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

(21) BR 112019010751-7 A2

(22) Data do Depósito: 29/12/2018

(43) Data da Publicação Nacional: 31/12/2019

(54) Título: SISTEMA E MÉTODO PARA PROTEÇÃO DE INFORMAÇÃO

(51) Int. Cl.: G06Q 40/02.

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

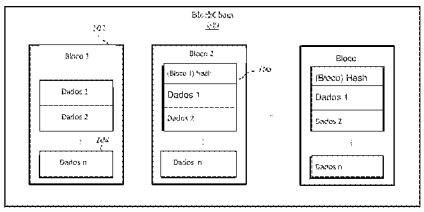
(72) Inventor(es): WENBIN ZHANG; LICHUN LI; BAOLI MA.

(86) Pedido PCT: PCT CN2018125749 de 29/12/2018

(87) Publicação PCT: WO 2019/072313 de 18/04/2019

(85) Data da Fase Nacional: 24/05/2019

(57) Resumo: A presente invenção se refere a um método de proteção de informação implementado por computador que compreende: obter uma pluralidade de valores de transação criptografados associados a transações entre uma pluralidade de contas, em que cada um dos valores de transação criptografados é associado a uma das contas que envia ou recebe um dos valores de transação, e a criptografia de cada um dos valores da transação pelo menos oculta se uma conta envia ou recebe um dos valores da transação; gerar uma prova de soma com base nos valores de transação criptografados obtidos, a prova de soma pelo menos indicando que os valores da transação estão equilibrados; e transmitir os valores de transação criptografados e a prova de soma para um ou mais nós em uma rede blockchain para que os nós verificarem as transações.



"SISTEMA E MÉTODO PARA PROTEÇÃO DE INFORMAÇÃO"

CAMPO DA TÉCNICA

[001] Essa divulgação refere-se em geral a tecnologias de computador e, em particular, a sistemas e métodos para proteção de informação.

FUNDAMENTOS DA INVENÇÃO

[002] A privacidade é importante para comunicações e transferências de dados entre vários usuários. Por exemplo, as informações referentes ao remetente, ao destinatário, e ao valor da transação entre as partes são partes importante da proteção da privacidade. Sem proteção, os usuários estão expostos ao risco de roubo de identidade, transferência ilegal ou outras perdas potenciais. O risco torna-se ainda maior quando as comunicações e transferências são implementadas on-line, devido ao livre acesso de informações on-line.

SUMÁRIO DA INVENÇÃO

[003] Várias modalidades da presente divulgação podem incluir sistemas, métodos e meios não transitórios legíveis por computador para proteção da informação.

[004] De acordo com um aspecto, um método de proteção de informação implementado por computador compreende: obter uma pluralidade de valores de transação criptografada associada a transações entre uma pluralidade de contas, em que cada um dos valores de transação criptografados é associado a uma das contas que envia ou recebe um dos valores da transação, e a criptografia de cada um dos valores da transação, pelo menos, oculta se uma conta envia ou recebe um dos valores da transação; gerar uma prova de soma com base nos valores de transação criptografados obtidos, a prova de soma, pelo menos, indicando que os valores da transação estão equilibrados; e transmitir os valores de transação criptografados e a prova de soma para um ou mais nós em uma rede “blockchain” (o protocolo de confiança) para que os nós verifiquem as transações.

[005] Em algumas modalidades, a criptografia de cada um dos valores de transação, pelo menos, oculta se uma conta envia ou recebe um dos valores de transação, ocultando se cada um dos valores de transação é de entrada ou de saída para uma conta.

[006] Em algumas modalidades, antes de gerar a prova de soma, o método compreende ainda: obter uma pluralidade de provas de variação, respectivamente, para as contas envolvidas nas transações, as provas de variação, indicando pelo menos que cada uma das contas que envia os valores de transação tem ativo suficiente.

[007] Em algumas modalidades, antes de transmitir os valores de transação criptografados e a prova de soma para um ou mais nós, o método compreende ainda: obter uma pluralidade de assinaturas, respectivamente, das contas. Transmitir os valores de transação criptografados e a prova de soma para um ou mais nós na rede blockchain para que os nós verifiquem as transações compreende transmitir os valores de transação criptografados, as provas de variação, a prova de soma e as assinaturas para o um ou mais nós na rede blockchain para que os nós verifiquem as transações com base nos valores de transação criptografados, nas provas de variação, na prova de soma e nas assinaturas.

[008] Em algumas modalidades, transmitir as valores de transação criptografados, as provas de variação, a prova de soma e as assinaturas para um ou mais nós na rede blockchain para que os nós verifiquem as transações com base nos valores de transação criptografados, nas provas de variação, na prova da soma e nas assinaturas compreende: transmitir os valores de transação criptografados, as provas de variação, a prova de soma e as assinaturas para um ou mais nós na rede blockchain; e levando os nós a: validarem as valores de transação criptografados, as provas de variação, a prova da soma e as assinaturas, executar as transações em resposta à verificação bem sucedida das transações e adicionar as transações em

um novo bloco de dados de um blockchain mantido pela rede blockchain.

[009] Em algumas modalidades, fazer com que os nós executem as transações em resposta à verificação bem-sucedida das transações compreende: fazer com que os nós deduzam as valores de transação criptografados correspondentemente dos saldos de conta criptografados das contas em resposta à verificação bem sucedida das transações.

[010] Em algumas modalidades, a criptografia de cada uma dos valores de transação compreende uma criptografia homomórfica.

[011] Em algumas modalidades, a criptografia de cada um dos valores de transação compreende um esquema de Compromisso de Pedersen.

[012] De acordo com outro aspecto, um sistema de proteção de informação compreende um ou mais processadores e uma ou mais memórias não transitórias legíveis por computador acopladas ao um ou mais processadores e configuradas com instruções executáveis por um ou mais processadores levar o sistema a realizar operações compreendendo: obter uma pluralidade de valores de transação criptografados associados a transações entre uma pluralidade de contas, em que cada um dos valores de transação criptografados é associado a uma das contas que envia ou recebe um dos valores de transação, e a criptografia de cada um dos valores da transação, pelo menos, oculta se uma conta envia ou recebe aquele dos valores da transação; gerar uma prova de soma com base nos valores de transação criptografados obtidos, a prova de soma pelo menos indicando que os valores da transação estão equilibrados; e transmitir os valores de transação criptografados e a prova de soma para um ou mais nós em uma rede blockchain para os nós verificarem as transações.

[013] De acordo com outro aspecto, um meio de armazenamento não transitório legível por computador é configurado com instruções executáveis por um ou mais processadores para fazer com que um ou mais processadores executem

operações compreendendo: obter uma pluralidade de valores de transação criptografados associados a transações entre uma pluralidade de contas, em que cada um dos valores de transação criptografados é associado a uma das contas que envia ou recebe um dos valores de transação, e a criptografia de cada um dos valores de transação pelo menos oculta se uma conta envia ou recebe aquela dos valores da transação; gerar uma prova de soma com base nos valores de transação criptografados obtidos, na prova de soma pelo menos indicando que os valores da transação estão equilibrados; e transmitir os valores de transação criptografados e a prova de soma para um ou mais nós em uma rede blockchain para os nós verificarem as transações.

[014] Estas e outras características dos sistemas, métodos e meios não transitórios legíveis por computador aqui divulgados, bem como os métodos de operação e funções dos elementos relacionados da estrutura e combinação de partes e economias de fabricação, tornar-se-ão mais claros com a consideração da descrição que se segue e das reivindicações anexas com referência aos desenhos anexos, os quais fazem parte deste relatório, em que números de referência semelhantes designam partes correspondentes nas várias figuras. Contudo, deve ser expressamente entendido que os desenhos são apenas para fins de ilustração e descrição e não pretendem ser uma definição dos limites da invenção.

BREVE DESCRIÇÃO DOS DESENHOS

[015] Determinadas características de várias modalidades da presente tecnologia são estabelecidas com particularidade nas reivindicações anexas. Uma melhor compreensão dos recursos e as vantagens da tecnologia serão obtidas por referência à descrição detalhada que se segue que estabelece modalidades ilustrativas, nas quais os princípios da invenção são utilizados, e aos desenhos anexos dos quais:

[016] A Figura 1 ilustra uma blockchain exemplificativa, de acordo com várias

modalidades.

[017] A Figura 2 lustra uma rede blockchain exemplificativa para proteção de informação, de acordo com várias modalidades.

[018] A Figura 3 ilustra um fluxo de execução de transação exemplificativo com remetentes e destinatários mistos, de acordo com várias modalidades.

[019] A Figura 4 ilustra um fluxograma de um método exemplificativo para proteção de informação, de acordo com várias modalidades.

[020] A Figura 5 ilustra um fluxograma de outro método exemplificativo para proteção de informação, de acordo com várias modalidades.

[021] A Figura 6 ilustra um fluxograma de um método exemplificativo para proteção de informação, de acordo com várias modalidades.

[022] A Figura 7 ilustra um diagrama de bloco de um sistema de computador exemplificativo no qual qualquer uma das modalidades aqui descritas pode ser implementada.

DESCRIÇÃO DETALHADA DAS MODALIDADES

[023] Será feita agora referência detalhada às modalidades exemplificativas, cujos exemplos são ilustrados nos desenhos em anexo. A descrição que se segue refere-se aos desenhos em anexo, nos quais os mesmos números em desenhos diferentes representam os mesmos elementos ou elementos semelhantes, salvo indicação em contrário. As implementações apresentadas na descrição que se segue das modalidades exemplificativas consistentes com a presente invenção não representam todas as implementações consistentes com a invenção. Em vez disso, elas são apenas exemplos de sistemas e métodos consistentes com aspectos relacionados à invenção.

[024] A tecnologia blockchain pode ser construída em uma rede ponto a ponto (igual), usando algoritmo de consenso de nó distribuído para validar e atualizar dados. O blockchain também pode usar criptografia para garantir a

segurança da transmissão e acesso de dados e usar contratos incluindo código de script automatizado para programar e manipular dados. Um blockchain pode incluir uma série de blocos de dados, cada um incluindo um cabeçalho que liga ao bloco de dados anterior, formando assim uma cadeia de blocos de dados. Para estabelecer o link, o cabeçalho de um bloco de dados atual pode incluir um hash criptográfico ou uma soma de verificação do cabeçalho do bloco de dados anterior. Uma rede blockchain pode facilitar a execução de transações. Uma transação refere-se a qualquer comunicação entre usuários (nós de usuário, como seus dispositivos de computação) ou entre um usuário e uma entidade financeira. Por exemplo, uma transação pode se referir a uma compra ou venda de bens ou serviços, uma oferta ou um retorno de bens ou serviços, uma transação de pagamento, uma transação de crédito ou outras interações semelhantes. Uma transação também pode ser chamada de “negócio” ou “negociação”. O objeto da transação pode compreender, por exemplo, dinheiro, símbolo, moeda digital, contrato, escritura, registro médico, detalhes do cliente, estoque, título, fiança, patrimônio líquido ou qualquer outro ativo que possa ser descrito em formato digital.

[025] O Blockchain pode ser considerado como um livro digital,compartilhado, à prova de adulteração, que registra transações em uma rede ponto a ponto pública ou privada. O livro é distribuído aos nós membros na rede e um histórico de transações de ativos ocorrendo na rede é registrado no blockchain. Como o livro do blockchain é público e o próprio livro não tem função de proteção da privacidade, informações importantes sobre transações no livro são expostas ao público e sob o risco de uso não autorizado ou maldoso. Por exemplo, em estruturas de transação de blockchain existentes, as transações precisam indicar explicitamente qual parte deve enviar um ativo, qual parte deve receber o ativo e o valor do ativo da transação, nenhum dos quais está protegido. Para pelo menos mitigar as deficiências nas tecnologias existentes e melhorar a funcionalidade de

proteção de informação de computadores, sistemas e métodos para proteção de informação são divulgados com referência às Figuras 1 a 7.

