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

(11) BR 112019007232-2 B1

(22) Data do Depósito: 27/11/2018

(45) Data de Concessão: 15/02/2022

(54) Título: MÉTODOS IMPLEMENTADOS POR COMPUTADOR PARA PROTEÇÃO DA INFORMAÇÃO, SISTEMAS PARA PROTEÇÃO DA INFORMAÇÃO E MEIO DE ARMAZENAMENTO LEGÍVEL POR COMPUTADOR NÃO TRANSITÓRIO

(51) Int.Cl.: F24F 1/02.

(73) Titular(es): ADVANCED NEW TECHNOLOGIES CO., LTD..

(72) Inventor(es): BAOLI MA; WENBIN ZHANG; LICHUN LI; ZHENG LIU; SHAN YIN.

(86) Pedido PCT: PCT CN2018117548 de 27/11/2018

(87) Publicação PCT: WO 2019/072275 de 18/04/2019

(85) Data do Início da Fase Nacional: 10/04/2019

(57) Resumo: Trata-se de um método implementado por computador para proteção da informação, o método compreendendo: determinar uma ou mais entradas de dados e uma ou mais saídas de dados para uma transação, em que as entradas de dados são associadas a tipos de dados de entrada, respectivamente, e as saídas de dados são associadas a tipos de dados de saída, respectivamente; criptografar os tipos de dados de entrada e os tipos de dados de saída; comprometer cada um dos tipos de dados de entrada criptografados e dos tipos de dados de saída criptografados com um esquema de compromisso para obter valores de compromisso correspondentes; obter ao menos um parâmetro R baseado ao menos nos valores de compromisso; e enviar a transação a um ou mais nós em uma rede de cadeia de blocos com a revelação do parâmetro R e sem a revelação dos tipos de dados de entrada e tipos de dados de saída aos nós para verificar a consistência entre os tipos de dados de entrada e os tipos de dados de saída.

“MÉTODOS IMPLEMENTADOS POR COMPUTADOR PARA PROTEÇÃO DA INFORMAÇÃO, SISTEMAS PARA PROTEÇÃO DA INFORMAÇÃO E MEIO DE ARMAZENAMENTO LEGÍVEL POR COMPUTADOR NÃO TRANSITÓRIO”

CAMPO TÉCNICO

[001]Em termos gerais, a presente invenção refere-se a métodos e dispositivos para proteção da informação.

FUNDAMENTOS DA INVENÇÃO

[002]A privacidade é importante para a comunicação e transferência de dados entre vários usuários. Sem proteção, os usuários ficam expostos ao risco de roubo de identidade, transferência ilegal ou outras possíveis perdas. O risco cresce ainda mais quando as comunicações e transferências são feitas online devido ao livre acesso às informações online.

SUMÁRIO DA INVENÇÃO

[003]Várias modalidades da presente invenção incluem sistemas, métodos e meios não transitórios legíveis por computadores para proteção da informação.

[004]De acordo com um aspecto, um método implementado por computador para proteção da informação compreende: determinar uma ou mais entradas de dados e uma ou mais saídas de dados para uma transação, em que as entradas de dados são associadas a tipos de dados de entrada, respectivamente, e as saídas de dados são associadas a tipos de dados de saída, respectivamente; criptografar os tipos de dados de entrada e os tipos de dados de saída; comprometer cada um dos tipos de dados de entrada criptografados e dos tipos de dados de saída criptografados com um esquema de compromisso para obter valores de compromisso correspondentes; obter ao menos um parâmetro R baseado ao menos nos valores de compromisso; e enviar a transação a um ou mais nós em uma rede de blockchain com a revelação do parâmetro R e sem a revelação dos tipos de dados de entrada e tipos de dados de saída aos nós para verificar a consistência entre os tipos de dados

de entrada e os tipos de dados de saída.

[005]Em algumas modalidades, criptografar os tipos de dados de entrada e os tipos de dados de saída compreende criptografar os tipos de dados de entrada e os tipos de dados de saída com uma função hash.

[006]Em algumas modalidades, o esquema de compromisso compreende um compromisso de Pedersen.

[007]Em algumas modalidades, o esquema de compromisso compreende ao menos um fator de cegamento; e o fator de cegamento muda na hora de comprometer os tipos de dados de entrada criptografados e os tipos de dados de saída criptografados.

[008]Em algumas modalidades, faz-se com que os nós verifiquem a consistência entre os tipos de dados de entrada e os tipos de dados de saída sem conhecimento dos tipos de dados de entrada e dos tipos de dados de saída.

[009]Em algumas modalidades, a transação baseia-se em ao menos um modelo de Saídas de Transações Não Gastas (UTXO); e as entradas de dados e as saídas de dados compreendem os tipos de um ou mais ativos sendo submetidos à transação.

[010]Em algumas modalidades, o esquema de compromisso compreende uma pluralidade de fatores de ofuscamento que correspondem respectivamente aos tipos de dados de entrada e aos tipos de dados de saída; e obter ao menos o parâmetro R com base ao menos nos valores de compromisso compreende: obter diferenças entre pares dos valores de compromisso; concatenar as diferenças obtidas; criptografar as diferenças concatenadas com uma função hash para obter um valor de criptografia x; e obter o parâmetro R com base ao menos no valor de criptografia x e diferenças entre pares dos fatores de ofuscamento.

[011]Em algumas modalidades, enviar a transação aos um ou mais nós na rede de blockchain com a revelação do parâmetro R e sem a revelação dos tipos de

dados de entrada e tipos de dados de saída aos nós para verificar a consistência entre os tipos de dados de entrada e os tipos de dados de saída compreende enviar a transação aos um ou mais nós na rede de blockchain com a revelação do parâmetro R e sem a revelação dos tipos de dados de entrada e tipos de dados de saída para fazer com que os nós: obtenham o parâmetro R e um ponto de base G; obtenham diferenças entre pares dos valores de compromisso; concatenem as diferenças obtidas; criptografem as diferenças concatenadas com uma função hash para obter um valor de criptografia x; obtenham uma soma C de polinômios com base ao menos nas diferenças obtidas e no valor de criptografia x; em resposta à determinação de que a soma C é igual ao produto do parâmetro R e ponto de base G, determinem que os tipos de dados de entrada e os tipos de dados de saída são consistentes; e, em resposta à determinação de que a soma C não é igual ao produto do parâmetro R e ponto de base G, determinem que os tipos de dados de entrada e os tipos de dados de saída são inconsistentes.

[012]De acordo com outro aspecto, um meio de armazenamento não transitório legível por computador armazena instruções para ser executadas por um processador para fazer com que este execute operações que compreendem: determinar uma ou mais entradas de dados e uma ou mais saídas de dados para uma transação, em que as entradas de dados são associadas a tipos de dados de entrada, respectivamente, e as saídas de dados são associadas a tipos de dados de saída, respectivamente; criptografar os tipos de dados de entrada e os tipos de dados de saída; comprometer cada um dos tipos de dados de entrada criptografados e dos tipos de dados de saída criptografados com um esquema de compromisso para obter valores de compromisso correspondentes; obter ao menos um parâmetro R baseado ao menos nos valores de compromisso; e enviar a transação a um ou mais nós em uma rede de blockchain com a revelação do parâmetro R e sem a revelação dos tipos de dados de entrada e tipos de dados de saída aos nós para verificar a consis-

tência entre os tipos de dados de entrada e os tipos de dados de saída.

[013]De acordo com outro aspecto, um sistema para proteção da informação compreende um processador e um meio de armazenamento não transitório legível por computador acoplado ao processador, o meio de armazenamento armazenando instruções para ser executadas pelo processador para fazer com que o sistema execute operações que compreendem: determinar uma ou mais entradas de dados e uma ou mais saídas de dados para uma transação, em que as entradas de dados são associadas a tipos de dados de entrada, respectivamente, e as saídas de dados são associadas a tipos de dados de saída, respectivamente; criptografar os tipos de dados de entrada e os tipos de dados de saída; comprometer cada um dos tipos de dados de entrada criptografados e dos tipos de dados de saída criptografados com um esquema de compromisso para obter valores de compromisso correspondentes; obter ao menos um parâmetro R baseado ao menos nos valores de compromisso; e enviar a transação a um ou mais nós em uma rede de blockchain com a revelação do parâmetro R e sem a revelação dos tipos de dados de entrada e tipos de dados de saída aos nós para verificar a consistência entre os tipos de dados de entrada e os tipos de dados de saída.

[014]De acordo com outro aspecto, um método implementado por computador para proteção da informação compreende: um ou mais nós em uma rede de blockchain obterem uma transação iniciada por um nó iniciador. A transação é associada a uma ou mais entradas de dados e uma ou mais saídas de dados. As entradas de dados são associadas respectivamente a tipos de dados de entrada, e as saídas de dados são associadas respectivamente a tipos de dados de saída respectivamente. Os tipos de dados de entrada e os tipos de dados de saída são criptografados e comprometidos a um esquema de compromisso para obter valores de compromisso correspondentes. Os tipos de dados de entrada e os tipos de dados de saída não são revelados aos um ou mais nós. O método de proteção da informação compre-

ende ainda: os um ou mais nós verificarem a consistência entre os tipos de dados de entrada e os tipos de dados de saída; em resposta à determinação de que os tipos de dados de entrada e os tipos de dados de saída são consistentes, os um ou mais nós adicionarem a transação à rede de blockchain; e, em resposta à determinação de que os tipos de dados de entrada e os tipos de dados de saída são inconsistentes, os um ou mais nós rejeitarem a adição da transação à rede de blockchain.

[015]Em algumas modalidades, verificar a consistência entre os tipos de dados de entrada e os tipos de dados de saída compreende: obter um parâmetro R e um ponto de base G; obter diferenças entre pares dos valores de compromisso; concatenar as diferenças obtidas; criptografar as diferenças concatenadas com uma função hash para obter um valor de criptografia x; obter uma soma C de polinômios com base ao menos nas diferenças obtidas e no valor de criptografia x; e determinar se a soma C é igual ao produto do parâmetro R e ponto de base G.

[016]Em algumas modalidades, o método compreende ainda: em resposta à determinação de que a soma C é igual ao produto do parâmetro R e ponto de base G, determinar que os tipos de dados de entrada e os tipos de dados de saída são consistentes; e, em resposta à determinação de que a soma C não é igual ao produto do parâmetro R e ponto de base G, determinar que os tipos de dados de entrada e os tipos de dados de saída são inconsistentes.

[017]Em algumas modalidades, os um ou mais nós compreendem nós de consenso.

[018]De acordo com outro aspecto, um meio de armazenamento não transitório legível por computador armazena instruções para ser executadas por um processador para fazer com que este execute operações que compreendem: um ou mais nós em uma rede de blockchain obterem uma transação iniciada por um nó iniciador. A transação é associada a uma ou mais entradas de dados e uma ou mais saídas de dados. As entradas de dados são associadas respectivamente a tipos de

dados de entrada, e as saídas de dados são associadas respectivamente a tipos de dados de saída respectivamente. Os tipos de dados de entrada e os tipos de dados de saída são criptografados e comprometidos a um esquema de compromisso para obter valores de compromisso correspondentes. Os tipos de dados de entrada e os tipos de dados de saída não são revelados aos um ou mais nós. As operações compreendem ainda: os um ou mais nós verificarem a consistência entre os tipos de dados de entrada e os tipos de dados de saída; em resposta à determinação de que os tipos de dados de entrada e os tipos de dados de saída são consistentes, os um ou mais nós adicionarem a transação à rede de blockchain; e, em resposta à determinação de que os tipos de dados de entrada e os tipos de dados de saída são inconsistentes, os um ou mais nós rejeitarem a adição da transação à rede de blockchain.

