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

(21) BR 112019007727-8 A2

(22) Data do Depósito: 27/11/2018

(43) Data da Publicação Nacional: 12/11/2019

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

(51) Int. Cl.: H04L 9/06.

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

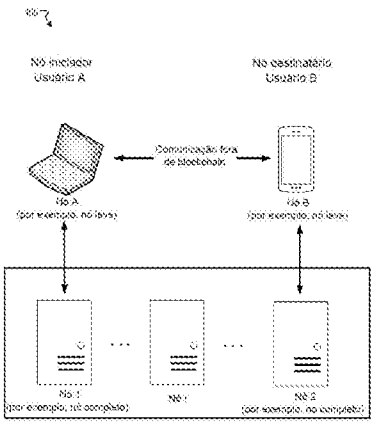
(72) Inventor(es): BAOLI MA; WENBIN ZHANG; HUANYU MA; ZHENG LIU; JIAHUI CUI.

(86) Pedido PCT: PCT CN2018117552 de 27/11/2018

(87) Publicação PCT: WO 2019/072276 de 18/04/2019

(85) Data da Fase Nacional: 16/04/2019

(57) Resumo: Trata-se de um método implementado por computador que compreende: comprometer uma quantia de transação de uma transação com um esquema de compromisso para obter um valor de compromisso de transação, sendo que o esquema de compromisso compreende pelo menos um fator randômico de transação; gerar uma primeira chave de um par de chaves simétricas; criptografar uma combinação do fator randômico de transação e uma quantia de transação t com a primeira chave; e transmitir o valor de compromisso de transação T e a combinação criptografada a um nó de destinatário associado a um destinatário da transação para o nó de destinatário para verificar a transação.



“SISTEMA E MÉTODO PARA PROTEÇÃO DE INFORMAÇÕES”

CAMPO DA TÉCNICA

[001]A presente revelação refere-se, em geral, a métodos e dispositivos para proteção de informações.

FUNDAMENTOS

[002]A privacidade é importante para comunicações e transferências de dados dentre vários usuários. Sem proteção, os usuários ficam expostos ao risco de falsidade ideológica, transferência ilegal, ou outras perdas potenciais. O risco se torna ainda maior quando as comunicações e transferências forem implementadas online, devido ao livre acesso de informações online.

SUMÁRIO

[003]Várias modalidades da presente revelação incluem sistemas, métodos e mídias legíveis por computador não transitórias para proteção de informações.

[004]De acordo com um aspecto, um método implementado por computador para proteção de informações compreende: comprometer uma quantia de transação t de uma transação com um esquema de compromisso para obter um valor de compromisso de transação T, sendo que o esquema de compromisso compreende pelo menos um fator randômico de transação r_t; gerar uma primeira chave de um par de chaves simétricas; criptografar uma combinação do fator randômico de transação r_t e da quantia de transação t com a primeira chave; e transmitir o valor de compromisso de transação T e a combinação criptografada a um nó de destinatário associado a um destinatário da transação para que o nó de destinatário verifique a transação.

[005]Em algumas modalidades, gerar a primeira chave compreende: gerar a primeira chave com base em uma chave privada SK_A de um remetente da transação e uma chave pública PK_B do destinatário sob um protocolo de troca de chave Diffie-Hellman (DH).

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

compromisso de Pedersen com base pelo menos no fator randômico de transação r_t e com a quantia de transação t sendo um valor comprometido.

[007]Em algumas modalidades, a combinação do fator randômico de transação r_t e da quantia de transação t compreende uma concatenação do fator randômico de transação r_t e da quantia de transação t.

[008]Em algumas modalidades, transmitir o valor de compromisso de transação T e a combinação criptografada ao nó de destinatário associado ao destinatário da transação para que o nó de destinatário verifique a transação compreende transmitir o valor de compromisso de transação T e a combinação criptografada ao nó de destinatário associado ao destinatário da transação, induzir o nó de destinatário a: gerar uma segunda chave do par de chaves simétricas com base em uma chave privada SK_B do destinatário e uma chave pública PK_A de um remetente da transação; descriptografar a combinação criptografada com a segunda chave gerada pelo nó de destinatário para obter o fator randômico de transação r_t e a quantia de transação t; e verificar a transação com base pelo menos no valor de compromisso de transação T, no fator randômico de transação r_t e na quantia de transação t.

[009]Em algumas modalidades, induzir o nó de destinatário a verificar a transação com base pelo menos no valor de compromisso de transação T, no fator randômico de transação r_t, e na quantia de transação t compreende induzir o nó de destinatário a: em resposta à determinação que o valor de compromisso de transação T não corresponde ao esquema de compromisso da quantia de transação t com base no fator randômico de transação r_t, rejeitar a transação; e em resposta à determinação que o valor de compromisso de transação T corresponde ao esquema de compromisso da quantia de transação t com base no fator randômico de transação r_t, aprovar a transação assinando-se a transação a gerar uma assinatura de destinatário SIGB para retornar a um nó de remetente associado ao remetente.

[010]Em algumas modalidades, antes de transmitir a combinação criptografada ao nó de destinatário associado ao destinatário, o método compreende, ainda: comprometer um troco y da transação com o esquema de compromisso para obter um valor de compromisso de troco Y, sendo que o esquema de compromisso compreende pelo menos um fator randômico de troco r_y, em que o troco y é um ou mais ativos do remetente explorados para a transação menos a quantia de transação t; gerar outra chave com base em uma chave privada SK_A do remetente e na chave pública PK_A do remetente; e criptografar outra combinação do fator randômico de troco r_y e do troco y com a outra chave.

[011]Em algumas modalidades, o método compreende, ainda: em resposta à recepção da assinatura de destinatário SIGB, aprovar a transação assinando-se a transação para gerar uma assinatura de remetente SIGA; e submeter a transação que compreende a combinação criptografada, a outra combinação criptografada, o valor de compromisso de transação T, o valor de compromisso de troco Y, a assinatura de remetente SIGA, e a assinatura de destinatário SIGB a um ou mais nós em uma rede de blockchain para um ou mais nós para verificar a transação.

[012]Em algumas modalidades, submeter a transação que compreende a combinação criptografada, a outra combinação criptografada, o valor de compromisso de transação T, o valor de compromisso de troco Y, a assinatura de remetente SIGA, e a assinatura de destinatário SIGB a um ou mais nós na rede de blockchain para um ou mais nós para verificar a transação compreende: submeter a transação que compreende a combinação criptografada, a outra combinação criptografada, o valor de compromisso de transação T, o valor de compromisso de troco Y, a assinatura de remetente SIGA, e a assinatura de destinatário SIGB a um ou mais nós na rede de blockchain, induzir um ou mais nós, em resposta à verificação bem-sucedida da transação, a emitir a quantia de transação t ao destinatário, eliminar um ou mais ativos explorados para a transação, e emitir o troco y ao remetente.

[013]De acordo com outro aspecto, uma mídia de armazenamento legível por computador não transitória armazena instruções a serem executadas por um processador para induzir o processador a realizar operações que compreendem: comprometer uma quantia de transação t de uma transação com um esquema de compromisso para obter um valor de compromisso de transação T, sendo que o esquema de compromisso compreende pelo menos um fator randômico de transação r_t; gerar uma primeira chave de um par de chaves simétricas; criptografar uma combinação do fator randômico de transação r_t e da quantia de transação t com a primeira chave; e transmitir o valor de compromisso de transação T e a combinação criptografada a um nó de destinatário associado a um destinatário da transação para o nó de destinatário para verificar a transação.

[014]De acordo com outro aspecto, um sistema para proteção de informações compreende um processador e uma mídia de armazenamento legível por computador não transitória acoplada ao processador, sendo que a mídia de armazenamento que armazena instruções a serem executadas pelo processador para induzir o sistema a realizar operações compreende: comprometer uma quantia de transação t de uma transação com um esquema de compromisso para obter um valor de compromisso de transação T, sendo que o esquema de compromisso compreende pelo menos um fator randômico de transação r_t; gerar uma primeira chave de um par de chaves simétricas; criptografar uma combinação do fator randômico de transação r_t e da quantia de transação t com a primeira chave; e transmitir o valor de compromisso de transação T e a combinação criptografada a um nó de destinatário associado a um destinatário da transação para o nó de destinatário para verificar a transação.

[015]De acordo com outro aspecto, um método implementado por computador para proteção de informações compreende: comprometer uma quantia de transação t de uma transação com um esquema de compromisso para obter um valor de compro-

misso de transação T, sendo que o esquema de compromisso compreende pelo menos um fator randômico de transação r_t; gerar uma primeira chave de um par de chaves simétricas; criptografar uma combinação do fator randômico de transação r_t e a quantia de transação t com a primeira chave; e transmitir o valor de compromisso de transação T e a combinação criptografada a um nó de destinatário associado a um destinatário da transação para o nó de destinatário para: gerar uma segunda chave do par de chaves simétricas com base em uma chave privada SK_B do destinatário e uma chave pública PK_A do remetente, descriptografar a combinação criptografada com a segunda chave gerada pelo nó de destinatário para obter o fator randômico de transação r_t e a quantia de transação t, e verificar a transação com base pelo menos no valor de compromisso de transação T, no fator randômico de transação r_t, e na quantia de transação t.

[016]De acordo com outro aspecto, uma mídia de armazenamento legível por computador não transitória armazena instruções a serem executadas por um processador para induzir o processador a realizar operações que compreendem: comprometer uma quantia de transação t de uma transação com um esquema de compromisso para obter um valor de compromisso de transação T, sendo que o esquema de compromisso compreende pelo menos a fator randômico de transação r_t; gerar uma primeira chave de um par de chaves simétricas; criptografar uma combinação do fator randômico de transação r_t e da quantia de transação t com a primeira chave; e transmitir o valor de compromisso de transação T e a combinação criptografada a um nó de destinatário associado a um destinatário da transação para o nó de destinatário para: gerar uma segunda chave do par de chaves simétricas com base em uma chave privada SK_B do destinatário e uma chave pública PK_A do remetente, descriptografar a combinação criptografada com a segunda chave gerada pelo nó de destinatário para obter o fator randômico de transação r_t e a quantia de transação t, e verificar a transação com base pelo menos no valor de compromisso de transação T, no fator

randômico de transação r_t, e na quantia de transação t.

[017]De acordo com outro aspecto, um sistema para proteção de informações compreende um processador e uma mídia de armazenamento legível por computador não transitória acoplada ao processador, sendo que a mídia de armazenamento armazena instruções a serem executadas pelo processador para induzir o sistema a realizar operações que compreendem: comprometer uma quantia de transação t de uma transação com um esquema de compromisso para obter um valor de compromisso de transação T, sendo que o esquema de compromisso compreende pelo menos a fator randômico de transação r_t; gerar uma primeira chave de um par de chaves simétricas; criptografar uma combinação do fator randômico de transação r_t e da quantia de transação t com a primeira chave; e transmitir o valor de compromisso de transação T e a combinação criptografada a um nó de destinatário associado a um destinatário da transação para o nó de destinatário para: gerar uma segunda chave do par de chaves simétricas com base em uma chave privada SK_B do destinatário e uma chave pública PK_A do remetente, descriptografar a combinação criptografada com a segunda chave gerada pelo nó de destinatário para obter o fator randômico de transação r_t e a quantia de transação t, e verificar a transação com base pelo menos no valor de compromisso de transação T, no fator randômico de transação r_t, e na quantia de transação t.

[018]De acordo com outro aspecto, um método implementado por computador para proteção de informações compreende: comprometer uma quantia de transação t de uma transação com um esquema de compromisso para obter um valor de compromisso de transação T, sendo que o esquema de compromisso compreende pelo menos a fator randômico de transação r_t; gerar uma primeira chave de um par de chaves simétricas; criptografar uma combinação do fator randômico de transação r_t e a quantia de transação t com a primeira chave; e transmitir o valor de compromisso de tran-

sação T e a combinação criptografada a um nó de destinatário associado a um destinatário da transação para o nó de destinatário para: gerar uma segunda chave do par de chaves simétricas com base em uma chave privada SK_B do destinatário e uma chave pública PK_A do remetente, descriptografar a combinação criptografada com a segunda chave gerada pelo nó de destinatário para obter o fator randômico de transação r_t e a quantia de transação t, e verificar a transação com base pelo menos no valor de compromisso de transação T, no fator randômico de transação r_t, e na quantia de transação t.

[019]De acordo com outro aspecto, uma mídia de armazenamento legível por computador não transitória stores instruções a serem executadas por um processador para induzir o processador a realizar operações que compreendem: comprometer uma quantia de transação t de uma transação com um esquema de compromisso para obter um valor de compromisso de transação T, sendo que o esquema de compromisso compreende pelo menos a fator randômico de transação r_t; gerar uma primeira chave de um par de chaves simétricas; criptografar uma combinação do fator randômico de transação r_t e a quantia de transação t com a primeira chave; e transmitir o valor de compromisso de transação T e a combinação criptografada a um nó de destinatário associado a um destinatário da transação para o nó de destinatário para: gerar uma segunda chave do par de chaves simétricas com base em uma chave privada SK_B do destinatário e uma chave pública PK_A do remetente, descriptografar a combinação criptografada com a segunda chave gerada pelo nó de destinatário para obter o fator randômico de transação r_t e a quantia de transação t, e verificar a transação com base pelo menos no valor de compromisso de transação T, no fator randômico de transação r_t, e na quantia de transação t.

[020]De acordo com outro aspecto, um sistema para proteção de informações compreende um processador e uma mídia de armazenamento legível por computador

não transitória acoplada ao processador, sendo que a mídia de armazenamento armazena instruções a serem executadas pelo processador para induzir o sistema a realizar operações compreende: comprometer uma quantia de transação t de uma transação com um esquema de compromisso para obter um valor de compromisso de transação T, sendo que o esquema de compromisso compreende pelo menos a fator randômico de transação r_t; gerar uma primeira chave de um par de chaves simétricas; criptografar uma combinação do fator randômico de transação r_t e a quantia de transação t com a primeira chave; e transmitir o valor de compromisso de transação T e a combinação criptografada a um nó de destinatário associado a um destinatário da transação para o nó de destinatário a: gerar uma segunda chave do par de chaves simétricas com base em uma chave privada SK_B do destinatário e uma chave pública PK_A do remetente, descriptografar a combinação criptografada com a segunda chave gerada pelo nó de destinatário para obter o fator randômico de transação r_t e a quantia de transação t, e verificar a transação com base pelo menos no valor de compromisso de transação T, no fator randômico de transação r_t, e na quantia de transação t.

[021]De acordo com outro aspecto, um método implementado por computador para proteção de informações compreende: obter uma combinação de um fator randômico de transação r_t e uma quantia de transação t criptografada com uma primeira chave de um par de chaves simétricas, e obter um valor de compromisso de transação T, em que: a quantia de transação t é comprometida com um esquema de compromisso por um nó de remetente associado a um remetente de uma transação para obter o valor de compromisso de transação T, sendo que o esquema de compromisso compreende pelo menos o fator randômico de transação r_t; gerar uma segunda chave do par de chaves simétricas; descriptografar a combinação obtida com a segunda chave gerada por um nó de destinatário associado a um destinatário da transação para obter o fator randômico de transação r_t e a quantia de transação t; e

verificar a transação com base pelo menos no valor de compromisso de transação T, no fator randômico de transação r_t, e na quantia de transação t.

[022]De acordo com outro aspecto, uma mídia de armazenamento legível por computador não transitória armazena instruções a serem executadas por um processador para induzir o processador a realizar operações que compreendem: obter uma combinação de um fator randômico de transação r_t e uma quantia de transação t criptografada com uma primeira chave de um par de chaves simétricas, e obter um valor de compromisso de transação T, em que: a quantia de transação t é comprometida com um esquema de compromisso por um nó de remetente associado a um remetente de uma transação para obter o valor de compromisso de transação T, sendo que o esquema de compromisso compreende pelo menos o fator randômico de transação r_t; gerar uma segunda chave do par de chaves simétricas; descriptografar a combinação obtida com a segunda chave gerada por um nó de destinatário associado a um destinatário da transação para obter o fator randômico de transação r_t e a quantia de transação t; e verificar a transação com base pelo menos no valor de compromisso de transação T, no fator randômico de transação r_t, e na quantia de transação t.

[023]De acordo com outro aspecto, um sistema para proteção de informações compreende um processador e uma mídia de armazenamento legível por computador não transitória acoplada ao processador, sendo que a mídia de armazenamento armazena instruções a serem executadas pelo processador para induzir o sistema a realizar operações compreende: obter uma combinação de um fator randômico de transação r_t e uma quantia de transação t criptografada com uma primeira chave de um par de chaves simétricas, e obter um valor de compromisso de transação T, em que: a quantia de transação t é comprometida com um esquema de compromisso por um nó de remetente associado a um remetente de uma transação para obter o valor de compromisso de transação T, sendo que o esquema de compromisso compreende

pelo menos o fator randômico de transação r_t; gerar uma segunda chave do par de chaves simétricas; descriptografar a combinação obtida com a segunda chave gerada por um nó de destinatário associado a um destinatário da transação para obter o fator randômico de transação r_t e a quantia de transação t; e verificar a transação com base pelo menos no valor de compromisso de transação T, no fator randômico de transação r_t, e na quantia de transação t.