[026] A Figura 1 ilustra um blockchain exemplificativo, de acordo com várias modalidades. Como mostrado na Figura 1, um blockchain 100 pode incluir uma pluralidade de blocos de dados 102. Cada bloco 102 é uma estrutura de dados que inclui dados 104 incluindo, por exemplo, transações, recibos de pagamento, etc. Cada bloco pode ligar ao bloco anterior através de um hash criptográfico. Por exemplo, o bloco 2 está ligado ao bloco 1 através de um hash 106 do bloco 1, o bloco n está ligado ao bloco n-1 através de outro hash do bloco n-1. À medida que novos dados são submetidos e validados, blocos adicionais, incluindo os novos dados, podem ser gerados e anexados ao último bloco do blockchain 100, incluindo o hash do bloco anterior.

[027] A Figura 2 ilustra uma rede blockchain exemplificativa 200 para executar transações, de acordo com várias modalidades. Como mostrado na Figura 2, a rede blockchain 200 pode incluir uma pluralidade de nós 202 e um ou mais dispositivos de computação de usuário 240, que podem se comunicar entre si através de um ou mais caminhos de comunicação. Um caminho de comunicação exemplificativo é uma rede 220 (por exemplo, conexões com ou sem fio, pela Internet, etc.) que usa um ou mais protocolos de comunicação, por exemplo, celular, WiFi e outros protocolos de comunicação, para transmitir e receber dados. A rede 220 pode ser baseada num modelo ponto a ponto e / ou num modelo cliente / servidor. Em algumas modalidades, a pluralidade de nós 202 pode compreender dispositivos de computação, cada um incluindo um ou mais processadores 204 e uma ou mais memórias 206 (por exemplo, uma ou mais instruções de armazenamento de mídia de armazenamento não transitórias legíveis por computador) acopladas a um ou mais processadores 204. O nó 202 pode ser um sistema exemplificativo para melhorar a segurança do contrato inteligente. A uma ou

mais memórias podem ser configuradas com instruções executáveis pelo um ou mais processadores para fazer com que o sistema (por exemplo, o um ou mais processadores) execute operações aqui descritas. Em algumas modalidades, o processador 204 pode ser implementado parcial ou totalmente como um ou mais circuitos lógicos. Em algumas modalidades, os nós 202 e os dispositivos de computação do usuário 240 podem incluir outros recursos de computação e / ou ter acesso (por exemplo, através de uma ou mais conexões / redes) a outros recursos de computação.

[028] Em algumas modalidades, o blockchain 100 é armazenado de forma descentralizada na pluralidade de nós 202. Em algumas modalidades, alguns dos nós 202 podem validar transações que receberam através de consenso e propagar as transações validadas para os outros nós 202. Consequentemente, os nós 202 podem atualizar o livro 208 de acordo com as transações validadas. Os nós 202 podem se comunicar entre si através da rede 220 para transmitir e receber dados relacionados ao livro 208. O livro razão 208 inclui os blocos de dados 102 que foram validados e adicionados ao blockchain 100. À medida que novos blocos de dados são adicionados ao livro 208, os nós 202 podem comunicar ou partilhar os novos blocos de dados através da rede 220. A memória 206 dos nós 202 pode armazenar pelo menos uma parte do livro 208 do blockchain 100.

[029] Em algumas modalidades, um ou mais usuários podem enviar transações para um ou mais nós 202 através dos dispositivos de computação de usuário 240 através dos caminhos de comunicação 220. Em algumas modalidades, as transações enviadas podem ser armazenadas temporariamente em um reservatório existente em toda a memória 206 nos nós 202 ou em uma base de dados remota acessível através a rede 220. Um ou mais dos nós 202 podem recuperar as transações submetidas do reservatório e processar as transações submetidas. Para concisão e simplicidade, a presente divulgação pode usar a forma

singular do nó 202. Aquele versado na técnica deve apreciar que a rede blockchain pode ter múltiplos nós 202 e um ou mais nós 202 podem estar envolvidos no processamento de uma transação. A forma singular do nó 202 pode representar um ou mais nós.

[030] Em algumas modalidades, o nó 202 pode atualizar o blockchain 100 com base nos resultados das transações. Em algumas modalidades, uma transação pode envolver dois ou mais participantes (também referidos como partes ou usuários, como um remetente e um destinatário). A transação pode ser um acordo entre as duas partes para troca de ativo (s). Por exemplo, uma transação pode incluir a transferência de uma parte ou o pagamento de um valor do ativo à outra parte, e o valor do pagamento pode ser acordado por ambas as partes. O ativo pode ter a forma de moeda digital, por exemplo, Bitcoin, Monero, etc. Alternativamente, o ativo pode ser uma moeda convencional, como dólares. As partes das transações podem estar associadas a contas, respectivamente. Cada conta das partes pode ter um endereço e um saldo armazenado no blockchain 100. Assim, após a transação ser executada, o nó 202 pode atualizar o saldo de cada conta das partes.

[031] Em algumas modalidades, o nó 202 pode executar a transação sem o conhecimento de qual parte é um remetente que envia ou paga o ativo e qual parte é um destinatário que recebe o ativo. Os sistemas e métodos divulgados podem ocultar as informações sobre qual parte é um remetente e qual parte é um destinatário, mas ainda permitir que a transação blockchain seja processada. Em algumas modalidades, a valor de ativo a ser transacionado pode ser rotulada com positivo ou negativo para indicar se a parte associada à quantia de ativo é um remetente ou um destinatário. Por exemplo, em uma transação entre a parte A e a parte B, uma quantia de $ 1.000 (positiva) para A indica que a parte A envia $ 1.000 para a parte B, enquanto uma quantia de - $ 1.000 (negativa) para A indica que a parte A recebe $ 1.000 da parte B. Portanto, se o valor da transação de uma conta A

for maior que zero, a conta A pagará ou enviará o valor da transação para outra conta B e, portanto, essa conta A será um remetente. Por outro lado, se o valor da transação de uma conta A for menor que zero (negativo), a conta A deve receber o valor e a conta A será um destinatário.

[032] Em algumas modalidades, a valor de transação pode ser criptografado através de vários métodos de criptografia. Em um exemplo, o valor da transação pode ser criptografado por meio de criptografia homomórfica. O esquema de criptografia homomórfica pode incluir, mas não se limitar a, criptografia homomórfica de Elgamal, criptografia homomórfica de Paillier, criptografia homomórfica de Benaloh, criptografia homomórfica de Okamoto-Uchiyama, criptografia homomórfica de Naccache-Stern, criptografia homomórfica de Damgård-Jurik, criptografia homomórfica de Boneh-Goh-Nissim, etc. Em outro exemplo, o valor da transação pode ser criptografado por meio de um esquema de comprometimento, como um compromisso homomórfico. Por exemplo, o compromisso homomórfico pode ser um Compromisso de Pedersen. O Compromisso Pedersen "T" de um valor de transação "t" pode ser representado como se segue.

$$T = PC(r, t) = rG + tH,$$

onde r é um fator de ofuscante aleatório (alternativamente referido como fator ofuscante) que fornece ocultação, G e H são os geradores acordados publicamente ou pontos de base da curva elíptica e podem ser escolhidos aleatoriamente. Por exemplo, r pode ser um número aleatório. G e H podem ser parâmetros conhecidos para o nó 202. Um esquema de confirmação mantém o sigilo de dados, mas se compromete com os dados para que não possam ser alterados posteriormente pelo remetente dos dados. Uma parte que recebe o compromisso (por exemplo, um nó receptor de uma transação) só conhece o valor de comprometimento (por exemplo, PC (r, t)), a parte não pode determinar qual o valor de dados subjacentes (por exemplo, t) foi submetido devido à presença do fator

ofuscante aleatório (por exemplo, r). No entanto, o nó 202 que recebe o compromisso pode executar o compromisso e verificar se os dados confirmados correspondem aos dados revelados. Dessa forma, ocultando os papéis (por exemplo, um remetente ou um destinatário) das partes, bem como criptografando o valor da transação, uma entidade de terceiros não saberá qual parte é remetente e qual parte é um destinatário, protegendo assim a privacidade das partes na transação.

[033] O Compromisso Pedersen tem uma propriedade adicional: compromissos podem ser adicionados, e a soma de um conjunto de compromissos é a mesma que um compromisso com a soma dos dados (com uma chave de ocultação definida como a soma das chaves de ocultação): PC (r_1 , t_1) + PC (r_2, t_2) = PC (r_1+ r_2, t_1 + t_2). Em outras palavras, o compromisso preserva a adição e aplica-se a propriedade comutativa, ou seja, o Compromisso Pedersen é aditivamente homomórfico, em que os dados subjacentes podem ser manipulados matematicamente como se não fossem criptografados. Portanto, ao aplicar o Compromisso Pedersen ao valor da transação e um saldo da parte da transação, o saldo pode ser atualizado usando o valor da transação adicionando diretamente os Compromissos Pedersen, sem descriptografar os Compromissos Pedersen do valor da transação e / ou do saldo.

[034] Em algumas modalidades, o nó 202 pode executar várias transações como a descrita acima em lote. Por exemplo, além das transações entre a parte A e a parte B, a parte C e a parte D também podem solicitar transações entre elas. Além disso, a parte E e a parte F também podem solicitar a transferência de ativos entre si. As transações entre a parte A e a parte B podem ser misturadas com as transações entre a parte C e a parte D e entre a parte E e a parte F. O nó 202 pode executar as transações entre as partes A, B, C, D, E e F de uma vez sem exigir indicação expressa dos respectivos remetentes e destinatários. Numa situação mais

complicada, o nó 202 pode executar múltiplas transações nas quais uma parte (por exemplo, a parte A) deva enviar valores de transação diferentes do ativo para diferentes partes (por exemplo, parte B, parte C, etc.).

[035] Com referência à Figura 3, um fluxo de execução de transação exemplificativo 300 com remetentes e destinatários mistos é ilustrado de acordo com várias modalidades. O fluxo de execução de transação 300 pode ser implementado em vários sistemas incluindo, por exemplo, a rede blockchain 200 da Figura 2. O fluxo de execução de transação 300 pode ser implementado por um ou mais dos nós 202 e pelos dispositivos de computação de usuário 240. As operações do fluxo de execução de transação 300 apresentadas abaixo destinam-se a ser ilustrativas. Dependendo da implementação, o fluxo de execução de transação exemplificativo 300 pode incluir menos etapas adicionais, ou etapas alternativas realizadas em várias ordens ou em paralelo.

[036] Nas modalidades ilustradas da Figura 3, os participantes de uma ou mais transações e suas contas associadas são mostrados no bloco 302. Por exemplo, cada um dos participantes pode estar associado a uma conta “Conta A_i”, onde $1 \leq i \leq n$ e n podem ser qualquer número inteiro positivo . Em algumas modalidades, n pode indicar o número total de participantes. Em outras modalidades, i pode não ser números inteiros contínuos e, portanto, n pode não indicar o número total de participantes. Como mostrado no bloco 302, cada uma das contas "Conta A_i" pode incluir um saldo "s_i", que pode ser o valor de ativo na conta disponível "Conta A_i." Em algumas modalidades, o saldo "s_1" pode estar na forma da moeda digital, por exemplo, Bitcoin, etc. Alternativamente, o saldo “s_1” pode representar moeda convencional. Além disso, como mostrado no bloco 302, o saldo “s_i” pode ser criptografado para obter um saldo criptografado “S_i” através de um ou mais esquemas de criptografia homomórfica ou de compromisso homomórfico como descrito acima. O saldo criptografado “S_i” pode ser um texto cifrado do saldo

“s_i” e referido como “HE(s_i)”. Portanto, S_i= HE(s_i), onde 1≤i≤n e n podem ser qualquer inteiro positivo . Por exemplo, a conta "Conta A_1" inclui um texto cifrado de seu saldo "S_1" representado por "S_1", onde S_1 = HE (s_1). Em algumas modalidades, o saldo criptografado "S_i" é um Compromisso Pedersen, e HE (s_i) = r_i * G + s_i * H, onde r é um fator de obscurecimento aleatório.