[019]De acordo com outro aspecto, um sistema para proteção da informação compreende um processador e um meio de armazenamento não transitório legível por computador acoplado ao processador, o meio de armazenamento armazenando instruções para ser executadas pelo processador para fazer com que o sistema execute operações que compreendem: um ou mais nós em uma rede de blockchain obterem uma transação iniciada por um nó iniciador. A transação é associada a uma ou mais entradas de dados e uma ou mais saídas de dados. As entradas de dados são associadas respectivamente a tipos de dados de entrada, e as saídas de dados são associadas respectivamente a tipos de dados de saída respectivamente. Os tipos de dados de entrada e os tipos de dados de saída são criptografados e comprometidos a um esquema de compromisso para obter valores de compromisso correspondentes. Os tipos de dados de entrada e os tipos de dados de saída não são revelados aos um ou mais nós. As operações compreendem ainda: os um ou mais nós verificarem a consistência entre os tipos de dados de entrada e os tipos de dados de saída; em resposta à determinação de que os tipos de dados de entrada e os tipos de dados de saída são consistentes, os um ou mais nós adicionarem a transa-

ção à rede de blockchain; e, em resposta à determinação de que os tipos de dados de entrada e os tipos de dados de saída são inconsistentes, os um ou mais nós rejeitarem a adição da transação à rede de blockchain.

[020]Essas e outras características dos sistemas, métodos e meios não transitórios legíveis por computador revelados neste documento, bem como os métodos de operação e funções dos elementos relacionados da estrutura e a combinação de peças e economias da fabricante, transparecerão melhor mediante a leitura da descrição a seguir e das reivindicações anexas tomando como referência os desenhos concomitantes, todos os quais constituem parte deste relatório descritivo e dentre os quais números de referência iguais indicam peças correspondentes nas várias figuras. Deve-se ter especialmente em mente, contudo, que os desenhos servem tão somente a fins de ilustração e descrição e não constituem, portanto, uma definição dos limites da invenção.

BREVE DESCRIÇÃO DOS DESENHOS

[021]Certas características de várias modalidades da presente tecnologia são estabelecidas com particularidade nas reivindicações anexas. Um melhor entendimento acerca dos traços e vantagens da tecnologia será apreendido tomando como referência a descrição detalhada a seguir, que estabelece modalidades ilustrativas, nas quais os princípios da invenção são adotados, e dentre cujos desenhos concomitantes:

[022]A FIG. 1 ilustra um sistema para proteção da informação exemplificativo de acordo com várias modalidades.

[023]A FIG. 2 ilustra etapas exemplificativas para o início e verificação de uma transação de acordo com várias modalidades.

[024]A FIG. 3 ilustra um fluxograma de um método para proteção da informação exemplificativo de acordo com várias modalidades.

[025]A FIG. 4 ilustra um fluxograma de um método para proteção da infor-

mação exemplificativo de acordo com várias modalidades.

[026]A FIG. 5 ilustra um diagrama em blocos de um sistema de computador exemplificativo no qual qualquer uma das modalidades descritas neste documento pode ser implementada.

DESCRIÇÃO DETALHADA

[027]A blockchain pode ser considerada um banco de dados descentralizado, comumente chamado de livro-razão distribuído porque a operação é executada por vários nós (por exemplo, dispositivos de computação) em uma rede. Qualquer informação pode ser escrita na blockchain e salva ou lida a partir dela. Qualquer pessoa pode instalar um servidor e aderir à rede de blockchain para tornar-se um nó. Qualquer nó pode contribuir com poder de computação para manter a blockchain ao executar computações complexas, tais como um cálculo de hash para adicionar um bloco a uma blockchain, e o bloco adicionado pode conter vários tipos de dados ou informações. O nó que contribuiu com o poder de computação para o bloco adicionado pode ser recompensado com um token (por exemplo, unidade de moeda digital). Como a blockchain não possui um nó central, cada nó é igual e mantém de pé todo o banco de dados de blockchain.

[028]Nós são, por exemplo, dispositivos de computação ou grandes sistemas de computador que sustentam a rede de blockchain e a mantêm operando harmoniosamente. Os nós podem ser operados por indivíduos ou grupos de pessoas que contribuem financeiramente comprando sistemas de computador potentes, conhecidos como equipamentos de mineração. Há dois tipos de nós, nós completos e nós leves. Os nós completos mantêm uma cópia completa da blockchain. Os nós completos na rede de blockchain validam transações e blocos que recebem e retransmitem-nos a pontos de rede conectados para prover uma verificação de consenso das transações. Já os nós leves, por outro lado, só baixam uma fração da blockchain. Por exemplo, os nós leves são usados para transações em moeda digital.

Um nó leve comunicará a um nó completo quando deseja fazer uma transação.

[029]Essa propriedade de descentralização ajuda a prevenir a emergência de um centro de gestão em uma posição controlada. Por exemplo, a manutenção da blockchain de bitcoin é feita pela rede de nós de comunicações do software de bitcoin na área em operação. Ou seja, em vez de bancos, instituições ou administradores no sentido tradicional da palavra, há vários intermediários na forma de servidores de computador executando o software de bitcoin. Esses servidores de computador compõem uma rede conectada via Internet, em que qualquer um pode eventualmente aderir à rede. As transações acomodadas pela rede podem ser em um formato: “o usuário A deseja enviar Z bitcoins ao usuário B”, onde as transações são transmitidas à rede usando aplicativos de software prontamente disponíveis. Os servidores de computador atuam como servidores de bitcoin que operam para validar essas transações financeiras, adicionar um registro delas à sua cópia do livro-razão e, em seguida, transmitir essas adições ao livro-razão a outros servidores da rede.

[030]A manutenção da blockchain é chamada de "mineração", e os que fazem essa manutenção são recompensados com bitcoins recém-criados e taxas de transação conforme mencionado acima. Por exemplo, os nós podem determinar se as transações são válidas com base em um conjunto de regas com que a rede de blockchain concordou. Os mineiros podem estar situados em qualquer continente e processar pagamentos verificando cada transação como válida e adicionando-a ao livro-razão. Essa verificação é obtida por consenso provido por vários mineiros e deduz que não há fraude sistemática. No fim das contas, todos os dados serão consistentes porque a computação precisa satisfazer certos requisitos para que seja válida e todos os nós serão sincronizados para garantir que a blockchain é consistente.

[031]Através do processo de mineração, transações tais como transferências de ativos são verificadas e adicionadas a uma crescente blockchain de uma blockchain por nós da rede. Ao percorrer toda a blockchain, a verificação pode incluir, por

exemplo, se a parte pagante tem acesso ao ativo sendo transferido, se o ativo foi gasto antes, se a quantia de transferência está certa etc. Por exemplo, em uma transação hipotética (por exemplo, uma transação de bitcoins de acordo com um modelo UTXO (saída de transação não gasta)) assinada por um transmissor, a transação proposta pode ser transmitida à rede de blockchain para mineração. Um mineiro precisa verificar se a transação tem qualificação para ser executada de acordo com o histórico da blockchain. Se o saldo da carteira do transmissor possui fundos suficientes de acordo com o histórico da blockchain atual, a transação é considerada válida e pode ser adicionada ao bloco. Uma vez verificadas, as transferências de ativos podem ser incluídas no bloco seguinte para ser adicionadas à blockchain.

[032]Um bloco é muito parecido com um registro de banco de dados. Toda vez que escrevem-se dados, cria-se um bloco. Esses blocos são interligados e protegidos usando criptografia para tornar-se redes interconectadas. Cada bloco conecta-se ao anterior, que também explica a origem do nome “blockchain”. Cada bloco geralmente contém o hash criptográfico do bloco anterior, o horário de geração e os dados em si. Por exemplo, cada bloco contém duas partes: um cabeçalho de bloco, para registrar o valor de recurso do bloco atual, e um corpo, para registrar os dados em si (por exemplo, dados de transação). A blockchain é interligada através dos cabeçalhos de bloco. Cada cabeçalho de bloco pode conter vários valores de recurso, tais como versão, hash do bloco anterior, raiz de Merkle, carimbo de tempo, alvo de dificuldade e nonce. O hash do bloco anterior não só contém o endereço do bloco anterior, mas também o hash dos dados dentro do bloco anterior, tornando assim as cadeias de blocos imutáveis. O nonce é um número que, quando incluído, produz um hash com um número específico de bits zero iniciais.

[033]Na mineração, o hash dos conteúdos do novo bloco é assumido por um nó. O nonce (por exemplo, sequência aleatória) é anexado ao hash para obter uma nova sequência. A nova sequência gera um novo hash. O hash final é então compa-

rado ao alvo (por exemplo, nível) de dificuldade e determina-se se o hash final é realmente menor que o alvo de dificuldade ou não. Se não, o nonce é alterado, e o processo repete novamente. Se sim, o bloco é adicionado à cadeia, e o livro-razão público é atualizado e avisado sobre a adição. O nó responsável pela adição bem-sucedida é recompensado com bitcoins, por exemplo, adicionando uma transação de recompensa a si próprio ao novo bloco (o que é conhecido como geração base de moeda).

[034]Ou seja, para toda saída “Y”, se k é escolhido dentre uma distribuição com alta entropia mínima, é impossível encontrar uma entrada x tal que H(k|x) = Y, onde K é o nonce, x é o hash do bloco, Y é o alvo de dificuldade, e “|” indica concatenação. Por os hashes criptográficos serem essencialmente aleatórios, no sentido em que sua saída não pode ser prevista com base em suas entradas, só há uma forma conhecida de encontrar o nonce: testar números inteiros um depois do outro, por exemplo, 1, depois 2, depois 3, e assim por diante, o que pode ser conhecido como força bruta. Quanto maior o número de zeros iniciais, mais demorará em média para encontrar um nonce Y necessário. Em um exemplo, o sistema de bitcoin ajusta constantemente o número de zeros iniciais, de tal modo que o tempo médio para encontrar um nonce seja de cerca de dez minutos. Assim, na medida em que a capacidade de processamento do hardware de computação aumenta com o tempo, ao longo dos anos, o protocolo bitcoin simplesmente exigirá mais bits zero iniciais de modo a fazer com que a mineração sempre leve uma duração de cerca de dez minutos para que seja implementada.

[035]Conforme descrito, o hashing é um pilar importante para a blockchain. O algoritmo de hash pode ser entendido como uma função que comprime mensagens de qualquer tamanho em uma compilação da mensagem de tamanho fixo. O MD5 e o SHA são usados com mais frequência. Em algumas modalidades, o tamanho de hash da blockchain é de 256 bits, o que significa que, não importa qual o

conteúdo original, em última instância um número binário de 256 bits é calculado. E pode-se garantir que o hash correspondente é exclusivo contanto que o conteúdo original seja diferente. Por exemplo, o hash da sequência “123” é a8fdc205a9f19cc1c7507a60c4f01b13d11d7fd0 (hexadecimal), que possui 256 bits quando convertido em binário, e apenas “123” possui esse hash. O algoritmo de hash na blockchain é irreversível, ou seja, o cálculo direto é fácil (de “123” para a8fdc205a9f19cc1c7507a60c4f01b1c7507a60c4f01b13d11d7fd0), e o cálculo reverso não pode ser feito ainda que todos os recursos de computação sejam exauridos. Sendo assim, o hash de cada bloco da blockchain é exclusivo.

[036]Além disso, se o conteúdo do bloco muda, seu hash mudará. O bloco e o hash são em correspondência um a um, e o hash de cada bloco é calculado especificamente para o cabeçalho de bloco. Ou seja, os valores de recurso dos cabeçalhos de bloco são conectados para formar uma sequência longa, e então o hash é calculado para a sequência. Por exemplo, “Hash = SHA256 (cabeçalho de bloco)” é uma fórmula calcular o hash do bloco, SHA256 é um algoritmo de hash de blockchain aplicado ao cabeçalho de bloco. O hash é determinado exclusivamente pelo cabeçalho de bloco, e não pelo corpo de bloco. Como mencionado acima, o cabeçalho de bloco possui muito conteúdo, inclusive o hash do bloco atual e o hash do bloco anterior. Isso significa que, se o conteúdo do bloco atual mudar, ou se o hash do bloco anterior mudar, ocorrerá uma mudança de hash no bloco atual. Se um hacker modifica um bloco, o hash desse bloco muda. A fim de que um bloco mais adiante conecte-se ao bloco modificado, o hacker, por sua vez, deve modificar todos os blocos subsequentes, porque o próximo bloco deve conter o hash do bloco anterior. Do contrário, o bloco modificado será destacado da blockchain. Por motivos de design, os cálculos de hash são demorados e é praticamente impossível modificar vários blocos em um curto período de tempo a não ser que o hacker tenha dominado mais de 51% do poder de computação de toda a rede. Sendo assim, a blockchain garante

sua própria confiabilidade, e, uma vez que os dados são escritos, não é possível adulterá-los.