[024]Esses e outros recursos dos sistemas, métodos e mídias legíveis por computador não transitórias revelados no presente documento, bem como os métodos de operação e funções dos elementos relacionados de estrutura e uma combinação de partes e economias de fabricação, se tornarão mais aparentes mediante consideração da descrição a seguir e das reivindicações anexas com referência aos desenhos anexos, sendo que todos formam uma parte deste relatório descritivo, em que referências numéricas similares designam partes correspondentes nas várias figuras. No entanto, deve-se compreender expressamente que os desenhos servem para propósitos de ilustração e descrição somente e não são destinados como uma definição dos limites da invenção.

BREVE DESCRIÇÃO DOS DESENHOS

[025]Determinados recursos de várias modalidades da presente tecnologia são particularmente apresentados nas reivindicações anexas. Uma melhor compreensão dos recursos e vantagens da tecnologia será obtida com referência à descrição detalhada a seguir que apresenta modalidades ilustrativas, em que os princípios da invenção são utilizados, e os desenhos anexos em que:

[026]A Figura 1 ilustra um sistema exemplificador para proteção de informações, de acordo com várias modalidades.

[027]A Figura 2 ilustra etapas exemplificadoras para iniciação e verificação de transação, de acordo com várias modalidades.

[028]A Figura 3A ilustra um fluxograma de um método exemplificador para

proteção de informações, de acordo com várias modalidades.

[029]A Figura 3B ilustra um fluxograma de um método exemplificador para proteção de informações, de acordo com várias modalidades.

[030]A Figura 4A ilustra um fluxograma de um método exemplificador para proteção de informações, de acordo com várias modalidades.

[031]A Figura 4B ilustra um fluxograma de um método exemplificador para proteção de informações, de acordo com várias modalidades.

[032]A Figura 5 ilustra um diagrama de blocos de um sistema computacional exemplificador no qual qualquer uma das modalidades descritas no presente documento pode ser implementada.

DESCRIÇÃO DETALHADA

[033]Blockchain pode ser considerado como um banco de dados descentralizado, comumente referido como uma razão distribuída porque a operação é realizada por vários nós (por exemplo, dispositivos computacionais) em uma rede. Qualquer informações pode ser gravada ao blockchain e salva ou lida a partir do mesmo. Qualquer um pode ajustar um servidor e participar da rede de blockchain para se tornar um nó. Qualquer nó pode contribuir computando potência para manter o blockchain realizando-se computações complexas, tal como um cálculo hash para adicionar um bloco a um blockchain atual, e o bloco adicionado pode conter vários tipos de dados ou informações. O nó que contribuiu computando potência para o bloco adicionado pode ser compensado com um token (por exemplo, unidade de moeda digital). Visto que o blockchain não tem um nó central, cada nó é igual e mantém todo o banco de dados de blockchain.

[034]Os nós são, por exemplo, dispositivos computacionais ou granes sistemas computacionais que suportam a rede de blockchain e a mantém funcionando sem percalços. Existem dois tipos de nós, nós completos e nós leves. Os nós completos mantêm uma cópia completa do blockchain. Os nós completos na rede de blockchain

validam transações e blocos que eles recebem e os retransmitem aos peers conectados para proporcionar uma verificação consenso das transações. Os nós leves, por outro lado, transferem por download somente uma fração do blockchain. Por exemplo, nós leves são usados para transações de moeda digital. Um nó leve se comunicará com um nó completo quando desejar fazer transação.

[035]Essa propriedade de descentralização pode ajudar a evitar o surgimento de uma central de gerenciamento em uma posição controlada. Por exemplo, a manutenção do blockchain de bitcoin é realizada pela rede de nós de comunicação do software de bitcoin na área em execução. Essa revelação usa um ou mais blockchains ou moedas digitais, tal como bitcoin e ethereum, como exemplos. Um indivíduo com conhecimento comum na técnica deve avaliar que as soluções técnicas reveladas nesta revelação podem usar ou se aplicar a outro tipo de blockchains e moedas digitais. Ou seja, ao invés de bancos, instituições, ou administradores no sentido tradicional, existem múltiplos intermediários soba forma de servidores computacionais que executa um software de bitcoin. Esses servidores computacionais formam uma rede conectada através da Internet, em que qualquer um pode potencialmente participar da rede. As transações acomodadas pela rede podem ser de uma forma: “usuário A deseja enviar Z bitcoins ao usuário B,” em que as transações são radiodifundidas à rede usando aplicativos de software prontamente disponíveis. Os servidores computacionais funcionam como servidores de bitcoin que são operáveis para validar essas transações financeiras, adicionar um registro das mesmas para sua cópia à contabilidade, e, então, radiodifundir essas adições de contabilidade a outros servidores da rede.

[036]A manutenção do blockchain é referida como “mineração,” e aqueles que fazem essa manutenção são concedidos com bitcoins recentemente criados e taxas de transação conforme supramencionado. Por exemplo, os nós podem determinar se

as transações são válidas com base em um conjunto de regras que a rede de blockchain concordou com. Os mineradores podem estar situados em qualquer continente e processar pagamentos verificando-se cada transação como válida e adicionando-a ao blockchain. Essa verificação é alcançada através de consenso proporcionado por uma pluralidade de mineradores e supõe que não existe uma colusão sistemática. No final das contas, todos os dados serão consistentes, porque a computação precisa satisfazer determinadas exigências como sendo válidas e todos os nós serão sincronizados para garantir que o blockchain seja consistente. Logo, os dados podem ser consistentemente armazenados em um sistema distribuído de nós de blockchain.

[037]Através do processo de mineração, as transações como transferências de ativos são verificadas e adicionadas a uma cadeia crescente de blocos de um blockchain por nós de rede. Atravessando-se todo o blockchain, a verificação pode incluir, por exemplo, se a parte pagante tem acesso ao ativo de transferência, se o ativo foi gasto antes, se a quantia de transferência está correta, etc. Por exemplo, em uma transação hipotética (por exemplo, uma transação de bitcoins sob um modelo UTXO (saída de transação não gasta), uma transação de moedas Ethereum sob um modelo de Conta/Saldo) assinado por um remetente, a transação proposta pode ser radiodifundida à rede de blockchain par mineração. Um minerador precisa verificar se a transação é plausível de ser executada de acordo com o histórico de blockchain. Se o saldo em carteira do remetente tiver fundos suficientes de acordo com o histórico de blockchain existente, a transação é considerada válida e pode r adicionada ao bloco. Uma vez verificadas, as transferências de ativos podem ser incluídas no próximo bloco a ser adicionado ao blockchain.

[038]Um bloco é muito semelhante a um registro de banco de dado. Cada gravação de dados cria um bloco. Esses blocos são ligados e protegidos usando criptografia para se tornarem redes interconectadas. Cada bloco é conectado ao bloco

anterior, que também é a origem do nome “blockchain.” Cada bloco geralmente contém o hash criptográfico do bloco anterior, o tempo de geração, e os dados reais. 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 reais (por exemplo, dados de transação). A cadeia de blocos é ligada através dos cabeçalhos de bloco. Cada cabeçalho de bloco pode conter múltiplos valores de recurso, como versão, hash de bloco anterior, raiz merkle, carimbo de data e hora, alvo de dificuldade, e nonce. O hash de bloco anterior contém não somente o endereço do bloco anterior, mas também o hash dos dados dentro do bloco anterior, tornando, assim, os blockchains mutáveis. O nonce é um número que, quando incluído, produz um hash com um número específico de bits de zeros à esquerda.

[039]Para mineração, o hash dos conteúdos do novo bloco é tomado por um nó. O nonce (por exemplo, sequência aleatória) é anexado ao hash para obter uma nova sequência. A nova sequência se encontra novamente em hash. O hash final é, então, comparado ao alvo de dificuldade (por exemplo, um nível) e determinado se o hash final é realmente menor que o alvo de dificuldade ou não. Caso negativo, então, o nonce é alterado e o processo se repete novamente. Caso positivo, então, o bloco é adicionado à cadeia e a contabilidade púbica é atualizada e alertada da adição. O nó responsável pela adição bem-sucedida é recompensado com bitcoins, por exemplo, adicionando-se uma transação de recompensa a ele mesmo no novo bloco (conhecido como geração de coinbase).

[040]Ou seja, para cada saída “Y”, se k for escolhido a partir de uma distribuição com entropia mínima alta, é improvável encontrar uma entrada x de modo que H(k|x) = Y, onde K é o nonce, x é o hash do bloco, Y é o alvo de dificuldade, e “|” denota uma concatenação. Considerando-se hashes criptográficos sendo essencialmente aleatórios, no sentido que sua saída não pode ser prevista a partir de suas

entradas, existe somente uma forma conhecida de encontrar o nonce: testar os inteiros um após o outro, por exemplo 1, então 2, então 3, e assim por diante, que podem ser conhecidos como força abruta. Quanto maior o número de zeros à esquerda, mais tempo em média levará para encontrar um nonce de requisito Y. Em um exemplo, o sistema de bitcoin ajusta constantemente o número de zeros à esquerda, de modo que o tempo médio para encontrar um nonce é cerca de dez minutos. Dessa forma, à medida que capacidades de processamento de hardware computacional aumentam com o tempo, com o passar dos anos, o protocolo de bitcoin simplesmente requer mais bits de zeros à esquerda para produzir a mineração leva uma duração de cerca de dez minutos para implementar.

[041]Conforme descrito, hashing é um alicerce importante para blockchain. O algoritmo hash pode ser entendido como uma função que compacta mensagens de qualquer comprimento em uma compilação de mensagem de comprimento fixo. Mais comumente usados são MD5 e SHA. Em algumas modalidades, o comprimento hash do blockchain é 256 bits, o que significa que não importa qual conteúdo original for, um número binário de 256 bits é finalmente calculado. E pode ser garantido que o hash correspondente é exclusivo desde que o conteúdo original seja diferente. Por exemplo, o hash da sequência “123” é a8fdc205a9f19cc1c7507a60c4f01b13d11d7fd0 (hexadecimal), que tem 256 bits quando convertido em binário, e somente “123” tem esse hash. O algoritmo hash no blockchain é irreversível, ou seja, o cálculo avançado é fácil (de “123” a a8fdc205a9f19cc1c7507a60c4f01b1c7507a60c4f01b13d11d7fd0), e o cálculo inverso não pode ser feito mesmo se todos os recursos computacionais forem esgotados. Logo, o hash de cada bloco do blockchain é exclusivo.

[042]Ademais, se o conteúdo do bloco se alterar, seu hash se alterará. O bloco e o hash são em uma correspondência um para um, e o hash de cada bloco é especificamente calculado 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 de cálculo de hash de bloco, SHA256 é um algoritmo de blockchain aplicado ao cabeçalho de bloco. O hash é exclusivamente determinado pelo cabeçalho de bloco, e não o corpo de bloco. Conforme mencionado anteriormente, o cabeçalho de bloco contém muitos conteúdos, incluindo o hash do bloco atual, e o hash do bloco anterior. Isso significa que os conteúdos da alteração de bloco atual, ou se o hash do bloco anterior se alterar, isso causará uma alteração de hash no bloco atual. Se um hacker modificar um bloco, o hash desse bloco s altera. A fim de que um último bloco se conecte ao bloco modificado, o hacker deve modificar todos os blocos subsequentes sucessivamente, porque o próximo bloco deve conter o hash do bloco anterior. Caso contrário, o bloco modificado será desanexado do blockchain. Devido a razões de design, os cálculos de hash são demorados, e é quase impossível modificar múltiplos blocos e um curto período de tempo a não ser que o hacker tenha dominado mais de 51% da potência computacional de toda a rede. Logo, o blockchain garante sua própria confiabilidade, e uma vez que os dados são gravados, o mesmo não pode ser adulterado.

[043]Uma vez que o minerador encontrar o hash (ou seja, uma assinatura ou solução legível) para o novo bloco, o minerador radiodifunde essa assinatura a todos os outros mineradores (nós do blockchain). Outros mineradores agora verifica em seus turnos se essa solução corresponde ao problema do bloco do remetente (ou seja, determinar se a entrada de hash realmente resulta nessa assinatura). E a solução for válida, os outros mineradores confirmarão a solução e concordarão que o novo bloco pode ser adicionado ao blockchain. Logo, o consenso do novo bloco é alcançado. Isso também é conhecido como “prova de trabalho.” O bloco ao qual o consenso foi alcançado agora pode ser adicionado ao blockchain e é radiodifundido a todos os nós na rede ao longo de sua assinatura. Os nós aceitarão o bloco e o salvará a seus dados de transação desde que as transações dentro do bloco correspondam corretamente

aos saldos em carteira atuais (histórico de transação) nesse ponto de tempo. Sempre que um novo bloco for adicionado no topo desse bloco, a adição também conta como outra "confirmação" para os blocos antes dela. Por exemplo, se uma transação for incluída no bloco 502, e o blockchain tiver 507 blocos de comprimento, isso significa que a transação tem cinco confirmações (correspondentes aos blocos 507 a 502). Quanto mais confirmações a transação tiver, mais difícil será para os invasores alterá-la.

[044]Em algumas modalidades, um sistema de ativo de blockchain exemplificador utiliza criptografia de chave pública, em que duas chaves criptográficas, uma chave pública e uma chave privada, são geradas. A chave pública pode ser considerada como sendo um número de conta, e a chave privada pode ser considerada como sendo credenciais de propriedade. Por exemplo, uma carteira de bitcoin é uma coleção das chaves públicas e privadas. A propriedade de um ativo (por exemplo, moeda digital, ativo em dinheiro, ação, títulos, caução) associado a um determinado endereço de ativo pode ser demonstrada com a confirmação da chave privada pertencendo ao endereço. Por exemplo, o software de carteira de bitcoin, algumas vezes referido como sendo um "software de cliente de bitcoin", permite que um dado usuário faça transação com bitcoins. Um programa de carteira gera e armazena chaves privadas e se comunica com peers na rede de bitcoin.

[045]Em transações de blockchain, os contribuintes e beneficiários são identificados no blockchain por suas chaves criptográficas públicas. Por exemplo, as transferências de bitcoin mais contemporâneas são de uma chave pública a uma chave pública diferente. Na prática, hashes dessas chaves são usadas no blockchain e são denominados como "endereços de bitcoin." Em princípio, se uma pessoa invasora hipotética S puder roubar dinheiro da pessoa A simplesmente adicionando-se transações à contabilidade de blockchain como "pessoa A pega a pessoa S 100 bitcoins," usando os endereços de bitcoin dos usuários ao invés de seus nomes. O protocolo de

bitcoin evita esse tipo de roubo exigindo-se que cada transferência seja digitalmente assinada com a chave privada do contribuinte, e somente transferências assinadas podem ser adicionadas à contabilidade de blockchain. Visto que a pessoa S não pode forjar a assinatura da pessoa A, a pessoa S não pode defraudar a pessoa A adicionando-se uma entrada ao blockchain equivalente a "pessoa A paga S 200 bitcoins." Ao mesmo tempo, qualquer um pode verificar a assinatura da pessoa A usando sua chave pública, e, portanto, que ele autorizou alguma transação no blockchain onde ele é o contribuinte.

[046]No contexto de transação de bitcoins, para transferir alguns bitcoins ao usuário B, o usuário A pode construir um registro contendo informações sobre a transação através de um nó. O registro pode ser assinado com uma chave de assinatura do usuário A (chave privada) e conter uma chave de verificação pública do usuário A e uma chave de verificação púbica do usuário B. A assinatura é usada para confirmar que a transação foi proveniente do usuário, e também evita que a transação seja alterada por qualquer um uma vez que foi lançada. O registro vinculado a outro registro que ocorreu na mesma janela de tempo em um novo bloco pode ser radiodifundido aos nós completos. Mediante a recepção dos registros, os nós completos podem funcionar em incorporar os registros na contabilidade de todas as transações que ocorreram no sistema de blockchain, adicionar o novo bloco a um blockchain previamente aceito através do processo de mineração descrito anteriormente, e validar o bloco adicionado contra as regras consenso da rede.

[047]O modelo UTXO (saída de transação não gasta) e o modelo de Conta/Saldo são dois modelos exemplificadores para implementar transações de blockchain. UTXO é um modelo de objeto de blockchain. Sob UTXO, os ativos são representados por saídas de transações de blockchain que não foram gastas, que podem ser usadas como entradas em novas transações. Por exemplo, o ativo do usuário A a ser transferido pode estar sob a forma de UTXO. Para gastar (fazer transação) o

ativo, o usuário A precisa assinar com a chave privada. Bitcoin é um exemplo de uma moeda digital que usa o modelo UTXO. No caso de uma transação de blockchain válida, as saídas não gastas podem ser usadas para efetuar outras transações. Em algumas modalidades, somente saídas não gastas podem ser usadas em transações adicionais para evitar gastar em dobro e fraudes. Por essa razão, as entradas em um blockchain são deletadas quando uma transação ocorre, enquanto ao mesmo tempo, saídas são criadas sob a forma de UTXOs. Essas saídas de transação não gastas podem ser usadas (pelos detentores de chaves privadas, por exemplo, pessoas com carteiras de moeda digital) para o propósito de transações futuras.

[048]O modelo de Conta/Saldo (ou referido como um Modelo de Transação baseado em Conta), por outro lado, acompanha o saldo de cada conta como um estado global. O saldo de uma conta é verificado para ter certeza que seja maior ou igual à quantia de transação gasta. Fornece-se m exemplo de como o Modelo de Conta/Saldo funciona em Ethereum:

1. Alice ganha 5 ethers através de mineração. Registra-se no sistema que Alice tem 5 ethers.

2. Alice deseja dar a Bob 1 ether, logo, o sistema primeiro deduzirá 1 ether da conta de Alice, logo Alice agora terá 4 ethers.

