do usuário ou um navegador da Internet, ou qualquer combinação deles. Os componentes do sistema podem ser conectados por qualquer forma ou meio de comunicação de dados digitais, como uma rede de comunicação. Exemplos de redes de comunicação incluem, por exemplo, uma rede de área local (LAN), uma rede de longa distância (WAN) e os computadores e redes que formam a Internet.

[00110] O sistema de computador pode incluir clientes e servidores. Um cliente e um servidor geralmente são remotos entre si e geralmente interagem através de uma rede, como a descrita. A relação de cliente e servidor surge em virtude de programas de computador em realização nos respectivos computadores e tendo um relacionamento cliente-servidor entre si.

[00111] Além disso, os fluxos lógicos representados nas figuras não exigem a ordem particular mostrada, ou ordem sequencial, para alcançar os resultados desejados. Além disso, outras etapas podem ser fornecidas, ou etapas podem ser eliminadas, dos fluxos descritos, e outros componentes podem ser adicionados ou removidos dos sistemas descritos. Por conseguinte, outras realizações estão dentro do escopo das reivindicações seguintes.

[00112] Um certo número de realizações da presente invenção foi descrito. No entanto, será entendido que várias modificações podem ser feitas sem se afastar do espírito e escopo da presente invenção. Por conseguinte, outras realizações estão dentro do escopo das seguintes reivindicações.

REIVINDICAÇÕES

1. MÉTODO (500) IMPLEMENTADO POR COMPUTADOR, caracterizado pelo fato de que compreende as etapas de:

obter (510), por um nó cliente de um primeiro caso de protocolo de confiança (*blockchain*), um nome de domínio do protocolo de confiança (310) de um segundo caso de protocolo de confiança diferente, em que:

o nome de domínio do protocolo de confiança (310) é um identificador único do segundo caso de protocolo de confiança em uma rede de protocolo de confiança unificada compreendendo uma pluralidade de casos de protocolo de confiança que são ligados de forma comunicativa por dois ou mais retransmissores;

o nome de domínio do protocolo de confiança (310) compreende um rótulo legível por humanos; e

o nome de domínio do protocolo de confiança (310) corresponde a um identificador de cadeia (320) do segundo caso de protocolo de confiança;

identificar (520) o identificador de cadeia (320) do segundo caso de protocolo de confiança com base no nome de domínio do protocolo de confiança (310) do segundo caso de protocolo de confiança, em que o identificador de cadeia (320) do segundo caso de protocolo de confiança indica uma configuração de rede de protocolo de confiança do segundo caso de protocolo de confiança; e

acessar (530), por meio do nó cliente, o segundo caso de protocolo de confiança com base na configuração de rede de protocolo de confiança indicada pelo identificador de cadeia (320) do segundo caso de protocolo de confiança.

2. MÉTODO (500), de acordo com a reivindicação 1, caracterizado pelo fato de que compreende ainda a realização (540) de transações de cadeia cruzadas entre o primeiro caso de protocolo de confiança

e o segundo caso de protocolo de confiança com base no nome de domínio protocolo de confiança (310) do segundo caso de protocolo de confiança.

3. MÉTODO (500), de acordo com a reivindicação 1, caracterizado pelo fato de que a rótulo legível por humanos compreende um rótulo baseado em texto.

4. MÉTODO (500), de acordo com a reivindicação 1, caracterizado pelo fato de que o identificador de cadeia (320) do segundo caso de protocolo de confiança compreende um valor hash de um bloco de gênese do segundo caso de protocolo de confiança e um identificador de rede do segundo caso de protocolo de confiança.

5. MÉTODO (500), de acordo com a reivindicação 1, caracterizado pelo fato de que cada um da pluralidade de casos de protocolo de confiança na rede de protocolo de confiança unificada tem apenas um nome de domínio do protocolo de confiança (310) que identifica exclusivamente cada um da pluralidade de casos de protocolo de confiança.

6. MÉTODO (500), de acordo com a reivindicação 1, caracterizado pelo fato de que identificar (520) o identificador de cadeia (320) do segundo caso de protocolo de confiança com base no nome de domínio do protocolo de confiança (310) compreende identificar o identificador de cadeia (320) do segundo caso de protocolo de confiança de acordo com informações de consulta armazenadas localmente no nó cliente com base no nome de domínio do protocolo de confiança (310).

7. MÉTODO (500), de acordo com a reivindicação 1, caracterizado pelo fato de que a identificação do identificador de cadeia (320) do segundo caso de protocolo de confiança com base no nome de domínio do protocolo de confiança (310) compreende:

enviar, para um servidor de nome de domínio do protocolo de confiança unificado, uma solicitação que inclui o nome de domínio do protocolo de confiança (310) para identificar o identificador de cadeia (320) do segundo caso de protocolo de confiança; e

receber, do servidor de nome de domínio do protocolo de confiança unificado, uma resposta que inclui o identificador de cadeia (320) do segundo caso de protocolo de confiança.

8. MÉTODO (500), de acordo com a reivindicação 1, caracterizado pelo fato de que o primeiro caso de protocolo de confiança e o segundo caso de protocolo de confiança são implementados com base em diferentes plataformas de protocolo de confiança.

9. MEIO LEGÍVEL POR COMPUTADOR, caracterizado pelo fato de que é acoplado a um ou mais processadores e com instruções armazenadas nele que, quando executadas por um ou mais processadores, fazem com que um ou mais processadores executem operações de acordo com o método, conforme definido em qualquer uma das reivindicações 1 a 8.