[037]Assim que o mineiro encontra o hash (ou seja, uma assinatura ou solução qualificada) para o novo bloco, o mineiro transmite essa assinatura a todos os outros mineiros (nós da blockchain). Outros mineiros agora verificam, um após o outro, se essa solução corresponde ao problema do bloco do transmissor (ou seja, determinam se a entrada de hash realmente resulta nessa assinatura). Se a solução for válida, os demais mineiros confirmarão a solução e concordarão que o novo bloco pode ser adicionado à blockchain. Assim, o consenso do novo bloco é atingido. Isso também é conhecido como “prova de trabalho”. O bloco para o qual obteve-se consenso pode agora ser adicionado à blockchain e é transmitido a todos os nós na rede junto com sua assinatura. Os nós aceitarão o bloco e o salvarão em seus dados de transações contanto que as transações dentro do bloco correspondam corretamente aos saldos de carteira atuais (histórico de transações) nesse ponto no tempo. Toda vez que um novo bloco é adicionado no topo desse bloco, a adição também conta como outra "confirmação" para os blocos antes dele. Por exemplo, se uma transação é incluída no bloco 502, e a blockchain tem 507 blocos de comprimento, significa que a transação possui cinco confirmações (correspondentes aos blocos de 507 a 502). Quanto mais confirmações a transação possui, mais difícil é para que piratas a alterem.

[038]Em algumas modalidades, um sistema de ativos de blockchain utiliza criptografia de chave pública, em que duas chaves criptográficas, uma pública e outra privada, são geradas. Pode-se pensar na chave pública como um número de conta e na chave privada como credenciais de propriedade. Por exemplo, uma carteira de bitcoins é uma coletânea das chaves públicas e privadas. A propriedade de um ativo (por exemplo, moeda digital, ativo financeiro, ação, participação, título) associado a certo endereço de ativo pode ser demonstrada com o conhecimento da

chave privada pertencente ao endereço. Por exemplo, um software de carteira de bitcoins, por vezes chamado de “software cliente de bitcoins”, permite que dado usuário faça transações em bitcoins. Um programa de carteira gera e armazena chaves privadas e comunica-se com pontos de rede na rede de bitcoins.

[039]Em transações na blockchain, os pagadores e credores são identificados na blockchain por suas chaves criptográficas públicas. Por exemplo, a maioria das transferências de bitcoins contemporâneas são de uma chave pública para uma chave pública diferente. Na prática, hashes dessas chaves são usados na blockchain e são chamados de “endereços de bitcoins”. Em teoria, se um criminoso hipotético S roubasse dinheiro da pessoa A simplesmente adicionando transações ao livro-razão da blockchain como "a pessoa A paga à pessoa S 100 bitcoins” usando endereços de bitcoins dos usuários em vez de seus nomes. O protocolo bitcoin impede esse tipo de roubo ao exigir que toda transferência seja assinada digitalmente com a chave privada do pagador, e somente transferências assinadas podem ser adicionadas ao livro-razão da blockchain. Como a pessoa S não pode forjar a assinatura da pessoa A, a pessoa S não pode lesar a pessoa A adicionando uma entrada à blockchain equivalente a "a pessoa A paga à pessoa S 200 bitcoins". Ao mesmo tempo, qualquer um pode verificar a assinatura da pessoa A usando sua própria chave pública e, assim, esse alguém autoriza qualquer transação na blockchain em que ele é o pagador.

[040]No contexto das transações em bitcoins, para transferir alguns bitcoins ao usuário B, o usuário A pode construir um registro contendo informações acerca da transação através de um nó. O registro pode ser assinado com a chave de assinatura do usuário A (chave privada) e contém a chave de verificação pública do usuário A e a chave de verificação pública do usuário B. A assinatura é usada para confirmar que a transação veio do usuário e também impede que a transação seja alterada por quem quer que seja uma vez feita. O registro junto ao outro registro que

ocorreu na mesma janela de tempo em um novo bloco pode ser transmitido aos nós completos. Ao receber os registros, os nós completos podem trabalhar para incorporar os registros ao livro-razão de todas as transações que já ocorreram no sistema de blockchain, adicionando o novo bloco a uma blockchain previamente aceita através do processo de mineração descrito acima, e validar o bloco adicionado levando em consideração as regras de consenso da rede.

[041]O ativo a ser transferido do usuário A pode ser em formato UTXO (saída de transação não gasta). O UTXO é um modelo de objetos de blockchain. De acordo com o UTXO, os ativos são representados por saídas de transações de blockchain que não foram gastas, que podem ser usadas como entradas em novas transações. Para gastar o ativo (fazer a transação do ativo), o usuário precisa assinar com a chave privada. O bitcoin é um exemplo de moeda digital que utiliza o modelo UTXO. No caso de uma transação em uma blockchain válida, saídas não gastas podem ser usadas para efetuar novas transações. Em algumas modalidades, somente saídas não gastas podem ser usadas em novas transações para prevenir despesas duplicadas e fraudes. Por esse motivo, as entradas em uma blockchain são excluídas quando ocorre uma transação, ao passo que, ao mesmo tempo, criam-se saídas na forma de UTXOs. Essas saídas de transações não gastas podem ser usadas (pelos donos de chaves privadas, por exemplo, pessoas com carteiras em moeda digital) para os fins de transações futuras.

[042]Como a blockchain e outros livros-razão semelhantes são completamente públicos, a blockchain em si não possui proteção à privacidade. O caráter público da rede P2P significa que, embora os que a utilizam não sejam identificados pelo nome, a correlação de transações com indivíduos e empresas é viável. Por exemplo, em remessas de valores internacionais ou na cadeia de abastecimento, os tipos de ativo têm um nível altíssimo de valor de proteção à privacidade porque, com as informações do tipo de ativo, é possível deduzir a localização e identidade espe-

cíficas das partes da transação. O tipo de ativo pode compreender, por exemplo, dinheiro, moeda digital, contrato, escritura, histórico médico, detalhes do cliente, ações, títulos, participações ou o tipo de qualquer outro ativo que possa ser descrito em formato digital. Embora o modelo UTXO ofereça anonimato às identidades e quantias das transações, e tenha sido aplicado a Monero e Zcash, o tipo de ativo de transação permanece desprotegido. Sendo assim, uma abordagem ao problema técnico de acordo com a presente invenção consiste em proteger informações online, tais como a privacidade do tipo de ativo, nas transações. Os sistemas e métodos revelados podem ser integrados ao modelo UTXO para oferecer proteção à privacidade para uma variedade de conteúdos de transação.

[043]Durante as transações, a proteção da informação é importante para garantir a privacidade do usuário, e o tipo de ativo de transação é um tipo de informação que carece de proteção. A FIG. 1 ilustra um sistema exemplificativo 100 para proteção da informação de acordo com várias modalidades. Conforme ilustrado, uma rede de blockchain pode compreender vários nós (por exemplo, nós completos implementados em servidores, computadores etc.). Em algumas plataformas de blockchain (por exemplo, NEO), nós completos com certo nível de poder de votação podem ser chamados de nós de consenso, que assumem a responsabilidade de verificação da transação. Na presente invenção, nós completos, nós de consenso ou outros nós equivalentes podem verificar a transação.

[044]Além disso, conforme ilustra a FIG. 1, o usuário A e o usuário B podem usar dispositivos correspondentes, tais como laptops e celulares que atuam como nós leves, para fazer transações. Por exemplo, o usuário A pode querer fazer uma transação com o usuário B transferindo algum ativo na conta do usuário A para a conta do usuário B. O usuário A e o usuário B pode usar dispositivos correspondentes instalados com um software de blockchain apropriado para a transação. O dispositivo do usuário A pode ser chamado de nó iniciador A, que inicia uma transação

com o dispositivo do usuário B, chamado de nó receptor B. O Nó A pode acessar a blockchain via comunicação com o nó 1, e o Nó B pode acessar a blockchain via comunicação com o nó 2. Por exemplo, o nó A e o nó B podem enviar transações à blockchain através do nó 1 e do nó 2 para solicitar a adição das transações à blockchain. Fora a blockchain, o nó A e o nó B podem ter outros canais de comunicação. Por exemplo, o nó A e o nó B podem obter a chave pública um do outro via comunicação normal pela Internet.

[045]Cada um dos nós na FIG. 1 pode compreender um processador e um meio não transitório legível por computador que armazena instruções para ser executadas pelo processador para fazer com que o nó (por exemplo, o processador do nó) execute várias etapas para proteção da informação descritas neste documento. Cada nó pode ter instalado nele um software (por exemplo, programa de transação) e/ou hardware (por exemplo, fios, conexões sem fio) para se comunicar com outros nós e/ou outros dispositivos. Outros detalhes do hardware e software dos nós são descritos mais adiante com referência à FIG. 5.

[046]A FIG. 2 ilustra etapas exemplificativas para o início e verificação de uma transação de acordo com várias modalidades.

[047]O início da transação pode ser implementado pelo nó iniciador. Em algumas modalidades, cada tipo de tipo de ativo pode ser mapeado ou ter uma identificação exclusiva atribuída a ele. Por exemplo, a identificação exclusiva pode ser um número de série sn computado da seguinte maneira:

Etapa 1.2 sn = Hash (tipo de ativo)

[048]onde Hash() é uma função hash. Além disso, o tipo de ativo pode ser criptografado por um esquema de compromisso (por exemplo, compromisso de Pedersen) de acordo com o seguinte:

Etapa 1.3C(sn) = r×G + sn×H

[049]onde r é um fator de cegamento aleatório (chamado alternativamente

de fator de cegamento) que oferece ocultação, G e H são geradores/pontos de base da curva elíptica publicamente acordados e podem ser escolhidos aleatoriamente, sn é o valor do compromisso, C(sn) é o ponto de curva usado como compromisso e fornecido à contraparte, e H é outro ponto de curva. Ou seja, G e H podem ser parâmetros conhecidos dos nós. Uma geração “nothing up my sleeve” de H pode ser obtida pelo hashing do ponto de base G com um mapeamento da função hash de um ponto a outro com H = Hash(G). H e G são os parâmetros públicos do dado sistema (por exemplo, pontos gerados aleatoriamente em uma curva elíptica). O nó transmissor pode ter H e G publicados para todos os nós. Embora a descrição acima ofereça um exemplo do compromisso de Pedersen no formato de curva elíptica, várias outras formas de compromisso de Pedersen ou outros esquemas de compromisso podem ser usados alternativamente.

[050]Um esquema de compromisso mantém o sigilo dos dados, mas compromete-os de modo que eles não possam ser alterados mais tarde pelo transmissor dos dados. Se uma parte só conhece o valor de compromisso (por exemplo, C(sn)), ela não é capaz de determinar quais valores de dados subjacentes (por exemplo, sn) foram comprometidos. Tanto os dados (por exemplo, sn) como o fator de cegamento (por exemplo, r) podem ser revelados mais tarde (por exemplo, pelo nó iniciador), e um receptor (por exemplo, nó de consenso) do compromisso pode executar o compromisso e verificar se os dados comprometidos coincidem com os dados revelados. O fator de cegamento se faz presente porque, sem ele, alguém poderia tentar adivinhar os dados.