[037] No bloco 304, múltiplas transações de uma pluralidade de contas “Conta A_i” dos participantes pode ser recebida pelo nó 202. Nas modalidades ilustradas da Figura 3, cada conta pode estar associada a uma identificação de conta (ID) como “A_i”, um valor de transação “t_i”, uma prova de variação “Pf_i” e uma assinatura “Sig_i.” Uma “assinatura” mostra a aprovação de uma identidade. O termo “assinatura” pode ser qualquer forma de indicação de aprovação real. Por exemplo, uma assinatura associada a uma transação de uma conta mostra que a conta aprova a transação. Em algumas modalidades, as transações podem ser criptografadas para ocultar pelo menos a identidade de um remetente ou destinatário de cada uma das transações. Por exemplo, as transações podem incluir um texto cifrado do valor real da transação de cada transação, representado como “T_i”, onde T_i = HE (t_i). O texto cifrado do valor de transação pode ser gerado através dos esquemas de codificação homomórfica ou compromisso homomórfico acima descritos. Por exemplo, o valor da transação criptografada "T_i" pode ser um Compromisso Pedersen do valor da transação real "t_i".

[038] A prova de variação pode ser um protocolo de prova seguro que é usado para provar que um número está dentro de uma variação, embora o não revele outras informações do número, como o valor real do número. Por exemplo, a prova de variação pode ser gerada através de esquemas incluindo, por exemplo, esquema de assinatura de anel de Borromean, esquema à prova de balas, etc. Outros esquemas podem também ser usados para gerar a prova de variação. A prova de variação “Pf_i” pode mostrar que a conta “A_i” possui saldo suficiente para

permitir que a transação, por exemplo, o saldo da conta “s_i” sendo maior ou igual ao valor absoluto do valor da transação “t_i”. A prova de variação “Pf_i” da conta “A_i” pode ser representada por Pf_i = Pf (s_i_t_i≥0).

[039] Em algumas modalidades, outra prova, por exemplo, Pf_sum = Pf (t_1 + t_2 + ⋯ + t_n = 0), pode ser gerada nas transações. Esta prova pode ser referida como uma prova de soma a seguir, a qual é usada para mostrar que a soma dos valores da transação é equilibrada, por exemplo, zero. Conforme descrito acima, o valor da transação do remetente pode ser indicado como um valor positivo, enquanto o do destinatário correspondente pode ser indicado como um valor negativo. Os valores absolutos dos valores de transação associados ao remetente e ao destinatário correspondente são os mesmos. Deste modo, o nodo 202 pode executar a transação entre o remetente e o destinatário sem exigir indicação expressa de qual das partes é o remetente e qual a parte que é o destinatário.

[040] No exemplo descrito acima, onde a parte A deve pagar US $ 1.000 para a parte B, supondo que a parte A esteja associada a uma ID de conta "A_1" enquanto a parte B está associada a uma ID de conta "A_2", o valor da transação "t_1" associado a "A_1" é de + $ 1.000, enquanto o valor da transação "t_2" associado a "A_2" é de - $ 1.000. Uma prova de soma “Pf_sum” pode ser gerada para mostrar que o valor da transação “t_1” e o valor da transação “t_2” compensam um ao outro, e a soma dos valores da transação “t_1” e “t_2” é zero.

[041] Em algumas modalidades, a prova de soma “Pf_sum” pode ser comprovada com base no valor de transação criptografada HE (t_i). Por exemplo, o texto cifrado do valor de transação HE (t_i) pode ser representado por HE (t_i) = $G^{\{t\_i\}} * H^{\{r\_i\}}$, onde r_i é um fator de obscurecimento aleatório, G e H são os geradores acordados publicamente ou pontos de base da curva elíptica e podem ser escolhidos aleatoriamente. Portanto, a prova de soma “Pf_sum” pode ser Pf (r = r_1 + r_2 + ⋯ + r_n). Ao validar a prova da soma, um nó 202 pode verificar se HE (t_1) *

... * HE (t_n) = H^r. Se HE (t_1) * ... * HE (t_n) = H^r, isso mostra que t_1 + t_2 + ⋯ + t_n = 0, provando assim que Pf_sum e os valores da transação são equilibrados. Caso contrário, os valores da transação não serão equilibrados e poderá haver um valor de transação incorreto. Em algumas modalidades, os valores de transação podem ser criptografados utilizando outros esquemas e, assim, a prova da soma e a verificação da prova da soma podem ser diferentes das aqui descritas.

[042] Quando há vários remetentes e / ou destinatários, os valores de transação entre cada dupla são equilibrados. Em algumas modalidades, quando um remetente deva transacionar com múltiplos destinatários, o valor de transação do remetente pode ser definido como a soma de todos os valores de transação a serem enviados para os múltiplos destinatários. Por exemplo, quando a conta "A_1" deva enviar um valor de transação de $ 1.000 para a conta "A_2" e um valor de transação de $ 2.000 para a conta "A_3", o valor da transação da conta "A_1" é $ 3.000 a soma de $ 1.000 e US $ 2.000). O valor da transação da conta "A_1" é compensado pelo valor da transação da conta "A_2", ou seja, - $ 1.000, e o valor da transação da conta "A_3", ou seja, - $ 2.000. Da mesma forma, outros valores de transação nas transações são equilibrados. Tal prova pode ser gerada e associada às transações.

[043] Como descrito acima, uma assinatura de cada conta pode ser recebida, e a assinatura é representada por "Sig_i" na Figura 3. Em algumas modalidades, a assinatura pode ser assinada por cada conta nas transações, na prova de variação e na prova de soma, representada por Sig_i = Assinatura (A_1: T_1, Pf_1;...; A_n: T_n, Pf_n; Pf_sum). Desta forma, cada conta envolvida na (s) transação (ões) expressou sua concordância com os vários parâmetros na Signature (). Em algumas modalidades, a assinatura pode estar associada a uma ou mais transações, provas de variação ou a prova de soma.

[044] No bloco 306, um nó 202 pode receber as transações associadas com as múltiplas contas descritas acima, provas de variação, uma prova de soma e

assinaturas associadas pelo menos a uma das transações, prova de variação ou prova de soma, para verificar a transações recebidas. Em algumas modalidades, o nó 202 pode receber as transações de um nó organizador que coordena entre os participantes da transação. Em algumas modalidades, o nó organizador pode ser uma entidade de terceiros, implementada por um dispositivo de computação (não mostrado, mas semelhante ao nó 202). Por exemplo, cada participante pode enviar, por meio de um dispositivo de computação de usuário 240, sua ID de conta junto com um valor de transação criptografado, uma prova de variação e semelhantes para o nó organizador. O nó organizador pode gerar uma prova de soma com base nos valores de transação recebidos dos participantes. O nó organizador pode enviar as transações associadas a uma pluralidade de contas, uma prova de variação para cada uma das transações, uma prova de soma nas transações e uma assinatura de cada uma da pluralidade de contas associada pelo menos a uma das transações, provas de variação, ou a prova de soma para a rede blockchain 200, incluindo os nós 202. Em algumas modalidades, o nó organizador pode ser um dos participantes coordenando os outros participantes. Alternativamente, o organizador pode ser um nó 202 da rede blockchain 200. O nó organizador 202 pode receber as transações associadas a várias IDs de conta, juntamente com uma prova de variação para cada uma das transações, uma assinatura associada pelo menos a uma das transações , provas de variação, ou a prova de soma, dos participantes. O nó organizador 202 pode realizar a prova de soma com base nos valores de transação recebidos dos participantes.

[045] No bloco 306, o nó 202 pode validar as transações, as provas de variação, a prova de soma e as assinaturas. Em resposta às transações e às informações associadas que estão sendo validadas, o nó 202 pode implementar as transações atualizando o saldo de cada conta envolvida nas transações. Por exemplo, o nó 202 pode verificar a assinatura de cada conta. Em algumas

modalidades, se nenhuma assinatura for inválida, o nó 202 pode rejeitar as transações. Após cada assinatura ser verificada, o nó 202 pode validar a prova de cada variação para cada uma das transações. Em algumas modalidades, o nó 202 pode recuperar o saldo criptografado "S_i" e verificar a prova de variação "Pf_i" contra o saldo criptografado "S_i." Em algumas modalidades, o nó 202 pode verificar a própria validade da prova de variação "Pf_i" . Em resposta a qualquer uma das provas de variação sendo inválida, o nó 202 pode rejeitar as transações.

[046] Em algumas modalidades, após cada prova de variação ser validada, o nó 202 pode validar a prova da soma das transações. Por exemplo, se a prova de soma for gerada nos valores de transação criptografados, o nó 202 pode verificar a prova de soma de acordo com o esquema de criptografia, como descrito acima com referência ao bloco 304. Em resposta à prova de soma ser inválida, o nó 202 pode rejeitar as transações. Em algumas modalidades, após a validação da prova de soma, o nó 202 pode atualizar o saldo de cada conta. Por exemplo, o nó 202 pode atualizar o saldo “s_i” subtraindo o valor da transação “t_i” do saldo “s_i”, ou seja, s_i-t_i. No exemplo acima, onde a conta "A_1" deva enviar um valor de transação de $ 1.000 para a conta "A_2", se o nó 202 tiver validado as transações, o nó 202 poderá subtrair $ 1.000 do saldo "S_1" da conta "A_1" e adicionar $ 1.000 ao saldo "S_2" da conta "A_2." Em algumas modalidades, o nó 202 pode atualizar diretamente o saldo criptografado, conforme representado por S_i-T_i. Como descrito acima, o Compromisso Pedersen é aditivamente homomórfico e os dados subjacentes podem ser manipulados matematicamente como se não fossem criptografados. Por exemplo, o nó 202 pode atualizar o Compromisso Pedersen do saldo adicionando o Compromisso Pedersen do valor da transação ao Compromisso Pedersen do saldo. No bloco 308, podem ser obtidos os resultados da transação. Como ilustrado na Figura 3, após a execução das transações, o saldo de cada conta foi atualizado como "S_i-T_i."

[047] A descrição acima descreve as validações das assinaturas, as provas de variáveis e a prova de soma em ordem cronológica. Uma pessoa com habilidade normal deve perceber que as validações podem ter qualquer ordem. Por exemplo, o nó pode validar na ordem de assinatura, prova de soma, prova de variação, ou prova de variação, prova de soma, assinatura ou prova de variação, assinatura, prova de soma ou prova de soma, prova de variação, assinatura ou prova de soma. assinatura, prova de alcance. Além disso, as validações são opcionais. Algumas das validações, por exemplo, prova de variação e / ou de assinatura podem ser omitidas.

[048] Como tal, a presente divulgação permite a execução simultânea de múltiplas transações entre remetentes e destinatários mistos com aumento de proteção de privacidade. Ou seja, a identidade do remetente e do destinatário estão ocultas do público. Um valor de transação de cada participante pode ser maior ou menor que zero. Um valor de transação positivo indica que a conta do participante deve gastar esse valor, enquanto um valor de transação negativo indica que a conta deva receber esse valor. Além disso, a presente divulgação também pode usar criptografia homomórfica, compromisso homomórfico ou outros esquemas de criptografia para criptografar o valor da transação e o saldo de cada conta na transação, tornando assim impossível para um não participante saber se o valor da transação é positivo ou negativo ou o número real do valor da transação ou do saldo, evitando assim que o não participante identifique quem é o remetente e quem é o destinatário.

[049] FIG. 4 ilustra um fluxograma de um método exemplificativo 400 para a execução de transação de acordo com várias modalidades. O método 400 pode ser implementado em vários sistemas, incluindo, por exemplo, um ou mais componentes da rede blockchain 200 da Figura 2. O método exemplificativo 400 pode ser implementado por um ou mais dos nós 202 e / ou pelos dispositivos de computação de usuário 240. Num exemplo, o método 400 pode ser implementado por um nó

organizador (por exemplo, um dos nós 202). Em outro exemplo, o método 400 pode ser implementado por um ou mais nós (por exemplo, os nós 202) realizando as transações. As operações do método 400 apresentadas abaixo pretendem ser ilustrativas. Dependendo da implementação, o método exemplificativo 400 pode incluir etapas adicionais, em menor quantidade, ou alternativas executadas em várias ordens ou em paralelo.