3. Então, o sistema aumenta a conta de Bob em 1 ether. O sistema sabe que Bob tem 2 ethers inicialmente, portanto, o saldo de Bob é aumentado para 3 ethers.

[049]A manutenção de registros para Ethereum pode ocorrer como em um banco. Uma analogia é usar um caixa eletrônico/cartão de débito. O banco monitora quanto de dinheiro cada cartão de débito tem, e quando Bob desejar gastar dinheiro, o banco verifica seus registros para ter certeza que Bob tem saldo suficiente antes de aprovar a transação.

[050]Visto que o blockchain e outras contabilidades similares são completamente públicas, o próprio blockchain não tem proteção de privacidade. A natureza

pública da rede P2P significa que, embora aqueles que a usam não sejam identificados por nome, vincular transações a indivíduos e empresas é viável. Por exemplo, em remessas transfronteiriças ou na cadeia de suprimentos, a quantia de transação tem um nível extremamente alto de valor de proteção de privacidade, porque com a quantia de informações de transação, é possível inferir o local específico e identidades das partes de transação. A matéria da transação pode compreender, por exemplo, dinheiro, token, moeda digital, contrato, escritura, registro médico, detalhamento de clientes, ações, caução, títulos, ou qualquer outro ativo que possa ser descrito sob a forma digital. Embora o modelo UTXO possa proporcionar anonimato às quantias de transação, por exemplo, através de assinatura em anel em Monero e criptografia de conhecimento zero Zcash, as quantias de transação permanecem desprotegidas sob um Modelo de Conta/Saldo. Logo, um problema técnico levantado pela presente revelação é como proteger informações online como a privacidade das quantias de transação. Essas transações podem estar sob o Modelo de Conta/Saldo.

[051]Algumas tecnologias existentes propõem usar o esquema de compromisso de Pedersen para criptografar a quantia de transação e substituir o Modelo de Conta/Saldo. Sob o esquema, o remetente envia a quantia de transação e um número aleatório correspondente ao compromisso de Pedersen da quantia de transação ao beneficiário através de um canal seguro fora do blockchain. O beneficiário verifica se o número aleatório corresponde ao compromisso de transação e realiza um armazenamento local. Por exemplo, sob o Modelo de Conta/Saldo, uma conta pode ser tratada como uma carteira (conta) para manter os ativos que sejam agregados, mas não incorporados. Cada ativo pode corresponder a um tipo de ativo (por exemplo, criptomoeda), e o saldo da conta é a soma dos valores patrimoniais. Mesmo ativos do mesmo tipo não são incorporados. Durante a transação, um destinatário de uma transferência de ativo pode ser especificado, e o ativo correspondente pode ser removido da carteira para financiar a transação. Os nós de blockchain verificam que a carteira

pagante tenha ativos suficientes para cobrir a transação, e, então, os nós excluem o ativo transferido da carteira pagante e adicionam um ativo correspondente à carteira do destinatário.

[052]No entanto, ainda existem limitações para esse esquema. Primeiro, o esquema requer que o usuário mantenha um armazenamento persistente localmente para gerenciar os números aleatórios e saldos em purotexto correspondentes ao saldo em conta criptografado, e a implementação de gerenciamento é complicada; segundo, o armazenamento de fatores randômicos (por exemplo, os números aleatórios) e os saldos em purotexto correspondentes ao “ativo de Pedersen” em um nó local único é propenso a perda ou corrupção, enquanto um armazenamento de backup multi-nodal é difícil de realizar devido à mudança frequente do saldo em conta.

[053]Os sistemas e métodos apresentados nesta revelação podem superar as limitações anteriores e alcançar uma proteção de privacidade robusta para quantias de transação, valores patrimoniais, e fatores randômicos em esquemas de compromisso. Nesse sentido, as chaves simétricas obtidas pelo protocolo de troca de chave de Diffie-Hellman (DH) podem ser usadas para criptografar/descriptografar os números aleatórios e os saldos em purotexto, proporcionando, assim, um gerenciamento conveniente. Ademais, armazenar as informações criptografadas em blockchain garante que as quantias de transação, valores patrimoniais, e fatores randômicos em esquemas de compromisso não sejam facilmente perdidos ou adulterados.

[054]Antes de discutir as figuras desta revelação, o Compromisso de Pedersen e o protocolo de troca de chave de Diffie-Hellman (DH) serão descritos abaixo.

[055]Em algumas modalidades, um esquema de compromisso (por exemplo, compromisso de Pedersen) pode criptografar um determinado valor a (por exemplo, quantia de transação, valor patrimonial, parâmetro de chave) da seguinte forma:

$$PC(a) = r \times G + a \times H$$

[056]onde r é um fator randômico aleatório (alternativamente referido como

um fator randômico) que proporciona ocultação, G e H são os geradores/pontos de base publicamente acordados da curva elíptica e podem ser escolhidos aleatoriamente, sn é o valor do compromisso, C(sn) é o ponto de curva usado como compromisso e dado à contraparte, e H é outro ponto de curva. Ou seja, G e H podem ser parâmetros conhecidos aos nós. Uma geração de "nothing up my sleeve" de H pode ser gerada realizando-se hash no ponto de base G com um mapeamento de função hash a partir de um ponto para outro com H= Hash(G). H e G são os parâmetros públicos do dado sistema (por exemplo, pontos aleatoriamente gerados em uma curva elíptica). Embora acima se proporcione um exemplo de compromisso de Pedersen sob a forma de curva elíptica, várias outras formas de compromisso de Pedersen ou outro esquema de compromissos podem ser alternativamente usadas.

[057]Um esquema de compromisso mantém sigilo de dados, mas se compromete aos dados de modo que não possam ser alterados posteriormente pelo remetente dos dados. Se uma parte souber somente o valor de compromisso (por exemplo, PC(a)), ela não pode determinar quais valores de dados subjacentes (por exemplo, a) foram comprometidos. Tanto os dados (por exemplo, a) como o fator randômico (por exemplo, r) podem ser revelados posteriormente (por exemplo, pelo nó iniciador), e um destinatário (por exemplo, nó de consenso) do compromisso pode executar o compromisso e verificar que os dados comprometidos correspondem aos dados revelados. O fator randômico está presente porque sem um, alguém pode tentar adivinhar os dados.

[058]Os esquemas de compromisso são uma forma que o remetente (parte de compromisso) se compromete a um valor (por exemplo, a) de modo que o valor comprometido permaneça privado, mas pode ser revelado em um momento posterior quando a parte de compromisso divulgar um parâmetro necessário do processo de compromisso. Esquemas de compromisso fortes podem ser ocultação e incorporação computacional de informações. Ocultação se refere à noção que um dado valor a e

um compromisso desse valor PC(a) devem ser irrelacionáves. Ou seja, PC(a) não deve revelar informações sobre a. Com PC(a), G e H conhecidos, é quase impossível conhecer a por causa do número aleatório r. Um esquema de compromisso é incorporação se não houver uma forma passível que dois valores diferentes posam resultar no mesmo compromisso. Um compromisso de Pedersen é ocultação perfeita e incorporação computacional sob a hipótese logarítmica discreta. Ademais, com r, G, H e PC(a) conhecidos, é possível verificar PC(a) determinando-se se PC(a) = r×G + a×H.

[059]Um compromisso de Pedersen tem uma propriedade adicional: compromissos podem ser adicionados, e a soma de um conjunto de compromissos é igual compromisso à soma dos dados (com um fator randômico ajustado como a soma dos fatores randômicos): $PC(r_1, dados_1) + PC(r_2, dados_2) == PC(r_1+r_2, dados_1+dados_2)$; $PC(r_1, dados_1) - PC(r_1, dados_1) == 0$. Em outras palavras, o compromisso preserva a adição e a propriedade comutativa se aplica, isto é, o compromisso de Pedersen é aditivamente homomórfico, pelo fato de que os dados subjacentes podem ser matematicamente manipulados como se não fossem criptografados.

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

[061]O compromisso de Pedersen para o valor de entrada pode ser criado escolhendo-se um gerador adicional para o grupo (H, nas equações abaixo) de modo que alguém saiba o log discreto para o segundo gerador H em relação ao primeiro gerador G (ou vice-versa), significando que ninguém conhece um x de modo que rG=H. Isso pode ser realizado, por exemplo, utilizando-se o hash criptográfico de G

para escolher H: H=to_point(SHA256(ENCODE(G))).

[062]Dados os dois geradores G e H, um esquema de compromisso exemplificador para criptografar o valor de entrada pode ser definido como: compromisso=rG+aH. Aqui, r pode ser o fator randômico secreto, e a pode ser o valor de entrada sendo comprometido. Portanto, se sn for comprometido, o esquema de compromisso descrito anteriormente PC(a) = r×G + a×H pode ser obtido. Os compromissos de Pedersen são informações teoricamente privadas: para qualquer compromisso, existe algum fator randômico que faria com que qualquer quantia correspondesse ao compromisso. Os compromissos de Pedersen podem ser computacionalmente seguros contra compromissos falsos, pelo fato de que um mapeamento arbitrário pode não ser computado.

[063]A parte (nó) que comprometeu o valor pode abrir o compromisso revelando-se o valor original a e o fator r que completa a equação de compromisso. A parte que deseja abrir o valor PC(a) então, computará o compromisso novamente para verificar que o valor original compartilhado de fato corresponde ao compromisso PC(a) inicialmente recebido. Logo, as informações de tipo de ativo podem ser protegidas mapeando-a a um número de série exclusivo, e, então, criptografando-a por compromisso de Pedersen. O número aleatório r escolhido ao gerar o compromisso torna quase impossível que alguém infira o tipo de ativo que é comprometido de acordo com o valor de compromisso PC(a).

[064]Em algumas modalidades, a troca de chave de Diffie-Hellman (DH) pode ser usada como um método para trocar seguramente chaves criptográficas por um canal público. A troca de chave DH, também denominada como troca de chave exponencial, é um método de criptografia digital que usa números elevados a potências específicas para produzir chaves de descriptografia com base nos componentes que nunca serão diretamente transmitidos, tornando a tarefa de um decifrador de códigos would-be matematicamente considerável.

[065]Em um exemplo de implementar uma troca de chave de Diffie-Hellman (DH), os dois usuários finais Alice e Bob, enquanto se comunicam por um canal que eles sabem ser privado, mutuamente concordam em números inteiros positivos p e q, de modo que p seja um número primo e q seja um gerador de p. O gerador q é um número que, quando elevado a potências de número inteiro positivo menores que p, nunca produz o mesmo resultado para quaisquer dois desses números inteiros. O valor de p pode ser grande, mas o valor de q é geralmente pequeno. Ou seja, q é um módulo de raiz primitiva p.

[066]Uma vez que Alice e Bob concordaram em p e q em privado, eles escolhem chaves pessoais de número inteiro positivo a e b, ambos menores que o nódulo de número primo p e ambos podem ser aleatoriamente gerados. O usuário não divulga sua chave pessoal a ninguém, e idealmente, ele memoriza esses números e não os escreve bem armazena em nenhum lugar. A seguir, Alice e Bob computam chaves públicas a* e b* com base em suas chaves pessoais de acordo com as fórmulas

$a^* = q^a \bmod p$

e

$b^* = q^b \bmod p$

[067]Os dois usuários podem compartilhar suas chaves públicas a* e b* por uma mídia de comunicação considerada como sendo insegura, tal como a Internet ou uma rede de área ampliada corporativa (WAN). A partir dessas chaves públicas, um número k1 pode ser gerado por qualquer usuário com base em suas próprias chaves pessoais.

Alice computa k1 usando a fórmula: $k1 = (b^*)^a \bmod p$

Bob computa k1 usando a fórmula: $k1 = (a^*)^b \bmod p$

[068]O valor de k1 fica sendo o mesmo de acordo com qualquer uma das duas fórmulas acima. No entanto, as chaves pessoais a e b, que são fundamentais no cálculo de k1, não foram transmitidas por um meio público. Mesmo com p, q, a* e b*,

ainda é muito difícil calcular a eb. Devido ao fato de ser grande e aparentemente um número aleatório, um hacker potencial quase não tem chance de adivinhar corretamente k1, mesmo com a ajuda de um computador poderoso para conduzir milhões de tentativas. Os dois usuários podem, portanto, em teoria, se comunicar privadamente por um meio público com um método de criptografia de sua escolha usando a chave de descriptografia k1.

[069]Em outro exemplo de implementar uma troca de chave de Diffie-Hellman (DH), todos os cálculos acontecem e um gripo discreto de tamanho suficiente, onde o problema de Diffie-Hellman é considerado difícil, geralmente o grupo multiplicativo modula um número primo grande (por exemplo, para DH clássico) ou um grupo de curva elíptica (por exemplo, para curva elíptica de Diffie-Hellman).

[070]Para duas partes em transação, cada parte escolhe uma chave privada a ou b.

[071]Cada parte calcula a chave pública aG ou bG correspondente.

[072]Cada parte envia a chave pública aG ou bG à outra parte.

[073]Cada parte usa a chave pública recebida junto com sua própria chave privada para calcular o novo segredo compartilhado a(bG) = b(aG), que pode ser referido como chaves simétricas de um par de chaves simétricas.

[074]Conforme descrito posteriormente, esse método exemplificador pode ser usado para gerar chaves simétricas abG e baG. O resultado dessa troca de chave é um segredo compartilhado, que pode, então, ser usado com uma função de derivação de chave (por exemplo, função de criptografia E() usando outra entrada conhecida por ambas as partes, tal como uma concatenação de um número aleatório e um valor patrimonial) para derivar um conjunto de chaves para um esquema de criptografia simétrico. Alternativamente, vários outros métodos de computação podem ser usados, por exemplo, gerando-se chaves públicas g^a e g^b e chave compartilhada g^{ab} ou g^{ba}.

[075]Durante as transações, a proteção de informações é importante para

manter a privacidade do usuário, e a quantia de transação é um tipo de informação que te proteção carente. A Figura 1 mostra um sistema exemplificador 100 para proteção de informações, de acordo com várias modalidades. Conforme mostrado, uma rede de blockchain pode compreender uma pluralidade de nós (por exemplo, nós completos implementados em servidores, computadores, etc.). Para alguma plataforma de blockchain (por exemplo, NEO), nós completos com determinados níveis de direito de voto podem ser referidos como nós de consenso, que assumem a responsabilidade de verificação de transação. Nesta revelação, nós completos, nós de consenso, ou outros nós equivalentes podem verificar a transação.

[076]Da mesma forma, conforme mostrado na Figura 1, o usuário A e o usuário B podem usar dispositivos correspondentes, tais como laptops e telefones móveis que servem como nós leves para realizar transações. Por exemplo, o usuário A pode desejar realizar transação com o usuário B transferindo-se algum ativo na conta do usuário A à conta do usuário B. O usuário A e o usuário B podem usar dispositivos correspondentes instalados com um software de blockchain apropriado para a transação. O dispositivo do usuário A pode ser referido como um nó iniciador A que inicia uma transação com o dispositivo do usuário B referido como nó de destinatário B. O nó A pode acessar o blockchain através da comunicação com o nó 1, e o Nó B pode acessar o blockchain através da comunicação com o nó 2. Por exemplo, o nó A e o nó B podem submeter transações ao blockchain através do nó 1 e do nó 2 para solicitar adicionar as transações ao blockchain. Fora do blockchain, o nó A e o nó B podem ter outros canais de comunicação (por exemplo, comunicação regular via internet sem passar através dos nós 1 e 2).

[077]Cada um dos nós na Figura 1 pode compreender um processador e uma mídia de armazenamento legível por computador não transitória que armazena instruções a serem executadas pelo processador para induzir o nó (por exemplo, o processador) a realizar várias etapas para proteção de informações descritas no presente

documento. Cada nó pode ser instalado com 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. Detalhes adicionais do hardware e software de nó serão descritos posteriormente com referência à Figura 5.

[078]A Figura 2 ilustra etapas exemplificadoras para transação e verificação dentre um nó de remetente A, um nó de destinatário B, e um ou mais nós de verificação, de acordo com várias modalidades. As operações apresentadas abaixo são destinadas a serem ilustrativas. Dependendo da implementação, as etapas exemplificadoras podem incluir etapas adicionais, menos ou alternativas realizadas em várias ordens ou em paralelo.

[079]Em várias modalidades, contas para partes de transação (usuário remetente A e usuário destinatário B) são configuradas par modelo de Conta/Saldo. O usuário A e o usuário B podem realizar as etapas a seguir para realizar a transação através de um ou mais dispositivos, tal como seu laptop, telefone móvel, etc. Os dispositivos podem ser instalados com software e hardware apropriados para realizar as várias etapas. Cada conta pode ser associada a um par de chave privada criptográfica (chave secreta) – chave pública. A chave privada pode ser denotada como SK=x, e a chave pública pode ser denotada como PK=xG, onde G é um gerador do grupo. Cada conta pode conter vários ativos, cada um denotado como: (V=PC(r, v), E(K, r, v)), onde v representa o valor nominal do ativo, V representa um compromisso de Pedersen do valor nominal v, r é um fator randômico (por exemplo, um número aleatório), PC() é um algoritmo de compromisso de Pedersen, E() é um algoritmo de criptografia (por exemplo, algoritmo de criptografia de chave simétrica), e K é uma chave de criptografia. Em um exemplo, cada ativo pode ser denotado como (V=PC(r, v), E(K, r||v)), onde || representa uma concatenação. Cada ativo também ode incluir informações diferentes daquelas listadas, como informações de origem do ativo.