10. SISTEMA PARA IMPLEMENTAR UM MÉTODO, caracterizado pelo fato de que inclui:

um dispositivo de computação; e

um dispositivo de armazenamento legível por computador acoplado ao dispositivo de computação e tendo instruções armazenadas nele que, quando executadas pelo dispositivo de computação, fazem com que o dispositivo de computação execute operações de acordo com o método, conforme definido em qualquer uma das reivindicações 1 a 8.

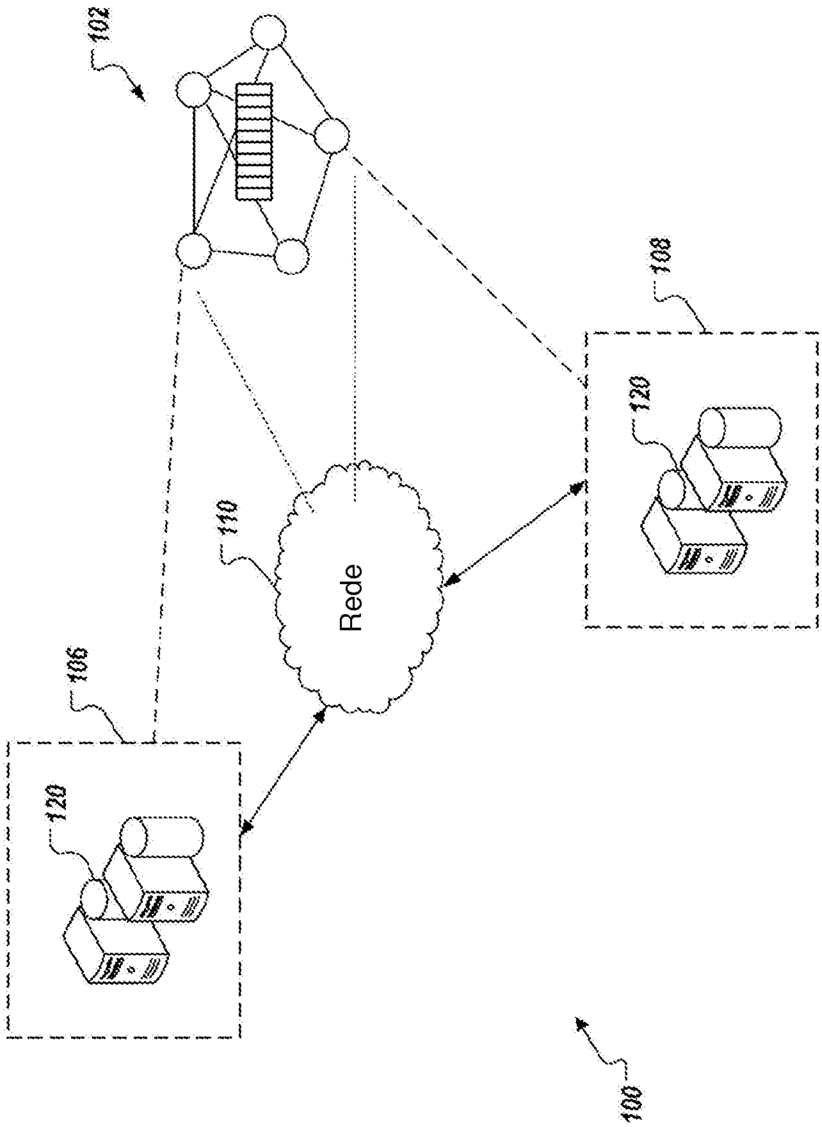


Figura 1

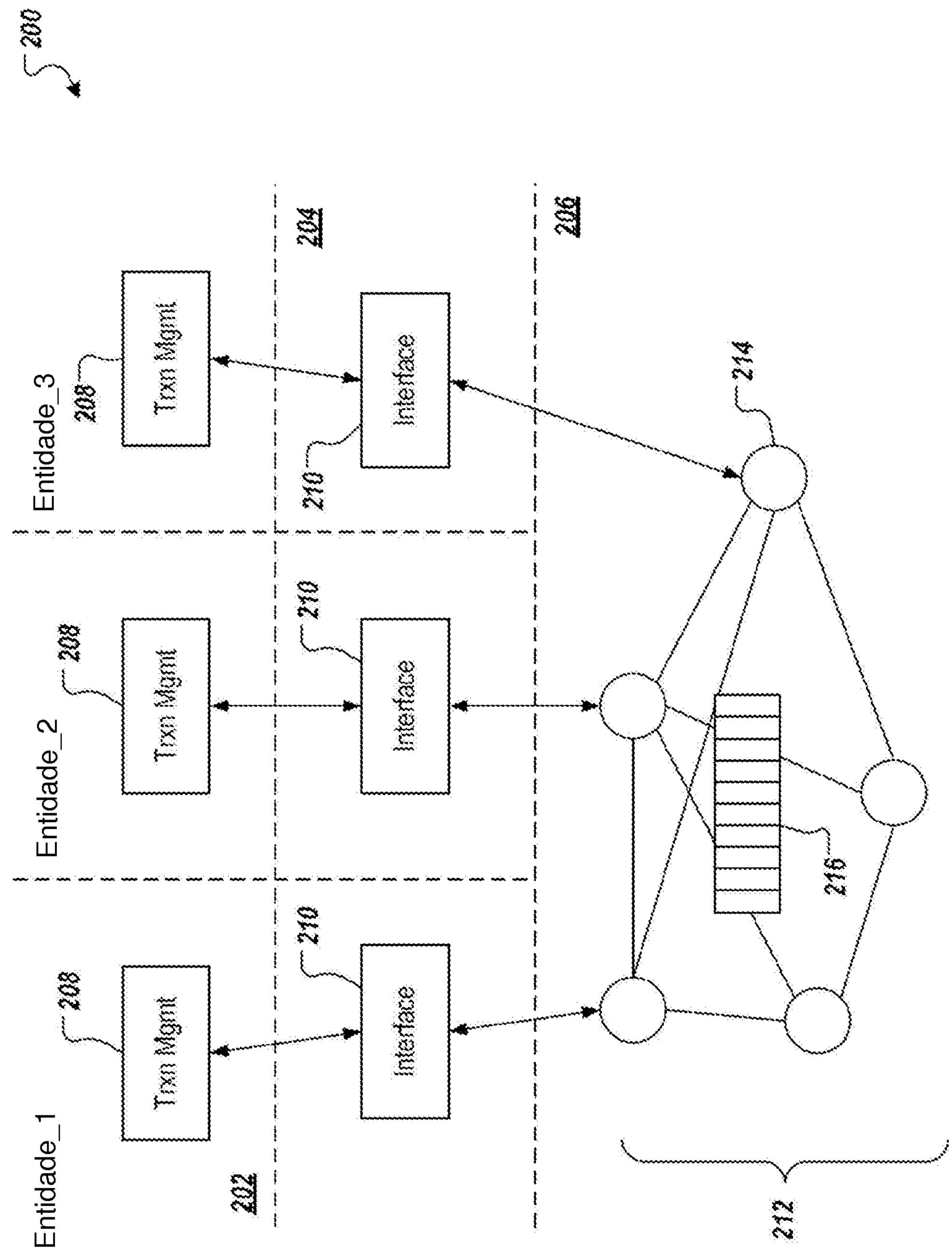

200
Entidade_1
Entidade_2
Entidade_3
Txn Mgmt
Txn Mgmt
Txn Mgmt
Interface
Interface
Interface
202
204
206
208
208
208
210
210
210
212
214
216