[050] O bloco 401 compreende obter uma pluralidade de valores de transação criptografada (por exemplo, HE (t_1), HE (t_2), ..., HE (t_n)) associada às transações entre uma pluralidade de contas (por exemplo, A_1, A_2,... A_n). , em que cada um dos valores de transação criptografados é associado a uma das contas que envia ou recebe um dos valores de transação, e a criptografia de cada um dos valores de transação, pelo menos, oculta se uma conta envia ou recebe um dos valores de transação.

[051] Em algumas modalidades, a criptografia pode ser executada pelo nó de organização ou pelos nós que atuam como remetentes ou destinatários das transações e recebidas pelo nó de organização. Vários métodos de criptografia podem ser usados para criptografar os valores de transação. A criptografia de cada um dos valores da transação compreende uma criptografia homomórfica. Por exemplo, a criptografia de cada um dos valores de transação pode ser uma criptografia homomórfica ou um esquema de comprometimento homomórfico (por exemplo, um esquema de Compromisso de Pedersen).

[052] Em algumas modalidades, uma transferência de ativos entre duas ou mais contas pode ser dissociada em uma pluralidade de transações, cada uma associada com uma conta do remetente ou uma conta do destinatário. Cada conta pode estar associada a um nó dos nós 202. Por exemplo, uma transferência de ativos de $ 100 da conta A para B pode compreender uma primeira transação de + $ 100 associada à conta A indicando que a conta A despende $ 100 e compreende

uma segunda transação de - $ 100 associada à conta B, indicando que a conta B recebe $100. Por outro exemplo, uma transferência de ativo de $ 100 da conta A para B e outra transferência de ativo de $ 80 da conta A para C pode compreender uma primeira transação de + $ 100 associada à conta A indicando que a conta A gasta $ 180, compreende uma segunda transação de US $ 100 associados à conta B indicando que a conta B recebe US $ 100, compreende uma terceira transação de + $ 80 associada à conta A indicando que a conta A gasta US $ 80 e compreende uma terceira transação de - US $ 80 associada à conta C indicando que a conta C recebe US $ 80. Os sinais “+” e “-” podem ser revertidos ou alterados para qualquer outra representação alternativa. Além disso, conforme mostrado, duas das contas podem ser as mesmas, por exemplo, quando uma conta gasta ou recebe de várias contas.

[053] Além disso, em algumas modalidades, a criptografia de cada um dos valores da transação, pelo menos, oculta se uma conta envia ou recebe um dos valores da transação, ocultando se cada um dos valores da transação é de entrada (por exemplo, recebendo ativo) ou de saída (por exemplo, enviando o ativo) para uma conta. No exemplo de uma transferência de ativos de $ 100 da conta A para B e de $ 80 da conta A para C, pela criptografia, informações indicando uma identidade de remetente ou destinatário como "+" no valor da transação "+ $ 180" e “-” nos valores da transação “- $ 100” e “- $ 80” podem ser removidos. Ou seja, os valores da transação criptografada não conterão informações que indiquem uma identidade de remetente ou destinatário. Mesmo que os valores das transações criptografadas possam (mas não necessariamente) incluir um sinal “+” ou “-”, o sinal não poderá mais indicar corretamente a identidade do remetente ou do destinatário. Assim, a identidade do remetente e do destinatário nas transações são protegidas do público.

[054] O bloco opcional 402 compreende: obter uma pluralidade de provas de

variação (por exemplo, Pf_1, Pf_2, ..., Pf_n) respectivamente para as contas envolvidas nas transações, as provas de variação, indicando pelo menos que cada uma das contas que envia os valores de transação possui ativo suficiente . Detalhes podem ser referidos ao Pf_i descrito acima.

[055] O bloco 403 compreende: gerar uma prova de soma (por exemplo, Pf_sum) com base nos valores de transação criptografados obtidos, a prova de soma, indicando pelo menos que os valores da transação estão equilibrados. Detalhes podem ser referidos ao Pf_sum descrito acima. Por exemplo, o nó organizador pode obter os valores da transação criptografados e determinar se HE (t_1) * ... * HE (t_n) = H^{r_1} * H^{r_2} *... * H^{r_n} = H^{r}. Se HE (t_1) * ... * HE (t_n) = H^{r}, isso mostra que t_1 + t_2 + ⋯ + t_n = 0, portanto, o nó organizador verifica se os valores da transação estão equilibrados. Caso contrário, os valores da transação não estão equilibrados e o nó organizador poderá rejeitar as transações. Com a criptografia e a propriedade homomórfica da criptografia, o nó organizador pode realizar essa verificação mesmo sem conhecer os valores das transações subjacentes e se eles são de entrada ou saída.

[056] O bloco opcional 404 compreende a obtenção de uma pluralidade de assinaturas (por exemplo, Sig_1, Sig_2,..., Sig_n), respectivamente, para as contas. As assinaturas são associadas pelo menos a um dos valores de transação criptografados, às provas de variação e à prova de soma. Os detalhes podem ser referidos à Sig_i descrita acima. A assinatura pode seguir o Algoritmo de Assinatura Digital (DSA), como o Algoritmo de Assinatura Digital de Curva Elíptica (ECDSA), pelo qual o destinatário (por exemplo, nós que validam as transações) da assinatura pode verificar a chave pública de signatário (por exemplo, nós que participam nas transações) para autenticar os dados assinados.

[057] O bloco 405 compreende transmitir os valores de transação criptografados e a prova da soma para um ou mais nós (por exemplo, nós de

consenso) em uma rede blockchain para os nós verificarem as transações. Em algumas modalidades, transmitir os valores de transação criptografados e a prova de soma para um ou mais nós na rede blockchain para os nós verificarem as transações compreende transmitir os valores de transação criptografados, as provas de variação, a prova de soma e as assinaturas para o um ou mais nós na rede blockchain para que os nós verifiquem as transações com base nos valores de transação criptografados, nas provas de variação, na prova de soma e nas assinaturas.

[058] Em algumas modalidades, a transmissão dos valores de transação criptografados, das provas de variação, da prova de soma e das assinaturas para um ou mais nós na rede blockchain para os nós verificarem as transações com base nos valores de transação criptografados, nas provas de variação, na prova de soma e nas assinaturas compreende: transmitir os valores de transação criptografados, as provas de variação, a prova de soma e as assinaturas para um ou mais nós na rede blockchain; e fazer com que os nós: validem os valores de transação criptografados, as provas de variação, a prova de soma e as assinaturas, executem as transações em resposta à verificação das transações bem sucedidas, e incluam as transações em um novo bloco de dados de um blockchain mantido pela rede blockchain. Com a criptografia e a propriedade homomórfica da criptografia, os nós podem realizar essa validação mesmo sem conhecer os valores das transações subjacentes e se eles são de entrada ou saída.

[059] Em algumas modalidades, fazer com que os nós executem as transações em resposta à verificação bem-sucedida das transações compreende: fazer com que os nós deduzam os valores de transação criptografados (T_i) correspondentemente dos saldos de conta criptografados (por exemplo, S_i das contas) em resposta à verificação das transações bem sucedida. Devido à propriedade homomórfica, (S_i - T_i) pode atualizar os saldos de acordo com as

transações enquanto mantém os saldos criptografados.

[060] Como tal, os sistemas e métodos divulgados permitem que as transações sejam executadas entre contas participantes sem divulgar qual conta é remetente e qual conta é uma destinatária. Embora o valor da transação subjacente possa ser maior ou menor que zero para indicar um remetente e um destinatário, a criptografia personalizada pode ser usada para ocultar os valores da transação de forma que os valores da transação não possam ser usados para indicar um remetente ou um destinatário por um não participante. Além disso, as contas participantes em várias transações podem ser misturadas em qualquer ordem, sem indicar se devem enviar ou receber ativos. E as múltiplas transações ou transferências de ativos podem ser executadas em lote. Desta forma, é alcançada a proteção da privacidade das contas participantes, o que melhora a funcionalidade dos computadores e torna as transações on-line mais seguras.

[061] A Figura 5 ilustra um fluxograma de outro método exemplificativo 500 para execução de transação, de acordo com várias modalidades. O método 500 pode ser implementado em vários sistemas, incluindo, por exemplo, um ou mais componentes da rede blockchain 200 da Figura 2. O método exemplificativo 500 pode ser implementado por um ou mais dos nós 202 e / ou pelos dispositivos de computação de usuários 240. As operações do método 500 apresentadas abaixo pretendem ser ilustrativas. Dependendo da implementação, o método exemplificativo 500 pode incluir algumas etapas adicionais ou alternativas executadas em várias ordens ou em paralelo.

[062] No bloco 502, transações criptografadas associadas a uma pluralidade de contas, uma prova de variação para cada uma das transações, uma prova de soma nas transações e uma assinatura de cada da pluralidade de contas associada pelo menos a uma das transações , provas de variação ou a prova de soma pode ser recebida. No bloco 504, as transações criptografadas, a prova de variação para

cada uma das transações, a prova de soma das transações e a assinatura de cada da pluralidade de contas podem ser validadas. No bloco 506, as transações podem ser implementadas com base na validação, atualizando um saldo de cada uma da pluralidade de contas.

[063] A Figura 6 ilustra um fluxograma de um método exemplificativo 600 para validação de transação, de acordo com várias modalidades. O método 600 pode ser implementado em vários sistemas incluindo, por exemplo, um ou mais componentes da rede blockchain 200 da Figura 2. O método exemplificativo 600 pode ser implementado por um ou mais dos nós 202 e / ou pelos dispositivos de computação de usuário 240. Por exemplo, o método 600 pode corresponder ao bloco 504 do método 500. As operações do método 600 apresentadas abaixo pretendem ser ilustrativos. Dependendo da implementação, o método exemplificativo 600 pode incluir algumas etapas adicionais, ou alternativos executadas em várias ordens ou em paralelo.

[064] No bloco 602, pode ser determinado se as assinaturas são válidas. Se for determinado que qualquer uma das assinaturas não é válida, no bloco 604, as transações podem ser rejeitadas. Se for determinado que cada uma das assinaturas é válida, no bloco 606, pode ser determinado se a prova de variação para cada uma das transações é válida. Se for determinado que qualquer uma das provas de variação não é válida, o método 600 prossegue para o bloco 604 e as transações podem ser rejeitadas. Se for determinado que cada uma das provas de variação é válida, no bloco 608, pode ser determinado se a prova de soma é válida. Se for determinado que a prova da soma não é válida, o método 600 prossegue para o bloco 604 e as transações podem ser rejeitadas. Se for determinado que a prova de soma é válida, o método 600 prossegue para o bloco 610 e um saldo de cada conta pode ser atualizado com base no valor da transação associado à conta. A descrição acima descreve as validações em uma ordem. Uma pessoa com habilidade normal

deve perceber que as validações podem ter qualquer ordem.

[065] As técnicas aqui descritas são implementadas por um ou mais dispositivos de computação para fins especiais. Os dispositivos de computação para fins especiais podem ser sistemas de computador de mesa, sistemas de computador servidor, sistemas de computador portátil, dispositivos portáteis, dispositivos de rede ou qualquer outro dispositivo ou combinação com fios e/ou lógico de programa para implementar as técnicas.

[066] A Figura 7 é um diagrama em bloco que ilustra um sistema de computador exemplificativo 700, que pode ser implementado por qualquer uma das modalidades aqui descritas. O sistema 700 pode corresponder aos nós 202 ou aos dispositivos de computação de usuário 240 descritos acima com referência à Figura 2. O sistema de computador 700 inclui um barramento 702 ou outro mecanismo de comunicação para comunicar informação, um ou mais processadores de hardware 704 acoplados ao barramento 702 para processar informação. O (s) processador (es) de hardware 704 pode ser, por exemplo, um ou mais microprocessadores de propósito geral.