[080]Em um exemplo, antes de o usuário A realizar com sucesso a transação

de uma quantia t ao usuário B em uma transação verificada por blockchain, os endereços e ativos na conta A e na conta B são da seguinte forma:

[081]Para Conta A (conta A):

Endereço: (SK_A=a, PK_A=aG)

Ativos A_1 a A_m respectivamente de valores a_1 a a_m são denotados como:

(A_1=PC(r_{a_1}, a_1), E(K_A, r_{a_1}||a_1)),

(A_2=PC(r_{a_2}, a_2), E(K_A, r_{a_2}||a_2)),

...

(A_m=PC(r_{a_m}, a_m), E(K_A, r_{a_m}||a_m))

[082]Para Conta B (conta B):

Endereço: (SK_B=b, PK_B=bG)

Ativos B_1 a B_n respectivamente de valores b_1 a b_n são denotados como:

(B_1=PC(r_{b_1}, b_1), E(K_B, r_{b_1}||b_1)),

(B_2=PC(r_{b_2}, b_2), E(K_B, r_{b_2}||b_2)),

...

(B_n=PC(r_{b_n}, b_n), E(K_B, r_{b_n}||b_n))

[083]Em algumas modalidades, a geração de chave pode se basear em uma curva elíptica ecp256k1 para cada conta sob o modelo de Conta/Saldo. Por exemplo, em Ethereum ecp256k1, qualquer número entre 1 a 2^{256}-1 pode ser uma chave privada válida SK. Uma biblioteca boa gera uma chave privada levando-se uma aleatoriedade suficiente em consideração. Ethereum requer que a chave privada SK tenha 256 bit de extensão. A geração de chave pública é realizada usando uma operação grupal de criptografia de ECC. Para derivar a chave pública PK, a chave privada pode ser multiplicada por G. A multiplicação usada para derivar a chave pública PK é uma multiplicação de ECC (multiplicação de ponto de curva elíptica), que é diferente da multiplicação normal. G é o ponto gerador que é um dos parâmetros de domínio de

criptografia de ECC. G pode ter um valor fixo para ecp256k1. O endereço pode ser, por exemplo, os últimos 20 bytes do hash da chave pública PK.

[084]Em algumas modalidades, na etapa 201, o nó A pode iniciar uma transação com o nó B. Por exemplo, usuário A e usuário B podem negociar uma quantia de transação t a partir da conta A do usuário A à conta B do usuário B. A conta A e a conta B podem corresponder às "carteiras" descritas no presente documento. A conta A pode ter um ou mais ativos. O ativo pode compreender, por exemplo, dinheiro, token, moeda digital, contrato, escritura, registro médico, detalhamento de clientes, ações, caução, títulos, ou qualquer outro ativo que possa ser descrito sob a forma digital. A conta B pode ter um ou mais ativos ou nenhum ativo. Cada ativo pode ser associado a várias informações de blockchain armazenadas nos blocos do blockchain, sendo que as informações de blockchain compreendem, por exemplo, NoteType que representa um tipo de ativo, NoteID que representa uma identificação exclusiva de um ativo, valores de compromisso que representam um valor de compromisso (por exemplo, compromisso de Pedersen) do valor patrimonial, criptografia de número aleatório e valor patrimonial, etc.

[085]Conforme descrito em relação à conta A, em algumas modalidades, os ativos A_1 a A_m respectivamente correspondem aos valores patrimoniais a_1 a a_m e números aleatórios r_1 a r_m. Com base nos números aleatórios r_1 a r_m, o nó A pode comprometer os valores patrimoniais na conta A a um esquema de compromisso (por exemplo, compromisso de Pedersen) para obter valores de compromisso criptografados. Por exemplo, os valores de compromisso criptografados podem ser PC_1 a PC_m, onde PC_i = PC(r_{a_i}, a_i) = r_{a_i}×G + a_i×H, onde G e H são parâmetros conhecidos, e i está entre 1 e m. Além do primeiro campo PC(...), cada ativo também é associado a um segundo campo E(...) conforme descrito anteriormente. O segundo campo E(...) pode representar uma criptografia do número aleatório correspondente e valor patrimonial criptografado com a chave K_A. Por exemplo, a criptografia pode

ser E(K_A, r_{a_i}||a_i)). PC(...) e(...) para cada ativo pode ser herdado a partir de transações prévias. O mesmo mecanismo pode se aplicar à conta B e seus ativos.

[086]Em algumas modalidades, K_A pode compreender vários tipos de chave de criptografia. Por exemplo, K_A pode ser a*PK_A=aaG que será adicionalmente descrito abaixo, e K_B pode ser a*PK_B=abG que será adicionalmente descrito abaixo, onde a, b e G podem ser multiplicados pela multiplicação de ECC.

[087]Em algumas modalidades, para satisfazer a quantia de transação t, o usuário A pode explorar um ou mais ativos de um valor agregado pelo menos t da conta A. Por exemplo, com referência à Figura 1, o nó A pode selecionar ativos A_1 e A_2 para essa transação. O nó A pode ler ativos PC(r_1, a_1) e PC(r_2, a_2) a partir do nó 1. Com os números aleatórios r_1 e r_2 conhecidos ao nó A, o nó A pode descriptografar os ativos lidos PC(r_1, a_1) e PC(r_2, a_2) para obter valores patrimoniais a_1 e a_2, para garantir que a soma de a_1 e a_2 não seja maior que a quantia de transação t. Diferentes ativos podem ser trocados entre si dentro da conta com base em várias taxas.

[088]Em algumas modalidades, a quantia do valor patrimonial selecionado superior a t, caso exista, é ajustada para y como o troco. Por exemplo, o nó A pode determinar o troco y = a_1 + a_2 - t. O nó A pode selecionar números aleatórios r_t e r_y como fatores randômicos para gerar compromissos de Pedersen para t e y: T=PC(r_t, t), Y=PC(r_y, y). Ou seja, o nó A pode gerar um número aleatório r_t para t e um número aleatório r_y para y. O nó A pode comprometer t e r_t a um esquema de compromisso (por exemplo, criptografia homomórfica) para obter um valor de compromisso T = PC(r_t, t), e comprometer y e r_y a um esquema de compromisso (por exemplo, criptografia homomórfica) para obter um valor de compromisso Y = PC(r_y, y).

[089]Ademais, em algumas modalidades, o nó A gera uma primeira chave de um par de chaves simétricas a*PK_B=abG e gera outra chave a*PK_A=aaG. O nó A

usa a primeira chave abG para criptografar (r_t||t), que proporciona uma criptografia E(abG, r_t||t), e usa a chave aaG para criptografar (r_y||y), que proporciona uma criptografia E(aaG, r_y||y). As Figuras 3A e 3B podem seguir esse exemplo. Alternativamente à obtenção da criptografia E(abG, r_t||t) pelo nó A, o usuário A pode enviar r_t e t ao nó B junto às informações de transação, induzindo o nó B a gerar uma segunda chave do par de chaves simétricas b*PK_A=baG para criptografar (r_t||t). O nó B enviaria a criptografia ao nó A para permitir que o nó A verifique. As Figuras 4A e 4B podem seguir esse exemplo. Embora concatenação seja usada em vários exemplos desta revelação, combinações alternativas de entradas, saídas, ou outros parâmetros podem ser usados para a função de criptografia ou outra operação.

[090]Ademais, em algumas modalidades, o nó A pode gerar uma prova de faixa RP para provar aos nós de blockchain se o valor de PC(r_t, t) e o valor de PC(r_y, y) são dentro de uma faixa válida. Por exemplo, para ter valores válidos de PC(r_t, t), a quantia de transação t pode estar dentro de uma faixa válida [0, 2^n-1]; e para ter valores válidos de PC(r_y, y), o troco y pode estar dentro de uma faixa valida [0, 2^n-1]. Em uma modalidade, o nó A pode usar a técnica de prova de bloco para gerar a prova de faixa RP relacionada a (r_y, y, Y, r_t, t, T) para os nós de blockchain (por exemplo, nós de consenso) para verificar em uma etapa posterior se a quantia de transação t e o troco y estão dentro da faixa válida com base na prova de faixa. A prova de faixa pode compreender, por exemplo, Bulletproofs, assinatura em anel Borromeana, etc.

[091]Na etapa 202, o nó A pode enviar as informações de transação ao nó B (por exemplo, através deum canal seguro fora do blockchain). As informações de transação enviadas podem compreender, por exemplo, valor de compromisso T=PC(r_t, t), valor de compromisso Y=PC(r_y, y), criptografia E(abG, r_t||t), criptografia E(aaG, r_y||y), prova de faixa RP, etc. O valor de compromisso Y=PC(r_y, y), criptografia E(aaG, r_y||y), e prova de faixa RP podem ser opcionais porque o nó B pode não se

importar com o troco enviado de volta à conta A. Em algumas modalidades, a transmissão através do canal de comunicação fora de blockchain pode evitar que as informações de transação sejam gravadas no blockchain e evitar que nós diferentes do nó de remetente A e do nó de destinatário B obtenham as informações de transação. E(aaG, r_y||y) pode não precisar ser enviado ao nó B, mas pode ser necessário no futuro para que o usuário A gaste o troco y visto que o troco deve ser retornado à conta A.

[092]Na etapa 203, o nó B pode verificar o número aleatório r_t, a quantia de transação t e o valor de compromisso T. Em algumas modalidades, o nó B pode gerar uma segunda chave do par de chaves simétricas b*PK_A=baG e usar a segunda chave baG para descriptografar a criptografia E(abG, r_t||t) para obter r_t||t. A partir de r_t||t, o nó B pode obter r_t e t, e, então, verificar se r_t e t correspondem a T=PC(r_t, t). Ou seja, o nó B pode verificar se o valor de compromisso T = PC(r_t, t) está correto com base no número aleatório r_t e na quantia de transação t de acordo com o algoritmo de compromisso de Pedersen. Se a correspondência/verificação falhar, o nó B pode rejeitar a transação; e se a correspondência/verificação for bem-sucedida, o nó B pode assinar a transação a responder o nó A na etapa 204.

[093]Na etapa 204, o nó B pode assinar a transação com a chave privada do usuário B SK_B para gerar uma assinatura SIGB. A assinatura pode seguir o Algoritmo de Assinatura Digital (DSA) tal como o Algoritmo de Assinatura Digital com Curvas Elípticas (ECDSA), desse modo, o destinatário da assinatura pode verificar a assinatura com a chave pública do signatário para autenticar os dados assinados. A assinatura SIGB indica que o nó de destinatário B concorda com a transação.

[094]Na etapa 205, o nó B pode transmitir a transação assinada de volta ao nó A com a assinatura SIGB.

[095]Na etapa 206, se SIGB não for verificado com sucesso, o nó A pode re-

jeitar a transação. Se SIGB for verificado com sucesso, o nó A pode assinar a transação com a chave privada do usuário A SK_A para gerar uma assinatura SIGA. De modo similar, a assinatura pode seguir o Algoritmo de Assinatura Digital (DSA). Em uma modalidade, o nó A pode assinar (E(abG, r_t||t); E(aaG, r_y||y); Y; T; RP) com a chave privada do usuário A para gerar a assinatura SIGA.

[096]Na etapa 207, o nó A pode submeter a transação ao blockchain, induzindo os nós de blockchain a verificar a transação e determinar se adiciona a transação ao blockchain. Em uma modalidade, o nó A pode submeter a transação (E(abG, r_t||t); E(aaG, r_y||y); Y; T; RP; SIGA; SIGB) ao blockchain através do nó 1 para executar a transação. A transação pode comprometer parâmetros adicionais ou pode não comprometer todos os parâmetros listados. A transação pode ser radiodifundida a um ou mais nós (por exemplo, nós de consenso) no blockchain para verificação. Se a verificação for bem-sucedida, a transação é adicionada ao blockchain. Se a verificação falhar, a transação de adição ao blockchain é rejeitada.

[097]Na etapas 208 a 213, um ou mais nós (por exemplo, nós de consenso) verificam as assinaturas, prova de faixa, e outras informações da transação submetida. Se a verificação falhar, os nós rejeitam a transação. Se a verificação for bem-sucedida, os nós aceitam a transação, atualizam a conta do usuário A e a conta do usuário B separadamente.

[098]Em algumas modalidades, para executar a transação, as informações de transação podem ser verificadas por vários nós de blockchain. As informações de transação podem compreender um endereço de transação TXID, assinaturas(s), entrada e saída. TXID pode compreender o hash do conteúdo de transação. As assinaturas podem compreender assinaturas de cripto-chave pelo remetente e destinatário. A entrada pode compreender um endereço da conta do remetente em blockchain, um ou mais ativos explorados a partir da conta de blockchain do remetente para transação, etc. A saída pode compreender um endereço da conta do destinatário em blockchain,

tipo(s) de ativos dos ativos do destinatário, valor(es) de compromisso dos ativos do destinatário, etc. A entrada e a saída podem compreender informações indexadas em uma forma tabular. Em algumas modalidades, o valor de NoteID pode ser “TXID + um índice do ativo na saída.”

[099]Em algumas modalidades, um ou mais nós do blockchain podem verificar a transação submetida (E(abG, r_t||t); E(aaG, r_y||y); Y; T; RP; SIGA; SIGB).

[0100]Na etapa 208, os nós podem verificar se a transação foi executada usando um mecanismo anti-gasto duplo ou um mecanismo anti-repetição de ataque. Se a transação tiver sido executada, os nós podem rejeitar a transação; caso contrário, o método pode proceder para a etapa 209.

[0101]Na etapa 209, os nós podem verificar as assinaturas SIGA e SIGB (por exemplo, com base na chave pública A e na chave pública B, respectivamente). Se alguma das assinaturas for incorreta, os nós podem rejeitar a transação; caso contrário, o método pode proceder para a etapa 210.

[0102]Na etapa opcional 210, os nós podem verificar se os tipos de ativos são consistentes. Por exemplo, os nós podem verificar se os tipos de ativos no NoteType para A_1 a A_2 são consistentes aos tipos de ativos da quantia de transação t. Se algum dos tipos de ativos for inconsistente, os nós podem rejeitar a transação; caso contrário, o método pode proceder para a etapa 211. Em algumas modalidades, o tipo de ativos original na carteira podem ter sido convertidos em outro tipo com base em uma taxa de troca, e essa etapa pode ser omitida.

[0103]Na etapa 211, os nós podem verificar a prova de faixa RP para validar o valor de PC(r_t, t) e o valor de PC(r_y, y). Em uma modalidade, os nós podem verificar a prova de faixa RP para verificar se a quantia de transação t não é menor que zero e o troco y não é menor que zero. Se a verificação falhar, o nós podem rejeitar a transação; caso contrário, o método pode proceder para a etapa 212.

[0104]Na etapa 212, os nós podem verificar se as entradas e as saídas da

transação são consistentes. Se a verificação falhar, os nós podem rejeitar a transação; caso contrário, o método pode proceder para a etapa 213.

[0105]Na etapa 213, os nós podem verificar se o nó A tem o(s) ativos explorados para a transação. Em uma modalidade, os nós podem realizar essa verificação com base nas informações armazenadas no blockchain, tais como informações correspondentes à conta A. As informações podem compreender informações de transações prévias de todos os ativos. Logo, os nós podem determinar se a conta A tem o ativo de transação para a transação. Se a determinação for negativa, os nós podem rejeitar a transação; caso contrário, o método pode proceder para a etapa 214.

[0106]Na etapa 214, os nós podem atualizar a conta A e a conta B. Por exemplo, os nós podem remover o ativo de transação da quantia t da conta A, e adicionar a mesma à conta B. Com base na propriedade homomórfica, visto que Y = PC(r_y, y) e o n[o 1 conhece r_y e pode avaliar o valor de compromisso Y a partir do blockchain, o nó 1 pode descriptografar Y para obter o valor patrimonial y e retornar o mesmo para a conta A. O nó 2 obtém na etapa 202 o número aleatório r_t a partir do nó 1 e pode obter a partir do blockchain o valor de compromisso T. Logo, o nó 2 pode descriptografar T para obter o valor patrimonial t e adicionar o mesmo à conta B.

[0107]Em um exemplo, após a atualização à conta A e à conta B, a conta A recebe o troco y aos ativos explorados e recebe seus ativos inexplorados. Por exemplo, os ativos explorados podem ser A_1 e A_2 que são removidos na transação com o troco y retornado à conta A, e os ativos inexplorados são A_3, ..., A_m. A conta B recebe a quantia de transação t e recebe seus ativos originais (por exemplo, B_1, ..., B_n). Os ativos na conta A e na conta B são os seguintes:

[0108]Para Conta A (conta A), ativos atualizados são denotados como:

(Y=PC(r_y, y), E(aaG, r_y||y)),

...

(A_m=PC(r_{a_m}, a_m), E(K_A, r_{a_m}||a_m))

[0109]Para Conta B (conta B), ativos atualizados são denotados como:

(B_1=PC(r_{b_1}, b_1), E(K_B, r_{b_1}||b_1)),

(B_2=PC(r_{b_2}, b_2), E(K_B, r_{b_2}||b_2)),

...