Figura 2

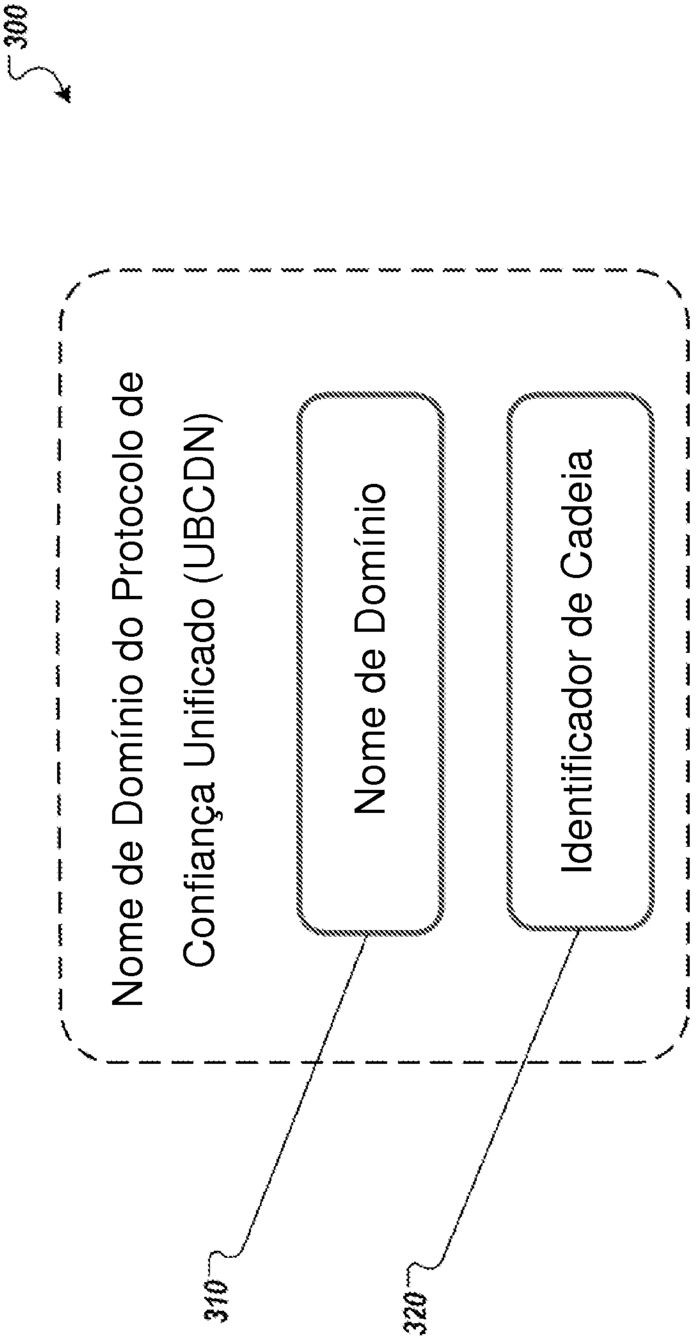

300
Nome de Domínio do Protocolo de Confiança Unificado (UBCDN)
Nome de Domínio
Identificador de Cadeia
310
320

Figura 3

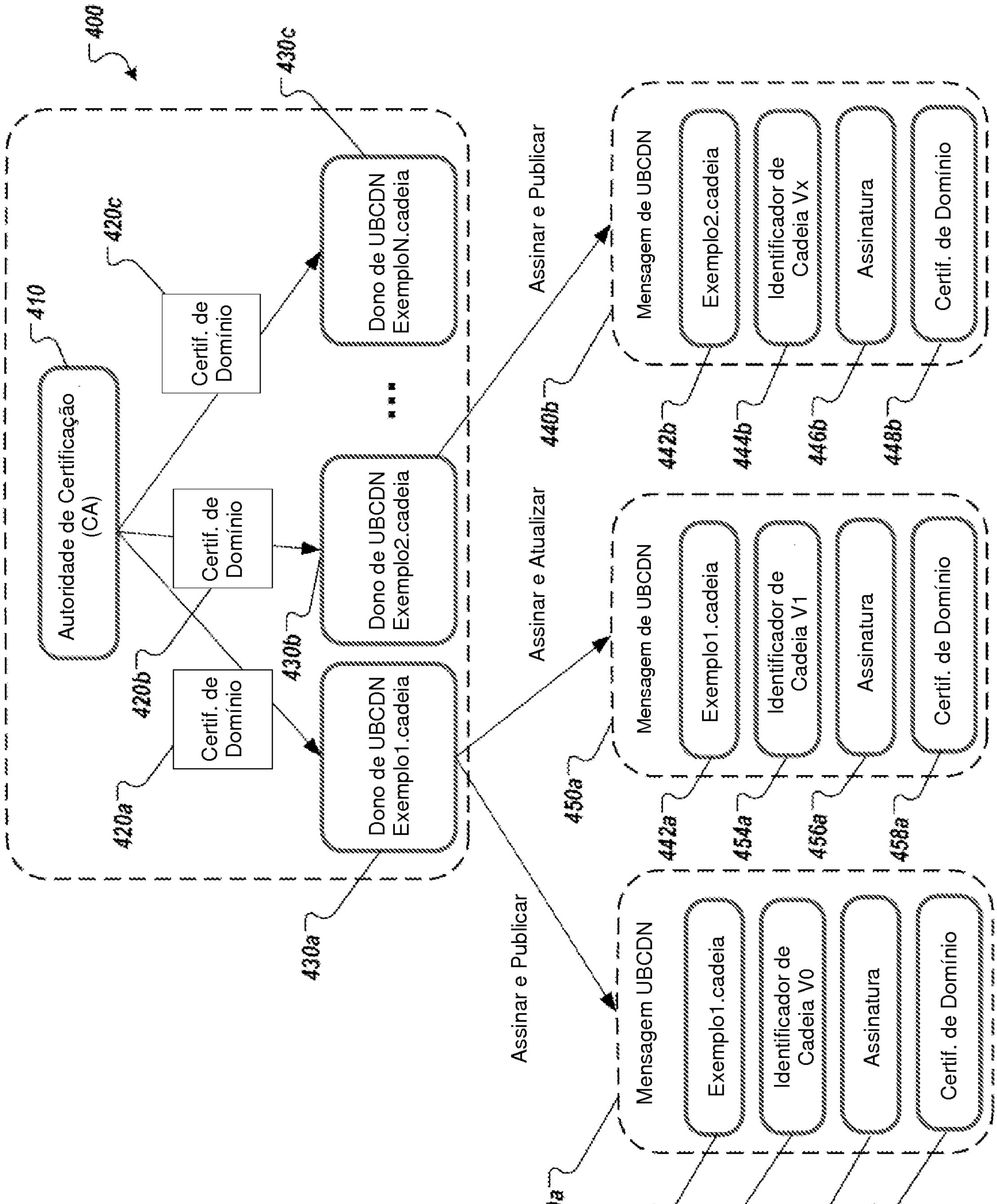

400
Autoridade de Certificação (CA)
410
Certif. de Domínio
420a
Certif. de Domínio
420b
Certif. de Domínio
420c
Dono de UBCDN Exemplo1.cadeia
430a
Dono de UBCDN Exemplo2.cadeia
430b
Dono de UBCDN ExemploN.cadeia
430c
Assinar e Publicar
Assinar e Atualizar
Assinar e Publicar
Mensagem UBCDN
Exemplo1.cadeia
Identificador de Cadeia V0
Assinatura
Certif. de Domínio
440a
442a
444a
446a
448a
Mensagem de UBCDN
Exemplo1.cadeia
Identificador de Cadeia V1
Assinatura
Certif. de Domínio
450a
442a
454a
456a
458a
Mensagem de UBCDN
Exemplo2.cadeia
Identificador de Cadeia Vx
Assinatura
Certif. de Domínio
440b
442b
444b
446b
448b