[067] O sistema de computador 700 também inclui uma memória principal 706, tal como uma memória de acesso aleatório (RAM), cache e / ou outros dispositivos de armazenamento dinâmicos, acoplada ao barramento 702 para armazenar informação e instruções a serem executadas pelo processador 704. A memória 706 também pode ser usada para armazenar variáveis temporárias ou outras informações intermediárias durante a execução de instruções a serem executadas pelo processador 704. Tais instruções, quando armazenadas em mídia de armazenamento acessível ao processador 704, submetem o sistema de computador 700 a uma máquina de propósito especial que é personalizada para executar as operações especificadas nas instruções. O sistema de computador 700 inclui ainda uma memória apenas de leitura (ROM) 708 ou outro dispositivo de

armazenamento estático acoplado ao barramento 702 para armazenar informação estática e instruções para o processador 704. Um dispositivo de armazenamento 710, tal como um disco magnético, disco óptico ou pen drive USB (Flash drive), etc., é fornecido e acoplado ao barramento 702 para armazenar informações e instruções.

[068] O sistema de computador 700 pode implementar as técnicas aqui descritas usando lógica com fio personalizada, um ou mais ASICs ou FPGAs, firmware e / ou lógica de programa que em combinação com o sistema de computador leva ou programa o sistema de computador 700 a ser uma máquina de propósito especial. De acordo com uma modalidade, as operações, métodos e processos aqui descritos são realizados pelo sistema de computador 700 em resposta ao (s) processador (es) 704 executando uma ou mais sequências de uma ou mais instruções contidas na memória principal 706. Tais instruções podem ser lidas na memória principal 706 de outro meio de armazenamento, tal como o dispositivo de armazenamento 710. A execução das sequências de instruções contidas na memória principal 706 faz com que o (s) processador (es) 704 execute as etapas do processo aqui descrito. Em modalidades alternativas, podem ser utilizados circuitos com fios em vez de ou em combinação com instruções de software.

[069] O processador (s) 704 pode corresponder ao processador 204 descrito acima, e a memória principal 706, a ROM 708, e / ou o armazenamento 710 podem corresponder à memória 206 descrita acima. A memória principal 706, a ROM 708 e / ou o armazenamento 710 podem incluir meio de armazenamento não transitório. O termo “meio não transitório” e termos similares, como aqui usados referem-se a qualquer meio que armazene dados e / ou instruções que façam com que uma máquina opere de maneira específica. Esses meios não transitórios podem incluir meios não voláteis e / ou meios voláteis. O meio não volátil inclui, por exemplo,

discos ópticos ou magnéticos, como o dispositivo de armazenamento 710. O meio volátil inclui memória dinâmica, como a memória principal 706. As formas comuns de meios não transitórios incluem, por exemplo, um disquete, um disco flexível, disco rígido, unidade de estado sólido, fita magnética ou qualquer outro meio de armazenamento de dados magnéticos, um CD-ROM, qualquer outro meio de armazenamento óptico de dados, qualquer meio físico com padrões de furos, RAM, PROM e EPROM, FLASH-EPROM, NVRAM, qualquer outro chip ou cartucho de memória e versões em rede dos mesmos.

[070] O sistema de computador 700 também inclui uma interface de comunicação 718 acoplada ao barramento 702. A interface de comunicação 718 fornece um acoplamento de comunicação de dados bidirecional para uma ou mais ligações de rede que estão conectadas a uma ou mais redes locais. Por exemplo, a interface de comunicação 718 pode ser uma placa de rede digital de serviços integrados (ISDN), modem de cabo, modem de satélite ou um modem para fornecer uma conexão de comunicação de dados a um tipo correspondente de linha telefônica. Como outro exemplo, a interface de comunicação 718 pode ser um cartão de rede local (LAN) para fornecer conexão de comunicação de dados para uma LAN compatível (ou componente WAN para se comunicar com uma WAN). Os links sem fio também podem ser implementados. Em qualquer implementação deste tipo, a interface de comunicação 718 envia e recebe sinais elétricos, eletromagnéticos ou ópticos que transportam fluxos de dados digitais representando vários tipos de informação.

[071] O sistema de computador 700 pode enviar mensagens e receber dados, incluindo código de programa, através de rede (s), link de rede e interface de comunicação 718. No exemplo da Internet, um servidor pode transmitir um código solicitado para um programa de aplicação através da Internet, o ISP, a rede local e a interface de comunicação 718. O código recebido pode ser executado pelo

processador 704 à medida que é recebido e / ou armazenado no dispositivo de armazenamento 710, ou outro armazenamento não volátil para execução posterior.

[072] Cada um dos esquemas, mecanismos, soluções, processos, métodos e algoritmos descritos nas seções anteriores podem ser incorporados e total ou parcialmente automatizados por módulos de código executados por um ou mais sistemas de computador ou processadores de computador que compreendem hardware de computador. . Os processos e algoritmos podem ser implementados parcial ou totalmente no circuito de aplicativo específico. Em algumas modalidades, o (s) processador (es) 704 pode (m) ser implementado parcial ou totalmente como um ou mais circuitos lógicos descritos acima.

[073] Os vários recursos e processos descritos acima podem ser usados independentemente uns dos outros, ou podem ser combinados de várias maneiras. Todas as combinações e subcombinações possíveis pretendem incidir no escopo desta divulgação. Além disso, determinados blocos de método ou processo podem ser omitidos em algumas implementações. Os métodos e processos aqui descritos também não estão limitados a qualquer sequência particular, e os blocos ou estados a eles relacionados podem ser realizados em outras sequências que sejam apropriadas. Por exemplo, blocos ou estados descritos podem ser realizados em uma ordem diferente da especificamente divulgada, ou múltiplos blocos ou estados podem ser combinados em um único bloco ou estado. Os blocos ou estados de exemplo podem ser executados em série, em paralelo ou de alguma outra maneira. Os blocos ou estados podem ser adicionados às ou removidos das modalidades de exemplo divulgadas. Os exemplos de sistemas e componentes aqui descritos podem ser configurados de maneira diferente do descrito. Por exemplo, elementos podem ser adicionados, removidos ou rearranjados em comparação com as modalidades de exemplo divulgadas.

[074] As várias operações dos métodos de exemplo aqui descritos podem

ser realizadas, pelo menos parcialmente, por um algoritmo. O algoritmo pode estar compreendido em códigos de programa ou instruções armazenadas numa memória (por exemplo, um meio de armazenamento legível por computador não transitório descrito acima). Tal algoritmo pode compreender um algoritmo de aprendizado de máquina. Em algumas modalidades, um algoritmo de aprendizado de máquina pode não programar explicitamente computadores para executar uma função, mas pode aprender com dados de treinamento para criar um modelo de previsão que execute a função.

[075] As várias operações dos métodos de exemplo aqui descritos podem ser realizadas, pelo menos parcialmente, por um ou mais processadores que são configurados temporariamente (por exemplo, por software) ou permanentemente configurados para executar as operações relevantes. Se configurados temporária ou permanentemente, tais processadores podem constituir máquinas implementadas pelo processador que operam para executar uma ou mais operações ou funções aqui descritas.

[076] Similarmente, os métodos aqui descritos podem ser pelo menos parcialmente implementados por processador, com um processador ou processadores particulares sendo um exemplo de hardware. Por exemplo, pelo menos algumas das operações de um método podem ser realizadas por um ou mais processadores ou máquinas implementados processador. Além disso, 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 um serviço" (SaaS). Por exemplo, pelo menos algumas das operações podem ser realizadas por um grupo de computadores (como exemplos de máquinas, incluindo processadores), sendo essas operações acessíveis por uma rede (por exemplo, a Internet) e por uma ou mais interfaces apropriadas (por exemplo, uma Interface de Programa de Aplicativo (API)).

[077] O desempenho de algumas das operações pode ser distribuído entre os processadores, não residindo apenas em uma única máquina, mas implantado em várias máquinas. Em algumas modalidades exemplificativas, os processadores ou máquinas implementadas por processador podem estar localizados em um único local geográfico (por exemplo, dentro de um ambiente doméstico, um ambiente de escritório ou um farm de servidor). Em outras modalidades de exemplo, os processadores ou máquinas implementados por processador podem ser distribuídos através de várias localizações geográficas.

[078] Ao longo deste relatório, vários caso podem implementar componentes, operações ou estruturas descritas como um único caso. Embora operações individuais de um ou mais métodos sejam ilustradas e descritas como operações separadas, uma ou mais das operações individuais podem ser realizadas simultaneamente, e nada exige que as operações sejam executadas na ordem ilustrada. As estruturas e funcionalidades apresentadas como componentes separados em configurações de exemplo podem ser implementadas como uma estrutura ou componente combinado. Da mesma forma, estruturas e funcionalidades apresentadas como um único componente podem ser implementadas como componentes separados. Estas e outras variações, modificações, adições e melhorias incidem no escopo do assunto aqui tratado.

[079] Quaisquer descrições de processo, elementos ou blocos nos diagramas de fluxo aqui descritos e / ou representados nas figuras anexas devem ser entendidos como potencialmente representando módulos, segmentos ou porções de código que incluem uma ou mais instruções executáveis para implementar funções ou etapas lógicas específicas no processo. Implementações alternativas estão incluídas no escopo das modalidades aqui descritas, nas quais elementos ou funções podem ser deletados, executados fora de ordem daqueles mostrados ou comentados, incluindo substancialmente ao mesmo tempo ou em

ordem reversa, dependendo da funcionalidade envolvida, como seria entendido por os aqueles versados na técnica.

[080] Embora uma descrição geral da matéria tenha sido descrita com referência às modalidades de exemplo específicas, várias modificações e alterações podem ser feitas a estas modalidades sem se afastar do âmbito mais amplo de modalidades da presente divulgação. Tais modalidades da matéria podem ser aqui referidas, individual ou coletivamente, pelo termo "invenção" apenas por conveniência e sem intenção de limitar voluntariamente o escopo deste pedido a qualquer divulgação ou conceito único se mais de uma for, de fato divulgado.

[081] As modalidades aqui ilustradas são descritas com detalhes suficientes para permitir que aqueles versados na técnica pratiquem os ensinamentos divulgados. Outras modalidades podem ser utilizadas e derivadas delas, de tal modo que substituições estruturais e lógicas e mudanças podem ser feitas sem se afastar do escopo desta divulgação. A Descrição Detalhada, por conseguinte, não deve ser tomada num sentido limitativo, e o escopo de várias modalidades é definido apenas pelas reivindicações anexas, juntamente com a variação completa de equivalentes a que tais reivindicações têm direito.

REIVINDICAÇÕES

1. Método de proteção da informação implementado através de computador, **CARACTERIZADO** pelo fato de que compreende:

obter uma pluralidade de valores de transação criptografados associada a transações entre uma pluralidade de contas, em que:

cada um dos valores da transação criptografada está associado a uma das contas que envia ou recebe um dos valores da transação, e

a criptografia de cada um dos valores da transação, pelo menos, oculta se uma conta envia ou recebe um dos valores da transação;

gerar uma prova de soma com base nos valores de transação criptografados obtidos, a prova de soma indicando pelo menos que os valores da transação estão equilibrados; e

transmitir os valores de transação criptografados e a prova de soma para um ou mais nós em uma rede blockchain para os nós verificarem as transações.

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a criptografia de cada um dos valores de transação oculta, pelo menos, se uma conta envia ou recebe um dos valores de transação ocultando se cada um dos valores de transação é de entrada ou de saída para uma conta.

3. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que, antes de gerar a prova de soma, compreende adicionalmente:

obter uma pluralidade de provas de variação respectivamente para as contas envolvidas nas transações, as provas de variação indicando pelo menos que cada uma das contas que envia os valores de transação tem ativo suficiente.