(B_n=PC(r_{b_n}, b_n), E(K_B, r_{b_n}||b_n)),

(T=PC(r_t, t), E(abG, r_t||t))

[0110]Embora esta revelação use nó A/usuário A e nó B/usuário B para ilustrar o remetente e o destinatário, respectivamente, o remetente e o destinatário podem ser o mesmo nó/usuário. Por exemplo, o troco y de uma transação (ativos explorados totais na conta A menos a quantia de transação) pode ser enviado de volta ao remetente da transação. Logo, as várias etapas realizadas pelo nó B conforme descrito no presente documento podem ser alternativamente realizados pelo nó A.

[0111]A Figura 3A ilustra um fluxograma de um método exemplificador 300 para proteção de informações, de acordo com várias modalidades da presente revelação. O método 300 pode ser implementado por um ou mais componentes (por exemplo, o nó A, nó 1, uma combinação de nó A e nó 1) do sistema 100 da Figura 1. O método 300 pode ser implementado por um sistema ou dispositivo (por exemplo, computador, servidor) que compreende um processador e uma mídia de armazenamento legível por computador não transitória (por exemplo, memória) que armazena instruções a serem executadas pelo processador para induzir o sistema ou dispositivo (por exemplo, o processador) para realizar o método 300. As operações do método 300 apresentado abaixo são destinadas a serem ilustrativas. Dependendo da implementação, o método exemplificador 300 pode incluir etapas adicionais, menos ou alternativas realizadas em várias ordens ou em paralelo.

[0112]O bloco 301 compreende: comprometer uma quantia de transação t de uma transação com um esquema de compromisso para obter um valor de compro-

misso de transação T, sendo que o esquema de compromisso compreende pelo menos um fator randômico de transação r_t. Por exemplo, conforme descrito anteriormente, T = PC(r_t, t). Em algumas modalidades, o esquema de compromisso compreende um compromisso de Pedersen com base pelo menos no fator randômico de transação r_t e com a quantia de transação t sendo um valor comprometido.

[0113]O bloco 302 compreende: gerar uma primeira chave de um par de chaves simétricas. Por exemplo, conforme descrito anteriormente, SK_A = a, PK_B = bG, e a primeira chave pode ser a*PK_B = abG. Em algumas modalidades, gerar a primeira chave e a segunda chave compreende: gerar a primeira chave e a segunda chave com base em uma chave privada SK_A de um remetente da transação e uma chave pública PK_B do destinatário sob um protocolo de troca de chave de Diffie-Hellman (DH).

[0114]O bloco 303 compreende: criptografar uma combinação (por exemplo, concatenação) do fator randômico de transação r_t e a quantia de transação t com a primeira chave. Por exemplo, conforme descrito anteriormente, o Nó A pode usar a primeira chave abG para criptografar (r_t||t), que proporciona a criptografia E(abG, r_t||t).

[0115]O bloco 304 compreende: transmitir o valor de compromisso de transação T e uma combinação criptografada a um nó de destinatário associado a um destinatário da transação para o nó de destinatário para verificar a transação. Em algumas modalidades, transmitir o valor de compromisso de transação T e a combinação criptografada ao nó de destinatário associado ao destinatário da transação para o nó de destinatário para verificar a transação compreende transmitir o valor de compromisso de transação T e a combinação criptografada ao nó de destinatário associado ao destinatário da transação, induzir o nó de destinatário a: gerar uma segunda chave do par de chaves simétricas com base em uma chave privada SK_B do destinatário e uma chave pública PK_A do remetente, descriptografar a combinação criptografada com a

segunda chave gerada pelo nó de destinatário para obter o fator randômico de transação r_t e a quantia de transação t, e verificar a transação com base pelo menos no valor de compromisso de transação T, no fator randômico de transação r_t, e na quantia de transação t. Vide, por exemplo, a Etapa 203. Por exemplo, conforme descrito anteriormente, o nó de destinatário pode gerar independentemente a segunda chave b*PK_A=baG. As chaves abG e baG são simétricas e iguais. Ou seja, o nó de destinatário pode não receber a primeira chave abG a partir do nó de remetente, e, ao invés disso, o nó de destinatário gera independentemente a segunda chave baG como um equivalente de abG.

[0116]Em algumas modalidades, induzir o nó de destinatário a verificar a transação com base pelo menos no valor de compromisso de transação T, no fator randômico de transação r_t, e na quantia de transação t compreende induzir o nó de destinatário a: em resposta à determinação que o valor de compromisso de transação T não corresponde ao esquema de compromisso da quantia de transação t com base no fator randômico de transação r_t, rejeitar a transação; e em resposta à determinação que o valor de compromisso de transação T corresponde ao esquema de compromisso da quantia de transação t com base no fator randômico de transação r_t, aprovar a transação assinando-se a transação para gerar uma assinatura de destinatário SIGB para retornar a um nó de remetente associado ao remetente.

[0117]Em algumas modalidades, antes (bloco 304) de transmitir a combinação criptografada ao nó de destinatário associado ao destinatário, o método compreende, ainda: comprometer um troco y da transação com o esquema de compromisso para obter um valor de compromisso de troco Y, sendo que o esquema de compromisso compreende pelo menos um fator randômico de troco r_y, em que o troco y é um ou mais ativos do remetente explorados para a transação menos a quantia de transação t; gerar outra chave com base em uma chave privada SK_A do remetente e na chave pública PK_A do remetente; e criptografar outra combinação do fator randômico de

troco r_y e o troco y com a outra chave. Por exemplo, conforme descrito anteriormente, Y = PC(r_y, y), PK_A =a, e nó A podem gerar uma chave a*PK_A=aaG e usar a chave aaG para criptografar (r_y||y), que proporciona uma criptografia E(aaG, r_y||y).

[0118]Em algumas modalidades, o método compreende, ainda: em resposta à recepção da assinatura de destinatário SIGB, aprovar a transação sinalizando-se a transação para gerar uma assinatura de remetente SIGA; e submeter a transação que compreende a combinação criptografada, a outra combinação criptografada, o valor de compromisso de transação T, o valor de compromisso de troco Y, a assinatura de remetente SIGA, e a assinatura de destinatário SIGB a um ou mais nós em uma rede de blockchain para um ou mais nós para verificar a transação. Maiores detalhes serão descritos acima com referência às Etapas 208 a 213.

[0119]Em algumas modalidades, submeter a transação que compreende a combinação criptografada, a outra combinação criptografada, o valor de compromisso de transação T, o valor de compromisso de troco Y, a assinatura de remetente SIGA, e a assinatura de destinatário SIGB a um ou mais nós na rede de blockchain para um ou mais nós para verificar a transação compreende: submeter a transação que compreende a combinação criptografada, a outra combinação criptografada, o valor de compromisso de transação T, o valor de compromisso de troco Y, a assinatura de remetente SIGA, e a assinatura de destinatário SIGB a um ou mais nós na rede de blockchain, induzir um ou mais nós para, em resposta à verificação bem-sucedida da transação, lançar a quantia de transação t ao destinatário, eliminar o um ou mais ativos explorados para a transação, e lançar o troco y ao remetente. Maiores detalhes são descritos acima com referência à Etapa 214.

[0120]A Figura 3B ilustra um fluxograma de um método exemplificador 400 para proteção de informações, de acordo com várias modalidades ad presente revelação. O método 400 pode ser implementado por um ou mais componentes (por exemplo, o nó B, nó 2, juma combinação de nó B e nó 2, etc.) do sistema 100 da Figura 1.

O método 400 pode ser implementado por um sistema ou dispositivo (por exemplo, computador, servidor) que compreende um processador e uma mídia de armazenamento legível por computador não transitória (por exemplo, memória) que armazena instruções a serem executadas pelo processador para induzir o sistema ou dispositivo (por exemplo, o processador) para realizar o método 400. As operações do método 400 apresentadas abaixo são destinadas a serem ilustrativas. Dependendo da implementação, o método exemplificador 400 pode incluir etapas adicionais, menos ou alternativas realizadas em várias ordens ou em paralelo.

[0121]O bloco 401 compreende: obter uma combinação de um fator randômico de transação r_t e uma quantia de transação t criptografada com uma primeira chave de um par de chaves simétricas, e obter um valor de compromisso de transação T. A quantia de transação t é comprometida com um esquema de compromisso por um nó de remetente associado a um remetente de uma transação para obter o valor de compromisso de transação T, sendo que o esquema de compromisso compreende pelo menos o fator randômico de transação r_t. Em algumas modalidades, a primeira chave é gerada pelo nó de remetente com base em uma chave privada SK_A do remetente da transação e uma chave pública PK_B de um destinatário da transação.

[0122]O bloco 402 compreende: gerar uma segunda chave do par de chaves simétricas. Em algumas modalidades, gerar a segunda chave do par de chaves simétricas compreende gerar a segunda chave do par de chaves simétricas com base em uma chave privada SK_B de um destinatário da transação e uma chave pública PK_A do remetente sob um protocolo de troca de chave de Diffie-Hellman (DH).

[0123]O bloco 403 compreende: descriptografar a combinação obtida com a segunda chave gerada por um nó de destinatário associado ao destinatário para obter o fator randômico de transação r_t e a quantia de transação t.

[0124]O bloco 404 compreende: verificar a transação com base pelo menos no valor de compromisso de transação T, no fator randômico de transação r_t, e na

quantia de transação t.

[0125]Alternativamente à criptografia, a combinação (r_t, t) tal como (r_t||t) no nó A, o nó A pode transmitir (r_t, t) ao nó B, induzir o nó B a criptografar a combinação (r_t, t), conforme descrito abaixo com referência às Figuras 4A e 4B. Outras etapas e descrições das Figuras 1 a 3B podem aplicar similarmente à Figuras 4A e 4B.

[0126]A Figura 4A ilustra um fluxograma de um método exemplificador 440 para proteção de informações, de acordo com várias modalidades da presente revelação. O método 440 pode ser implementado por um ou mais componentes (por exemplo, o nó A, nó 1, uma combinação do nó A e nó 1) do sistema 100 da Figura 1. O método 440 pode ser implementado por um sistema ou dispositivo (por exemplo, computador, servidor) que compreende um processador e uma mídia de armazenamento legível por computador não transitória (por exemplo, memória) que armazena instruções a serem executadas pelo processador para induzir o sistema ou dispositivo (por exemplo, o processador) para realizar o método 440. As operações do método 440 apresentado abaixo são destinadas a serem ilustrativas. Dependendo da implementação, o método exemplificador 440 pode incluir etapas adicionais, menos ou alternativas realizadas em várias ordens ou em paralelo.

[0127]Bloco 441 compreende: comprometer uma quantia de transação t de uma transação com um esquema de compromisso para obter um valor de compromisso de transação T, sendo que o esquema de compromisso compreende pelo menos a fator randômico de transação r_t.

[0128]O bloco 442 compreende: enviar a quantia de transação t, o fator randômico de transação r_t, e o valor de compromisso de transação T a um nó de destinatário associado a um destinatário da transação para o nó de destinatário para verificar a transação e criptografar o fator randômico de transação r_t e a quantia de transação t com uma segunda chave de um par de chaves simétricas. Por exemplo, o nó B pode verificar se T=PC(r_t, t), e o nó B pode criptografar a combinação com a chave

baG para obter E(baG, r_t||t).

[0129]O bloco 443 compreende: obter uma combinação criptografada (por exemplo, E(baG, r_t||t)) do fator randômico de transação r_t e a quantia de transação t a partir do nó de destinatário.

[0130]O bloco 444 compreende: gerar uma primeira chave do par de chaves simétricas para descriptografar a combinação criptografada para verificar a transação. Por exemplo, o nó A pode gerar a primeira chave abG para descriptografar E(baG, r_t||t) e verificar se r_t e t estão corretos. Uma vez que r_t e t são mutuamente verificados pelos nós de remetente e destinatário, a transação pode ser submetida à blockchain para verificação.

[0131]A Figura 4B ilustra um fluxograma de um método exemplificador 450 para proteção de informações, de acordo com várias modalidades da presente revelação. O método 450 pode ser implementado por um ou mais componentes (por exemplo, o nó B, nó 2, uma combinação de nó B e nó 2, etc.) do sistema 100 da Figura 1. O método 450 pode ser implementado por um sistema ou dispositivo (por exemplo, computador, servidor) que compreende um processador e uma mídia de armazenamento legível por computador não transitória (por exemplo, ,memória) que armazena instruções a serem executadas pelo processador para induzir o sistema ou dispositivo (por exemplo, o processador) para realizar o método 450. As operações do método 450 apresentado abaixo são destinadas a serem ilustrativas. Dependendo da implementação, o método exemplificador 450 pode incluir etapas adicionais, menos ou alternativas realizadas em várias ordens ou em paralelo.

[0132]O bloco 451 compreende: obter uma quantia de transação t de uma transação, um fator randômico de transação r_t, e um valor de compromisso de transação T.

[0133]O bloco 452 compreende: verificar a transação com base na quantia de

transação obtida t, no fator randômico de transação obtido r_t, e no valor de compromisso de transação obtido T.

[0134]O bloco 453 compreende: em resposta à verificar com sucesso a transação, criptografar o fator randômico de transação r_t e a quantia de transação t com uma segunda chave de um par de chaves simétricas para obter uma combinação criptografada (por exemplo, E(baG, r_t||t)).

[0135]O bloco 454 compreende: transmitir a combinação criptografada a um nó de remetente associado a um remetente da transação.

[0136]Conforme mostrado, a privacidade para a quantia de transação pode ser protegida através de vários aperfeiçoamentos da tecnologia da computação. Por exemplo, a estrutura de conta compreende um ou mais campos, tal como um primeiro campo associado ao compromisso de Pedersen do valor patrimonial (por exemplo, o primeiro campo sendo PC(r_{a_i}, a_i), com i estando entre 1 e m) e um segundo campo associado ao número aleatório para o compromisso de Pedersen e o valor patrimonial (por exemplo, o segundo campo sendo E(...)). O primeiro e segundo campos também são usados nas etapas de transação e armazenados em blockchain.

[0137]Para outro exemplo, uma chave simétrica é usada para criptografar o número aleatório de cada compromisso de Pedersen e o valor patrimonial correspondente, e armazenar a transação incluindo os números aleatórios criptografados e valores patrimoniais no blockchain. Essa maneira evita que o gerenciamento local desses números aleatórios e promove segurança com base no armazenamento de blockchain distribuído e consistente.

[0138]Ademais, sob o protocolo de troca de chave DH ou um protocolo alternativo, mesmo sem comunicação direta, o usuário A e o usuário B compartilham um segredo comum (o par de chaves simétricas abG e baG) para criptografar/descriptografar o número aleatório do compromisso e o valor patrimonial. Visto que o par de

chaves simétricas é obtido a partir do par de chave pública-privada das contas correspondentes, o número aleatório para o compromisso pode ser efetivamente armazenado através do blockchain, sem adicionar adicionalmente uma chave de criptografia.

[0139]Ainda em outro exemplo, a prova de faixa é usada para provar que os ativos preexistentes da transação são equilibrados em relação a novos ativos e à transação, e que o valor de cada novo ativo se encontra em uma faixa razoável. Ademais, as partes de transação podem transmitir o número aleatório comprometido e o valor do novo ativo ao destinatário través de um canal fora de blockchain seguro para verificar se o valor comprometido correspondente ao valor do ativo de transação.

[0140]Como tal, números aleatórios de compromissos de Pedersen podem ser convenientemente gerenciados, sem o risco de corrupção e sem efetuar um encargo de gerenciamento de chave adicional. Logo, a privacidade de transação pode ser minunciosamente protegida, e as quantias de transação podem ser mantidas como secretas.

[0141]As técnicas descritas no presente documento são implementadas por um ou mais dispositivos computacionais para propósitos especiais. Os dispositivos computacionais para propósitos especiais podem ser sistemas computacionais desktop, sistemas computacionais de servidor, sistemas computacionais portáteis, dispositivos de mão, dispositivos de rede ou qualquer outro dispositivo ou combinação de dispositivos que incorporam uma lógica cabeada e/ou lógica de programa para implementar as técnicas. O(s)s dispositivo(s) computacional(is) é(são) geralmente controlado(s) e coordenado(s) operando-se um software de sistema. Os sistemas operacionais convencionais controlar e agendam processos computacionais para execução, realizam gerenciamento de memória, proporcionam sistema de arquivo, rede, serviços I/O, e proporcionam uma funcionalidade de interface de usuário, tal como uma interface gráfica de usuário (“GUI”), dentre outras coisas.

[0142]A Figura 5 é um diagrama de blocos que ilustra um sistema computacional 500 mediante o qual qualquer uma das modalidades descritas no presente documento pode ser implementada. O sistema 500 pode ser implementado em qualquer um dos nós descritos no presente documento e configurados para realizar etapas correspondentes para métodos de proteção de informações. O sistema computacional 500 inclui um barramento 502 ou outro mecanismo de comunicação para comunicar informações, um ou mais processadores de hardware 504 acoplados ao barramento 502 para processar informações. Os processadores de hardware 504 podem ser, por exemplo, um ou mais microprocessadores para propósitos gerais.