[051]Os esquemas de compromisso são uma forma de o transmissor (parte comprometedora) comprometer um valor (por exemplo, sn) de tal modo que o valor comprometido permaneça privado, mas possa ser revelado mais tarde quando a parte comprometedora divulgar um parâmetro necessário do processo de compromisso. Fortes esquemas de compromisso podem envolver tanto a ocultação de informações

como o cegamento computacional. Ocultação refere-se à noção de que dado valor sn e um compromisso desse valor C(sn) deveriam ser não relacionáveis. Ou seja, C(sn) não deve revelar nenhuma informação acerca de sn. Com C(sn), G e H conhecidos, é praticamente impossível conhecer sn por causa do número aleatório r. O esquema de compromisso é o cegamento se não houver uma maneira plausível de que dois valores diferentes possam resultar no mesmo compromisso. O compromisso de Pedersen consiste em ocultar perfeitamente e cegar computacionalmente de acordo com a suposição do logaritmo discreto.

[052]O compromisso de Pedersen possui uma propriedade adicional: compromissos podem ser adicionados, e a soma de um conjunto de compromissos é a mesma que um compromisso à soma dos dados (com um conjunto de chaves de cegamento como a soma das chaves de cegamento): C(BF1, data1) + C(BF2, data2) == C(BF1+BF2, data1+data2); C(BF1, data1) − C(BF1, data1) == 0. Em outras palavras, o compromisso preserva a adição e a propriedade comutativa aplica-se, isto é, o compromisso de Pedersen é aditivamente homomórfico, no sentido que os dados subjacentes podem ser manipulados matematicamente como se não criptografados.

[053]Em uma modalidade, um compromisso de Pedersen usado para criptografar o valor de entrada pode ser construído usando pontos de curva elípticos. Convencionalmente, uma chave pública de criptografia de curva elíptica (ECC) é criada multiplicando um gerador para o grupo (G) pela chave secreta (r): Pub=rG. O resultado pode ser serializado como um conjunto de 33 bytes. Chaves públicas ECC podem obedecer a propriedade aditivamente homomórfica supramencionada com relação a compromissos de Pedersen. Ou seja: Pub1+Pub2=(r1+r2(mod n))G.

[054]O compromisso de Pedersen para o valor de entrada pode ser criado selecionando um gerador adicional para o grupo (H nas equações abaixo) de modo que ninguém saiba o log discreto para o segundo gerador H em relação ao primeiro gerador G (ou vice-versa), o que significa que ninguém conhece x tal que [[r]]xG=H.

Isso pode ser obtido, por exemplo, usando o hash criptográfico de G para selecionar H: H=to_point(SHA256(ENCODE(G))).

[055]Dados os dois geradores G e H, um esquema de compromisso exemplificativo para criptografar o valor de entrada pode ser definido por: compromisso=rG+aH. Aqui, r pode ser o valor de cegamento secreto, e a pode ser o valor de entrada sendo comprometido. Por conseguinte, se sn for comprometido, o esquema de compromisso descrito acima C(sn) = r×G + sn×H pode ser obtido. Os compromissos de Pedersen são informações teoricamente privadas: para qualquer compromisso, existe algum fator de cegamento que faria com que qualquer quantia coincidisse com o compromisso. Os compromissos de Pedersen podem ser computacionalmente protegidos contra compromissos falsos, porque o mapeamento arbitrário não pode ser computado.

[056]A parte (nó) que comprometeu o valor pode abrir o compromisso revelando o valor original sn e o fator r que completa a equação de compromisso. A parte que deseja abrir o valor C(sn) computará então o compromisso novamente para verificar se o valor original compartilhado de fato coincide com o compromisso C(sn) inicialmente recebido. Assim, as informações do tipo de ativo podem ser protegidas mapeando-as a um número de série exclusivo e, então, criptografando-as pelo compromisso de Pedersen. O número aleatório r escolhido ao gerar o compromisso torna praticamente impossível para qualquer um deduzir o tipo de tipo de ativo que é comprometido de acordo com o valor de compromisso C(sn).

[057]Em algumas modalidades, ao incorporar o método de proteção da informação do tipo de ativo de acordo com o modelo UTXO, a consistência do tipo de ativo da entrada (sn_in) e do tipo de ativo da saída (sn_out) de uma transação pode ser verificada para determinar a autenticidade da transação. Por exemplo, os nós de blockchain podem rejeitar transações ou blocos que fracassem no teste de consistência em que sn_in = = sn_out. Visto que o tipo de ativo sn é criptografado (por

exemplo, por compromisso de Pedersen), o teste de consistência serve para verificar se C(sn_in) = = C(sn_out).

[058]Em algumas modalidades, conforme ilustra a FIG. 2, etapa 1, uma transação do tipo UTXO pode compreender m entradas (por exemplo, ativos disponíveis) e n saídas (por exemplo, ativos transferidos e ativos remanescentes). As entradas podem ser indicadas por sn_in_k, onde $1 \leq k \leq m$ e as saídas podem ser indicadas por sn_out_k, onde $1 \leq k \leq n$. Algumas das saídas podem ser transferidas ao nó receptor B, ao passo que as saídas remanescentes podem voltar ao nó iniciador A. Por exemplo, em uma transação hipotética, o usuário A pode ter um total de 5 bitcoins e 10 ações nessa carteira, e, para entradas de transação, sn_in_1 = Hash(bitcoin) e sn_in_2 = Hash(stock). Se o usuário A quiser transferir 3 bitcoins ao usuário B, para saídas de transação, sn_out_1 = Hash(bitcoin), sn_out_2 = Hash(bitcoin) e sn_out_3 = Hash(stock), com o que uma das saídas de bitcoin (3 bitcoins) é endereçada ao usuário B, e a outra saída de bitcoin (2 bitcoins) e a saída de ação são endereçadas de volta ao usuário A.

[059]Logo, em algumas modalidades, o tipo de ativo correspondente à entrada pode ser criptografado no formato:

$C\_in\_k = r\_in\_k \times G + sn\_in\_k \times H$, onde $1 \leq k \leq m$

[060]O tipo de ativo de saída corresponde ao formato de criptografia:

$C\_out\_k = r\_out\_k \times G + sn\_out\_k \times H$, onde $1 \leq k \leq n$

[061]Com os tipos de ativo sendo ocultados, o iniciador de transação precisa provar aos nós (por exemplo, nós completos, nós de consenso) que os tipos de ativo de entrada da transação são respectivamente consistentes com os tipos de ativo de saída. Logo, os nós completos podem verificar se a transação é válida.

[062]Em algumas modalidades, para iniciar uma transação do tipo UTXO com um tipo de ativo ocultado por compromisso de Pedersen, o iniciador de transação pode selecionar entradas e saídas apropriadas para realizar as Etapas 2.1 a 2.5

abaixo (correspondentes à FIG. 2, etapa 2):

[063]Etapa 2.1 Calcular

C_1 = C_in_1 – C_in_2,

C_2 = C_in_2 – C_in_3,

…

C_(m-1) = C_in_(m-1) – C_in_m,

C_m = C_out_1 – C_out_2,

C_(m+1) = C_out_2 – C_out_3,

…

C_(m+n-2) = C_out_(n-1) – C_out_n,

C_(m+n-1) = C_in_1 – C_out_1;

[064]Etapa 2.2 Calcular x = Hash (C_1 || C_2 || C_3 || … || C_(m+n-1)), onde "||" representa concatenação;

[065]Etapa 2.3 Calcular $C = C\_1 + x \times C\_2 + x^2 \times C\_3 + \ldots + x^{(m+n-2)} \times C\_(m+n-1)$. Note-se que os termos polinômios podem corresponder aos na Etapa 2.1;

[066]Etapa 2.4 Calcular $R = (r\_in\_1 - r\_in\_2) + x \times (r\_in\_2 - r\_in\_3) + x^2 \times (r\_in\_3 - r\_in\_4) + \ldots + x^{(m+n-2)} \times (r\_in\_1 - r\_out\_1)$. Note-se que os termos polinômios podem corresponder aos na Etapa 2.1, por exemplo, (r_in_1 – r_in_2) corresponde a C_in_1 – C_in_2;

[067]Etapa 2.5 Publicar R para nós, por exemplo, em uma transmissão de informações de transação.

[068]Em algumas modalidades, para verificar se os tipos de ativo de entrada e os tipos de ativo de saída são consistentes, C = R × G deve ser verdadeiro. Por exemplo, durante a verificação da transação, os nós realizam as Etapas 3.3 (correspondentes à FIG. 2, Etapa 3.1 a 3.3) abaixo para verificar se o tipo de ativo de transação é consistente:

[069]Etapa 3.1 Calcular x = Hash (C_1 || C_2 || C_3 || … || C_(m+n-1));

[070]Etapa 3.2 Calcular $C = C\_1 + x \times C\_2 + x^2 \times C\_3 + \ldots + x^{(m+n-2)} \times C\_(m+n-1)$;

[071]Etapa 3.3 Verificar se C = R × G. Se C = R × G, o tipo de ativo é consistente; do contrário, o tipo de ativo é inconsistente, e a transação é rejeitada. Em algumas modalidades, o C(sn) pode ser publicado nos nós, e os algoritmos das Etapas 2.1 a 2.3 são conhecidos dos nós (por exemplo, incluindo o nó que envia a transação e os nós que verificam a transação). Sendo assim, os nós que verificam a transação podem executar as Etapas 3.1 a 3.3 de maneira correspondente para realizar a confirmação. Assim, a transação rejeitada não será adicionada à blockchain. Conforme ilustra a etapa 4 na FIG. 2, com base na determinação de consistência, os nós podem determinar se adicionam a transação à blockchain ou se rejeitam a adição da transação.

[072]Como tal, um iniciador de transação pode enviar informações para nós de blockchain a fim de verificar a transação com base na consistência da entrada e saída de tipos de ativo da transação sem revelar os tipos de ativo reais e sem a capacidade de alterar as informações enviadas. A alocação de números de série (por exemplo, hashes) para cada tipo de ativo alarga e randomiza a representação de cada tipo de ativo, dificultando que o iniciador de transação forje um tipo de ativo para passar a verificação. Além disso, por causa da existência do número aleatório r, o mesmo tipo de ativo criptografado em diferentes momentos não é o mesmo. Aplicar o compromisso de Pedersen para criptografar o hash de tipo de ativo aprimora a proteção à privacidade do tipo de ativo em um nível ainda mais alto. Assim, pelas Etapas de 2.1 a 2.5, o iniciador de transação pode comprovar aos outros nós que os tipos de ativo da transação são válidos sem revelar os tipos de ativo. Por exemplo, diferenças entre os tipos de ativo de entrada e saída são obtidas e baseadas nelas constroem-se polinômios, de tal modo que o iniciador de transação pode passar os

tipos de ativo transformados aos outros nós para comprovar a consistência dos tipos de ativo e a autenticidade da transação. Ao mesmo tempo, a probabilidade de o iniciador de transação ou outro nó ser capaz de forjar o tipo de ativo pode ser negligenciada porque x é computado por hashing para servir como a base de vários exponenciais nos polinômios. Ademais, a revelação de R permite que os outros nós verifiquem se os tipos de ativo na transação são consistentes sem saber os tipos de artigos através das Etapas 3.1 a 3.3. Logo, com os sistemas e métodos revelados, informações de dados podem ser verificadas por terceiros, ao mesmo tempo em que mantém-se uma proteção à privacidade excepcional.

[073]A FIG. 3 ilustra um fluxograma de um método exemplificativo 300 para proteção da informação de acordo com várias modalidades da presente invenção. O método 300 pode ser implementado por um ou mais componentes (por exemplo, nó A) do sistema 100 da FIG. 1. O método 300 pode ser implementado por um sistema ou dispositivo (por exemplo, computador) que compreende um processador e um meio de armazenamento não transitório legível por computador (por exemplo, memória) que armazena instruções para ser executadas pelo processador para fazer com que o sistema ou dispositivo (por exemplo, o processador) execute o método 300. As operações do método 300 apresentadas abaixo visam a ser ilustrativas Dependendo da implementação, o método exemplificativo 300 pode incluir etapas a mais, a menos ou alternativas executadas em várias ordens ou em paralelo.