Figura 4

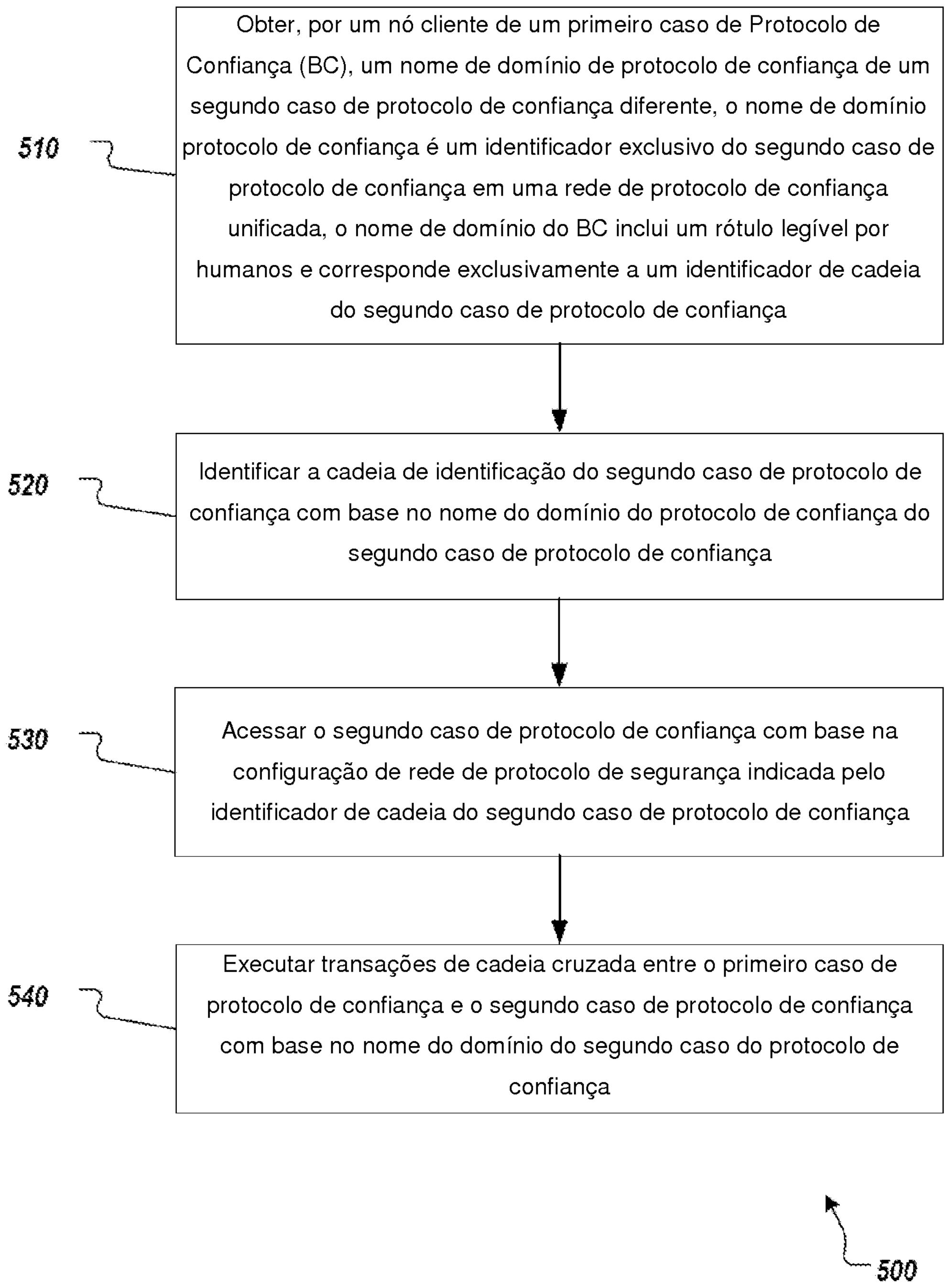

510
Obter, por um nó cliente de um primeiro caso de Protocolo de Confiança (BC), um nome de domínio de protocolo de confiança de um segundo caso de protocolo de confiança diferente, o nome de domínio protocolo de confiança é um identificador exclusivo do segundo caso de protocolo de confiança em uma rede de protocolo de confiança unificada, o nome de domínio do BC inclui um rótulo legível por humanos e corresponde exclusivamente a um identificador de cadeia do segundo caso de protocolo de confiança
520
Identificar a cadeia de identificação do segundo caso de protocolo de confiança com base no nome do domínio do protocolo de confiança do segundo caso de protocolo de confiança
530
Acessar o segundo caso de protocolo de confiança com base na configuração de rede de protocolo de segurança indicada pelo identificador de cadeia do segundo caso de protocolo de confiança
540
Executar transações de cadeia cruzada entre o primeiro caso de protocolo de confiança e o segundo caso de protocolo de confiança com base no nome do domínio do segundo caso do protocolo de confiança
500