4. Método, de acordo com a reivindicação 3, **CARACTERIZADO** pelo fato de que antes de transmitir os valores de transação criptografados e a prova de soma para um ou mais nós, compreende adicionalmente: obter uma pluralidade de assinaturas, respectivamente, das contas, em que:

transmitir os valores de transação criptografados e a prova de soma para um ou mais nós na rede blockchain para os nós verificarem as transações compreende transmitir os valores de transação criptografados, as provas de variação, a prova de soma e as assinaturas para um ou mais nós na rede blockchain para que os nós verifiquem as transações com base nos valores de transação criptografados, nas provas de variação, na prova de soma e nas assinaturas.

5. Método, de acordo com a reivindicação 4, **CARACTERIZADO** pelo fato de que transmitir os valores de transação criptografados, as provas de variação, a prova de soma e as assinaturas para um ou mais nós na rede blockchain para que os nós verifiquem as transações com base nos valores de transação criptografados, nas provas de variação, na prova de soma, e nas assinaturas compreende:

transmitir os valores de transação criptografados, as provas de variação, a prova de soma e as assinaturas para um ou mais nós na rede blockchain; e

levar os nós a:

validar os valores de transação criptografados, as provas de variação, a prova de soma, e as assinaturas,

executar as transações em resposta à verificação bem-sucedida das transações, e

adicionar as transações em um novo bloco de dados de um blockchain mantido pela rede blockchain.

6. Método, de acordo com a reivindicação 5, **CARACTERIZADO** pelo fato de que levar os nós a executarem as transações em resposta a uma verificação bem-sucedida das transações compreende:

levar os nós a deduzirem os valores de transação criptografados de forma correspondente aos saldos de contas criptografados das contas em resposta à verificação bem sucedida das transações.

7. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de

que a criptografia de cada um dos valores de transação compreende uma criptografia homomórfica.

8. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a criptografia de cada um dos valores de transação compreende um esquema de Compromisso Pedersen.

9. Sistema de proteção de informação, **CARACTERIZADO** pelo fato de que compreende: um ou mais processadores e uma ou mais memórias não transitórias legíveis por computador acopladas a um ou mais processadores e configuradas com instruções executáveis por um ou mais processadores para fazer com que o sistema realize operações compreendendo:

obter uma pluralidade de valores de transação criptografados associada a transações entre uma pluralidade de contas, em que:

cada um dos valores da transação criptografados está associado a uma das contas que envia ou recebe um dos valores da transação, e

a criptografia de cada um dos valores da transação oculta pelo menos se uma conta envia ou recebe um dos valores da transação;

gerar uma prova de soma com base nos valores de transação criptografados obtidos, a prova de soma pelo menos indicando que os valores da transação estão equilibrados; e

transmitir os valores de transação criptografados e a prova de soma para um ou mais nós em uma rede blockchain para que os nós verifiquem as transações.

10. Sistema, de acordo com a reivindicação 9, **CARACTERIZADO** pelo fato de que a criptografia de cada um dos valores da transação pelo menos oculta se uma conta envia ou recebe um dos valores da transação, ocultando se cada um dos valores da transação é de entrada ou de saída para a conta.

11. Sistema, de acordo com a reivindicação 9, **CARACTERIZADO** pelo fato de que antes de gerar a prova da soma, as operações compreendem ainda:

obter uma pluralidade de provas de variação respectivamente para as contas envolvidas nas transações, as provas de variação pelo menos indicando que cada uma das contas que envia os valores de transação tem ativo suficiente.

12. Sistema, de acordo com a reivindicação 11, **CARACTERIZADO** pelo fato de que:

antes de transmitir os valores de transação criptografados e a prova de soma para um ou mais nós, as operações compreendem ainda: obter uma pluralidade de assinaturas, respectivamente, para as contas; e

transmitir os valores de transação criptografados e a prova de soma para um ou mais nós na rede blockchain para os nós verificarem as transações compreende transmitir os valores de transação criptografados, as provas de variação, a prova de soma e as assinaturas para um ou mais nós na rede blockchain para que os nós verifiquem as transações com base nos valores de transação criptografados, nas provas de variação, na prova de soma e nas assinaturas.

13. Sistema, de acordo com a reivindicação 12 , **CARACTERIZADO** pelo fato de que transmitir os valores de transação criptografados, as provas de variação, a prova de soma e as assinaturas para um ou mais nós na rede blockchain para que os nós verifiquem as transações com base nos valores de transação criptografados, nas provas de variação, na prova de soma e nas assinaturas compreende:

transmitir os valores de transação criptografados, as provas de variação, a prova de soma e as assinaturas para um ou mais nós na rede blockchain; e

levar os nós a:

validar os valores de transação criptografados, as provas de variação, a prova de soma e as assinaturas,

executar as transações em resposta à verificação bem-sucedida das transações, e

adicionar as transações em um novo bloco de dados de um blockchain

mantido pela rede blockchain.

14. Sistema, de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que levar os nós a executarem as transações em resposta à verificação bem sucedida compreende:

levar os nós a deduzirem os valores de transação criptografados de forma correspondente dos saldos de contas criptografados das contas em resposta à verificação bem sucedida das transações.

15. Sistema, de acordo com a reivindicação 9, **CARACTERIZADO** pelo fato de que a que a criptografia de cada um dos valores de transação compreende uma criptografia homomórfica.

16. Sistema, de acordo com a reivindicação 9, **CARACTERIZADO** pelo fato de que a que a criptografia de cada um dos valores de transação compreende um esquema de Compromisso Pedersen.

17. Meio de armazenamento não transitório legível por computador configurado com instruções executáveis por um ou mais processadores para fazer com que um ou mais processadores executem operações, **CARACTERIZADO** pelo fato de que compreende:

obter uma pluralidade de valores de transação criptografados associados a transações entre uma pluralidade de contas, em que:

cada um dos valores da transação criptografados está associado a uma das contas que envia ou recebe um dos valores da transação, e

a criptografia de cada um dos valores da transação pelo menos oculta se uma conta envia ou recebe um dos valores da transação;

gerar uma prova de soma com base nos valores de transação criptografados obtidos, a prova de soma, pelo menos, indicando que os valores da transação estão equilibrados; e

transmitir os valores de transação criptografados e a prova de soma para um

ou mais nós em uma rede blockchain para os nós verificarem as transações.

18. Meio de armazenamento, de acordo com a reivindicação 17, **CARACTERIZADO** pelo fato de que a criptografia de cada um dos valores de transação pelo menos oculta se uma conta envia ou recebe um dos valores de transação, ocultando se cada um dos valores de transação é de entrada ou de saída para uma conta.

19. Meio de armazenamento, de acordo com a reivindicação 17, **CARACTERIZADO** pelo fato de que:

antes de gerar a prova de soma, as operações compreendem ainda: obter uma pluralidade de provas de variação respectivamente para as contas envolvidas nas transações, as provas de variação indicando pelo menos que cada uma das contas que envia os valores de transação tem ativo suficiente;

antes de transmitir os valores de transação criptografados e a prova de soma para um ou mais nós, as operações compreendem ainda: obter uma pluralidade de assinaturas, respectivamente, para as contas; e

transmitir os valores de transação criptografados e a prova de soma para um ou mais nós na rede blockchain para os nós verificarem as transações compreende transmitir os valores de transação criptografados, as provas de variação, a prova de soma e as assinaturas para um ou mais nós na rede blockchain para que os nós verifiquem as transações com base nos valores de transação criptografados, nas provas de variação, na prova de soma e nas assinaturas.

20. Meio de armazenamento, de acordo com a reivindicação 19, **CARACTERIZADO** pelo fato de que

transmitir os valores de transação criptografados, as provas de variação, a prova de soma e as assinaturas para um ou mais nós na rede blockchain para os nós verificarem as transações com base nos valores de transação criptografados, nas provas de variação, na prova de soma e nas assinaturas compreende:

transmitir os valores de transação criptografados, as provas de variação, a prova de soma e as assinaturas para um ou mais nós na rede blockchain; e

levar os nós a:

validar os valores de transação criptografados, as provas de variação, a prova de soma e as assinaturas,

executar as transações em resposta à verificação bem-sucedida das transações e

adicionar as transações em um novo bloco de dados de um blockchain mantido pela rede blockchain.

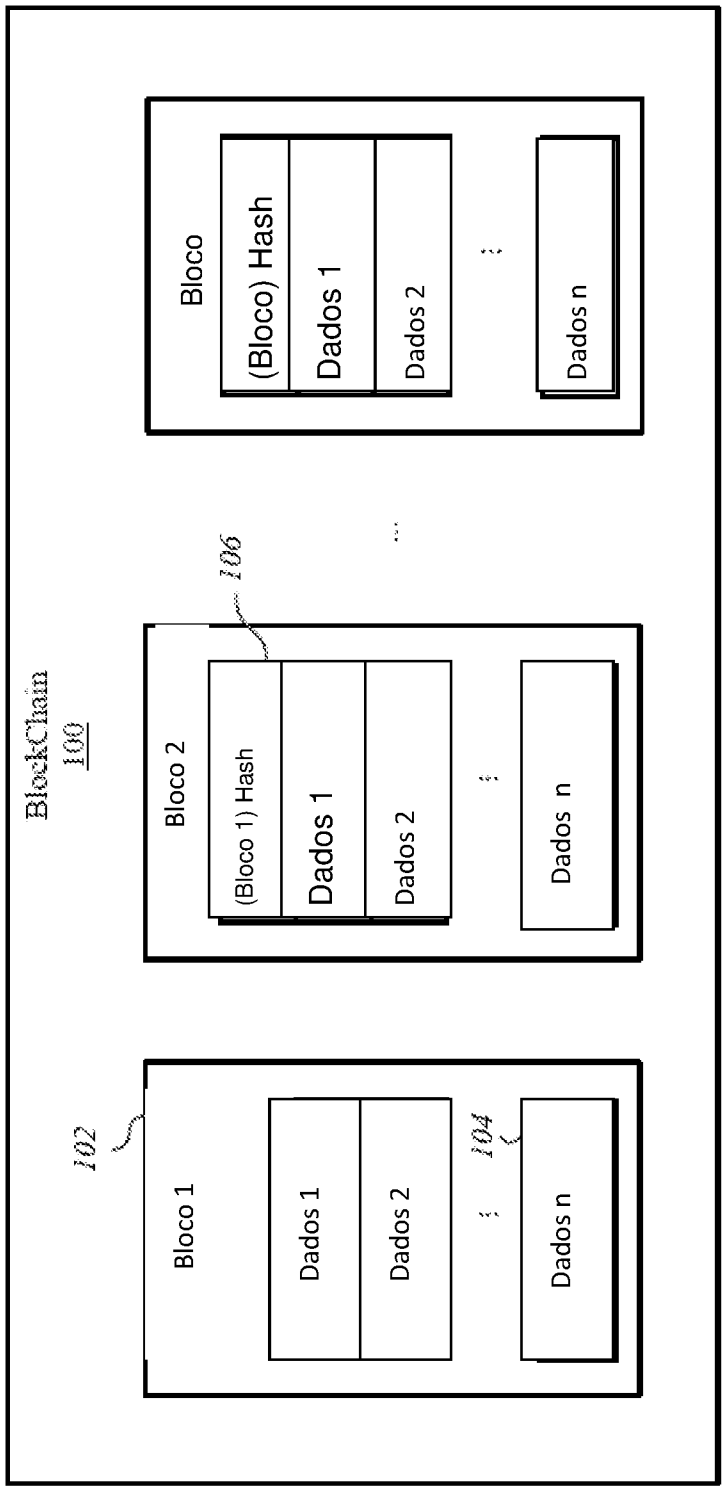

BlockChain
100
102
Bloco 1
Dados 1
Dados 2
104
Dados n
106
Bloco 2
(Bloco 1) Hash
Dados 1
Dados 2
Dados n
Bloco
(Bloco) Hash
Dados 1
Dados 2
Dados n