[074]O bloco 301 compreende: determinar uma ou mais entradas de dados e uma ou mais saídas de dados para uma transação, em que as entradas de dados são associadas a tipos de dados de entrada, respectivamente, e as saídas de dados são associadas a tipos de dados de saída, respectivamente. Vide, por exemplo, a Etapa 1 na FIG. 2. Em algumas modalidades, a transação baseia-se em ao menos um modelo de Saídas de Transações Não Gastas (UTXO); e as entradas de dados e as saídas de dados compreendem tipos de um ou mais ativos sendo submetidos à

transação entre um transmissor (nó iniciador) e um receptor (nó receptor). O tipo de ativo pode compreender, por exemplo, dinheiro, moeda digital, contrato, escritura, histórico médico, detalhes do cliente, ações, títulos, participações ou o tipo de qualquer outro ativo que possa ser descrito em formato digital.

[075]O bloco 302 compreende: criptografar os tipos de dados de entrada e os tipos de dados de saída. Vide, por exemplo, a Etapa 1.2 descrita acima. Em algumas modalidades, criptografar os tipos de dados de entrada e os tipos de dados de saída compreende criptografar cada um dos tipos de dados de entrada e dos tipos de dados de saída com uma função hash ou outra função unidirecional.

[076]O bloco 303 compreende: comprometer cada um dos tipos de dados de entrada criptografados e dos tipos de dados de saída criptografados com um esquema de compromisso para obter valores de compromisso correspondentes. Vide, por exemplo, a Etapa 1.3 descrita acima. Em algumas modalidades, o esquema de compromisso compreende um compromisso de Pedersen. Em algumas modalidades, o esquema de compromisso compreende ao menos um fator de cegamento; e o fator de cegamento muda na hora de comprometer os tipos de dados de entrada criptografados e os tipos de dados de saída criptografados. Ou seja, até mesmo os mesmos dados (por exemplo, mesmo tipo de dados) comprometidos em diferentes momentos teriam valores de compromisso diferentes devido ao fator de cegamento em constante mudança.

[077]O bloco 304 compreende: obter ao menos um parâmetro R baseado ao menos nos valores de compromisso. Vide, por exemplo, as Etapas 2.1 a 2.4 descritas acima. Em algumas modalidades, o esquema de compromisso compreende uma pluralidade de fatores de ofuscamento que correspondem respectivamente aos tipos de dados de entrada e aos tipos de dados de saída (vide, por exemplo, r_in_k e r_out_k); e obter ao menos o parâmetro R com base ao menos nos valores de compromisso compreende: obter diferenças entre pares dos valores de compromisso

(vide, por exemplo, a Etapa 2.1 para vários pares dos valores de compromisso entre os tipos de ativo de entrada e os tipos de ativo de saída, para os quais as diferenças podem ser obtidas); concatenar as diferenças obtidas (vide, por exemplo, a Etapa 2.2); criptografar as diferenças concatenadas com uma função hash para obter um valor de criptografia x (vide, por exemplo, a Etapa 2.2); e obter o parâmetro R com base ao menos no valor de criptografia x e diferenças entre pares dos fatores de ofuscamento (vide, por exemplo, a Etapa 2.4).

[078]O bloco 305 compreende: enviar a transação a um ou mais nós em uma rede de blockchain com a revelação do parâmetro R e sem a revelação dos tipos de dados de entrada e tipos de dados de saída aos nós para verificar a consistência entre os tipos de dados de entrada e os tipos de dados de saída. Em algumas modalidades, faz-se com que os nós verifiquem a consistência entre os tipos de dados de entrada e os tipos de dados de saída sem conhecimento dos tipos de dados de entrada e dos tipos de dados de saída.

[079]Em algumas modalidades, enviar a transação aos um ou mais nós na rede de blockchain com a revelação do parâmetro R e sem a revelação dos tipos de dados de entrada e tipos de dados de saída aos nós para verificar a consistência entre os tipos de dados de entrada e os tipos de dados de saída compreende enviar a transação aos um ou mais nós na rede de blockchain com a revelação do parâmetro R e sem a revelação dos tipos de dados de entrada e tipos de dados de saída para fazer com que os nós: obter o parâmetro R e um ponto de base G (vide, por exemplo, o G na Etapa 3.1. H e G podem ser parâmetros públicos disponíveis para todos os nós); obter diferenças entre pares dos valores de compromisso dos tipos de ativo de entrada e tipos de ativo de saída (vide, por exemplo, uma etapa semelhante à Etapa 2.1); concatenar as diferenças obtidas (vide, por exemplo, a Etapa 3.1); criptografar as diferenças concatenadas com uma função hash para obter um valor de criptografia x (vide, por exemplo, a Etapa 3.1); obter uma soma C de polinômios com

base ao menos nas diferenças obtidas e no valor de criptografia x (vide, por exemplo, a Etapa 3.2); em resposta à determinação de que a soma C é igual ao produto do parâmetro R e ponto de base G, determinar que os tipos de dados de entrada e os tipos de dados de saída são consistentes e adicionar a transação à blockchain (vide, por exemplo, a Etapa 3.3); e, em resposta à determinação de que a soma C não é igual ao produto do parâmetro R e ponto de base G, determinar que os tipos de dados de entrada e os tipos de dados de saída são inconsistentes e rejeitar a adição da transação à blockchain (vide, por exemplo, a Etapa 3.3).

[080]A FIG. 4 ilustra um fluxograma de um método exemplificativo 400 para proteção da informação de acordo com várias modalidades da presente invenção. O método 400 pode ser implementado por um ou mais componentes (por exemplo, nó i) do sistema 100 da FIG. 1. O nó i pode compreender um nó completo implementado em um servidor. O método 400 pode ser implementado por um sistema ou dispositivo (por exemplo, computador) que compreende um processador e um meio de armazenamento não transitório legível por computador (por exemplo, memória) que armazena instruções para ser executadas pelo processador para fazer com que o sistema ou dispositivo (por exemplo, o processador) execute o método 400. As operações do método 400 apresentadas abaixo visam a ser ilustrativas Dependendo da implementação, o método exemplificativo 400 pode incluir etapas a mais, a menos ou alternativas executadas em várias ordens ou em paralelo.

[081]O bloco 401 compreende: um ou mais nós (por exemplo, nós de consenso) em uma rede de blockchain obterem uma transação iniciada por um nó iniciador. A transação é associada a uma ou mais entradas de dados e uma ou mais saídas de dados. As entradas de dados são associadas respectivamente a tipos de dados de entrada, e as saídas de dados são associadas respectivamente a tipos de dados de saída respectivamente. Os tipos de dados de entrada e os tipos de dados de saída são criptografados e comprometidos a um esquema de compromisso para

obter valores de compromisso correspondentes. Os tipos de dados de entrada e os tipos de dados de saída não são revelados aos um ou mais nós.

[082]O bloco 402 compreende: os um ou mais nós verificarem a consistência entre os tipos de dados de entrada e os tipos de dados de saída; Em algumas modalidades, verificar a consistência entre os tipos de dados de entrada e os tipos de dados de saída compreende: obter um parâmetro R e um ponto de base G (vide, por exemplo, R nas Etapas 2.4 e 2.5, e G na Etapa 3.1); obter diferenças entre pares dos valores de compromisso dos tipos de ativo de entrada e tipos de ativo de saída (vide, por exemplo, uma etapa semelhante à Etapa 2.1); concatenar as diferenças obtidas (vide, por exemplo, a Etapa 3.1); criptografar as diferenças concatenadas com uma função hash para obter um valor de criptografia x (vide, por exemplo, a Etapa 3.1); obter uma soma C de polinômios com base ao menos nas diferenças obtidas e no valor de criptografia x (vide, por exemplo, a Etapa 3.2); e determinar se a soma C é igual ao produto do parâmetro R e ponto de base G (vide, por exemplo, a Etapa 3.3).

[083]O bloco 403 compreende: em resposta à determinação de que os tipos de dados de entrada e os tipos de dados de saída são consistentes, os um ou mais nós adicionarem a transação à rede de blockchain.

[084]O bloco 404 compreende: em resposta à determinação de que os tipos de dados de entrada e os tipos de dados de saída são inconsistentes, os um ou mais nós rejeitarem a adição da transação à rede de blockchain.

[085]Em algumas modalidades, o método compreende ainda: em resposta à determinação de que a soma C é igual ao produto do parâmetro R e ponto de base G, determinar que os tipos de dados de entrada e os tipos de dados de saída são consistentes; e, em resposta à determinação de que a soma C não é igual ao produto do parâmetro R e ponto de base G, determinar que os tipos de dados de entrada e os tipos de dados de saída são inconsistentes.

[086]Como tal, um iniciador de transação pode enviar informações para nós de blockchain a fim de verificar a transação com base na consistência da entrada e saída de tipos de ativo da transação sem revelar os tipos de ativo reais e sem a capacidade de alterar as informações enviadas. A alocação de números de série (por exemplo, hashes) para cada tipo de ativo alarga e randomiza a representação de cada tipo de ativo, dificultando que o iniciador de transação forje um tipo de ativo para passar a verificação. Além disso, por causa da existência do número aleatório r, o mesmo tipo de ativo criptografado em diferentes momentos não é o mesmo. Aplicar o compromisso de Pedersen para criptografar o hash de tipo de ativo aprimora a proteção à privacidade do tipo de ativo em um nível ainda mais alto. Assim, pelas Etapas de 2.1 a 2.5, o iniciador de transação pode comprovar aos outros nós que os tipos de ativo da transação são válidos sem revelar os tipos de ativo. Por exemplo, diferenças entre os tipos de ativo de entrada e saída são obtidas e baseadas nelas constroem-se polinômios, de tal modo que o iniciador de transação pode passar os tipos de ativo transformados aos outros nós para comprovar a consistência dos tipos de ativo e a autenticidade da transação. Ao mesmo tempo, a probabilidade de o iniciador de transação ou outro nó ser capaz de forjar o tipo de ativo pode ser negligenciada porque x é computado por hashing para servir como a base de vários exponenciais nos polinômios. Ademais, a revelação de R permite que os outros nós verifiquem se os tipos de ativo na transação são consistentes sem saber os tipos de artigos através das Etapas 3.1 a 3.3. Logo, com os sistemas e métodos revelados, informações de dados podem ser verificadas por terceiros, ao mesmo tempo em que mantém-se uma proteção à privacidade excepcional.

[087]As técnicas descritas neste documento são implementadas por um ou mais dispositivos de computação de propósito especial. Os dispositivos de computação de propósito especial podem ser sistemas de computador de mesa, sistemas de computador servidor, sistemas de computador portátil, dispositivos de mão, disposi-

tivos de rede ou qualquer outro dispositivo ou combinação de dispositivos que incorpore lógica com fio e/ou de programa para implementar as técnicas. Os dispositivos de computação de propósito especial podem ser sistemas de computador de mesa, sistemas de computador servidor, sistemas de computador portátil, dispositivos de mão, dispositivos de rede ou qualquer outro dispositivo ou combinação de dispositivos que incorpore lógica com fio e/ou de programa para implementar as técnicas. Sistemas operacionais convencionais controlam e agendam processos de computador para execução, realizam a gestão de memória, oferecem um sistema de arquivos, rede e serviços E/S, e oferecem funcionalidade de interface do usuário, tal como uma interface gráfica do usuário ("GUI"), entre outros.

[088]A FIG. 5 traz um diagrama em blocos que ilustra um sistema de computador 500 no qual qualquer uma das modalidades descritas neste documento pode ser implementada. O sistema 500 pode ser implementado em qualquer um dos nós descritos neste documento e configurado para realizar etapas correspondentes para métodos de proteção da informação. O sistema de computador 500 inclui um barramento 502 ou outro mecanismo de comunicação para comunicar informações e um ou mais processadores de hardware 504 acoplados ao barramento 502 para processar informações. Os um ou mais processadores de hardware 504 podem ser, por exemplo, um ou mais microprocessadores de propósito geral.