Figura 5

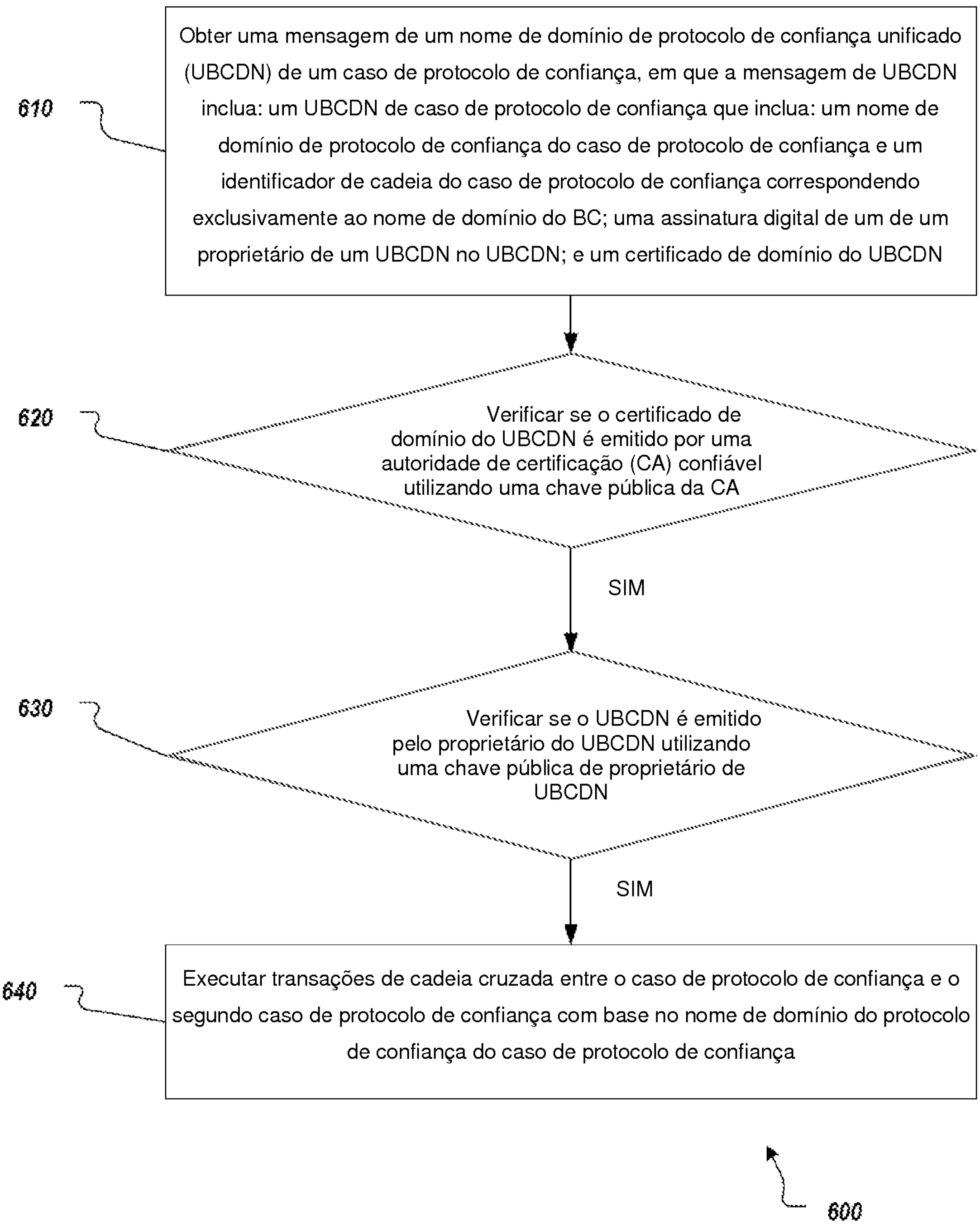

610
Obter uma mensagem de um nome de domínio de protocolo de confiança unificado (UBCDN) de um caso de protocolo de confiança, em que a mensagem de UBCDN inclua: um UBCDN de caso de protocolo de confiança que inclua: um nome de domínio de protocolo de confiança do caso de protocolo de confiança e um identificador de cadeia do caso de protocolo de confiança correspondendo exclusivamente ao nome de domínio do BC; uma assinatura digital de um de um proprietário de um UBCDN no UBCDN; e um certificado de domínio do UBCDN
620
Verificar se o certificado de domínio do UBCDN é emitido por uma autoridade de certificação (CA) confiável utilizando uma chave pública da CA
SIM
630
Verificar se o UBCDN é emitido pelo proprietário do UBCDN utilizando uma chave pública de proprietário de UBCDN
SIM
640
Executar transações de cadeia cruzada entre o caso de protocolo de confiança e o segundo caso de protocolo de confiança com base no nome de domínio do protocolo de confiança do caso de protocolo de confiança
600