FIG. 1

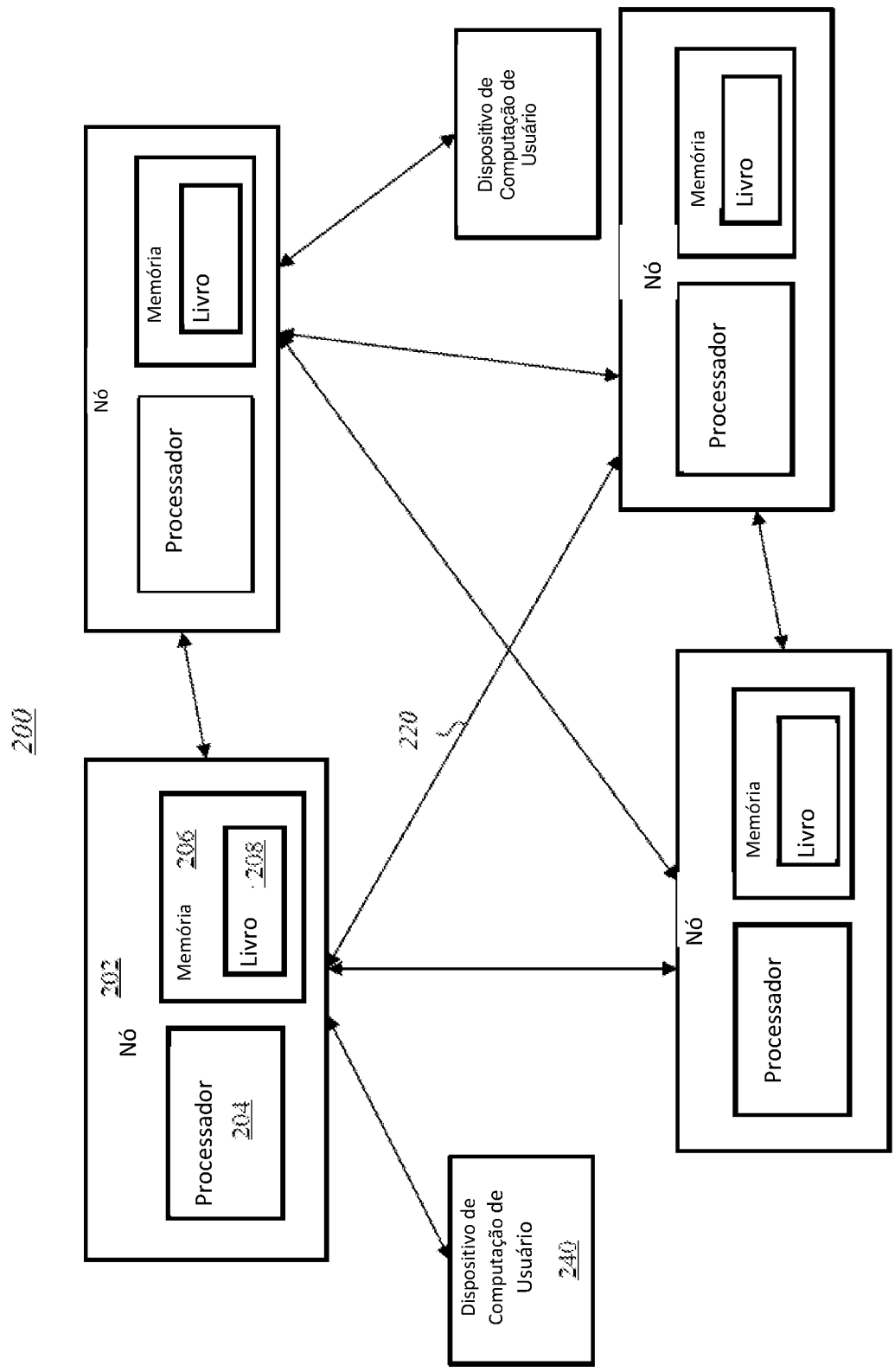

200
Nó
202
Processador
204
Memória
206
Livro
208
220
Dispositivo de Computação de Usuário
240
Nó
Processador
Memória
Livro
Dispositivo de Computação de Usuário
Nó
Processador
Memória
Livro
Nó
Processador
Memória
Livro

FIG. 2

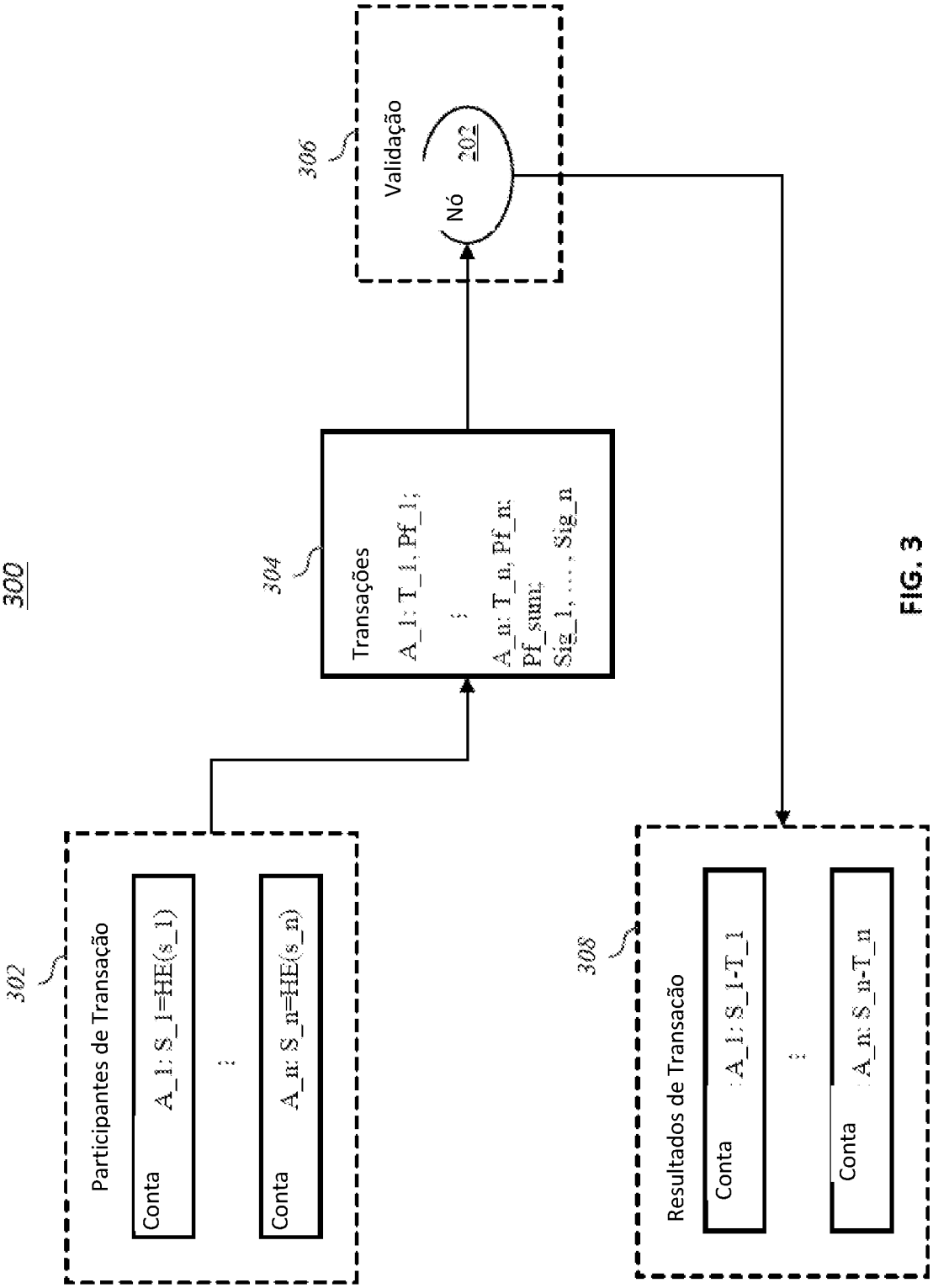

300
302
Participantes de Transação
Conta A_1: S_1=HE(s_1)
Conta A_n: S_n=HE(s_n)
304
Transações
A_1: T_1, Pf_1;
A_n: T_n, Pf_n;
Pf_sum;
Sig_1, ..., Sig_n
306
Validação
Nó 202
308
Resultados de Transacão
Conta A_1: S_1-T_1
Conta A_n: S_n-T_n

FIG. 3

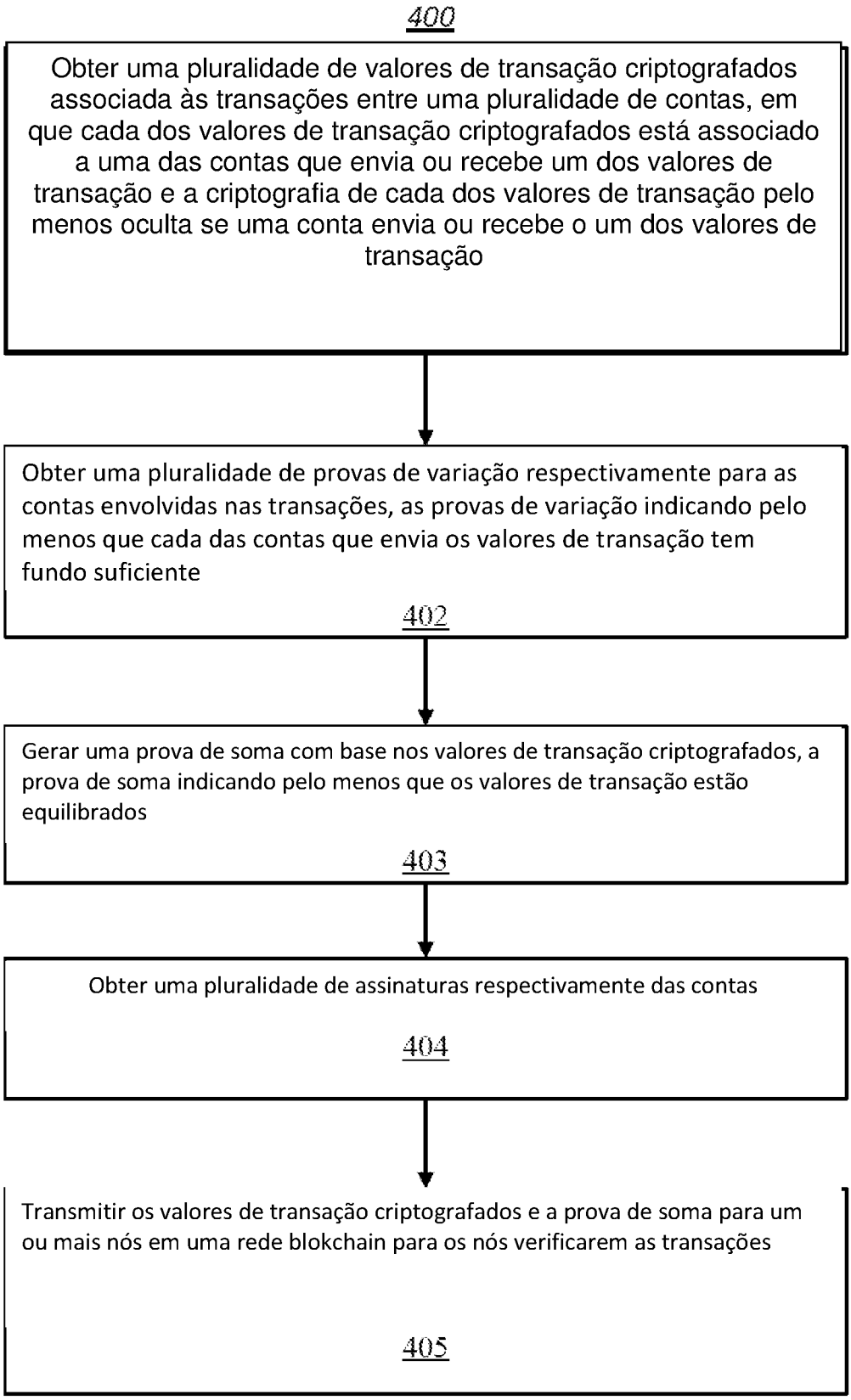

400
Obter uma pluralidade de valores de transação criptografados associada às transações entre uma pluralidade de contas, em que cada dos valores de transação criptografados está associado a uma das contas que envia ou recebe um dos valores de transação e a criptografia de cada dos valores de transação pelo menos oculta se uma conta envia ou recebe o um dos valores de transação
Obter uma pluralidade de provas de variação respectivamente para as contas envolvidas nas transações, as provas de variação indicando pelo menos que cada das contas que envia os valores de transação tem fundo suficiente
402
Gerar uma prova de soma com base nos valores de transação criptografados, a prova de soma indicando pelo menos que os valores de transação estão equilibrados
403
Obter uma pluralidade de assinaturas respectivamente das contas
404
Transmitir os valores de transação criptografados e a prova de soma para um ou mais nós em uma rede blokchain para os nós verificarem as transações
405