[089]O sistema de computador 500 também inclui uma memória principal 506, tal como uma memória de acesso aleatório (RAM), cache e/ou outros dispositivos de armazenamento dinâmico, acoplados a um barramento 502 para armazenar informações e instruções para ser executadas pelos um ou mais processadores 504. A memória principal 506 também pode ser usada para armazenar variáveis temporárias ou outras informações intermediárias durante a execução das instruções para ser executadas pelos um ou mais processadores 504. Essas instruções, quando armazenadas em meios de armazenamento acessíveis aos um ou mais processadores

504, tornam o sistema de computador 500 uma máquina de propósito especial que é personalizada para executar as operações especificadas nas instruções. O sistema de computador 500 inclui ainda uma memória somente para leitura (ROM) 508 ou outro dispositivo de armazenamento estático acoplado ao barramento 502 para armazenar informações e instruções para os um ou mais processadores 504. Um dispositivo de armazenamento 510, tal como um disco magnético, disco óptico ou mini-unidade USB (unidade Flash) etc., é provido e acoplado a um barramento 502 para armazenar informações e instruções.

[090]O sistema de computador 500 pode implementar as técnicas descritas neste documento usando lógica com fio personalizada, um ou mais ASICs ou FPGAs, firmware e/ou lógica de programa que, junto com o sistema de computador, fazem com que o sistema de computador 500 se torne ou programam-no para que seja uma máquina de propósito especial. De acordo com uma modalidade, as operações, métodos e processos descritos neste documento são realizados pelo sistema de computador 500 em resposta aos um ou mais processadores 504 executarem uma ou mais sequências de uma ou mais instruções contidas na memória principal 506. Essas instruções podem ser lidas na memória principal 506 a partir de outro meio de armazenamento, tal como dispositivo de armazenamento 510. A execução das sequências de instruções contidas na memória principal 506 faz com que os um ou mais processadores 504 executem as etapas de processo descritas neste documento. Em modalidades alternativas, um sistema de circuitos com fio pode ser usado no lugar de instruções de software ou em combinação às mesmas.

[091]A memória principal 506, a ROM 508 e/ou o dispositivo de armazenamento 510 podem incluir meios de armazenamento não transitórios. O termo “meios não transitórios” e termos semelhantes, conforme usados neste documento, referem-se a meios que armazenam dados e/ou instruções que fazem com que uma máquina opere de uma maneira específica; os meios excluem sinais transitórios. Esses meios

não transitórios podem compreender meios não voláteis e/ou meios voláteis. Meios não voláteis incluem, por exemplo, discos ópticos ou magnéticos, tais como o dispositivo de armazenamento 510. Meios voláteis incluem memória dinâmica, tal como a memória principal 506. Formas comuns de meios não transitórios legíveis por computador incluem, por exemplo, um disquete, um disco flexível, um disco rígido, uma unidade de estado sólido, uma fita magnética ou qualquer outro meio de armazenamento de dados magnético, um CD-ROM, qualquer outro meio de armazenamento de dados óptico, qualquer meio físico com padrões de orifícios, RAM, PROM e EPROM, FLASH-EPROM, NVRAM, qualquer outro chip ou cartucho de memória, e versões em rede dos mesmos.

[092]O sistema de computador 500 também inclui uma interface de rede 518 acoplada ao barramento 502. A interface de rede 518 oferece um acoplamento para a comunicação bidirecional de dados com um ou mais elos de rede que conectam-se a uma ou mais redes locais. Por exemplo, a interface de rede 518 pode ser um cartão de rede digital de serviços integrados (ISDN), cable modem, modem de satélite ou um modem para prover uma conexão para comunicação de dados com um tipo correspondente de linha telefônica. Em outro exemplo, a interface de rede 518 pode ser um cartão de rede de área local (LAN) para prover uma conexão de comunicação de dados com uma LAN compatível (ou componente WAN para comunicar-se com uma WAN). Elos sem fio também podem ser implementados. Em qualquer implementação desse tipo, a interface de rede 518 envia e recebe sinais elétricos, eletromagnéticos ou ópticos que transportam fluxos de dados digitais que representam vários tipos de informação.

[093]O sistema de computador 500 pode ler mensagens e receber dados, incluindo código de programa, através das uma ou mais redes, elo de rede e interface de rede 518. No caso da Internet, um servidor pode transmitir um código solicitado para um programa de aplicativo via Internet, ISP, rede local e interface de rede

518.

[094]O código recebido pode ser executado por um ou mais processadores 504 assim que recebido, e/ou ser armazenado no dispositivo de armazenado 510 ou outro meio de armazenamento não volátil para uso futuro.

[095]Cada um dos processos, métodos e algoritmos descritos nas seções anteriores pode ser incorporado a, e automatizado em parte ou por inteiro por, módulos de código executados por um ou mais sistemas de computador ou processadores de computador compreendendo hardware de computador. Os processos e algoritmos podem ser implementados em parte ou por inteiro em um sistema de circuitos de aplicação específica.

[096]Os vários traços e processos descritos acima podem ser usados independentemente uns dos outros, ou podem ser combinados de diversas maneiras. Tenciona-se que todas as combinações e subcombinações possíveis enquadrem-se no âmbito da presente invenção. Além disso, certos blocos de método ou processo podem ser omitidos em algumas implementações. Os métodos e processos descritos neste documento também não são limitados a nenhuma sequência específica, e os blocos e estados relacionados a eles podem ser executados em outras sequências que sejam apropriadas. Por exemplo, os blocos ou estados descritos podem ser executados em uma ordem diferente da especificamente revelada, ou vários blocos ou estados podem ser combinados em um único bloco ou estado. Os blocos ou estados exemplificativos podem ser executados em série, em paralelo ou de alguma outra maneira. Blocos ou estados podem ser adicionados às modalidades exemplificativas reveladas ou removidos delas. Os sistemas e componentes exemplificativos descritos neste documento podem ser configurados de maneira diferente da descrita. Por exemplo, é possível adicionar, remover ou reordenar elementos em comparação às modalidades exemplificativas reveladas.

[097]As várias operações de métodos exemplificativos descritas neste do-

cumento podem ser executadas, ao menos em parte, por um algoritmo. O algoritmo pode ser contido em códigos de programa ou instruções armazenadas em uma memória (por exemplo, um meio de armazenamento não transitório legível por computador descrito acima). Esse algoritmo pode compreender um algoritmo de aprendizagem de máquina. Em algumas modalidades, um algoritmo de aprendizagem de máquina pode não programar explicitamente os computadores para executar uma função, mas pode aprender com base em dados de treinamento para criar um modelo de predições que executa a função.

[098]As várias operações de métodos exemplificativos descritas neste documento podem ser realizadas, ao menos em parte, por um ou mais processadores configurados temporariamente (por exemplo, por software) ou permanentemente para realizar as operações relevantes. Sejam configurados temporária ou permanentemente, esses processadores podem constituir motores implementados por processador que operam para executar uma ou mais operações ou funções descritas neste documento.

[099]À semelhança, os métodos descritos neste documento podem ser implementados ao menos em parte por processador, sendo um ou mais processadores específicos um exemplo de hardware. Por exemplo, ao menos algumas das operações de um método podem ser executadas por um ou mais processadores ou motores implementados por processador. Além disso, os um ou mais processadores também podem operar para suportar o desempenho das operações relevantes em um ambiente de “computação em nuvem” ou como um “software como serviço” (SaaS). Por exemplo, ao menos algumas das operações podem ser realizadas por um grupo de computadores (como exemplo de máquinas com processadores), essas operações sendo acessíveis por meio de uma rede (por exemplo, a Internet) e por meio de uma ou mais interfaces adequadas (por exemplo, uma Interface de Programação de Aplicativos (API)).

[0100]O desempenho de algumas das operações pode ser distribuído entre os processadores, não só alojados dentro de uma única máquina, mas implementados em várias máquinas. Em algumas modalidades exemplificativas, os processadores ou motores implementados por processador podem situar-se em um mesmo local geográfico (por exemplo, dentro de uma casa, de um escritório ou de uma torre de servidores). Em outras modalidades exemplificativas, os processadores ou motores implementados por processador podem ser distribuídos em vários locais geográficos.

[0101]Ao longo deste relatório descritivo, instâncias no plural podem indicar a implementação de componentes, operações ou estruturas descritas como uma instância no singular. Embora operações individuais de um ou mais métodos sejam ilustradas e descritas como operações distintas, uma ou mais das operações individuais podem ser realizadas ao mesmo tempo e não há nenhuma restrição segundo a qual as operações devam ser realizadas na ordem ilustrada. As estruturas e funcionalidades apresentadas como componentes distintos em configurações exemplificativas podem ser implementadas como uma estrutura ou componente combinados. À semelhança, estruturas e funcionalidades apresentadas como um único componente podem ser implementadas como componentes distintos. Essas e outras variações, modificações, adições e melhorias encontram-se dentro do âmbito da matéria inventiva revelada neste documento.

[0102]Embora tenha-se descrito uma visão geral da matéria inventiva descrita com referência a modalidades exemplificativas específicas, ficará evidente que várias modificações e alterações podem ser feitas a essas modalidades sem divergir do âmbito, mais amplos, de modalidades da presente invenção. Essas modalidades da matéria inventiva podem ser indicadas neste documento, individual ou coletivamente, pelo termo “invenção” para fins meramente de conveniência e sem a intenção de limitar voluntariamente o âmbito deste pedido a qualquer invenção ou concei-

to inventivo exclusivo se, na prática, mais de um for revelado.

REIVINDICAÇÕES

1. Método implementado por computador para proteção da informação, **CARACTERIZADO** por compreender:

determinar uma ou mais entradas de dados e uma ou mais saídas de dados para uma transação, em que a uma ou mais entradas de dados correspondem, respectivamente a um ou mais tipos de ativos de entrada, e a uma ou mais saídas de dados correspondem, respectivamente, a um ou mais tipos de ativos de saída;

fazer hashing no um ou mais tipos de ativos de entrada e no um ou mais tipos de ativos de saída;

gerar uma pluralidade de valores de compromisso ao comprometer cada um dos tipos de ativos de entrada hasheados (*hashed*) e os tipos de ativos de saída hasheados de acordo com um esquema de compromisso, em que o esquema de compromisso é baseado em um ponto de base G e uma pluralidade de fatores de ofuscamento (*blinding factors*), correspondendo respectivamente aos tipos de ativos de entrada e os tipos de ativos de saída;

gerar uma pluralidade de diferenças, respectivamente, entre uma pluralidade de pares dos valores de compromisso;

concatenar a pluralidade de diferenças gerada;

gerar um valor hash ao fazer hashing na pluralidade concatenada de diferenças;

gerar um parâmetro R com base pelo menos no valor hash e diferenças entre uma pluralidade de pares de fatores de ofuscamento; e

submeter a transação a um ou mais nós em uma rede de blockchain com a revelação do parâmetro R e sem a revelação dos tipos de ativos de entrada e tipos de ativos de saída aos nós para verificar a consistência entre os tipos de ativos de entrada e os tipos de ativos de saída sem conhecimento dos tipos de ativos de entrada e tipos de ativos de saída.

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que:

a uma ou mais entradas de dados formam uma série de entrada ordenada começando a partir de uma primeira entrada de dados;

a uma ou mais saídas de dados formam uma série de saída ordenada começando a partir de uma primeira saída de dados; e

a pluralidade de diferenças compreende uma ou mais diferenças entre os valores de compromisso correspondentes a cada duas entradas de dados vizinhas na série de entrada ordenada, uma ou mais diferenças entre os valores de compromisso correspondentes a cada duas saídas de dados vizinhas na série de saída ordenada e uma diferença entre valores de compromisso correspondentes à primeira entrada de dados e à primeira saída de dados.

3. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a geração do parâmetro R com base pelo menos no valor hash e nas diferenças entre a pluralidade de pares dos fatores de ofuscamento compreende:

gerar o parâmetro R com base no valor de hash, uma ou mais diferenças entre fatores de ofuscamento correspondentes a cada duas entradas de dados vizinhas na série de entrada ordenada, uma ou mais diferenças entre fatores de ofuscamento correspondentes a cada duas saídas de dados vizinhas na série de saída ordenada e uma diferença entre fatores de ofuscamento correspondentes à primeira entrada de dados e à primeira saída de dados.

4. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que: o esquema de compromisso compreende um compromisso de Pedersen.

5. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que quaisquer duas das uma ou mais entradas de dados ou saídas de dados que são comprometidas em diferentes pontos de tempo correspondem a diferentes fatores de ofuscamento.

6. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que submeter a transação aos um ou mais nós na rede de blockchain com a revelação do parâmetro R e sem a revelação dos tipos de ativos de entrada e tipos de ativos de saída aos nós para verificar a consistência entre os tipos de ativos de entrada e os tipos de ativos de saída sem o conhecimento dos tipos de ativos de entrada e tipos de ativos de saída compreende fazer com que os nós:

obtenham o parâmetro R e um ponto de base G;

obtenham uma pluralidade de diferenças não verificadas entre a pluralidade de pares de valores de compromisso;

concatenem a pluralidade de diferenças não verificadas obtidas;

gerem um valor de hash não verificado, fazendo hashing na pluralidade concatenada de diferenças não verificadas;

gerem uma soma C de polinômios com base ao menos na pluralidade de diferenças não verificadas e o valor de hash não verificado;

em resposta à determinação de que a soma C é igual ao produto do parâmetro R e ponto de base G, determinem que os tipos de ativos de entrada e os tipos de ativos de saída são consistentes; e

em resposta à determinação de que a soma C não é igual ao produto do parâmetro R e do ponto de base G, determinem que os tipos de ativos de entrada e os tipos de ativos de saída são inconsistentes.

7. Método, de acordo com a reivindicação 6, **CARACTERIZADO** pelo fato de que compreende adicionalmente fazer com que um ou mais nós, em resposta à determinação de que os tipos de ativos de entrada e os tipos de ativos de saída são consistentes, adicionem a transação a uma blockchain.

8. Meio de armazenamento não transitório legível por computador **CARACTERIZADO** por armazenar instruções para ser executadas por um processador para fazer com que o processador execute o método conforme definido nas

reivindicações de 1 a 7.

9. Sistema para proteção da informação, **CARACTERIZADO** pelo fato de que compreende um processador e um meio de armazenamento legível por computador não transitório acoplado ao processador, o meio de armazenamento armazenando instruções para serem executadas pelo processador para fazer com que o sistema realize operações compreendendo o método conforme definido em qualquer uma das reivindicações de 1 a 7.

10. Método implementado por computador para proteção de informação **CARACTERIZADO** pelo fato de que compreende:

obter, por um ou mais nós em uma rede blockchain, uma pluralidade de diferenças não verificadas entre uma pluralidade de pares de valores de compromisso, um ponto de base G e um parâmetro R, em que:

uma transação iniciada por um nó iniciador corresponde a uma ou mais entradas de dados e uma ou mais saídas de dados,

a uma ou mais entradas de dados correspondem, respectivamente, a um ou mais tipos de ativos de entrada,

a uma ou mais saídas de dados correspondem, respectivamente, a um ou mais tipos de ativos de saída,

o um ou mais tipos de ativos de entrada e o um ou mais tipos de ativos de saída são hasheados (*hashed*),

a pluralidade de valores de compromisso são saídas de comprometimento de cada um dos tipos de ativos de entrada hasheados e tipos de ativos de saída hasheados de acordo com um esquema de compromisso com base no ponto de base G e uma pluralidade de fatores de ofuscamento, correspondendo, respectivamente, aos tipos de ativos de entrada e os tipos de ativos de saída , e

o um ou mais tipos de ativos de entrada e o um ou mais tipos de ativos de saída não são divulgados para os um ou mais nós;

concatenar a pluralidade de diferenças não verificadas;

gerar, por um ou mais nós, um valor hash não verificado, fazendo hashing na pluralidade concatenada de diferenças não verificadas;

gerar, por um ou mais nós, uma soma C de polinômios com base, pelo menos, na pluralidade de diferenças não verificadas e no valor de hash não verificado;

determinar, por um ou mais nós, se a soma C é igual a um produto do parâmetro R e o ponto base G; e

em resposta à determinação de que a soma C é igual ao produto do parâmetro R e o ponto base G, determinar que os tipos de ativos de entrada e os tipos de ativos de saída são consistentes; e

em resposta à determinação de que a soma C não é igual ao produto do parâmetro R e do ponto base G, determinar que os tipos de ativos de entrada e os tipos de ativos de saída são inconsistentes.

11. Método, de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que compreende adicionalmente:

em resposta à determinação de que os tipos de ativos de entrada e os tipos de ativos de saída são consistentes, adicionar, por um ou mais nós, a transação à rede blockchain; e

em resposta à determinação de que os tipos de ativos de entrada e os tipos de ativos de saída são inconsistentes, rejeitar, por um ou mais nós, que a transação seja adicionada à rede blockchain.

12. Método, de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que:

a uma ou mais entradas de dados formam uma série de entrada ordenada começando a partir de uma primeira entrada de dados;

a uma ou mais saídas de dados formam uma série de saída ordenada começando a partir de uma primeira saída de dados; e

a pluralidade de diferenças não verificadas compreende uma pluralidade de diferenças entre os valores de compromisso correspondentes a cada duas entradas de dados vizinhas na série de entrada ordenada, uma ou mais diferenças entre os valores de compromisso correspondentes a cada duas saídas de dados vizinhas na série de saída ordenada e uma diferença entre valores de compromisso correspondentes à primeira entrada de dados e à primeira saída de dados.

13. Meio de armazenamento legível por computador não transitório **CARACTERIZADO** pelo fato de que armazena instruções para serem executadas por um processador, fazendo com que o processador realize operações compreendendo o método conforme definido em qualquer uma das reivindicações de 10 a 12.

14. Sistema para proteção de informações **CARACTERIZADO** pelo fato de que compreende um processador e um meio de armazenamento legível por computador não transitório acoplado ao processador, o meio de armazenamento armazenando instruções a serem executadas pelo processador para fazer com que o sistema realize operações compreendendo o método conforme definido em qualquer uma das reivindicações de 10 a 12.

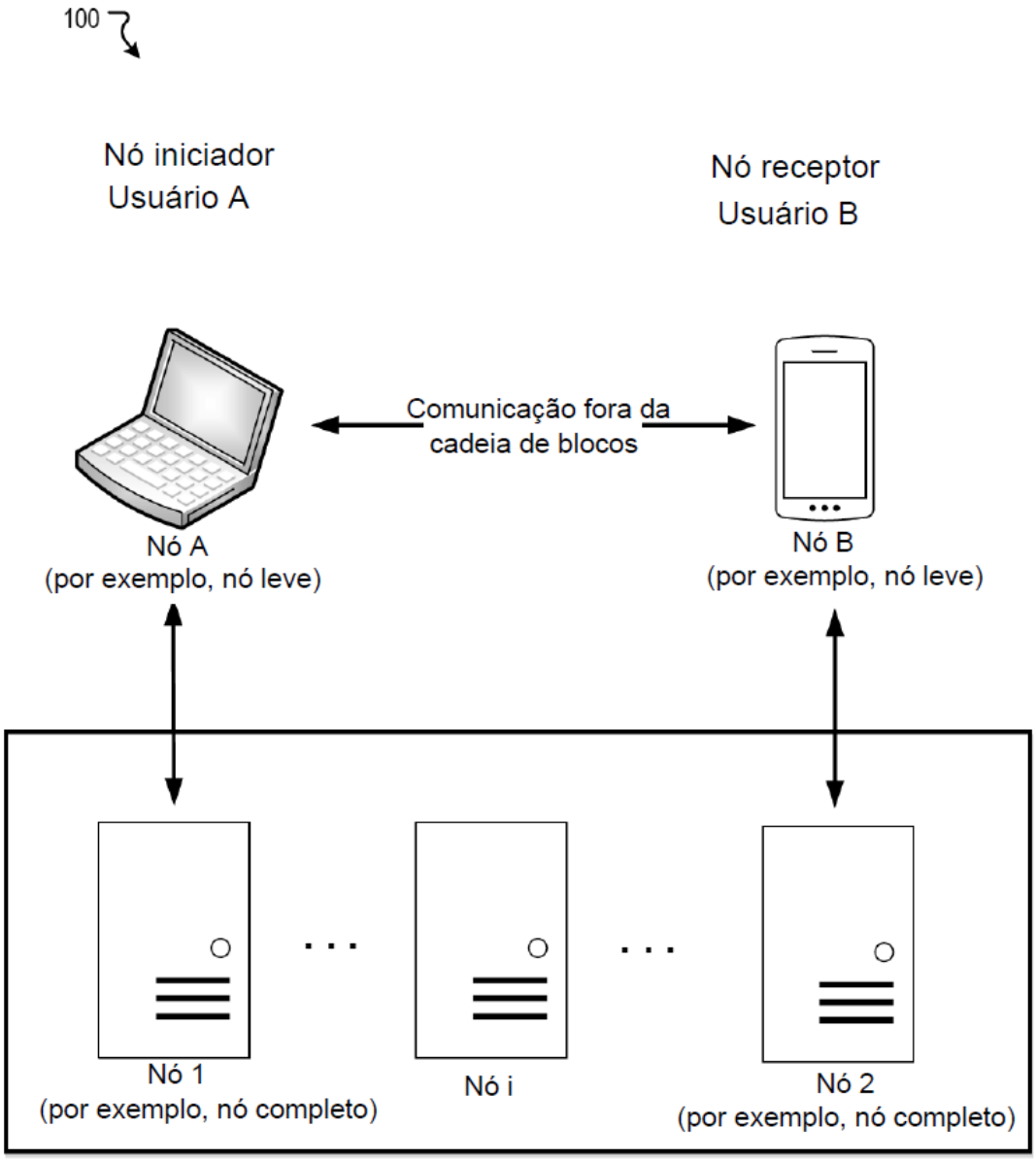
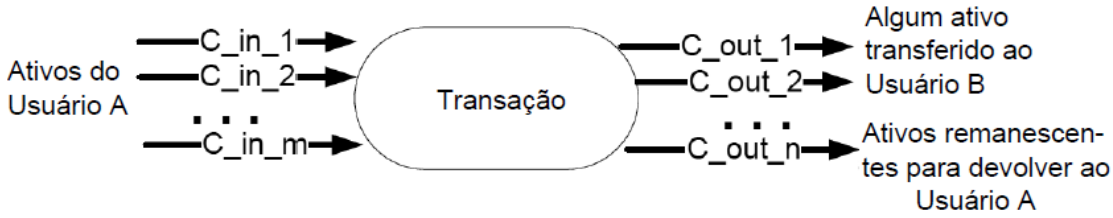

100
Nó iniciador
Usuário A
Nó receptor
Usuário B
Comunicação fora da
cadeia de blocos
Nó A
(por exemplo, nó leve)
Nó B
(por exemplo, nó leve)
Nó 1
(por exemplo, nó completo)
Nó i
Nó 2
(por exemplo, nó completo)