Figura 6

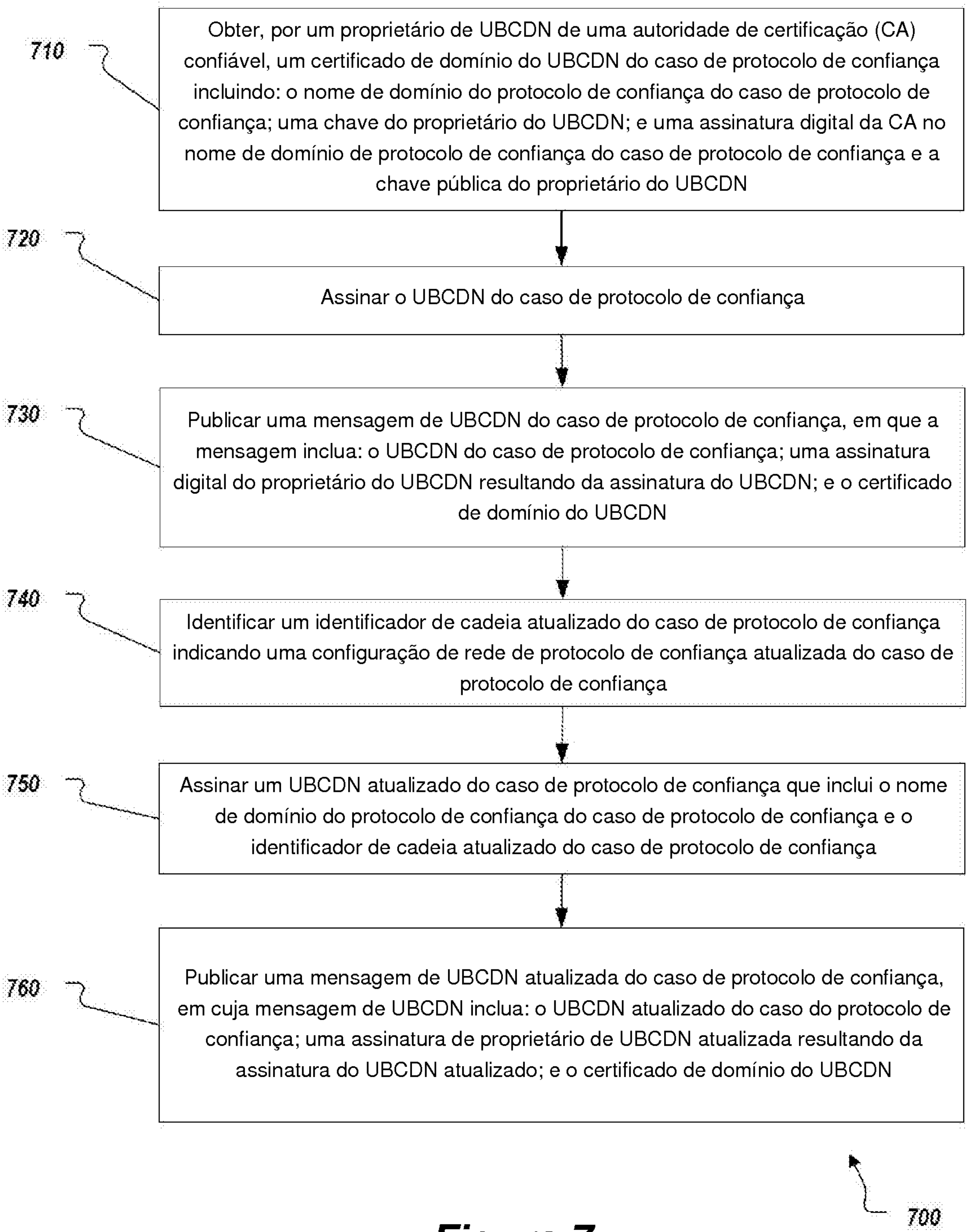

710
Obter, por um proprietário de UBCDN de uma autoridade de certificação (CA) confiável, um certificado de domínio do UBCDN do caso de protocolo de confiança incluindo: o nome de domínio do protocolo de confiança do caso de protocolo de confiança; uma chave do proprietário do UBCDN; e uma assinatura digital da CA no nome de domínio de protocolo de confiança do caso de protocolo de confiança e a chave pública do proprietário do UBCDN
720
Assinar o UBCDN do caso de protocolo de confiança
730
Publicar uma mensagem de UBCDN do caso de protocolo de confiança, em que a mensagem inclua: o UBCDN do caso de protocolo de confiança; uma assinatura digital do proprietário do UBCDN resultando da assinatura do UBCDN; e o certificado de domínio do UBCDN
740
Identificar um identificador de cadeia atualizado do caso de protocolo de confiança indicando uma configuração de rede de protocolo de confiança atualizada do caso de protocolo de confiança
750
Assinar um UBCDN atualizado do caso de protocolo de confiança que inclui o nome de domínio do protocolo de confiança do caso de protocolo de confiança e o identificador de cadeia atualizado do caso de protocolo de confiança
760
Publicar uma mensagem de UBCDN atualizada do caso de protocolo de confiança, em cuja mensagem de UBCDN inclua: o UBCDN atualizado do caso do protocolo de confiança; uma assinatura de proprietário de UBCDN atualizada resultando da assinatura do UBCDN atualizado; e o certificado de domínio do UBCDN
700