[0143]O sistema computacional 500 também inclui uma memória principal 506, tal como uma memória de acesso aleatório (RAM), cache e/ou outros dispositivos de armazenamento dinâmico, acoplados ao barramento 502 para armazenar informações e instruções a serem executadas pelos processadores 504. A memória principal 506 também pode ser usada para armazenar variáveis temporárias ou outras informações intermediárias durante a execução de instruções a serem executadas por processadores 504. Essas instruções, quando armazenadas em mídia de armazenamento acessíveis a processadores 504, renderizam o sistema computacional 500 em uma máquina para propósitos especiais que seja customizada para realizar as operações especificadas nas instruções. O sistema computacional 500 inclui, ainda, uma memória somente para leitura (ROM) 508 ou outro dispositivo de armazenamento estático acoplado ao barramento 502 para armazenar informações estáticas e instruções para processadores 504. Um dispositivo de armazenamento 510, tal como um disco magnético, disco óptico, ou pendrive USB (unidade Flash), etc., é proporcionado e acoplado ao barramento 502 para armazenar informações e instruções.

[0144]O sistema computacional 500 pode implementar as técnicas descritas no presente documento usando uma lógica cabeada customizada, um ou mais ASICs ou FPGAs, firmware e/ou lógica de programa que, em combinação com o sistema

computacional, induz ou programa o sistema computacional 500 a ser uma máquina para propósitos especiais. De acordo com uma modalidade, as operações, métodos e processos descritos no presente documento são realizados pelo sistema computacional 500 em resposta aos processadores 504 executando 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 outra mídia de armazenamento, tal como um dispositivo de armazenamento 510. A execução das sequências de instruções contidas na memória principal 506 induz os processadores 504 a realizar as etapas de processo descritas no presente documento. Em modalidades alternativas, um conjunto de circuitos cabeados pode ser usado ao invés ou em combinação com instruções de software.

[0145]A memória principal 506, a ROM 508, e/ou o armazenamento 510 podem incluir uma mídia de armazenamento não transitória. O termo “mídia não transitória,” e termos similares, conforme o uso em questão se refere à mídia que armazena dados e/ou instruções que induze uma máquina a operarem de forma específica, a mídia exclui sinais transitórios. Essa mídia não transitória pode compreender uma mídia não volátil e/ou mídia volátil. A mídia não volátil inclui, por exemplo, discos ópticos ou magnéticos, como o dispositivo de armazenamento 510. A mídia volátil inclui uma memória dinâmica, tal como uma memória principal 506. As formas comuns de mídia não transitória incluem, por exemplo, um disquete flexível, um disco flexível, um disco rígido, uma unidade em estado sólido, fita magnética, ou quaisquer outras mídias de armazenamento de dados magnéticos, uma CD-ROM, qualquer outra mídia de armazenamento de dados ópticos, qualquer mídia física com padrões de furos, uma RAM, uma PROM, e EPROM, uma FLASH-EPROM, NVRAM, qualquer outro chip de memória ou cartucho, e versões em rede das mesmas.

[0146]O sistema computacional 500 também inclui uma interface de rede 518 acoplada ao barramento 502. A interface de rede 518 proporciona uma comunicação

de dados bidirecional que se acopla a um ou mais links de rede que são conectados a uma ou mais redes locais. Por exemplo, a interface de rede 518 pode ser um cartão de rede digital de serviços integrados (ISDN), modem via cabo, modem via satélite, ou um modem para proporcionar uma conexão de comunicação de dados a um tipo correspondente de linha telefônica. Como outro exemplo, a interface de rede 518 pode ser um cartão de rede de área local (LAN) para proporcionar uma conexão de comunicação de dados a uma LAN compatível (ou componente WAN para se comunicar com uma WAN). Os links sem fio também podem ser implementados. Em qualquer uma dessas implementações, a interface de rede 518 envia e recebe sinais elétricos, eletromagnéticos ou ópticos que porta fluxos de dados digitais que representam vários tipos de informações.

[0147]O sistema computacional 500 pode enviar mensagens e receber dados, incluindo um código de programa, através das redes, link de rede e interface de rede 518. No exemplo da Internet, um servidor pode transmitir um código solicitado para um programa de aplicativo através da Internet, o ISP, a rede local e a interface de rede 518.

[0148]O código recebido pode ser executado pelos processadores 504 à medida que é recebido, e/ou armazenado no dispositivo de armazenamento 510, ou outro armazenamento não volátil para execução posterior.

[0149]Cada um dos processos, métodos e algoritmos descritos nas seções anteriores pode ser incorporado a, e total ou parcialmente automatizado por, módulos de código executados por um ou mais sistemas computacionais ou processadores computacionais que compreendem hardware computacional. Os processos e algoritmos podem ser implementados parcial ou totalmente em um conjunto de circuitos para aplicação específica.

[0150]Os vários recursos e processos descritos anteriormente podem ser usados independentemente entre si, ou podem ser combinados de várias formas. Todas

as combinações e subcombinações possíveis são destinadas a se enquadrarem no escopo desta revelação. Além disso, determinados blocos de método ou processo podem ser omitidos em algumas implementações. Os métodos e processos descritos no presente documento também não são limitados a qualquer sequência particular, e os blocos ou estados relacionados a mesmo podem ser realizados em outras sequências que sejam apropriadas. Por exemplo, os blocos ou estados descritos podem ser realizados em uma ordem diferente daquela especificamente revelada, ou múltiplos blocos ou estados podem ser combinados em um único bloco ou estado. Os blocos ou estados exemplificadores podem ser realizados em série, em paralelo, ou de alguma outra forma. Os blocos ou estados podem ser adicionados ou removidos das modalidades exemplificadoras reveladas. Os sistemas e componentes exemplificadores descritos no presente documento podem ser configurados diferentemente dos descritos. Por exemplo, elementos podem ser adicionados, removidos, ou rearranjados comparados às modalidades exemplificadoras reveladas.

[0151]As várias operações de métodos exemplificadores descritos no presente documento podem ser realizadas, pelo menos parcialmente, por um algoritmo. O algoritmo pode ser composto em códigos de programa ou instruções armazenadas em uma memória (por exemplo, uma mídia de armazenamento legível por computador não transitória descrita anteriormente). Esse algoritmo pode compreender um algoritmo de aprendizagem por máquina. Em algumas modalidades, um algoritmo de aprendizagem por máquina pode não programar explicitamente computadores para realizar uma função, mas pode aprender a partir dos dados de treinamento para produzir um modelo de previsões que realiza a função.

[0152]As várias operações de métodos exemplificadores descritos no presente documento podem ser realizadas, pelo menos parcialmente, por um ou mais processadores que são temporariamente configurados (por exemplo, por software) ou

permanentemente configurados para realizar as operações relevantes. Sejam temporárias ou permanentemente configurados, esses processadores podem constituir mecanismos implementados por processador que operam para realizar uma ou mais operações ou funções descritas no presente documento.

[0153]De modo similar, os métodos descritos no presente documento 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 mecanismos implementados por processador. Ademais, um ou mis 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 exemplo de máquinas incluindo processadores), com essas operações sendo acessíveis através de uma rede (por exemplo, a Internet) e através de uma ou mais interfaces apropriadas (por exemplo, uma Interface de Programa de Aplicativo (API)).

[0154]O desempenho de determinadas operações pode ser distribuído dentre os processadores, não somente residindo em uma máquina simples, mas implantadas por uma série de máquinas. Em algumas modalidades exemplificadoras, os processadores ou mecanismos implementados por processador podem estar situados em uma localização geográfica única (por exemplo, dentro de um ambiente doméstico, um ambiente empresarial, ou uma fazenda de servidores). Em outras modalidades exemplificadoras, os processadores ou mecanismos implementados por processador podem ser distribuídos por uma série de localizações geográficas.

[0155]Ao longo deste relatório descritivo, várias instâncias podem implementar componentes, operações ou estruturas descritas como uma instância única. 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 requer que as operações sejam realizadas na ordem ilustrada. As estruturas e funcionalidade apresentadas como componentes separados em configurações exemplificadoras podem ser implementadas como uma estrutura ou componente combinados. De modo similar, estruturas e funcionalidade apresentadas como um componente único podem ser implementadas como componentes separados. Essas e outras variações, modificações, adições, e aperfeiçoamentos se enquadram no escopo da matéria em questão.

[0156]Muito embora uma visão geral da matéria tenha sido descrita com referências às modalidades exemplificadoras específicas, várias modificações e alterações podem ser feitas a essas modalidades sem divergir do escopo mais amplo das modalidades da presente revelação. Essas modalidades da matéria podem ser referidas no presente documento, individual ou coletivamente, pelo termo “invenção” meramente por conveniência e sem a intenção de limitar voluntariamente o escopo deste pedido a nenhuma revelação ou conceito único se mais de um for, de fato, revelado. A Descrição Detalhada não deve ser tomada em um sentido limitativo, e o escopo de várias modalidades é definido somente pelas reivindicações anexas, junto à gama completa de equivalentes aos quais essas reivindicações são concedidas.

REIVINDICAÇÕES

1. Método implementado por computador para proteção de informações, **CARACTERIZADO** pelo fato de que compreende:

comprometer uma quantia de transação t de uma transação com um esquema de compromisso para obter um valor de compromisso de transação T, sendo que o esquema de compromisso compreende pelo menos a fator randômico de transação r_t;

gerar uma primeira chave de um par de chaves simétricas;

criptografar uma combinação do fator randômico de transação r_t e a quantia de transação t com a primeira chave; e

transmitir o valor de compromisso de transação T e a combinação criptografada a um nó de destinatário associado a um destinatário da transação para o nó de destinatário para verificar a transação.

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que gerar a primeira chave compreende: gerar a primeira chave com base em uma chave privada SK_A de um remetente da transação e uma chave pública PK_B do destinatário sob um protocolo de troca de chave de Diffie-Hellman (DH).

3. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que: o esquema de compromisso compreende um compromisso de Pedersen com base pelo menos no fator randômico de transação r_t e com a quantia de transação t sendo um valor comprometido.

4. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que: a combinação do fator randômico de transação r_t e a quantia de transação t compreendem uma concatenação do fator randômico de transação r_t e da quantia de transação t.

5. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que transmitir o valor de compromisso de transação T e a combinação criptografada

ao nó de destinatário associado ao destinatário da transação para o nó de destinatário para verificar a transação compreende transmitir o valor de compromisso de transação T e a combinação criptografada ao nó de destinatário associado ao destinatário da transação, induzindo o nó de destinatário a:

gerar uma segunda chave do par de chaves simétricas com base em uma chave privada SK_B do destinatário e uma chave pública PK_A de um remetente da transação;

descriptografar a combinação criptografada com a segunda chave gerada pelo nó de destinatário para obter o fator randômico de transação r_t e a quantia de transação t; e

verificar a transação com base pelo menos no valor de compromisso de transação T, no fator randômico de transação r_t, e na quantia de transação t.

6. Método, de acordo com a reivindicação 5, **CARACTERIZADO** pelo fato de que induzir o nó de destinatário a verificar a transação com base pelo menos no valor de compromisso de transação T, no fator randômico de transação r_t, e na quantia de transação t compreende induzir o nó de destinatário a:

em resposta à determinação que o valor de compromisso de transação T não correspondente ao esquema de compromisso da quantia de transação t com base no fator randômico de transação r_t, rejeitar a transação; e

em resposta à determinação que o valor de compromisso de transação T correspondente ao esquema de compromisso da quantia de transação t com base no fator randômico de transação r_t, aprovar a transação assinando-se a transação para gerar uma assinatura de destinatário SIGB para retornar a um nó de remetente associado ao remetente.

7. Método, de acordo com a reivindicação 6, antes de transmitir a combinação criptografada ao nó de destinatário associado ao destinatário, **CARACTERIZADO** pelo fato de que compreende, ainda:

comprometer um troco y da transação com o esquema de compromisso para obter um valor de compromisso de troco Y, sendo que o esquema de compromisso compreende pelo menos um fator randômico de troco r_y, em que o troco y é um ou mais ativo s do remetente explorados para a transação menos a quantia de transação t;

gerar outra chave com base em uma chave privada SK_A do remetente e na chave pública PK_A do remetente; e

criptografar outra combinação do fator randômico de troco r_y e do troco y com a outra chave.

8. Método, de acordo com a reivindicação 7, **CARACTERIZADO** pelo fato de que compreende, ainda:

em resposta à recepção da assinatura de destinatário SIGB, aprovar a transação assinando-se a transação para gerar uma assinatura de remetente SIGA; e

submeter a transação que compreende a combinação criptografada, a outra combinação criptografada, o valor de compromisso de transação T, o valor de compromisso de troco Y, a assinatura de remetente SIGA, e a assinatura de destinatário SIGB a um ou mais nós e uma rede de blockchain para um ou mais nós para verificar a transação.

9. Método, de acordo com a reivindicação 8, **CARACTERIZADO** pelo fato de que submeter a transação que compreende a combinação criptografada, a outra combinação criptografada, o valor de compromisso de transação T, o valor de compromisso de troco Y, a assinatura de remetente SIGA, e a assinatura de destinatário SIGB a um ou mais nós na rede de blockchain para um ou mais nós para verificar a transação compreende:

submeter a transação que compreende a combinação criptografada, a outra combinação criptografada, o valor de compromisso de transação T, o valor de compromisso de troco Y, a assinatura de remetente SIGA, e a assinatura de destinatário

SIGB a um ou mais nós na rede de blockchain, induzir um ou mais nós a, em resposta à verificação bem-sucedida da transação, lançar a quantia de transação t ao destinatário, eliminar um ou mais ativos explorados para a transação, e lançar o troco y ao remetente.

10. Mídia de armazenamento legível por computador não transitória, **CARACTERIZADA** pelo fato de que armazena instruções a serem executadas por um processador para induzir o processador a realizar operações que compreendem:

comprometer uma quantia de transação t de uma transação com um esquema de compromisso para obter um valor de compromisso de transação T, sendo que o esquema de compromisso compreende pelo menos um fator randômico de transação r_t;

gerar uma primeira chave de um par de chaves simétricas;

criptografar uma combinação do fator randômico de transação r_t e a quantia de transação t com a primeira chave; e

transmitir o valor de compromisso de transação T e a combinação criptografada a um nó de destinatário associado a um destinatário da transação para o nó de destinatário para verificar a transação.

11. Mídia de armazenamento, de acordo com a reivindicação 10, **CARACTERIZADA** pelo fato de que gerar a primeira chave compreende: gerar a primeira chave com base em uma chave privada SK_A de um remetente da transação e uma chave pública PK_B do destinatário sob um protocolo de troca de chave de Diffie-Hellman (DH).

12. Mídia de armazenamento, de acordo com a reivindicação 10, **CARACTERIZADA** pelo fato de que: o esquema de compromisso compreende um compromisso de Pedersen com base pelo menos no fator randômico de transação r_t e com a quantia de transação t sendo um valor comprometido.

13. Mídia de armazenamento, de acordo com a reivindicação 10,

CARACTERIZADA pelo fato de que: a combinação do fator randômico de transação r_t e a quantia de transação t compreendem uma concatenação do fator randômico de transação r_t e da quantia de transação t.

14. Mídia de armazenamento, de acordo com a reivindicação 10, **CARACTERIZADA** pelo fato de que transmitir o valor de compromisso de transação T e a combinação criptografada ao nó de destinatário associado ao destinatário da transação para o nó de destinatário para verificar a transação compreende transmitir o valor de compromisso de transação T e a combinação criptografada ao nó de destinatário associado ao destinatário da transação, induzi o nó de destinatário a:

gerar uma segunda chave do par de chaves simétricas com base em uma chave privada SK_B do destinatário e uma chave pública PK_A de um remetente da transação;

descriptografar a combinação criptografada com a segunda chave gerada pelo nó de destinatário para obter o fator randômico de transação r_t e a quantia de transação t; e

verificar a transação com base pelo menos no valor de compromisso de transação T, no fator randômico de transação r_t, e na quantia de transação t.

15. Mídia de armazenamento, de acordo com a reivindicação 14, **CARACTERIZADA** pelo fato de que induzir o nó de destinatário a verificar a transação com base pelo menos no valor de compromisso de transação T, no fator randômico de transação r_t, e na quantia de transação t compreende induzir o nó de destinatário a:

em resposta à determinação que o valor de compromisso de transação T não corresponde ao esquema de compromisso da quantia de transação t com base no fator randômico de transação r_t, rejeitar a transação; e

em resposta à determinação que o valor de compromisso de transação T corresponde ao esquema de compromisso d aquantia de transação t com base no fator

randômico de transação r_t, aprovar a transação assinando-se a transação para gerar uma assinatura de destinatário SIGB para retornar a um nó de remetente associado ao remetente.

16. Mídia de armazenamento, de acordo com a reivindicação 15, **CARACTERIZADA** pelo fato de que antes de transmitir a combinação criptografada ao nó de destinatário associado ao destinatário, as operações compreendem, ainda:

comprometer um troco y da transação ao esquema de compromisso para obter um valor de compromisso de troco Y, sendo que o esquema de compromisso compreende pelo menos um fator randômico de troco r_y, em que o troco y é um ou mais ativos do remetente explorados para a transação menos a quantia de transação t;

gerar outra chave com base em uma chave privada SK_A do remetente e na chave pública PK_A do remetente; e

criptografar outra combinação do fator randômico de troco r_y e troco y com a outra chave.

17. Mídia de armazenamento, de acordo com a reivindicação 16, **CARACTERIZADA** pelo fato de que as operações compreendem, ainda:

em resposta à recepção da assinatura de destinatário SIGB, aprovar a transação assinando-se a transação para gerar uma assinatura de remetente SIGA; e

submeter a transação que compreende a combinação criptografada, a outra combinação criptografada, o valor de compromisso de transação T, o valor de compromisso de troco Y, a assinatura de remetente SIGA, e a assinatura de destinatário SIGB a um ou mais nós em uma rede de blockchain para um ou mais nós para verificar a transação.