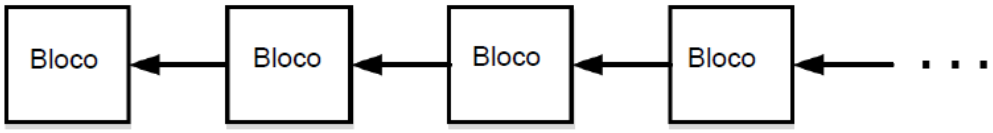
FIG. 1

Nó iniciador inicia uma transação para ser adicionada à cadeia de blocos

1. Iniciar transação



2. Calcular x, C e R e publicar R para os nós



Nó de consenso verifica se a transação é válida

3.1. Calcular x

3.2. Calcular c

3.3. Verificar se C=rG para validar a transação

4. Adicionar a transação à cadeia de blocos ou rejeitar com base na validade

FIG. 2

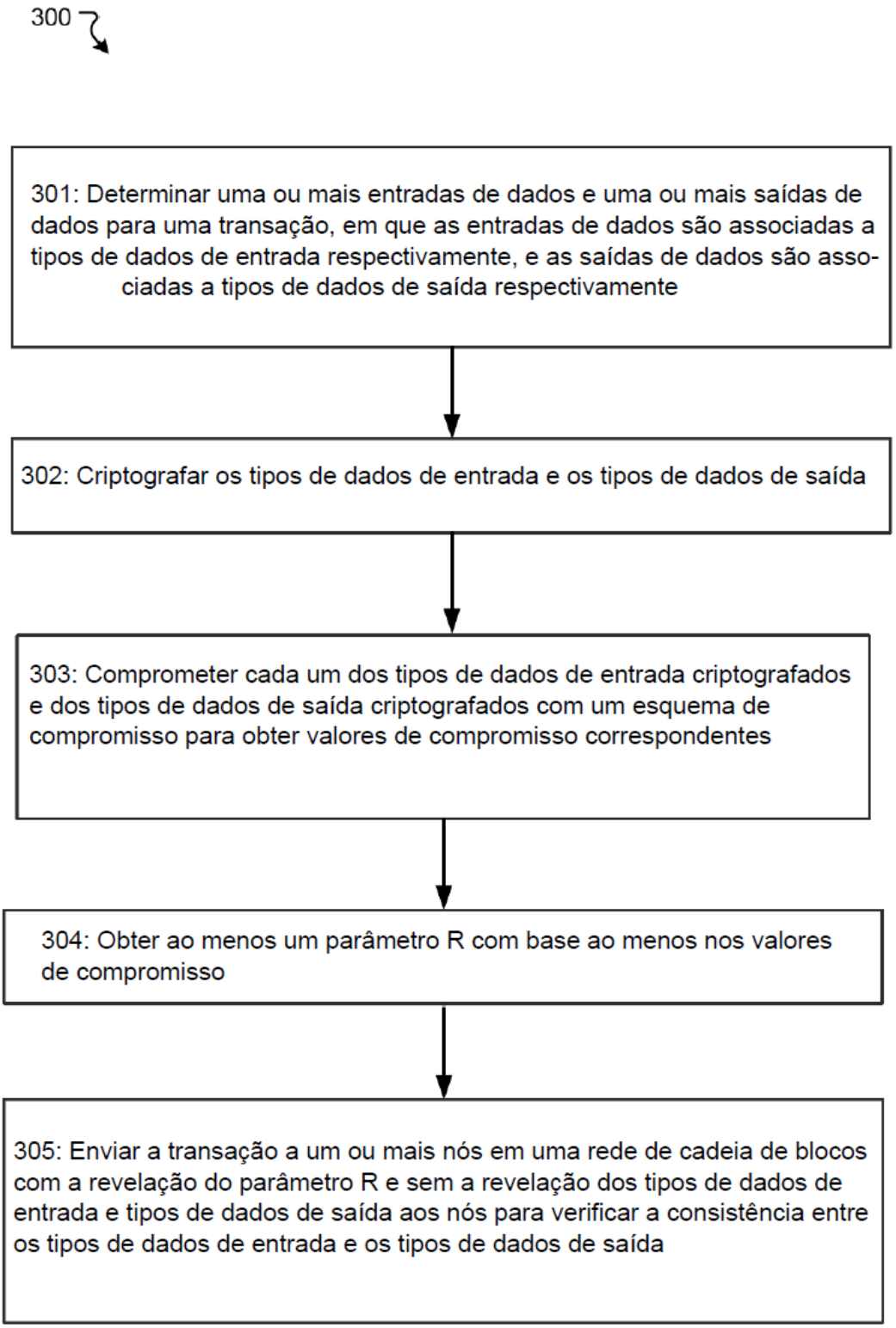

300
301: Determinar uma ou mais entradas de dados e uma ou mais saídas de dados para uma transação, em que as entradas de dados são associadas a tipos de dados de entrada respectivamente, e as saídas de dados são associadas a tipos de dados de saída respectivamente
302: Criptografar os tipos de dados de entrada e os tipos de dados de saída
303: Comprometer cada um dos tipos de dados de entrada criptografados e dos tipos de dados de saída criptografados com um esquema de compromisso para obter valores de compromisso correspondentes
304: Obter ao menos um parâmetro R com base ao menos nos valores de compromisso
305: Enviar a transação a um ou mais nós em uma rede de cadeia de blocos com a revelação do parâmetro R e sem a revelação dos tipos de dados de entrada e tipos de dados de saída aos nós para verificar a consistência entre os tipos de dados de entrada e os tipos de dados de saída

FIG. 3

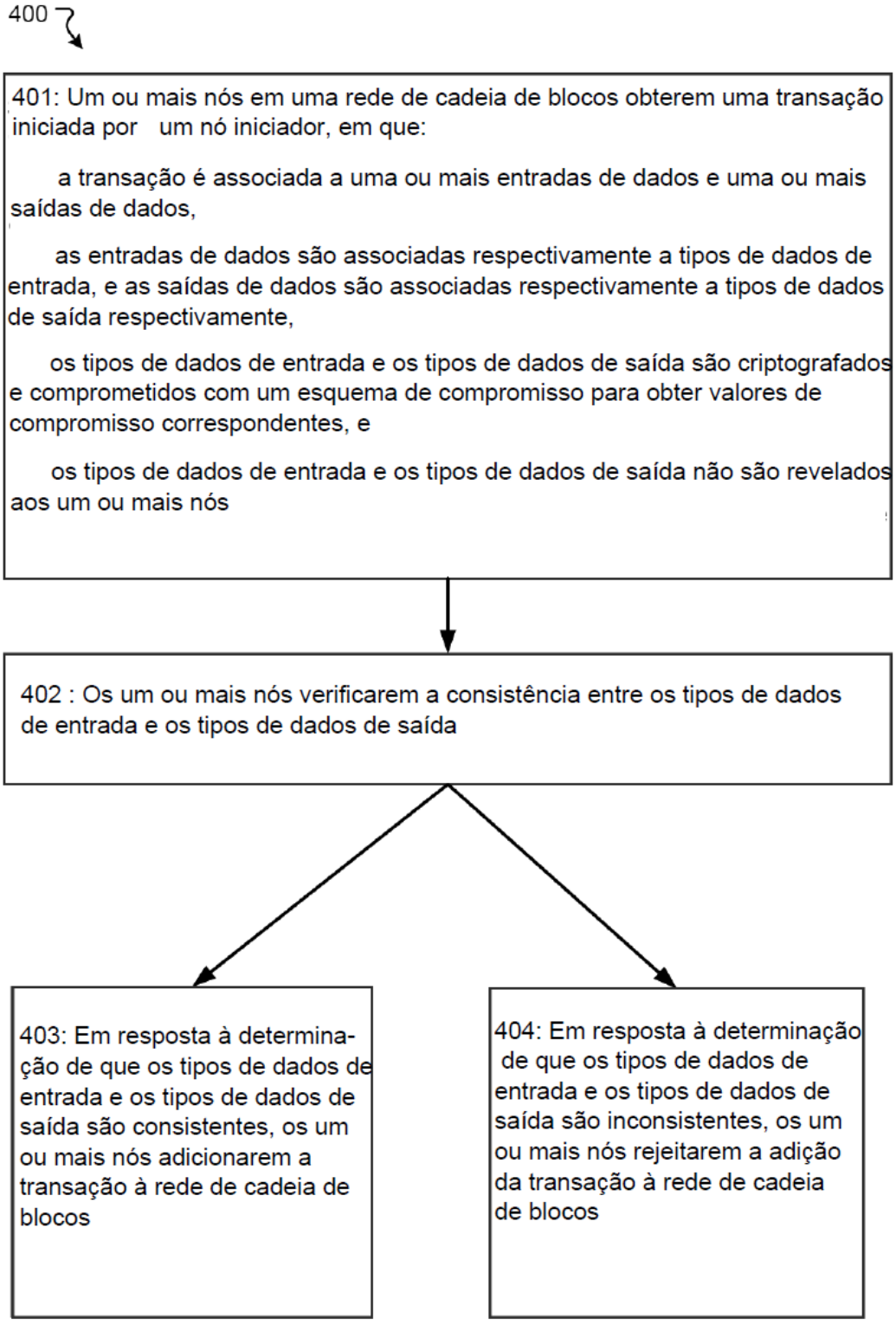

400
401: Um ou mais nós em uma rede de cadeia de blocos obterem uma transação iniciada por um nó iniciador, em que:
a transação é associada a uma ou mais entradas de dados e uma ou mais saídas de dados,
as entradas de dados são associadas respectivamente a tipos de dados de entrada, e as saídas de dados são associadas respectivamente a tipos de dados de saída respectivamente,
os tipos de dados de entrada e os tipos de dados de saída são criptografados e comprometidos com um esquema de compromisso para obter valores de compromisso correspondentes, e
os tipos de dados de entrada e os tipos de dados de saída não são revelados aos um ou mais nós
402 : Os um ou mais nós verificarem a consistência entre os tipos de dados de entrada e os tipos de dados de saída
403: Em resposta à determinação de que os tipos de dados de entrada e os tipos de dados de saída são consistentes, os um ou mais nós adicionarem a transação à rede de cadeia de blocos
404: Em resposta à determinação de que os tipos de dados de entrada e os tipos de dados de saída são inconsistentes, os um ou mais nós rejeitarem a adição da transação à rede de cadeia de blocos

FIG. 4

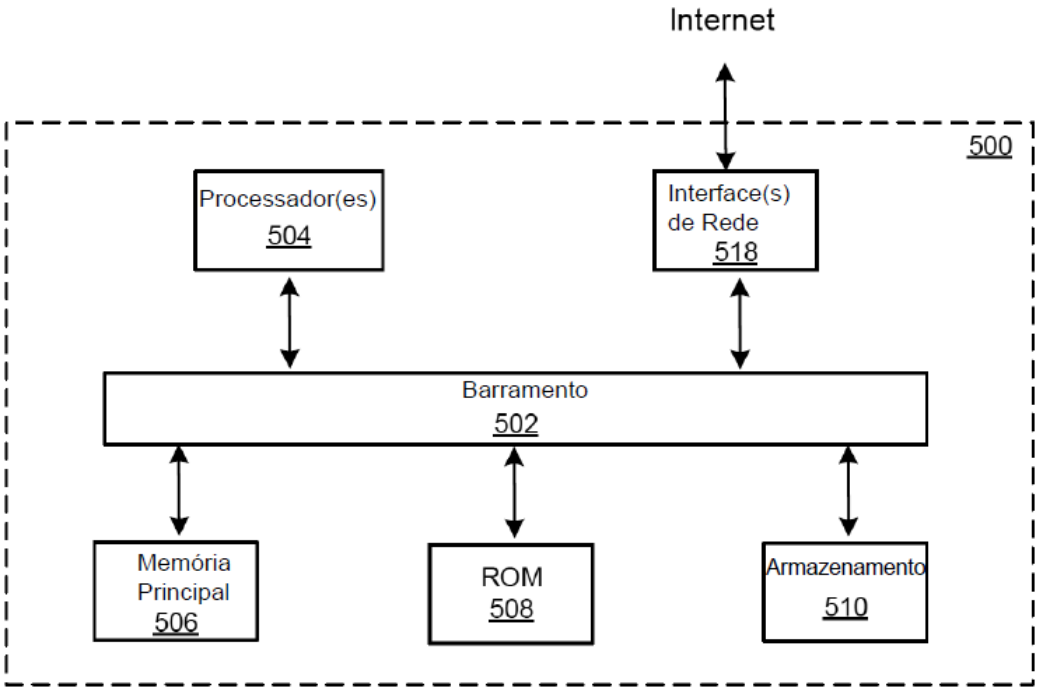

Internet
500
Processador(es)
504
Interface(s)
de Rede
518
Barramento
502
Memória
Principal
506
ROM
508
Armazenamento
510

FIG. 5