Figura 7

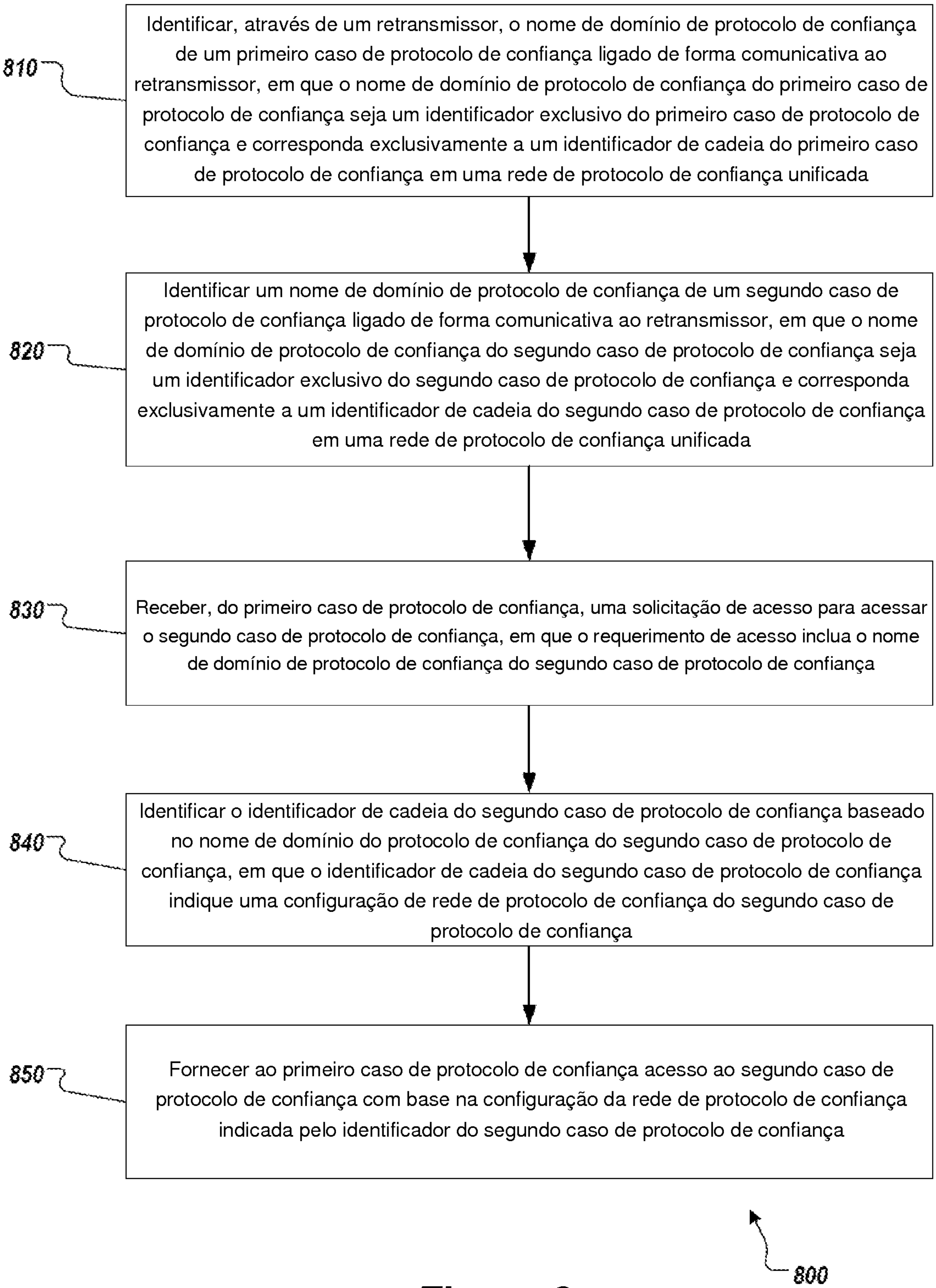

810
Identificar, através de um retransmissor, o nome de domínio de protocolo de confiança de um primeiro caso de protocolo de confiança ligado de forma comunicativa ao retransmissor, em que o nome de domínio de protocolo de confiança do primeiro caso de protocolo de confiança seja um identificador exclusivo do primeiro caso de protocolo de confiança e corresponda exclusivamente a um identificador de cadeia do primeiro caso de protocolo de confiança em uma rede de protocolo de confiança unificada
820
Identificar um nome de domínio de protocolo de confiança de um segundo caso de protocolo de confiança ligado de forma comunicativa ao retransmissor, em que o nome de domínio de protocolo de confiança do segundo caso de protocolo de confiança seja um identificador exclusivo do segundo caso de protocolo de confiança e corresponda exclusivamente a um identificador de cadeia do segundo caso de protocolo de confiança em uma rede de protocolo de confiança unificada
830
Receber, do primeiro caso de protocolo de confiança, uma solicitação de acesso para acessar o segundo caso de protocolo de confiança, em que o requerimento de acesso inclua o nome de domínio de protocolo de confiança do segundo caso de protocolo de confiança
840
Identificar o identificador de cadeia do segundo caso de protocolo de confiança baseado no nome de domínio do protocolo de confiança do segundo caso de protocolo de confiança, em que o identificador de cadeia do segundo caso de protocolo de confiança indique uma configuração de rede de protocolo de confiança do segundo caso de protocolo de confiança
850
Fornecer ao primeiro caso de protocolo de confiança acesso ao segundo caso de protocolo de confiança com base na configuração da rede de protocolo de confiança indicada pelo identificador do segundo caso de protocolo de confiança
800

Figura 8

RESUMO

"MÉTODO IMPLEMENTADO POR COMPUTADOR, MEIO LEGÍVEL POR COMPUTADOR E SISTEMA PARA IMPLEMENTAR UM MÉTODO"

A presente invenção se refere a métodos implementados por computador para um esquema de nome de domínio para sistemas de protocolo de confiança. O método (500) implementado por computador, compreende as etapas de: obter (510), por um nó cliente de um primeiro caso de protocolo de confiança (*blockchain*), um nome de domínio do protocolo de confiança (310) de um segundo caso de protocolo de confiança diferente, em que o nome de domínio do protocolo de confiança (310) é um identificador único do segundo caso de protocolo de confiança em uma rede de protocolo de confiança unificada compreendendo uma pluralidade de casos de protocolo de confiança que são ligados de forma comunicativa por dois ou mais retransmissores; o nome de domínio do protocolo de confiança (310) compreende um rótulo legível por humanos; e o nome de domínio do protocolo de confiança (310) corresponde a um identificador de cadeia (320) do segundo caso de protocolo de confiança; identificar (520) o identificador de cadeia (320) do segundo caso de protocolo de confiança com base no nome de domínio do protocolo de confiança (310) do segundo caso de protocolo de confiança, em que o identificador de cadeia (320) do segundo caso de protocolo de confiança indica uma configuração de rede de protocolo de confiança do segundo caso de protocolo de confiança; e acessar (530), por meio do nó cliente, o segundo caso de protocolo de confiança com base na configuração de rede de protocolo de confiança indicada pelo identificador de cadeia (320) do segundo caso de protocolo de confiança.