18. Mídia de armazenamento, de acordo com a reivindicação 17, **CARACTERIZADA** pelo fato de que submeter a transação compreende a combinação criptografada, a outra combinação criptografada, o valor de compromisso de transa-

ção T, o valor de compromisso de troco Y, a assinatura de remetente SIGA, e a assinatura de destinatário SIGB a um ou mais nós na rede de blockchain para um ou mais nós para verificar a transação compreende:

submeter a transação que compreende a combinação criptografada, a outra combinação criptografada, o valor de compromisso de transação T, o valor de compromisso de troco Y, a assinatura de remetente SIGA, e a assinatura de destinatário SIGB a um ou mais nós na rede de blockchain, induzir um ou mais nós a, em resposta à verificação bem-sucedida da transação, lançar a quantia de transação t ao destinatário, eliminar um ou mais ativos explorados para a transação, e lançar o troco y ao remetente.

19. Sistema para proteção de informações, **CARACTERIZADO** pelo fato de que compreende um processador e uma mídia de armazenamento legível por computador não transitória acoplada ao processador, sendo que a mídia de armazenamento armazena instruções a serem executadas pelo processador para induzir o sistema a realizar operações compreende:

comprometer uma quantia de transação t de uma transação com um esquema de compromisso para obter um valor de compromisso de transação T, sendo que o esquema de compromisso compreende pelo menos um fator randômico de transação r_t;

gerar uma primeira chave de um par de chaves simétricas;

criptografar uma combinação do fator randômico de transação r_t e a quantia de transação t com a primeira chave; e

transmitir o valor de compromisso de transação T e a combinação criptografada a um nó de destinatário associado a um destinatário da transação para o nó de destinatário para verificar a transação.

20. Método implementado por computador para proteção de informações, **CARACTERIZADO** pelo fato de que compreende:

obter uma combinação de um fator randômico de transação r_t e uma quantia de transação t criptografada com uma primeira chave de um par de chaves simétricas, e obter um valor de compromisso de transação T, em que: a quantia de transação t é comprometida com um esquema de compromisso por um nó de remetente associado a um remetente de uma transação para obter o valor de compromisso de transação T, sendo que o esquema de compromisso compreende pelo menos o fator randômico de transação r_t;

gerar uma segunda chave do par de chaves simétricas;

descriptografar a combinação obtida com a segunda chave gerada por um nó de destinatário associado a um destinatário da transação para obter o fator randômico de transação r_t e a quantia de transação t; e

verificar a transação com base pelo menos no valor de compromisso de transação T, no fator randômico de transação r_t, e na quantia de transação t.

21. Método, de acordo com a reivindicação 20, **CARACTERIZADO** pelo fato de que:

gerar a segunda chave do par de chaves simétricas compreende gerar a segunda chave do par de chaves simétricas com base em uma chave privada SK_B do destinatário e uma chave pública PK_A do remetente sob um protocolo de troca de chave de Diffie-Hellman (DH); e

o esquema de compromisso compreende um compromisso de Pedersen com base pelo menos no fator randômico de transação r_t e com a quantia de transação t sendo um valor comprometido.

22. Mídia de armazenamento legível por computador não transitória, **CARACTERIZADA** pelo fato de que armazena instruções a serem executadas por um processador para induzir o processador a realizar operações que compreendem:

obter uma combinação de um fator randômico de transação r_t e uma quantia de transação t criptografada com uma primeira chave de um par de chaves simétricas,

e obter um valor de compromisso de transação T, em que: a quantia de transação t é comprometida com um esquema de compromisso por um nó de remetente associado a um remetente de uma transação para obter o valor de compromisso de transação T, sendo que o esquema de compromisso compreende pelo menos o fator randômico de transação r_t;

gerar uma segunda chave do par de chaves simétricas;

descriptografar a combinação obtida com a segunda chave gerada por um nó de destinatário associado a um destinatário da transação para obter o fator randômico de transação r_t e a quantia de transação t; e

verificar a transação com base pelo menos no valor de compromisso de transação T, no fator randômico de transação r_t, e na quantia de transação t.

23. Sistema para proteção de informações, **CARACTERIZADO** pelo fato de que compreende um processador e uma mídia de armazenamento legível por computador não transitória acoplada ao processador, sendo que a mídia de armazenamento armazena instruções a serem executadas pelo processador para induzir o sistema a realizar operações compreende:

obter uma combinação de um fator randômico de transação r_t e uma quantia de transação t criptografada com uma primeira chave de um par de chaves simétricas, e obter um valor de compromisso de transação T, em que: a quantia de transação t é comprometida com um esquema de compromisso por um nó de remetente associado a um remetente de uma transação para obter o valor de compromisso de transação T, sendo que o esquema de compromisso compreende pelo menos o fator randômico de transação r_t;

gerar uma segunda chave do par de chaves simétricas;

descriptografar a combinação obtida com a segunda chave gerada por um nó de destinatário associado a um destinatário da transação para obter o fator randômico de transação r_t e a quantia de transação t; e

verificar a transação com base pelo menos no valor de compromisso de transação T, no fator randômico de transação r_t, e na quantia de transação t.

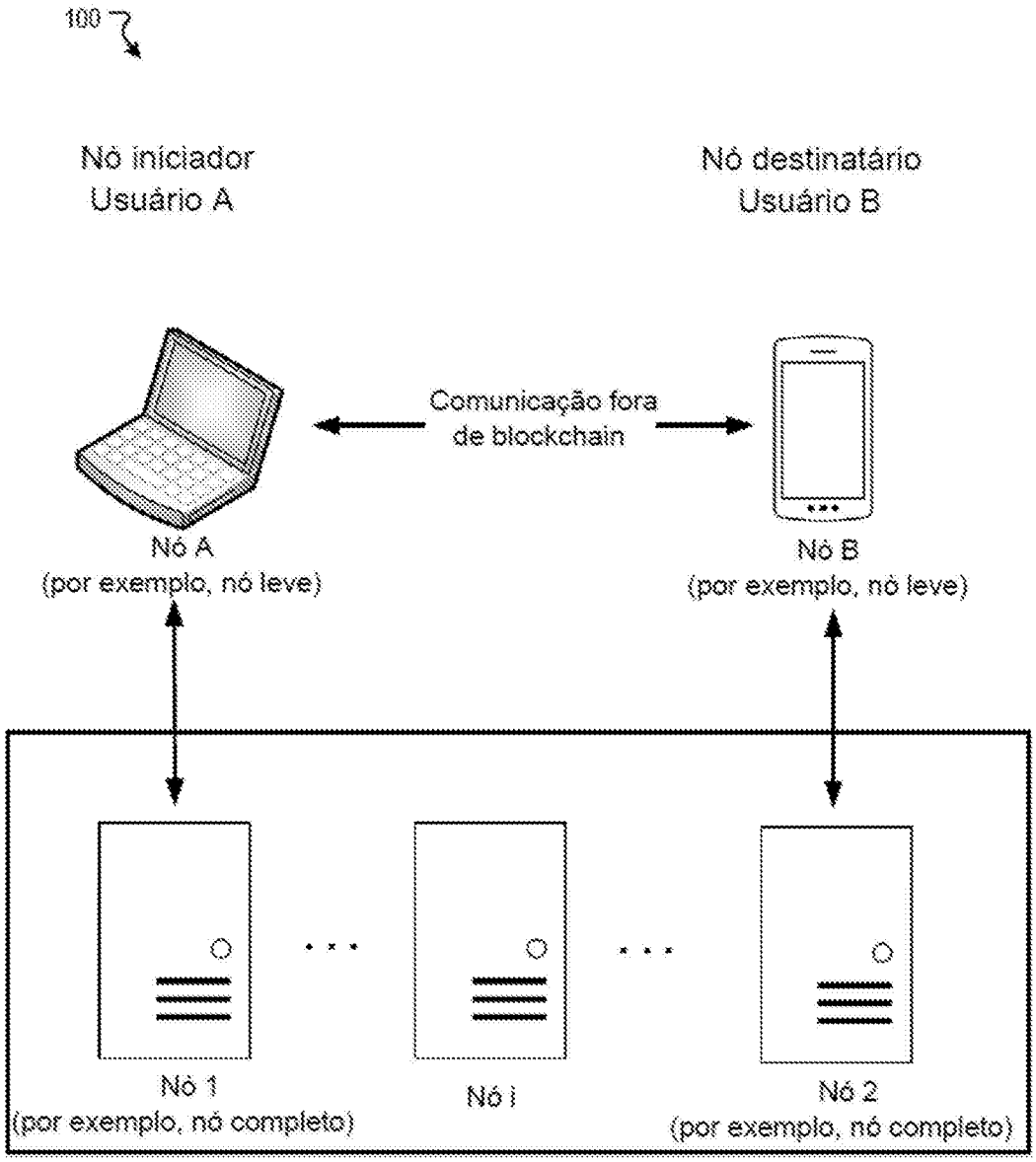

100
Nó iniciador
Usuário A
Nó destinatário
Usuário B
Comunicação fora
de blockchain
Nó A
(por exemplo, nó leve)
Nó B
(por exemplo, nó leve)
Nó 1
(por exemplo, nó completo)
Nó i
Nó 2
(por exemplo, nó completo)

FIG. 1

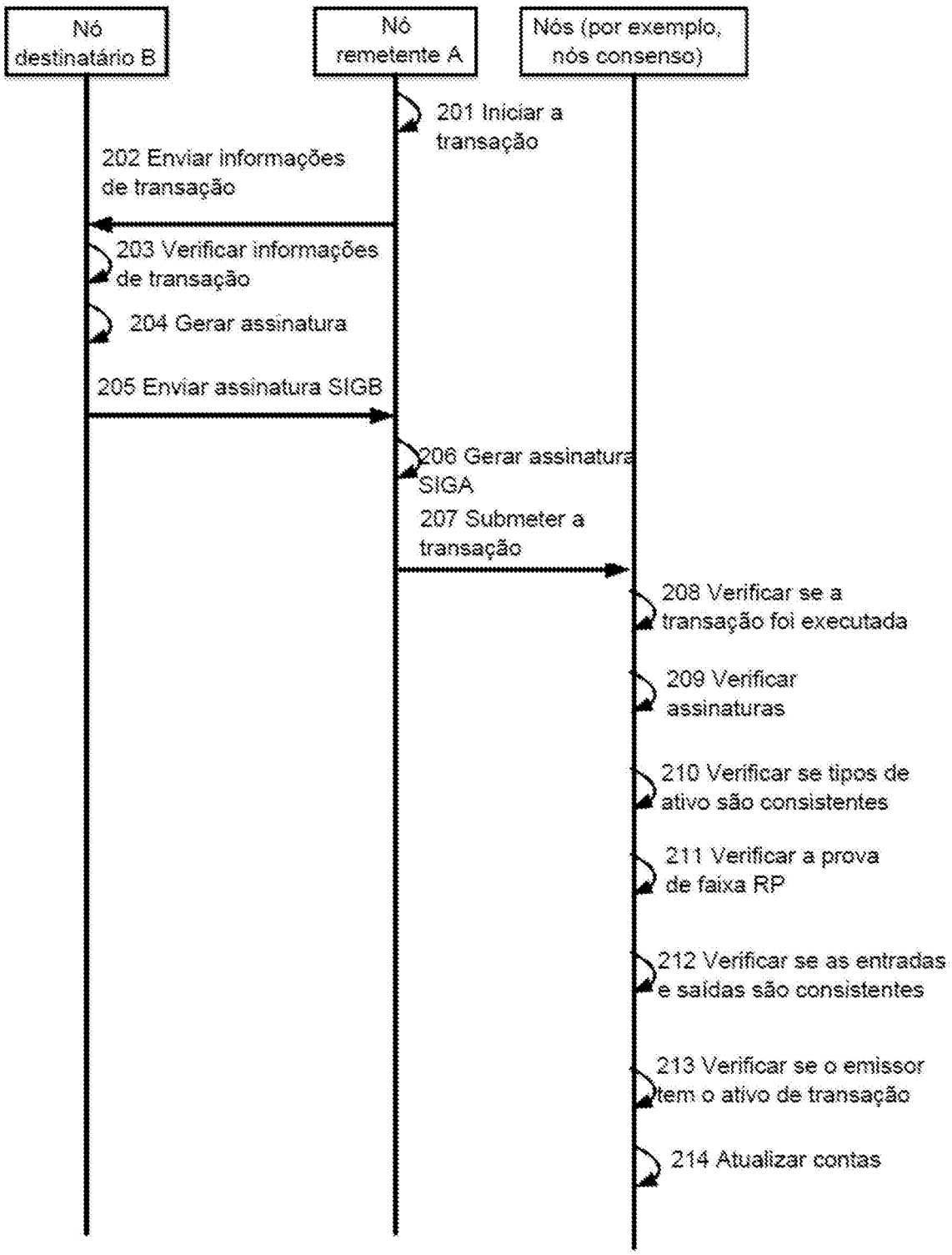

Nó destinatário B
Nó remetente A
Nós (por exemplo, nós consenso)
201 Iniciar a transação
202 Enviar informações de transação
203 Verificar informações de transação
204 Gerar assinatura
205 Enviar assinatura SIGB
206 Gerar assinatura SIGA
207 Submeter a transação
208 Verificar se a transação foi executada
209 Verificar assinaturas
210 Verificar se tipos de ativo são consistentes
211 Verificar a prova de faixa RP
212 Verificar se as entradas e saídas são consistentes
213 Verificar se o emissor tem o ativo de transação
214 Atualizar contas

FIG. 2

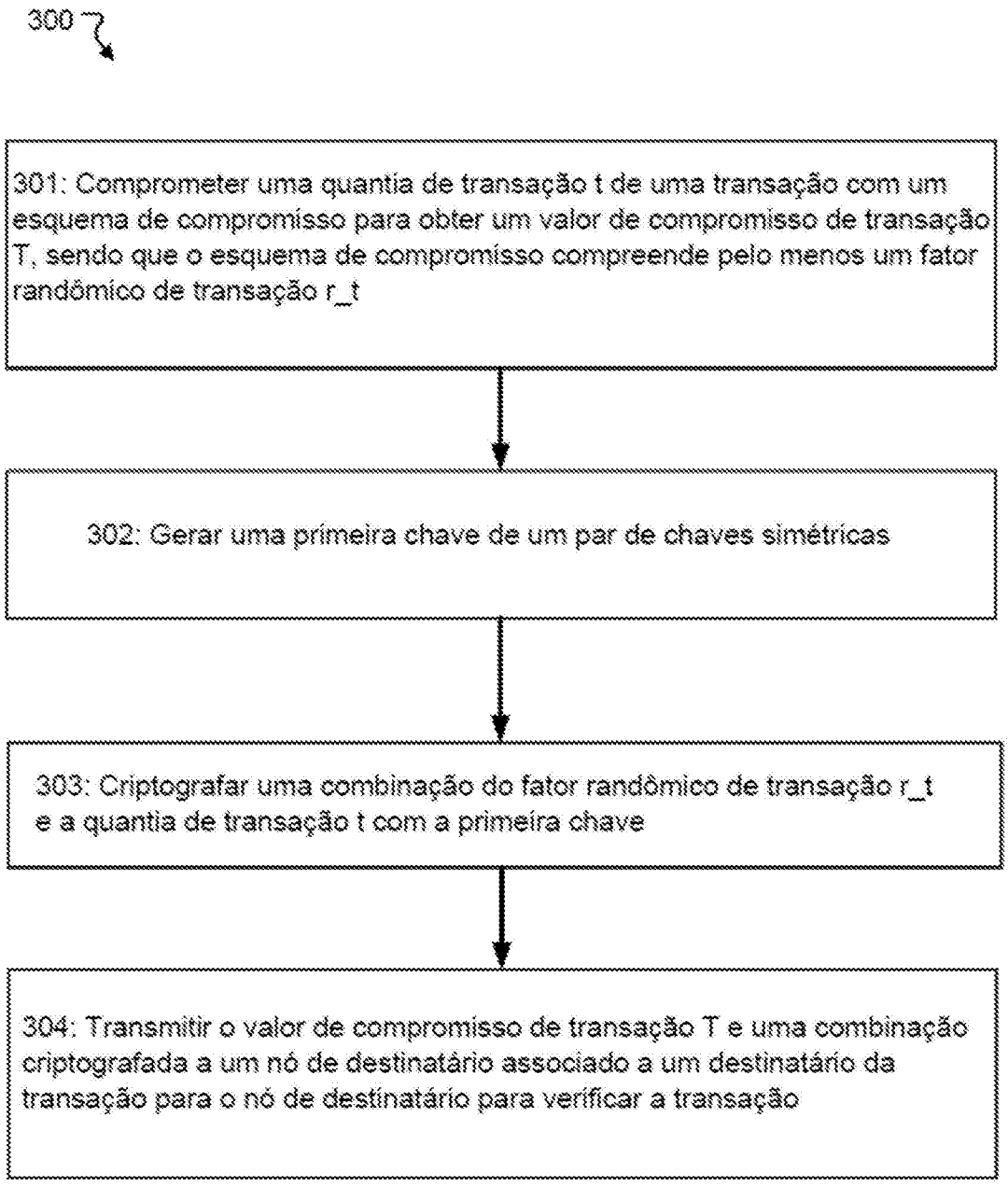

300
301: Comprometer uma quantia de transação t de uma transação com um esquema de compromisso para obter um valor de compromisso de transação T, sendo que o esquema de compromisso compreende pelo menos um fator randômico de transação r_t
302: Gerar uma primeira chave de um par de chaves simétricas
303: Criptografar uma combinação do fator randômico de transação r_t e a quantia de transação t com a primeira chave
304: Transmitir o valor de compromisso de transação T e uma combinação criptografada a um nó de destinatário associado a um destinatário da transação para o nó de destinatário para verificar a transação