FIG. 4

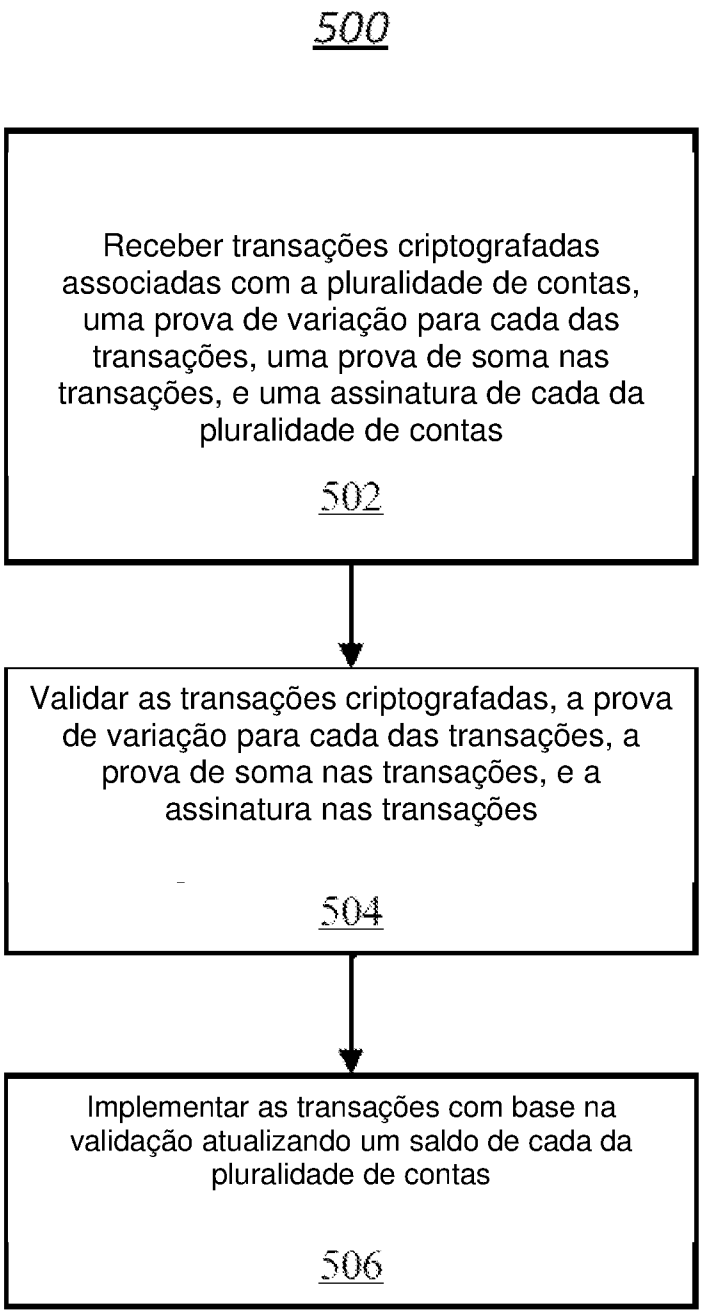

500
Receber transações criptografadas associadas com a pluralidade de contas, uma prova de variação para cada das transações, uma prova de soma nas transações, e uma assinatura de cada da pluralidade de contas
502
Validar as transações criptografadas, a prova de variação para cada das transações, a prova de soma nas transações, e a assinatura nas transações
504
Implementar as transações com base na validação atualizando um saldo de cada da pluralidade de contas
506

FIG. 5

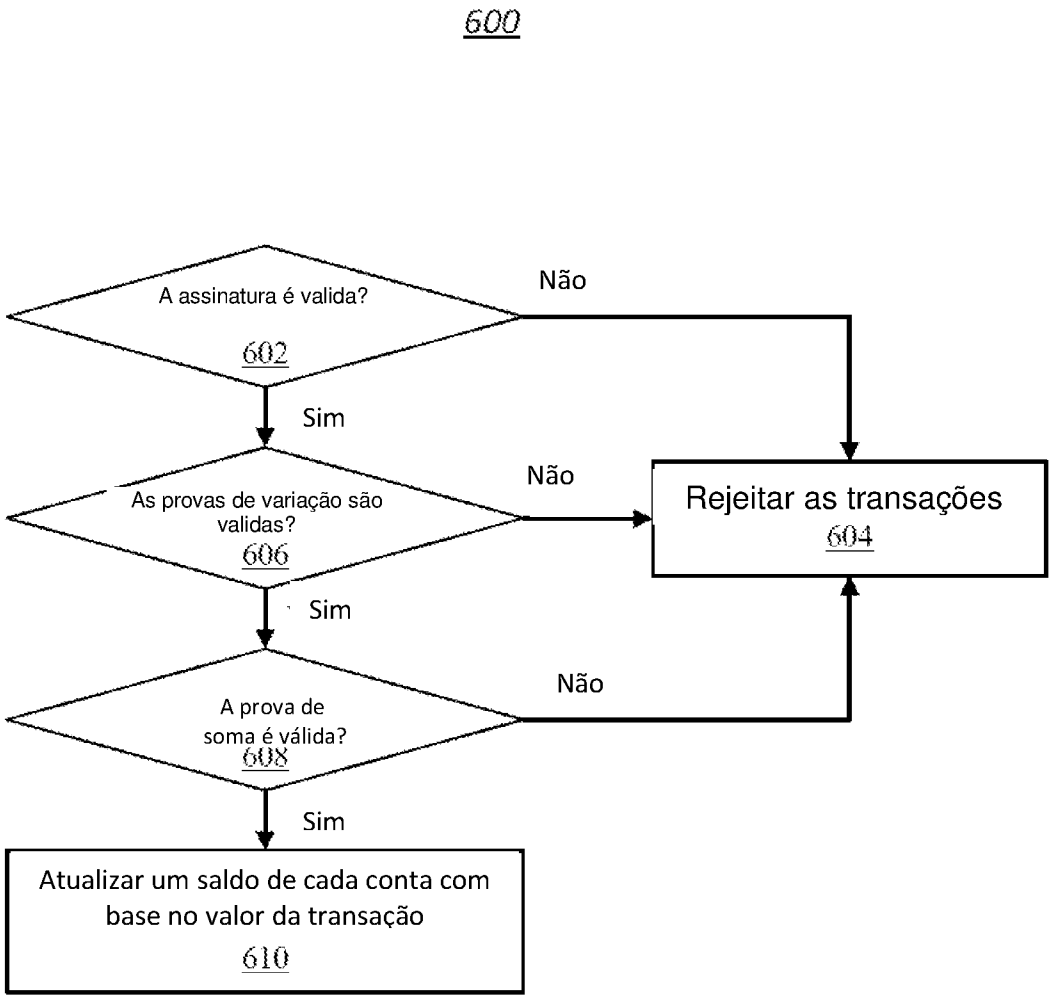

600
A assinatura é valida?
602
Não
Sim
As provas de variação são validas?
606
Não
Rejeitar as transações
604
Sim
A prova de soma é válida?
608
Não
Sim
Atualizar um saldo de cada conta com base no valor da transação
610

FIG. 6

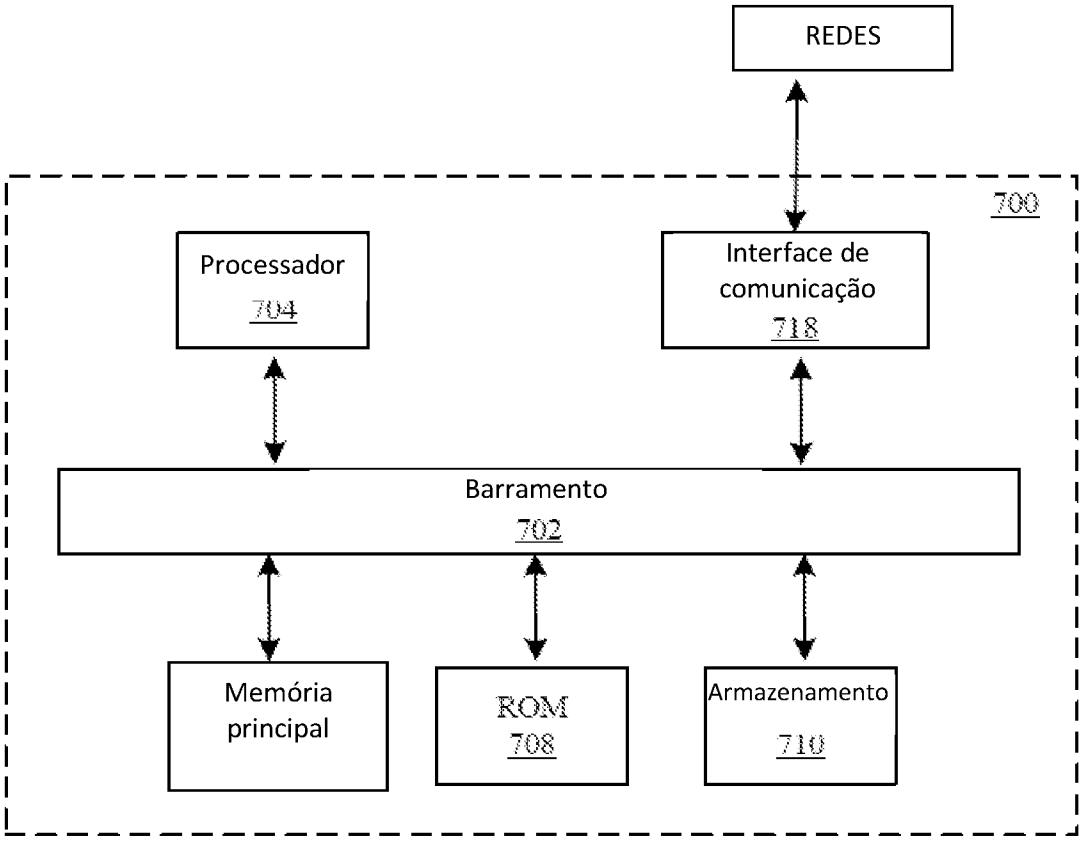

REDES
700
Processador
704
Interface de
comunicação
718
Barramento
702
Memória
principal
ROM
708
Armazenamento
710

FIG. 7

RESUMO

"SISTEMA E MÉTODO PARA PROTEÇÃO DE INFORMAÇÃO"

A presente invenção se refere a um método de proteção de informação implementado por computador que compreende: obter uma pluralidade de valores de transação criptografados associados a transações entre uma pluralidade de contas, em que cada um dos valores de transação criptografados é associado a uma das contas que envia ou recebe um dos valores de transação, e a criptografia de cada um dos valores da transação pelo menos oculta se uma conta envia ou recebe um dos valores da transação; gerar uma prova de soma com base nos valores de transação criptografados obtidos, a prova de soma pelo menos indicando que os valores da transação estão equilibrados; e transmitir os valores de transação criptografados e a prova de soma para um ou mais nós em uma rede blockchain para que os nós verificarem as transações.