FIG. 3A

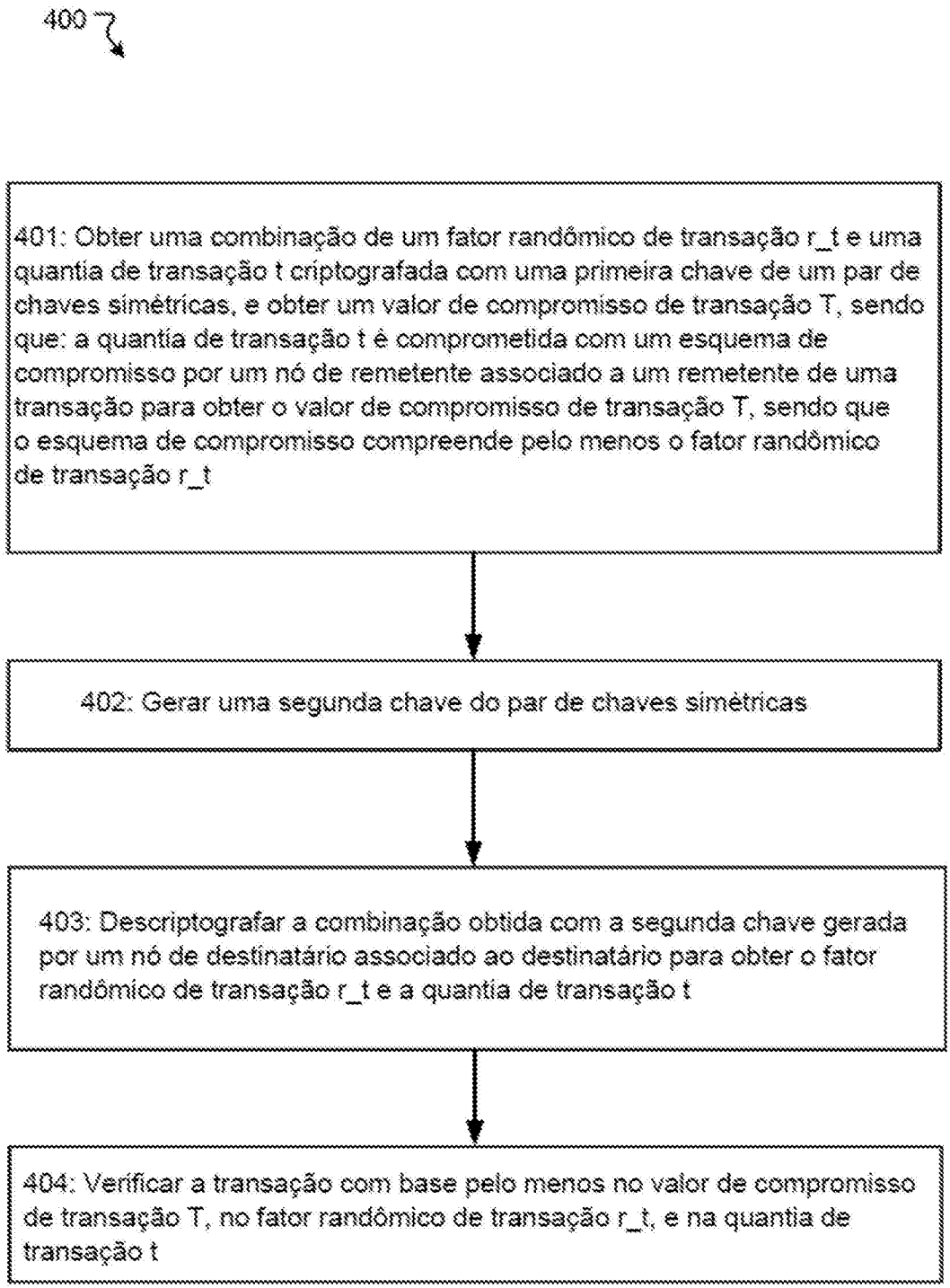

400
401: Obter uma combinação de um fator randômico de transação r_t e uma quantia de transação t criptografada com uma primeira chave de um par de chaves simétricas, e obter um valor de compromisso de transação T, sendo que: a quantia de transação t é comprometida com um esquema de compromisso por um nó de remetente associado a um remetente de uma transação para obter o valor de compromisso de transação T, sendo que o esquema de compromisso compreende pelo menos o fator randômico de transação r_t
402: Gerar uma segunda chave do par de chaves simétricas
403: Descriptografar a combinação obtida com a segunda chave gerada por um nó de destinatário associado ao destinatário para obter o fator randômico de transação r_t e a quantia de transação t
404: Verificar a transação com base pelo menos no valor de compromisso de transação T, no fator randômico de transação r_t, e na quantia de transação t

FIG. 3B

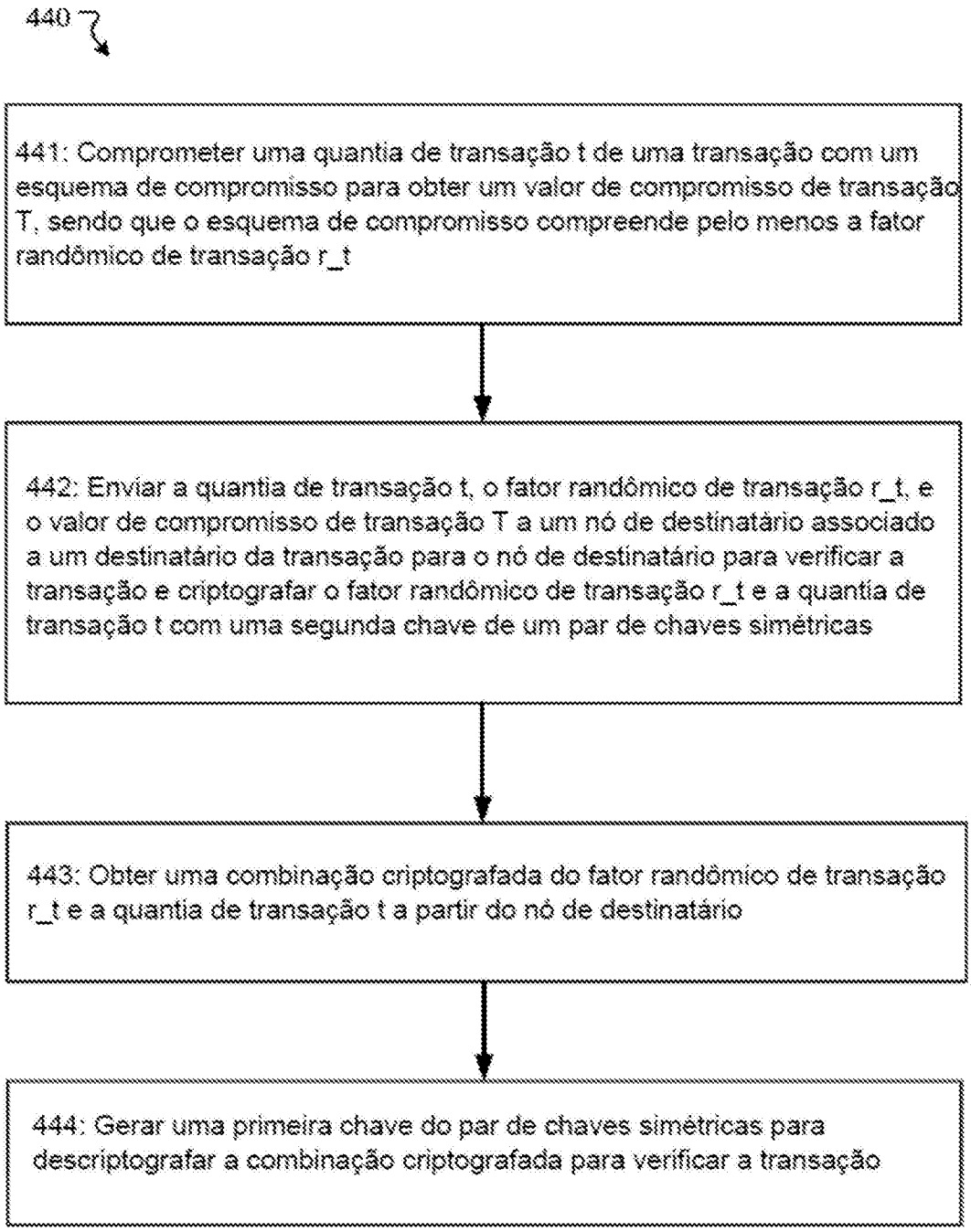

440
441: Comprometer uma quantia de transação t de uma transação com um esquema de compromisso para obter um valor de compromisso de transação T, sendo que o esquema de compromisso compreende pelo menos a fator randômico de transação r_t
442: Enviar a quantia de transação t, o fator randômico de transação r_t, e o valor de compromisso de transação T a um nó de destinatário associado a um destinatário da transação para o nó de destinatário para verificar a transação e criptografar o fator randômico de transação r_t e a quantia de transação t com uma segunda chave de um par de chaves simétricas
443: Obter uma combinação criptografada do fator randômico de transação r_t e a quantia de transação t a partir do nó de destinatário
444: Gerar uma primeira chave do par de chaves simétricas para descriptografar a combinação criptografada para verificar a transação

FIG. 4A

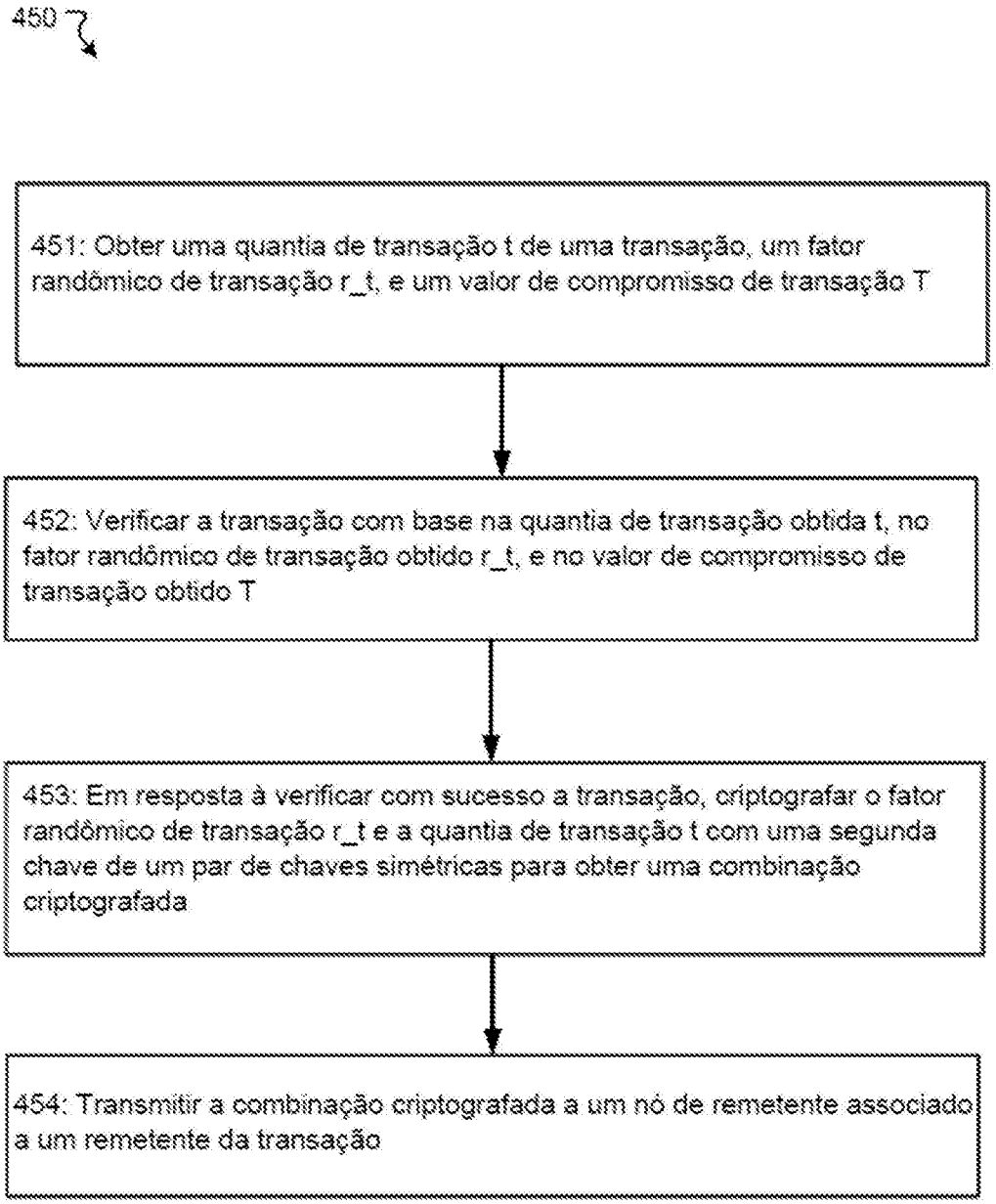

450
451: Obter uma quantia de transação t de uma transação, um fator randômico de transação r_t, e um valor de compromisso de transação T
452: Verificar a transação com base na quantia de transação obtida t, no fator randômico de transação obtido r_t, e no valor de compromisso de transação obtido T
453: Em resposta à verificar com sucesso a transação, criptografar o fator randômico de transação r_t e a quantia de transação t com uma segunda chave de um par de chaves simétricas para obter uma combinação criptografada
454: Transmitir a combinação criptografada a um nó de remetente associado a um remetente da transação

FIG. 4B

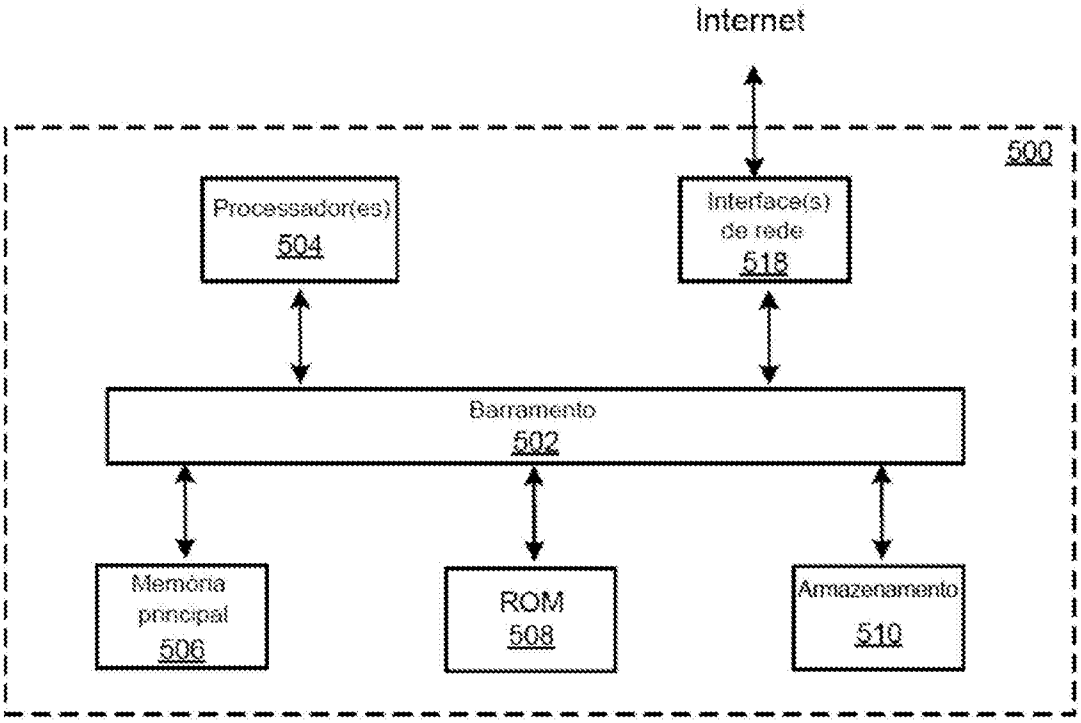

Internet
500
Processador(es)
504
Interface(s)
de rede
518
Barramento
502
Memória
principal
506
ROM
508
Armazenamento
510

FIG. 5

RESUMO

"SISTEMA E MÉTODO PARA PROTEÇÃO DE INFORMAÇÕES"

Trata-se de um método implementado por computador que compreende: comprometer uma quantia de transação de uma transação com um esquema de compromisso para obter um valor de compromisso de transação, sendo que o esquema de compromisso compreende pelo menos um fator randômico de transação; gerar uma primeira chave de um par de chaves simétricas; criptografar uma combinação do fator randômico de transação e uma quantia de transação t com a primeira chave; e transmitir o valor de compromisso de transação T e a combinação criptografada a um nó de destinatário associado a um destinatário da transação para o nó de destinatário para verificar a transação.